Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra Informačních Technologií

Analýza nástrojů pro automatizovanou analýzu a ošetření operačního systému Windows v případě napadení malware

Bakalářská práce

Autor: Jiří Hladík
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Tomáš Svoboda Ph.D.

Hradec Králové Listopad 2023

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne 10.11.2023 Jiří Hladík

Poděkování:

Rád bych poděkoval svému vedoucímu bakalářské práce Ing. Tomáši Svobodovi Ph.D. za trpělivost, odborné vedení a vstřícnost při konzultacích a vypracování mé práce. Rád bych také poděkoval své sestře za podporu při začátcích studentského života na vysoké škole Univerzity HK.

Anotace

Cílem této práce je představení problematiky analýzy nástrojů pro automatizovanou analýzu a ošetření operačního systému Windows v případě napadení malware. Pro uvedení do problematiky jsou popsány oblasti operačních systémů, zajištění bezpečnosti v operačních systémech, kybernetické hrozby a zranitelnosti s důrazem na možnosti ochrany proti napadení operačního systému a snížení rizika následných škod.

Annotation

Title: Analysis of tools for automated logging and treatment of the Windows operating system in case of malware infection

The aim of this thesis is to present the issue of analyzing tools for automated analysis and treatment of the Windows operating system in the event of a malware attack. To introduce the issue, the areas of operating systems, ensuring security in operating systems, cyber threats and vulnerabilities are described, with an emphasis on the possibilities of protection against operating system attacks and reducing the risk of subsequent damage.

Obsah

1 Úvod 1

2 Cíl práce 2

3 Teoretická část 3

3.1 Typy OS 4

3.1.1 Operační systém pro jednoho uživatele 4

3.1.2 Operační systém pro více uživatelů 9

3.2 Platforma Windows 13

3.2.1 Autentizace a autorizace uživatelů 13

3.2.2 Kontrola výkonu systému 13

3.2.3 Účetnictví práce 14

3.2.4 Podpora detekce chyb 14

3.2.5 Koordinace mezi softwarem a uživateli 14

3.2.6 Správa paměti 14

3.2.7 Správa procesoru 14

3.2.8 Správa zařízení 15

3.2.9 Správa souborů 15

3.3 Bezpečnost v OS 15

3.4 Hrozby 18

3.4.1 Počítačový Virus 18

3.4.2 Trojský kůň 18

3.4.3 Počítačový červ 19

3.4.4 Spyware 19

3.4.5 Ransomware 20

3.4.6 Spam 20

3.5 Možnosti ochrany OS 21

3.5.1 Antivirus 21
3.5.2 Anti-Spyware 22
3.5.3 Anti-Phishing 22
3.5.4 Skripty na míru 23
4 Praktická část 25
4.1 Sestavení virtuálního prostředí 25
4.1.1 Instalace VirtualBox 25
4.1.2 Tvorba instalačního média Windows 10 28
4.1.3 Instalace virtuálního stroje Windows 10 32
4.1.4 Konfigurace virtuálního stroje pro testování 35
4.2 Tron 39
4.2.1 Postup instalace Tron 39
4.2.2 Popis konfigurace čištění Tron skriptu 41
4.3 Popis infikace systému a jeho čištění 51
5 Závěry a doporučení 54
6 Seznam použité literatury 55
7 Přílohy 61

Seznam obrázků

Obrázek 1: Interakce jednoho uživatele s OS 4
Obrázek 2: Část stromové reprezentace distribucí Linuxu 9
Obrázek 3: Interakce více uživatelů s OS 10
Obrázek 4: Triáda CIA 16
Obrázek 5: Parkerianská Hexáda 17
Obrázek 6: Fungování virového skeneru: na vyžádání 21
Obrázek 7: Informační okno programu VirtualBox 25
Obrázek 8: Stránka VirtualBox 26
Obrázek 9: Uvítací okno VirtualBox 26
Obrázek 10: Okno přizpůsobení instalace 27
Obrázek 11: Varovné okno sítového připojení 27
Obrázek 12: Oznamovací okno chybějících balíčků 28
Obrázek 13: Uvítací okno programu VirtualBox 28
Obrázek 14: Stránka nástroje Microsoft 29
Obrázek 15: Uvítací okno nástroje 29
Obrázek 16: Dotazovací okno záměru instalace 30
Obrázek 17: Dotazovací okno parametrů instalace 30
Obrázek 18: Dotazovací okno způsobu instalace 31
Obrázek 19: Oznamovací okno splněné instalace 31
Obrázek 20: Počátek instalace virtuálního stroje v programu 32
Obrázek 21: Úvodní okno průvodce instalací 33
Obrázek 22: Okno pro bezobslužnou instalaci 33
Obrázek 23: Okno na nastavení Hardware 34
Obrázek 24: Okno na nastavení Virtuálního disku 34
Obrázek 25: Okno shrnutí nastavení virtuálního stroje 34
Obrázek 26: Okno instalace Windows 10 35
Obrázek 27: Okno plochy Windows 10 35
Obrázek 28: Spuštění Windows Update 35
Obrázek 29: Okno instalace aktualizací 35
Obrázek 30: Zapnutí funkce .NET Framework 36

Obrázek 31: Vstup do nastavení 37
Obrázek 32: Vytvoření sdílené složky 37
Obrázek 33: Okno shrnutí nastavení virtuálního stroje 38
Obrázek 34: Vytvoření snímku virtuálního stroje 38
Obrázek 35: Stránka TronScript v sociální síti Reddit 39
Obrázek 36: Postup stažení balíčku TronScript 40
Obrázek 37: Výsledek složek sdílení a Tron skriptu 41

Seznam tabulek

Tabulka 1: Funkce příprav skriptu Tron 42

1 Úvod

Toto téma bylo zvoleno za účelem testování a studie automatizovaných nástrojů pro kontrolu funkčnosti operačního systému Windows, který za napadením kybernetickým útokem může způsobit nejenom dočasnou, ale i permanentní škodu. Práce bude rozdělena na teoretickou a praktickou část. V teoretické části bude představen koncept operačních systémů spojenou s jejich historií. Budou nastíněny příklady platforem operačních systémů, jejichž způsob používání bude porovnáván. V pozdější kapitole se popíšou funkce platformy Windows důležité pro jeho chod. Následně se vysvětlí koncept bezpečnosti v operačním systému. Dále se vysvětlí základní pojmy kybernetických hrozeb operačních systémů a nastíní se jak známé, tak i alternativní možnosti jejich ochran. Na základě výstupů z teoretické části bude vybrán automatizovaný nástroj pro analýzu malwaru. Praktická část práce bude popisovat přípravu ideálního prostředí pro testování a čištění malware. V rámci přípravy budou popsány postupy vytvoření virtuálního prostředí a následně bude nastíněn postup konfigurace virtuálního stroje pro testování. V testování systému bude využit automatizovaného nástroje pro analýzu a ošetření hrozeb malware, tvořený ve skriptovacím jazyce. Přestaví se způsob jeho instalace a bude podrobně popsán v chronologickém sledu jeho chování. Na závěr praktické části se znázorní výstup automatizovaného nástroje za dané konfigurace virtuálního stroje.

2 Cíl práce

Cílem této práce je přednést obecné poznatky v oblasti informačních technologiích a také poučit o bezpečnosti v operačních systémech. Je dbán důraz na bezpečnost operačních systémů, jejich zranitelnost a v případech narušení bezpečnosti představit způsoby jejich náprav. Konkrétně v interakci s jinými počítačovými sítěmi, které mohou představovat bezpečností riziko.

3 Teoretická část

Operační systém je kolekce navzájem komunikujícího software. Tento software je nutnou výbavou počítačů, které mají za úkol správu počítačových komponent na fyzické úrovni a zajišťuje komunikaci s vnějším světem, ať je to uživatel pracující s operačním systémem, nebo sdílením informací mezi programy. Chová se jako fundamentální vrstva softwaru v počítači a hraje klíčovou roli při udržování bezpečnosti počítače.

Před vývojem operačních systémů se zpracováním dat v počítačích provádělo ručně, za použití děrných štítků a papírové pásky. Programy byly vytvářeny pomocí strojového jazyka nebo jazyka symbolických instrukcí a každý program bylo nutné nahrát do paměti počítače ručně pomocí přepínačů nebo jiných mechanických metod. Když byl program spuštěn, běžel do dokončení a pak by se načetl a provedl další program. Tento ruční proces byl pomalý a náchylný k chybám a nebyl proveditelný pro rozsáhlé výpočty. Největší potřeba rychlého zpracování dat bylo směřováno na sčítání lidu. Sčítání v době 1870 v Americkém institutu pro sčítání lidu bylo zapotřebí automatizace pomocí stroje, které by dokázal svázat několik děrných štítku dohromady, aby se usnadnilo a zrychlilo jejich počítání. První operační systémy byly vyvinuty k automatizaci těchto procesů, což uživatelům umožňuje efektivněji komunikovat s počítačem. [1]

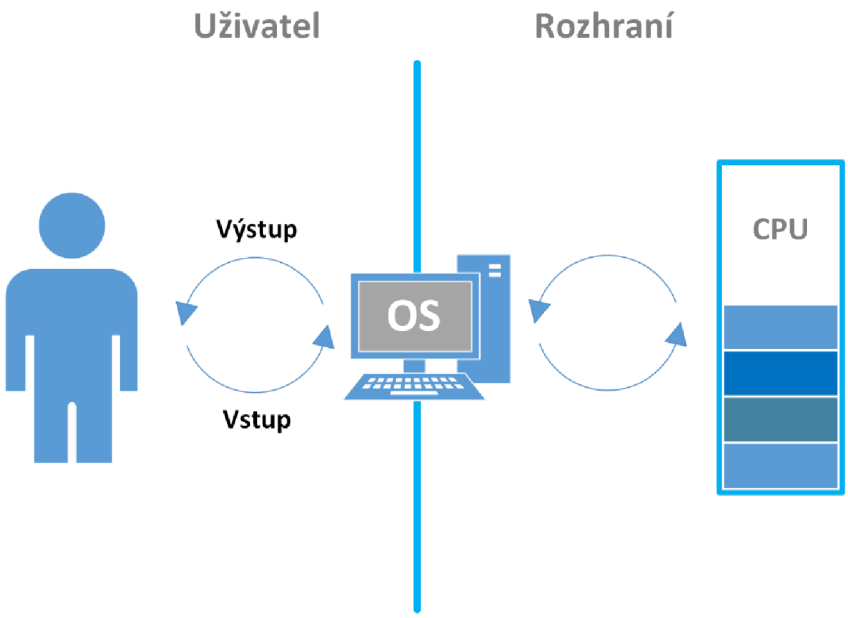
Pro správné fungování operačního systému je nezbytná vzájemná spolupráce vnitřních prostředků OS, které se řadí do základních charakteristik, určují jeho efektivitu, spolehlivost a použitelnost [2]:

- Spravování prostředků počítače a jejich přidělování aplikacím a procesům
- Spouštění, zastavování a plánování procesů včetně komunikace mezi nimi
- Organizace paměti podle potřeby různých procesů
- Souborový systém pro správu ukládání a načítání dat souborů.
- Uživatelské rozhraní pro interakci s počítačem
- Bezpečnostní mechanismy k ochraně počítače a jeho dat
- Síťové funkce umožňující komunikaci s jinými zařízeními v síti

3.1 Typy OS

3.1.1 Operační systém pro jednoho uživatele

Operační systém pro jednoho uživatele je operační systém navržený tak, aby jej mohl současně používat jen jeden uživatel, který se obvykle instaluje na osobní počítače a pracovní stanice. Tento systém se liší od víceuživatelských operačních systémů, které umožňují více uživatelům přistupovat ke stejnému počítači nebo síti současně.



Obrázek 1: Interakce jednoho uživatele s OS
Zdroj: vlastní zpracování dle [3]

Poskytuje jednoduché a uživatelsky přívětivé výpočetní prostředí, kde má uživatel plnou kontrolu nad systémem a jeho prostředky. Tento typ operačního systému se obvykle používá pro osobní počítače jako je procházení webu, e-mail, vytváření dokumentů a konzumace médií. Pokud se zaměříme na zabezpečovací stránku tohoto systému, tento systém poskytuje relativně bezpečné výpočetní prostředí, protože do systému má přístup pouze jeden uživatel. To snižuje pravděpodobnost narušení zabezpečení způsobeného více uživateli, kteří přistupují ke stejnému počítači a potenciálně zavádějí malware, viry nebo jiný škodlivý software. [3] Na druhou stranu také představuje některá bezpečnostní rizika, zejména v oblastech autentizace uživatelů a ochrany dat. Pokud jsou například prozrazeny přihlašovací údaje uživatele, může útočník snadno získat přístup k celému systému a jeho datům.

Díky této chybě se nastává situace, kde systém může být zranitelný vůči krádeži, ztrátě nebo poškození, protože obvykle ukládá všechna uživatelská data lokálně a uživatel nepřistoupil k pravidelné záloze svých dat nebo nepoužívá vhodná bezpečnostní opatření. Toto řešení se zaměřuje na oblast osobních počítačů a nedoporučuje se pro podnikové nebo kritické aplikace, kde je prvořadá bezpečnost a spolehlivost.

3.1.1.1 Windows

Microsoft Windows je stále dominantním operačním systémem v odvětví osobních počítačů s bohatou historií trvající více než tři desetiletí. Od svého vzniku prošel Windows významnými změnami, přičemž každá generace zavedla nové funkce a pokrok v technologii, díky čemuž se stal jedním z celosvětově nejrozšířenějších operačních systémů. [4]

Vývoj Windows začal v roce 1981, kdy spoluzakladatel Microsoftu Billu Gatesovi viděl příležitost vytvořit grafické uživatelské rozhraní (GUI) pro osobní počítače. První verze Windows, Windows 1.0, byla vydána v roce 1985 a zavedla použití myši k navigaci v počítači. V průběhu let následující verze systému Windows, včetně Windows 2.0, Windows 3.0 a Windows 3.1, nadále zlepšovaly uživatelské rozhraní, výkon a stabilitu. V roce 1995 vydal Microsoft Windows 95, což byl významný milník v historii Windows. Představil nový hlavní panel a nabídku Start, což byly ve své době revoluční funkce. Následovaly Windows 98, Windows 2000 a Windows ME, přičemž každá verze přidala nové funkce a vylepšení. V roce 2001 Microsoft vydal Windows XP, který byl pravděpodobně jednou z nejpopulárnějších a nejstabilnějších verzí Windows. Představoval nový vizuální styl, vylepšený výkon a vylepšené zabezpečení. Zahrnovala jí například podporu bezdrátové sítě, nástroje pro internet a obsluhu videa, fotek a hudby. Windows Vista vydal Microsoft v roce 2006 jako nástupce Windows XP. Představila nové uživatelské rozhraní s názvem Aero, které mělo průhledné rámy oken. Dalšími funkcemi doprovázelo zlepšené vyhledávání a nový multimediální přehrávač. Vista však měla problémy s výkonem a byla kritizována za kompatibilitu se starším softwarem a hardwarem. [5]

V roce 2009 Microsoft vydal Windows 7 a jako nástupce systému Windows Vista byl navržen tak, aby reagoval na mnoho výtek a stížností, které uživatelé s Vistou měli.

Měl vylepšený výkon, stabilitu a funkce zabezpečení, jako je například vylepšený Taskbar, kde se programy jeví jako ikony a rychlejší odezva hledání souborů pomocí indexace. Windows 7 byl také verzí Windows, která poprvé podporovala vícedotykovou interakci, díky čemuž byla přístupnější pro zařízení s dotykovou obrazovkou. [6]

Microsoft Windows 8 byl vydán v roce 2012 s cílem přinést do operačního systému moderní dotykové rozhraní. Návrh se soustředil kolem rozhraní Metro, které bylo optimalizováno pro interakci pomocí dotyku a obsahovalo velké dlaždice představující aplikace a informace. Windows 8 také zavedl vylepšení doby spouštění a výkonu a také podporu nového hardwaru, jako je USB 3.0 a možnost spuštění systému pod architekturou procesorů firmy ARM. [7]

Windows 8 však obdržel smíšenou odezvu od uživatelů a kritiků. Mnoho z nich bylo frustrováno odstraněním tradiční nabídky Start a zavedením panelu Charms, který byl optimalizován pro dotykové zadávání, ale pro uživatele klávesnice a myši byl méně intuitivní. K vyřešení těchto problémů vydal Microsoft v roce 2013 Windows 8.1, který obnovil tlačítko Start a zavedl další vylepšení použitelnosti v rámci rychlejšího spuštění, snížení spotřeby baterií u laptopů a celkově nižší stopu na kapacitu disku. [8]

Jako jeho nástupce byl vydána v roce 2015 nová verze Windows 10. Cílem Windows 10 bylo reagovat na některé kritiky Windows 8 tím, že vrátil nabídku Start a začlenil funkce, které by se mohly přizpůsobit široké škále zařízení, včetně stolních počítačů, tablety a smartphony. Windows 10 také představil řadu nových funkcí, jako je virtuální asistentka Cortana, prohlížeč Microsoft Edge a možnost spouštět univerzální aplikace na více typech zařízení. Mezi další vylepšení patřily lepší funkce zabezpečení Windows Hello. [9] I po vydání nových potomků skupiny Windows se Windows 10 stále řadí mezi nejpoužívanější operační systémy. [10]

Windows 11 je nejnovější verze operačního systému Windows vydaná v roce 2021. Byla oznámena v červnu 2021 se zaměřením na nový designový jazyk nazvaný „Windows 11 UI“, který zahrnoval nové vizuální prvky, jako je vycentrovaná nabídka Start, Hlavní panel a nové ikony. Windows 11 byl také navržen tak, aby fungoval na různých zařízeních, včetně notebooků, stolních počítačů a tabletů. Kromě vizuálních změn obsahuje Windows 11 několik nových funkcí, jako je vylepšený multitasking a

virtuální desktopy, nová integrace Microsoft Teams a podpora aplikací pro Android prostřednictvím Amazon Appstore. Windows 11 také představil zefektivnění mechanismu doručování aktualizací. [11]

3.1.1.2 Mac OS

MacOS je operační systém vyvinutý a uváděný na trh společností Apple Inc. pro její řadu osobních počítačů Macintosh. Má bohatou historii, která se datuje od představení prvního Macintoshe v roce 1984, který obsahoval první verzi MacOS, známou jako System 1.0 [12]. V průběhu let prošel MacOS řadou změn a upgradů, včetně změn uživatelského rozhraní, základní technologie a kompatibility hardwaru. Jedním z nejvýznamnějších milníků v historii MacOS bylo vydání Mac OS X v roce 2001, což bylo zásadní přepracování operačního systému, který zahrnoval architekturu založenou na Unixu a představil několik nových funkcí, jako je rozhraní Aqua, které je navrženo tak, aby bylo intuitivní a snadno použitelné. Toto rozhraní se stále používá v moderních verzích MacOS. [13]

Další klíčovou vlastností MacOS je jeho integrace s dalšími produkty a službami Apple, jako je iCloud, který uživatelům umožňuje ukládat a synchronizovat své soubory na více zařízeních [14]. MacOS navíc obsahuje funkce, jako je AirDrop, který umožňuje snadné sdílení souborů mezi zařízeními Apple, a Handoff, který uživatelům umožňuje bezproblémový přechod mezi jejich Macem a jinými zařízeními Apple [15].

3.1.1.3 Unix

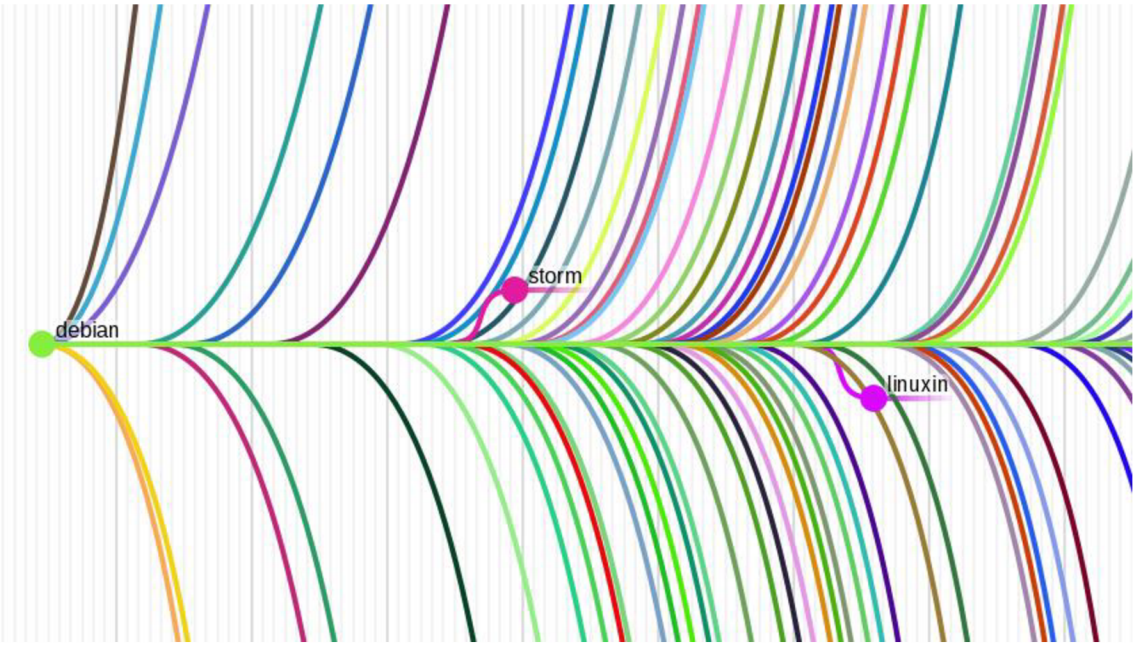
Ke konci 60. let firma Bell Labs, dříve výzkumná a vývojová divize AT&T, se zaměřila na vývoj operačního systému pro sdílení času pro sálové počítače. Jedni z výzkumníků byl Ken Thompson a Dennis Ritchie a v roce 1969 začali pracovat na jednodušší a praktičtější alternativě svého předchůdce Multics, což nakonec vedlo k vytvoření Unixu. Ken Thompson napsal v jazyce assembly počáteční verzi Unixu na minipočítači PDP-7 a se spoluprací s vývojářem programovacího jazyka C Dennisem Ritchiem, byli budoucí verze systému Unix přepsán v onom jazyce C. Díky programovacímu jazyku C byl Unix vysoce přenosný a umožnil jeho běh na různých hardwarových platformách. [16]

Název “Unix" je odvozen od slovní hříčky s operačním systémem "Multics", který je kombinací slov "Uniplexed Information and Computing Service", což dává důraz na jednoduchost a koncept operačního systému pro jednoho uživatele. [17]
Verze 6 Unix, vydaná v roce 1975, obsahovala významné funkce, jako je hierarchický souborový systém, roury pro meziprocesovou komunikaci a textový editor vi. [16]
Unix verze 7, vydaná v roce 1979, dále zdokonalila a rozšířila systém a představila klíčové komponenty jako je Bourne shell a kompilátor C. [18] Po vydání V7 byly vyvinuty varianty Unixu, ze kterých každá má vlastní sadu funkcí a vylepšení.
Jedna z variant zahrnuje BSD Unix vyvinutý z kódové báze Unixu verze 6 a 7, a zavedl řadu vylepšení a inovací v rámci síťových schopností v Unixu. Představila rozhraní Berkeley sockets a integrovalo síťové protokoly TCP/IP do Unixu. [19]
Další větví Unixu se stal System V. Tento systém disponoval meziprocesové komunikaci a synchronizaci za pomoci mechanismů. Mechanismus message queues zajišťuje komunikaci mezi procesy za pomocí zpráv, u které čtenář musí dostat zprávu celou oproti mechanismu pipes ve formě nedefinovaného bajtového proudu. Mechanismus semaphores spravuje synchronizaci akcí procesů, aby zabránil přístup k bloku sdílené paměti v okamžiku, kdyby ho jiný proces v daný moment aktualizoval. Shared memory umožnuje procesům vytvořit oblast paměti, ve kterém je změna registrována pro ostatní procesy. [20]

3.1.1.4 Linux

V roce 1983 Richard Stallman zahájil projekt GNU, jehož cílem bylo vytvořit svobodný a otevřený operační systém. Stallman vyvinul různé komponenty, včetně GNU General Public License (GPL). Projektu však chybělo jádro, klíčová součást operačního systému. [21]
Linuxové jádro, s více než 8 miliony řádků kódu a více než 1000 přispěvatelů ke každé verzi, je jedním z největších a nejaktivnějších projektů svobodného softwaru. Od svých skromných počátků v roce 1991 se toto jádro vyvinulo v prvotřídní komponentu operačního systému, které běží na kapesních digitálních přehrávačích, stolních počítačích, největších superpočítačích na světě a všech typech systémů mezi tím. Je to robustní, efektivní a škálovatelné řešení pro téměř každou situaci. [22]

Aby byl Linux dostupnější, různé skupiny zabalily linuxové jádro s dalším softwarem a vydaly kompletní operační systémy známé jako linuxové distribuce. Tyto distribuce zahrnovaly další software, jako jsou systémové nástroje, knihovny a grafické desktopové prostředí. Příklady populárních distribucí Linuxu zahrnují Red Hat, Debian a Ubuntu. [21]



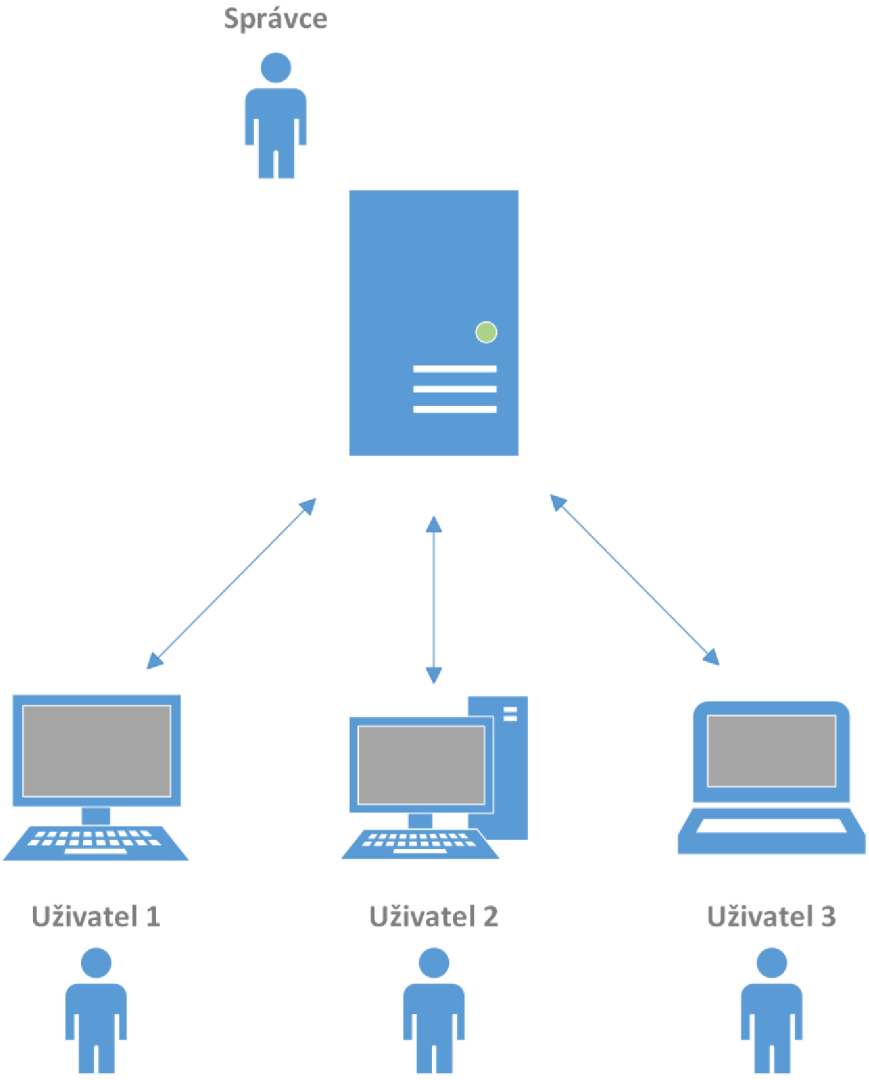
Obrázek 2: Část stromové reprezentace distribucí Linuxu
Zdroj: upraveno dle [23]

Linux ztělesňuje principy hnutí open-source, které vychází z principů spolupráce, transparentnosti a svobody. Otevřenost Linuxu umožňuje komunitně řízený vývoj, kde zdrojový kód je volně přístupný, upravitelný a šiřitelný. Kdokoli může přispět svými úpravami, opravami chyb, přidáním nových funkcí a zlepšováním výkonu. Zdrojový kód Linuxu je přístupný všem, což podporuje transparentnost. To umožňuje jednotlivcům porozumět fungování systému, identifikovat zranitelnosti a navrhovat vylepšení. Filozofie otevřeného zdrojového kódu Linuxu podporuje inovace tím, že povzbuzuje experimentování a přizpůsobování. Vývojáři mohou přizpůsobit Linux svým potřebám, což vede k diverzifikaci distribucí. [24]

3.1.2 Operační systém pro více uživatelů

Tento typ operačního systému je navržený na užití více uživatelům přistupovat ke stejnému počítači nebo síti současně. Běžně se používá v podnikových a organizačních prostředích, kde oproti domácímu prostředí se běžně sdílejí zdroje,

jako jsou soubory, aplikace a databáze. Více uživatelů s přístupem ke stejným datům a aplikacím dokážou spojit síly za dosažení efektivnějšího dokončení projektů a provedení více komplexních úkolů.



Obrázek 3: Interakce více uživatelů s OS
Zdroj: vlastní zpracování dle [25]

Obvykle využívá různé mechanismy pro správu přístupu uživatelů a alokaci zdrojů, jako je autentizace uživatelů, řízení přístupu, plánování procesů a správa paměti. Uživatelé musí například pro přístup do systému poskytnout platná pověření, jako je uživatelské jméno a heslo. Po ověření jsou uživatelům udělena specifická oprávnění a oprávnění na základě jejich role a odpovědnosti. Kromě toho využívá plánování procesů pro přidělování časových a paměťových zdrojů mezi konkurenční procesy a uživatele, což zajišťuje spravedlivé a efektivní využití

systémových zdrojů. Vzhledem k povaze sdílení počítačových prostředků je nutné dbát na výší úroveň zabezpečení, aby se zamezilo narušení systému. Pokud by se dostalo k narušení systému formou infikace počítačovým virusem, dokázala by se infikace rozšířit mezi další propojené počítače v síti. [26]

3.1.2.1 Windows Server

Při tvorbě IT infrastruktury mezi společností poskytující služby a jejími klienty využívající tyto služby je zapotřebí data centra obsahující servery. Od správy emailů, sdílení souborů po aplikaci virtuálních desktopů a správy databází, servery poskytují možnost splnění úloh zadané společností [27].

Firma Microsoft umožnuje tvorbu infrastruktury za pomocí proprietárního platformy Windows Server a poskytuje služby organizacím podle jejich potřeb. Na rozsah uspokojení potřeb jsou nabízeny edice. Edice Standard je vhodná pro malé a střední podniky, zatímco edice Datacenter je určena pro rozsáhlou virtualizaci a nasazení cloud computing[1]. Edice Essentials se zaměřuje na malé podniky s méně než 25 uživateli a poskytuje zjednodušenou správu a integraci s cloudovými službami např. Microsoft 365. [28]

Windows Server nabízí možnost konfigurovat funkce serveru tak, aby vyhovovaly konkrétním úkolům a požadavkům organizace. Jedním z úkolům může být konfigurace sdílení úložiště souborů v síti, které Windows Server zajišťuje jednoduché spravování dat a přístupu k nim. Zajištuje jí řešení Storage Spaces Direct, jejímž úkolem je kombinace interních úložných jednotek ve fyzických serverech. S kombinací jednotek je spravována ve formě virtuálního fondu uložiště. Z fondu se dají vytvářet svazky úložiště, na které se souborový server dokáže přes sít umožnit jejich sdílení. [29]

Další funkcí Windows Server spočívá strukturovat informace o objektů v síti. Active Directory Domain Services (AD DS) je příkladem adresářové služby, která spravuje data a zpřístupňuje je uživatelům a správcům. Ukládá podrobnosti, jako jsou uživatelské účty, hesla a telefonní čísla, což umožňuje oprávněným uživatelům v síti

[1] Cloud computing je možnost zákazníků využívat infrastruktury firem a používání aplikací, aniž by je museli sami instalovat, anebo udržovat

přístup k těmto informacím. Služba Active Directory organizuje data logickým, hierarchickým způsobem, což správcům a uživatelům zjednodušuje hledání a použití uložených informací. Integruje také bezpečnostní funkce pro ověřování a řízení přístupu, což i u komplexních sítích umožňuje správu dat a zdrojů za pomocí jediného přihlášení. [30]

3.1.2.2 Unix Server

Mezi dlouholeté soupeře v oblasti operačních systémů pro více uživatelů patří systém Unix [16].

S jeho širokou kompatibilitou je používán v kriticky důležitých úlohách, jakož hraje roli páteře internetu. Pracuje za pomocí protokolů TCP/IP pro síťovou komunikaci a SMTP pro funkci e-mailu. [31]

Unix potýká se sníženou poptávkou způsobenou migrací z počítačových platforem s redukovanou instrukční sadou na alternativy na bázi x86, jelikož vlastní výhody rychlejšího zpracování úloh za menší cenu. I po postupném útlumu je Unix stále preferovaným systémem pro případy aplikací datových center. [32]

Další alternativou verzi Unixu představila firma Apple serverovou variantu Mac OS X Server. Jeho implementace je postavená z distribuce FreeBSD, u jaké se pyšní funkcemi kompilace a spuštění existujícího kódu Unixu, a lze ho proto nasadit v prostředí vyžadující plnou kompatibilitu. Díky Unixové architektuře se Mac OS X Server poskytuje správcům nástroje pro správu služeb bez možnosti připojení na displej serveru. Obsahuje pro administraci nástroje zabezpečení, jakož může být spojení přes internet přes protokol SSH. [33]

V roce 2022 se firma Apple rozhodla Mac OS X Server ukončit provoz a stávající zákazníci mohou i nadále stahovat a používat aplikaci s macOS Monterey [34].

3.1.2.3 Linux Server

Linux se po vývoji linuxového jádra rozvětvil do distribucí a je považován za jeden z nejstabilnějších, nejbezpečnějších a nejspolehlivějších operačních systémů. Je široce používán na serverech, superpočítačích a podnikových prostředích. [21]

Jednou z technologií myšlenky Linux Server je správa webového obsahu Apache HTTP Server podporovaný Apache Software Foundation. Jeho otevřený zdrojový

kód a stabilita ho učinily jedním z oblíbených operačních systémů pro servery v celém světě. [35]
Díky své modulární architektuře a schopnosti provádět zatížení a rovnoměrné rozložení zajišťuje Apache bezpečný a efektivní provoz webových aplikací. [36]

Následující kapitola je zaměřená na jeden z nejrozšířenějších operačních systémů na světě od firmy Microsoft, tj. Microsoft Windows.

3.2 Platforma Windows

Nový příspěvek k operačním systémů z rodiny NT je označován pod názvem Windows 10, které se od jeho doby vydání byl oznámen firmou Microsoft: *„jsme nadšeni oznámit, že přes 1 miliardu lidi si zvolilo Windows 10 přes 200 zemí, ve kterém vyplývá přes více než 1 miliardu aktivních zařízení Windows 10*“ [37].
Na úvod do operačních systémů je nutné se podívat na jednotlivé funkce, které jsou důležité pro chod systému, se zaměřením na systémy skupiny Windows. Hlavním úkolem operačního systému je správná alokace prostředků, paměti, zařízení a informací. Informace ke kapitolám od 4.2.1. do 4.2.9. byly přejaté z [38].

3.2.1 Autentizace a autorizace uživatelů

Operační systém využívá ochranu za použití hesla, aby se zajistila ochrana dat uživatele a další podobné techniky. Také zabraňuje neautorizovaný přístup k programům a uživatelských datech.

3.2.2 Kontrola výkonu systému

Monitoruje celkové zdraví systému pro zajištění vylepšení výkonu. Zaznamenává dobu odezvy mezi požadavky na službu a odezvou systému, aby měl úplný přehled o stavu systému. To může pomoci zlepšit výkon poskytnutím důležitých informací potřebných k řešení problémů.

3.2.3 Účetnictví práce

Operační systém sleduje čas a prostředky využívané různými úkoly a uživateli. Tyto informace lze použít ke sledování využití zdrojů pro konkrétního uživatele nebo skupinu uživatelů.

3.2.4 Podpora detekce chyb

Operační systém neustále monitoruje systém, aby zjistil chyby a zabránil selhání počítačového systému.

3.2.5 Koordinace mezi softwarem a uživateli

Operační systémy také koordinují a přidělují interprety, kompilátory, assemblery a další software různým uživatelům počítačových systémů.

3.2.6 Správa paměti

Operační systém spravuje primární paměť nebo hlavní paměť. Hlavní paměť se skládá z velkého pole bajtů nebo slov, kde je každému bajtu nebo slovu přiřazena určitá adresa. Hlavní paměť je rychlé úložiště a lze k ní přistupovat přímo z procesoru. Aby byl program spuštěn, měl by být nejprve načten do hlavní paměti. Operační systém provádí pro správu paměti následující činnosti:

- Sleduje primární paměť, tj. které bajty paměti používá který uživatelský program. Adresy paměti, které již byly přiděleny, a adresy paměti, která ještě nebyla použita. Při multiprogramování rozhoduje OS o pořadí, ve kterém je procesům udělen přístup k paměti, a na jak dlouho.
- Přiděluje paměť procesu, když to proces požaduje, a uvolňuje paměť, když se proces ukončí nebo když se provádí I/O operace.

3.2.7 Správa procesoru

V prostředí s větší škálou programovacích jazyků rozhoduje OS o pořadí, v jakém mají procesy přístup k procesoru, a jak dlouhou dobu zpracování má každý proces. Tato funkce OS se nazývá plánování procesů. Operační systém provádí následující činnosti pro správu procesoru:

- Sleduje stav procesů. Program, který provádí tento úkol, se nazývá I/O dopravní kontrolor.
- Přiděluje procesu dostupné jádro procesoru.
- Zruší přidělení procesoru, když proces již není potřeba.

3.2.8 Správa zařízení

Dále operační systém spravuje komunikaci zařízení prostřednictvím příslušných ovladačů. Provádí následující činnosti pro správu zařízení:

- Sleduje všechna zařízení připojená k systému.
- Označuje program zodpovědný za každé zařízení známé jako Input/Output Controller.
- Rozhoduje, který proces získá přístup k určitému zařízení a na jak dlouho.
- Přiděluje zařízení efektivním a účinným způsobem.
- Odpojuje zařízení, když již nejsou potřeba.

3.2.9 Správa souborů

Souborový systém je organizován do adresářů pro efektivní nebo snadnou navigaci a použití. Tyto adresáře mohou obsahovat další adresáře a jiné soubory. Operační systém provádí následující činnosti správy souborů:

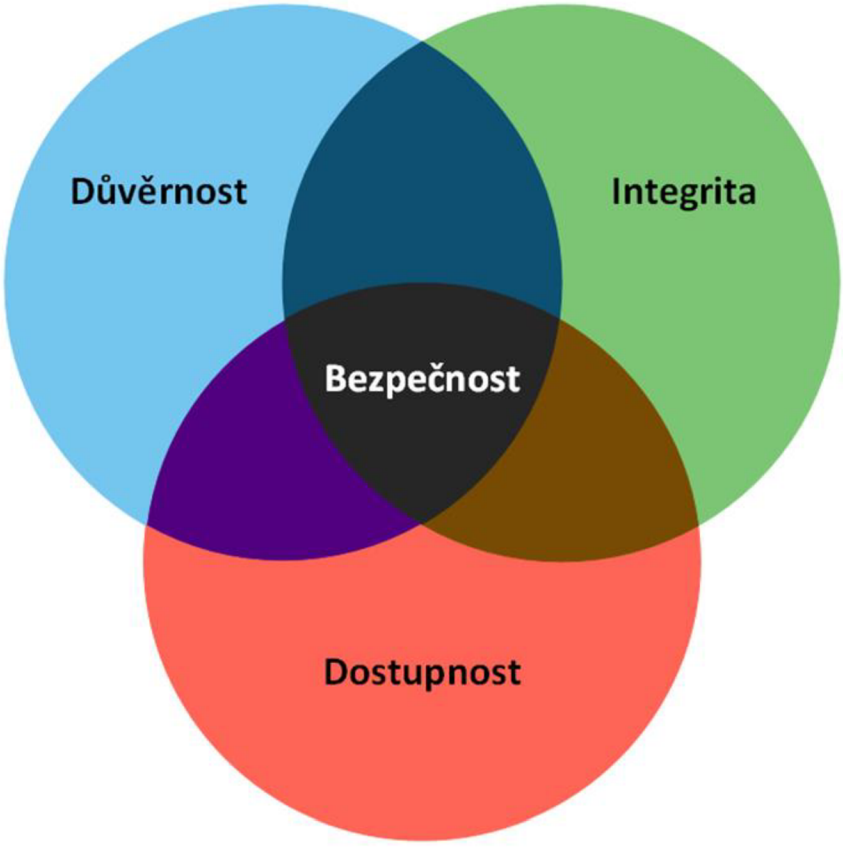
- Sleduje, kde jsou informace uloženy
- Nastavuje uživatelského přístupu a stav každého souboru

Tyto funkce jsou souhrnně známé jako souborový systém.

3.3 Bezpečnost v OS

Bezpečnost jakékoliv zařízení a jejího operačního systému je v dnešní době z cela zásadní. V dnešní době kvůli vysoké integraci internetových služeb a využití softwarových balíčků, které jsou z většiny ze třetích stran, se zvyšuje riziko napadení neznámým útočníkem. To neznamená ve smyslu přímého fyzického napadení, ale použití prostředků dostupný v programovém vybavení operačního

systému. Pro zajištění základní bezpečnosti informací je využívána triáda informační bezpečnosti CIA[2].



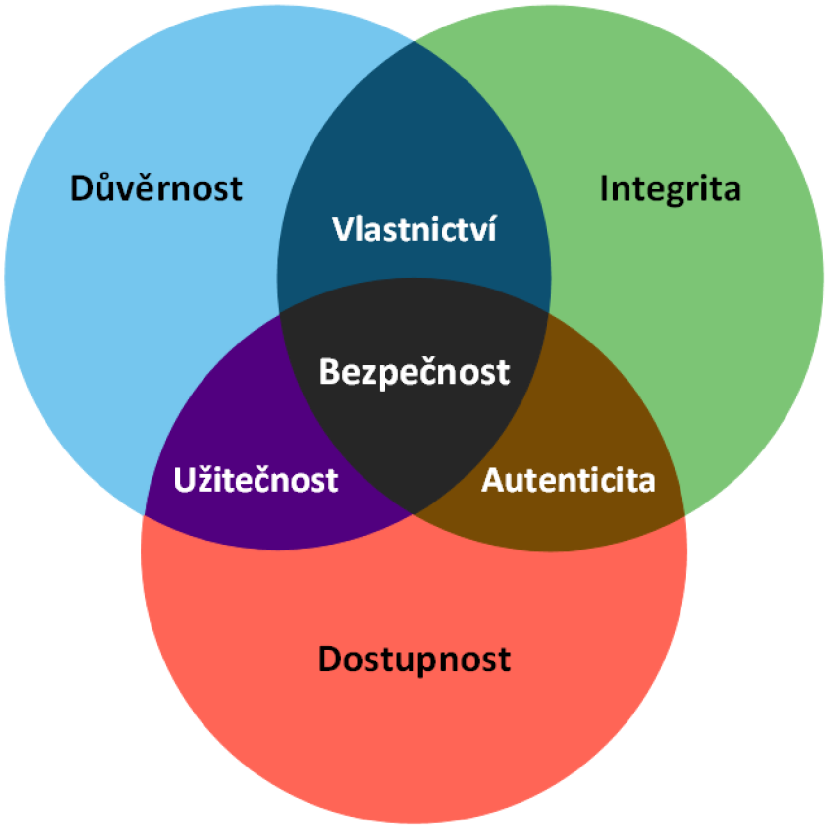
Obrázek 4: Triáda CIA
Zdroj: vlastní zpracování dle [39]

Tomuto konceptu se věnoval Donn B. Parker r. 1998. V konceptu jsou zahrnuty tři atributy ochrany informací. Jedním z nich je důvěrnost, kde se u informace předpokládá, že její obsah není odhalen, nebo odcizen neoprávněným jedincem, entitám, nebo procesům. U integrity je dbát ohled na přesnost a úplnost. Kupříkladu integrita dat znamená, že informace jako data v jistotě nebyla změněná a neztratily jejich platnost. Na atribut dostupnosti se nejčastěji definuje jako zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby. [40]

CIA triáda byla využita na příklad nastavení parametrů bezpečnosti informačních systémů pro zajištění národní bezpečnosti USA. Vzhledem k faktům, že počítače byli

[2] Zkratka je složená ze tří slov: confidentiality (důvěrnost), integrity (integrita) a availability (dostupnost)

velmi drahé a fyzický přístup k nim byl velmi omezený, a tedy hrozba ztráty důvěrnosti, dostupnosti a integrity byla minimální, nebyla CIA triáda často aplikována v praxi. S touto věcí byl dbán ohled na bezpečnost dat pouze v oblasti integrity systému, jelikož hrozby nebyly rozšířené, hlavní pozorností byla samotná spolehlivost systému. Ve výsledku, ochrana informací byla dosažena pomocí kontroly fyzického přístupu k počítačům. [41]



Obrázek 5: Parkerianská Hexáda
Zdroj: vlastní zpracování dle [39]

Ke stávajícímu modelu se připojily další tři atributy, které obohacují a upřesňují ochranu informací. K přejetí nových atributů se název modelu se šesti atributy nazývá Parkeriánská Hexáda[3].

Prvním přidaným atributem je vlastnictví, popřípadě kontrola. Tento atribut se zaměřuje na to, kdo nebo co má kontrolu nad informacemi a jakým způsobem jsou

[3] Z důvodu nedostatku českých termínů byl použit vlastní překlad nově přidaných atributů Parkeriánské Hexády: possesion/control (vlastnictví), authenticity (autenticita), utility (užitečnost)

tyto informace spravovány. U atributu autenticity je kladen důraz zhodnocení pravdivosti a věrohodnosti informací a zda informace pocházejí ze spolehlivých a důvěryhodných zdrojů. Atribut užitečnosti poukazuje, v jaké formě jsou informace předkládány a jakým způsobem jsou užitečné vzhledem k jejich dostupnosti. [42]

3.4 Hrozby

Kyberbezpečností firma Trellix podala prognózu v roce 2022 o stavu kyberútoků, kde aktéři pokračuji s výzvou použití ransomware, kde organizace více závisí na zaměstnancích, kteří pracují ze vzdálených míst, jako jsou jejich domovy nebo jiná místa mimo pracoviště, aby plnili své pracovní povinnosti. V hlášení stálo, že aktéři s jejich větším odhodláním způsobují větší škody. Průměr žádostí ransomware se zvýšil z $5000 v roce 2018 na okolo $200000 v roce 2020. [43]

V internetové bezpečnosti jsou hrozby kategorizované do oblasti tzv. tříd malware. Malware (zkr. Malicious software) má různé podoby, kde jejím cílem je použití škodlivého kódu, který se dokáže dostat k citlivým údajům vlastníka počítačového systému bez jeho vědomí a bez jeho souhlasu. Informace ke kapitolám 3.4.1 a 3.4.5 byly přejaté z [44], [45] a ke kapitolám 3.4.3 a 3.4.6 byly přejaté z [46] a ke kapitole 3.4.2 byla přejata z [47].

3.4.1 Počítačový Virus

Virus je jeden z nejznámějších druhů malware. Stejně jako virus v lidském organismu, virus v počítačovém systému dokáže znepříjemnit uživateli život. Jeho hlavní schopností je infikovat a oklamat bezpečností prvky operačního systému a s převzetím tohoto systému má nad ním kontrolu. Ke vzniku této zranitelnosti může docházet velmi snadno. Uživatel může obdržet infikovaný soubor v příloze emailu, nebo ho získat pouhým stažením z internetu. Po následku napadení se virus a jeho škodlivý kód mohou kopírovat do dalších souborů.

3.4.2 Trojský kůň

Jak již můžeme znát z řecké mytologie báji o dobití města Troja, kde se pod vedením Odysea použil válečný stroj v podobě koně jako dar. Tímto darem se zajistilo oklamání nepřátelských Trojanů. Touto válečnou lstí se zajistilo jejich zaručenou

porážku. V informatice se trojský kůň chová stejně, jako jeho řecký protějšek, kde se škodlivý program tváří jako užitečná aplikace, nebo jako rutina operačního systému. Rozdíl mezi trojskými koňmi a počítačovými viry se řadí například neschopnost duplikace svého škodlivého kódu do dalších částí operačního systému. Pro představení své činnosti se můžeme zaměřit na proceduru přihlašování do operačního systému. Trojský kůň se přichytí do procedury tak, že si nastaví prioritu spouštěcího kódu na sebe. Požádá uživatele, aby zadal své jedinečné jméno a heslo, který potom trojský kůň následně uloží a předá tvůrci malware. Kůň potom předá zpátky prioritu na původní rutinu přihlašování, na čemž uživatel se znovu přihlásí úspěšně.

3.4.3 Počítačový červ

Počítačový čer je jakýkoliv kus kódu, který se dokáže replikovat počítači oběti útoku. Počítačový červi jsou samostatní. To znamená, že pro jejich životní cyklus není potřeba spuštění hostitelského programu. K jejím vlohám může patřit celkově pomalá odezva systému, protože počítačový červy spotřebovávají ke své činnosti prostředky systému, konkrétně se může jednat o šířku pásma sítě, ve kterém je počítač umístěný, nebo větší aktivita na interním disku. Červi se dostávají do počítače většinou přes zavirované přílohy emailu nebo přes nebezpečné webové stránky.

3.4.4 Spyware

Spyware se dá nazvat na tzv. Špionážní software, o kterém uživatel nemusí vědět, že ho má nainstalovaný ve svém operačním systému. K infikaci dochází často při instalaci nedůvěryhodného balíčku programového vybavení, nebo i při předcházejícím kroku stažení škodlivého balíčku stačí stáhnout škodlivý balíček i bez následné interakce ze strany uživatele. Svojí existencí dokáže ovlivnit systém tak, že prostředky RAM spotřebují pochybně velké množství paměti. Další metodou ovlivňování systému spyware je monitorování a datová kolekce dat, u které se dokáže projevit dojem zpomalení systému, většinou dané zvýšení obsazenosti procesoru. Po kolekci dat získaném z nevědomky uživatele se finální data s citlivými údaji snaží nahrát do internetu. Dalším více zřetelným dojmem mohou nastat

častější problémy s chodem operačního systému, kde se náhle objevují nestability aplikací, náhodné výpadky systému a neschopnost zprovoznění operačního systému.

3.4.5 Ransomware

Ransomware (alias rogueware nebo scareware) omezuje uživatelům přístup k jejich počítačovému systému nebo souborům. Za obnovení přístupu požaduje program zaplacení výkupného. Ransomware je účinný i tím, že i po znovuobnovení systému je hrozba stále aktivní. Nepříjemnost pro vlastníka systému garantuje ransomware tím, že šifruje data pomocí složitých algoritmů, aby obsah souborů systému nebyly čitelné a použitelné bez dešifrovacího klíče, který má pouze útočník k dispozici. Za obnovení přístupu pomocí tohoto klíče požaduje program zaplacení výkupného. Ransomware může infikovat počítač řadou metod, včetně škodlivých e-mailových příloh, zranitelností softwaru a útoků sociálního inženýrství.

3.4.6 Spam

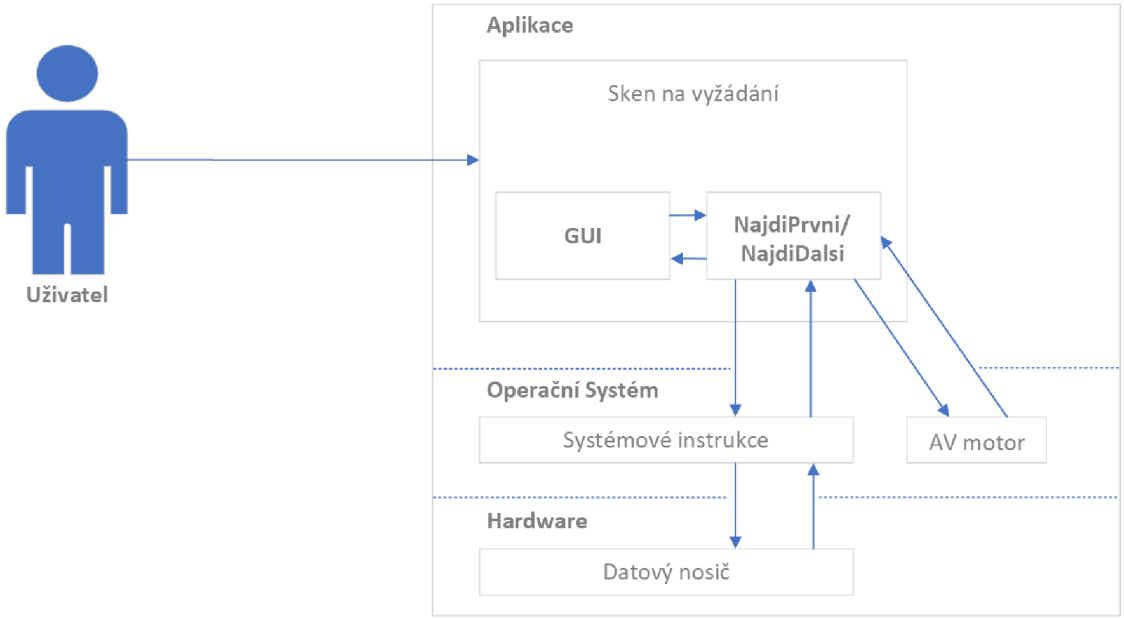
Spam je nevyžádaná pošta v elektronické podobě. Jejím smyslem je nalákání uživatelů na reklamní nabídky produktu nebo služby. Tento proces zpracovává automatizovaný program, který specificky vyhledává kontakty a emailové adresy. Při získání nových cílových uživatelů spam přepošle identické zprávy emailem. Spam svým způsobem dokáže spotřebovat šířku pásma se vzrůstajícím počtem emailů. Phishingové útoky jsou běžným typem kybernetického útoku, při kterém se útočníci snaží přimět lidi, aby jim poskytli citlivé informace, jako jsou přihlašovací údaje, čísla kreditních karet nebo jiné osobní údaje. E-maily se často používají při phishingových útocích, protože jsou běžným způsobem, jakým lidé komunikují online. Jak v osobní sféře, tak i profesní se útočníci mohou v e-mailu snadno vydávat za někoho jiného. Metodou spoofing si útočník podvrhne e-mailové adresy, aby to vypadalo, že e-mail pochází z důvěryhodného zdroje, jako je např. banka nebo blízá osoba. Pro zvýšení efektivity útoku spoofing se v emailu mohou používat loga, značky a další prvky, aby e-mail vypadal autenticky.

3.5 Možnosti ochrany OS

Za dobu evoluce počítačových síti, lidé s dostatečným know-how[4] vytvářejí lepší postupy při infiltraci systému. Naštěstí tato informační válka je vedena po obou stranách, kde softwarové bezpečnostní firmy se přizpůsobují novým zranitelnostem a vytvářejí nové standardy v oblasti informační a kybernetické bezpečnosti.

3.5.1 Antivirus

Antivirový program je jeden z typů softwarového vybavení. Antivirový software používá řadu technik k ochraně počítače před různými bezpečnostními hrozbami, včetně virů, malwaru a dalších typů škodlivého kódu. Dokáže udržet systém v bezpečí tím, že neustále sleduje podezřelé aktivity v počítači a analýzou souborů a programů na přítomnost malwaru. Pro svoji činnost používají metodu skenování lokálních souborů, které se dějí na pozadí. Tato funkce jde spustit uživatelem manuálně na vyžádání. Obrázek 1 reprezentuje funkcionalitu virového skeneru při skenování na vyžádání.



Obrázek 6: Fungování virového skeneru: na vyžádání
Zdroj: vlastní zpracování dle [48]

[4] Know-how je anglické sousloví, které popisuje znalosti určené pro uskutečnění činnosti

3.5.2 Anti-Spyware

Anti-spywarový software je typ počítačového programu určený k detekci a odstranění nežádoucího spywaru z počítačového systému. Techniky rozpoznání spyware mohou zahrnovat skenování paměti počítače a pevného disku na přítomnost známých spywarových struktur. Pro validaci rozpoznání těchto struktur se používá detekční databáze, kteří provozovatelé anti-spywarového balíčku zveřejňují pravidelnou aktualizací. Další z funkcí obsahuje skenování hrozeb v reálném čase a v případě nalezení, možnost umístit spyware do karantény nebo odstranit z počítačového systému. Společnost Microsoft přistoupila k riziku hrozby spyware tím, že získala intelektuální vlastnictví anti-spywarového lídra GIANT Company její akvizicí. Pro integraci nového zabezpečovacího nástroje Microsoft AntiSpyware, která tato firma s podporou Microsoftu vytvořila, je dostupná pro Windows 2000 a pozdější verze. [49] Forma tohoto nástroje byla pouze první iterací a o necelý rok později se tento nástroj přejmenoval na Windows Defender, u které Microsoft představil zjednodušené prostředí a v podstatném vylepšení aktualizace definic pomocí Windows Update [50]. Pro oblast počítačové bezpečnosti se řadí anti-spywarový program jako jednu bezpečnostní jednotku a pro ucelenost zabezpečení je vhodné spojit tuto jednotku s dalšími bezpečnostními opatřeními k ochraně počítačových systémů před škodlivým softwarem.

3.5.3 Anti-Phishing

Společnost Microsoft poskytuje několik nástrojů a funkcí, které mohou chránit před phishingovými útoky. Hlavní podstatou brouzdání internetu je využití webového prohlížeče Microsoft Edge, který je předinstalován v systému Windows 10. Má vestavěnou ochranu proti phishingu jménem SmartScreen, která se pokusí vyhnout škodlivým webům. Když navštívíte web, SmartScreen zkontroluje reputaci webu se seznamem známých škodlivých webů. Pokud je web na seznamu, SmartScreen včas upozorní, že web může být nebezpečný a dá uživateli možnost web opustit. Jako další funkci disponuje kontrolu reputaci stažených aplikací a souborů se seznamem známých škodlivých souborů. Za včasného varování předloží možnost soubor smazat nebo jej přesto spustit. SmartScreen také kontroluje adresy URL v e-mailech a jiných zprávách se seznamem známých phishingových webů. Za použití tohoto

seznamu se na webu, se kterým se chce uživatel spojit, může dojít k varování o potencionálním riziku a dovolí uživateli se rozhodnout, zdali chce stránku navštívit. [51] Microsoft Defender for Endpoint je řešení zabezpečení, které může pomoci chránit vaše zařízení před malwarem a phishingovými útoky. K detekci a reakci na hrozby využívá umělou inteligenci a strojové učení. [52] Pomocí těchto nástrojů a funkcí můžete pomoci chránit sebe a svá zařízení před phishingovými útoky. Je však také důležité zůstat ve střehu a být obezřetní při otevírání e-mailů nebo klikání na odkazy z neznámých zdrojů.

3.5.4 Skripty na míru

Dalším způsobem posílení ochrany operačního systému před různými hrozbami může být za využití skriptů. Skripty jsou soubory obsahující instrukce, které ovládají různé funkce operačního systému. Instrukce mohou být napsány v různých programovacích jazycích a slouží k automatizaci různých úkolů a operací na počítači. Tyto skripty umožňují uživatelům nastavit specifická pravidla a zabezpečení, které odpovídají jejich individuálním potřebám a preferencím.
Jejich povahou nabývá faktu, že skripty mohou být podporovány vývojáři ze strany firmy, která vytvořila onen operační systém, na kterém skripty pracují. Jedním z nich, který obsahuje skriptovací prostředí a skriptovací jazyk podporovaný firmou Microsoft se nazývá PowerShell [53].
Existuje skript, který pracuje se sbírkou dalších skriptů a nástrojů. Jeho plným názvem se jmenuje Tron, skript pro automatické čištění PC. Tron se obvykle používá pro účely:

- Odstranění malwaru a virů
- Vyčištění systému
- Aktualizace softwaru
- Optimalizace systému
- Volitelná systémová vylepšení

Je důležité si uvědomit, že Tron není oficiálním produktem ani softwarem poskytovaným společností Microsoft nebo jakoukoli konkrétní organizací. Jedná se o skript vytvořený a podporovaný komunitou programátorů, který může být

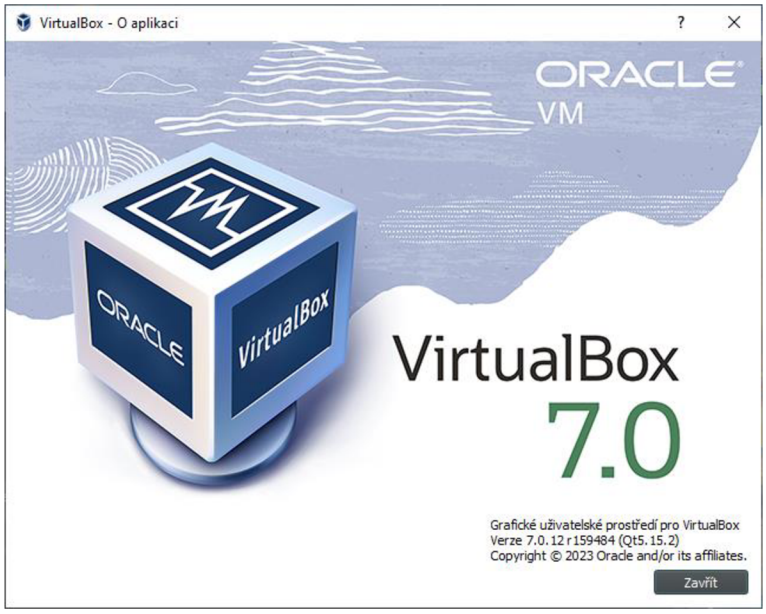
užitečným nástrojem pro uživatele, kteří chtějí provést úklid a optimalizaci systémů Windows. [54]

U vytvořených skriptů neplatí pravidlo, že jejich prezentace pro uživatele nabývá ve formě oken, jak je na tom uživatel zvyklý ze systému Windows. Pro přehlednost a prevenci neočekávaných situací je pro každý skript nutností předložit specifikaci skriptu ve formě dokumentace. V dokumentaci by se měl každý uživatel dozvědět, jak skript pracuje a co by měl vykonávat za dobu svého životního cyklu. Využití komunitně vytvořených skriptů, nebo oficiálních skriptů z první ruky se může zvýšit bezpečnost systému a bránit hrozbám, které by jinak mohly uniknout běžným antivirovým a anti-spyware programům. Je povinností každého uživatele vzít v úvahu, že použití skriptů s sebou nese potencionální nebezpečí nevratného poškození systému dat a následkem vzniká nutnost reinstalace systému.

4 Praktická část

4.1 Sestavení virtuálního prostředí

Za účelem testování systému byl použit program pro vznik virtuálních strojů VirtualBox od společnosti Oracle. Tento program zajistí vytvoření ideální prostředí pro virtualizaci, který simuluje chování operačního systému v již probíhajícím operačním systémem. Obyčejně se virtuální stroj zobrazí jako okno na ploše počítače.



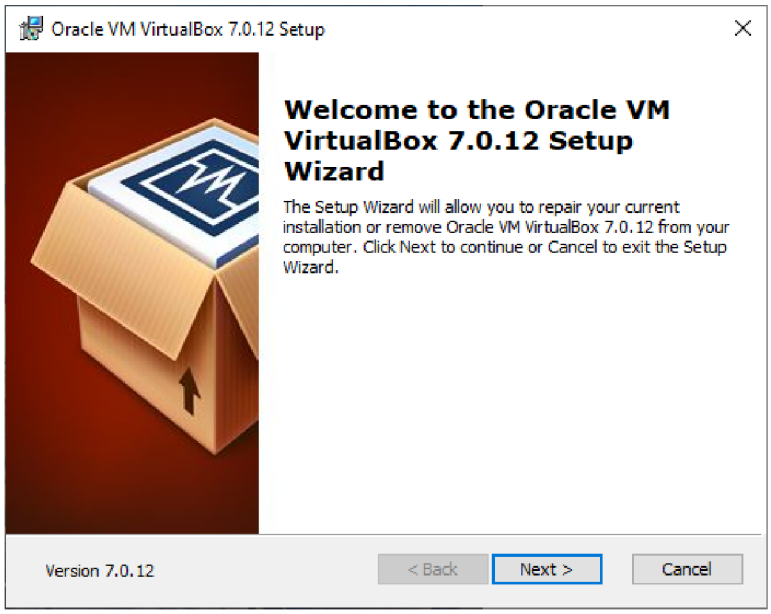
Obrázek 7: Informační okno programu VirtualBox
Zdroj: vlastní zpracování dle [55]

4.1.1 Instalace VirtualBox

Program je distribuován pod licencí GNU General Public License (GPL). To znamená, že VirtualBox můžeme instalovat a používat bezplatně na počítači. Je instalován s nejnovějšími aktualizacemi, které budou instalovány automaticky a verze programu je kontrolována při každém jeho zapnutí. Odkaz ke stažení je zde: https://www.virtualbox.org/wiki/Downloads. Program je komprimován do balíčku, který se po stažení instaluje do operačního systému. V záložce Downloads se dělí na balíčky přizpůsobený daným operačním systémem a jsou seskupené pod číslem jeho verze. Zvolíme odkaz nejnovější verze (7.0.12) pro systémy Windows, jež je nazýván Windows hosts.

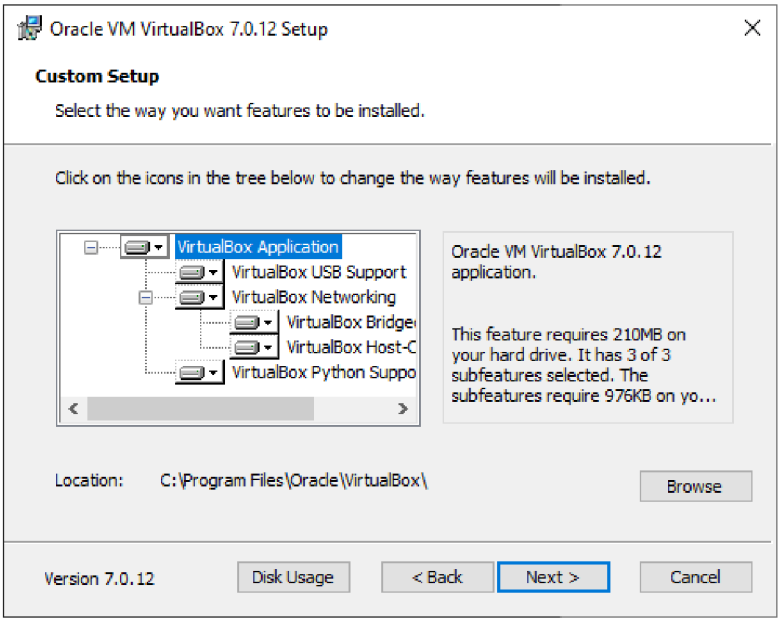
Obrázek 8: Stránka VirtualBox
Zdroj: vlastní zpracování

Proces instalování programu je stejný, jak bývá u jiných spustitelných souborů systému Windows. Kliknutím myši na stažený program se spustí proces instalace. Instalace vyžaduje práva administrátora. Při spuštění se zobrazí uvítací okno.



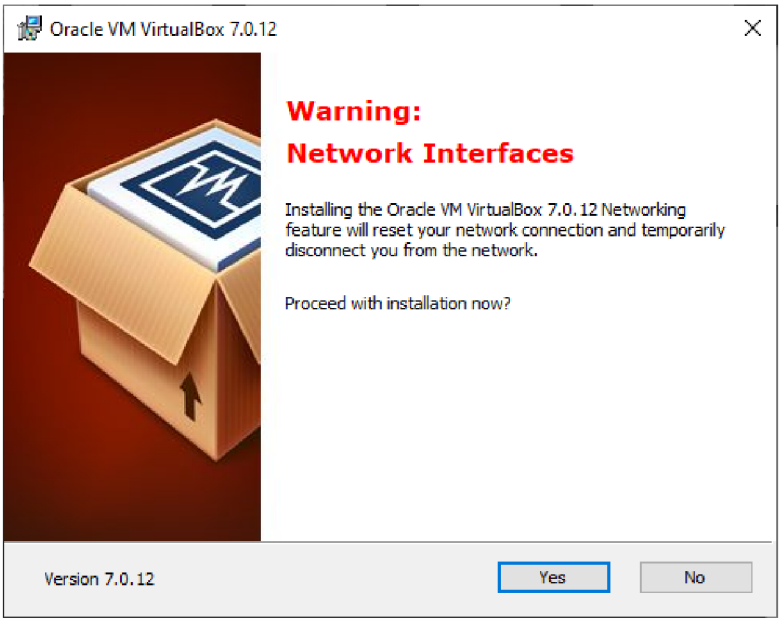
Obrázek 9: Uvítací okno VirtualBox
Zdroj: vlastní zpracování

Další okno představuje způsob instalace programu, ve kterém se určí instalování jednotlivým součástí programu, který se podle nutnosti může upravit. Za účelem testování není potřeba měnit součásti instalace programu.



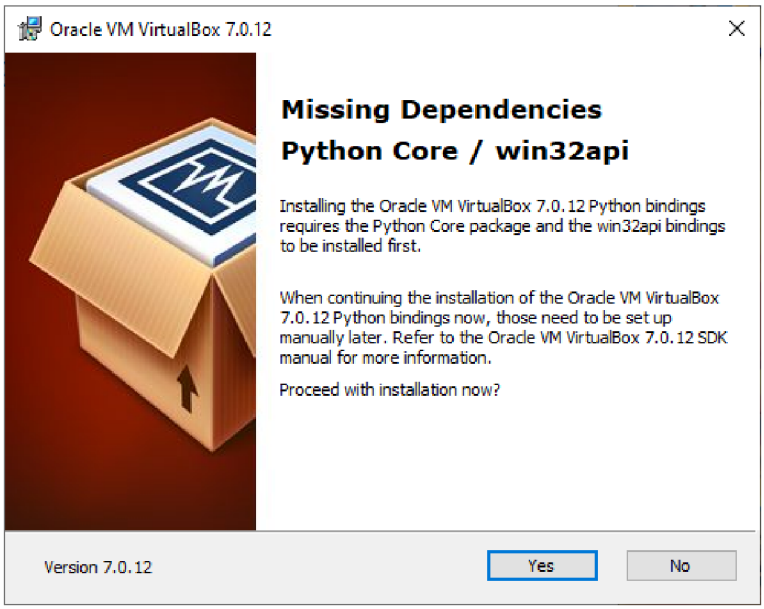
Obrázek 10: Okno přizpůsobení instalace
Zdroj: vlastní zpracování

Při instalaci součásti VirtualBox Networking je za potřeby dočasně přerušit všechny síťové připojení, na které program upozorňuje.



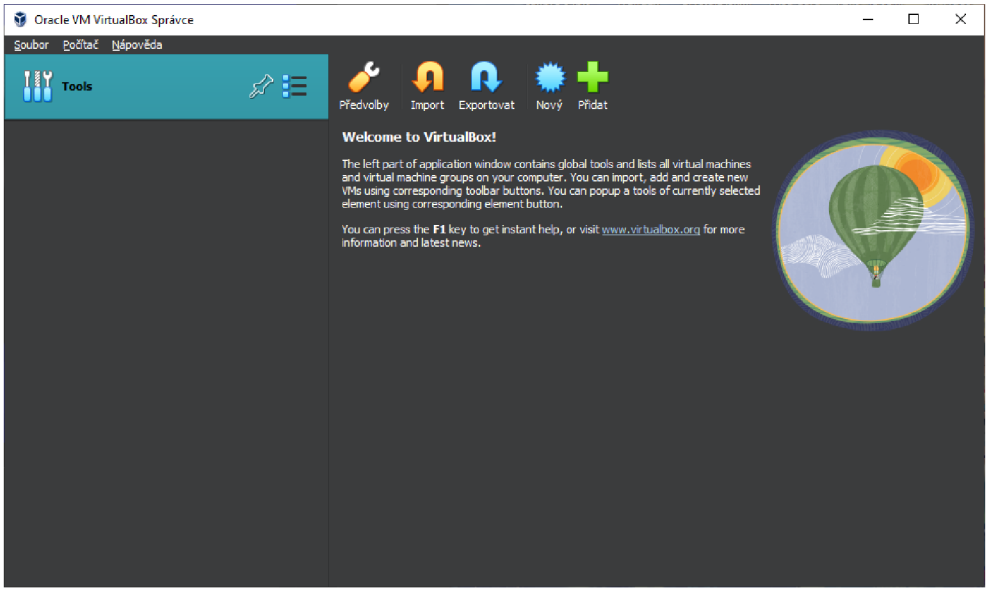
Obrázek 11: Varovné okno sítového připojení
Zdroj: vlastní zpracování

Před instalací programu je nejdříve nutné instalace závislých balíčku programu.



Obrázek 12: Oznamovací okno chybějících balíčků
Zdroj: vlastní zpracování

Po úspěšné instalaci se objeví úvodní okno programu. Počáteční nastavení se přizpůsobí nastavení operačního systému.

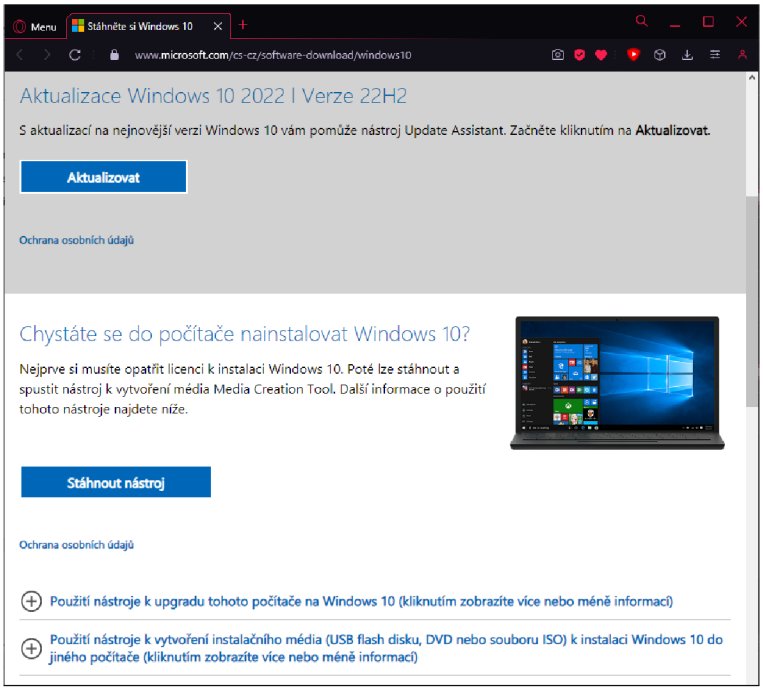


Obrázek 13: Uvítací okno programu VirtualBox
Zdroj: vlastní zpracování

4.1.2 Tvorba instalačního média Windows 10

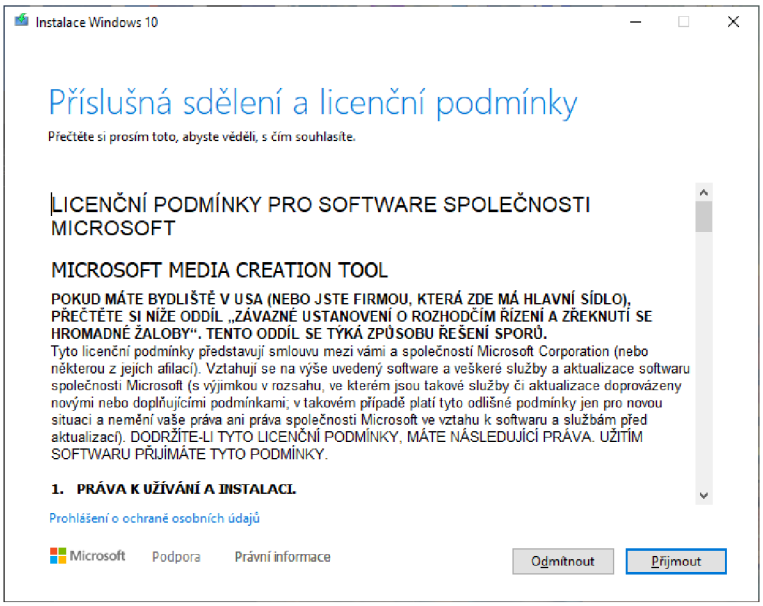
Za potřebí virtualizace desktopu Windows 10 je zapotřebí tento systém vlastnit ve formátu instalačního média. Nejčastějším formátem na distribuci operačních systémů bývá souborem typu ISO, na kterém lze vytvořit spouštěcí instalační

médium. V procesu tvorby instalačního média existuje oficiální nástroj od firmy Microsoft, ze kterého tento proces bude probíhat. Odkaz ke stažení nástroje se nachází zde: https://www.microsoft.com/cs-cz/software-download/windows10



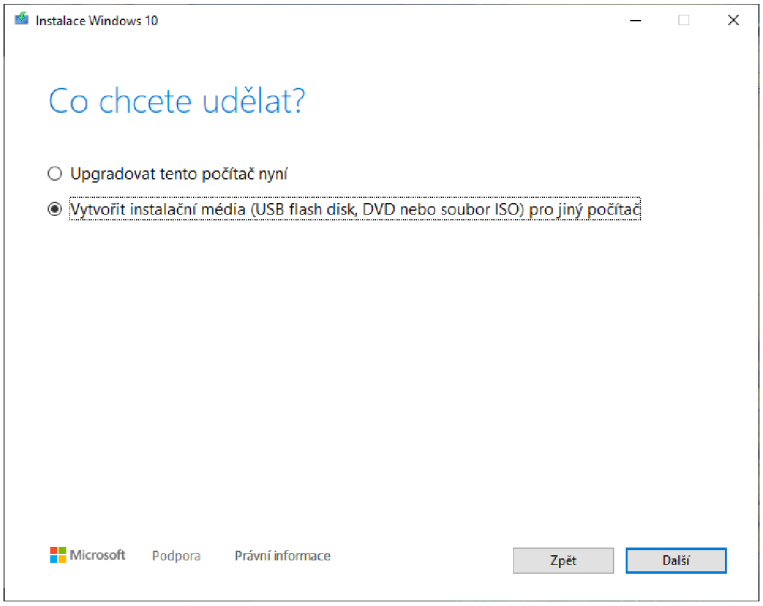
Obrázek 14: Stránka nástroje Microsoft
Zdroj: vlastní zpracování dle [56]

Při úspěšném stažení lze nástroj jakožto program spustit. Po spuštění se v prvním okně představí příslušné sdělení a licenční podmínky, se kterými souhlasíme.



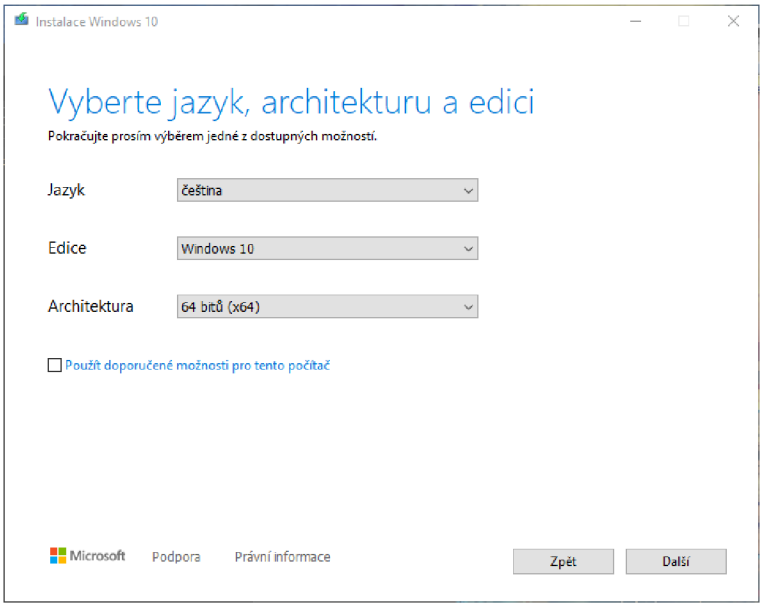
Obrázek 15: Uvítací okno nástroje
Zdroj: vlastní zpracování

V dalším okně přizpůsobíme instalaci vytvořením instalačního média než aktualizaci stávajícího systému.



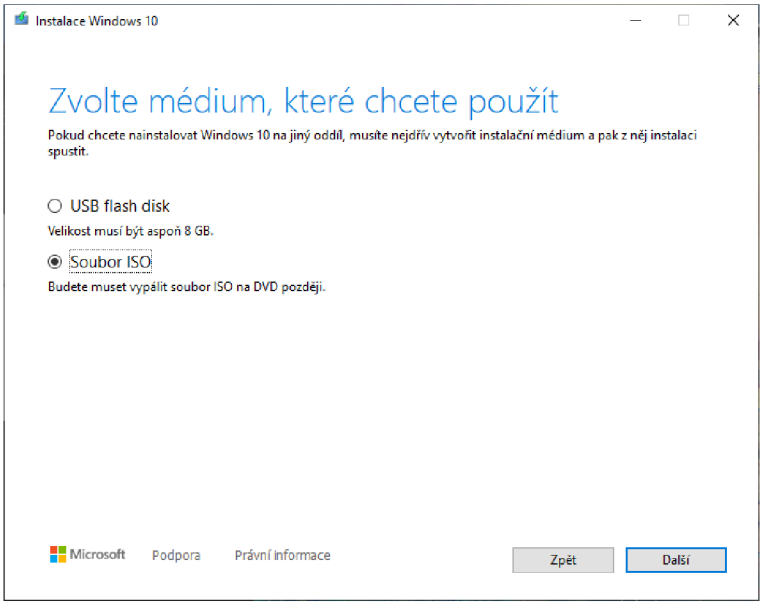
Obrázek 16: Dotazovací okno záměru instalace
Zdroj: vlastní zpracování

Po zadaném vstupu se zobrazí nabídka dostupných variant instalace Windows 10 podle parametrů jazyka, edice a architektury. V zájmu konzistentnosti instalace odškrtneme možnost použití doporučených možností pro tento počítač a soustředíme se na nově odemknuté parametry. V instalaci nastavíme jazyk češtiny, edici Windows 10 a architekturu 64 bitů (x64).



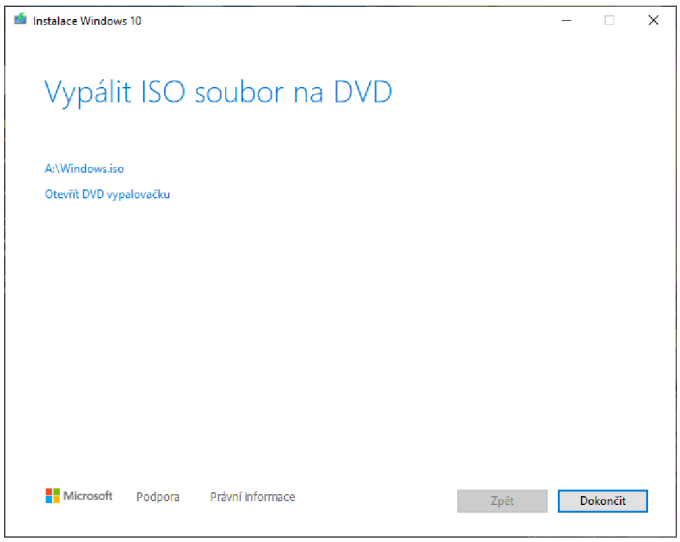
Obrázek 17: Dotazovací okno parametrů instalace
Zdroj: vlastní zpracování

Po zadání těchto parametrů se program dotáže, jak se bude instalační médium používat. Zvolíme druhou možnost souborem ISO, které později využijeme programem VirtualBox. Soubor řádně pojmenujeme a určíme, kam se má uložit.



Obrázek 18: Dotazovací okno způsobu instalace
Zdroj: vlastní zpracování

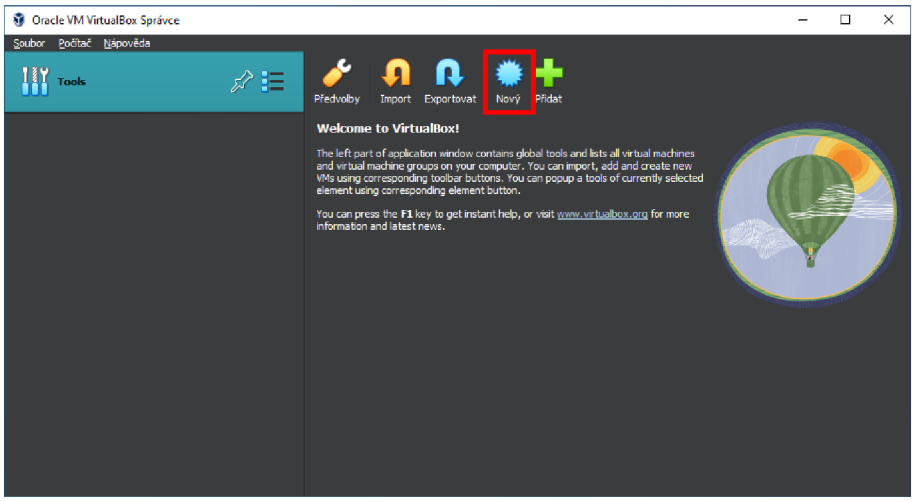
Po stažení Windows 10 a následného vytvoření instalačního média může uběhnout nemálo času, který je určen rychlostí internetového připojení, výpočetního výkonu procesoru a rychlost disku určený cílovým adresářem.



Obrázek 19: Oznamovací okno splněné instalace
Zdroj: vlastní zpracování

4.1.3 Instalace virtuálního stroje Windows 10

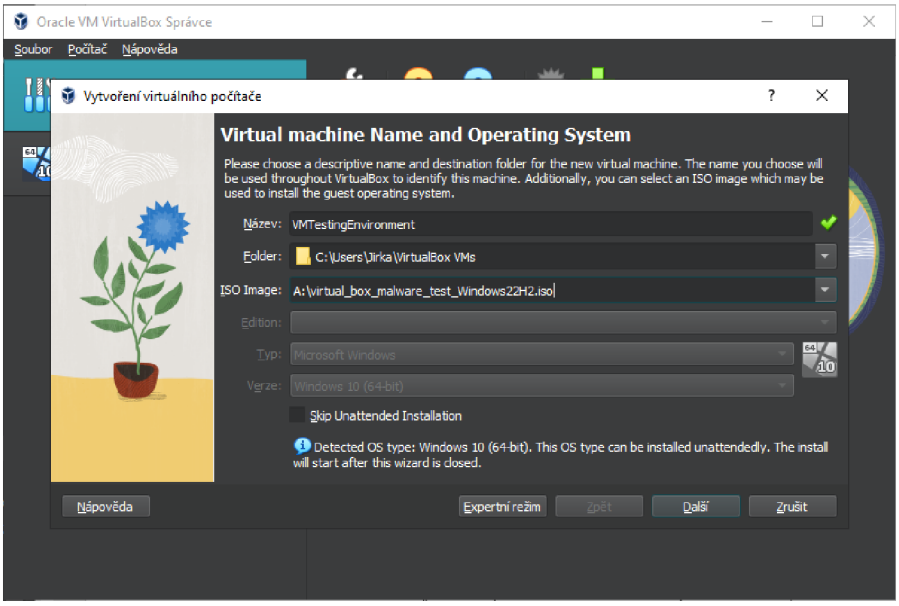
K testování systému Windows 10 je zapotřebí ho instalovat. To se udělá s připraveným instalačním médiem Windows 10 a nainstalovaným programem VirtualBox. V uvítací obrazovce spustíme průvodce instalací zaškrtnutím tlačítka „Nový“.



Obrázek 20: Počátek instalace virtuálního stroje v programu
Zdroj: vlastní zpracování

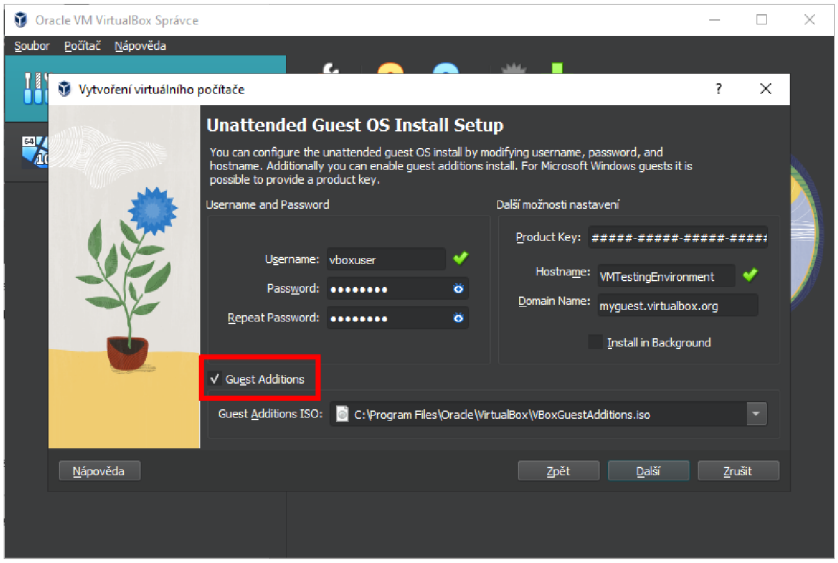
Po objevení okna průvodce vyplníme průvodce instalací ISO. Pro režim testování jsem zvolil tyto konfiguraci:

- Název: VMTestingEnvironment
- Folder:
  - Defaultní: C:\Users\[username]\VirtualBox VMs
  - Moje nastavení: A:\W10Testing
- ISO Image: A:\virtual_box_malware_test_Windows22H2.iso



Obrázek 21: Úvodní okno průvodce instalací
Zdroj: vlastní zpracování

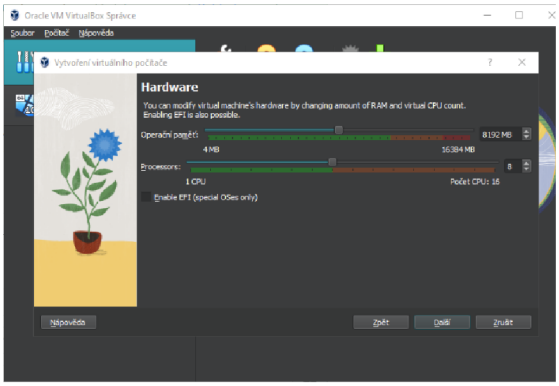
Po nastavení cílového ISO souboru jsou zbylé nastavení uzamčeny, protože program si je vědom interní struktury instalovaného operačního systému. V pokračování instalace se objeví okno pro bezobslužnou instalaci OS. Tu můžeme nechat předpřipravenou, jak je s menší úpravou zaškrtnutí políčka Guest Additions. Tím bude po instalaci systému instalován balíček Guest Additions, který obsahuje ovladače zařízení a systémové aplikace, které optimalizují hostovaný operační systém pro lepší výkon a použitelnost [57].



Obrázek 22: Okno pro bezobslužnou instalaci
Zdroj: vlastní zpracování

Pro zbylé nastavení virtuálního stroje se mohou použít defaultní hodnoty, ale v zájmu rychlejšího provedení testování jsem zvolil tyto hodnoty:

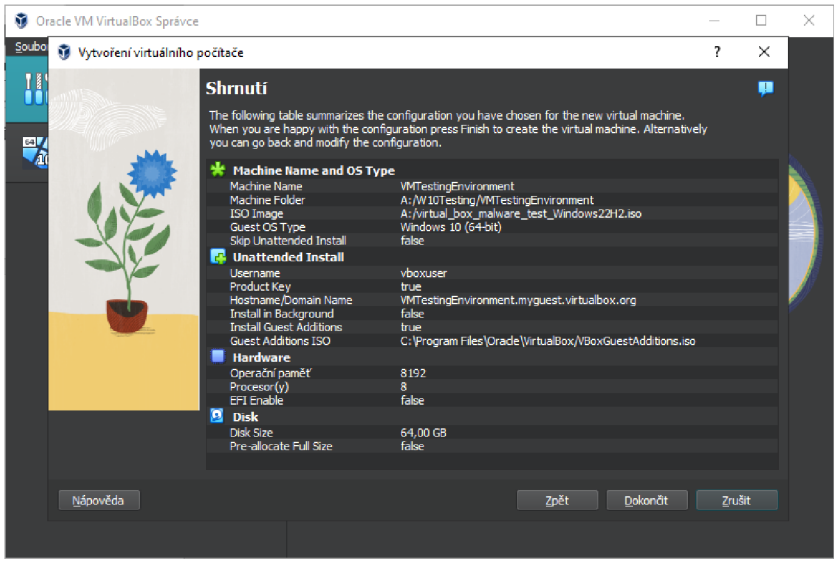
- Hardware:
  - Operační paměť: 8192 MB
  - Processors: 8
- Virtual Hard disk:
  - Create a Virtual Hard Disk Now:
    - Disk size: 64GB



Obrázek 23: Okno na nastavení Hardware
Zdroj: vlastní zpracování

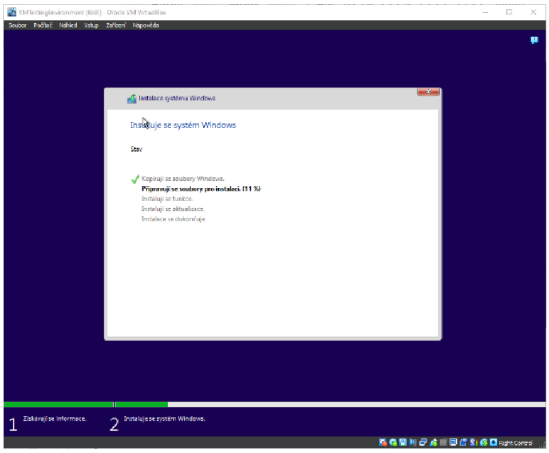
Obrázek 24: Okno na nastavení Virtuálního disku
Zdroj: vlastní zpracování

Na konci průvodce instalací se objeví shrnutí na vytvoření virtuálního stroje.

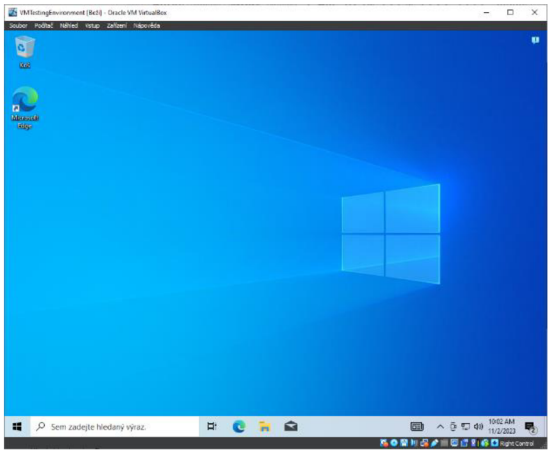


Obrázek 25: Okno shrnutí nastavení virtuálního stroje
Zdroj: vlastní zpracování

Po shrnutí průvodce se instalace automaticky spustí. Instalace operačního systému Windows 10 je zrychlená bez zásahu uživatele, protože požadované vlastnosti jsme již vyplnili v průvodci instalací.



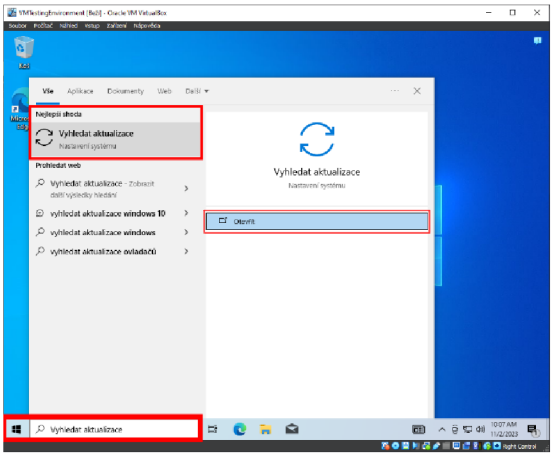
Obrázek 26: Okno instalace Windows 10
Zdroj: vlastní zpracování



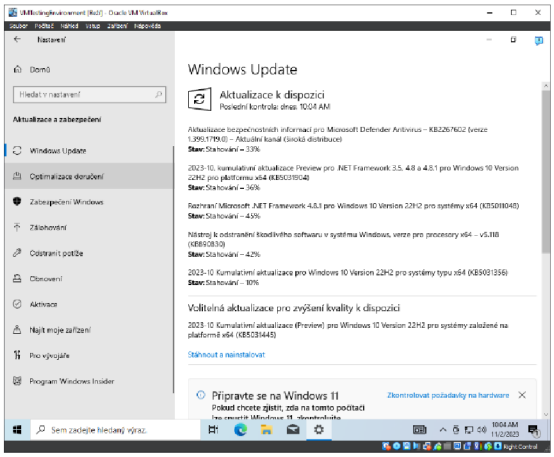
Obrázek 27: Okno plochy Windows 10
Zdroj: vlastní zpracování

4.1.4 Konfigurace virtuálního stroje pro testování

Je správné konfigurovat virtuální stroj tak, abychom minimalizovali riziko infekce malware do hostitelského počítače, nebo sítě. Na přípravu plně fungujícího Windows 10 aktualizujeme systém za pomocí Windows update.



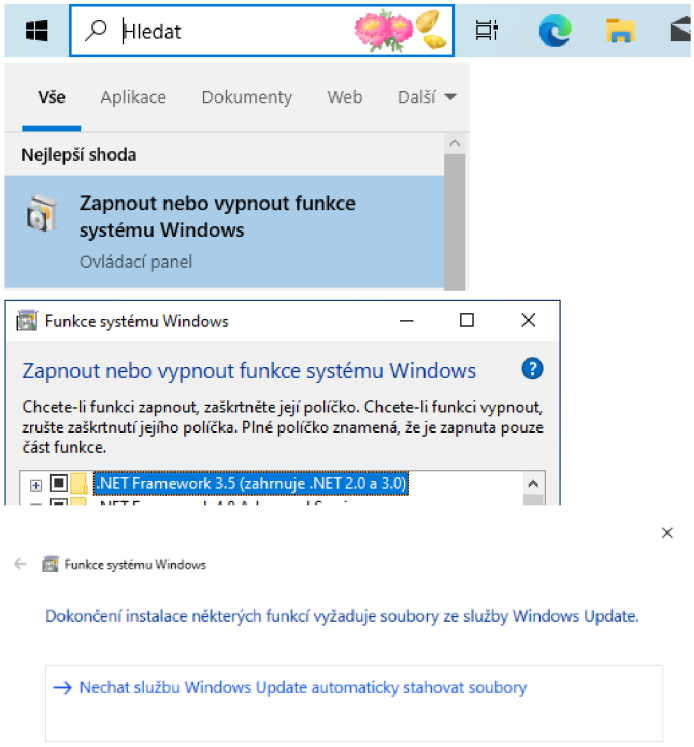
Obrázek 28: Spuštění Windows Update
Zdroj: vlastní zpracování



Obrázek 29: Okno instalace aktualizací
Zdroj: vlastní zpracování

Po provedení aktualizací a restartem systému zopakujeme postup aktualizace, dokud nám Windows Update nenabídne žádné další povinné aktualizace. Ve vyhledávacím poli vyhledejme „Zapnout nebo vypnout funkce systému Windows“.

V nabídce funkcí zaškrtneme políčko s funkcí .NET Framework 3.5 a po potvrzení necháme službě Windows Update automaticky stáhnout soubory.

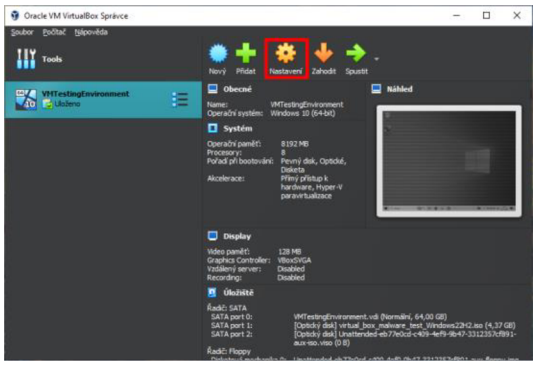


Obrázek 30: Zapnutí funkce .NET Framework
Zdroj: vlastní zpracování

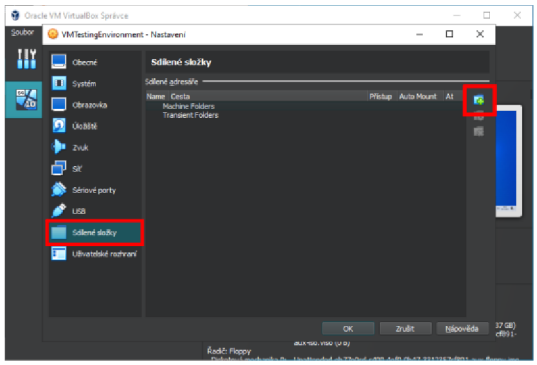
V hostitelském počítači vytvoříme složku, ze které budeme sdílet soubory s virtuálním strojem. Vytvoříme ji v blízkosti složky s vytvořeným virtuálním strojem, z přehlednosti na stejné úrovni složek. V mém nastavení vytvářím složku do:

- A:\W10Testing\Shared_VM_Folder

Dále přidáme složku do virtuálního počítače formou sdílení. V nastavení virtuálního stroje přejdeme na Sdílené složky a v ikoně přidání použijeme parametry pro sdílenou složku.



Obrázek 31: Vstup do nastavení
Zdroj: vlastní zpracování

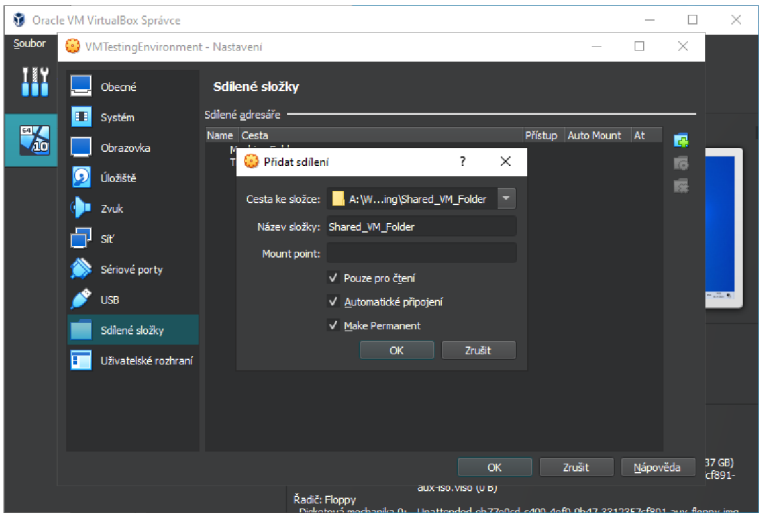


Obrázek 32: Vytvoření sdílené složky
Zdroj: vlastní zpracování

Použijeme následující parametry:

- Cesta ke složce:
  - Obecná cesta: C:\Users\[název_uživatele]\Desktop\[název_složky]
  - Moje nastavení: A:\W10Testing\Shared_VM_Folder
- Název složky: Shared_VM_Folder
- Mount point: (prázdné)
- Zaškrtnout:
  - Pouze pro čtení
  - Automatické připojení
  - Make Permanent

Když je Mount point nechán prázdný, virtuální stroj si složku vhodně namapuje sám. Zaškrtávací políčko „Pouze pro čtení“ brání virtuálnímu počítači provádět změny na hostiteli, ale umožňuje virtuálnímu počítači stahovat jakýkoli obsah umístěný ve složce. Políčko „Automatické připojení“ umožní hostitelskému operačnímu systému automaticky připojit sdílenou složku. U políčka „Make Permament“ se zajistí, že složka bude stále připojena.

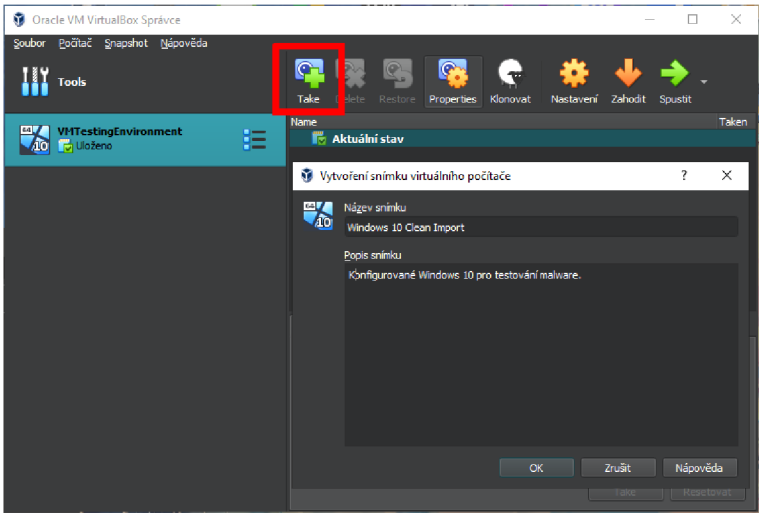


Obrázek 33: Okno shrnutí nastavení virtuálního stroje
Zdroj: vlastní zpracování

Po vytvoření sdíleného adresáře máme virtuální stroj připravený na testování malware. Na zopakování testování využijeme funkcionalitu vytvoření snímku virtuálního počítače. Snímky umožňují vrátit počítač do předchozího stavu. Spustíme pomocí kliknutí na „Aktuální stav“ nově vytvořeného virtuálního stroje a tlačítkem „Take“ vytvoříme nový snímek. Snímek se dá vytvořit i za běhu systému přes horní lištu virtuálního stroje:

- Počítač -> Sejmout snímek

S příslušným názvem a volitelným popiskem uděláme první snímek.



Obrázek 34: Vytvoření snímku virtuálního stroje
Zdroj: vlastní zpracování

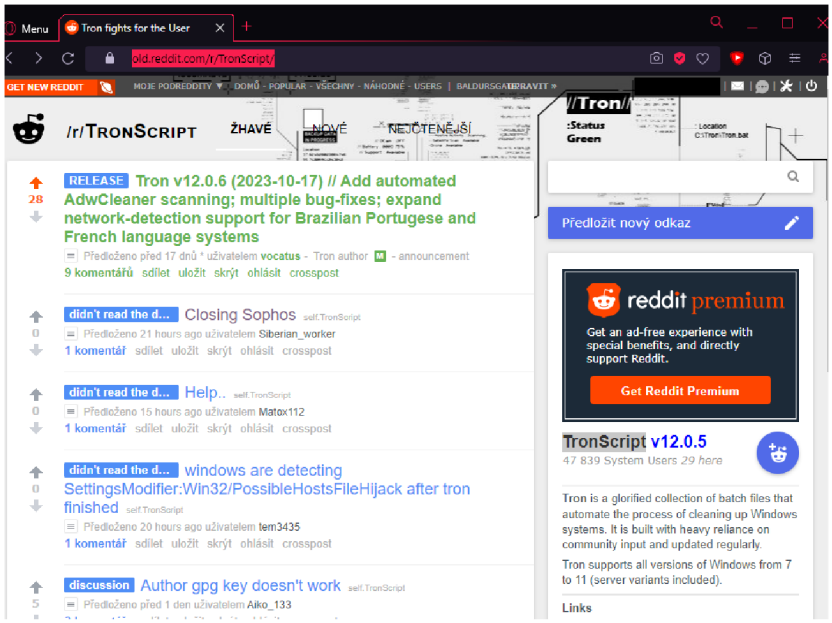
4.2 Tron

Tron je komplexní balíček skriptů, nástrojů, utilit a funkcí Windows, které spolupracují při řešení různých problémů. Jeho primárním účelem je eliminovat malware a nepotřebný software, opravit poškozené operační systémy, aktualizovat zastaralé aplikace, vymazat mezipaměť pro uvolnění úložného prostoru a provádět další úlohy optimalizace systému. S automatizací těchto procesů do jediného provedení šetří čas a zvyšuje efektivitu. Tron není určen pro systémy, které již fungují správně nebo které nedávno prošly čistou instalací operačního systému. Místo toho je jeho primárním cílem pomáhat vrátit ztracený výkon počítačů se systémem Windows, které mohli být ovlivněny bloatwarem, malwarovými infekcemi nebo zanedbávání čištění. [58]

4.2.1 Postup instalace Tron

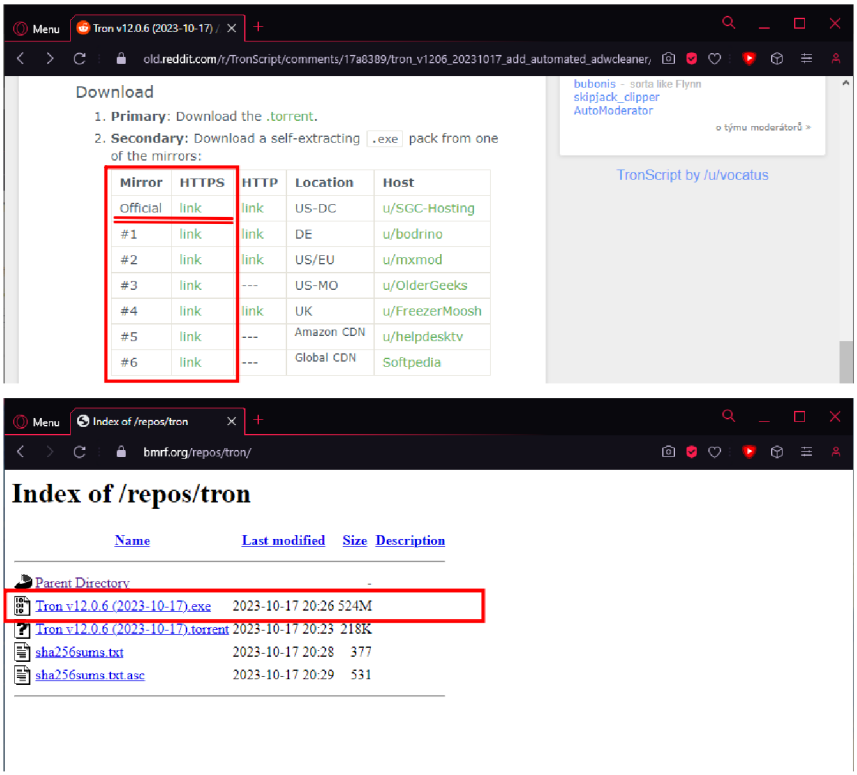
Tron byl vytvořen Vocatus Gatem a jako projekt je komunitně řízený [54]. Plně funkční balíček je dostupný na sociální platformě Reddit, ve které je jeho nejnovější verze sdílen jako první příspěvek na stránce [59]. Bývá barevně vyznačený pod kategorií „RELEASE“a jeho název začíná ve formátu:

- Tron v#.#.# ([YYYY-MM-DD])



Obrázek 35: Stránka TronScript v sociální síti Reddit
Zdroj: vlastní zpracování

Klikneme na tento příspěvek a v sekci Download vybere způsob stažení balíčku. Pro zkrácení postupu stažení vybereme druhý způsob stažení samorozbalovacího balíčku .EXE spojené s tabulkou. Vybereme v rámci bezpečnosti sloupec „HTTPS“, který zaručuje zabezpečený proud dat. Odkaz může být libovolný, ale zvolím stáhnutí z oficiálního repositáře.



Obrázek 36: Postup stažení balíčku TronScript
Zdroj: vlastní zpracování

Jelikož budeme s tímto balíčkem pracovat uvnitř virtuálního stroje, můžeme ho uložit do předem sdílené složky v hostitelském počítači. Cesta pro mojí sdílenou složku je:

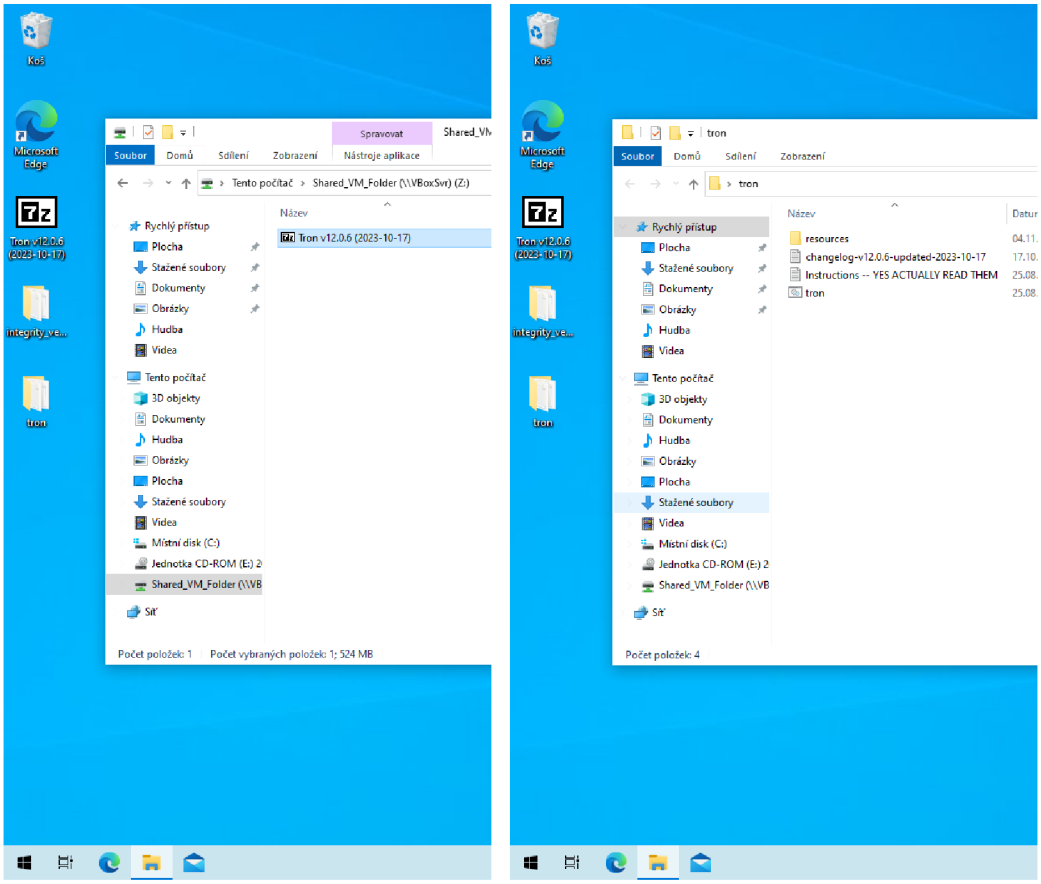
- A:\W10Testing\Shared_VM_Folder

Přejdeme do virtuálního stroje, kde je v systému namapována složka pro sdílení. Systém virtuálního stroje ji pojmenoval jako:

- Shared_VM_Folder (\\VBoxSvr) (Z:)

Přetáhneme stažený soubor .EXE na plochu a poté na něj dvakrát klikneme, aby se začal proces rozbalování. Pro uživatele Windows 10 se může dostat varování, že se jedná o nepodepsanou aplikaci. V tomto případě necháme povolit spuštění souboru

.EXE. Měli by se objevit ploše dvě složky s názvem tron a integrity_verification. V tento moment je Tron skript nainstalován a pracuje se pouze se složkou tron.



Obrázek 37: Výsledek složek sdílení a Tron skriptu
Zdroj: vlastní zpracování

4.2.2 Popis konfigurace čištění Tron skriptu

Ve vyextrahované složce se tron spouští dávkovým souborem tron.bat, který řídí jednotlivé fáze čištění v hlavní složce resources. Každá fáze je očíslovaná a pojmenovaná. Při vyvolání funkce čištění Tron skriptu se nastaví jeho vnitřní parametry ve formě přepínačů nalezený v \tron\resources\functions\tron_settings.bat a jeví se v předloze:

- set <NÁZEV_FUNKCE>=[no | yes]

Informace v následujících podkapitolách byly přejaté z [54].

4.2.2.1 Interní příprava skriptu

Před čištěním si Tron připraví prostředí Windows, aby se zamezila chybovost jeho průběhu. Tato příprava proběhne i v případě předčasného vypnutí Tron skriptu. Obsahem přípravy spočívá:

Tabulka 1: Funkce příprav skriptu Tron
Zdroj: vlastní zpracování

Název úlohy	Popis úlohy
Zjištění spuštění TEMP	Zabrání spuštění Tronu v adresáři TEMP, protože v něm bude vymazávat dočasné soubory.
Vytváření adresáře protokolu	Zabrání spuštění Tronu v adresáři TEMP, protože v něm bude vymazávat dočasné soubory.
Zjištění verze Windows a webového prohlížeče	Určí použití příkazů skriptu, které se provedou za podmínky verze Windows a webové prohlížeče.
Blokování nepodporovaného operačního systému	Přeruší skript, pokud je spuštěn na nepodporované verzi Windows.
Kontrola konfigurace disku	Zkontroluje, zda je disk systému typu SSD, virtuální disk nebo nahlásí nespecifikovanou chybu. Podle konfigurace disku může Tron přeskočit fázi 5 pro defragmentaci.
Zjištění volného místa disku	Zjistí a uloží dostupné místo na disku pro pozdější porovnání.
Zjištění obnovení	Detekuje, zda se skript obnovuje po přerušení například po restartu systému.
Povolení výběru nouzového režimu	Povoluje možnost výběru nouzového režimu klávesou F8 při spouštění systému.

Kontrola síťového připojení	Zkontroluje aktivní síťové připojení. Přeskočí kontrolu aktualizací, pokud žádné připojení není.
Kontrola aktuální verze	Porovná místí kopii Tronu s verzí na oficiálním úložišti. Pokud je zastaralá, Tron požádá o automatické stažení nejnovější kopie.
Aktualizace seznamů nežádoucích aplikací	Provede se stažení nejnovější verze seznamů pro odstranění nežádoucích aplikací. Aktualizace seznamů bude přeskočena přepínačem „set SKIP_DEBLOAT_UPDATE=yes“
Detekce administrátorských práv	Upozorní uživatele, zda je skript spouštěn s právy administrátora.
Vytvoření RunOnce klíče registru	Vytváří klíč v registru sytému Windows pro podporu obnovení skriptu, pokud dojde k přerušení. Přinutí systém Windows, aby skript byl spouštěn v nouzovém režimu.
Kontrola SMART	Zobrazí upozornění, zda jakýkoliv disk netrpí poruchou stavu zdraví.

4.2.2.2 Fáze 0

Fáze nula přestavuje přípravu infikovaného systému Windows přes skript Tron, aby předcházel následek jeho přerušení za doby čištění. Příprava se provádí v tomto pořadí:

- Vytvoření bodu obnovení systému

Vytvoří bod obnovení systému před spuštěním. Ve Windows 10 tato funkce nefunguje, pokud je systém v jakékoli formě nouzového režimu. Autor skriptu nebyl schopen najít řešení tohoto problému. Kdyby tato funkce byla žádaná, tak je skript doporučen běžet v normálním režimu.

- Spuštění programu Rkill

Rkill je nástroj proti malwaru. Vyhledává a ničí řadu malwarů, které narušují nástroje pro čištění. Rkill nevypíná žádný proces uvedený v souboru \resources\stage_0_prep\rkill\rkill_process_whitelist.txt.

- Vytvoření datového profilu

Vypíše seznam nainstalovaných programů a seznam všech souborů v systému, aby se později porovnalo, co přesně bylo odstraněno.

- Výpis programů GUID

Vypíše seznam nainstalovaných programů s unikátním identifikátory GUID. Tento výpis je užitečný pro posílení výpisu známých špatných GUID v projektu.

- Výpis seznamu aplikací Metro

Vypíše seznam všech aplikací Metro v systému. Je užitečný pro projekt, jak se bude chovat v procesu odstranění aplikací.

- Spuštění programu ProcessKiller

Nástroj vypíná různé uživatelské procesy, které mohou narušovat nástroje pro čištění. Výjimky nastávají například u průzkumníka přes explorer.exe, příkazového řádku přes cmd.exe a podobně.

- Nouzový režim

Nastaví systém do nouzového režimu se sítí, pokud dojde k restartu. Na konci skriptu nastaví systém zpátky do režimu s normálním spuštěním.

- Nastavení systémového času přes NTP

Nastaví systémové hodiny na synchronizaci s časovými servery NTP.

- Kontrola WMI

Zkontroluje sadu rozhraní WMI a v případě poruchy se pokusí o opravu. Fungování Tronu s WMI je zásadní pro usnadnění práce například pro odstranění OEM nežádoucích aplikací.

- Využití McAfee Stinger

McAfee Stinger je samostatný nástroj používaný k detekci a odstranění virů.

- Využití programu TDSS

Slouží jako nástroj pro odstranění malware typu rootkit od společnosti Kaspersky Labs.

- Záložní registr

Před zahájení skenování použije program Erunt k zálohování registru.

- Čištění VSS

Vyčistí nejstarší sadu souborů služby Volume Shadow Service v podezření ukrytí malware. Slouží pro tvorbu snímků jako kopie souborů v čase.

- Omezení Obnovení systému

Omezí nástroj Obnovení systému, aby využil pouze 7 % dostupného místa na pevném disku.

- Zákaz režimu spánku

Tron používá program caffeine k deaktivaci režimu spánku při spuštění skriptu. Na konci skriptu obnoví nastavení napájení na výchozí hodnoty systému Windows. V rámci konzistentnosti systému tato funkce bude vypnuta přes přepínač „set PRESERVE_POWER_SCHEME=yes“.

4.2.2.3 Fáze 1

Po splnění fáze nula předává Tron skript kontrolu nad čištěním fázi jedna, která se stará o čištění dočasných souborů. Ve fázi se pokračuje takto:

- Vyčištění Internet Exploreru

Spustí vestavěný nástroj Windows rundll32 k vyčištění a resetování aplikace Internet Explorer verze 7 a vyšší.

- CCLeaner

Nástroj CCLeaner se používá k vyčištění dočasných souborů před spuštěním antivirových skenerů od společnosti Piriform. CCleaner vymazává soubory ve uživatelské složce AppData. V testování bude chování programu upraveno tak, že se ponechají všechny soubory cookies v zájmu zachování běžných přihlašovacích cookies přes přepínač „set SKIP_COOKIE_CLEANUP=yes“.

- Použití skriptu TempFileCleanup

Skript byl napsán autorem Tronu pro vyčistění oblastí dat, které ostatní nástroje neberou v úvahu. Podle vnitřní struktury skriptu se jedná o oblasti dočasných souborů webových prohlížečů firem Microsoft a Google a mezipaměti systému Windows.

- Čištění zařízení USB

Odinstaluje nepoužívaná nebo nepřítomná USB zařízení ze systému pomocí programu drivecleanup.

- Vyčištění duplicitních stažených souborů

Vyhledá a odstraní duplicitní soubory nalezené ve složkách Stažené soubory každého uživatelského profilu. Nedotýká se žádných jiných složek. Používá nástroj Finddupe.

- Vymazání protokolů událostí systému Windows

Zálohuje protokoly událostí systému Windows a poté vymaže všechny položky.

- Vymazání mezipaměti Windows Update

Vymaže soubory již nainstalovaných aktualizací systému Windows pro uvolnění místa na disku.

- Vyprázdnění mezipaměti BranchCache

Tron provede příkaz pro vyprázdnění všech dat uložených v mezipaměti BranchCache, které fungují v distribuovaných sítích kancelářského typu.

4.2.2.4 Fáze 2

Po skončení fáze jedna Tron skript přechází do fáze dvě ve formě odstraňování nežádoucích aplikací. Odstraňování probíhá přes sadu rozhraní WMI formou textových seznamů. Seznamy jsou vytvořeny v cílových složkách:

- \resources\stage_2_de-bloat\oem\programs_to_target_by_name.txt
- \resources\stage_2_de-bloat\oem\programs_to_target_by_GUID.txt
- \resources\stage_2_de-bloat\oem\toolbars_BHOs_to_target_by_GUID.txt

Je zavedený proces pro odstranění Windows Metro aplikací tvořené přes textový seznam ve složce:

- \resources\stage_2_de-bloat\metro\metro_3rd_party_modern_apps_to_target_by_name.txt
- \resources\stage_2_de-bloat\metro\metro_Microsoft_modern_apps_to_target_by_name.txt

Ve fázi dva se také odstraňuje aplikace pro osobní úložiště OneDrive. Pro účely testování a zachování věrohodnosti systému před infikací bude tato fáze vynechána přes přepínače „set SKIP_DEBLOAT=yes“, „set PRESERVE_METRO_APPS=yes“ a „set SKIP_ONEDRIVE_REMOVAL=yes“.

4.2.2.5 Fáze 3

Fáze tři Tron skriptu řídí cyklus dezinfikace systému. Ve fázi se spouští následující kroky:

- Vymazání mezipaměti CryptNet SSL

Vymaže mezipaměť certifikátu Windows CryptNet SSL. Při skenování a případně odstranění hrozeb malware se spustí tyto programy:

- Malwarebytes Anti-Malware
- Malwarebytes AdwCleaner
- Kaspersky Virus Removal Tool.
- Sophos Virus Removal Tool

U programu Malwarebytes Anti-Malware se očekává interakce uživatele za dobu fáze tři, protože program není stavěný na automatizaci přes příkazový řádek. V době čištění fáze sedm se tento program automaticky vymazává, a proto je doporučené ho spustit v době jeho instalace ve fázi tři.

4.2.2.6 Fáze 4

Po fázi dezinfikace systému přichází fáze čtyři s opravou systému. V této fázi se Tron skript pokusí opravit systém:

- Čištění instalačních souborů MSI

Pomocí nástroje Microsoft msizap se odstraní nezávislé instalační soubory typu .MSI z mezipaměti instalovaných programů.

- Kontrola systémových souborů

Nástroj System File Checker zkontroluje souborový systém na chyby a při nalezení se je pokusí opravit.

- Využití služby DISM

Nástroj slouží k úpravě a opravě obrazu systému Windows.

- Využití opravy disku přes chkdsk

Vnitřní příkaz systému Windows zkontroluje disk na chyby a naplánuje opravu při příštím restartu, pokud jsou na něm nalezeny chyby.

- Zákaz telemetrie

Zakáže funkce telemetrie společnosti Microsoft. Tron skript vymaže cílené aktualizace na podporu sledování, které jsou ve výchozím nastavení přítomné ve Windows 10. Tron například zastaví a odstraní službu sledování diagnostiky DiagTrack a provede podrobnější deaktivaci telemetrických funkcí za pomocí nástrojů Spybot Anti-Beacon a O&O ShutUp10. Za účelem celistvosti systému Windows nebude tato část vykonávána přes přepínač „set SKIP_TELEMETRY_REMOVAL=yes“.

- Zakázat upgradu Windows 10

Pokud byl Tron skript spuštěn ve Windows verze 7, 8, nebo 8.1, přepne klíč registru na sdělení uživatele pro instalaci systému Windows 10.

- Oprava sítě

Tron spouští příkazy na opravu sítě v případě ovlivnění síťového připojení.

- Oprava přípon souborů

Tron opravuje většinu výchozích přípon souborů pomocí dávkového souboru, který prochází řadou souborů registru uložených v resources\stage_4_repair\repair_file_extensions\.

4.2.2.7 Fáze 5

Tato fáze navazuje na minulou fázi tím, že opravuje systém formou aktualizace programů. Tron se pokusí aktualizovat jenom ty programy, které už jsou nainstalovány a bude ignorovat aktualizaci těch, které nejsou. Fáze pět se zaměřuje na programy:

- 7-Zip

Nástroj pro kompresi a extrakci souborů.

- Adobe Flash Player

Prohlížeč multimediálního obsahu vytvořeného na platformě Adobe Flash.

- Windows Update

Hlavní aplikace Windows 10 pro aktualizaci systému za využití internetu. Pokud existují stažené WSUS Offline aktualizace, tak Tron skript dá přednost těmto aktualizacím. Díky předpřipravenému prostředí Windows 10 budou oba způsoby přeskočeny přepínači „set SKIP_WINDOWS_UPDATES=yes“ a „set SKIP_WSUS_OFFLINE=yes“.

- Reset báze DISM

Složka WinSxS se rekompiluje a nabude nižší velikosti. Složka obsahuje balíčky s komponentami, které jsou součástí aktualizací. V rámci čištění jsou zastaralé komponenty odstraněny a jakékoli nainstalované aktualizace po tomto procesu nelze znovu odinstalovat.

4.2.2.8 Fáze 6

Fáze šest představuje optimalizaci systému ve formě:

- Obnovení souboru stránek

Obnovuje nastavení souboru stránek systému na hodnotu, aby si sám systém automaticky spravoval velikost stránkovacího souboru pro všechny jednotky.

- Defragmentace pomocí Defraggler

Defraggler je nástroj pro defragmentaci. Proces je automaticky přeskočen, pokud systémový disk je typu SSD nebo pokud byli zjištěny nějaké chyby SMART.

4.2.2.9 Fáze 7

K fázi sedm je proces čištění splněn a je spuštěn proces k dokončení skriptu Tron. Nabízí se nám funkce dokončení ve formě:

- Generování souhrnného protokolu

Generují se protokoly s podrobnostmi o tom, které soubory a programy byly odstraněny. Protokoly jsou umístěny defaultně ve složce C:\logs\tron\summary_logs.

- E-mailová zpráva

Po dokončení Tronu existuje možnost poslání e-mailové zprávy s připojeným souborem protokolu. Tato funkce se nebude využívat.

- Nahrávání protokolu ladění

Funkce nahraje tron.log a seznam všech nainstalovaných programů a výpis seznamu aplikací Metro vývojáři Tronu. Tato funkce není v režimu testování vyžadována.

- Odstranění Malwarebytes

Automaticky odebere nainstalovaný Malwarebytes z fáze tři.

4.2.2.10 Fáze 8

V této fázi byl Tron skript postaven tak, aby umožnil spustit skripty nesouvisející s projektem TronScript. Tron spustí všechny soubory typu .BAT umístěné v adresáři \tron\resources\stage_8_custom_scripts. Žádný spustitelný soubor v této složce neexistuje, a proto Tron skript bude tuto fázi ignorovat. Přesto pro jistotu se nastaví přepínačem „set SKIP_CUSTOM_SCRIPTS=yes“.

4.2.2.11 Fáze 9

Fáze devět spočívá v úložišti programů, které buď nepodporují automatizaci přes použití příkazového řádku, nebo mohou být použity jen ve speciálních případech. Mohou být spuštěny pouze manuálně a na vlastní uvážení uživatele. Popis těchto programů se dá zobrazit v textovém souboru v \resources\stage_9_manual_tools.

4.3 Popis infikace systému a jeho čištění

Ve virtuálním stroji přes sdílenou složku se zkopírovaly různé typy malware. Přes hostitelský počítač byli staženy ze stránky pro shromažďování a sdílení vzorků

malwaru na https://bazaar.abuse.ch/browse/ [60]. Vzorky malwaru stažený pro testování byli nazývány v hashovací funkci jako:

- 3f143e73dca2b93182b5871b4df93dad4c5def58dc4b1f0d7c7cfdbd47d39c88
- 523365b77d29365c6ac6df9ff8b270525fe9db7f59d505fcd153e646a036ef34
- 5f57537d18adcc1142294d7c469f565f359d5ff148e93a15ccbceb5ca3390dbd
- 87df66fc4ca5703a631f8d8528965437e348d87c137af08cda544108199ccaa7
- 8ee7d7a663d55c5337c218f2c00262fc361ea7c5981ed38da26a7197d471d699
- 9b475868e6aafcb6b81d3c4d92d039987b75ef3829c2a834917698845400199e
- e6199c29d7656617e794d4ecd836601db0dae5999e9b6fe7eb30a50f76df0d21
- e6a6d08cc8e55ef5604b2fd58da6694d02bb6244f80947f24ce066083d40f25b
- e8f15cce81d73dd30199ac900f7c6b04b213121a8a8b00440399422d65a7b083

Soubory jsou typu .ZIP a jsou zaheslované pod klíčem „infected“. Jelikož systém Windows 10 ve virtuálním stroji nepodporuje rozbalování souboru .ZIP s funkcí zaheslování, rozhodl jsem se instalovat program pro rozbalování 7-Zip v nejnovější verzi 23.01 nalezený v https://www.7-zip.org [61]. Po rozbalení souborů jsem spustil jednotlivý spustitelný soubor. Ihned po infikaci se jevil systém Windows zpomalený. Aby byli výsledky relevantní a zamezilo se zpomalení skriptu Tron, systému byl po restartování spuštěn v nouzovém režimu.

Zapnul jsem hlavní skript tron.bat a při výstupu skriptu podle Přílohy 1 se začalo specifikací stroje.

Pro počáteční přípravu se zastavovala služba Themes. Při pokusu vytvoření bodu obnovení systému došlo chybě, protože Tron skript byl spuštěn v nouzovém režimu. Za fáze nula se spustil rkill pro zastavení procesů. Nebyl nalezen žádný malware ve službách, v procesech, ani v registru a následně byli resetovány přípony .EXE, .COM a .BAT. Po provedení různých kontrol se nenašli žádné problémy rozsahu chybějících digitálních signatur a u souboru hosts. Až na výjimku vypsání seznamu aplikací Metro z důvodu nouzového režimu systému byli provedeny akce fáze nula, převážně výpisem seznamu služeb.

Ve fázi jedna proběhlo čištění dočasných souborů pro mezipaměť certifikátů SSL, souborů Internet Exploreru a čištění oblastí uživatelských a systémových dat složek Appdata a TEMP. K pokračování přišel CCleaner se zachováním všech souborů

cookies a začal proces čištění zařízení USB a čištění duplicitních stažených souborů. Před vymazáním protokolů událostí systému Windows se jejich záloh provedly úspěšně. K poslednímu kroku fáze jedna se vymázání mezipamětí Windows Update a BranchCache provedlo úspěšně.

Fáze dva se kompletně zamezila podle nastavení Tron skriptu.

Fáze tři začala postupem instalací MalwareBytes a spuštěním dalších čistících prostředků Malwarebytes AdwCleaner, Kaspersky Virus Removal Tool a Sophos Virus Removal Tool. U posledního z nich byl proces nejpomalejší a po výpisu jeho interních komponent jsme mohli ignorovat chybové hlášky neotevření souborů.

Ve fázi čtyři se nenašli žádné instalační soubory .MSI pro čištění. Za využití služby DISM se nenašlo poškození obrazu systému a výsledný log relací DISM se uložil do souboru cestou C:\logs\tron\raw_logs\dism_check.log. U nástroje System File Checker se transakce ověřování a oprav vydařila bez chyb. Vnitřním příkazem chkdsk se začala kontrola disku, u kterého nebyli nalezeny žádné chyby. U zamezení odstranění služeb telemetrie se nastavilo jejich vypnutí. Operace byli dokončeny se dvěma chybami. Po vypnutí instalací aplikací ze třetích stran a vypnutí neexistující telemetrie od firmy Nvidia se provedli zbytek fáze čtyři pro opravu sítě a přípon souborů.

K fázi pět se detekoval program 7-Zip a nastalo jeho aktualizování. Aktualizace Windows Defender nebyla provedena z důvodu spuštění systému v nouzovém režimu. Byli přeskočeny metody aktualizací Windows, protože všechny nastávající aktualizace byli provedeny. Byl také proveden postup resetu báze DISM.

K optimalizaci ve fázi šest se úspěšně provedla akce obnovení souboru stránek. K defragmentaci disku nedošlo z detekce disku virtuálního stroje.

Sedmá fáze varovala o přeskočení k obnovení nastavení napájení a přešlo se ke kalkulaci výsledků čištění. Ke konci se odinstaloval MalwareBytes ze systému.

K osmé fázi nedošlo z důvodu nastavení Tron skriptu. Tron vyzýval k manuálnímu použití nástrojů k fázi 9 na uvážení a doporučil restartovat systém co nejdříve. Ve výsledku čištění se na závěr objevila specifikace stroje se statistikami uvolněného místa na disku.

5 Závěry a doporučení

Za účelem naplnění cíle bakalářské práce byla tato práce rozdělena na teoretickou a praktickou část. V teoretické části byli představeny operační systémy, bezpečnost a obecné poznatky o hrozbách, které operační systémy mohou zastihnout. V praktické části byl popsán postup infikace systému Windows ve virtuálním prostředí a jakým bylo provedeno čištění za pomocí skriptovacího nástroje Tron. Na upřesnění jsme stručně popsali jednotlivé funkcionality skriptu Tron, které se dělí do jednotlivých fází čištění. Fáze čištění měli chronologický charakter, kde byla zásadní analýza systému k detekci malware. Na vzorcích testovaného malware se hledání přes Tron skript proběhlo úspěšně. Po kroku analýzy systému byly podniknuty kroky, které zamezily nepovolenému ovlivňování chodu operačního systému a v nejzazším čase se systém dopracovával k jeho obnově. Ve fázi pro čištění byli podniknuty kroky na izolaci a odstranění příslušného malware. Ve výsledku v posledních fázích Tron skriptu byl splněn předpoklad použití alternativních metod čištění od následků infikace malware. I když nastal úspěšný proces čištění, tak výsledky tohoto procesu nemusí nutně znamenat kompletní nahrazení technik čištění anti-malwarových programů. Byl vytvořen specifický případ užití v rámci testování malware a za okolnostech neustálého vývoje malwaru se nedá přesně předpokládat dlouhodobé užití Tron skriptu.

6 Seznam použité literatury

[1] History: Tabulation and Processing [online]. Suitland (Maryland): U.S. Census Bureau, 5 December 2022 [cit. 2023-03-20]. Dostupné z: https://www.census.gov/history/www/innovations/technology/tabulation_and_processing.html

[2] Introduction of Operating System – Set 1: major Functionalities of Operating System;features of operating systems [online]. Uttar Pradesh: GeeksforGeeks, 2023, 25 Mar, 2023 [cit. 2023-03-28]. Dostupné z: https://www.geeksforgeeks.org/introduction-of-operating-system-set-1/

[3] Single User Operating System [online]. In: . Noida (India): JavaTPoint, c2011-2021 [cit. 2023-03-21]. Dostupné z: https://www.javatpoint.com/single-user-operating-system

[4] TILMANS, Sjoerd, RAO, Pallavi, ed. Animated: Most Popular Desktop Operating Systems Since 2003 [online]. Vancouver (Kanada): Visual Capitalist, June 23, 2023 [cit. 2023-08-01]. Dostupné z: https://www.visualcapitalist.com/cp/most-popular-desktop-operating-systems/

[5] MOLINA, Brett. From Windows 1.0 to Windows 10: A history of Microsoft's signature PC software [online]. In: . Tysons (Virginia): Gannett, c2023 [cit. 2023-03-25]. Dostupné z: https://eu.usatoday.com/story/tech/2021/06/24/windows-history-look-back-microsoft-os/5319007001/

[6] ROSENBLATT, Seth. Microsoft Windows 7 review: Microsoft Windows 7: features: Taskbar and Aero Peek;search, touch screens, and XP mode [online]. In: . Indian Land (South Carolina): Red Ventures, July 31, 2009 [cit. 2023-03-25]. Dostupné z: https://www.cnet.com/reviews/microsoft-windows-7-review/

[7] MUCHMORE, Michael. Windows 8: What We Know So Far [online]. In: . New York: PCMag, 2012, February 3, 2012 [cit. 2023-03-26]. Dostupné z: https://www.pcmag.com/news/windows-8-what-we-know-so-far

[8] MUCHMORE, Michael. Microsoft Windows 8.1 Review: help, Start Screen, Settings;a Better Desktop PC, Too [online]. In: . New York: PCMag, 2014, April 3, 2014 [cit. 2023-03-26]. Dostupné z: https://www.pcmag.com/reviews/microsoft-windows-81

[9] RALPH, Nate. Microsoft Windows 10 review: Microsoft gets it right [online]. In: . Indian Land (South Carolina): Red Ventures, 2015, July 28, 2015 [cit. 2023-03-26]. Dostupné z: https://www.cnet.com/reviews/microsoft-windows-10-review/

[10] NOREM, Josh. Windows 11 Gains Market Share but Windows 10 Still Leads by a Mile [online]. In: . New York: Ziff Davis, 2023, February 2, 2023 [cit. 2023-03-30]. Dostupné z: https://www.extremetech.com/computing/342819-windows-11-gains-market-share-but-windows-10-still-leads-by-a-mile

[11] MUCHMORE, Michael. Microsoft Windows 11 Review [online]. In: . New York: PCMag, 2023, March 22, 2023 [cit. 2023-03-26]. Dostupné z: https://www.pcmag.com/reviews/microsoft-windows-11

[12] MESA, Andy F. System 1 - 2 [online]. In: . c1997-98 [cit. 2023-03-27]. Dostupné z: https://applemuseum.bott.org/sections/os.html

[13] EDWARDS, Benj. Looking back at OS X's origins: the NeXT connection;enter OS X [online]. In: . Needham (Massachusetts): IDG, 2010, SEP 12, 2010 [cit. 2023-03-27]. Dostupné z: https://www.macworld.com/article/207664/osxorigins.html

[14] Co je iCloud pro Windows? [online]. In: . Cupertino (California): Apple, c2023 [cit. 2023-03-27]. Dostupné z: https://support.apple.com/cs-cz/guide/icloud-windows/icwd3c1cca5e/icloud

[15] Use Continuity to connect your Mac, iPhone, iPad, and Apple Watch [online]. In: . Cupertino (California): Apple, c2023 [cit. 2023-03-27]. Dostupné z: https://support.apple.com/en-us/HT204681

[16] The UNIX Time-Sharing System: introduction:hardware and Software Environment [online]. 17. New York: Association for Computing Machinery, 01 July 1974n. l. [cit. 2023-07-16]. ISSN 0001-0782. Dostupné z: https://doi.org/10.1145/361011.361061

[17] The invention of Unix: inventing the world's most important computer operating system:how Unix achieved success [online]. Murray Hill (New Jersey): Nokia Bell Labs, 2019, 8 January 2019 [cit. 2023-07-16]. Dostupné z: https://www.bell-labs.com/institute/blog/invention-unix/

[18] MCILROY, Malcolm Douglas. A Research UNIX... [A Research UNIX Reader: Annotated Excerpts from the Programmer's Manual, 1971-1986]: the Shell:the People [online]. Murray Hill (New Jersey): AT&T Bell Laboratories, 1987 [cit. 2023-07-16]. Dostupné z: https://www.cs.dartmouth.edu/~doug/reader.pdf

[19] COMER, Douglas E. Computer Networks and Internets: 21.17 IPv4 Berkeley Broadcast Address Form [online]. Sixth Edition. West Lafayette (Indiana): Pearson Education, 2015 [cit. 2023-07-17]. ISBN 978-1-292-06182-5. Dostupné z: https://bmansoori.ir/book/Computer%20Networks%20and%20Internets.pdf

[20] KERRISK, Michael. The Linux Programming Interface: system V Message Queues:system V Semaphores:system V Shared Memory [online]. San Francisco: No Starch Press, October 2010 [cit. 2023-07-17]. ISBN 978-1-59327-220-3. Dostupné z: https://static1.squarespace.com/static/59c4375b8a02c798d1cce06f/t/59cfb6a032601e11ca5b1cbe/1506784947301/The+Linux+Programming+Interface.pdf

[21] ASHUTOSHHYR9N. Linux History [online]. Uttar Pradesh: GeeksforGeeks, 22 May 2023 [cit. 2023-07-13]. Dostupné z: https://www.geeksforgeeks.org/linux-history/

[22] CORBET, Jonathan. The Linux Kernel: introduction:what this document is about [online]. San Francisco (Kalifornie): The Linux Kernel Organization, c1997-2014, b. r. [cit. 2023-07-13]. Dostupné z: https://docs.kernel.org/process/1.Intro.html

[23] Visual family tree of Linux distributions. In: DistroWatch.com [online]. Copenhagen: Atea Ataroa, c2001-2023 [cit. 2023-07-13]. Dostupné z: https://distrowatch.com/dwres.php?resource=family-tree

[24] Co je to svobodný software?. [The GNU Operating System...] [online]. Boston (Massachusetts): Free Software Foundation, c1996-2001, 2001-12-21 [cit. 2023-07-15]. Dostupné z: https://www.gnu.org/philosophy/free-sw.cs.html

[25] Multi-User Operating System [online]. In: . Noida (India): JavaTPoint, c2011-2021 [cit. 2023-03-21]. Dostupné z: https://www.javatpoint.com/multi-user-operating-system

[26] BHARTI, Nisha. Multi-user Operating System: features of the Multi-user Operating System;advantages of the Multi-user Operating System [online]. In: . Bengaluru (Karnataka): Scaler, 2022, 5 Dec 2022 [cit. 2023-03-25]. Dostupné z: https://www.scaler.com/topics/multi-user-operating-system/

[27] What Is a Data Center? [online]. San Jose (Kalifornie): Cisco Systems, c2023 [cit. 2023-07-30]. Dostupné z: https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html

[28] Windows Server Editions Comparison [online]. Sofia (Bulgaria): Digital Content Distribution, 2023 [cit. 2023-07-30]. Dostupné z: https://www.licencedeals.com/blogs/licencedeals-info-corner/windows-server-editions-comparison

[29] COSMOS, Darwin a kol. Storage Spaces Direct overview: what is Storage Spaces Direct?:how it works [online]. Redmond: Microsoft Corporation, 2023, 04/18/2023 [cit. 2023-07-30]. Dostupné z: https://learn.microsoft.com/en-us/azure-stack/hci/concepts/storage-spaces-direct-overview

[30] FOULDS, Iain a kol. Active Directory Domain Services Overview [online]. Redmond: Microsoft Corporation, 2022, 08/17/2022 [cit. 2023-07-30]. Dostupné z: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

[31] Unix: unix Is Everywhere. PCMag [online]. New York: Ziff Davis, c1996-2023 [cit. 2023-07-31]. Dostupné z: https://www.pcmag.com/encyclopedia/term/unix

[32] SHELDON, Robert a Erica MIXON. Unix: what is the future of Unix? [online]. Newton (Massachusetts): TechTarget, 2022 [cit. 2023-07-31]. Dostupné z: https://www.techtarget.com/searchdatacenter/definition/Unix

[33] Unix Rock [online]. California: Apple, c2011 [cit. 2023-07-31]. Dostupné z: https://web.archive.org/web/20110609032125/http:/www.apple.com/server/macosx/technology/unix.html

[34] MacOS Server 5.7.1 a novější [online]. California: Apple, 2023 [cit. 2023-07-31]. Dostupné z: https://support.apple.com/cs-cz/HT208312

[35] Usage statistics of web servers [online]. Maria Enzersdorf, Niederosterreich (Austria): W3Techs [cit. 2023-08-01]. Dostupné z: https://w3techs.com/technologies/overview/web_server

[36] MAROTEL, Alexandre. Apache Server : A Complete Beginner's Guide: 2.1. Advantages of Apache [online]. Paříž: Twaino, c2023 [cit. 2023-08-01]. Dostupné z: https://www.twaino.com/en/blog/website-creation/apache-server-2/

[37] MEHDI, Yusuf. From one to one billion devices—one customer at a time. Windows 10: Powering the world with 1 billion monthly active devices [online]. Redmond: Windows Blogs, 2020, 2020-03-16 [cit. 2022-06-29]. Dostupné z: https://blogs.windows.com/windowsexperience/2020/03/16/windows-10-powering-the-world-with-1-billion-monthly-active-devices/

[38] SINGH, Amaninder. What is an Operating System?. Functions of Operating System [online]. Uttar Pradesh: GeeksforGeeks, 2022, 2022-06-28 [cit. 2022-06-29]. Dostupné z: https://www.geeksforgeeks.org/functions-of-operating-system/?ref=lbp

[39] MCALLESTER, Erin. What Is the CIA Triad? How to Use It Today [online]. New York: The Arena Group, FEB 18, 2023 [cit. 2023-08-01]. Dostupné z: https://turbofuture.com/internet/The-CIA-Triad-and-How-to-Use-It

[40] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: důvěrnost Confidentiality: integrita Integrity: integrita dat Data integrity: dostupnost Availability: [online]. 3. dopl. vyd. Praha: Policejní akademie České republiky, 2015 [cit. 2023-10-13]. ISBN 978-80-7251-436-6. Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf

[41] SAMONAS, Spyridon a David COSS. The CIA strikes back: Redefining confidentiality, integrity and availability in security. In: JISSec Journal of Information System Security [online]. 10. Washington DC: Information Institute Publishing, 2014, s. 23 [cit. 2023-03-28]. ISSN: 1551-0123. Dostupné z: https://www.proso.com/dl/Samonas.pdf

[42] Our Excessively Simplistic Information Security Model and How to Fix It: confidentiality and possession: integrity and authenticity: availability and utility [online]. Portland (Oregon): Information Systems Security Association, July 2010 [cit. 2023-10-13]. Dostupné z: https://www.bluetoad.com/publication/?i=41813

[43] Trellix 2022 Threat Predictions. Trellix [online]. Milpitas (Kalifornie): Trellix, 2022, 19.1.2022 [cit. 2022-06-30]. Dostupné z: https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/2022-threat-predictions.html

[44] Počítačový Virus. Bezplatný antivirus je prvním krokem k online svobodě [online]. Praha 4 (Česká republika): Avast Software, c1988-2022 [cit. 2022-06-30]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus

[45] Ransomware. Bezplatný antivirus je prvním krokem k online svobodě [online]. Praha 4 (Česká republika): Avast Software, c1988-2022 [cit. 2022-06-30]. Dostupné z: https://www.avast.com/cs-cz/c-ransomware

[46] A. SAEED, Imtithal, Ali SELAMAT a Ali M. A. ABUAGOUB. A Survey on Malware and Malware Detection Systems. International Journal of Computer Applications [online]. 2013, 67(16), 26 [cit. 2022-06-30]. ISSN 0975–8887. Dostupné z: DOI:10.5120/11480-7108

[47] Trojan Horses. In: Foundations of Computer Security [online]. Londýn: Springer-Verlag, 2006, s. 113-114 [cit. 2023-03-14]. ISBN 1-84628-193-8. Dostupné z: doi:10.1007/1-84628-341-8_5

[48] Antivirové programy: Co vás skutečně chrání… [online]. 9. Praha 3: Chip, 2009 [cit. 2022-06-30]. Dostupné z: https://www.chip.cz/dokumenty/05-09-064-antiviry-pdf/

[49] MICROSOFT. Microsoft Acquires Anti-Spyware Leader GIANT Company [online]. Redmond: Microsoft Corporation, 2004, Dec. 16, 2004 [cit. 2023-03-18]. Dostupné z: https://news.microsoft.com/2004/12/16/microsoft-acquires-anti-spyware-leader-giant-company/

[50] JASONG. What's in a name?? A lot!! Announcing Windows Defender! [online]. Redmond: Microsoft Corporation, 2005, November 04, 2005 [cit. 2023-03-18]. Dostupné z: https://web.archive.org/web/20051123220536/http:/blogs.technet.com/antimalware/archive/2005/11/04/413700.aspx

[51] MICROSOFT. How can SmartScreen help protect me in Microsoft Edge?. Microsoft Support [online]. Redmond: Microsoft Corporation, c2023 [cit. 2023-03-16]. Dostupné z: https://support.microsoft.com/en-us/microsoft-edge/how-can-smartscreen-help-protect-me-in-microsoft-edge-1c9a874a-6826-be5e-45b1-67fa445a74c8

[52] GANACHARYA, Tanmay. Inside out: Get to know the advanced technologies at the core of Microsoft Defender ATP next generation protection. Microsoft Security Blog [online]. Redmond: Microsoft Corporation, 2019, June 24, 2019 [cit. 2023-03-16]. Dostupné z: https://www.microsoft.com/en-us/security/blog/2019/06/24/inside-out-get-to-know-the-advanced-technologies-at-the-core-of-microsoft-defender-atp-next-generation-protection/

[53] WHEELER, Sean a kol. What is PowerShell? [online]. MICROSOFT CORPORATION. 2023, 06/28/2023 [cit. 2023-10-27]. Dostupné z: https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.3

[54] GATE, Vocatus a kol. Tron, an automated PC cleanup script [online]. [2015], 2023-10-17 [cit. 2023-11-01]. Dostupné z: https://github.com/bmrf/tron

[55] ORACLE. Oracle VM VirtualBox [online]. Redwood City (California): Oracle, c2023 [cit. 2023-11-01]. Dostupné z: https://www.virtualbox.org

[56] MICROSOFT. Stáhněte si Windows 10 [online]. Redmond: Microsoft Corporation, c2023 [cit. 2023-11-01]. Dostupné z: https://www.microsoft.com/cs-cz/software-download/windows10

[57] ORACLE. 4.1. Introduction to Guest Additions [online]. c2004, 2020 [cit. 2023-11-02]. Dostupné z: https://docs.oracle.com/en/virtualization/virtualbox/6.0/user/guestadd-intro.html

[58] Tron fights for the User: general Info [online]. 2014, Fri Oct 06 2023 [cit. 2023-11-04]. Dostupné z: www.reddit.com/r/TronScript/wiki/index/

[59] GATE, Vocatus. TronScript [online]. [cit. 2023-11-04]. Dostupné z: https://old.reddit.com/r/TronScript/

[60] MalwareBazaar Database [online]. c2023 [cit. 2023-11-08]. Dostupné z: https://bazaar.abuse.ch/browse/

[61] 7-Zip [online]. c2023 [cit. 2023-11-08]. Dostupné z: https://www.7-zip.org

7 Přílohy

Příloha č. 1

```
-------------------------------------------------------------------------------
 Tron v12.0.6 (2023-10-17)
                Windows 10 Home (AMD64)
                Executing as "VMTESTINGENVIRO\vboxuser" on VMTESTINGENVIRO
                Logfile: C:\logs\tron\tron.log
                Command-line switches:
                Time zone: Stredn˘ Evropa (bezny cas)
                Safe Mode: yes NETWORK
                Free space before Tron run: 39 MB
-------------------------------------------------------------------------------
2023-11-07 14:24:24,04 ! NOTE: Tron doesn't think the system has a network connection. Update checks were skipped.
2023-11-07 14:24:24,04   Setting system to always boot to Safe Mode w/ Networking...
2023-11-07 14:24:24,04   Will re-enable regular boot when Tron is finished.
Operace byla dokoncena Łspesne.
2023-11-07 14:24:24,05   Done.
2023-11-07 14:24:24,05   stage_0_prep begin...
2023-11-07 14:24:24,07   Temporarily stopping Themes service...
2023-11-07 14:24:24,79   Done.
2023-11-07 14:24:24,82 !  WARNING: Windows 10 blocks creating SysRestore points in Safe Mode. Why? Because Microsoft.
2023-11-07 14:24:24,82   Skipping restore point creation. Reboot to Normal mode and re-run Tron if you absolutely require one.
2023-11-07 14:24:24,82   Saving desktop screenshot to "C:\logs\tron\raw_logs"...
2023-11-07 14:24:25,45   Done.
2023-11-07 14:24:25,45   Launch job 'rkill'...
2023-11-07 14:24:25,45   If this job takes more than 20 minutes, kill solitaire.exe with Task Manager
Rkill 2.9.1 by Lawrence Abrams (Grinler)
http://www.bleepingcomputer.com/
Copyright 2008-2023 BleepingComputer.com
More Information about Rkill can be found at this link:
 http://www.bleepingcomputer.com/forums/topic308364.html
Program started at: 11/07/2023 02:24:25 PM in x64 mode. (Safe Mode)
Windows Version: Windows 10 Home
Whitelist Mode: C:\Users\vboxuser\Desktop\tron\resources\stage_0_prep\\rkill\rkill_process_whitelist.txt
Checking for Windows services to stop:
 * No malware services found to stop.
Checking for processes to terminate:
 * No malware processes found to kill.
Processes not terminated due to white list:
 * C:\Windows\System32\conhost.exe [WL]
Checking Registry for malware related settings:
 * No issues found in the Registry.
Resetting .EXE, .COM, & .BAT associations in the Windows Registry.
Performing miscellaneous checks:
 * No issues found.
Searching for Missing Digital Signatures:
 * No issues found.
Checking HOSTS File:
 * No issues found.
Program finished at: 11/07/2023 02:25:01 PM
Execution time: 0 hours(s), 0 minute(s), and 35 seconds(s)
2023-11-07 14:25:01,44   Done.
2023-11-07 14:25:01,44   Generating pre-run system profile...
2023-11-07 14:25:07,63   Done.
2023-11-07 14:25:07,63   Dumping GUID list to "C:\logs\tron\raw_logs"...
2023-11-07 14:25:07,85   Done.
2023-11-07 14:25:07,87  ! Skipping Metro app list dump as it doesn't work in Safe Mode.
2023-11-07 14:25:07,87   Launch job 'Temporarily disable system sleep and screensaver'...
2023-11-07 14:25:07,88   Done.
2023-11-07 14:25:07,90   Launch Job 'ProcessKiller'...
2023-11-07 14:25:08,85   Done.
2023-11-07 14:25:08,85   Launch Job 'Set system clock via NTP'...
Operace byla dokoncena Łspesne.
[SC] ChangeServiceConfig SUCCESS
Sluzba Windows Time nen˘ spustena.
Dals˘ n povedu z˘sk te pr˘kazem NET HELPMSG 3521.
The following arguments were unexpected:
 /syncfromswitches:manual
Spousten˘ sluzby Windows Time.
Sluzba Windows Time byla Łspesne spustena.
Sending resync command to local computer
The command completed successfully.
2023-11-07 14:25:10,93   Done.
2023-11-07 14:25:10,93   Launch job 'Check WMI health'...
2023-11-07 14:25:10,98   Done.
2023-11-07 14:25:10,98   Launch job 'Back up registry' to "C:\logs\tron"...
2023-11-07 14:25:25,21   Done.
2023-11-07 14:25:25,21   Launch job 'McAfee Stinger'...
2023-11-07 14:25:25,22   Stinger doesn't support text logs, saving HTML log to "C:\logs\tron\raw_logs\"
2023-11-07 14:27:18,19   Done.
2023-11-07 14:27:18,19   Launch job 'TDSS Killer'...
14:27:18.0528 0x1070  TDSS rootkit removing tool 3.1.0.28 Apr  9 2019 21:11:46
14:27:18.0543 0x1070  ============================================================
14:27:18.0543 0x1070  Current date / time: 2023/11/07 14:27:18.0543
14:27:18.0543 0x1070  SystemInfo:
14:27:18.0543 0x1070
14:27:18.0543 0x1070  OS Version: 10.0.19045 ServicePack: 0.0
14:27:18.0543 0x1070  Product type: Workstation
14:27:18.0543 0x1070  ComputerName: VMTESTINGENVIRO
14:27:18.0543 0x1070  UserName: vboxuser
14:27:18.0543 0x1070  Windows directory: C:\Windows
14:27:18.0543 0x1070  System windows directory: C:\Windows
14:27:18.0543 0x1070  Running under WOW64
14:27:18.0543 0x1070  Processor architecture: Intel x64
14:27:18.0543 0x1070  Number of processors: 8
14:27:18.0543 0x1070  Page size: 0x1000
14:27:18.0543 0x1070  Boot type: Safe boot with network
14:27:18.0543 0x1070  CodeIntegrityOptions = 0x00000001
14:27:18.0543 0x1070  ============================================================
14:27:18.0543 0x1070  KLMD registered as C:\Windows\system32\drivers\60372843.sys
14:27:18.0543 0x1070  KLMD ARK init status: drvProperties = 0xF0F02, osBuild = 19045.0, osProperties = 0x1D
14:27:18.0559 0x1070  System UUID: {0C6E12E3-7E70-6675-F574-EEC6E38F66AC}
14:27:18.0590 0x1070  !crdlk
14:27:18.0590 0x1070  Drive \Device\Harddisk0\DR0 - Size: 0x1000000000 ( 64.00 Gb ), SectorSize: 0x200, Cylinders: 0x20A2, SectorsPerTrack: 0x3F, TracksPerCylinder: 0xFF, Type 'A'
14:27:18.0590 0x1070  ============================================================
14:27:18.0590 0x1070  \Device\Harddisk0\DR0:
14:27:18.0590 0x1070  MBR partitions:
```

```
14:27:18.0590 0x1070  \Device\Harddisk0\DR0\Partition1: MBR, Type 0x7, StartLBA 0x800, BlocksNum 0x7FFF000
14:27:18.0590 0x1070  ============================================================
14:27:18.0590 0x1070  C: <-> \Device\Harddisk0\DR0\Partition1
14:27:18.0590 0x1070  ============================================================
14:27:18.0590 0x1070  Initialize success
14:27:18.0590 0x1070  ============================================================
14:27:18.0653 0x13a8  ============================================================
14:27:18.0653 0x13a8  Scan started
14:27:18.0653 0x13a8  Mode: Auto (DCExact ); TDLFS; Silent;
14:27:18.0653 0x13a8  ============================================================
14:27:18.0653 0x13a8  KSN ping started
14:27:18.0699 0x13a8  KSN ping finished: true
14:27:19.0543 0x13a8  ================ Scan BIOS ================================
14:27:19.0543 0x13a8  BIOS info: vendor = innotek GmbH, version = VirtualBox, releaseDate = 12/01/2006
14:27:19.0543 0x13a8  Base board info: manufacturer = Oracle Corporation, product = VirtualBox, version = 1.2
14:27:19.0543 0x13a8  [ 4D62C8F6D681184ACE5F56AF6C201C7C, 503C9E7F55C6C1D141F32E930B18FA9B8C409F649A0145E75DCE6F9CF8341604 ] BIOS
14:27:19.0543 0x13a8  BIOS - ok
14:27:19.0543 0x13a8  ================ Scan system memory ========================
14:27:19.0543 0x13a8  System memory - ok
14:27:19.0543 0x13a8  ================ Scan services =============================
14:27:19.0574 0x13a8  [ AF50A9D10FF7B1D999BA99D00CC128B3, 3D6E0579821BFA91B7F0A6E6DDC6E03BD3389202AD1A079B825D18D2A76250A0 ] 1394ohci
C:\Windows\System32\drivers\1394ohci.sys
14:27:19.0574 0x13a8  1394ohci - ok
14:27:19.0591 0x13a8  [ 1C29610EDF5FE3C9D313207BD65BCDD0, 5A29D80AF47D08998125CB81BC1D4E84093291A74DE422B63F7BBDA7BDE95311 ] 3ware
C:\Windows\system32\drivers\3ware.sys
14:27:19.0591 0x13a8  3ware - ok
14:27:19.0591 0x13a8  [ B8E126B7E67BE5DA308635EE0F9838CE, 2604BC12CB9E700B6DB37E9078A3E42017EB737C0C5FD81AEF08D8AD83833420 ] AarSvc
C:\Windows\System32\AarSvc.dll
14:27:19.0591 0x13a8  AarSvc - ok
14:27:19.0606 0x13a8  [ F9755217EE7A711EC77CCD07262193F7, 212606A0E10C3D03D765A3AA8B5379954C9E5E7A5511255204C75B5B52A6B57B ] ACPI
C:\Windows\system32\drivers\ACPI.sys
14:27:19.0606 0x13a8  ACPI - ok
14:27:19.0622 0x13a8  [ 6A424E6ABD1970E23ECF3DA85725B6BF, 1D576471A8035AD3FF5B0616F47B79E43AA367ECDF009D7CADDA0F11F13A1345 ] AcpiDev
C:\Windows\System32\drivers\AcpiDev.sys
14:27:19.0622 0x13a8  AcpiDev - ok
14:27:19.0622 0x13a8  [ 70D9FC69CED08E86B888717CC5C37367, 34856C805B67F3EE4ABFD81B61879112344C343BC7E76A7A466FAD276E0E5165 ] acpiex
C:\Windows\system32\Drivers\acpiex.sys
14:27:19.0622 0x13a8  acpiex - ok
14:27:19.0622 0x13a8  [ EF7CB34FB2D56305EF942012499AB8F7, 3A9A504797FD22BB5447BB36597D5001320ABC0D4A1853D478C038EAC6847913 ] acpipagr
C:\Windows\System32\drivers\acpipagr.sys
14:27:19.0622 0x13a8  acpipagr - ok
14:27:19.0622 0x13a8  [ 33B5ED555018128792AFFCDC9AF7AFD2, 1E7C5FADA2486EE31289A4BEFB70AEA173190671C64995441651903CF31E5033 ] AcpiPmi
C:\Windows\System32\drivers\acpipmi.sys
14:27:19.0622 0x13a8  AcpiPmi - ok
14:27:19.0622 0x13a8  [ 85A86944A6163F0B7A8B10203B70CB9A, 72D35F5DB8714D38E4050A7F7A457C4AD99E3EA212040704F1C1ECBB70E865E9 ] acpitime
C:\Windows\System32\drivers\acpitime.sys
14:27:19.0622 0x13a8  acpitime - ok
14:27:19.0637 0x13a8  [ 166E74C0F97881888AF93292A566BAF0, D20512B12B5441D4ABD1CC7576FD68E87CFDB2761FFE9DC453C31DB41ECFB057 ] Acx01000
C:\Windows\system32\drivers\Acx01000.sys
14:27:19.0637 0x13a8  Acx01000 - ok
14:27:19.0653 0x13a8  [ B4B75D49BFBCFB2762593F77E5BD7789, B83072D77685F973701EC6629D8AC2626FDEFD657A4DB9AA7D532960A29FC67C ] ADP80XX
C:\Windows\system32\drivers\ADP80XX.SYS
14:27:19.0669 0x13a8  ADP80XX - ok
14:27:19.0669 0x13a8  [ 55ED0A572978BEFA7DD04597F9962FD0, 634F6CAE240C2E4793B9C14FD4D57E53202940D8583F11FCA4C8376614FCD184 ] AFD
C:\Windows\system32\drivers\afd.sys
14:27:19.0684 0x13a8  AFD - ok
14:27:19.0684 0x13a8  [ DD049F3E63A59C3E2803012A1E327145, 5A8D3F844C7F1AFA3F808D2BC4653241A01FD33491048F0093856A862D25CB8E ] afunix
C:\Windows\system32\drivers\afunix.sys
14:27:19.0684 0x13a8  afunix - ok
14:27:19.0684 0x13a8  [ E4FD4530DA5FD0068CA88AB7FC2EB5F7, 93BF16C23DB81917D237EA19A576F73F4493923EEB231525BC3D6A2B5577817F ] ahcache
C:\Windows\system32\DRIVERS\ahcache.sys
14:27:19.0684 0x13a8  ahcache - ok
14:27:19.0700 0x13a8  [ 526FE18DB976D9A1AE19FBC53FA690B1, 4E2623243A9BB61F7211E591C24EDB70B07974A7FA21E3F14C683F27E975777F ] AJRouter
C:\Windows\System32\AJRouter.dll
14:27:19.0700 0x13a8  AJRouter - ok
14:27:19.0700 0x13a8  [ 3956A3AB1E0424C705258D1F4FDBC964, BAF162329A0FB82D5420342E130DFC53B0C55D76EC946AE70A272A962B1DC16A ] ALG          C:\Windows\System32\alg.exe
14:27:19.0700 0x13a8  ALG - ok
14:27:19.0700 0x13a8  [ 55578CF027B0AE9F0D653B209C9F1B6D, 46A53925BAA34FA9D87E7C3157504A4557D81CD8B8608E7AB6CAF02F482F7792 ] amdgpio2
C:\Windows\System32\drivers\amdgpio2.sys
14:27:19.0700 0x13a8  amdgpio2 - ok
14:27:19.0700 0x13a8  [ D0E26E590DE1424CCC4F77D1687049EF, 387811D57DEF06C9736D9F0BAB0DFB0F83DBAB19E5489BF9A6DCDCBD682DD8FE ] amdi2c
C:\Windows\System32\drivers\amdi2c.sys
14:27:19.0700 0x13a8  amdi2c - ok
14:27:19.0700 0x13a8  [ A7465F9066AFF7F005E1BF2B58A93A3A, 5F44EB738F0F82F10574C946733CEA749A40DE5A6C3FF76C6103A02282C66B84 ] AmdK8
C:\Windows\System32\drivers\amdk8.sys
14:27:19.0700 0x13a8  AmdK8 - ok
14:27:19.0715 0x13a8  [ 6C9EDA68537710EF1AAA83F844BE5622, ECE970076555BA820E7A93D595C3AF3B9CC4FE53F4F9F83501E3E499E88A4BA4 ] AmdPPM
C:\Windows\System32\drivers\amdppm.sys
14:27:19.0715 0x13a8  AmdPPM - ok
14:27:19.0715 0x13a8  [ 70D7BE6BB8D22A38AD0040A1EC41C1FE, D5231F97E5432234A8A19904E59C324E825AF04881AA195C19CCC9E6A7684B14 ] amdsata
C:\Windows\system32\drivers\amdsata.sys
14:27:19.0715 0x13a8  amdsata - ok
14:27:19.0715 0x13a8  [ C47EDC5D81546677A772CFC86281ED29, 71C7E7E5AA74596A6725D8F70F1DE9A0C63D3C3E120D9CCF8A508854AC340A23 ] amdsbs
C:\Windows\system32\drivers\amdsbs.sys
14:27:19.0731 0x13a8  amdsbs - ok
14:27:19.0731 0x13a8  [ F1A1CA86A1E3782A0CABB07EF3663C70, 1FC1D4287DB56A387BDF917C0CB3BFC30CA5D792A350E2EDBBDDEBF8127E1AF9 ] amdxata
C:\Windows\system32\drivers\amdxata.sys
14:27:19.0731 0x13a8  amdxata - ok
14:27:19.0731 0x13a8  [ 736FBFC1F046576F4072826330DE0443, 65AC77803AD5FF0733A772051AAAA524EE249393E2FCFC821E8A37ECEF64DC5C ] AppID
C:\Windows\system32\drivers\appid.sys
14:27:19.0731 0x13a8  AppID - ok
14:27:19.0731 0x13a8  [ 1E113DD6835E309A0042BF3247381A33, F158F906E2AEB8D3FDFC42358F632E39BDEC33F2782AB09D2ADCE5E66E1AF681 ] AppIDSvc
C:\Windows\System32\appidsvc.dll
14:27:19.0731 0x13a8  AppIDSvc - ok
14:27:19.0746 0x13a8  [ A7B058C8B3E705D560AA51155EBC0177, 741B63E76CB9CA74275A2FE46BE32234920B3E8D0B81EF86FBD40D305497BF36 ] Appinfo
C:\Windows\System32\appinfo.dll
14:27:19.0746 0x13a8  Appinfo - ok
14:27:19.0746 0x13a8  [ F132A9D25B491F923A1853484C317DF5, 7CC47D4DB71996BF139EA97BC81BE73F504D1D144629F8B975DEBB1383AEC374 ] applockerfltr
C:\Windows\system32\drivers\applockerfltr.sys
14:27:19.0746 0x13a8  applockerfltr - ok
14:27:19.0746 0x13a8  [ B8315EB478A472EF1DF9ED63B0E01B8F, 1967BFE2B8EDB8B889AF9FD7ED463750ACA0F32178875F036179A3DD70DFCA61 ] AppReadiness
C:\Windows\system32\AppReadiness.dll
14:27:19.0762 0x13a8  AppReadiness - ok
14:27:19.0793 0x13a8  [ 1E6023CB6BE9598F3A88FB7C2222461D, 9AC1CF700BBF2D26BB96DA95FC0C39EF56C14A0A3A3EF658031982D7C71FAA0A ] AppXSvc
C:\Windows\system32\appxdeploymentserver.dll
14:27:19.0824 0x13a8  AppXSvc - ok
14:27:19.0840 0x13a8  [ 46FD8469080917EE12425AF692C4BC20, 96DCA25AE619F38640B22702A10BC3191626F3A36DE0E1B0EDA3B079EA9DEB24 ] arcsas
C:\Windows\system32\drivers\arcsas.sys
14:27:19.0840 0x13a8  arcsas - ok
14:27:19.0840 0x13a8  [ D930AAE80A55116D07C41E95DE5671DB, 14985D6D2D52689C1B012F64ED0D7C9C5F6BADB51C4528BF6456D3EAE2FE69A7 ] AsyncMac
C:\Windows\System32\drivers\asyncmac.sys
14:27:19.0840 0x13a8  AsyncMac - ok
14:27:19.0840 0x13a8  [ 313860F0188E4DF23896451225EA3F19, 26DF58213189EB510CE5CD5DB6C18E1A8943FEF1DADF265EEB5B7579C58CCF74 ] atapi
C:\Windows\system32\drivers\atapi.sys
```

14:27:19.0840 0x13a8 atapi - ok
14:27:19.0856 0x13a8 [74C228C6639055255F05872749C5E475, 4D4334B9B53B5751CFE9251B0DB20B92B971C08615ACA0CA03F55422EAD1A151] AudioEndpointBuilder
C:\Windows\System32\AudioEndpointBuilder.dll
14:27:19.0856 0x13a8 AudioEndpointBuilder - ok
14:27:19.0871 0x13a8 [E91C41E5356219A833F09F1BE062CEFC, 89B2FC8BE89ABC5AF1F288D1EC92BCC7FBB8FD08F17F1EF5E0281AAF08E14067] Audiosrv
C:\Windows\System32\Audiosrv.dll
14:27:19.0887 0x13a8 Audiosrv - ok
14:27:19.0887 0x13a8 [4B652F8244AD13DD4A66F8A6CDB6210E, 5C8324FC0FD2221A61EB8F34A30E27D1DB20AA66C2EC93E38F724353926715D9] autotimesvc
C:\Windows\System32\autotimesvc.dll
14:27:19.0902 0x13a8 autotimesvc - ok
14:27:19.0902 0x13a8 [37E8EAD274F9AA436D71E78E5D3BC292, 95F8398C1EEB27D9D209826F4FD965EEC034C31BE9D17C0331C09E1F0979050B] AxInstSV
C:\Windows\System32\AxInstSV.dll
14:27:19.0902 0x13a8 AxInstSV - ok
14:27:19.0902 0x13a8 [638C59D330A7AF943074678A70F22E7C, FEB2771428706126FEA1CC9A50EBE3CF4F8E8FB6FCB3CA19996497CA44FDAC45] b06bdrv
C:\Windows\system32\drivers\bxvbda.sys
14:27:19.0919 0x13a8 b06bdrv - ok
14:27:19.0919 0x13a8 [26E2320D24C66EB72B36EB71EBEF2558, 7D06B6499FE915480DF4DAD658281C8B85F7AD71F49B089A270AE0B45713F2E9] bam
C:\Windows\system32\drivers\bam.sys
14:27:19.0919 0x13a8 bam - ok
14:27:19.0933 0x13a8 [94529FC323CB2B5397BD5009A4D330AE, 8ED8D22C0E7153B503D9213B68BAE00242F8FB61C2005783AAB971EBAF2B5CFF] BasicDisplay
C:\Windows\System32\DriverStore\FileRepository\basicdisplay.inf_amd64_d4186f58a551c471\BasicDisplay.sys
14:27:19.0933 0x13a8 BasicDisplay - ok
14:27:19.0933 0x13a8 [728E949BF5B5169712E1A0F44AB3889F, 516219D548D7167CF173D0EE2E26C0124A956F3DBB91FFC1D4E58BFDC91B3782] BasicRender
C:\Windows\System32\DriverStore\FileRepository\basicrender.inf_amd64_9eeaaced803186c6\BasicRender.sys
14:27:19.0933 0x13a8 BasicRender - ok
14:27:19.0950 0x13a8 [F1AA9CAFE4B447EB53F88F531AF2DE6E, 050C12D0154A9AA494C417027C388FEDFDE2E4C56712AF15A97AD568B129B800] BcastDVRUserService
C:\Windows\System32\BcastDVRUserService.dll
14:27:19.0950 0x13a8 BcastDVRUserService - ok
14:27:19.0965 0x13a8 [739D089777D2B66DBE7201E5EA4BA2D7, 9AD12E18A042C5B8EFB19297BC2E7BD1FEF75A138FEFB64C6BF0261FD3E53AB1] bcmfn2
C:\Windows\System32\drivers\bcmfn2.sys
14:27:19.0965 0x13a8 bcmfn2 - ok
14:27:19.0965 0x13a8 [D2A5B234D73460EDB65D2895E99D151A, 0F093B9C6261641AB6FCE589914F3D0D3EB7FD699D0CE25E83BF98ADA236D26C] BDESVC
C:\Windows\System32\bdesvc.dll
14:27:19.0981 0x13a8 BDESVC - ok
14:27:19.0981 0x13a8 [4280B427B81EB8C265F3206E2298761E, 121AF03BBE6ECC1622C2540805A30AE9555EB5D5FE25B55939C045ECE7FC37EB] Beep
C:\Windows\system32\drivers\Beep.sys
14:27:19.0981 0x13a8 Beep - ok
14:27:19.0981 0x13a8 [D8A5DBA443C75CD78B1C01DF119A0A0F, 547584455D91FBE5D38263BA7FD8C0D9F520894679896C3FBC98DCF01C77A3AB] BFE   C:\Windows\System32\bfe.dll
14:27:19.0997 0x13a8 BFE - ok
14:27:19.0997 0x13a8 [928FCF2A9BFB76EBC9BF07C640A03D44, 80C25C52C0AE0DE6FF4BC049C8C6BFE4021408FA862123C68B2A2B2315EFDB66] bindflt
C:\Windows\system32\drivers\bindflt.sys
14:27:19.0997 0x13a8 bindflt - ok
14:27:20.0012 0x13a8 [AC7D43F5A3E3097392A91E0095F9E8D5, 3DC267E2759C83F96BE1015B55F0907BDB80AB24AC99D3261D992ABDB9E1869B] BITS
C:\Windows\System32\qmgr.dll
14:27:20.0028 0x13a8 BITS - ok
14:27:20.0043 0x13a8 [EDA43C79608063D5395BA7F6B6D72E9C, 3CB0C0F59A35C6A0EEC3358B03B38B1B782060A786DE7D31E6BE968D810574D2] BluetoothUserService
C:\Windows\System32\Microsoft.Bluetooth.UserService.dll
14:27:20.0043 0x13a8 BluetoothUserService - ok
14:27:20.0043 0x13a8 [7880E984456D0F4513B0D76FFF868C85, C809850E9C274C9117CB881CB9996B41762E8679BBB6F27F363F4A7279417E8C] bowser
C:\Windows\system32\DRIVERS\bowser.sys
14:27:20.0043 0x13a8 bowser - ok
14:27:20.0043 0x13a8 [47283C7BEA84F84EB28011FE8758E884, D520FFD1575E2563C0166FFE1ED219F4D48A6CCCBA0D9372F61B69EFB9B9DA5A] BrokerInfrastructure
C:\Windows\System32\psmsrv.dll
14:27:20.0059 0x13a8 BrokerInfrastructure - ok
14:27:20.0059 0x13a8 [93AF20E5E98358F613662B8F637A8989, 45436028C42D78CEA48A1ACDBF2D519DD6CCCC0AAFA0AC07119FCE9288703B88] Browser
C:\Windows\System32\browser.dll
14:27:20.0059 0x13a8 Browser - ok
14:27:20.0074 0x13a8 [833A531F5EEBA7979188F0AA91E1A5D2, 32BED655AD3B3F6766E82AAB08AA280FB598BE904DF9C88748BA9CC636582307] BTAGService
C:\Windows\System32\BTAGService.dll
14:27:20.0074 0x13a8 BTAGService - ok
14:27:20.0090 0x13a8 [B508CC4293B2336BE12565B2A34302F2, E83447CDCF07A5C95997E90B4E6B50DE2236E7B1721146FFACB58D502C3A2319] BthA2dp
C:\Windows\System32\drivers\BthA2dp.sys
14:27:20.0090 0x13a8 BthA2dp - ok
14:27:20.0090 0x13a8 [29E477BE8EEAF5135EA07A09E6B9005A, 7BE4A2E0366EDD480D6E091D90C96C14456A9210957022239B7E0E77669A4646] BthAvctpSvc
C:\Windows\System32\BthAvctpSvc.dll
14:27:20.0090 0x13a8 BthAvctpSvc - ok
14:27:20.0106 0x13a8 [7E3D4882E9CE7717FD4B14FC4134674E, D315749FA9C77E69443A8C81DE0E341D600BEB236106A6254B821EF95FEBB21D] BthEnum
C:\Windows\System32\drivers\BthEnum.sys
14:27:20.0106 0x13a8 BthEnum - ok
14:27:20.0106 0x13a8 [AE49604779C44D3B345B98AE08618591, A4276D2BA483DFA59C74FCE66054C0E0202BE913EC78A3F7A29081E5C4782A85] BthHFEnum
C:\Windows\System32\drivers\bthhfenum.sys
14:27:20.0106 0x13a8 BthHFEnum - ok
14:27:20.0106 0x13a8 [E992167814BFB2B3F28EB7076BA301AE, FCA64E66FCD5FD52E73A2FE13D44C56C91F89EA4ED2F21D1160256859C4C35CF] BthLEEnum
C:\Windows\System32\drivers\Microsoft.Bluetooth.Legacy.LEEnumerator.sys
14:27:20.0106 0x13a8 BthLEEnum - ok
14:27:20.0106 0x13a8 [834FDDB2F618238279A0AF32478C7B91, 9B46F2AC6AFE4CAC8308D9C6FF826F7573AEB3D451892AE896FE0D0BAF4E0F51] BthMini
C:\Windows\System32\drivers\BTHMINI.sys
14:27:20.0106 0x13a8 BthMini - ok
14:27:20.0106 0x13a8 [11D609CC74F0EB1DF6C0171331CDE9A1, 9412DC92F16C0B8A937D6FB1AD83D7169F4EC0F08FAE0E2B244346428CE99EE1] BTHMODEM
C:\Windows\System32\drivers\bthmodem.sys
14:27:20.0121 0x13a8 BTHMODEM - ok
14:27:20.0121 0x13a8 [83016DA2C1CA3EBB1A6E7BFB688120C7, F46BF2E7B20D4A6D2158738C587E8482828D62C2E0E8210874EEB79493DC853D] BTHPORT
C:\Windows\System32\drivers\BTHport.sys
14:27:20.0138 0x13a8 BTHPORT - ok
14:27:20.0152 0x13a8 [D293AC628357F2F75B8579087F732970, 1E536D8863D695944214D55E9B0B4BFE04F705DB7ECA18A0CF8B37AAF4893B1E] bthserv
C:\Windows\system32\bthserv.dll
14:27:20.0152 0x13a8 bthserv - ok
14:27:20.0152 0x13a8 [E597CE85BD6FD2E4D23B7CE880AC7E7A, 7E9E22ACC0DE17E810442DAE3FDF58652F024ABF59B1E24B67574A2DA703829D] BTHUSB
C:\Windows\System32\drivers\BTHUSB.sys
14:27:20.0152 0x13a8 BTHUSB - ok
14:27:20.0152 0x13a8 [4FF20E869FE2B5A0B8CE2E8BE61C7F7F, 8DE3B7C87D88CF375417355A7C5052B2DE38805B563D61D0E483DB4AD96BD741] bttflt
C:\Windows\system32\drivers\bttflt.sys
14:27:20.0152 0x13a8 bttflt - ok
14:27:20.0152 0x13a8 [EF2A1F3C5EC4EFFFBE9A69B892FBA29C, 16A900FBAB30D008F01F4CAE96347BF313D9D13C7FE430249A0BF4322534CB18] buttonconverter
C:\Windows\System32\drivers\buttonconverter.sys
14:27:20.0168 0x13a8 buttonconverter - ok
14:27:20.0168 0x13a8 [E7690568D2A5FA3D4E6D28B42358A122, CDBD820B6D383EC0A8151EA4300435C2BAD085EC55DB185C5E16CAF961443888] CAD
C:\Windows\System32\drivers\CAD.sys
14:27:20.0168 0x13a8 CAD - ok
14:27:20.0168 0x13a8 [0B982E6EDEC6EAD4EADCF3C2973919AD, 0DB44964E2797629260DCFAD8190556359F6E57C7AFCF5F79B85C4A719AD218C] camsvc
C:\Windows\system32\CapabilityAccessManager.dll
14:27:20.0168 0x13a8 camsvc - ok
14:27:20.0168 0x13a8 [E889F163CFA5D6A5FA0A55775A035C27, FED20D9EC24D827B8FC96116147AA9277212E6CAE2F8B45479DD01560C75DB52] CaptureService
C:\Windows\System32\CaptureService.dll
14:27:20.0184 0x13a8 CaptureService - ok
14:27:20.0184 0x13a8 [55AAD28CCDC5E6673B88D54C200C14EB, 94603FD04428DBB0B82C423820B322DA01397A6D44EB55B1D0513D19A9FA4DFD] cbdhsvc
C:\Windows\System32\cbdhsvc.dll
14:27:20.0199 0x13a8 cbdhsvc - ok
14:27:20.0199 0x13a8 [44EDC69011C8C7C4802D320DCAA2DD85, 41354D3153017D249FFD4D7917009AA527FDE3DE08582B79D276723082AA4554] cdfs
C:\Windows\system32\DRIVERS\cdfs.sys
14:27:20.0199 0x13a8 cdfs - ok
14:27:20.0215 0x13a8 [0C5E3C60AC5827FE5B43F427F7DCAC91, 8987DA1AAFB69B320689C8FC3481D2F3082825B4566BD9B9898EB150221818D9] CDPSvc
C:\Windows\System32\CDPSvc.dll
14:27:20.0215 0x13a8 CDPSvc - ok

14:27:20.0231 0x13a8 [6BDBE34FC5F6A3229609E3D149C5FAA1, F2FE0FBB7B887CEAC8B2E705A470A4633C62E963C244E2D379B9DDBC5CA8AAF2] CDPUserSvc
C:\Windows\System32\CDPUserSvc.dll
14:27:20.0231 0x13a8 CDPUserSvc - ok
14:27:20.0231 0x13a8 [050804442DAD3428C6E7F02EB86DBEF4, EE6A4CD3B6F20A0658EE9B310BBA90FFB0585B0F72038886E1D3BEB3A6A80769] cdrom
C:\Windows\System32\drivers\cdrom.sys
14:27:20.0231 0x13a8 cdrom - ok
14:27:20.0231 0x13a8 [D0843B744F4E7E30BD74A1CF5426A44C, 8E2A05A464A9671232E25D7C0505300F2BAD6D96C2CBF4F4427D1F795621EAEF] CertPropSvc
C:\Windows\System32\certprop.dll
14:27:20.0246 0x13a8 CertPropSvc - ok
14:27:20.0246 0x13a8 [198D403332FB8F2DA289BEBFEC8199AD, 5A7FD2D58C433B9B498A1B37A2F2D877061215360D8E6A752601F2ED4F283A8F] cht4iscsi
C:\Windows\system32\drivers\cht4sx64.sys
14:27:20.0246 0x13a8 cht4iscsi - ok
14:27:20.0262 0x13a8 [77065056FBE4E29054CB1D20303B9F59, 83E2C81274DDBE695EF845E541F7A2DB60EF5E195AE14FACDEEEBD30C0EF4E67] cht4vbd
C:\Windows\System32\drivers\cht4vx64.sys
14:27:20.0293 0x13a8 cht4vbd - ok
14:27:20.0293 0x13a8 [9C00DAF72B049951C39571B9E1FBD484, 8C48F09C6D4EBE9463D089024EBCC69237CB5CF2F18D8E8F0EB82F6E54E3F8B5] CimFS
C:\Windows\system32\drivers\CimFS.sys
14:27:20.0293 0x13a8 CimFS - ok
14:27:20.0293 0x13a8 [115CC1E142CE29C9006D59943108DF47, 564FA08C5BEC6DAF1A83C80C9139A6E1AA7E05D251DB3BA379B57C9FDAE83E1B] circlass
C:\Windows\System32\drivers\circlass.sys
14:27:20.0293 0x13a8 circlass - ok
14:27:20.0293 0x13a8 [44373E2F0C1B85F8A19BCAE46BFB3536, BB67EEFE6E56013829EC949D5C7C9DBB8CCFD2DC40965E1DD472290B5E34BD79] CldFlt
C:\Windows\system32\drivers\cldflt.sys
14:27:20.0309 0x13a8 CldFlt - ok
14:27:20.0309 0x13a8 [3E37BC55ABF85997534998A58B616422, FC960EB2580D128EB8D4465E083D97F9A937D1CFED3B92198FC7A6F4CCDDCF44] CLFS
C:\Windows\system32\drivers\CLFS.sys
14:27:20.0309 0x13a8 CLFS - ok
14:27:20.0325 0x13a8 [4BBEFD079975622BC1630A2C3F097ED4, 31935CC8E72490805B1DEB1CE5E0B67C35C521B6D1AE7C1B455E088F35BDA097] ClipSVC
C:\Windows\System32\ClipSVC.dll
14:27:20.0340 0x13a8 ClipSVC - ok
14:27:20.0340 0x13a8 [E127E772A705CD32BE34166F679C61C8, 2097236323694043 08EF6DF734077A99A295C2E380DB85AD1F8498CC8DFBC88A] CmBatt
C:\Windows\System32\drivers\CmBatt.sys
14:27:20.0340 0x13a8 CmBatt - ok
14:27:20.0355 0x13a8 [D9DC1EC71B9083C7BDBE645E60CDA4FD, 26889542E5FFFB60A60EA2E704E1A080B55B0634D34D1C2F9D25D4060E7A7CFD] CNG
C:\Windows\system32\Drivers\cng.sys
14:27:20.0355 0x13a8 CNG - ok
14:27:20.0355 0x13a8 [A46B4D1484227900F7615FE2A569D828, A06B8002E7A708890222C777DDF8B67FED7015C0943C1FC4F9036E9F9DC14494] cnghwassist
C:\Windows\system32\DRIVERS\cnghwassist.sys
14:27:20.0355 0x13a8 cnghwassist - ok
14:27:20.0371 0x13a8 [99392FDADF3CE5EB47403E5A52866E6F, 63CEF51971EB85D9823CE9A95F1ED9907D20525ED8E32230068CC36E9082A8C3] CompositeBus
C:\Windows\System32\DriverStore\FileRepository\compositebus.inf_amd64_7500cffa210c6946\CompositeBus.sys
14:27:20.0371 0x13a8 CompositeBus - ok
14:27:20.0371 0x13a8 COMSysApp - ok
14:27:20.0371 0x13a8 [E1E1F5198DF9E784DDA895398736A691, 31991225A505F0D375F8DEECB55A7D080FD3A04558983B76AB7C45B799B1D9A4] condrv
C:\Windows\system32\drivers\condrv.sys
14:27:20.0371 0x13a8 condrv - ok
14:27:20.0371 0x13a8 [9864B10556D39F7FC5BBF6D4DE4F7B73, FFAC481CFF223F3D55B1797DCA06F4473412DF7A86CD32B8664976618B22BF05] ConsentUxUserSvc
C:\Windows\System32\ConsentUxClient.dll
14:27:20.0371 0x13a8 ConsentUxUserSvc - ok
14:27:20.0387 0x13a8 [1D2942A5A7E13D49077EE0365E45072D, 89067221C8D7F8661513AEDFF11DB34AA9C2B57C3E812EC9D9D76AAEF6AE2DBE] CoreMessagingRegistrar
C:\Windows\system32\coremessaging.dll
14:27:20.0387 0x13a8 CoreMessagingRegistrar - ok
14:27:20.0403 0x13a8 [C05A15022C00CC3D19FB034D89BE9418, 8FB6567263EB215333D159BD2658224B659096816EEB4CE7F8D87263A5FB7F74] CredentialEnrollmentManagerUserSvc
C:\Windows\system32\CredentialEnrollmentManager.exe
14:27:20.0403 0x13a8 CredentialEnrollmentManagerUserSvc - ok
14:27:20.0403 0x13a8 [C05A15022C00CC3D19FB034D89BE9418, 8FB6567263EB215333D159BD2658224B659096816EEB4CE7F8D87263A5FB7F74]
CredentialEnrollmentManagerUserSvc_30901 C:\Windows\system32\CredentialEnrollmentManager.exe
14:27:20.0418 0x13a8 CredentialEnrollmentManagerUserSvc_30901 - ok
14:27:20.0418 0x13a8 [8AB3568419872D1A8A7B45153AF7B3D4, 5171ED876E0EC5CAE2BE9161ACC90F4865FF6416EFA376C82D8A5B65724A8910] CryptSvc
C:\Windows\system32\cryptsvc.dll
14:27:20.0418 0x13a8 CryptSvc - ok
14:27:20.0418 0x13a8 [12DE0DE630EE25149CE30303B9661AEE, 9C3E86A9842EBCFE3A43F1B51809B2F8397D3B091368881BD6B4A8BCADB301ED] dam
C:\Windows\system32\drivers\dam.sys
14:27:20.0418 0x13a8 dam - ok
14:27:20.0434 0x13a8 [5A344C5D2140BD836AE545A9351373F4, 1C1DEF25FB645F9789A41F8533ECB144680F36D5F3B91B806D2DED972B1A0203] DcomLaunch
C:\Windows\system32\rpcss.dll
14:27:20.0449 0x13a8 DcomLaunch - ok
14:27:20.0465 0x13a8 [92173A69EB75DF92955E7EE12D68E346, 5A43143EF22336DB82B4FD77D066951232E98F74237289DF124D17DD0F1480AC] dcsvc
C:\Windows\system32\dcsvc.dll
14:27:20.0465 0x13a8 dcsvc - ok
14:27:20.0481 0x13a8 [EBA8DD2A13A0B623E8F5316D2C8CE8E0, 0DF0B642ECB53625B1DC2C7D1EC66A32AE1799B78F45239D85F066D85D11B2A0] defragsvc
C:\Windows\System32\defragsvc.dll
14:27:20.0481 0x13a8 defragsvc - ok
14:27:20.0481 0x13a8 [F551C7E5CFA7D2AB0758393F61B2E8DA, 07751C35B9C7BC0ABBB2A3C459EBFA52F45148913261A4C83258DF10DD2924A6] DeviceAssociationBrokerSvc
C:\Windows\System32\deviceaccess.dll
14:27:20.0481 0x13a8 DeviceAssociationBrokerSvc - ok
14:27:20.0496 0x13a8 [0BA4032BA0F8155DC017D29E11BE9C71, BF872BEE20D3208CC105019F8837A0606D236524F76B77D203848139 01DBE220] DeviceAssociationService
C:\Windows\system32\das.dll
14:27:20.0496 0x13a8 DeviceAssociationService - ok
14:27:20.0496 0x13a8 [73EE8DC7CBEAB344DA440676B9DD4F43, 9535A927C3A16BF5EB23F975CC50251B33F4982E47D357EFD6BF3736C544792A] DeviceInstall
C:\Windows\system32\umpnpmgr.dll
14:27:20.0496 0x13a8 DeviceInstall - ok
14:27:20.0512 0x13a8 [2CC6992894F23399DA9B6B2BE2CA5FD9, A8E1AB82B623952C5720B12E1E119650DCCBE29C7FEC590FC5AA1884E652A3 40] DevicePickerUserSvc
C:\Windows\System32\Windows.Devices.Picker.dll
14:27:20.0512 0x13a8 DevicePickerUserSvc - ok
14:27:20.0527 0x13a8 [8CE23DD2F7AD3FA0D9093B862DB755AC, CD8CEFF82CE29F47B7C55CDBA39C45C0077994B01276D5C3D3E02A52F514902B] DevicesFlowUserSvc
C:\Windows\System32\DevicesFlowBroker.dll
14:27:20.0527 0x13a8 DevicesFlowUserSvc - ok
14:27:20.0527 0x13a8 [F8BE99B9EA9B110F7CB3F46BA844C1FF, EABF953864C0AE4FB6426C0B7E92DD81EE4A8852081F9D2EA02B61D4C8DB6188] DevQueryBroker
C:\Windows\system32\DevQueryBroker.dll
14:27:20.0527 0x13a8 DevQueryBroker - ok
14:27:20.0543 0x13a8 [C4BB07F3246B853D6473BDF468EB6A10, 7F59FFE78257AF0DD79B3A515966BADF8E5A77C739743AF8A2FB4E3D8675545A] Dfsc
C:\Windows\system32\Drivers\dfsc.sys
14:27:20.0543 0x13a8 Dfsc - ok
14:27:20.0543 0x13a8 [3A57324322740143 75C4D98149F3729C, 2B514B5712C533AF66ABC44AC9CA2358355E1EF2BC30D4CB2B04DF8E0BC3C496] Dhcp
C:\Windows\system32\dhcpcore.dll
14:27:20.0543 0x13a8 Dhcp - ok
14:27:20.0543 0x13a8 [92E340FAA5F4EDEAA4FC1A1F982C601A, 42E4BE3749F5C1817B9AAF641F5E9AADFAA7F8D7AC93C90D6D86DA2E4E3E1A54] diagnosticshub.standardcollector.service
C:\Windows\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe
14:27:20.0559 0x13a8 diagnosticshub.standardcollector.service - ok
14:27:20.0559 0x13a8 [83521C317CCBF325D877C421E9D14BC9, D50F185CA024100E6748983D8C5721BAC5F775347D9F7958D4F82C02157F2B4D] diagsvc
C:\Windows\system32\DiagSvc.dll
14:27:20.0559 0x13a8 diagsvc - ok
14:27:20.0590 0x13a8 [9749F08B43D3AADCDC1688F791092A2A, 55BBAF6BE67096B0D58774927D6B1880C95826CD7787D66553CCA1495EE2CC23] DiagTrack
C:\Windows\system32\diagtrack.dll
14:27:20.0621 0x13a8 DiagTrack - ok
14:27:20.0637 0x13a8 [78D62E87AAFEA823FFBE4E1D7B26BD50, ED408F8E4B654AF8D54AFA1ED6B18BAC8C76DF535DDEF9F038D6831CCBC2E27A] disk
C:\Windows\system32\drivers\disk.sys
14:27:20.0637 0x13a8 disk - ok
14:27:20.0637 0x13a8 [619D3165454D8C8F24AFA6D9938856E5, 238550045E082BC2B2087F946FA4F8B8C8D5D1D4012D75E34D4C1722EC96B1EE] DispBrokerDesktopSvc
C:\Windows\System32\DispBroker.Desktop.dll
14:27:20.0637 0x13a8 DispBrokerDesktopSvc - ok
14:27:20.0652 0x13a8 [F2528F2A9C25BFA2DC135819438EB732, 68F8F85CABFF6905CBF51D7CF5CF2A59801254ACBAD0F00E6071EB307932B989] DisplayEnhancementService
C:\Windows\system32\Microsoft.Graphics.Display.DisplayEnhancementService.dll

14:27:20.0668 0x13a8 DisplayEnhancementService - ok
14:27:20.0684 0x13a8 [BA05D2B56648F9C63029938041EB346D, 799D37078318B386A2F2D02ADACBDC2BC4D54EC9AD235BE8964D927F9393CA84] DmEnrollmentSvc
C:\Windows\system32\Windows.Internal.Management.dll
14:27:20.0699 0x13a8 DmEnrollmentSvc - ok
14:27:20.0699 0x13a8 [48AA813AAA7E347CD7D6D56FE32144C6, 6604DC0E7607E46B83F1239934646AC4ADF5CA4CC463FB9DF521B243F434579B] dmvsc
C:\Windows\System32\drivers\dmvsc.sys
14:27:20.0699 0x13a8 dmvsc - ok
14:27:20.0699 0x13a8 [F24BD3A6EF5FB5C49163EF8E8D78AF63, B8F89F003F28BCE0D933E9C2490FDC7EB11CAF6928DBC6E91461A4AD72E88880] dmwappushservice
C:\Windows\system32\dmwappushsvc.dll
14:27:20.0699 0x13a8 dmwappushservice - ok
14:27:20.0699 0x13a8 [B483E908D662A4B2383C52561972379F, 9676EE9DC2A0BEE813218CE1C735DC8DC1A343573392CA71699DCA737AE654F3] Dnscache
C:\Windows\System32\dnsrslvr.dll
14:27:20.0715 0x13a8 Dnscache - ok
14:27:20.0715 0x13a8 [1E3B65845E952CF5D7291D6D4BA6CECD, 599EB61D1DE9CD2712F8B63A963F8EDFF540E1883CDE3A1E2730C9D5B92AC368] dot3svc
C:\Windows\System32\dot3svc.dll
14:27:20.0715 0x13a8 dot3svc - ok
14:27:20.0715 0x13a8 [9E65C33CB7FB50453F7F4407070EAF53, A8707BD19D584DAECA39990A2E791194140AFCA4FCE31F23CC7E931DF8C17361] DPS   C:\Windows\system32\dps.dll
14:27:20.0730 0x13a8 DPS - ok
14:27:20.0730 0x13a8 [8A11EDDA5257886A5788CDBA894EB7C9, F9753304AD59A01F29BBCC8F2CFDC592FAE96CD2B2A4350D2C6CE7F6D3C99B1C] drmkaud
C:\Windows\System32\drivers\drmkaud.sys
14:27:20.0730 0x13a8 drmkaud - ok
14:27:20.0730 0x13a8 [DA9FAF551FC9CE219F79366C44E322D2, 00325631922853F499826F074BC9748303AA841AB37FEB0D0CA636DEA694AEFE] DsmSvc
C:\Windows\System32\DeviceSetupManager.dll
14:27:20.0730 0x13a8 DsmSvc - ok
14:27:20.0730 0x13a8 [8A561D97BAA2A2EDA494B4E2D5E073F3, A24D84E6EF004EE6A6B9AD015A4A9B6E844FED8C4DD6F3B28DA2FF43A723139A] DsSvc
C:\Windows\System32\DsSvc.dll
14:27:20.0746 0x13a8 DsSvc - ok
14:27:20.0746 0x13a8 [81DF23EC4009D307479D5C169539CD67, 65AEE1E876CBE801A763F14930D15CF2E6A10697620B5903AA04BA30585A5676] DusmSvc
C:\Windows\System32\dusmsvc.dll
14:27:20.0746 0x13a8 DusmSvc - ok
14:27:20.0778 0x13a8 [4D8FEC5D09BDF2BBCB2BC0E723FDA9B1, 79229694FABE8EE0EB308999ED8C5DCE9AA5D60DD26C8AB186D9FF8A6FC7AC6E] DXGKrnl
C:\Windows\System32\drivers\dxgkrnl.sys
14:27:20.0824 0x13a8 DXGKrnl - ok
14:27:20.0824 0x13a8 [CCED99682127E8582E5F716ECE775EF8, 3B0A51E1FC4D5BD3E7EC182799AD712AEEAF1DCD761D7E98BEC8A0A67F7334AF] E1G60
C:\Windows\System32\drivers\E1G6032E.sys
14:27:20.0824 0x13a8 E1G60 - ok
14:27:20.0824 0x13a8 [AF7B5676A104F8A7D87DDA84DDFD5240, C89BE2506C647924E94FA2F44AA4AF9EAA2F794FA444C8854FEA5B3F563AC185] Eaphost
C:\Windows\System32\eapsvc.dll
14:27:20.0824 0x13a8 Eaphost - ok
14:27:20.0871 0x13a8 [E7B7E38AD720352CFE9A5FF3A82AB124, 48D9F61E943A7855562950FF26B866BD51A27D980757B065504FCD3F1A1D6F07] ebdrv
C:\Windows\system32\drivers\evbda.sys
14:27:20.0903 0x13a8 ebdrv - ok
14:27:20.0903 0x13a8 [C019E421D9F897108E51666CBAE2C8B0, 3096D8E82917A9B73F322F4B1743E52E9B0C8B3C5933A957E73E29D6973CDD5B] edgeupdate   C:\Program Files
(x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
14:27:20.0903 0x13a8 edgeupdate - ok
14:27:20.0918 0x13a8 [C019E421D9F897108E51666CBAE2C8B0, 3096D8E82917A9B73F322F4B1743E52E9B0C8B3C5933A957E73E29D6973CDD5B] edgeupdatem   C:\Program Files
(x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
14:27:20.0918 0x13a8 edgeupdatem - ok
14:27:20.0918 0x13a8 [B4DE3D04AE3C71E67236B841BEADEB74, 8567CDBA80952B2B7AF647B9D2630FE12B73E87517498BCCDCC27EC1ED6E1545] EFS
C:\Windows\System32\lsass.exe
14:27:20.0918 0x13a8 EFS - ok
14:27:20.0918 0x13a8 [A03C16B3BC08469B74378DC7FFBF308F, 3BAA0C59FD72DDB3E806B849D07FD17AF1FA65D41E67A6A69440E927B3062ED0] EhStorClass
C:\Windows\system32\drivers\EhStorClass.sys
14:27:20.0918 0x13a8 EhStorClass - ok
14:27:20.0918 0x13a8 [9F04CF369B93A78B2E56A3DF9B41F25F, 514A0687D2ABE6C52D6BFF8F0F5E47DD77EBEEDC4E6C6539B05BD0EC27B6704D] EhStorTcgDrv
C:\Windows\system32\drivers\EhStorTcgDrv.sys
14:27:20.0918 0x13a8 EhStorTcgDrv - ok
14:27:20.0934 0x13a8 [BBA65A8FE53F6DE18F63D680441FB885, 3F9413D31AEADCF83AE1A43E7B3FD989760675416A0A3745A95CE3C4993EB233] embeddedmode
C:\Windows\System32\embeddedmodesvc.dll
14:27:20.0934 0x13a8 embeddedmode - ok
14:27:20.0934 0x13a8 [3E301BE942FB2DF11617B0C12E57CB1A, 47386ED2FB1274715562EAF0757421B908514D1E76EAED9065408030069C72F4] EntAppSvc
C:\Windows\system32\EnterpriseAppMgmtSvc.dll
14:27:20.0949 0x13a8 EntAppSvc - ok
14:27:20.0949 0x13a8 [E87F3FA1F9133DEEC1B3692976487777, BF14DB2762B48ACE54977E98DC2A4060B8B1122B58FDEFBB4C84546ABEB410A5] ErrDev
C:\Windows\System32\drivers\errdev.sys
14:27:20.0949 0x13a8 ErrDev - ok
14:27:20.0965 0x13a8 [1954A92911AF72C0CF1CE51B6433AB65, B08AF5CE5440212522886495227749323EA082088ACEACC5118CB789B828AA99] EventLog
C:\Windows\System32\wevtsvc.dll
14:27:20.0980 0x13a8 EventLog - ok
14:27:20.0996 0x13a8 [7EDEC0DABFD8F2009F46EC1829E1FCC6, 06F7F1DC8FAE85C0560E2E9905D3E97B8A70ECF6689DC9A72B85941F303D8685] EventSystem
C:\Windows\system32\es.dll
14:27:20.0996 0x13a8 EventSystem - ok
14:27:20.0996 0x13a8 [F17A9B2716AAC231F1A0B7934F660307, E861C999C70D4A68976D3056D9F34C24BB88A03906DB402F5FC21E14F5A06036] exfat
C:\Windows\system32\drivers\exfat.sys
14:27:20.0996 0x13a8 exfat - ok
14:27:21.0012 0x13a8 [310154D9B2A6B25C251E04A715C9904D, 4F994B714160ABB8D6318A77A1DC5DC1C30B2042C3341102BD7A69A8DC3DB2AF] fastfat
C:\Windows\system32\drivers\fastfat.sys
14:27:21.0012 0x13a8 fastfat - ok
14:27:21.0028 0x13a8 [D94DF8349B8E387A809735930BB062D8, 9BA451EF593B7056F2DBC6388336CB9C0285D1A88839C362344D94591FFEF4DE] Fax
C:\Windows\system32\fxssvc.exe
14:27:21.0028 0x13a8 Fax - ok
14:27:21.0028 0x13a8 [F567A0C101AECF4548E0BF61EE25D332, 26BC9C2F1D42CE5BEF55E98DC0DA557F09B747186580C796003CF84229F6D151] fdc
C:\Windows\System32\drivers\fdc.sys
14:27:21.0028 0x13a8 fdc - ok
14:27:21.0028 0x13a8 [0439B82F6034ADA3E71C0C9F169082BD, 0918728669077235B2F2DB7EE22CE819FA570D8A7A497BA5F11E76774EA75099] fdPHost
C:\Windows\system32\fdPHost.dll
14:27:21.0028 0x13a8 fdPHost - ok
14:27:21.0028 0x13a8 [AD64C91B3CC71226785DCE688842E5AB, 056E1091468D268E7970045AB329EB3DFF48BB6B22448046A14C309678847B6E] FDResPub
C:\Windows\system32\fdrespub.dll
14:27:21.0043 0x13a8 FDResPub - ok
14:27:21.0043 0x13a8 [78A98E902D87BE26600530275D94FFE5, 73CC6944F351B22ACEF9358B94372FD4D538F2F56E2897F4C443D1AA373E8015] fhsvc   C:\Windows\system32\fhsvc.dll
14:27:21.0043 0x13a8 fhsvc - ok
14:27:21.0043 0x13a8 [8E59D944EE4EFAED65A341A71297C4CD, CFFFD7007AB7FB04ECB44D0079BFE8EEB53AECC988135199C388AF425EBCF2AD] FileCrypt
C:\Windows\system32\drivers\filecrypt.sys
14:27:21.0043 0x13a8 FileCrypt - ok
14:27:21.0043 0x13a8 [EE7605E60374CBD2DDAAA120FA2E458A, 832BF32B9EFA04FBDD9638D00B209DFC88C4C69E0AEC7FF1B5AD4DDEC0F20878] FileInfo
C:\Windows\system32\drivers\fileinfo.sys
14:27:21.0043 0x13a8 FileInfo - ok
14:27:21.0043 0x13a8 [C7F6F4B73E410087C6DE5658AAD70232, 42C56B93FF52CAC5B74CE0A16D9D4425E8B3E690B3BD76A5A3C657655B62A34A] Filetrace
C:\Windows\system32\drivers\filetrace.sys
14:27:21.0043 0x13a8 Filetrace - ok
14:27:21.0058 0x13a8 [C867FE1865F45469DD96957900073361, 1534A840C56912D34DEC8F487683C0A782070A89726BF87DFAAF7F953A18A1DA] flpydisk
C:\Windows\System32\drivers\flpydisk.sys
14:27:21.0058 0x13a8 flpydisk - ok
14:27:21.0058 0x13a8 [A04557215A602894DC3CC4F2A232C023, 6EED0DDD85F468B93460076027588757B53BC658D1F636E485A8CE9155E8104D] FltMgr
C:\Windows\system32\drivers\fltmgr.sys
14:27:21.0058 0x13a8 FltMgr - ok
14:27:21.0075 0x13a8 [0585E7B386121BC2EBBA5D7200AEE01A, 6EC4701DA52D64F6BD8BEE0D2BED9D7A6927876C85D94B4EB5F57720F1ED7CB5] FontCache
C:\Windows\system32\FntCache.dll
14:27:21.0090 0x13a8 FontCache - ok
14:27:21.0090 0x13a8 [91857D4F6633493CF03C22BD86ED7F81, 80982C4DA12FDD501C234782A14243DFFA8AA4D6EB94BA5E37E3575ADE53000D] FontCache3.0.0.0
C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
14:27:21.0090 0x13a8 FontCache3.0.0.0 - ok

14:27:21.0106 0x13a8 [22A078B224FD504B15B4D68FD05B86E3, FD41E6B2645D7B3518CCD243901EFF81EC3CA90B8578489911C4D9ACD6619D8E] FrameServer
C:\Windows\system32\FrameServer.dll
14:27:21.0121 0x13a8 FrameServer - ok
14:27:21.0121 0x13a8 [BFCF35E5365C4DF006C376A26487853C, 2284CC336BD9AF6DF98928C94BAE26D060BC0E7CA56CFDCBC3F7194BE240E57E] FsDepends
C:\Windows\system32\drivers\FsDepends.sys
14:27:21.0121 0x13a8 FsDepends - ok
14:27:21.0121 0x13a8 [A3631ADDD926826110A436D6A04B31CA, 2073327E5C1E542EA2740CA0D43204940EB72652619B5209A2E4A4A0FB18D20A] Fs_Rec
C:\Windows\system32\drivers\Fs_Rec.sys
14:27:21.0121 0x13a8 Fs_Rec - ok
14:27:21.0137 0x13a8 [25E63BA86AF3320BF40A0D5EA0EE0352, 5D9533D562D229B627A9D6B177E736D5B2606A67B1998F001774C913B4AED0B8] fvevol
C:\Windows\system32\DRIVERS\fvevol.sys
14:27:21.0137 0x13a8 fvevol - ok
14:27:21.0137 0x13a8 [A1E06E4E8CB863C74DE428D4D6681185, DA46502C009FD4C847A547610DEE2684A5A583467BF76009BD46104AAE2F6B1B] gencounter
C:\Windows\System32\drivers\vmgencounter.sys
14:27:21.0137 0x13a8 gencounter - ok
14:27:21.0137 0x13a8 [DF2344160D1E58AB5E1DDB174D46853D, B263D352479812A4DEB6BB8AF573150491EA9F5D55DCD00185AF6759FF2601F6] genericusbfn
C:\Windows\System32\DriverStore\FileRepository\genericusbfn.inf_amd64_53931f0ae21d6d2c\genericusbfn.sys
14:27:21.0152 0x13a8 genericusbfn - ok
14:27:21.0152 0x13a8 [596E544EB9110CB258530812F18C8529, 90837CCE27E7B9C4BD30D0280D22BDAAA3B227A632BA8FA7BF01B1BEB9EEE0D4] GPIOClx0101
C:\Windows\system32\Drivers\msgpioclx.sys
14:27:21.0152 0x13a8 GPIOClx0101 - ok
14:27:21.0168 0x13a8 [E1761F8FEAED19FB886D4C397C024C4D, B5C20275A2C658650C5C8A2ECE93F19B7603CDDE519EDC589F6BEDD575485CA3] gpsvc
C:\Windows\System32\gpsvc.dll
14:27:21.0184 0x13a8 gpsvc - ok
14:27:21.0184 0x13a8 [8C06046B6A8C1ACDAEA15682058FDFB4, 3E0CC301249B7D8D5BEB932F4DFD1EAB8037679EC153772F63B430713903B0AC] GpuEnergyDrv
C:\Windows\system32\drivers\gpuenergydrv.sys
14:27:21.0184 0x13a8 GpuEnergyDrv - ok
14:27:21.0184 0x13a8 [0B0D41B3043B941E1B52DF3CB0ABD65E, 2AB425B46C1016243402A1D4634AFE6D41CFF847843DA4DB33F016D3A9134CB5] GraphicsPerfSvc
C:\Windows\System32\GraphicsPerfSvc.dll
14:27:21.0184 0x13a8 GraphicsPerfSvc - ok
14:27:21.0184 0x13a8 [74B792FB24E372FEA93E36981AA2C993, 52D9FA9E6923B2E0F79DFFDB4DA0BDB28A7973FBB4815A208F64620CC543D390] HdAudAddService
C:\Windows\System32\drivers\HdAudio.sys
14:27:21.0199 0x13a8 HdAudAddService - ok
14:27:21.0199 0x13a8 [7F5C738256606DF98AC670979ECF3D928, 12798A6EC9E4148F4FD9CBD37D7E567235614163B84E5EA6BD42AA94ECAFE6F9] HDAudBus
C:\Windows\System32\drivers\HDAudBus.sys
14:27:21.0199 0x13a8 HDAudBus - ok
14:27:21.0199 0x13a8 [05FC1B768ACB2D5CADDCA2F2E89F579C, D773640F980BF832D74FBB5E19FC1FFC06F9401C10698C0C26CFB7C067F3DB73] HidBatt
C:\Windows\System32\drivers\HidBatt.sys
14:27:21.0199 0x13a8 HidBatt - ok
14:27:21.0199 0x13a8 [9A8C89D7C563049A3E37FA4E98EABFA4, 5F129D9A8BBF79DEA60E5B22094261DED89761848AB8481227C199519F503687] HidBth
C:\Windows\System32\drivers\hidbth.sys
14:27:21.0199 0x13a8 HidBth - ok
14:27:21.0215 0x13a8 [1E129E905072A79282D6CC929284DFE5, C161D2122638690CE4DA546CE8827B4BBD96747A4A7D799A776FEC5BC57D1582] hidi2c
C:\Windows\System32\drivers\hidi2c.sys
14:27:21.0215 0x13a8 hidi2c - ok
14:27:21.0215 0x13a8 [1E9F3C9B201614CF4816C5D5B6C570D8, 60CF06F1668FFFB870E76D8231A090AB3AD7EA44F1F45A36FC28814CC845B94D] hidinterrupt
C:\Windows\System32\drivers\hidinterrupt.sys
14:27:21.0215 0x13a8 hidinterrupt - ok
14:27:21.0215 0x13a8 [6B46E3061EC0523CB46ED28060FCD946, 6089305AF73CC584963865482448CD5CA4252EC9BD3E72AF16D45E4F95C3EBF2] HidIr
C:\Windows\System32\drivers\hidir.sys
14:27:21.0215 0x13a8 HidIr - ok
14:27:21.0215 0x13a8 [2A41AF60430E686985E9101C07A77B80, 2B6EC0692A09E5943C5BBA0E3AEFC746E96412E1836C84B1857B4DCF242DD28B] hidserv
C:\Windows\system32\hidserv.dll
14:27:21.0215 0x13a8 hidserv - ok
14:27:21.0215 0x13a8 [1F355AE0AEA1CDE6AD27CB6C63522FB4, 0303FA32EA2D78F37446CC28ED7B35C6B8EF88ABA1E4800463532ECCA081FFA5] hidspi
C:\Windows\System32\drivers\hidspi.sys
14:27:21.0230 0x13a8 hidspi - ok
14:27:21.0230 0x13a8 [1AD03347E3D050B0383016C70085A2FC, 4967091F13F5912F828824C4FE28AC69A961B076DA24F79FD97BD125DD093D49] HidSpiCx
C:\Windows\system32\drivers\HidSpiCx.sys
14:27:21.0230 0x13a8 HidSpiCx - ok
14:27:21.0230 0x13a8 [C79631159CD02EC7E2EBEB98A646DFF6, 2B85B64DAA955C19E44C69CD042B07D15DF8526953E07ECA7B618A8CAF15C48D] HidUsb
C:\Windows\System32\drivers\hidusb.sys
14:27:21.0230 0x13a8 HidUsb - ok
14:27:21.0230 0x13a8 [530C0E730B5E6BA332FB4AC98F760789, 0ADE20523619D5705B941591DF0C19D6B0030F96FECEBBC7A4ADEF963A476383] HpSAMD
C:\Windows\system32\drivers\HpSAMD.sys
14:27:21.0230 0x13a8 HpSAMD - ok
14:27:21.0246 0x13a8 [E307338CEECC6032B652755EB7E52C00, A100A9C9E6A699E4FFB2C8FCBAAE246DF1F493CD9B16990C1322CB838B5A0CAF] HTTP
C:\Windows\system32\drivers\HTTP.sys
14:27:21.0262 0x13a8 HTTP - ok
14:27:21.0262 0x13a8 [2692243C220CAA68C08318D3C8C4D9CE, 21BA06FF864031CDD47A4F361084FB32635779F4690608D59DBFA4A431FCEB9F] hvcrash
C:\Windows\System32\drivers\hvcrash.sys
14:27:21.0262 0x13a8 hvcrash - ok
14:27:21.0277 0x13a8 [855F55BB462B7D8B6BC31A94A592DF3D, 776C772E69CF9D81D8511201813DD79F2106DC7D2547B4FA700432AE9B73C202] HvHost
C:\Windows\System32\hvhostsvc.dll
14:27:21.0277 0x13a8 HvHost - ok
14:27:21.0277 0x13a8 [E8344EA5FC9BA8392BFF3B594493ABD0, 9E952D0A8E64FB13E782C6B912BF5A15BEBBDAD1BECC60A5B50978C3E13FE3B5] hvservice
C:\Windows\system32\drivers\hvservice.sys
14:27:21.0277 0x13a8 hvservice - ok
14:27:21.0277 0x13a8 [5DC7DFED5FEDD923B874B51D0C6752BB, 69714A8B74EB02282572B34E156051FFC10693B816905CE18A8C6C8CCB95B846] HwNClx0101
C:\Windows\system32\Drivers\mshwnclx.sys
14:27:21.0277 0x13a8 HwNClx0101 - ok
14:27:21.0277 0x13a8 [72ADA5C5DED6013BC10CFE70B7E8AB22, AEAFCC774068985775E1E64A70FAD7B2B803B276B149266C3A455F1DC94665A9] hwpolicy
C:\Windows\system32\drivers\hwpolicy.sys
14:27:21.0277 0x13a8 hwpolicy - ok
14:27:21.0277 0x13a8 [22362F7C8B7B1456DDF019BFB0523C26, 3DCA435A621FC3CD786E02D013B363ADA9399839E0A31F2969E094F69AD3A183] hyperkbd
C:\Windows\System32\drivers\hyperkbd.sys
14:27:21.0277 0x13a8 hyperkbd - ok
14:27:21.0294 0x13a8 [92467EB53970CA7338F7586392823E7C, 03AD4A49F442F273616AC9513D4D732971A0F7040DF197328B5D166F0F617C26] HyperVideo
C:\Windows\System32\drivers\HyperVideo.sys
14:27:21.0294 0x13a8 HyperVideo - ok
14:27:21.0294 0x13a8 [E4B36C6EAAAB703CBFECB92EE590FB31, E1887A4E678BBA7226E7EBE5B49EC821C2F23642D321A9E1513F7477E4B9340D] i8042prt
C:\Windows\System32\drivers\i8042prt.sys
14:27:21.0294 0x13a8 i8042prt - ok
14:27:21.0294 0x13a8 [9E5AECAB5F05218D9AC923E7CEA1CE15, FAAA46F22944E043A90AE6E9F0F86AF187FC2819C563DA375B2A409347BB2C35] iagpio
C:\Windows\System32\drivers\iagpio.sys
14:27:21.0294 0x13a8 iagpio - ok
14:27:21.0294 0x13a8 [48EDB9B5DAB7D294951A520330F13715, 9296A14590DFD94A3C728CAF3CA91BA211F27974F9CFF8417CDDC00D1453315C] iai2c
C:\Windows\System32\drivers\iai2c.sys
14:27:21.0294 0x13a8 iai2c - ok
14:27:21.0294 0x13a8 [6C3EDE394C71D5A67A504F55E35B6F47, 6FF5D13EF69E8FBCB4772C7B5C4D5770C78E0B29F9164FA1611EFDE91CE876BE] iaLPSS2i_GPIO2
C:\Windows\System32\drivers\iaLPSS2i_GPIO2.sys
14:27:21.0309 0x13a8 iaLPSS2i_GPIO2 - ok
14:27:21.0309 0x13a8 [806D14CEAF25E5F2DFCBA8E7E33B86BB, 2141DE558461B592D4111A0388D1AAC8062FA72CD1E2A2D2D68279A9633288E9] iaLPSS2i_GPIO2_BXT_P
C:\Windows\System32\drivers\iaLPSS2i_GPIO2_BXT_P.sys
14:27:21.0309 0x13a8 iaLPSS2i_GPIO2_BXT_P - ok
14:27:21.0309 0x13a8 [87DDDAE1693484BD0A210C877BDA00C2, E353D90D0B79A70F976FD5EA1CB7E25A97835E25116962EA035424715B2F43FE] iaLPSS2i_GPIO2_CNL
C:\Windows\System32\drivers\iaLPSS2i_GPIO2_CNL.sys
14:27:21.0309 0x13a8 iaLPSS2i_GPIO2_CNL - ok
14:27:21.0309 0x13a8 [8D3E3C4313673E3BA632B4396CA662E1A, 71FDC25244298D62A335769D6ED43394C33FBD8DB05AA54CA924A2977F37858F] iaLPSS2i_GPIO2_GLK
C:\Windows\System32\drivers\iaLPSS2i_GPIO2_GLK.sys
14:27:21.0309 0x13a8 iaLPSS2i_GPIO2_GLK - ok
14:27:21.0325 0x13a8 [149F1260537C4F68C3F67C363B62F3C5, 3F1F9EC7571D0F82D3F5BBA298965491260708F05EBAAA2CC23483521A5FF079] iaLPSS2i_I2C
C:\Windows\System32\drivers\iaLPSS2i_I2C.sys
14:27:21.0325 0x13a8 iaLPSS2i_I2C - ok

14:27:21.0325 0x13a8 [3E641E905A6DBF29CBA1E72BBE349808, BF354297A55713D9E2DD4044D42810C007733EE54D5A80D58B96DD279D92C716] iaLPSS2i_I2C_BXT_P
C:\Windows\System32\drivers\iaLPSS2i_I2C_BXT_P.sys
14:27:21.0325 0x13a8 iaLPSS2i_I2C_BXT_P - ok
14:27:21.0325 0x13a8 [897478D8FACEAE8681F6F3502201EC68, F105EDD16E38F5C0044CC7139E4084A04B0AE3212171A1C7F6FE759F3F5F77FC] iaLPSS2i_I2C_CNL
C:\Windows\System32\drivers\iaLPSS2i_I2C_CNL.sys
14:27:21.0325 0x13a8 iaLPSS2i_I2C_CNL - ok
14:27:21.0340 0x13a8 [2ED3B41C7CB4101ACB15D84D8AB5AA9D, A92487129B81376471C842B9932FF3A7B3ABBBB89797978E3FDEAF71A6FD5E3F] iaLPSS2i_I2C_GLK
C:\Windows\System32\drivers\iaLPSS2i_I2C_GLK.sys
14:27:21.0340 0x13a8 iaLPSS2i_I2C_GLK - ok
14:27:21.0340 0x13a8 [16A10CCEDCF5AC4CAAE43DC9FC40392F, F77696AE55B992154A3B35F7660BD73E0AB35A6ECEEC1931C0D35748CFA605C0] iaLPSSi_GPIO
C:\Windows\System32\drivers\iaLPSSi_GPIO.sys
14:27:21.0340 0x13a8 iaLPSSi_GPIO - ok
14:27:21.0340 0x13a8 [EB82A11613326691508D9ED9A4FE29E7, 8445E41BAB21964C7F014742795E462BDDC6C37A261990B3D6BF4E637A719547] iaLPSSi_I2C
C:\Windows\System32\drivers\iaLPSSi_I2C.sys
14:27:21.0340 0x13a8 iaLPSSi_I2C - ok
14:27:21.0355 0x13a8 [E2E64636CD6A6902BD81AC3B90089484, 7274F33E5EED8AF739FFCC80B9A62CDF12553EBD2724E2F8E93FD67376CC6E84] iaStorAVC
C:\Windows\system32\drivers\iaStorAVC.sys
14:27:21.0355 0x13a8 iaStorAVC - ok
14:27:21.0371 0x13a8 [215525477CBDCD07A82AC518BAE3DEC3, 30BEE94794953E2DBF0FC5AFCE0566F335AF022E89819DE145329E7C09C636BD] iaStorV
C:\Windows\system32\drivers\iaStorV.sys
14:27:21.0371 0x13a8 iaStorV - ok
14:27:21.0387 0x13a8 [329F2FEC47FD8754FC44A8F3F283C915, 0F3E4F33B019B278B6657B4ECEC25D04B128578622539FF5855330BDB6537545] ibbus
C:\Windows\System32\drivers\ibbus.sys
14:27:21.0387 0x13a8 ibbus - ok
14:27:21.0387 0x13a8 [7AF61F0F29E6B962E9D63CBB0E9CF91C, 00C4D7F2AD6849895CBE681D4206F9E160324291 97C6F68DA6B3BAF6BCCCF4DE] icssvc
C:\Windows\System32\tetheringservice.dll
14:27:21.0387 0x13a8 icssvc - ok
14:27:21.0449 0x13a8 [56129985C2C2AFCDB4861FD14CC3F728, 647B2B95B26E3027EAFEC51BCAB5D4E84D9C888A273C42116BA893DF655882C3] IKEEXT
C:\Windows\System32\ikeext.dll
14:27:21.0449 0x13a8 IKEEXT - ok
14:27:21.0465 0x13a8 [EA2362F5AE9DCD7960D3E0F1703A9D45, 3FD9B958700ADEF5B2DC023B300B805037DB45DAD9FC82DE51306B6ABABC9855] IndirectKmd
C:\Windows\System32\drivers\IndirectKmd.sys
14:27:21.0465 0x13a8 IndirectKmd - ok
14:27:21.0481 0x13a8 [83FC19C16AB19DA57AB0500235F764FE, F441BF9D8805C9BFA11C5116775376B58E354B19039FFB5D745D9945A59AEA1E] InstallService
C:\Windows\system32\InstallService.dll
14:27:21.0512 0x13a8 InstallService - ok
14:27:21.0512 0x13a8 [A8B2FF169AB39717D53017435CE2E9F0, B3A935202FC707F1B3ADE67C06D4BCB72A9E7589B34477521F1BEF09372BE067] intelide
C:\Windows\system32\drivers\intelide.sys
14:27:21.0512 0x13a8 intelide - ok
14:27:21.0512 0x13a8 [61DEB3F85866777A907F627627512A40, 4A94EA4EE6A6EB61559F2AE7B61E59B65C721CADC42D30018340E0CB601B9B38] intelpep
C:\Windows\system32\drivers\intelpep.sys
14:27:21.0527 0x13a8 intelpep - ok
14:27:21.0527 0x13a8 [AECBF5BE2F9A2A50B978E0BF31041A81, A62F436C66DEFEB438A7891857DFB830995714A7E4FE4BDCA6B4EB1606BD2101] intelpmax
C:\Windows\System32\drivers\intelpmax.sys
14:27:21.0527 0x13a8 intelpmax - ok
14:27:21.0527 0x13a8 [F21B57F4A6A8B9A3B244E12853D793EF, D487EA17D6F46815221081F9283EBDE3BA03BCD5211AA3FB9DBCFF9D2F0FC840] intelppm
C:\Windows\System32\drivers\intelppm.sys
14:27:21.0527 0x13a8 intelppm - ok
14:27:21.0527 0x13a8 [00C9E07A72BD009C3B74943B3BB2F818, 14DE03ABFD07A2929DB75C81B719A66E4DACE4804223615C70EEB0A4EB7698BE] iorate
C:\Windows\system32\drivers\iorate.sys
14:27:21.0527 0x13a8 iorate - ok
14:27:21.0543 0x13a8 [286A2D1E138C081935532477209 2A7A6, 420A7868E596191020ACD63FE594D40AEC61446DA1E233787A94CA9BE0764796] IpFilterDriver
C:\Windows\system32\DRIVERS\ipfltdrv.sys
14:27:21.0543 0x13a8 IpFilterDriver - ok
14:27:21.0543 0x13a8 [F6387B817A9CFE2A9F2B7829B9E57CAF, 0F981D8EB3092A9F7187558D5127BABDB752C6B7BEFDFF4DEFD64196C8D4D76C] iphlpsvc
C:\Windows\System32\iphlpsvc.dll
14:27:21.0559 0x13a8 iphlpsvc - ok
14:27:21.0559 0x13a8 [7E54CF6D093F937A4E722C6D4184D4B9, DFA6D5A570CF88D04236822DA9E6DD63725D8F27FC69D71FF02D53455F6A0AD5] IPMIDRV
C:\Windows\System32\drivers\IPMIDrv.sys
14:27:21.0559 0x13a8 IPMIDRV - ok
14:27:21.0559 0x13a8 [5BAFE7E7FBD95B5FE36F4E0AFF26D6A3, 51332BB5D518B5824783F80FEFC3557FD415B469E0AEB932D3D3EBE7AF48BCBF] IPNAT
C:\Windows\system32\drivers\ipnat.sys
14:27:21.0559 0x13a8 IPNAT - ok
14:27:21.0574 0x13a8 [B5B6D1F86E40E785D6650DB923DB6BEA, 7A2D92A2274E0379B5FA6351D18E2F0DD55960BB783EA3528FE9E303E1A4256D] IPT
C:\Windows\System32\drivers\ipt.sys
14:27:21.0574 0x13a8 IPT - ok
14:27:21.0574 0x13a8 [77494E26B28465D2A09B9455F8A3B34E, B778D4BC71A5F5CF687175CA53AC342E4740156D4B96E6E96D918BD46C2C1459] IpxlatCfgSvc
C:\Windows\System32\IpxlatCfg.dll
14:27:21.0574 0x13a8 IpxlatCfgSvc - ok
14:27:21.0574 0x13a8 [6B1DD42A574FBD3719F05550B111624C, 438298217D8D9C7C518FF03B9FA886C88067168B3828A35917B5D6D4DA12213A] isapnp
C:\Windows\system32\drivers\isapnp.sys
14:27:21.0574 0x13a8 isapnp - ok
14:27:21.0574 0x13a8 [49E3EF46E5A9E4AA8BD9C0C19725CF4C, 6B311A3D089AC6D061B29952FB346BA723F65BEB36AAA14B9215210C98BD136B] iScsiPrt
C:\Windows\System32\drivers\msiscsi.sys
14:27:21.0574 0x13a8 iScsiPrt - ok
14:27:21.0590 0x13a8 [2DAB988FDD06CACD99B9DB2A05569449, A66C90009C7B20736A8B291889C518CBAF9D0C32A5EC720330EF25F30C056F1B] ItSas35i
C:\Windows\system32\drivers\ItSas35i.sys
14:27:21.0590 0x13a8 ItSas35i - ok
14:27:21.0590 0x13a8 [02A6967D5AEF2F15AA9C838DBF3E1C04, 7639DCD4328C14F3FB522EC501F4DF374CCBE87699EB4A2B238C9F9C526FDF59] kbdclass
C:\Windows\System32\drivers\kbdclass.sys
14:27:21.0590 0x13a8 kbdclass - ok
14:27:21.0590 0x13a8 [DD56D35E1708207B5006B491AFBD47D7, 4DDDE0AF2816A5302511E99FD26F77517EA5C2C6D9BE76D70199A33BF3EE9FE3] kbdhid
C:\Windows\System32\drivers\kbdhid.sys
14:27:21.0590 0x13a8 kbdhid - ok
14:27:21.0590 0x13a8 [6B7422A382C1788AAF7C6CE6D4A4B375, F14AC6EF3695E05CD2D5CD9524AF7D0327E11A8B2BA9315A1EBF53828A608D33] kdnic
C:\Windows\System32\drivers\kdnic.sys
14:27:21.0590 0x13a8 kdnic - ok
14:27:21.0606 0x13a8 [B4DE3D04AE3C71E67236B841BEADEB74, 8567CDBA80952B2B7AF647B9D2630FE12B73E87517498BCCDCC27EC1ED6E1545] KeyIso
C:\Windows\system32\lsass.exe
14:27:21.0606 0x13a8 KeyIso - ok
14:27:21.0606 0x13a8 [14A03E7E5ED4B73BAA214E270A2CC6EA, F4DFD14038EFA20F13C3A1BE6DB03645954AFAE7162FC1176C6461486B36406D] KSecDD
C:\Windows\system32\Drivers\ksecdd.sys
14:27:21.0606 0x13a8 KSecDD - ok
14:27:21.0606 0x13a8 [0FB1EB3921484248CDBF04436112A545, E590F18410AA7E7F49B89B7B31B28EA77E78EA3287B6B7AF3BA2E60455AC6AFA] KSecPkg
C:\Windows\system32\Drivers\ksecpkg.sys
14:27:21.0606 0x13a8 KSecPkg - ok
14:27:21.0606 0x13a8 [E5304DE29BB9666DF0E57E5BA71C0E10, 491802A11F9E563369DB69E1D838C6F0F54F69F31BDC14018339CEE1B6C9C3CA] ksthunk
C:\Windows\system32\drivers\ksthunk.sys
14:27:21.0606 0x13a8 ksthunk - ok
14:27:21.0668 0x13a8 [EA6D7953D60C7FBD8B5454CD9905A828, D2CEBBCFE050DE119D67CD19A2D295CA03C69B323844C97CEE27AF9FB925146B] KtmRm
C:\Windows\system32\msdtckrm.dll
14:27:21.0668 0x13a8 KtmRm - ok
14:27:21.0668 0x13a8 [9CF61CEE390E8E53E381982FBB05DDC5, 518E8AA4E0DCF4B3B4D96BAEEF1D02B23EA677A0BA754AD8CA6EABF8CF00F3C0] LanmanServer
C:\Windows\system32\srvsvc.dll
14:27:21.0684 0x13a8 LanmanServer - ok
14:27:21.0684 0x13a8 [7C1202298780E1285EEC216FCE9CE4A5, 1883E2EC3021FE96DD3966A3225877560C717589E91300BC159F732113D0DF4B] LanmanWorkstation
C:\Windows\System32\wkssvc.dll
14:27:21.0684 0x13a8 LanmanWorkstation - ok
14:27:21.0684 0x13a8 [A997488F4EDAAD59C748CF9FB1D9DAC0, A0B145041F984DD4E0A6F8D0E9C8363DA6F2DA7460E140F028C320CEAC03759C] lfsvc C:\Windows\System32\lfsvc.dll
14:27:21.0699 0x13a8 lfsvc - ok
14:27:21.0699 0x13a8 [87B41765B098F2EB33442DA31FABE3AC, 06C2768ADCE532B6AB180E675CA535838F7167A63C7103A6B95A317AD885890D] LicenseManager
C:\Windows\system32\LicenseManagerSvc.dll
14:27:21.0699 0x13a8 LicenseManager - ok

14:27:21.0699 0x13a8 [78779BD92081CB27967E77561683AFBE, 05EC91E194336D1BB1EE323E70FAC54F6DC0CEF53FD4925F394399531A37A0DD] lltdio
C:\Windows\system32\drivers\lltdio.sys
14:27:21.0699 0x13a8 lltdio - ok
14:27:21.0699 0x13a8 [800DA45C161E965A8FE626AE72412B7C, A3751118E789D72535174FE66CD41B31D391AE149D46FD4814E0D200A02F854D] lltdsvc
C:\Windows\System32\lltdsvc.dll
14:27:21.0715 0x13a8 lltdsvc - ok
14:27:21.0715 0x13a8 [4A501E9429650B678610ABCCAD1D2609, 71F33FD997D36B8CFB7FD36397CB768AEF1B6329B3882D445B72246621F3BD7E] lmhosts
C:\Windows\System32\lmhsvc.dll
14:27:21.0715 0x13a8 lmhosts - ok
14:27:21.0762 0x13a8 [89EB90814DA5FB6F5299240AD8B9C7A7, 36857AFABD064196B7D2A7CFAE3696D96C1FE13431DB49ACE161E706680231DA] LSI_SAS
C:\Windows\system32\drivers\lsi_sas.sys
14:27:21.0762 0x13a8 LSI_SAS - ok
14:27:21.0762 0x13a8 [2FD85E518EA97BB642B018EEB453401A, 7EA218BB57843B80AB5A987BA915829B8262629F72EEC84238634A016D05504E] LSI_SAS2i
C:\Windows\system32\drivers\lsi_sas2i.sys
14:27:21.0777 0x13a8 LSI_SAS2i - ok
14:27:21.0777 0x13a8 [8B7995D9E487C8F90BEA8F1EF6331C10, 2EE68AFEB6D5EC98A996C1722057275C1648411898359248D390B6AA9F697AB5] LSI_SAS3i
C:\Windows\system32\drivers\lsi_sas3i.sys
14:27:21.0777 0x13a8 LSI_SAS3i - ok
14:27:21.0777 0x13a8 [ED902EBC8DEEF6E5FC00D0816DDFFB42, FFDDB7BA54C999D5689152E4EDACC838A769B6C479F0A0FCF294C8632F4E4C1F] LSI_SSS
C:\Windows\system32\drivers\lsi_sss.sys
14:27:21.0777 0x13a8 LSI_SSS - ok
14:27:21.0794 0x13a8 [C812C171972750B1048B3E9BF65647A2, 08E11EF2BC61D36030E39F4BA0104071188044C0E4D3F7DD3A49557F04152620] LSM C:\Windows\System32\lsm.dll
14:27:21.0794 0x13a8 LSM - ok
14:27:21.0809 0x13a8 [AD3154722B51D13B59D82696D19CEF8B, 2EF1B313702E2AAE04952EF8E1E82C8871C9F63B7642A57F5AD4A7CB69D7FFFA] luafv
C:\Windows\system32\drivers\luafv.sys
14:27:21.0809 0x13a8 luafv - ok
14:27:21.0809 0x13a8 [AE3606235EEEA50AA6D3DFB8EA7C7857, EFF06FE55E7F45AF78DF13F21C11848CC3D15A7D11EFE11A147F67AC9907DE69] LxpSvc
C:\Windows\System32\LanguageOverlayServer.dll
14:27:21.0809 0x13a8 LxpSvc - ok
14:27:21.0840 0x13a8 [AE03D8F1B7863268EAED2FE0105ED75F, F5172A1A3E24FC5271FCB0118861EA0EC33AA8ABB01AE9CAD50E2F032B92486C] MapsBroker
C:\Windows\System32\moshost.dll
14:27:21.0871 0x13a8 MapsBroker - ok
14:27:21.0871 0x13a8 [6C965A0AC264AF1A8E0A69882A7EAFDC, DA40E73A7F584D944F58C7F489B701315B8D30A29E5A6C840C9D291302271834] mausbhost
C:\Windows\System32\drivers\mausbhost.sys
14:27:21.0871 0x13a8 mausbhost - ok
14:27:21.0887 0x13a8 [6C6C1EFC46A62091224333E1E9304FBC, AEADB11E2BE2EEB4BB5E4E13ADDA4633475022312AEE777CFE7FEB27C490B54C] mausbip
C:\Windows\System32\drivers\mausbip.sys
14:27:21.0887 0x13a8 mausbip - ok
14:27:21.0887 0x13a8 [FFDFCDE522E34188F517F9F1E1BAD53D, 851788BEA35882D3A04489A59C077262E30999E4915B815FB1CE0195624B5831] MbbCx
C:\Windows\system32\drivers\MbbCx.sys
14:27:21.0887 0x13a8 MbbCx - ok
14:27:21.0903 0x13a8 [DF64803704630BF0B6969E4C3FEC365C, 0B9575543063FC5C360D77E83789AAD27A520E2B10191A931A5F0D0F3F250127] McpManagementService
C:\Windows\System32\McpManagementService.dll
14:27:21.0903 0x13a8 McpManagementService - ok
14:27:21.0903 0x13a8 [CE4B01081B8FD211A7A34219D5E8154A, 9041FDEB932F2CBBCE4A017256C81B3733604403AA343D4532910436E8288CA9] megasas
C:\Windows\system32\drivers\megasas.sys
14:27:21.0903 0x13a8 megasas - ok
14:27:21.0903 0x13a8 [F3C6B901E3FF70F27A17CFDDD7BA85AA, 6D67F52F0B63724126DD7B75B3489D14A6CBC3BD1E0D19188026DA21E85A620A] megasas2i
C:\Windows\system32\drivers\MegaSas2i.sys
14:27:21.0903 0x13a8 megasas2i - ok
14:27:21.0903 0x13a8 [EB84966D14F9342C8AD3D78BA9AA8754, 83C982FC61094A9E9F3E3CB5174B7409698C12FE3B6BF9B2F4C9365E56C642B2] megasas35i
C:\Windows\system32\drivers\megasas35i.sys
14:27:21.0903 0x13a8 megasas35i - ok
14:27:21.0918 0x13a8 [A4DC7070D92AD82A7BDF2F69C155AF69, 8A902DDB6016E4D5C28808FBA5741751D94FFBD4B55724D47BBA0A8C29900E53] megasr
C:\Windows\system32\drivers\megasr.sys
14:27:21.0965 0x13a8 megasr - ok
14:27:21.0981 0x13a8 [15B8E4038C02CD66535C050DDA3C4EDF, 8BF2FAF27914EB754959FE7CB2E5229150B4B65278888E737E8BF9752CF5AE21] MessagingService
C:\Windows\System32\MessagingService.dll
14:27:21.0981 0x13a8 MessagingService - ok
14:27:21.0981 0x13a8 MicrosoftEdgeElevationService - ok
14:27:21.0981 0x13a8 [B74FFC6301B3312A9F59E04E487BC72A, 76F71824E80D10EB71BEDE5EE3A64CAD7CAC3DDFBB6670D1537E6B75FF0217E9] Microsoft_Bluetooth_AvrcpTransport
C:\Windows\System32\drivers\Microsoft.Bluetooth.AvrcpTransport.sys
14:27:21.0981 0x13a8 Microsoft_Bluetooth_AvrcpTransport - ok
14:27:21.0981 0x13a8 [29AE1F3D395696A4DE6D01ED1FE60851, C9A606DCFF2B68175E38AFC9F51FE8D5D9A5F410CD6AD9142B50873FA384FAFB] MixedRealityOpenXRSvc
C:\Windows\System32\MixedRealityRuntime.dll
14:27:21.0996 0x13a8 MixedRealityOpenXRSvc - ok
14:27:21.0996 0x13a8 [517DC2DF12A391699F8432AF89947F2B, 2C6B268486AD0F3BFB82DE0F61D076DF7C334C1C94A0316084713EBDB0C9C518] mlx4_bus
C:\Windows\System32\drivers\mlx4_bus.sys
14:27:22.0012 0x13a8 mlx4_bus - ok
14:27:22.0012 0x13a8 [08237E61C03A2FB26BBE7137C48FFE25, A94479A52150020523A4B55BA7609D879005EC73C9C40D1141BB85559E951F6C] MMCSS
C:\Windows\system32\drivers\mmcss.sys
14:27:22.0012 0x13a8 MMCSS - ok
14:27:22.0012 0x13a8 [2CC49A179B7AD9DD252900A77A5D7FCA, C518799A4EB0DAAD65AFBA5F5C1E517298E9E9A7562B96042348A605542303EE] Modem
C:\Windows\system32\drivers\modem.sys
14:27:22.0012 0x13a8 Modem - ok
14:27:22.0059 0x13a8 [20A23F92EC618E449E326FFEA6C26D5D, 91AFA411708A0E1FED17D56F2C4A36A84D1F30E13D854A6F55DE9773E6433CB6] monitor
C:\Windows\System32\drivers\monitor.sys
14:27:22.0074 0x13a8 monitor - ok
14:27:22.0074 0x13a8 [4352C109DD892A5A5413897A74103024, DB5D99DBFF8C84A7D87109DFB71396DF8E0F0754FC0D263E45116915A39735CE] mouclass
C:\Windows\System32\drivers\mouclass.sys
14:27:22.0074 0x13a8 mouclass - ok
14:27:22.0074 0x13a8 [66E41E31DEBD4E1A2762945B4F15C780, 3A05D657E03B6CD9D62023061F9C652357F16DA2F2337FB6C617AEEFFAD794B4] mouhid
C:\Windows\System32\drivers\mouhid.sys
14:27:22.0074 0x13a8 mouhid - ok
14:27:22.0074 0x13a8 [180D9E273A958B6D2B55410DB2C431C4, EE3598DECA591E8735DE0F449F292E9DDDBCE28A8A7B814E78DFD90AC867B7F2] mountmgr
C:\Windows\system32\drivers\mountmgr.sys
14:27:22.0074 0x13a8 mountmgr - ok
14:27:22.0074 0x13a8 [19623B4213820840730EF00BA52201B6, E9AF731D982F2E6D6DEF9239E4912881043804E6C557C6DBA9B16AD6AE0473F7] mpsdrv
C:\Windows\system32\drivers\mpsdrv.sys
14:27:22.0074 0x13a8 mpsdrv - ok
14:27:22.0090 0x13a8 [16AD3B4D4F2C44DF210AEB80C87ABFF5, 9A2C57F513712B5EA60B2111755F9C5A37DFE653C166161F249499582631 97FE] mpssvc
C:\Windows\system32\mpssvc.dll
14:27:22.0106 0x13a8 mpssvc - ok
14:27:22.0106 0x13a8 [F182553C8D5E5541196F2A1EB7C1908E, 93C62B07FC406851BC9E6EDF8868CF5201AB8526F5E943DC59C22C0A4AFF4E28] MRxDAV
C:\Windows\system32\drivers\mrxdav.sys
14:27:22.0106 0x13a8 MRxDAV - ok
14:27:22.0168 0x13a8 [D2693248895A7BF0D3230D9E97F82150, 3CDEA72E0AA5859E06EA8E65F56044ED77BDD80210FF7DF972D575F4231CABD6] mrxsmb
C:\Windows\system32\DRIVERS\mrxsmb.sys
14:27:22.0168 0x13a8 mrxsmb - ok
14:27:22.0168 0x13a8 [D3C3AB236BE9E749BDFA334E798CABF8, 573EB077558264A292AF6741C75548934E7F53B6F9A8669A0A3FCB9BA0645554] mrxsmb10
C:\Windows\system32\DRIVERS\mrxsmb10.sys
14:27:22.0184 0x13a8 mrxsmb10 - ok
14:27:22.0184 0x13a8 [88A7C41BFA7FDCE151F205A9650120EA, 7A6C2C466D0568994E69C7B37EE6ABF58E5055BBC5B74A283FD358FAA4E2A79C] mrxsmb20
C:\Windows\system32\DRIVERS\mrxsmb20.sys
14:27:22.0184 0x13a8 mrxsmb20 - ok
14:27:22.0184 0x13a8 [E587396A4C8151ABBF13A96C4465DE31, A3AA5D51E34657479CFCDC3DBB7821B7255F7CB57D5686B7F709A7953AD537EB] MsBridge
C:\Windows\system32\drivers\bridge.sys
14:27:22.0184 0x13a8 MsBridge - ok
14:27:22.0184 0x13a8 [7226218CB617DF0CBBDC04296BA2F592, C6983231171AF90413061A4365BAA8C0C0CDCA0BD13DD29DF5094D3052D8C20D] MSDTC
C:\Windows\System32\msdtc.exe
14:27:22.0199 0x13a8 MSDTC - ok
14:27:22.0199 0x13a8 [4D8C5C0B06D8F4B28AAD865ACA6C5494, 8AC1A5358691DA4FBEC7BAA3711321EAD20439029031696F12BB287771E82893] Msfs
C:\Windows\system32\drivers\Msfs.sys
14:27:22.0199 0x13a8 Msfs - ok

14:27:22.0199 0x13a8 [6092FD060EC4132A799BDAD61845DDB7, B45F9D3A71FC8A73AED3C5B8CF6F14A25EBDD3D4D47C9F39FFCD75C7D22F4A9E] msgpiowin32
C:\Windows\System32\drivers\msgpiowin32.sys
14:27:22.0199 0x13a8 msgpiowin32 - ok
14:27:22.0199 0x13a8 [78689B7121F3DA06A879FBBD039B29AA, C656B13E0329B86663C2382943B1DD6F6E5080FAC71E3FEFA056D261F30E273E] mshidkmdf
C:\Windows\System32\drivers\mshidkmdf.sys
14:27:22.0199 0x13a8 mshidkmdf - ok
14:27:22.0199 0x13a8 [9E90FE6DF363D2427A5C773120E7B27D, 1FDB7E28CCAF757603C4B754E1AC9C470E5E60E85DE067375902F108F5E34608] mshidumdf
C:\Windows\System32\drivers\mshidumdf.sys
14:27:22.0199 0x13a8 mshidumdf - ok
14:27:22.0199 0x13a8 [22C778DB480E9A425EEA4E6D3D93FC15, 46DE47E2D046236F05B2AD11D32139B4F06E82CC949D1EF00037EB71DC24FB43] msisadrv
C:\Windows\system32\drivers\msisadrv.sys
14:27:22.0199 0x13a8 msisadrv - ok
14:27:22.0215 0x13a8 [3A679D4F3FCD9D7FBADFDB93BB0959E8, E45F3D5CEBC75D0B5D4D14A10A085EFFFBFF2E79C42052694D6798474919A50A] MSiSCSI
C:\Windows\system32\iscsiexe.dll
14:27:22.0215 0x13a8 MSiSCSI - ok
14:27:22.0215 0x13a8 msiserver - ok
14:27:22.0262 0x13a8 [0ACF0D7051EA417D3870730592B848DB, 209945BC6EEB1EF4D730170D154CE8BAF34D11C5783CAEBEE494C610CFBB5C71] MSKSSRV
C:\Windows\System32\drivers\MSKSSRV.sys
14:27:22.0262 0x13a8 MSKSSRV - ok
14:27:22.0278 0x13a8 [9FB5040C8CEAE4C32B7884ECBBCAFDAF, 0EC3E53C5B1B202440DE22A5BF7E1EBE9AF5BBB6BA69DB9D018A6D8EC97B477E] MsLldp
C:\Windows\system32\drivers\mslldp.sys
14:27:22.0278 0x13a8 MsLldp - ok
14:27:22.0278 0x13a8 [4B5CD00DEAB6BC5FE650D5E90BA5719A, 6E5DAA5D9826A3165514CE2AC4AEC23033D7BA993F06D2BDFFC68052CA71C4A0] MSPCLOCK
C:\Windows\System32\drivers\MSPCLOCK.sys
14:27:22.0278 0x13a8 MSPCLOCK - ok
14:27:22.0278 0x13a8 [3FC09B334BB53D2EB289887CFBD79D0B, AD55F307A8146BC2ACB1B2437C19B405F7BC3F5E4A81DB685B0C046FEC4C30BC] MSPQM
C:\Windows\System32\drivers\MSPQM.sys
14:27:22.0278 0x13a8 MSPQM - ok
14:27:22.0278 0x13a8 [9917DDFFCF1AC5103455818F8EB5B43A, A582DF8CDDFAC1E25D9D766C41D0AFD4DB4933D3E9800415F55F3C126B09CA98] MsQuic
C:\Windows\system32\drivers\msquic.sys
14:27:22.0278 0x13a8 MsQuic - ok
14:27:22.0293 0x13a8 [D6CFF079C30F9CF1AD7A1DB835E276E4, A53FC4419F2B9B021254B9CA6347891C21080BC1A707EE12E9365DB0617EB951] MsRPC
C:\Windows\system32\drivers\MsRPC.sys
14:27:22.0293 0x13a8 MsRPC - ok
14:27:22.0293 0x13a8 [DB89919F84809686BD4F8C24EB6CB3FA, 360A199A6D4690FE248C6EAA4E84673F299FA4CA6C21E940F4DF1B28216BA23C] mssmbios
C:\Windows\System32\drivers\mssmbios.sys
14:27:22.0293 0x13a8 mssmbios - ok
14:27:22.0293 0x13a8 [244C73253E165582DDC43AF4467D23DF, 808FF81F0030CC7390B4790F91CE1763EAC02CCECA6014A2D9D990A40DBD0580] MSTEE
C:\Windows\System32\drivers\MSTEE.sys
14:27:22.0293 0x13a8 MSTEE - ok
14:27:22.0309 0x13a8 [8EE2EEE12398FEA5BC8E37AAAFE59852, E37965B9EFD9ADA6A81585DD792A20CD03BFC28512E92FC63CD2CBAE9A41AD1A] MTConfig
C:\Windows\System32\drivers\MTConfig.sys
14:27:22.0309 0x13a8 MTConfig - ok
14:27:22.0309 0x13a8 [EE1EFB2BFECE08E096BA51E61582DE23, EFE0E220A8D82CF4B6605C1A1A90DA83867917A6C997D9E9C7AF6947749E8949] Mup
C:\Windows\system32\Drivers\mup.sys
14:27:22.0309 0x13a8 Mup - ok
14:27:22.0309 0x13a8 [82B6567127134 24A707F1E127C68E02F, 69FBB0692C37DA498014CC6CDC609E612A3207A17B280EDE5C02248571F91F11] mvumis
C:\Windows\system32\drivers\mvumis.sys
14:27:22.0309 0x13a8 mvumis - ok
14:27:22.0325 0x13a8 [45E3F42805E050F6CB9F4CD1C481BF40, FF7DCAA62FC92B4DB60D833F94D83128474E8339AE283A995751742DA0CC9A6A] NativeWifiP
C:\Windows\system32\DRIVERS\nwifi.sys
14:27:22.0325 0x13a8 NativeWifiP - ok
14:27:22.0340 0x13a8 [C3067E19C4058469EE53D2DF08BE12F2, 9EC7876B39883890606F5EBC757C4F3334F5008FC528AC4EE7811646669E8663] NaturalAuthentication
C:\Windows\System32\NaturalAuth.dll
14:27:22.0340 0x13a8 NaturalAuthentication - ok
14:27:22.0340 0x13a8 [D47A20839608B8213065D7AFC8C42195, 7B0187BE9705ED2F925616C13B3744BAC0A9C96B21BE503D96BC9EE7EE125B33] NcaSvc
C:\Windows\System32\ncasvc.dll
14:27:22.0340 0x13a8 NcaSvc - ok
14:27:22.0355 0x13a8 [7AE4315A82F2DFE6F78DF00A674474C7, F07CEB86C72BA4E4F115B8AAD0732FAD9E939073CAF8B06EDEFA1F3C81D6E154] NcbService
C:\Windows\System32\ncbservice.dll
14:27:22.0355 0x13a8 NcbService - ok
14:27:22.0355 0x13a8 [8C938E851CDF2CE30BBEA14555B61820, F853F526C811893BD40B1124BAEC543099381E7BF091729B6A6665DF3CE10B94] NcdAutoSetup
C:\Windows\System32\NcdAutoSetup.dll
14:27:22.0355 0x13a8 NcdAutoSetup - ok
14:27:22.0371 0x13a8 [D62777BD13AC73F8FB20039B701D5292, E3708D62DEA31BA03D7CE7EEF6A270DA2B3556559140B556F5AB4EA289F921E2] ndfltr
C:\Windows\System32\drivers\ndfltr.sys
14:27:22.0371 0x13a8 ndfltr - ok
14:27:22.0387 0x13a8 [88F21082BC4AB8D754A639DE993AD6F0, CACD1FB168B1ED04D6966E3410366C097D458EF7ECCF436AD9C22B66F9E9D3EE] NDIS
C:\Windows\system32\drivers\ndis.sys
14:27:22.0387 0x13a8 NDIS - ok
14:27:22.0403 0x13a8 [6BEC0929C7A7BF2A7C44F585ECC7DAEB, 5F6395268CBD26A4B90960479040C114B2C8A3F24C188C2D5F62D6AB43A637D1] NdisCap
C:\Windows\system32\drivers\ndiscap.sys
14:27:22.0403 0x13a8 NdisCap - ok
14:27:22.0403 0x13a8 [7EAEC42F63372FE76C2D513DE7A94F47, 7F19B0E3DE05E6C4BBCCB2CCD8CED9BCD8AECB6037C27A3DF1385E7C4CC03C63] NdisImPlatform
C:\Windows\system32\drivers\NdisImPlatform.sys
14:27:22.0403 0x13a8 NdisImPlatform - ok
14:27:22.0403 0x13a8 [E298887ABA3F4E2308CB76A68071EEF1, E65B464A0B5B750385BC69A85C87F6E1D9BB5A67FFD2A177E05DFBC0552CAAA5] NdisTapi
C:\Windows\system32\DRIVERS\ndistapi.sys
14:27:22.0403 0x13a8 NdisTapi - ok
14:27:22.0403 0x13a8 [09BD40437780ED584D06519373ACEDC7, 3D7685D3960382FB102E225634D54A2370DA53DEB89CAE4765AD00C9AFE030B7] Ndisuio
C:\Windows\system32\drivers\ndisuio.sys
14:27:22.0403 0x13a8 Ndisuio - ok
14:27:22.0403 0x13a8 [31AE9050FF9D6CBE1BC2A7EA5F98D6A3, 2960AF22637EDA95DF6ED154278B23AC157AF2DE6F342DA7D8083E4F7F70730F] NdisVirtualBus
C:\Windows\System32\drivers\NdisVirtualBus.sys
14:27:22.0403 0x13a8 NdisVirtualBus - ok
14:27:22.0418 0x13a8 [556AD635190D8E0CD2E85026F684C022, 4851829E12D72816CA4AB4C3C9595AD88AAAE083ADA8A2D53A11024F74DC7E19] NdisWan
C:\Windows\System32\drivers\ndiswan.sys
14:27:22.0418 0x13a8 NdisWan - ok
14:27:22.0418 0x13a8 [556AD635190D8E0CD2E85026F684C022, 4851829E12D72816CA4AB4C3C9595AD88AAAE083ADA8A2D53A11024F74DC7E19] ndiswanlegacy
C:\Windows\system32\DRIVERS\ndiswan.sys
14:27:22.0418 0x13a8 ndiswanlegacy - ok
14:27:22.0418 0x13a8 [33CDAEDC7CBE8339A8324CEC2461BFB4, DAAEACDB4506D2BDDED61957D92FB4983E11D9CE6E7B25119B4CBFB431C945F4] NDKPing
C:\Windows\system32\drivers\NDKPing.sys
14:27:22.0418 0x13a8 NDKPing - ok
14:27:22.0434 0x13a8 [C752C100988841607A3711056787F1399, 3F5365B1789613FA9ABA341CAB9C83E356BADC8AF3B3AF4A2C577FCEFE89FBD0] ndproxy
C:\Windows\system32\DRIVERS\NDProxy.sys
14:27:22.0434 0x13a8 ndproxy - ok
14:27:22.0434 0x13a8 [77621E74FD79B267071A0D12C643A48A, 8228B7D1237A0FFABCCC150B299EA494C8F0CB4CCB51AB0DBFF08CBAA9EFC4BB] Ndu
C:\Windows\system32\drivers\Ndu.sys
14:27:22.0434 0x13a8 Ndu - ok
14:27:22.0434 0x13a8 [0D793CFA97490F987BC76D69401B387E, 5F24BFB3834C6F00C6F2FA80EB30F7C2A8ECD5CF19C483B7B08A2488C898F585] NetAdapterCx
C:\Windows\system32\drivers\NetAdapterCx.sys
14:27:22.0434 0x13a8 NetAdapterCx - ok
14:27:22.0449 0x13a8 [4687FAC962855BDB1896C02334E95D54, E7F7F30D9513FDD2236FCFD5549DCD93101562BA1117213EA4DF32B70BB48A73] NetBIOS
C:\Windows\system32\drivers\netbios.sys
14:27:22.0449 0x13a8 NetBIOS - ok
14:27:22.0449 0x13a8 [FFE0E3844802DFC4C783FB745DF34DC9, 9BB063E987984F468986683353B73E8E2D8F2A85CA0FAA6A5841E4FEBB535AD] NetBT
C:\Windows\system32\DRIVERS\netbt.sys
14:27:22.0449 0x13a8 NetBT - ok
14:27:22.0449 0x13a8 [B4DE3D04AE3C71E67236B841BEADEB74, 8567CDBA80952B2B7AF647B9D2630FE12B73E87517498BCCDCC27EC1ED6E1545] Netlogon
C:\Windows\system32\lsass.exe
14:27:22.0449 0x13a8 Netlogon - ok
14:27:22.0465 0x13a8 [7B2330140BAF9910B3FFD8E95BEEFD97, B06665E972D294C89C17372BBE0773E468A3321DFC69DBD84CF5189E79992F1D] Netman
C:\Windows\System32\netman.dll

14:27:22.0465 0x13a8 Netman - ok
14:27:22.0481 0x13a8 [7527B94860B34D7454B1830B2E6C0151, 8A07C2444903AE6653DF9461BE6CD29111D5BF9953ED67A82263B3B266E55A3C] netprofm
C:\Windows\System32\netprofmsvc.dll
14:27:22.0481 0x13a8 netprofm - ok
14:27:22.0497 0x13a8 [88E05C384685FFC9C8817D9C0C46A54F, 95818DD9B9253237D1D6FB3F5B000CB5CDB45FAA16EB52040785000AD74EDEE7] NetSetupSvc
C:\Windows\System32\NetSetupSvc.dll
14:27:22.0497 0x13a8 NetSetupSvc - ok
14:27:22.0497 0x13a8 [8CEA342B36598DD7A03CC34D62032761, C4C0F11C4BF070D80FC1BEF5B9A88ABF8283EB11BD0F850F41F0F4E20C18571C] NetTcpPortSharing
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
14:27:22.0497 0x13a8 NetTcpPortSharing - ok
14:27:22.0512 0x13a8 [FF845719F471F82EA639B399D68C399C, 57C95E506AF10EFC7AEFE4C083764FAB6B381E3A8AFC4FEFDC968264D54E73A1] netvsc
C:\Windows\System32\drivers\netvsc.sys
14:27:22.0512 0x13a8 netvsc - ok
14:27:22.0527 0x13a8 [A5E243A77E3694A4C132C7A35841F434, 74A1365290A9861964C29F3B18986005BC3A686A8806B2C66D2017A1F966794D] NgcCtnrSvc
C:\Windows\System32\NgcCtnrSvc.dll
14:27:22.0527 0x13a8 NgcCtnrSvc - ok
14:27:22.0543 0x13a8 [7EB88A70CA621A222B437C531462EB6D, 3ACC6C5129DA16BCACB1287749044457A71B029B2EBFD57A11968995AF1A8293] NgcSvc
C:\Windows\system32\ngcsvc.dll
14:27:22.0543 0x13a8 NgcSvc - ok
14:27:22.0559 0x13a8 [3613F4211657ABE3C4E91B344847550A, 1ED718E40E6337C5BFF57C9DC8B2CF7A4C53C3FA119E2DBA49472426DFF82D74] NlaSvc
C:\Windows\System32\nlasvc.dll
14:27:22.0559 0x13a8 NlaSvc - ok
14:27:22.0559 0x13a8 [E59F60A6A6CF903CD274774313AA574D, C4AFB4372F610795929 17EE1982A38508C883DF1B74437CE15CFD14D6BA7CFBF] Npfs
C:\Windows\system32\drivers\Npfs.sys
14:27:22.0559 0x13a8 Npfs - ok
14:27:22.0559 0x13a8 [B2B57F620C085F2EA764BDF79AF7BE30, CA3657D9365D34FFECF6B5DE8E5905A2491756B1CC227D9AB8762B09111E9860] npsvctrig
C:\Windows\System32\drivers\npsvctrig.sys
14:27:22.0574 0x13a8 npsvctrig - ok
14:27:22.0574 0x13a8 [0D6DDDE46C2281618EDA497EADD063DE, 8E7A6DBE9B40686D42AF4838D0FE8336DF0BBA9A939ED5AB95F2B342BE31ECE4] nsi
C:\Windows\system32\nsisvc.dll
14:27:22.0574 0x13a8 nsi - ok
14:27:22.0574 0x13a8 [B7E742F58E056224BCCECCE112CC462D, A8251D829E4C81BD4DE6A50E92237B1E1E56682D1587FDD88FF196A889BE83F1] nsiproxy
C:\Windows\system32\drivers\nsiproxy.sys
14:27:22.0574 0x13a8 nsiproxy - ok
14:27:22.0606 0x13a8 [3C31E4C2BFBDEF9A412F59F788E5B3DF, 011653B916AD68E58A9EEF4B3A08FD2BA47FB75D76E95DF897CC3F57868E2FEC] Ntfs
C:\Windows\system32\drivers\Ntfs.sys
14:27:22.0621 0x13a8 Ntfs - ok
14:27:22.0637 0x13a8 [2CB7C3B739D8D34B9249F7DC6C8B5C1A, 318DD3D989EBED3F29A4C3F6FA819F060BE9C14C549B7DAD8ECA2B73C7932722] Null
C:\Windows\system32\drivers\Null.sys
14:27:22.0637 0x13a8 Null - ok
14:27:22.0637 0x13a8 [BEB8637D4B098B286B8B4F46E88A57AD, C0515F0F429A3B60AEC5F9F2AEDCF387CF941D306A21C9BCB56571C83560C6C1] nvdimm
C:\Windows\system32\drivers\nvdimm.sys
14:27:22.0637 0x13a8 nvdimm - ok
14:27:22.0637 0x13a8 [5281A4F23E594AE6EDE1E38B1F8518E0, 628927EB91C6A323CA67B97EF743775B68D30599A0F0593BC3B5C0BA6C5AB82C] nvraid
C:\Windows\system32\drivers\nvraid.sys
14:27:22.0637 0x13a8 nvraid - ok
14:27:22.0637 0x13a8 [A11D15751217EEB734033BB5A929B1CD, F07CD88B7939C53DF83E93D40FB5AB115946393AFBE8DBA75FEE7247BF3063A9] nvstor
C:\Windows\system32\drivers\nvstor.sys
14:27:22.0652 0x13a8 nvstor - ok
14:27:22.0652 0x13a8 [36FF245EDFB96504125761A4E9FED443, 59131F023D8F49A73E70A7946FE1E1D636849C5BD33F84A1B89983F2DFD5AE8ED] OneSyncSvc
C:\Windows\System32\APHostService.dll
14:27:22.0652 0x13a8 OneSyncSvc - ok
14:27:22.0668 0x13a8 [A14E30EDF51BC0A2C8AC76498D4BD13D, FC204664DD63EA323FC6C5033EED09435C4B589672AC8B1C51767F88BC7034E9] p2pimsvc
C:\Windows\system32\pnrpsvc.dll
14:27:22.0668 0x13a8 p2pimsvc - ok
14:27:22.0668 0x13a8 [05841CB27E861C9D75A6EB2E01141BCD, 64C94456A34BA8180D0538B192060F61DA9C6006833257F0D1DA2A41E7322BF8] p2psvc
C:\Windows\system32\p2psvc.dll
14:27:22.0684 0x13a8 p2psvc - ok
14:27:22.0684 0x13a8 [138FDB1EBCB61287A645BD3B06DBED5E, 1E59DE429B54E910688BF917F2AD97E66241EE3FB924C24E3627E9603E8A9C5D] Parport
C:\Windows\System32\drivers\parport.sys
14:27:22.0684 0x13a8 Parport - ok
14:27:22.0684 0x13a8 [54B9176B944977CB0735EDE71A89C647, C9B2D3F3B88D82EA986DEE9DF119841C50E4EB70FD3BD9BE7140C63FBA8C2A03] partmgr
C:\Windows\system32\drivers\partmgr.sys
14:27:22.0684 0x13a8 partmgr - ok
14:27:22.0699 0x13a8 [84037692EECD69055C9A3BE98AF68243, 13DB8D3677131552138F122D51CB59953786B62E405E55AFCD01D24A6EF924FA] PcaSvc
C:\Windows\System32\pcasvc.dll
14:27:22.0699 0x13a8 PcaSvc - ok
14:27:22.0715 0x13a8 [A6DD35030D2FA1993C9A0C3B1B9F3E6B, 7C7CC67114D960C14CDB1376D92493AE83CFD20731B94F5C77160D5C2B4F0A1E] pci
C:\Windows\system32\drivers\pci.sys
14:27:22.0715 0x13a8 pci - ok
14:27:22.0715 0x13a8 [4240C538C850DCEE9DA845DC34BB9F06, 2E41D440FDE7E9CD9F38796E829BD5D7BFE5EF0E808F59BAAE9415D1E55DFC25] pciide
C:\Windows\system32\drivers\pciide.sys
14:27:22.0715 0x13a8 pciide - ok
14:27:22.0715 0x13a8 [0543F01C97CE2D3ABB4F8CEA56B99721, CD84890DEB63C782A51A7F4D962B88CAC9AA226C3C7DDC2D2B0A56E81B00B07C] pcmcia
C:\Windows\system32\drivers\pcmcia.sys
14:27:22.0715 0x13a8 pcmcia - ok
14:27:22.0731 0x13a8 [2DBA97C1B687F7C6D279818216026642, 0F5F4F688145C76A35B21FA1F11784734769E76E13FA095316DBCEEDE01CD17C] pcw
C:\Windows\system32\drivers\pcw.sys
14:27:22.0731 0x13a8 pcw - ok
14:27:22.0731 0x13a8 [8CF08C13B8D964F0776E4F2527A602E8, 1DECEB7ECB2E2ECADDC4729A312017B0AE54DFCD43D5A22ED9576888BE9CB21F] pdc
C:\Windows\system32\drivers\pdc.sys
14:27:22.0731 0x13a8 pdc - ok
14:27:22.0746 0x13a8 [CD7D21AEDE629EC661883FC98B6DEB33, C599F6640E3373BE4775E9C0C5B8A8499822BD2B1038C7887CE66E1987532211] PEAUTH
C:\Windows\system32\drivers\peauth.sys
14:27:22.0746 0x13a8 PEAUTH - ok
14:27:22.0746 0x13a8 [9D1890D2132CBF4DC2E2E5FD52445F5B, ADB2E0BE7C61B715288F4FAE5889B6604DB50F8F025FFA9F1B642E59BBD4FECF] perceptionsimulation
C:\Windows\system32\PerceptionSimulation\PerceptionSimulationService.exe
14:27:22.0746 0x13a8 perceptionsimulation - ok
14:27:22.0762 0x13a8 [2E2E8BA514A93C297F124BAB53F4E921, D6B8116E5C920032A5926D5D047BFD72B05ACBB08E26F177A0B0E6B4EC735FA1] percsas2i
C:\Windows\system32\drivers\percsas2i.sys
14:27:22.0762 0x13a8 percsas2i - ok
14:27:22.0762 0x13a8 [1C6720616FF300235509D5EFBB2CAE20, 92017ECB36EAA35AC454E890734915A658EB898C95970531D43C19461BE6562B] percsas3i
C:\Windows\system32\drivers\percsas3i.sys
14:27:22.0762 0x13a8 percsas3i - ok
14:27:22.0777 0x13a8 [2FC7CFCEDBF7E038351C7CEB1036D2E1, 41D7DA706F0CF613DF768B6795CD09C5C1035F9F101051FB58F5042EB4352DB6] PerfHost
C:\Windows\SysWow64\perfhost.exe
14:27:22.0777 0x13a8 PerfHost - ok
14:27:22.0793 0x13a8 [83E8F723D87814EA21E94811CFC1CD43, 74F430B0B0846AE470088CB3D812C31873737389A8E556A3C98D56EAE4F94A01] PhoneSvc
C:\Windows\System32\PhoneService.dll
14:27:22.0809 0x13a8 PhoneSvc - ok
14:27:22.0809 0x13a8 [07BB135B216B9DD88DA2AA3F4B893B9A, 2A4BF8A284652E06A455399BC2C41A2A9B0023CEAAE2053901E35EF7D5B4F2D0] PimIndexMaintenanceSvc
C:\Windows\System32\PimIndexMaintenance.dll
14:27:22.0809 0x13a8 PimIndexMaintenanceSvc - ok
14:27:22.0809 0x13a8 [1D27638 18209371F73BC986F2739C254, D175BDB3605A4E33818304F44A38E9752BBA960CA898E11E0569E9F3B9FFAFF4] PktMon
C:\Windows\system32\drivers\PktMon.sys
14:27:22.0809 0x13a8 PktMon - ok
14:27:22.0825 0x13a8 [9E431A5D697432DD6F4DB48C9A185104, 44C16E194258C9143A45F4022F9C5DE229E217D6FF7F944F105FE631BE9EF4A7] pla C:\Windows\system32\pla.dll
14:27:22.0840 0x13a8 pla - ok
14:27:22.0856 0x13a8 [73EE8DC7CBEAB344DA440676B9DD4F43, 9535A927C3A16BF5EB23F975CC50251B33F4982E47D357EFD6BF3736C544792A] PlugPlay
C:\Windows\system32\umpnpmgr.dll
14:27:22.0856 0x13a8 PlugPlay - ok
14:27:22.0856 0x13a8 [17AD4222598666BFE9CC0D70AE29A06A, CCF50F3C82FBB5D9926B917F14BF8D7B03FC6935353ECE4DF7D3311BA5B9309E] pmem
C:\Windows\system32\drivers\pmem.sys
14:27:22.0856 0x13a8 pmem - ok

14:27:22.0856 0x13a8 [2769F200292C0F941A10BD60C33EA4A6, B8345C32585C45E6248D7194B1071F2B8617718E7C9B270AAF44C132D029DB4C] PNPMEM
C:\Windows\System32\drivers\pnpmem.sys
14:27:22.0856 0x13a8 PNPMEM - ok
14:27:22.0856 0x13a8 [6AAAC8AD69AEFBE5FE04738B687EE85E, 83427082298E2FC021D5D39A43DB4A5783D95213F2CA8D3A997DB6C815BD9CB2] PNRPAutoReg
C:\Windows\system32\pnrpauto.dll
14:27:22.0871 0x13a8 PNRPAutoReg - ok
14:27:22.0871 0x13a8 [A14E30EDF51BC0A2C8AC76498D4BD13D, FC204664DD63EA323FC6C5033EED09435C4B589672AC8B1C51767F88BC7034E9] PNRPsvc
C:\Windows\system32\pnrpsvc.dll
14:27:22.0871 0x13a8 PNRPsvc - ok
14:27:22.0888 0x13a8 [7B7DD80EBFF46E14D6FA64488F2D9D0D, 0D192C986F8A1B384B8880E8C7BEE011DA0D849A4B2492F53E37B7392F3F8C35] PolicyAgent
C:\Windows\System32\ipsecsvc.dll
14:27:22.0888 0x13a8 PolicyAgent - ok
14:27:22.0888 0x13a8 [562B9409AA8777204E78C629647344EC, 65C33D25E0C00731D7DEF3F127523AA5178133481915287F3267A52C74577572] portcfg
C:\Windows\System32\drivers\portcfg.sys
14:27:22.0888 0x13a8 portcfg - ok
14:27:22.0888 0x13a8 [EAAAD6CBE66F082E2AE1348A3345418E, CB950E6DB2E5A4B4E3ECD2E37F9DAA48317D5B71F8E821590994BC86973642D3] Power
C:\Windows\system32\umpo.dll
14:27:22.0902 0x13a8 Power - ok
14:27:22.0902 0x13a8 [2E0C8A0212DA1A835CE9DDF775441F86, 35C4851CE7C78363F469DD212389B9A71B7A01E48848040A150C20441F700C00] PptpMiniport
C:\Windows\System32\drivers\raspptp.sys
14:27:22.0902 0x13a8 PptpMiniport - ok
14:27:22.0949 0x13a8 [F833AD1FB0E1D21F1232C555280F18EF, 1805BF76A9A373B0C17C4840964BFB0C443C7A54D231ECE9B7BDAC0F45CB3F3E] PrintNotify
C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll
14:27:22.0997 0x13a8 PrintNotify - ok
14:27:22.0997 0x13a8 [8860AE9314D3CD6B4DBC53AF50B514F6, 63925C65E115C86BBEDF1E45DB39B1E1C02D585A3E4C67BA3CF09FF93CEDB586] PrintWorkflowUserSvc
C:\Windows\System32\PrintWorkflowService.dll
14:27:23.0012 0x13a8 PrintWorkflowUserSvc - ok
14:27:23.0012 0x13a8 [34A3BC11F0A2964E730DD6EA1FB4BE3A, DD8E0EDF252352FA11D34421B5CF38C7109AF2410A3C43C792475A74D2716A6B] Processor
C:\Windows\System32\drivers\processr.sys
14:27:23.0012 0x13a8 Processor - ok
14:27:23.0012 0x13a8 [984EA74642BF61C4BBE455EE32E9C651, 3B9B13DC0BEC1B5A8556D5AC71E0C5D4C8EDB30F3667F75CB8B4B1830D7EC93C] ProfSvc
C:\Windows\system32\profsvc.dll
14:27:23.0027 0x13a8 ProfSvc - ok
14:27:23.0027 0x13a8 [22A4EF7DAAFE1A16AEE0E99DAEFADAD4, 3AFAFB314E689DF08E7987ACCB5E9DF00B6F5661B5610243553426144B5EC8D2] Psched
C:\Windows\system32\drivers\pacer.sys
14:27:23.0027 0x13a8 Psched - ok
14:27:23.0027 0x13a8 [A2C42528A1EF3D636E5249DB1D980248, E9AA97EDE611244CC2ED939C51B2968457424FF612E396D6B44AE9894BD32B07] PushToInstall
C:\Windows\system32\PushToInstall.dll
14:27:23.0043 0x13a8 PushToInstall - ok
14:27:23.0043 0x13a8 [90DB4F0A7AB40DABDF58E905464BD1CC, FF69F229DD6F0509B53E343329939650A081A1709E7701BFBF010FA097919AFE] QWAVE
C:\Windows\system32\qwave.dll
14:27:23.0043 0x13a8 QWAVE - ok
14:27:23.0043 0x13a8 [CE51A9A997D2830C6C64A36D7F8D8879, 706D683CAF92C259C121222446D34ED43F6E8872407C3615E2ED118ACD24D21D] QWAVEdrv
C:\Windows\system32\drivers\qwavedrv.sys
14:27:23.0059 0x13a8 QWAVEdrv - ok
14:27:23.0059 0x13a8 [9D377A5872A0A7A33E258FFCBDB3F25F, D461798C6348C5D96EA002E4A1AC588B87A1A9B01AD84AB1FA6D9C6393616892] Ramdisk
C:\Windows\system32\DRIVERS\ramdisk.sys
14:27:23.0059 0x13a8 Ramdisk - ok
14:27:23.0059 0x13a8 [EFD1B9E87D4291EDA39B6048E09DF285, 45FAAB862270D05681CCFF3426D6441D70EE783E08464060C8B0E04EA35537A4] RasAcd
C:\Windows\system32\DRIVERS\rasacd.sys
14:27:23.0059 0x13a8 RasAcd - ok
14:27:23.0059 0x13a8 [1B9D9034B00320B14591F8F871DA1E2B, FECEA513DB7ADE92809B03CBC0C5E0400733D2A497460F8ECFD3839C96BE3F36] RasAgileVpn
C:\Windows\System32\drivers\AgileVpn.sys
14:27:23.0059 0x13a8 RasAgileVpn - ok
14:27:23.0059 0x13a8 [F949CF7B1C3A4ECC6C6B320D93F693F9, 49C7D8E2CEBDD607B233B6AEA288190B40AA00ADDFDC9FFD4330924A910D94ED] RasAuto
C:\Windows\System32\rasauto.dll
14:27:23.0059 0x13a8 RasAuto - ok
14:27:23.0074 0x13a8 [4D437E9763F74517E7799B0569A5E17F, 6598AAA369A23C20D4E5597EFBA982C95A051523165DD547D1A4A1FCDB3665E5] Rasl2tp
C:\Windows\System32\drivers\rasl2tp.sys
14:27:23.0074 0x13a8 Rasl2tp - ok
14:27:23.0074 0x13a8 [B8A4797B20DCB29AFAC5277EAB8AA425, CAF640AB6C5C93E296F2B29A6B142001878D1854EE3A67823FF2145991EAFBCF] RasMan
C:\Windows\System32\rasmans.dll
14:27:23.0090 0x13a8 RasMan - ok
14:27:23.0090 0x13a8 [A0F6CED6B9E3F5F1F4B0123927359115, B0525F3AE3767C4A07B9FD2C86AFD0CB17DE5E2A47BFF7208D59B49DA93D70DD] RasPppoe
C:\Windows\system32\DRIVERS\raspppoe.sys
14:27:23.0090 0x13a8 RasPppoe - ok
14:27:23.0090 0x13a8 [55EA7A21E1D14658F624C997F7D549C1, DE93281086E5E86C66E520FD04C3FFBC56204D7B951A77847FCA7C33156E71D9] RasSstp
C:\Windows\System32\drivers\rassstp.sys
14:27:23.0106 0x13a8 RasSstp - ok
14:27:23.0106 0x13a8 [EC99C828C7A5CDBF0270575B13860CE9, 090B9D46F51641FB9C4C627E3B9AD2908E97F60FA975FD2D1EC8B805492EFBE8] rdbss
C:\Windows\system32\DRIVERS\rdbss.sys
14:27:23.0106 0x13a8 rdbss - ok
14:27:23.0106 0x13a8 [B7BAD23CA994EFF8EA11261626326004, 056495FB4A54984CE9D28D7B45550990D4A4B0736669F0F69138BEF51A695EFA] rdpbus
C:\Windows\System32\drivers\rdpbus.sys
14:27:23.0106 0x13a8 rdpbus - ok
14:27:23.0121 0x13a8 [FE64EC423603644DCFB39CE9539A046E, 0F3B2F637E4FDAFBB43316CF6BA8C1CD73A58F9FB78A79B300F5FE0BBBCCD747] RDPDR
C:\Windows\system32\drivers\rdpdr.sys
14:27:23.0121 0x13a8 RDPDR - ok
14:27:23.0121 0x13a8 [B8CCBE0170C63D8E980D4AE42A8E197E, 09CDC6CFC132E328C5FA7DD79427FF76DB08C847CB918A6FBC3F10DFD45F3BE3] RdpVideoMiniport
C:\Windows\system32\drivers\rdpvideominiport.sys
14:27:23.0121 0x13a8 RdpVideoMiniport - ok
14:27:23.0121 0x13a8 [B4A6F3BFB5A07DAF4E18C14A6337A226, F906865E349390D24A3DCBC563154BBB9F307B97361832BE93BC9D44A9F3B486] rdyboost
C:\Windows\system32\drivers\rdyboost.sys
14:27:23.0137 0x13a8 rdyboost - ok
14:27:23.0153 0x13a8 [BDDB18355C2E5157734B1C8CE4F512EC, C536CA7A7C6B07643BEC4E3C8E1D2817E250D6B229A72C547B366F1890AFF6FF] ReFS
C:\Windows\system32\drivers\ReFS.sys
14:27:23.0168 0x13a8 ReFS - ok
14:27:23.0184 0x13a8 [161C3442E0A9B454933ED475451D7705, 6107285B9B1ADA7D8910474BDEB86CE058A81CC8ECC875250466EDB19EE68926] ReFSv1
C:\Windows\system32\drivers\ReFSv1.sys
14:27:23.0184 0x13a8 ReFSv1 - ok
14:27:23.0199 0x13a8 [C972C88554537B2C54DADDC2940D354F, 9CD032E0C3257C55A00D1CC69D5FA6F17BF46624E477A5A81C6EC74A892F9E06] RemoteAccess
C:\Windows\System32\mprdim.dll
14:27:23.0199 0x13a8 RemoteAccess - ok
14:27:23.0199 0x13a8 [F4CE1E848124CA85D854609670886492, FFD090423C92B47BD3ED24689F2FA67044ED953ABEA1AC913C8E4F96C360E74A] RemoteRegistry
C:\Windows\system32\regsvc.dll
14:27:23.0215 0x13a8 RemoteRegistry - ok
14:27:23.0215 0x13a8 [FDCCCA45661AD7093F0A1A5BAEFF6F5B, 1AC0847F509932781FF487917C595360C525DAD4A80C5C4FDC68024EF04E270D] RetailDemo
C:\Windows\system32\RDXService.dll
14:27:23.0231 0x13a8 RetailDemo - ok
14:27:23.0231 0x13a8 [D2EE9CCE0187C616E50D61EB30ECA262, 825C918D22FC8DBF3EE9BDB41D121A0AC3CCBFFBA147E2B26F0197552E0675DE] RFCOMM
C:\Windows\System32\drivers\rfcomm.sys
14:27:23.0231 0x13a8 RFCOMM - ok
14:27:23.0231 0x13a8 [4DD0EFE49F0C020DAFEAE6F5F231362C, DF04978AF6CD34C8251B3DDE381CD77518684DCB1D2B16BD2DAFEE63AC9D5858] rhproxy
C:\Windows\System32\drivers\rhproxy.sys
14:27:23.0231 0x13a8 rhproxy - ok
14:27:23.0246 0x13a8 [D2B64CEF249497778FF7F1297EB993FD, 7CA00ABC438E00FE1F0C82EC51BE9C4C4C00AD5E3A92871AE63DCC4CD27E0F44] RmSvc
C:\Windows\System32\RMapi.dll
14:27:23.0246 0x13a8 RmSvc - ok
14:27:23.0246 0x13a8 [684E3334544179346B9BF04FD3CF58AA, E39F942AB5CD69A253AAF72B161094CDDB7947D216F03E5D004E63BAD40ADF63] RpcEptMapper
C:\Windows\System32\RpcEpMap.dll
14:27:23.0246 0x13a8 RpcEptMapper - ok
14:27:23.0246 0x13a8 [D45676C47616B9ABBFAEC97DD3B240A8, E13985D667F66B7A0082356F23270F61A57B8C2DD211B1E09D66D7970D7B4D6A] RpcLocator
C:\Windows\system32\locator.exe
14:27:23.0246 0x13a8 RpcLocator - ok

14:27:23.0262 0x13a8 [5A344C5D2140BD836AE545A9351373F4, 1C1DEF25FB645F9789A41F8533ECB144680F36D5F3B91B806D2DED972B1A0203] RpcSs
C:\Windows\system32\rpcss.dll
14:27:23.0278 0x13a8 RpcSs - ok
14:27:23.0278 0x13a8 [EABD30C39742A79913B595A5B6F809D4, 9067160F566220A2B21FEEE181729A796A3F3EECF75FFB75815BE5CCC7BBA64F] rspndr
C:\Windows\system32\drivers\rspndr.sys
14:27:23.0278 0x13a8 rspndr - ok
14:27:23.0293 0x13a8 [5914CC0C1E99A3C1711BDB1E224526D1, 54BB8636F27282B396D487B3FEA8BD73F2F6FE6DA4DE8D718EE498F75A6A5DCE] s3cap
C:\Windows\System32\drivers\vms3cap.sys
14:27:23.0293 0x13a8 s3cap - ok
14:27:23.0293 0x13a8 [B4DE3D04AE3C71E67236B841BEADEB74, 8567CDBA80952B2B7AF647B9D2630FE12B73E87517498BCCDCC27EC1ED6E1545] SamSs
C:\Windows\system32\lsass.exe
14:27:23.0293 0x13a8 SamSs - ok
14:27:23.0293 0x13a8 [3CEBF4FDFBF13FE29B294AA4DA79C56B, 603943FE869B6CE3596921BC708227D1FB600749CBE0F5923DF3D5E8151BEA54] sbp2port
C:\Windows\system32\drivers\sbp2port.sys
14:27:23.0293 0x13a8 sbp2port - ok
14:27:23.0293 0x13a8 [33EDC31E750253CFF50D94AADB72A58A, 09A3B279AA4C3C1A6BC0CD98DC7CA05319A8D1AA8FD209B4AA26CB37AE46D7C3] SCardSvr
C:\Windows\System32\SCardSvr.dll
14:27:23.0309 0x13a8 SCardSvr - ok
14:27:23.0309 0x13a8 [E5865E3E00097E5B5675785C8A53CE60, 795091E33C1C983BEFD79D36699CDFCD2DA00F4601A89219B57228505566DFCD] ScDeviceEnum
C:\Windows\System32\ScDeviceEnum.dll
14:27:23.0309 0x13a8 ScDeviceEnum - ok
14:27:23.0309 0x13a8 [275D0700B1DA2FCE6B979BB1B8EEBB3B, AD3B9126B375846B0E42A2B60E6F6D1BD7D6EA54E625B4E5C60E153E099A6538] scfilter
C:\Windows\system32\DRIVERS\scfilter.sys
14:27:23.0309 0x13a8 scfilter - ok
14:27:23.0325 0x13a8 [94D8B4E7A97B749999C63C584F4AA25C, 5D8FF339C2AE0E1EF015031CFE32F32A988531ED90131A895AECB6A1095F8D24] Schedule
C:\Windows\system32\schedsvc.dll
14:27:23.0325 0x13a8 Schedule - ok
14:27:23.0340 0x13a8 [E049CF53E7F8AA2341198A7D78A8ACF9, 9CD35EA78E211AE9D2342A031DEF0D199362BC80030883399B70F6E015F61C06] scmbus
C:\Windows\system32\drivers\scmbus.sys
14:27:23.0340 0x13a8 scmbus - ok
14:27:23.0340 0x13a8 [D0843B744F4E7E30BD74A1CF5426A44C, 8E2A05A464A9671232E25D7C0505300F2BAD6D96C2CBF4F4427D1F795621EAEF] SCPolicySvc
C:\Windows\System32\certprop.dll
14:27:23.0340 0x13a8 SCPolicySvc - ok
14:27:23.0355 0x13a8 [2D7D34D09BBEFA88E47D2225EC8F73F2, 896FCD7ED93BE3F92205498D526DEA5F73E88E8CE30B0671CB77D758E4537A20] sdbus
C:\Windows\System32\drivers\sdbus.sys
14:27:23.0355 0x13a8 sdbus - ok
14:27:23.0355 0x13a8 [3200667DB433F0A2032FAF4DC02E2089, 5E940CA63AD21CEA08C334AC61D985BAFDBA7DCB2D388F355B5C72EFA3E23E0A] SDFRd
C:\Windows\System32\drivers\SDFRd.sys
14:27:23.0355 0x13a8 SDFRd - ok
14:27:23.0355 0x13a8 [C9D45DA3CDEC8A8D455B8A1B1DE94BEE, BD5ACD1CE9304F8BBE993298DF7B69F7512A012EF3B53E7C3232C779E881BC44] SDRSVC
C:\Windows\System32\SDRSVC.dll
14:27:23.0355 0x13a8 SDRSVC - ok
14:27:23.0371 0x13a8 [8C0C961B03F68705096E36C3ED96229D, 28C9CC61985DF2D60DDFA099BC416875309839FD187CA029D70BE96C1F5C8062] sdstor
C:\Windows\System32\drivers\sdstor.sys
14:27:23.0371 0x13a8 sdstor - ok
14:27:23.0371 0x13a8 [2A0FF7C885BF7CAFADCF60F4B2F5F2BC, 1C6DE87C19502F2672843D9FF21D3C85367CF70921E64DE56681DDEF25665087] seclogon
C:\Windows\system32\seclogon.dll
14:27:23.0371 0x13a8 seclogon - ok
14:27:23.0387 0x13a8 [B6B4D87D649E6FFF0E25416D8F360B23, 9FB99DD6648998EDDC4AF6AE101C621BB52AA0E7C65F93F3E9B2F6B0CEFD1106] SecurityHealthService
C:\Windows\system32\SecurityHealthService.exe
14:27:23.0387 0x13a8 SecurityHealthService - ok
14:27:23.0402 0x13a8 [5E49967298FF00A720971162DE48449D, D988B919B364D8B6D70071F6B476DFD89DC63066E086CBCB110F14F19130CDB9] SEMgrSvc
C:\Windows\system32\SEMgrSvc.dll
14:27:23.0418 0x13a8 SEMgrSvc - ok
14:27:23.0418 0x13a8 [1EA7972A4C7163FF1D3EFE9988404D4E, 56A94B1617815C1E8A79D832B0F0CBA683C3080105CC4C87DBB9B8EAB4CD2690] SENS
C:\Windows\System32\sens.dll
14:27:23.0418 0x13a8 SENS - ok
14:27:23.0434 0x13a8 [77B6DF651E377D2270115054B9896F85, 7F66A5FCE8FA2F89681F31C8483F194BB7930B32ECDF535876C037CBD4F7C25B] SensorDataService
C:\Windows\System32\SensorDataService.exe
14:27:23.0449 0x13a8 SensorDataService - ok
14:27:23.0449 0x13a8 [ED9AAEC1AB631791254D1AC1D13C4914, 5BDDB26F6791F24C13F8F6BC13CE175387414EAFEF24B52FFE32A1C1CF037B83] SensorService
C:\Windows\system32\SensorService.dll
14:27:23.0465 0x13a8 SensorService - ok
14:27:23.0465 0x13a8 [0BCFFAD6F3B180DD60C941B01768F733, A0B73C1BF636F14504B69606999287B6FE148C958A4F6E31E9022FF129A048E0] SensrSvc
C:\Windows\system32\sensrsvc.dll
14:27:23.0465 0x13a8 SensrSvc - ok
14:27:23.0465 0x13a8 [22068CA363EAF69A8EF6EBBBD580A8E8, 45F87C7D04B8F20290BBA8517BACE138D1E2112A268CCFFC2DFC407A81C0A197] SerCx
C:\Windows\system32\drivers\SerCx.sys
14:27:23.0465 0x13a8 SerCx - ok
14:27:23.0480 0x13a8 [A5E6D99D319610030C3CA982DCAA3624, 8F1BCEDC5FEA5AF0260B573EE171E1D895EBAB5A51BEA1F84D3043F6612050A9] SerCx2
C:\Windows\system32\drivers\SerCx2.sys
14:27:23.0480 0x13a8 SerCx2 - ok
14:27:23.0480 0x13a8 [7A289A4FFAA43D81F091A302512059A6, 9A4EC5EAF65ECB6518C462E837EB76286F1BA7A8C9E26DC46586DC4F189BD1B7] Serenum
C:\Windows\System32\drivers\serenum.sys
14:27:23.0480 0x13a8 Serenum - ok
14:27:23.0480 0x13a8 [DCE5D050F3B06D30985EE126257DEEB6, 024C1F9FBEFDCBC174733A5C97B121A6D7AD30E836C1820054BCB45F99FB4373] Serial
C:\Windows\System32\drivers\serial.sys
14:27:23.0480 0x13a8 Serial - ok
14:27:23.0480 0x13a8 [B13F5A8574F0B71B2E4C84B171C28724, C812F61726BDFEFFE468DFA3491E5F465D22835C54E3559E04B452940C0EEEEE] sermouse
C:\Windows\System32\drivers\sermouse.sys
14:27:23.0480 0x13a8 sermouse - ok
14:27:23.0496 0x13a8 [7F3F7304C32808B2DB8690BB1EA6748B, DC95D02FDA4EA527F342AD6EF169837A93EFAD8491B520744C43344EB0560852] SessionEnv
C:\Windows\system32\sessenv.dll
14:27:23.0496 0x13a8 SessionEnv - ok
14:27:23.0496 0x13a8 [AD1B790A42984A825068B849A88AD322, 63881202D6D900656F50A0E40CB743D0769C2AD9810FE96387E9DAF2BC89E4C5] sfloppy
C:\Windows\System32\drivers\sfloppy.sys
14:27:23.0496 0x13a8 sfloppy - ok
14:27:23.0512 0x13a8 [C05648C2BE6176BE557D9C7F02916388, C65D8FEDDCD9A52B04F42C64DAD2A499BF51246D36042E8DC09DD04C4C0B7BEE] SgrmAgent
C:\Windows\system32\drivers\SgrmAgent.sys
14:27:23.0512 0x13a8 SgrmAgent - ok
14:27:23.0512 0x13a8 [89F3A411DDEDF767ACDF94B11486E3EE, 5F2F668394FBED842D0FE461059F6C71C95B5F0D476206B7003E63AA1DE7C684] SgrmBroker
C:\Windows\system32\SgrmBroker.exe
14:27:23.0512 0x13a8 SgrmBroker - ok
14:27:23.0528 0x13a8 [9B017BFFBB5A4338446844 81E61C34E7, FB609DD7073F03CD00BC935E3629DAC5669347D1F8001855D84597E5CDDAF364] SharedAccess
C:\Windows\System32\ipnathlp.dll
14:27:23.0528 0x13a8 SharedAccess - ok
14:27:23.0543 0x13a8 [739E825B9DA34DDAAB28B81D94171705, 3583A842B37FEB3DE4C870ADFB45C9D580D46147F97119DC6BEB02FED8E144D5] SharedRealitySvc
C:\Windows\System32\SharedRealitySvc.dll
14:27:23.0543 0x13a8 SharedRealitySvc - ok
14:27:23.0543 0x13a8 [BE5ECC669E744390AB00D8F63217977A, 30C42E31F12354DB8DB0D99BBD7D5617A5CDED7E1737F636429899703948C34D] ShellHWDetection
C:\Windows\System32\shsvcs.dll
14:27:23.0543 0x13a8 ShellHWDetection - ok
14:27:23.0559 0x13a8 [0A36B6954818CF6AA3C7CBE80C52B958, 27694BC08D4320FB06D07814BEC96CD1249DA3D6FD813F5B79833E55BE55DE41] shpamsvc
C:\Windows\system32\Windows.SharedPC.AccountManager.dll
14:27:23.0559 0x13a8 shpamsvc - ok
14:27:23.0559 0x13a8 [9AB1BADC5A324DA39186B81BC6CE6E2E, 567710C90BD71600A31A3408DB065B43C844DCFD12045FDE04CD59D932DC8353] SiSRaid2
C:\Windows\system32\drivers\SiSRaid2.sys
14:27:23.0559 0x13a8 SiSRaid2 - ok
14:27:23.0559 0x13a8 [60213AF297023C005453E1CBF7CB6FE7, 718C833E5EDFE642F3B254515E29641BF2D8E56E22F6B795024BF64721AB874E] SiSRaid4
C:\Windows\system32\drivers\sisraid4.sys
14:27:23.0559 0x13a8 SiSRaid4 - ok
14:27:23.0574 0x13a8 [196A46BA842A219EC6DE7B7B7D9AAB7E, 4EF7BE37F92557C8B0D30999541F284CC4A3E8FD98E0D78146F9F00D54E11BB9] SmartSAMD
C:\Windows\system32\drivers\SmartSAMD.sys
14:27:23.0574 0x13a8 SmartSAMD - ok

14:27:23.0574 0x13a8 [4ADF84157BC2EBD1D6D91DEC0921F9C9, 98C24ECF700194AB36840DB530148A2487A1CC76AF6EBC80D70320111E8FA01E] smphost
C:\Windows\System32\smphost.dll
14:27:23.0574 0x13a8 smphost - ok
14:27:23.0574 0x13a8 [AE73F050453F5AC76235857C414DA4C2, 2476E3C013A73798CA9525C7A8AC78B8F3B2243D1B374068ADBEF6015D895A9B] SmsRouter
C:\Windows\system32\SmsRouterSvc.dll
14:27:23.0590 0x13a8 SmsRouter - ok
14:27:23.0590 0x13a8 [1971BBC71602B928CF9257759E3C05E8, 9D665698FF26ED333AD385B4B7A6C0F2B6806371D278E281FA4188002A5317E8] SNMPTRAP
C:\Windows\System32\snmptrap.exe
14:27:23.0590 0x13a8 SNMPTRAP - ok
14:27:23.0590 0x13a8 [27B7D9E872939EBB34C30343F991893D, 879AFDC8C50487ED0D3CB58C70A206E185F94BE75C25C31C387F3F08740771F9] spaceparser
C:\Windows\system32\drivers\spaceparser.sys
14:27:23.0590 0x13a8 spaceparser - ok
14:27:23.0606 0x13a8 [32308CA6506E36661CA9E6E5FDEB3D95, 7267FF3601F475B6BC63661BAFB1B0CEF24512FE2BC69F0E5927D64FB53DAB6B] spaceport
C:\Windows\system32\drivers\spaceport.sys
14:27:23.0606 0x13a8 spaceport - ok
14:27:23.0606 0x13a8 [AB3BDEC793187CEDF1229AC98BB7DEDF, D2EA0C5FC534C89310207AA26A8816B30FEEF3F2708A067D8BB93D3CFF9C3936] SpatialGraphFilter
C:\Windows\system32\drivers\SpatialGraphFilter.sys
14:27:23.0621 0x13a8 SpatialGraphFilter - ok
14:27:23.0621 0x13a8 [B9B40C14564A487A873DE3604A4856A9, 4A49A0449A93C97870A6E7ACE9B3AE2FB7DA07D5A6064B2EC8D20639F155FD1C] SpbCx
C:\Windows\system32\drivers\SpbCx.sys
14:27:23.0621 0x13a8 SpbCx - ok
14:27:23.0621 0x13a8 [7093263C3E0BA5EE1F8994CE0E5C580E, 2ADBF6D8B71ABBB381F7945BF416009CD186711DD06FA7594206FF0765D246E9] spectrum
C:\Windows\system32\spectrum.exe
14:27:23.0637 0x13a8 spectrum - ok
14:27:23.0652 0x13a8 [00A0010EE931C491DDDC6EE5AF16F2DD, 27C0563663B843CB229DB1B266FDF01BBB62846F2CE480DC804EA3B5A32074CB] Spooler
C:\Windows\System32\spoolsv.exe
14:27:23.0652 0x13a8 Spooler - ok
14:27:23.0699 0x13a8 [2343450F4CBEB3FBE73EF032B9AF2EC6, 61A199A6CC11A4E6E4098B6AF04549E7E69DABB0D8115049B79E75495E909E32] sppsvc
C:\Windows\system32\sppsvc.exe
14:27:23.0746 0x13a8 sppsvc - ok
14:27:23.0746 0x13a8 [F0A262C8C6A45C51F39D4147511CD3F2, B3911A9490FA67B23A63F66994EA41F2E3D9356D9B75218930A67851D5677A16] srv2
C:\Windows\system32\DRIVERS\srv2.sys
14:27:23.0762 0x13a8 srv2 - ok
14:27:23.0762 0x13a8 [B24200CE5FF43D72ADA0EDB6EEB24D6B, 1F6DC2F5354A8159A200483D713E82AC8BE9B38E598D1ED5A1546133BF2E10FA] srvnet
C:\Windows\system32\DRIVERS\srvnet.sys
14:27:23.0762 0x13a8 srvnet - ok
14:27:23.0777 0x13a8 [958FCD240BE02FCB92192246BA4AB785, 4053074B0D077EA0AE523873A195F880D9F7BD1A7ECE5BE1D41F9A0E66193F58] SSDPSRV
C:\Windows\System32\ssdpsrv.dll
14:27:23.0777 0x13a8 SSDPSRV - ok
14:27:23.0777 0x13a8 [66969AA56E77953E596470C73A9004E0, 71F4CC7595C6D5E93AAA14259DF817C6C1D4BBCF285545FD980F6DBC86A30379] ssh-agent
C:\Windows\System32\OpenSSH\ssh-agent.exe
14:27:23.0794 0x13a8 ssh-agent - ok
14:27:23.0794 0x13a8 [90E5D79F3607BA423F2B30D1F7344CF4, A87A72E9C854D51318C0F132BF042052A0CFA2FA1294B3DD3166A5E419206E78] SstpSvc
C:\Windows\system32\sstpsvc.dll
14:27:23.0794 0x13a8 SstpSvc - ok
14:27:23.0855 0x13a8 [66676FE32FCA0B63833DA8D99D5F417B, 1A492D076C55A4454E1B11C4BE453BD9821E673E64AEC1DF506ADC73A91A4993] StateRepository
C:\Windows\system32\windows.staterepository.dll
14:27:23.0903 0x13a8 StateRepository - ok
14:27:23.0903 0x13a8 [09DC471B4573F3D01D7E448B526AE70A, 766FD1E1D2F73DE202FB337F6A6A5BA0317772AAAA644E9103BB5DF438162F51] stexstor
C:\Windows\system32\drivers\stexstor.sys
14:27:23.0903 0x13a8 stexstor - ok
14:27:23.0918 0x13a8 [4853187B1874FE88C6045AB8308C540A, 53531585EE3F0B39DE8B606ECE547E81DB704A118BF03C73B36A8772594F26CD] stisvc
C:\Windows\System32\wiaservc.dll
14:27:23.0918 0x13a8 stisvc - ok
14:27:23.0934 0x13a8 [534830E54E93805ADAC272AD07965A34, F008D11E24C8E3FC5E4246C32F63B939532FC5D062C75B0ABA79ECE43CFD514F] storahci
C:\Windows\system32\drivers\storahci.sys
14:27:23.0934 0x13a8 storahci - ok
14:27:23.0934 0x13a8 [E5A45BC1B04CB65869AFAAA06A014D91, FFD95493EC4712C0BEFD96F85DC9566C1F8358ABA48192E5A603867BBD08270F] storflt
C:\Windows\system32\drivers\vmstorfl.sys
14:27:23.0934 0x13a8 storflt - ok
14:27:23.0934 0x13a8 [4C10E085AB38A0487AE26AB5DADF67E3, C41E009AA0284B2A7106C4F6ECB10A216C2E442EBD320ABAD7CCDBC6B1DDCBAE] stornvme
C:\Windows\system32\drivers\stornvme.sys
14:27:23.0934 0x13a8 stornvme - ok
14:27:23.0949 0x13a8 [995F082126674C6D1423E29FBCEA9F39, E86386156F982B59C00991D40A6E1862CA322F151BF965B14572D13AA207D614] storqosflt
C:\Windows\system32\drivers\storqosflt.sys
14:27:23.0949 0x13a8 storqosflt - ok
14:27:23.0949 0x13a8 [48A39E15B94D4C6405EA71D9CB64A301, 1CA096DAB3874342DC4B84EE706936867E58F5DA1D42EDE122A74AE952D159CF] StorSvc
C:\Windows\system32\storsvc.dll
14:27:23.0965 0x13a8 StorSvc - ok
14:27:23.0965 0x13a8 [FF456F376E6CDA609438C3740119E333, F38B0E60C6F6C8AA73C7F6F64821919B0A89906BDACC0B9842702A5A47A8BC5C] storufs
C:\Windows\system32\drivers\storufs.sys
14:27:23.0965 0x13a8 storufs - ok
14:27:23.0965 0x13a8 [ECBA758F75B186C70F100EA3F8999FBD, 2E5637B3123E8F7B1C91C93FAB6B8CE08C0EEC5D6D1BC924DB7C5E5E759C0E57] storvsc
C:\Windows\system32\drivers\storvsc.sys
14:27:23.0965 0x13a8 storvsc - ok
14:27:23.0981 0x13a8 [D73F83E795F3BC100C21EDA2BD6DE307, 0DC828C46E057ADA9934424BF00067B17EEB8E0108CE1E309C8DEA4CC42448BA] svsvc
C:\Windows\system32\svsvc.dll
14:27:23.0981 0x13a8 svsvc - ok
14:27:23.0981 0x13a8 [0547BB19EFA07BEF0F679A054EB5CFEC, D618F57B78B3FFEC29E8C4472E0AA72EF1CA0C83DE968373B818ABA4D9747E2D] swenum
C:\Windows\System32\DriverStore\FileRepository\swenum.inf_amd64_16a14542b63c02af\swenum.sys
14:27:23.0981 0x13a8 swenum - ok
14:27:23.0996 0x13a8 [70936B7B21AD4C84863C4FB215AF63A6, 5A4FD095EAA23CD69CB6133FB3B3DC80B42ACB7E5044331A5C4E71449DA068B6] swprv
C:\Windows\System32\swprv.dll
14:27:23.0996 0x13a8 swprv - ok
14:27:23.0996 0x13a8 [12C03F0F7F86E13D32CBD7472A5A09E5, 4DE8FF1730A7908C9580734FF0E5863125FCF0839FDCE03E8EC48DFC859D590F] Synth3dVsc
C:\Windows\System32\drivers\Synth3dVsc.sys
14:27:23.0996 0x13a8 Synth3dVsc - ok
14:27:24.0012 0x13a8 [B23AF3CB41EA6669F5957B980BD513BA, 81ED6A14B27EA69C77C581C49766B3F48B6522DCE9AE3FEA839D3A3B40C3D25E] SysMain
C:\Windows\system32\sysmain.dll
14:27:24.0027 0x13a8 SysMain - ok
14:27:24.0027 0x13a8 [7C3C3BBD8F2C27540DD94D7ABA5CCFFE, E95500B44F8663C37D039C3BA91ABE41FC8502D87A7C5EF97319BFA13A467916] SystemEventsBroker
C:\Windows\System32\SystemEventsBrokerServer.dll
14:27:24.0027 0x13a8 SystemEventsBroker - ok
14:27:24.0043 0x13a8 [F6A932ADED4C6D0ABC3464F919903CA6, BE62DEA86790B82E4B46A8E579947736788B341848259B4D7BF40EE38F0C003A] TabletInputService
C:\Windows\System32\TabSvc.dll
14:27:24.0043 0x13a8 TabletInputService - ok
14:27:24.0043 0x13a8 [180B8470737107F0B96875D16E3181B4, 62AFDEAB7D98BDC8D566F66076D76F0D6EF2B5EEA1D0EE1F2E841A01315306BF] TapiSrv
C:\Windows\System32\tapisrv.dll
14:27:24.0043 0x13a8 TapiSrv - ok
14:27:24.0074 0x13a8 [A218D0DC32AC9358AE355F995E57E878, 9318B3E78B9B6B0D5F4E9387DA63CC7C29395163E2E9609AD5718AD673603064] Tcpip
C:\Windows\system32\drivers\tcpip.sys
14:27:24.0105 0x13a8 Tcpip - ok
14:27:24.0137 0x13a8 [A218D0DC32AC9358AE355F995E57E878, 9318B3E78B9B6B0D5F4E9387DA63CC7C29395163E2E9609AD5718AD673603064] Tcpip6
C:\Windows\system32\drivers\tcpip.sys
14:27:24.0152 0x13a8 Tcpip6 - ok
14:27:24.0168 0x13a8 [C347F16F69A12F07D21CAE562C58D4F1, 22AC04675A098790DE7572E4DF774045BFA8073C08BC2A496DBBD02DB825A1AD] tcpipreg
C:\Windows\system32\drivers\tcpipreg.sys
14:27:24.0168 0x13a8 tcpipreg - ok
14:27:24.0168 0x13a8 [ACA4E52E500D39B5F24EAEAB441AEC59, 4AE1CB302AB67053393FE448A735A454D22FFE2BD9546E458980F811D9CD9CA8] tdx
C:\Windows\system32\DRIVERS\tdx.sys
14:27:24.0168 0x13a8 tdx - ok
14:27:24.0168 0x13a8 [1D35CBEA001C38B5BF2FF0C2E8CF77AB, A341365C286B93B7B2861BFF90497BEABA8F7DE0ECB04270311EAB446A2981E1] Telemetry
C:\Windows\system32\drivers\IntelTA.sys
14:27:24.0168 0x13a8 Telemetry - ok

14:27:24.0168 0x13a8 [C225B94F2B27AC97C3E66C0550AEA249, 6F88375DD12A648B77BB6EB4BE527FF6678EE76A2059DB5B4CC971CDB31D0DB8] terminpt
C:\Windows\System32\drivers\terminpt.sys
14:27:24.0184 0x13a8 terminpt - ok
14:27:24.0184 0x13a8 [618A97628E9C3882675205B07559EE4E, 1132A5F691C061E272B70B0A93688BB0FD2A7CD74FF9340013BBC30F239A7872] TermService
C:\Windows\System32\termsrv.dll
14:27:24.0200 0x13a8 TermService - ok
14:27:24.0215 0x13a8 [8EC4197962A0349DFFBDC11586099DB8, 8DD5348A4983C376F63E6B209227D4D02300555F8C80A0E0DB2EA16074ABC334] Themes
C:\Windows\system32\themeservice.dll
14:27:24.0215 0x13a8 Themes - ok
14:27:24.0215 0x13a8 [E64A2EE3B6C0877BEDC8D2B09262CCF3, F85CA601B1D538936A2F092C4A720E3AEC33BB1132D2301C3D0244ADFC5D4180] TieringEngineService
C:\Windows\system32\TieringEngineService.exe
14:27:24.0215 0x13a8 TieringEngineService - ok
14:27:24.0230 0x13a8 [334C39E3D937DE018BB4A70C65E13A00, 3BBD60D603E6B3B6CD4B44D851AD98010851CA12545627361DB881F1F6949483] TimeBrokerSvc
C:\Windows\System32\TimeBrokerServer.dll
14:27:24.0230 0x13a8 TimeBrokerSvc - ok
14:27:24.0246 0x13a8 [83E506C203F6AEB1718F0148944E994C, 23A34CE047D6CF20A6C61857A5C13044433CF40BFA4C6ACB78B07D1FF5942131] TokenBroker
C:\Windows\System32\TokenBroker.dll
14:27:24.0262 0x13a8 TokenBroker - ok
14:27:24.0262 0x13a8 [EBB2729FB8B0B166322B01BF7B409375, DEB344A48CAE8BE1C7ED8CE5215B61733D9DEE8EEB3F931951E71E6FA6CCA110] TPM
C:\Windows\System32\drivers\tpm.sys
14:27:24.0262 0x13a8 TPM - ok
14:27:24.0262 0x13a8 [4FF3D175D3C14156F368BDEB4A3155A4, 2C608CCC3D1C23A67176EAA0E7088618284948F4377A07DF7044E894C8D174C4] TrkWks
C:\Windows\System32\trkwks.dll
14:27:24.0278 0x13a8 TrkWks - ok
14:27:24.0278 0x13a8 [4F9DFBF585D04997C6F587057B9AEBAA, 456EF0FB4D082F9E7ADB7ECF7F558D192C8F2E4C36BF43A7CEAC0E981D1BEF68] TroubleshootingSvc
C:\Windows\system32\MitigationClient.dll
14:27:24.0278 0x13a8 TroubleshootingSvc - ok
14:27:24.0293 0x13a8 [9AB25E301DAC8A8F6CF14D51E7284545, 2A47E31B708C2AB1D0B4A40802B56C49505361FFB275E4B4C14370B3BFC12245] TrustedInstaller
C:\Windows\servicing\TrustedInstaller.exe
14:27:24.0293 0x13a8 TrustedInstaller - ok
14:27:24.0293 0x13a8 [F613A8618CC19DD96D1E0C81C5DCB7D1, AD6DE675AC033BE6BF75FF6303EAED4B5C672689D3AEC6DB94816D60E19B7030] TsUsbFlt
C:\Windows\system32\drivers\tsusbflt.sys
14:27:24.0293 0x13a8 TsUsbFlt - ok
14:27:24.0293 0x13a8 [F7CE17347B4112725722A03B2522BF06, A1A46B531D771F00B44DB5FBD02F57AB47189E057B48D7F877A2B6F929BA7314] TsUsbGD
C:\Windows\System32\drivers\TsUsbGD.sys
14:27:24.0293 0x13a8 TsUsbGD - ok
14:27:24.0309 0x13a8 [DDA930C1ED5D0885F367E430C9F97777, 6275B56592576F9213C7DE79D67B029AB80B372B71E72204122296772743C501] tunnel
C:\Windows\system32\drivers\tunnel.sys
14:27:24.0309 0x13a8 tunnel - ok
14:27:24.0309 0x13a8 [7D0493BAC5A760D29C0A4E1EFD53A321, 6B7EB10203723F67B58541A354C383E30276D7BAE25DA0D95EE666F9269DD454] tzautoupdate
C:\Windows\system32\tzautoupdate.dll
14:27:24.0309 0x13a8 tzautoupdate - ok
14:27:24.0309 0x13a8 [94743AD42166CD506FD34C9A06CB5A10, 89CF9D1C37657C1A50C9706C03202E76980611B639443C65D5D110E955F00918] UASPStor
C:\Windows\System32\drivers\uaspstor.sys
14:27:24.0309 0x13a8 UASPStor - ok
14:27:24.0309 0x13a8 [04D6823B08D8B8D428EDF81AA8A03C12, 45A8D660738C52163394CA526E9C2F8B41D7EAF7958B523C1D6AD6F6C5291F48] UcmCx0101
C:\Windows\system32\Drivers\UcmCx.sys
14:27:24.0324 0x13a8 UcmCx0101 - ok
14:27:24.0324 0x13a8 [229B33B8499F4F2AAB1F3B590423611F, E70A2D9EEEF0C6894A0DB7990CFF6ECE3B8F389FD30B7B1949FCBDD3300B6148] UcmTcpciCx0101
C:\Windows\system32\Drivers\UcmTcpciCx.sys
14:27:24.0324 0x13a8 UcmTcpciCx0101 - ok
14:27:24.0324 0x13a8 [7FDC3A6FD8547468CE554C8821640103, 3626760AEE42EE36E047DA6899A81E0646DFBA344A234270EAE5D635F049BE37] UcmUcsiAcpiClient
C:\Windows\System32\drivers\UcmUcsiAcpiClient.sys
14:27:24.0324 0x13a8 UcmUcsiAcpiClient - ok
14:27:24.0324 0x13a8 [2E0D9627CA5A23D0C93ED5FA4E8CE6DE, 192B69BAE67E1439A6294AE7FBB9283D4291C5E90F3A1C871733F9DD71708859] UcmUcsiCx0101
C:\Windows\system32\Drivers\UcmUcsiCx.sys
14:27:24.0324 0x13a8 UcmUcsiCx0101 - ok
14:27:24.0340 0x13a8 [D6BEDCCB2E48589944EDC675D335677E, 2F5A5BA7AEC40C1A440C8DFF81DCE5AB0BDF9CC70ADDE48F8B652665B61F9915] Ucx01000
C:\Windows\system32\drivers\ucx01000.sys
14:27:24.0340 0x13a8 Ucx01000 - ok
14:27:24.0340 0x13a8 [6861422B7FFADDEAAA64A0539C910178, 4F8193C0A3525B78CA3CAF4731AE997A214F3DF180F0A3ADCEB2D31D3217850C] UdeCx
C:\Windows\system32\drivers\udecx.sys
14:27:24.0340 0x13a8 UdeCx - ok
14:27:24.0340 0x13a8 [DAA928BA472C091678CA4CD6225CD3E5, 4B1F7F61E0D05EF55B7EEE338D908A1B400CA5EABCE34D8410645756FA839CA6] udfs
C:\Windows\system32\DRIVERS\udfs.sys
14:27:24.0356 0x13a8 udfs - ok
14:27:24.0371 0x13a8 [620FD4CDFCA26011A9BADB2D5CA55EA0, 27F42FE4ED368BC93D655DA6F0273171ABB7485B9E4FDC88CA95EC8EF34F1004] UdkUserSvc
C:\Windows\System32\windowsudk.shellcommon.dll
14:27:24.0402 0x13a8 UdkUserSvc - ok
14:27:24.0402 0x13a8 [264C183C222EF95D4C64DFA8BA5F0479, 3EF244E91851E03BE77DE49FA7E36769DE287B0CB732CD0140C39FE5118D80B9] UEFI
C:\Windows\System32\DriverStore\FileRepository\uefi.inf_amd64_c1628ffa62c8e54c\UEFI.sys
14:27:24.0402 0x13a8 UEFI - ok
14:27:24.0419 0x13a8 [D134F439D22F317A9576FC0CB296109A, 7D850D69EC69E1632C32C80CCAAC1488F1EF374EF9103295076A0C945B13EA54] Ufx01000
C:\Windows\system32\drivers\ufx01000.sys
14:27:24.0419 0x13a8 Ufx01000 - ok
14:27:24.0419 0x13a8 [EEEECAFD642DB20A8470090C2ACAA6AC, 70FEAD3371792160701D47A808FC78786766E4C7CA7C5ED8DA356BFC991A275A] UfxChipidea
C:\Windows\System32\DriverStore\FileRepository\ufxchipidea.inf_amd64_1c78775fffab6a0a\UfxChipidea.sys
14:27:24.0419 0x13a8 UfxChipidea - ok
14:27:24.0419 0x13a8 [3341A2F6FBBA73041952F12737814BC4, 4FE86EF74C56C0E730791B2A21B956789439326928041064EAEAA4B189E7917] ufxsynopsys
C:\Windows\System32\drivers\ufxsynopsys.sys
14:27:24.0434 0x13a8 ufxsynopsys - ok
14:27:24.0434 0x13a8 [DC9D40A4F86E2A16384FE7C1941037F2, 4B1BECDA7C202198BB33FE5B750C1DB5BA3B7D43554A4B557C342AC6E138A57F] uhssvc C:\Program Files\Microsoft
Update Health Tools\uhssvc.exe
14:27:24.0434 0x13a8 uhssvc - ok
14:27:24.0449 0x13a8 [E0E764F688DCACBA011BAEB2017B903F, 7802DCDA6F49494245EC9304AECED7BB2E90908BED25A4D47F1FF4615B03DED0] umbus
C:\Windows\System32\DriverStore\FileRepository\umbus.inf_amd64_b78a9c5b6fd62c27\umbus.sys
14:27:24.0449 0x13a8 umbus - ok
14:27:24.0449 0x13a8 [493AF687E60E144F59E3F5B7E27AA39B, 3062B25A7747BC417E1D498DB1B11C9631D80F57E4A048101EF5AA26206AE838] UmPass
C:\Windows\System32\drivers\umpass.sys
14:27:24.0449 0x13a8 UmPass - ok
14:27:24.0449 0x13a8 [D986BDDA3BADD0B4CDB4880CB2450358, 54710C3FE4E657772BD0DF7B94B183E3AFB2451386D53A0FC9ED79545E14C75A] UmRdpService
C:\Windows\System32\umrdp.dll
14:27:24.0449 0x13a8 UmRdpService - ok
14:27:24.0465 0x13a8 [FA02AFEFF7A4D8AB3447879EC2FB552E, 0B8910E81B7B36CB475EC14F6F90FCE1263CFB6454EC29CA7AC0FCF4C1E91749] UnistoreSvc
C:\Windows\System32\unistore.dll
14:27:24.0480 0x13a8 UnistoreSvc - ok
14:27:24.0496 0x13a8 [2B54990CF0127CE3B61609BAF1E077F9, BF040998C13E142CE1AB19419555031CB271C9533AA2CD090D14C416C14686DE] upnphost
C:\Windows\System32\upnphost.dll
14:27:24.0496 0x13a8 upnphost - ok
14:27:24.0496 0x13a8 [5C33B91675BE0C9693358C1AAA723D20, A5BB54ABBB0F7B13ACCA0997F567A81395688C6D68EB87F67F688737DC16918F] UrsChipidea
C:\Windows\System32\DriverStore\FileRepository\urschipidea.inf_amd64_78ad1c14e33df968\urschipidea.sys
14:27:24.0496 0x13a8 UrsChipidea - ok
14:27:24.0496 0x13a8 [ADFAB87405AE22290E24D0E8E6141AF1, BC0982BEFE4CABEA1E260C8A3266EA18A4CA158A07D1C5176890A04CC3B6A84A] UrsCx01000
C:\Windows\system32\drivers\urscx01000.sys
14:27:24.0496 0x13a8 UrsCx01000 - ok
14:27:24.0512 0x13a8 [BBDE7BF496327115DD744E7D4105C7BC, 5A8CC47603A1C9D58A30A5E897F1BCDC56199B08317B9FF319D469D6DD6CAAF0] UrsSynopsys
C:\Windows\System32\DriverStore\FileRepository\urssynopsys.inf_amd64_057fa37902020500\urssynopsys.sys
14:27:24.0512 0x13a8 UrsSynopsys - ok
14:27:24.0512 0x13a8 [90692B7994748A85D2C81018FB542F52, F1F88F57174F0B1298067C6B9BDD3A155AF0FE8335C895C134F7339338A57FEC] usbaudio
C:\Windows\system32\drivers\usbaudio.sys
14:27:24.0512 0x13a8 usbaudio - ok
14:27:24.0512 0x13a8 [FB9F25ACEBCBAEABFE30CACCB17D4EE6, 7D38FA294DA179E5535E3E481746F07E2AE47CE57192C2D1C5B780B583FD9C6D] usbaudio2
C:\Windows\System32\drivers\usbaudio2.sys
14:27:24.0512 0x13a8 usbaudio2 - ok

14:27:24.0528 0x13a8 [8B3961FDEAE656F7E87DA48C5947944C, C541ACE018B96161818020B65B0A37B1F1E29E7BFCF8893BA1B63510EAF318CE] usbccgp
C:\Windows\System32\drivers\usbccgp.sys
14:27:24.0528 0x13a8 usbccgp - ok
14:27:24.0528 0x13a8 [11561FC5BAA2DEB5AC8B179B591A882E, 2AD595BF4ABC146D8F533981848FF8271E983038566937BEB48A6A8F09BC60FB] usbcir
C:\Windows\System32\drivers\usbcir.sys
14:27:24.0528 0x13a8 usbcir - ok
14:27:24.0528 0x13a8 [7C2CE0F8E35DDAD7B1682A307EADDF22, 70A428AB29A1E6D47849513D74F659194F2AE942AA9EF7D2FF9F0141BA3AD3EA] usbehci
C:\Windows\System32\drivers\usbehci.sys
14:27:24.0528 0x13a8 usbehci - ok
14:27:24.0543 0x13a8 [0FC4BEA882686E7C70859625D723D2DB, 85C45DA0740ADA277B61EB6706BC6AF8525910A131BD2B4F619E8E8B3BB2BD3E] usbhub
C:\Windows\System32\drivers\usbhub.sys
14:27:24.0543 0x13a8 usbhub - ok
14:27:24.0559 0x13a8 [B355A648C79F254AF075E2F561056579, 203EA5F2A2F5B1894A485F5EFF2CE97ABA8B4F63EB7590D6BB781544C94F3403] USBHUB3
C:\Windows\System32\drivers\UsbHub3.sys
14:27:24.0559 0x13a8 USBHUB3 - ok
14:27:24.0559 0x13a8 [6F3E9F85EC160BE0009702158679F8D5, 81963EB5DE40AF981E3FFC224D5DE0EC0C591AF92ECAFE502A883F28D9AE13CD] usbohci
C:\Windows\System32\drivers\usbohci.sys
14:27:24.0559 0x13a8 usbohci - ok
14:27:24.0559 0x13a8 [0CFDC0F7C84F7A7CF71271B83B8ECD88, 283D34556F77078940B7EC349412BD8AA41BA9D19E586771355EE230A8BA6FDE] usbprint
C:\Windows\System32\drivers\usbprint.sys
14:27:24.0559 0x13a8 usbprint - ok
14:27:24.0574 0x13a8 [5A361D0A1D8025847AE8D8D066B0A563, 30B2E53692AB7F469E3E0483BA45635008CBC7E4D311F4E2CB12F2FC512C4F61] usbser
C:\Windows\System32\drivers\usbser.sys
14:27:24.0574 0x13a8 usbser - ok
14:27:24.0574 0x13a8 [64C7C056CD0900E5506CFF414445BA38, 2C2F3D501830B5752E6EE5B5E888CA8755D82F7C0178FB0FAAB1EEC28C1420A0] USBSTOR
C:\Windows\System32\drivers\USBSTOR.SYS
14:27:24.0574 0x13a8 USBSTOR - ok
14:27:24.0574 0x13a8 [E9118966B25633115636CB4C123013CE, 262D78329A69103F2FFB63E0D294CC20134579CBF2458F0250BB5E96E4AC1C84] usbuhci
C:\Windows\System32\drivers\usbuhci.sys
14:27:24.0574 0x13a8 usbuhci - ok
14:27:24.0590 0x13a8 [3F6C1AFDEB04C626A4E7A07CCA233EAE, 11285ECE5033883CC8C168F6B5E3A259AF1C447DCAC4205C7CEEF38CE3AE602B] USBXHCI
C:\Windows\System32\drivers\USBXHCI.SYS
14:27:24.0590 0x13a8 USBXHCI - ok
14:27:24.0605 0x13a8 [24AA81EE933EFED464AFA752D3B77AF3, 33A6564A2803C084F0EC228CB93FB546628C139787B1BA4C644F1854B8F606C9] UserDataSvc
C:\Windows\System32\userdataservice.dll
14:27:24.0621 0x13a8 UserDataSvc - ok
14:27:24.0637 0x13a8 [66E62E579DAB466C0BEB258EC2651108, FAF559F9EA8BBCC77B665BFD503C385683EE84F28772B245DCFDBEB6A97609E6] UserManager
C:\Windows\System32\usermgr.dll
14:27:24.0653 0x13a8 UserManager - ok
14:27:24.0668 0x13a8 [8521830A065C48292E8474FD98AC081C, 2D7CB863359071DACE0D48100520AD8AA5E0A9FEA6A5076244018D2EDBE43449] UsoSvc
C:\Windows\system32\usosvc.dll
14:27:24.0668 0x13a8 UsoSvc - ok
14:27:24.0668 0x13a8 [06275C2089FFBF992082891A626CCE13, 11B8411EF109BD48315FD02D6506DCD5587033BAD6CAB293CD395BB746FE973F] VacSvc   C:\Windows\System32\vac.dll
14:27:24.0684 0x13a8 VacSvc - ok
14:27:24.0684 0x13a8 [B4DE3D04AE3C71E67236B841BEADEB74, 8567CDBA80952B2B7AF647B9D2630FE12B73E87517498BCCDCC27EC1ED6E1545] VaultSvc
C:\Windows\system32\lsass.exe
14:27:24.0684 0x13a8 VaultSvc - ok
14:27:24.0684 0x13a8 [A91741981158 73F31CE569EF29F553B9, 1A6FD5EC9E4BF40296867C0E3BFB09E5843FE541BC2B9C27D5AFBCF4EC683761] VBoxGuest
C:\Windows\system32\DRIVERS\VBoxGuest.sys
14:27:24.0699 0x13a8 VBoxGuest - ok
14:27:24.0699 0x13a8 [BC67D23222C1EBA8BC65BE0DAF4683AB, 56744551C56637C3C6D57E5A8EED5C43823C9466D514719359CD2808C64D5969] VBoxMouse
C:\Windows\system32\DRIVERS\VBoxMouse.sys
14:27:24.0699 0x13a8 VBoxMouse - ok
14:27:24.0715 0x13a8 [3A0355E0EDF718ACE8DE8AE084655099, E1520A22AE1203A0AB8083FE2ECF42BA8A327EEA469CCC0E09CCF066D5C47615] VBoxService
C:\Windows\System32\VBoxService.exe
14:27:24.0715 0x13a8 VBoxService - ok
14:27:24.0731 0x13a8 [BCC04D8DB36BBAF6BE11ECF8438E5A82, C337F9ACD1844B9929929810C890BDC7EAACB8C6D659EC51C1E588299B6CE7AD] VBoxSF
C:\Windows\System32\drivers\VBoxSF.sys
14:27:24.0731 0x13a8 VBoxSF - ok
14:27:24.0731 0x13a8 [A637CEADAF21CAC624E9BC7F5FAB5A65, F04FE7C6136511876B9181EFF9ECFF2386089B60BD7C911E8642505EFDA83918] VBoxWddm
C:\Windows\System32\drivers\VBoxWddm.sys
14:27:24.0746 0x13a8 VBoxWddm - ok
14:27:24.0746 0x13a8 [661233B58190B487682839F1559A7962, 2BE132106C26A9073B6E9CB646E6A2C003558B8924ED0BDC3A0533FC98E03BF4] vdrvroot
C:\Windows\system32\drivers\vdrvroot.sys
14:27:24.0746 0x13a8 vdrvroot - ok
14:27:24.0746 0x13a8 [14EC80399610295EE3F6FDDF82DDD5F9, 033F069224F65753E9EC006DBB6961824389911B7B0D679F85B2E33D4B6479DD] vds   C:\Windows\System32\vds.exe
14:27:24.0762 0x13a8 vds - ok
14:27:24.0762 0x13a8 [46684A95E908F0A6A2355AA46A3B2A77, A25DFDA0572EF014905619DF21427518EA5C01CFB13B9927ADA305B29DBBFEFE] VerifierExt
C:\Windows\system32\drivers\VerifierExt.sys
14:27:24.0777 0x13a8 VerifierExt - ok
14:27:24.0777 0x13a8 [90C461B1A0C4B06C9C8DB684FB46C6BA, AA8E04AE64E47151E390488CDADA0C6E23DF0D36099743612EC82FA4E39FFA0C] vhdmp
C:\Windows\System32\drivers\vhdmp.sys
14:27:24.0793 0x13a8 vhdmp - ok
14:27:24.0793 0x13a8 [7F2F04A354582D3D34F5B2B4EFF07189, 98188182D328414832D06E957601A997AD2B2B0F088B089181EDE8FAB0AF733C] vhf
C:\Windows\System32\drivers\vhf.sys
14:27:24.0793 0x13a8 vhf - ok
14:27:24.0809 0x13a8 [EF06FE7572AAEBF458C5B35FE71667FC, 0387D04478F267642AF7C38878861A2A3E6C04AD1A5467DE6160577349CB3D13] Vid
C:\Windows\System32\drivers\Vid.sys
14:27:24.0809 0x13a8 Vid - ok
14:27:24.0809 0x13a8 [B37F0BF662BB504F0A9C247F24C281AD, 6281D573D9AD9AA204778C3823737726E882B17657B23CF5458C012FF7990E52] VirtualRender
C:\Windows\System32\DriverStore\FileRepository\vrd.inf_amd64_81fbd405ff2470fc\vrd.sys
14:27:24.0809 0x13a8 VirtualRender - ok
14:27:24.0809 0x13a8 [9C99B98210A4562DD98D81C219D00F29, 2CE76C8E69912AFCDF302665904B59232E242F2FEF0253FC872226CF2F432489] vmbus
C:\Windows\system32\drivers\vmbus.sys
14:27:24.0809 0x13a8 vmbus - ok
14:27:24.0824 0x13a8 [C29F63BB3B99B3F2030113160A741684, 43DF7A6DD305D1696D28A54E12B75AE041B075E789DB5D0C8DDF250E75585AA1] VMBusHID
C:\Windows\System32\drivers\VMBusHID.sys
14:27:24.0824 0x13a8 VMBusHID - ok
14:27:24.0824 0x13a8 [E5BB075B6B5A1DA3C3F48CA5DFF54E77, E13E8F9523F51F976084561C9D0A843CAF550FA233521FF13FFE1C5634CA6472] vmgid
C:\Windows\System32\drivers\vmgid.sys
14:27:24.0824 0x13a8 vmgid - ok
14:27:24.0824 0x13a8 [6ADE603113ED6E38192EC0FECA9B6015, E01415741007D86927849516A0E853F210935C57A0144FB9B19E5D407401CB22] vmicguestinterface
C:\Windows\System32\icsvc.dll
14:27:24.0824 0x13a8 vmicguestinterface - ok
14:27:24.0840 0x13a8 [6ADE603113ED6E38192EC0FECA9B6015, E01415741007D86927849516A0E853F210935C57A0144FB9B19E5D407401CB22] vmicheartbeat
C:\Windows\System32\icsvc.dll
14:27:24.0840 0x13a8 vmicheartbeat - ok
14:27:24.0840 0x13a8 [6ADE603113ED6E38192EC0FECA9B6015, E01415741007D86927849516A0E853F210935C57A0144FB9B19E5D407401CB22] vmickvpexchange
C:\Windows\System32\icsvc.dll
14:27:24.0840 0x13a8 vmickvpexchange - ok
14:27:24.0856 0x13a8 [2D46BF6B72540A881F80C5DFCCDE64DE, 112E0BF9B61FEC83978DC7FBC269B83A81520A4BFD944EE0C19878B922BF3006] vmicrdv
C:\Windows\System32\icsvcext.dll
14:27:24.0856 0x13a8 vmicrdv - ok
14:27:24.0856 0x13a8 [6ADE603113ED6E38192EC0FECA9B6015, E01415741007D86927849516A0E853F210935C57A0144FB9B19E5D407401CB22] vmicshutdown
C:\Windows\System32\icsvc.dll
14:27:24.0856 0x13a8 vmicshutdown - ok
14:27:24.0872 0x13a8 [6ADE603113ED6E38192EC0FECA9B6015, E01415741007D86927849516A0E853F210935C57A0144FB9B19E5D407401CB22] vmictimesync
C:\Windows\System32\icsvc.dll
14:27:24.0872 0x13a8 vmictimesync - ok
14:27:24.0872 0x13a8 [6ADE603113ED6E38192EC0FECA9B6015, E01415741007D86927849516A0E853F210935C57A0144FB9B19E5D407401CB22] vmicvmsession
C:\Windows\System32\icsvc.dll
14:27:24.0872 0x13a8 vmicvmsession - ok
14:27:24.0887 0x13a8 [2D46BF6B72540A881F80C5DFCCDE64DE, 112E0BF9B61FEC83978DC7FBC269B83A81520A4BFD944EE0C19878B922BF3006] vmicvss
C:\Windows\System32\icsvcext.dll

14:27:24.0887 0x13a8 vmicvss - ok
14:27:24.0887 0x13a8 [07CD0208217041A3BBF176AA9667B1F9, B4D4C39D68901BE0E9F3D0AA8E28663B02999AEEDBCC343279BFF0C5BE236510] volmgr
C:\Windows\system32\drivers\volmgr.sys
14:27:24.0887 0x13a8 volmgr - ok
14:27:24.0887 0x13a8 [796F1C83861C02A97571D0EDAB490B70, 71CE8D930AE82C2B2628CBF3BB3AE1A8CF039BD702BDE912D499FCF45332F5A6] volmgrx
C:\Windows\system32\drivers\volmgrx.sys
14:27:24.0902 0x13a8 volmgrx - ok
14:27:24.0902 0x13a8 [0CB8B8D76F858E23339F1EA16B820F19, 3927E0DFA3235C746F42F075A6FF426052197CACE77800EE16FA63C20FE4CCD1] volsnap
C:\Windows\system32\drivers\volsnap.sys
14:27:24.0902 0x13a8 volsnap - ok
14:27:24.0919 0x13a8 [770E710BEA3CCC595EE3703297B40D76, C03E3367B92307993BC169583CB298265FC1C35CF5973EC352C1E08FFCFD1928] volume
C:\Windows\system32\drivers\volume.sys
14:27:24.0919 0x13a8 volume - ok
14:27:24.0919 0x13a8 [94ECF74167F4B837FFB99A135E8FBB7C, 7E901722F7D0D279F36A6A34A901A8CF1FB864F2A6543F8217A39E8895B9DB17] vpci
C:\Windows\system32\drivers\vpci.sys
14:27:24.0919 0x13a8 vpci - ok
14:27:24.0919 0x13a8 [1A4D9FAED669BC42E5A1CD8442729AB2, E70778AF6B0C9709CB8CEF655C6DD8B5A61CC70BFD35A43304C1308EA478C550] vsmraid
C:\Windows\system32\drivers\vsmraid.sys
14:27:24.0919 0x13a8 vsmraid - ok
14:27:24.0934 0x13a8 [D2621CE831403E4E00F4A9E721416ACE, FEF32BF8C8094CD680F11E95A21F675DFBA54FA504692A18A8FD060EBBDEB0DD] VSS
C:\Windows\system32\vssvc.exe
14:27:24.0950 0x13a8 VSS - ok
14:27:24.0965 0x13a8 [6E0092973E35BE6A1F5ED5CBDD202036, 33DAF53C81D5BAF9337192A84DF50C108BAE9B8A858081E2208939CCFF2622F8] VSTXRAID
C:\Windows\system32\drivers\vstxraid.sys
14:27:24.0965 0x13a8 VSTXRAID - ok
14:27:24.0965 0x13a8 [7BC30ADCCC9BCF2B0A29A320A395EC3B, 373C85F659F07366649697823B4A8B14313F0042A7A04E932429D049D18C7646] vwifibus
C:\Windows\System32\drivers\vwifibus.sys
14:27:24.0965 0x13a8 vwifibus - ok
14:27:24.0965 0x13a8 [8A2CE127139A81B797BFCCC0E82D2EC5, 402BFC58F99C7F375D9C4C10008C4FB03F8909B4DBB5BEF390F19A9635BB18CE] vwififlt
C:\Windows\system32\drivers\vwififlt.sys
14:27:24.0965 0x13a8 vwififlt - ok
14:27:24.0981 0x13a8 [EA38357524EE188D7494893A8548B74D, 6D0C5A652A839C53E98749C4B7EA4ACEBE01C9E8CC568E05B4A931AB7AA9FAD1] W32Time
C:\Windows\system32\w32time.dll
14:27:24.0981 0x13a8 W32Time - ok
14:27:24.0996 0x13a8 [4EA5DD0117FFCDA0DEBA2172CB063B8B, 166A0DCE27B22274B33CA8C78D0E070858EC0667943082945A7D8DA07EE20E49] WaaSMedicSvc
C:\Windows\System32\WaaSMedicSvc.dll
14:27:24.0996 0x13a8 WaaSMedicSvc - ok
14:27:24.0996 0x13a8 [1F16C8283230EF1F1C4E135D1C2C859B, E4F672C7E58490F82F859CAEEDD57D8ABCC31DE62A42A956BEE47113D365BE35] WacomPen
C:\Windows\System32\drivers\wacompen.sys
14:27:24.0996 0x13a8 WacomPen - ok
14:27:25.0012 0x13a8 [A1B1122D66CECE3D95E73E5FF02BFBDB, B347A6C1B50088557BDE3D60F70F5F0326387F3FD169421B016143F27DC1FAD8] WalletService
C:\Windows\system32\WalletService.dll
14:27:25.0012 0x13a8 WalletService - ok
14:27:25.0012 0x13a8 [619FD75FE36AC056352F168A1833DD6B, 6D2A46F13ACD500B5BA377B66326990128A73D23C7EA4AF538EB2507287D355A] wanarp
C:\Windows\system32\DRIVERS\wanarp.sys
14:27:25.0012 0x13a8 wanarp - ok
14:27:25.0012 0x13a8 [619FD75FE36AC056352F168A1833DD6B, 6D2A46F13ACD500B5BA377B66326990128A73D23C7EA4AF538EB2507287D355A] wanarpv6
C:\Windows\system32\DRIVERS\wanarp.sys
14:27:25.0012 0x13a8 wanarpv6 - ok
14:27:25.0012 0x13a8 [8449398F11D49864117105679B539816, 8FD3B9C72066D6A983D062DE72EEF9769339EACBF4E0D303B9E12343C9D5DE6C] WarpJITSvc
C:\Windows\System32\Windows.WARP.JITService.dll
14:27:25.0028 0x13a8 WarpJITSvc - ok
14:27:25.0043 0x13a8 [EED1A99613EF7E62EB2742553469901D, 0904BD67CFBF11BC08CB283D1646676A16A388CC0E0A2184472C751EF6539485] wbengine
C:\Windows\system32\wbengine.exe
14:27:25.0058 0x13a8 wbengine - ok
14:27:25.0058 0x13a8 [503C023023A3D43781CBEC7F62504901, 1F224685D26DAF36BD9403D37E1993EEE45315B958B50D652B70D6708134EBAF] WbioSrvc
C:\Windows\System32\wbiosrvc.dll
14:27:25.0074 0x13a8 WbioSrvc - ok
14:27:25.0074 0x13a8 [3EF2A983E2AA64F9288B325D94FD404D, C6D712709A7AAFAC6765CED965690C1DE59F5192DF34D8119F78E9EC60AF6FC2] wcifs
C:\Windows\system32\drivers\wcifs.sys
14:27:25.0074 0x13a8 wcifs - ok
14:27:25.0090 0x13a8 [04A9A5C44DC5064533BC386DED490E49, 3BA6B959DB689142C85706B988FC08A1516BBC480CC4C41B1279F3048E61B84B] Wcmsvc
C:\Windows\System32\wcmsvc.dll
14:27:25.0106 0x13a8 Wcmsvc - ok
14:27:25.0106 0x13a8 [67F75D52843E8B585B57F7A620A7AF00, F89B752C9C6199026D26390DB1BC8F2CFB7D656AB2DD1697F764B442B21B96F5] wcncsvc
C:\Windows\System32\wcncsvc.dll
14:27:25.0121 0x13a8 wcncsvc - ok
14:27:25.0121 0x13a8 [72140DB17B445DE60E6EAEC4C3634535, 46016919A7A42CE274B410808EBD3E90DFCAB8215F5E6ADEA62E250D5FD316C1] wcnfs
C:\Windows\system32\drivers\wcnfs.sys
14:27:25.0121 0x13a8 wcnfs - ok
14:27:25.0121 0x13a8 WdBoot - ok
14:27:25.0137 0x13a8 [D52DDDD034B11F48B3CDFB0313381417, 8110E24D2CFCB29A74715D8C27A72B0BAF5293E3280E5C90EF905BA105745A31] Wdf01000
C:\Windows\system32\drivers\Wdf01000.sys
14:27:25.0137 0x13a8 Wdf01000 - ok
14:27:25.0137 0x13a8 WdFilter - ok
14:27:25.0137 0x13a8 [BB37AF6E45E0F69222E057A74B4AFE1E, 4662064205BEC0DB7B10F1412E0A09A6E5E3B16DE443AEF7F79ACA3ACE24A51D] WdiServiceHost
C:\Windows\system32\wdi.dll
14:27:25.0152 0x13a8 WdiServiceHost - ok
14:27:25.0152 0x13a8 [BB37AF6E45E0F69222E057A74B4AFE1E, 4662064205BEC0DB7B10F1412E0A09A6E5E3B16DE443AEF7F79ACA3ACE24A51D] WdiSystemHost
C:\Windows\system32\wdi.dll
14:27:25.0152 0x13a8 WdiSystemHost - ok
14:27:25.0168 0x13a8 [E1496DE5778D3B97F632E42B7DE503B3, D227F604C76DD932962B1FA454C10A9499883CCFB71AD22ACD0D65396E2101B4] wdiwifi
C:\Windows\system32\DRIVERS\wdiwifi.sys
14:27:25.0168 0x13a8 wdiwifi - ok
14:27:25.0168 0x13a8 [A6C92A5F2982EBB8788E0690C19048C4, 85C54A99DD43DC1FAC7FD2A31288CEC7501F795DE8FA86857790F4CCD5AF7C18] WdmCompanionFilter
C:\Windows\system32\drivers\WdmCompanionFilter.sys
14:27:25.0168 0x13a8 WdmCompanionFilter - ok
14:27:25.0185 0x13a8 WdNisDrv - ok
14:27:25.0185 0x13a8 WdNisSvc - ok
14:27:25.0185 0x13a8 [16A87010C08B70315523A393A4A55A3E, 8C6414E0EE518B2FFB4859E178C168BBE2CC5DCA11D23B1A6B9D9DF636C51DD7] WebClient
C:\Windows\System32\webclnt.dll
14:27:25.0185 0x13a8 WebClient - ok
14:27:25.0231 0x13a8 [8875798C97BBAEAB26FC5785F9F87FD3, BC1335C94CF36AE621144B096EE9B4ED1787ECB0FD0CC0E8939AFE13266D3B4B] Wecsvc
C:\Windows\system32\wecsvc.dll
14:27:25.0246 0x13a8 Wecsvc - ok
14:27:25.0246 0x13a8 [CBA85827716DE89106F8E4AD7430620C, EF2FEAD68FE003DAC52BC2098962F397DF80B7DCD79A8F45012A050C7C0E2DB1] WEPHOSTSVC
C:\Windows\system32\wephostsvc.dll
14:27:25.0246 0x13a8 WEPHOSTSVC - ok
14:27:25.0246 0x13a8 [3998B8FA3D5B2EC29CF75BAF97CCEF80, AA61BADC0BD3ED41AE343F26216BEDDF66148F2C6FE2EDC837725CA3E01B9A52] wercplsupport
C:\Windows\System32\wercplsupport.dll
14:27:25.0246 0x13a8 wercplsupport - ok
14:27:25.0262 0x13a8 [AEE1F99DB06B3A325673DA3A72443FD0, 6808CE26F95048BF1EC064FBBDECB0ADD7576C906FB39F04E9A4A334E2C88A8D] WerSvc
C:\Windows\System32\WerSvc.dll
14:27:25.0262 0x13a8 WerSvc - ok
14:27:25.0262 0x13a8 [3A6954FC9A9A01F56B64D8DF7CF11005, 0100B3F2D4EC4D7F6E7F092D817AE4B970C06F6B5B625B543FE2B57870A0DE20] WFDSConMgrSvc
C:\Windows\System32\wfdsconmgrsvc.dll
14:27:25.0277 0x13a8 WFDSConMgrSvc - ok
14:27:25.0277 0x13a8 [6D7A8D1ACA3742EBAF98439D68A8DD5E, 14D3415A78C9E5DFDEAF2F624FA19E2FE80D64D4B91F8BDFC10B785CE27949CC] WFPLWFS
C:\Windows\system32\drivers\wfplwfs.sys
14:27:25.0277 0x13a8 WFPLWFS - ok
14:27:25.0277 0x13a8 [6F0F2D9D9BF7604CD94CE5B7B0A4814F, FDAAEBCEA9F87D56283D2B96088FA77CF31D0EE1B686350CFF406492AB4CF0FD] WiaRpc
C:\Windows\System32\wiarpc.dll
14:27:25.0293 0x13a8 WiaRpc - ok

14:27:25.0293 0x13a8 [B50E80B21F08D8C530AFBB537B436BAB, F61B63E6F2881BC57B0978AC99B58CB9F0875F30D1ABE6DD1E17E6B310F358E9] WIMMount
C:\Windows\system32\drivers\wimmount.sys
14:27:25.0293 0x13a8 WIMMount - ok
14:27:25.0340 0x13a8 WinDefend - ok
14:27:25.0340 0x13a8 [B434A84F46C70F4E67B70ED70F024B7F, 64EEB8093BA2590E83D83C5AF7C2A025B88AF5681143BCA83671104266FEEA99] WindowsTrustedRT
C:\Windows\system32\drivers\WindowsTrustedRT.sys
14:27:25.0340 0x13a8 WindowsTrustedRT - ok
14:27:25.0340 0x13a8 [982774B74EE1419D641CEB66E394A4BA, 090C4CE6B76B3904B5AE73E4F1EEBCE619194C358874D7584537012F954C54BE] WindowsTrustedRTProxy
C:\Windows\system32\drivers\WindowsTrustedRTProxy.sys
14:27:25.0340 0x13a8 WindowsTrustedRTProxy - ok
14:27:25.0356 0x13a8 [6CBF6006F616B4745DB1863B8F80B4C0, D00EC0B07CB280464D8455347609CBD91B2757F437157544D87BEB2B854C3BD2] WinHttpAutoProxySvc
C:\Windows\system32\winhttp.dll
14:27:25.0371 0x13a8 WinHttpAutoProxySvc - ok
14:27:25.0371 0x13a8 [0816C30E3395E667EFFFB92B4EA66A05, F6A9E7026AA60A6627680F232AE785EA9CF55FE970708E6E49151F601CC42FEE] WinMad
C:\Windows\System32\drivers\winmad.sys
14:27:25.0371 0x13a8 WinMad - ok
14:27:25.0371 0x13a8 [340E0C67A9C7F4A13E4B731A9AC9D142, 7097C578B53D1402D9B93FB05364E333A59E76530DACC86AAF03A92126BC529A] Winmgmt
C:\Windows\system32\wbem\WMIsvc.dll
14:27:25.0387 0x13a8 Winmgmt - ok
14:27:25.0387 0x13a8 [D813A670D81D75E1145A3B3C41A51F02, DC378FC65690EE7E81A51481DFD3011AC13486D956408279F3DE1DD11ED0A245] WinNat
C:\Windows\system32\drivers\winnat.sys
14:27:25.0387 0x13a8 WinNat - ok
14:27:25.0418 0x13a8 [0660BA96E067499FA0A16CCCDF0E5BC7, 0C5466160357DE325E242FF28830044AC67323E62080E9272F1DAAC0E2134453] WinRM
C:\Windows\system32\WsmSvc.dll
14:27:25.0450 0x13a8 WinRM - ok
14:27:25.0450 0x13a8 [91D3DC62C6EDDB6554CE14C0E0B4290F, 6F8F89B350FC6BC0D23A50C593F02514854AB7D6CD234D8C8AD4B5DDDD586BA0] WINUSB
C:\Windows\System32\drivers\WinUSB.SYS
14:27:25.0450 0x13a8 WINUSB - ok
14:27:25.0450 0x13a8 [F4C4FD42F8DD657157823DB617CC3A3D, D2A5ED039ED83010E0BB4BB1A69F9D142D42BE2C75E56CFCF3F157A735CB688E] WinVerbs
C:\Windows\System32\drivers\winverbs.sys
14:27:25.0450 0x13a8 WinVerbs - ok
14:27:25.0465 0x13a8 [85CC170D0432B45697C4BACD11958802, 728F0483F388E347CE009C21354DA306221F932B4089BC5D8C20851C0712B39F] wisvc
C:\Windows\system32\flightsettings.dll
14:27:25.0480 0x13a8 wisvc - ok
14:27:25.0496 0x13a8 [90F0D507A20105409E76F6877812C2D7, 9491B675525F47B3C32F5E3AC4654E125D1BBD63C05A0B0EDD236F8E5BDE0CD4] WlanSvc
C:\Windows\System32\wlansvc.dll
14:27:25.0528 0x13a8 WlanSvc - ok
14:27:25.0543 0x13a8 [D5A5C966DDE23DAB79C1F4DFE5FC9C96, 48BD8CBAE0A852C6097D6A567B08BBCA062E730FB1024658AD94DE085513FB25] wlidsvc
C:\Windows\system32\wlidsvc.dll
14:27:25.0575 0x13a8 wlidsvc - ok
14:27:25.0606 0x13a8 [F32810E93D8B73D6B9C1B0D5111FEA4B, 8AB714FE052270125B27BF32CE620EFE7B46D930A4AF00317B74A7153FDA0BCF] wlpasvc
C:\Windows\System32\lpasvc.dll
14:27:25.0621 0x13a8 wlpasvc - ok
14:27:25.0637 0x13a8 [0050CCCF22E55499B638058D65AAE2EE, 8BF4F834AACCFBDE6341A10434A6676072DF58FF1557FE21D7E5735FE8ACAA0C] WManSvc
C:\Windows\system32\Windows.Management.Service.dll
14:27:25.0637 0x13a8 WManSvc - ok
14:27:25.0637 0x13a8 [E4F25E6E790747073A09F9F8C997889C, 98455DD24AE076A2413EA599F83E0894F608C335F3FF2F3624A17E8EAF3B3C42] WmiAcpi
C:\Windows\System32\drivers\wmiacpi.sys
14:27:25.0637 0x13a8 WmiAcpi - ok
14:27:25.0652 0x13a8 [FD9A490AF8BAD2193AA2BE680665BB33, ED8A0B7F9995567A76AF23F1685301A8B692E4DF699522C1C79EBEBFC912AFF3] wmiApSrv
C:\Windows\system32\wbem\WmiApSrv.exe
14:27:25.0652 0x13a8 wmiApSrv - ok
14:27:25.0699 0x13a8 WMPNetworkSvc - ok
14:27:25.0699 0x13a8 [36407D449333DBF64DE6939BD0991BEC, 1901652C578590023F3F0E2336B3D0CD863A3354B78DBD8A6D68E0CA7D512AF8] Wof
C:\Windows\system32\drivers\Wof.sys
14:27:25.0699 0x13a8 Wof - ok
14:27:25.0731 0x13a8 [0B78B5F4021127C9A2C479E9240D0724, 5A3D13080059F9F426CC744AFBA41E352F6FD4E024A7559F2DD4D80F425B6789] workfolderssvc
C:\Windows\system32\workfolderssvc.dll
14:27:25.0746 0x13a8 workfolderssvc - ok
14:27:25.0778 0x13a8 [EBD341786686DA18ED9F5B8529B5278E, 31892DF9293701D48A353568562E78327960A3538D40691DEAE105AB95A3B9F1] WpcMonSvc
C:\Windows\System32\WpcDesktopMonSvc.dll
14:27:25.0794 0x13a8 WpcMonSvc - ok
14:27:25.0824 0x13a8 [D5613AD516CEC2BDD5BF057036CA4331, 9D2A59564544914F9DE896407375D8EE6E3828A17E8D42FA35B576A4F4BD43DD] WPDBusEnum
C:\Windows\system32\wpdbusenum.dll
14:27:25.0824 0x13a8 WPDBusEnum - ok
14:27:25.0824 0x13a8 [024924C9E79F51560B9133EEAB866BBF, F4D464BC02C7B96EF72AA9229A99A1AD32F56390F97972C33525EF0D85304261] WpdUpFltr
C:\Windows\system32\drivers\WpdUpFltr.sys
14:27:25.0824 0x13a8 WpdUpFltr - ok
14:27:25.0840 0x13a8 [B8C8527ACD90CF1488D89925B535DB54, 3DA7A75B6C0E8318DD52A41C89FF82AFA1D688A1B640B34DD169BDECEF2183B3] WpnService
C:\Windows\system32\WpnService.dll
14:27:25.0840 0x13a8 WpnService - ok
14:27:25.0840 0x13a8 [31778E964AFE30D5997B2242A56CBFD3, 6ADF456D41C899B86842B60CB226D98020D311AE26D2F805280C2957CE2B6497] WpnUserService
C:\Windows\System32\WpnUserService.dll
14:27:25.0840 0x13a8 WpnUserService - ok
14:27:25.0840 0x13a8 [2B98DFC181823C8D8AA39C4CC577DE3E, DAFF7CE8868299AF5EFA844C2E1F84B7EE7E498B1AFF16965CE41C2E75B2F4E4] ws2ifsl
C:\Windows\system32\drivers\ws2ifsl.sys
14:27:25.0840 0x13a8 ws2ifsl - ok
14:27:25.0855 0x13a8 [E3903AD613F970DD57326A714B84123D, F0BC75C7F40D57E4CDED86AF5A4EED6CD253FB7257FD30BA71D62402DDDF68F9] wscsvc
C:\Windows\System32\wscsvc.dll
14:27:25.0855 0x13a8 wscsvc - ok
14:27:25.0855 0x13a8 WSearch - ok
14:27:25.0887 0x13a8 [C8DC00685F50001CF67A32A97A997C9A, 820914BBB4C3736C5D8FEA2FB44DDA87708EDAD5BCAED02F63DA095CAC5FE46E] wuauserv
C:\Windows\system32\wuaueng.dll
14:27:25.0918 0x13a8 wuauserv - ok
14:27:25.0933 0x13a8 [AD4E4FFF4754A8320CBC3976BED0960A, B733E6B1BBC6D7E862F2C53D6CFB45A0D8625B4CA32D6D17D3010FAC5E90B4CC] WudfPf
C:\Windows\system32\drivers\WudfPf.sys
14:27:25.0933 0x13a8 WudfPf - ok
14:27:25.0933 0x13a8 [B670768AB4859D3B97EA9FCDD7CA2E7F, 346B0550D8927D5ED777096E03DAFA6EA96F50556F65E9252DE94ACA15C28657] WUDFRd
C:\Windows\System32\drivers\WUDFRd.sys
14:27:25.0933 0x13a8 WUDFRd - ok
14:27:25.0949 0x13a8 [5EE1C6B162FC7D57816A8AACF9564D0B, 3342A7DDA9127F899945FCA78A0D070A8D3E868C76599F400F32349269E06EB5] WwanSvc
C:\Windows\System32\wwansvc.dll
14:27:25.0965 0x13a8 WwanSvc - ok
14:27:25.0981 0x13a8 [AF736AF74B1C59C459D0A4FFB1E3906E, 104FE6AB7BD113CE39E382EF75DBAF7737B16649D90C3C27329951D1C4C1E10F] XblAuthManager
C:\Windows\System32\XblAuthManager.dll
14:27:25.0996 0x13a8 XblAuthManager - ok
14:27:26.0043 0x13a8 [6FF45F14C377307A291CF6F30AFBDD62, 26213B5D107DA99E0E1C8254FCEEA35DCE819632E5CE4C6D06DE601E7B0153D3] XblGameSave
C:\Windows\System32\XblGameSave.dll
14:27:26.0059 0x13a8 XblGameSave - ok
14:27:26.0059 0x13a8 [0211FCAC8F3F73D6B6AD08B7DEAA4333, E1F172C42FB08EE5E5A4F60CD7CC65A3E6F73CC199B4086024386467737A311C] xboxgip
C:\Windows\System32\drivers\xboxgip.sys
14:27:26.0074 0x13a8 xboxgip - ok
14:27:26.0074 0x13a8 [07FF7BC9D6419AAD15123B52F6D3AD41, 974F3FA563A97427F966F216D3C704EE5958B90FCB0FBF1082E3379972F4D36E] XboxGipSvc
C:\Windows\System32\XboxGipSvc.dll
14:27:26.0074 0x13a8 XboxGipSvc - ok
14:27:26.0090 0x13a8 [1ACBD3F4A891E19D365FA11528A27621, 320E1FFA692AA0BBDD35F500994F443B74C7CD6C58A400BB1ECA04FA85BC6021] XboxNetApiSvc
C:\Windows\system32\XboxNetApiSvc.dll
14:27:26.0106 0x13a8 XboxNetApiSvc - ok
14:27:26.0137 0x13a8 [1BDE4DFE545AB7A315EA2BCDFECACC13, 1F33E8881CA34076CE599E9B707F33C6C1874312D1A08411EF3EEFA8A7FA134F] xinputhid
C:\Windows\System32\drivers\xinputhid.sys
14:27:26.0137 0x13a8 xinputhid - ok
14:27:26.0137 0x13a8 ================ Scan global ===============================
14:27:26.0152 0x13a8 [019FC80D9AFCDE0E3CC39C8B3BC908B1, BA2202CC20A6BEB37544000DBB6B592322B0A7CCCAC42B1B5416A6DEA1B9465D] C:\Windows\system32\basesrv.dll
14:27:26.0152 0x13a8 [19979E1729CFA0E56EB4CCCB198DFD05, 7F2A683F28877562409D810946DDCA2F069715CDFB249602251DFA50065FFF7A] C:\Windows\system32\winsrv.dll

```
14:27:26.0152 0x13a8  [ E7CA6090092F0DF1639E87268FBD8419, 2F0A00B5FAD1ED02BF01911A412CE391AEAAF00F2ECA4AE0C12A7620F403BE23 ] C:\Windows\system32\sxssrv.dll
14:27:26.0169 0x13a8  [ F26F9B26E933078756832B864EB627B7, F016360C75E8250AF691929082BA2066078FBA4E84EAC3D496E4EDA9A0B6EC62 ] C:\Windows\system32\services.exe
14:27:26.0169 0x13a8  [ Global ] - ok
14:27:26.0169 0x13a8  ================ Scan MBR ==================================
14:27:26.0169 0x13a8  [ A36C5E4F47E84449FF07ED3517B43A31 ] \Device\Harddisk0\DR0
14:27:26.0262 0x13a8  \Device\Harddisk0\DR0 - ok
14:27:26.0262 0x13a8  ================ Scan VBR ==================================
14:27:26.0262 0x13a8  [ 8C050AB6978DBBF6C678C9EDA72E914D ] \Device\Harddisk0\DR0\Partition1
14:27:26.0262 0x13a8  \Device\Harddisk0\DR0\Partition1 - ok
14:27:26.0262 0x13a8  ================ Scan active images ========================
14:27:26.0262 0x13a8  ================ Scan generic autorun ======================
14:27:26.0278 0x13a8  [ 783C99AFD4C2AE6950FA5694389D2CFA, 570B37A7A3FFDAFCCECCC33CBC1968FEB857B73CA3CB4DFFEDC2E67E9ABD0878 ]
C:\Windows\system32\SecurityHealthSystray.exe
14:27:26.0278 0x13a8  SecurityHealth - ok
14:27:26.0278 0x13a8  [ 1F4F474A7E4E45C5C0498F089E63BB11, 23397D279C959054CF79BD16EBCD3EBD87D3C2473DE9DEDE0C289ED332A64707 ] C:\Windows\system32\VBoxTray.exe
14:27:26.0294 0x13a8  VBoxTray - ok
14:27:26.0309 0x13a8  OneDriveSetup - ok
14:27:26.0309 0x13a8  OneDriveSetup - ok
14:27:26.0309 0x13a8  OneDrive - ok
14:27:26.0325 0x13a8  [ 3FA9AE698A600FF3422995504CD088C4, A8E1533F87AC5273F908FBB67EDB786F231FCAE44B49DD5E6CEB3C777C1F01A9 ]
C:\Users\vboxuser\AppData\Local\Microsoft\EdgeUpdate\1.3.181.5\MicrosoftEdgeUpdateCore.exe
14:27:26.0325 0x13a8  Microsoft Edge Update - ok
14:27:26.0356 0x13a8  [ D5174A0327DD4AD65F24959049C7113D, 68455B27EDDB80B63612778347 8F0014AEB80ABE98D788C37F18B342AE15BE27 ] C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
14:27:26.0387 0x13a8  MicrosoftEdgeAutoLaunch_181C8C6F62941D485E9DA88A14DF8CD2 - ok
14:27:26.0387 0x13a8  Waiting for KSN requests completion. In queue: 267
14:27:27.0434 0x13a8  AV detected via SS2: Windows Defender, windowsdefender:// (  ), 0x61100 ( enabled : updated )
14:27:27.0434 0x13a8  Win FW state via NFP2: enabled ( trusted )
14:27:27.0497 0x13a8  ============================================================
14:27:27.0497 0x13a8  Scan finished
14:27:27.0497 0x13a8  ============================================================
14:27:28.0027 0x1030  Deinitialize success
2023-11-07 14:27:28,04    Done.
2023-11-07 14:27:28,04    Launch job 'Purge oldest Shadow Copy set (Win7 and up)'...
2023-11-07 14:27:30,69    Done.
2023-11-07 14:27:30,69    Reducing max allowed System Restore space to 7% of disk...
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
2023-11-07 14:27:30,71    Done.
2023-11-07 14:27:30,71    stage_0_prep complete.
2023-11-07 14:27:30,71    stage_1_tempclean begin...
2023-11-07 14:27:30,73    Launch job 'Clear CryptNet SSL certificate cache'...
https://oneclient.sfx.ms/Win/Prod/4879ac1d41b6a4bd24625a6d319fcf11a409fa00.xml?OneDriveUpdate=b9f7fc77d339862bab6c54c3cb2a
https://oneclient.sfx.ms/Win/Prod/4879ac1d41b6a4bd24625a6d319fcf11a409fa00.xml?OneDriveUpdate=c266690a439882b51ca8f31dc8
https://oneclient.sfx.ms/Win/Prod/4879ac1d41b6a4bd24625a6d319fcf11a409fa00.xml?OneDriveUpdate=50eeed2aa6cc8bbea6c8992870d5
https://download5.operacdn.com/ftp/pub/opera/desktop/104.0.4944.36/win/Opera_104.0.4944.36_Autoupdate_x64.exe
https://download5.operacdn.com/ftp/pub/.assistant/103.0.4928.25/Assistant_103.0.4928.25_Setup.exe
https://features.opera-api2.com/api/v2/features?country=CZ&language=cs&uuid=7967623a-9d2b-4072-b94a-e9b38e6ff7d2&product=&channel=Stable&version=104.0.4944.36
https://features.opera-api2.com/api/v2/features?country=CZ&language=cs&uuid=2ffa771d-aee8-40bc-a4e7-bd49a16da3dc&product=&channel=Stable&version=104.0.4944.36
https://features.opera-api2.com/api/v2/features?country=CZ&language=cs&uuid=61fc426d-50cb-4ae7-afcf-2b80f29ff2c1&product=&channel=Stable&version=104.0.4944.36
https://features.opera-api2.com/api/v2/features?country=CZ&language=cs&uuid=7d08646c-8953-48d2-ab92-37505d2acbe3&product=&channel=Stable&version=104.0.4944.36
https://addons-extensions.operacdn.com/media/direct/90/287790/6e46db723146bd6bb16114a78a7f3ed7.crx
https://api.msn.com/v1/News/Feed/Windows?apikey=qrUeHGGYvVowZJuHA3XaH0uUvg1ZJ0GUZnXk3mxxPF&ocid=windows-windowsShell-feeds&osLocale=cs-
CZ&CheckEnable=true&activityId=5E5D829C-885E-4907-8E8A-02ED38CD0AC0&user=m-56abb202c01c4327997385e9e6e74c8a
https://api.msn.com/v1/News/Feed/Windows?apikey=qrUeHGGYvVowZJuHA3XaH0uUvg1ZJ0GUZnXk3mxxPF&ocid=windows-windowsShell-feeds&osLocale=cs-
CZ&CheckEnable=true&activityId=684B3DA8-77EC-4CEB-9B08-6D10D6F181D7&user=m-3c7a3b91154d4d34b8f4da1a005d5f0d
https://api.msn.com/v1/News/Feed/Windows?apikey=qrUeHGGYvVowZJuHA3XaH0uUvg1ZJ0GUZnXk3mxxPF&ocid=windows-windowsShell-feeds&osLocale=cs-
CZ&CheckEnable=true&activityId=C27CA761-929C-416B-8F76-E6876127ED56&user=m-e428ff5e304d4929ab6cb43ab48ab3bd
Cookie:vboxuser@live.com/
Cookie:vboxuser@msn.com/
Cookie:vboxuser@api.msn.com/
Visited: vboxuser@file:///C:/Users/vboxuser/Desktop/MBReport.txt
Visited: vboxuser@file:///C:/logs/tron/tron.log
Visited: vboxuser@file:///C:/logs/tron/summary_logs/tron_removed_programs.txt
Visited: vboxuser@file:///C:/logs/tron/summary_logs/tron_removed_files.txt
Visited: vboxuser@file:///C:/Users/vboxuser/AppData/Local/Programs/Opera
WinINet Cache entries deleted: 21
http://x.ss2.us/x.cer
http://www.microsoft.com/pkiops/crl/Microsoft%20ID%20Verified%20CS%20AOC%20CA%2001.crl
http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl
http://ocsp.globalsign.com/rootr1/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCDQHuXxad%2F5c1K2Rl1mo%3D
http://crl.microsoft.com/pki/crl/products/MicCodSigPCA_2010-07-06.crl
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQrHR6YzPN2BNbByL0VoiTIBBMAOAQUCrwIKReMpTlteg7OM8cus%2B37w3oCEAkWPlmkY2sM4Y0QWNg2IJM%3D
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBT3xL4LQLXDRDM9P665TW442vrsUQQUReuir%2FSSy4IxLVGLp6chnfNtyA8CEA6bGI750C3n79tQ4ghAGFo%3D
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAo3h2ReX7SMIk79G%2B0UDDw%3D
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAonX%2BcE1u7LI9XNW0saTgQ%3D
http://oneocsp.microsoft.com/ocsp/MFQwUjBQME4wTDAJBgUrDgMCGgUABBTDHsfuqfubd3pihvq4mgQVWgHWNwQUyH7SaoUqG8oZmAQHJ89QEE9oqKICEzMAAAAHh6M0o3uljhwAAAAAAAc%3
D
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAxq6XzO1ZmDhpCgCp6lMhQ%3D
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEA177el9ggmWelJjG4vdGL0%3D
http://oneocsp.microsoft.com/ocsp/MFQwUjBQME4wTDAJBgUrDgMCGgUABBTOQYLFSE5GO%2FpaRVfYu7d9gZEbQAQU2UEpsA8PY2zvadf1zSmepEhqM0YCEzMAAAAHN4xbodlbjNQAAAAAAAc%
3D
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSRXerF0eFeSWRripTgTkcJWMm7iQQUaDfg67Y7%2BF8Rhvv%2BYXsIiGX0TkICEARO0eQCVRZszqCQCpEIZGVE%3D
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSRXerF0eFeSWRripTgTkcJWMm7iQQUaDfg67Y7%2BF8Rhvv%2BYXsIiGX0TkICEAowIeDPMFmFwVZmGNshK9c%3D
http://oneocsp.microsoft.com/ocsp/MFQwUjBQME4wTDAJBgUrDgMCGgUABBRBq81UG1MnDOVNKqff0SSEz6JuZwQU6IPEM9fcnwycdpoKptTfh6ZeWO4CEzMAACowMwDWgbj3glQAAAAAKjA%3D
http://ocsp.globalsign.com/codesigningrootr45/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQVFZP5vqhCrtRN5SWf40Rn6NM1IAQUHwC%2FRoAK%2FHg5t6W0Q9lWULvOljsCEHe9DgOhtwj4VKsGch
DZBEc%3D
http://ocsp.globalsign.com/gsgccr45codesignca2020/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBTLuA3ygnKW%2F7xuSx%2F09F%2BhHVuEUQQU2rONwCSQo2t30wygWd0hZ2R2C3gCDFzND7mML
NACIZYo2Q%3D%3D
http://ocsp.globalsign.com/rootr3/MFEwTzBNMEswSTAJBgUrDgMCGgUABBT1nGh%2FJBjWKnkPdZIzB1bqhelHBwQUj%2FBLf6guRSSuTVD6Y5qL3uLdG7wCEHgDGEJFcIpBz28BuO60qVQ%3D
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAbY2QTVWENG9oovp1QifsQ%3D
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAfy81yHqHeveu%2FpR5k1Jb0%3D
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfls%2BLjDtGwQ09XEB1Yeq%2BtX%2BBgQQU7NfjgtJxXWRM3y5nP%2Be6mK4cD08CEAitQLJg0pxMn17Nqb2Trtk%3D
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEA77flR%2B3w%2FxBpruV2lte6A%3D
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEApDqVCbATUviZV57HIIulA%3D
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab
WinHttp Cache entries deleted: 27
CertUtil: -URLCache command FAILED: 0x80070103 (WIN32/HTTP: 259 ERROR_NO_MORE_ITEMS)
CertUtil: Žádná další data nejsou k dispozici.
2023-11-07 14:27:30,77    Done.
2023-11-07 14:27:30,77    Launch job 'Clean Internet Explorer'...
2023-11-07 14:27:31,66    Done.
2023-11-07 14:27:31,66    Launch job 'TempFileCleanup'...
 Starting temp file cleanup
 ---------------------------
 Cleaning USER temp files...
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Caches\cversions.3.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Caches\{311B3FF8-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x000000000000000c.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x000000000000000e.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000002.db
```

Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000003.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_1280.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_16.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_1920.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_256.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_2560.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_32.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_48.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_768.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_96.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_custom_stream.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_exif.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_idx.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_sr.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_wide_alternate.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1280.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_16.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1920.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_2560.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_48.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_768.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_custom_stream.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_exif.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_wide.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_wide_alternate.db
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\INetCache\Low\SmartScreenCache.dat
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\WebCache\V01.chk
C:\Users\vboxuser\AppData\Local\Microsoft\Windows\WebCache\V01.log
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\WebCache\V0100004.log
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\WebCache\V01res00001.jrs
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\WebCache\V01res00002.jrs
Deleted file - C:\Users\vboxuser\AppData\Local\Microsoft\Windows\WebCache\V01tmp.log
C:\Users\vboxuser\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
C:\Users\vboxuser\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.jfm
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\.ses
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\112233445566778899001122334455 66
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\37aabf04-8856-413c-96fe-4f276784bc13.tmp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\9d11db89-3e29-4924-83b3-212a853b885b.tmp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\assistant_installer_20231107111207.log
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\assistant_installer_20231107111917.log
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\baab8ef4-43b2-4400-8fad-2318903771ba.tmp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\CUsersvboxuserAppDataLocalProgramsOpera104.0.4944.36opera_autoupdate.download.lock
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\cv_debug.log
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\MBAMInstallerService.exe
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\mbsetup.log
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\mb_setup.log
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\MicrosoftEdgeUpdate.log
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\MpCmdRun.log
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\Opera_installer_2311071012285873068.dll
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\Opera_installer_2311071012303851 0092.dll
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\Opera_installer_2311071322234527872.dll
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\Opera_installer_2311071322240518092.dll
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\Opera_installer_2311071322249358372.dll
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\Setup Log 2023-11-07 #001.txt
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\.opera\Opera Installer Temp\installer.exe
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\.opera\Opera Installer Temp\opera_package_202311071112291\opera_package
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\.opera\Opera Installer Temp\opera_package_20231107142224 1\opera_package
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_1005701859\44b6fc18-5e6d-4cb0-93dc-762c66604835
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_1124975060\4643befd-79b8-4e0c-a2fb-c0e3ee78dcd5
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_1412599191\0ee18f6d-5bb2-4a69-abd7-6fb33b65fe1f
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_1545207708\f22c863f-657e-4ae8-b972-495f0d906687
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_168526143\376d5b20-4ccf-4ab3-92ec-d2fa66fb039b
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_1770616839\621a4ceb-00df-4de7-b7ca-42b2435b0a29
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_209144193\9e51170b-7adf-40ab-83b6-5f97b13bedcb
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_2112597148\d42688a1-b719-4314-b0ae-562104cecf02
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_2140800977\dd65cd6e-da04-4d01-9089-b864f080118b
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_578992660\2c37d5c4-d1c7-4302-92ab-98a42c509ab7
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_887385109\2aaa8eb1-4390-495e-873c-71f03ed02d54
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\edge_BITS_2172_926094335\2e8a592b-0ad4-414c-b996-21bd8749e2fd
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\mbam\qt-jl-icons\46322b0.ico
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\mbam\qt-jl-icons\4632380.ico
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\mbam\qt-jl-icons\4632470.ico
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\mbam\qt-jl-icons\46325e0.ico
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir10192_1557704322\opera-one.jpg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir10192_1557704322\persona.ini
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\37aabf04-8856-413c-96fe-4f276784bc13.tmp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\favicon.ico
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\index.html
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\manifest.json
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\service.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\service.js.LICENSE.txt
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\1360.75e0390e.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\1433.8e533891.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\2438.8e533891.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\3272.c9f6f9dc.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\332.4ab6799e.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\3855.0bdf9311.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\3876.8e533891.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\4451.6d768aba.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\4800.6d768aba.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\5062.95da8d8e.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\5257.1a2e1ad0.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\5319.1d9d2087.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\6827.6d768aba.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\7465.aa0a2a9a.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\8724.3263b3cb.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\9309.9d57b55f.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\css\app.b0d55aea.css
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\fonts\icon.0b24eda7.eot
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\fonts\icon.1989ce45.woff
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\fonts\icon.328be64c.woff2
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\fonts\icon.f90a6881.ttf
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\1inch.c2dd2051.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\attention.8ceed8ab.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\backup_phrase_cyan.cc8f0c1e.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\backup_phrase_gray.b5f70190.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\bell.1ec148fb.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\bg_dark.6fbd364a.svg

Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\buzzer.2dcc83b6.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\cashback.c4599857.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\cashback_paidout.e44c6a10.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\cashback_pending.385f3286.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\cashback_received.4c0ef33a.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\cashback_rejected.2bdca35b.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\cc.aca1a1de.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\check.feed8769.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\check_selected.1169a7e5.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\chevron_up.316e082e.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\close.949d073c.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\cog.a0203a09.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\collectible_placeholder.76169588.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\complete_big.fe2ecc72.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\contract.de7f06d5.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\copypaster_mini.6681e653.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\cryptobackup_backedup.722c816a.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\cryptobackup_backup.7122ac41.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\crypto_wallet_background.34d522e0.webp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\crypto_wallet_background_blurred.ed3d8ee7.webp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\empty_assets.49ddba55.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\empty_error.6fa940d6.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\empty_nfts.5db12a65.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\empty_nfts2.ae2593f7.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\empty_tokens.b8ef79b4.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\ens.14260065.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\error.93c0e5ce.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\external_link.2f3f3ba3.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\external_link_cyan.ca83253e.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\eye.68efa0bc.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\eye_closed.55a4bebc.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\fantom.d14ded30.png
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\fio.82458516.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\fio.a9a38124.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\fio_domain.8c9954e5.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\fio_handle.b1d53b26.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\fio_handle_gray.16f2df1a.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\fio_onboarding_illustration.04fb36a2.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\generic_token.f1b5406c.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\generic_token_unverified.abfdc94c.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\goplus.22036c0b.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\help.5bb18606.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\help_cyan.7021933d.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\help_gray.25094ae0.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\help_outlined.73bf57c3.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\help_outlined_gray.e12f2f7f.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\icon.b5b5f9a8.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\import_wallet.07c43928.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\info.088cf412.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\in_progress_big.35353198.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\language.d2d2f226.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\loading_arrow.9aa43d9b.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\menu_kebab_gray.a1987164.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\moonpay.8cd24a6f.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\network.dc85aa41.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\non_verified.acef51e5.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\opera_points.d0f84991.webp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\opera_token_icon.3a4907cf.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\opera_token_icon_gray.d0eb5f3f.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\opera_token_icon_red.929ec8ec.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\pancakeswap.ae54e455.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\plus.b6e7e961.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\portfolio_background.e09645c2.webp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\portfolio_background_2.60b0f212.webp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\processing.124be38f.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\reload_nfts.32e9429a.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\secure_backup_phrase.63c2d6d2.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\sort.0524b1ce.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\squircle_desktop.95656e11.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\success.49cc4914.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\swap_to.02a4598e.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\ud.65fd7dae.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\ud.b36519bf.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\unverified.3e563384.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\warning_circle.f03f1ac1.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\warning_circle_dark.b4231eac.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\warning_triangle.07b323b5.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\welcome_page_coin_logos.0d4e909e.webp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\yat.4ca801f0.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\img\icons\icon_512.png
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1292.c5178ec1.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1360.025400ca.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1385.65836de8.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1433.eb7b2a73.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1645.bcbaf41b.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\173.fa037303.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1755.4c5cb5ad.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1758.d3b113e2.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1811.4bf22f5e.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1898.b5668999.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1913.a4b2ecfb.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1941.9c166280.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\1965.dd2c2447.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\2084.86475033.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\2161.7817011e.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\2201.306fc905.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\2438.24c16d3d.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\246.5114059c.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\2463.940f943d.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\2756.4210856f.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\3010.a42dfb40.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\3084.7599b224.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\3272.34988dea.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\3285.e4d9e404.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\332.db7b7740.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\3624.f14d66f0.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\3679.6f9ac6f7.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\3723.e2205fa9.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\3855.0940fb02.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\3876.80008ba4.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\4103.7ca837e1.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\4319.7ec1fcc2.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\4404.d23dfdcd.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\4451.2e060230.js

Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\4564.4643d7f2.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\4800.06dd74ff.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\4853.61da4d96.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\5035.0c7847af.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\5062.a4cc597d.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\5100.05f3071c.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\5133.77db4db7.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\5257.b6d1dbd4.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\5291.ca8ebe18.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\5319.f5dab04c.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\5371.f5c473a2.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\5439.83eb580c.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\5493.310c9191.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6084.ec181a64.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6086.af1a035d.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6192.1eb117b1.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6222.f481d6f0.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6287.b44f1462.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6334.385bc947.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6411.fd98065e.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6434.81d049bf.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6501.a929cb9b.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6662.d26f5c77.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6822.025820c4.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\6827.2cf8af01.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\7058.59c5aac3.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\7227.ff72a521.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\7349.0b22f6cd.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\7465.59bcc958.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\7566.555cf9b5.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\7584.23bf14e1.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\7662.93265589.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\7839.c500e2e9.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\8513.11acab08.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\8599.fb53ee8d.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\8724.1fcd6ee7.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\8851.307c937e.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\8929.215ed5f3.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\8933.2a9e0471.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\8977.d28bbe76.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\9212.d7a52796.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\9309.c1c64e05.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\9477.290f91ee.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\9600.a462bed6.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\9702.ea0a3a5b.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\9703.2ae4849b.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\9857.ff9284dc.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\9858.3bf83207.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\app.83494ebb.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\js\chunk-vendors.39ed5e34.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\opera-services\cashback.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\web3\dispatcher.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\web3\provider.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL\web3\provider.js.LICENSE.txt
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1511211183\CRX_INSTALL_locales\en\messages.json
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1627050902\baab8ef4-43b2-4400-8fad-2318903771ba.tmp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1627050902\CRX_INSTALL\history-tags.json
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1627050902\CRX_INSTALL\main.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1627050902\CRX_INSTALL\manifest.json
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1627050902\CRX_INSTALL\startpage_test_function.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_1627050902\CRX_INSTALL\targeted_sd_section.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\9d11db89-3e29-4924-83b3-212a853b885b.tmp
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\0246e88ab3b60542f582.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\046461fc1a778fe43d99.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\0eebbdfb27d542c486ce.ttf
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\119f3e8d7e064a605fa9.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\13a27524bd914f383b14.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\1b3b83dac50be6b9c503.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\1e1c0e29b79b49a6ff4d.ttf
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\212532323374ae2448ec.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\2b1d5bea6b59d7df7543.ttf
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\2d0dbf42750207f78ffa.ttf
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\35f1c167ca2db828deac.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\36c7b8b5ca8e5fb1c18c.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\3732873d6bcc644421fa.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\3dcbef40ef1b04e21951.ttf
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\44d85d37ca16b0b3a224.ttf
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\519414858d6d3c29c8c7.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\5d1a909f3c0b18e897f0.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\637f22f6137db0081579.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\6e912113b807d9defcf7.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\70eba12308e7984fd14b.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\7120b68615ebe4b28075.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\75bd363a076f7029be1d.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\763c3b026deaf11f0f62.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\7be90d1afea9e1266308.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\823d9899847c2950d3b26.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\8b1e2eeb08e4775da979.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\9abe40fc417dcd471d7d.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\a51e03c27e5ae6ba4c04.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\a6ea629634c3a0842004.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\aa9f6c109f0b3947dac2.ttf
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\ae085df80c1e2592528f.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\ae7f5d2b09428c3c1222.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\aria.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\b2ad8477497f8fc95224.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\b3baca6de20012788f7d.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\ba5622550ada9b5ff2cd.ttf
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\background_worker.js
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\d6554a0accc0fc7dada5.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\d7a6c05a1e25e642f6ab.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\d8c997123e645906d03c.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\e357c7e21fb8a2224b04.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\e563de5c65c7d63f04e7.ttf
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\e5dc591367f544aac02d.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\f192f471a1a8ea34754a.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\f2b98fe9fec84abf11de.svg
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\manifest.json
Deleted file - C:\Users\vboxuser\AppData\Local\Temp\scoped_dir8028_62178650\CRX_INSTALL\prompt.js
 Done.
 Cleaning SYSTEM temp files...
Deleted file - C:\Windows\TEMP\mbamiservice.log
Deleted file - C:\Windows\TEMP\MBAMSERVICE.LOG
Deleted file - C:\Windows\TEMP\mb_errors999.log

```
Deleted file - C:\Windows\TEMP\MpCmdRun.log
  Done.
-------------------------------------------------------------------------------------------------------
2023-11-07 14:27:32,10  TempFileCleanup v1.2.2-TRON, finished. Executed as VMTESTINGENVIRO\vboxuser
-------------------------------------------------------------------------------------------------------
 Cleanup complete.
 Log saved at: C:\logs\tron\tron.log
2023-11-07 14:27:32,10    Done.
2023-11-07 14:27:32,12    Launch job 'CCleaner'...
2023-11-07 14:27:32,12 !  SKIP_COOKIE_CLEANUP (-scc) set to yes. Preserving ALL cookies.
2023-11-07 14:30:44,01    Done.
2023-11-07 14:30:44,02    Launch job 'Clean duplicate files from Download folders'...
Error: No files matched 'C:\Users\C:\Users\vboxuser\AppData\Local\Temp\userlist.txt\Downloads\**'
No files to process
2023-11-07 14:30:44,02    Done.
2023-11-07 14:30:44,02    Launch job 'USB Device Cleanup'...
DriveCleanup V1.6.3 (x64)
Uninstalls non present USB hubs, USB storage devices, Disks, CDROMs, Floppies, storage volumes and WPD devices
and deletes their registry items
Freeware by Uwe Sieber - www.uwe-sieber.de
removing volume 'STORAGE\VOLUMESNAPSHOT\HARDDISKVOLUMESNAPSHOT1'
 OK
removing volume 'STORAGE\VOLUMESNAPSHOT\HARDDISKVOLUMESNAPSHOT2'
 OK
Removed 0 USB devices
Removed 0 USB hubs
Removed 0 Disk devices
Removed 0 CDROM devices
Removed 0 Floppy devices
Removed 2 Storage volumes
Removed 0 WPD devices
Removed 0 Items from registry
2023-11-07 14:30:45,09    Done.
2023-11-07 14:30:45,09    Launch job 'Clear Windows event logs'...
2023-11-07 14:30:45,09    Saving logs to "C:\logs\tron\backups" first...
No Instance(s) Available.
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Application.evtx")->BackupEventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 80;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\HardwareEvents.evtx")->BackupEventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 80;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Internet Explorer.evtx")->BackupEventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 80;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Key Management Service.evtx")->BackupEventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 80;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Parameters.evtx")->BackupEventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 80;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Security.evtx")->BackupEventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 80;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\State.evtx")->BackupEventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 80;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\System.evtx")->BackupEventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 80;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Windows PowerShell.evtx")->BackupEventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 80;
};
2023-11-07 14:30:45,66    Backups done, now clearing...
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Application.evtx")->cleareventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 0;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\HardwareEvents.evtx")->cleareventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
                ReturnValue = 0;
};
```

```
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Internet Explorer.evtx")->cleareventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Key Management Service.evtx")->cleareventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Parameters.evtx")->cleareventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Security.evtx")->cleareventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\State.evtx")->cleareventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\System.evtx")->cleareventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
Executing (\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\Windows\\System32\\Winevt\\Logs\\Windows PowerShell.evtx")->cleareventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
2023-11-07 14:30:45,76    Done.
2023-11-07 14:30:45,76    Launch job 'Clear Windows Update cache'...
Operace byla dokoncena Łspesne.
Sluzba Windows Update nen˝ spustena.
Dals˝ n povedu z˝sk te pr˝kazem NET HELPMSG 3521.
Spousten˝ sluzby Windows Update.
Sluzba Windows Update byla Łspesne spustena.
2023-11-07 14:30:47,80    Done.
2023-11-07 14:30:47,80    Launch job 'Reset BranchCache'...
The following command was not found: branchcache show status all.
The following command was not found: branchcache flush.
2023-11-07 14:30:47,93    Done.
2023-11-07 14:30:47,93    Launch job 'Windows Disk Cleanup'...
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
Operace byla dokoncena Łspesne.
2023-11-07 14:31:15,73   stage_1_tempclean complete.
2023-11-07 14:31:15,73 ! SKIP_DEBLOAT (-sdb) set, skipping Stage 2...
2023-11-07 14:31:15,73   stage_3_disinfect begin...
2023-11-07 14:31:15,74    Launch job 'Install Malwarebytes Anti-Malware'...
Zastavov n˝ sluzby Malwarebytes Service.
Sluzba Malwarebytes Service byla Łspesne zastavena.
stage_3_disinfect\mbam\AeConfig.json
stage_3_disinfect\mbam\ArwControllerConfig.json
stage_3_disinfect\mbam\CleanControllerConfig.json
stage_3_disinfect\mbam\CloudConfig.json
stage_3_disinfect\mbam\LicenseConfig.json
stage_3_disinfect\mbam\MbamClientConfig.json
stage_3_disinfect\mbam\MwacControllerConfig.json
stage_3_disinfect\mbam\PoliciesConfig.json
stage_3_disinfect\mbam\RtpConfig.json
stage_3_disinfect\mbam\ScanConfig.json
stage_3_disinfect\mbam\SpConfigFile.json
stage_3_disinfect\mbam\TelemCtrlConfig.json
stage_3_disinfect\mbam\telemetry.json
stage_3_disinfect\mbam\UpdateControllerConfig.json
      14 file(s) copied.
2023-11-07 14:31:32,67    Loading bundled definitions package...
2023-11-07 14:32:07.176   Log opened. (Time zone: UTC+01:00)
2023-11-07 14:32:07.176   Setup version: Inno Setup version 5.5.6 (a)
2023-11-07 14:32:07.176   Original Setup EXE: C:\Users\vboxuser\Desktop\tron\resources\stage_3_disinfect\mbam\mbam2-rules.exe
2023-11-07 14:32:07.176   Setup command line: /SL5="$702CC,10937194,56832,C:\Users\vboxuser\Desktop\tron\resources\stage_3_disinfect\mbam\mbam2-rules.exe" /sp- /verysilent
/suppressmsgboxes /log="C:\logs\tron\raw_logs\mbam_rules_install.log" /norestart
2023-11-07 14:32:07.176   Windows version: 10.0.19045  (NT platform: Yes)
2023-11-07 14:32:07.176   64-bit Windows: Yes
2023-11-07 14:32:07.176   Processor architecture: x64
2023-11-07 14:32:07.176   User privileges: Administrative
```

2023-11-07 14:32:07.176 64-bit install mode: No
2023-11-07 14:32:07.176 Created temporary directory: C:\Users\vboxuser\AppData\Local\Temp\is-QCDRE.tmp
2023-11-07 14:32:07.239 Starting the installation process.
2023-11-07 14:32:07.239 Creating directory: C:\Program Files (x86)\Malwarebytes Anti-Malware
2023-11-07 14:32:07.239 -- File entry --
2023-11-07 14:32:07.239 Dest filename: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\rules.ref
2023-11-07 14:32:07.239 Time stamp of our file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.239 Dest file exists.
2023-11-07 14:32:07.239 Time stamp of existing file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.239 Version of our file: (none)
2023-11-07 14:32:07.239 Version of existing file: (none)
2023-11-07 14:32:07.239 Installing the file.
2023-11-07 14:32:07.286 Successfully installed the file.
2023-11-07 14:32:07.286 Setting permissions on file: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\rules.ref
2023-11-07 14:32:07.286 -- File entry --
2023-11-07 14:32:07.286 Dest filename: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\actions.ref
2023-11-07 14:32:07.286 Time stamp of our file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.286 Dest file exists.
2023-11-07 14:32:07.286 Time stamp of existing file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.286 Version of our file: (none)
2023-11-07 14:32:07.286 Version of existing file: (none)
2023-11-07 14:32:07.286 Installing the file.
2023-11-07 14:32:07.286 Successfully installed the file.
2023-11-07 14:32:07.286 Setting permissions on file: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\actions.ref
2023-11-07 14:32:07.286 -- File entry --
2023-11-07 14:32:07.286 Dest filename: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\swissarmy.ref
2023-11-07 14:32:07.286 Time stamp of our file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.286 Dest file exists.
2023-11-07 14:32:07.286 Time stamp of existing file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.286 Version of our file: (none)
2023-11-07 14:32:07.286 Version of existing file: (none)
2023-11-07 14:32:07.286 Installing the file.
2023-11-07 14:32:07.286 Successfully installed the file.
2023-11-07 14:32:07.286 Setting permissions on file: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\swissarmy.ref
2023-11-07 14:32:07.286 -- File entry --
2023-11-07 14:32:07.286 Dest filename: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\domains.ref
2023-11-07 14:32:07.286 Time stamp of our file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.286 Dest file exists.
2023-11-07 14:32:07.286 Time stamp of existing file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.286 Version of our file: (none)
2023-11-07 14:32:07.286 Version of existing file: (none)
2023-11-07 14:32:07.286 Installing the file.
2023-11-07 14:32:07.301 Successfully installed the file.
2023-11-07 14:32:07.301 Setting permissions on file: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\domains.ref
2023-11-07 14:32:07.301 -- File entry --
2023-11-07 14:32:07.301 Dest filename: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\ips.ref
2023-11-07 14:32:07.301 Time stamp of our file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.301 Dest file exists.
2023-11-07 14:32:07.301 Time stamp of existing file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.301 Version of our file: (none)
2023-11-07 14:32:07.301 Version of existing file: (none)
2023-11-07 14:32:07.301 Installing the file.
2023-11-07 14:32:07.301 Successfully installed the file.
2023-11-07 14:32:07.301 Setting permissions on file: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\ips.ref
2023-11-07 14:32:07.301 -- File entry --
2023-11-07 14:32:07.301 Dest filename: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\akadomains.ref
2023-11-07 14:32:07.301 Time stamp of our file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.301 Dest file exists.
2023-11-07 14:32:07.301 Time stamp of existing file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.301 Version of our file: (none)
2023-11-07 14:32:07.301 Version of existing file: (none)
2023-11-07 14:32:07.301 Installing the file.
2023-11-07 14:32:07.301 Successfully installed the file.
2023-11-07 14:32:07.301 Setting permissions on file: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\akadomains.ref
2023-11-07 14:32:07.301 -- File entry --
2023-11-07 14:32:07.301 Dest filename: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\akaips.ref
2023-11-07 14:32:07.301 Time stamp of our file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.301 Dest file exists.
2023-11-07 14:32:07.301 Time stamp of existing file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.301 Version of our file: (none)
2023-11-07 14:32:07.301 Version of existing file: (none)
2023-11-07 14:32:07.301 Installing the file.
2023-11-07 14:32:07.301 Successfully installed the file.
2023-11-07 14:32:07.301 Setting permissions on file: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\akaips.ref
2023-11-07 14:32:07.301 -- File entry --
2023-11-07 14:32:07.301 Dest filename: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\Configuration\manifest.conf
2023-11-07 14:32:07.301 Time stamp of our file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.301 Dest file exists.
2023-11-07 14:32:07.301 Time stamp of existing file: 2019-10-17 09:00:56.000
2023-11-07 14:32:07.301 Version of our file: (none)
2023-11-07 14:32:07.301 Version of existing file: (none)
2023-11-07 14:32:07.301 Installing the file.
2023-11-07 14:32:07.301 Successfully installed the file.
2023-11-07 14:32:07.301 Setting permissions on file: C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\Configuration\manifest.conf
2023-11-07 14:32:07.301 Installation process succeeded.
2023-11-07 14:32:07.301 Need to restart Windows? No
2023-11-07 14:32:07.301 Deinitializing Setup.
2023-11-07 14:32:07.301 Log closed.
2023-11-07 14:32:07,31 Done.
2023-11-07 14:32:07,33 Launch job 'Malwarebytes AdwCleaner'...
2023-11-07 14:32:07,33 Tool-specific log will be saved to "C:\logs\tron\raw_logs\AdwCleaner"
2023-11-07 14:32:18,41 Done.
2023-11-07 14:32:18,41 Launch job 'Kaspersky Virus Removal Tool'...
2023-11-07 14:32:18,41 Tool-specific log will be saved to "C:\logs\tron\raw_logs\Reports"
2023-11-07 14:35:09,26 Done.
2023-11-07 14:35:09,26 Launch job 'Sophos Virus Removal Tool' (slow, be patient)...
2023-11-07 14:35:09,28 Scan output REDUCED by default (use -v to show full output)...
1 file(s) copied.
d'»ž2023-11-07 13:35:09.332 Sophos Virus Removal Tool version 2.9.0
2023-11-07 13:35:09.332 Copyright (c) 2009-2021 Sophos Limited. All rights reserved.
2023-11-07 13:35:09.332 You can safely ignore "could not open" errors during this portion
2023-11-07 13:35:09.332 Windows version 6.2 SP 0.0 build 9200 SM=0x300 PT=0x1 WOW64
2023-11-07 13:35:09.332 Log file path: C:\ProgramData\Sophos\Sophos Virus Removal Tool\Logs\SophosVirusRemovalTool.log
2023-11-07 13:35:19.941 Option all = no
2023-11-07 13:35:19.941 Option recurse = yes
2023-11-07 13:35:19.941 Option archive = no
2023-11-07 13:35:19.941 Option service = yes
2023-11-07 13:35:19.941 Option confirm = yes
2023-11-07 13:35:19.941 Option ssl = yes
2023-11-07 13:35:19.941 Option max-data-age = 35
2023-11-07 13:35:19.941 Option EnableSafeClean = no
2023-11-07 13:35:19.941 Couldn't apply option 'EnableSafeClean' to the detection engine [0xa004020c].
2023-11-07 13:35:19.941 Option vdl-logging = yes
2023-11-07 13:35:19.941 Component SVRTcli.exe version 2.9.0

```
2023-11-07 13:35:19.941	Component control.dll version 2.9.0
2023-11-07 13:35:19.941	Component SVRTservice.exe version 2.9.0
2023-11-07 13:35:19.941	Component engine\osdp.dll version 1.44.1.2561
2023-11-07 13:35:19.957	Component engine\veex.dll version 3.86.1.2561
2023-11-07 13:35:19.957	Component engine\savi.dll version 9.0.31.2561
2023-11-07 13:35:19.957	Component rkdisk.dll version 1.5.33.1
2023-11-07 13:35:19.957	Version info:	Product version 2.9.0
2023-11-07 13:35:19.957	Version info:	Detection engine		3.86.1
2023-11-07 13:35:19.957	Version info:	Detection data	5.95
2023-11-07 13:35:19.957	Version info:	Build date	8/30/2022
2023-11-07 13:35:19.957	Version info:	Data files added 857
2023-11-07 13:35:19.957	Version info:	Last successful update		(not yet updated)
2023-11-07 13:36:49.202	Could not open C:\Boot\BCD
2023-11-07 13:36:50.624	Could not open C:\pagefile.sys
2023-11-07 13:38:03.265	Could not open C:\swapfile.sys
2023-11-07 13:38:15.842	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\GameBarElevatedFT_Alias.exe
2023-11-07 13:38:15.842	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\MediaPlayer.exe
2023-11-07 13:38:15.842	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\python.exe
2023-11-07 13:38:15.842	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\python3.exe
2023-11-07 13:38:15.842	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\WindowsPackageManagerServer.exe
2023-11-07 13:38:15.842	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\winget.exe
2023-11-07 13:38:15.842	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe
2023-11-07 13:38:15.858	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\Microsoft.SkypeApp_kzf8qxf38zg5c\Skype.exe
2023-11-07 13:38:15.858	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe\GameBarElevatedFT_Alias.exe
2023-11-07 13:38:15.858	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\Microsoft.ZuneMusic_8wekyb3d8bbwe\MediaPlayer.exe
2023-11-07 13:38:15.858	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\MicrosoftEdge.exe
2023-11-07 13:38:15.858	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\python.exe
2023-11-07 13:38:15.858	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\python3.exe
2023-11-07 13:38:15.858	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\Skype.exe
2023-11-07 13:38:15.858	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\WindowsPackageManagerServer.exe
2023-11-07 13:38:15.858	Could not open C:\Users\vboxuser\AppData\Local\Microsoft\WindowsApps\winget.exe
2023-11-07 13:40:38.496	Could not open C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb
2023-11-07 13:40:38.496	Could not open C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
2023-11-07 13:40:39.574	Could not open C:\Windows\System32\config\BBI
2023-11-07 13:46:07.480	Error level 0
2023-11-07 13:46:07.480	Scan completed.
2023-11-07 13:46:07.480
-------------------------------------------------------------------
[SC] OpenService FAILED 1060:
Zadan sluzba nen" nainstalovan sluzba.
2023-11-07 14:46:07,49  Done.
2023-11-07 14:46:07,49  stage_3_disinfect complete.
2023-11-07 14:46:07,57  stage_4_repair begin...
2023-11-07 14:46:07,59  Cleaning up orphaned MSI cache files...
MsiZapInfo: Performing operations for user S-1-5-21-1612337995-798698995-356962622-1000
Removing orphaned cached files.
No product data was found.
2023-11-07 14:46:07,62  Done.
2023-11-07 14:46:07,62  Launch job 'DISM Windows image check'...
2023-11-07 14:47:54,53  DISM: No image corruption detected.
2023-11-07 14:47:54,53  Compiling DISM logs into main Tron log...
d'»ž2023-11-07 11:00:32, Info	DISM	DISM	PID=8372 TID=1272 Scratch directory set to 'C:\Users\vboxuser\AppData\Local\Temp\'. - CDISMManager::put_ScratchDir
2023-11-07 11:00:32, Info	DISM	DISM	PID=8372 TID=1272 DismCore.dll version: 10.0.19041.3570 - CDISMManager::FinalConstruct
2023-11-07 11:00:32, Info	DISM	DISM	Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 11:00:32, Info	DISM	DISM	PID=8372 TID=1272 Successfully loaded the ImageSession at "C:\Windows\system32\Dism" - CDISMManager::LoadLocalImageSession
2023-11-07 11:00:32, Info	DISM	DISM	Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8372 TID=1272 Found and Initialized the DISM Logger. - CDISMProviderStore::Internal_InitializeLogger
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8372 TID=1272 Failed to get and initialize the PE Provider.  Continuing by assuming that it is not a WinPE image. - CDISMProviderStore::Final_OnConnect
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8372 TID=1272 Finished initializing the Provider Map. - CDISMProviderStore::Final_OnConnect
2023-11-07 11:00:32, Info	DISM	DISM	Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 11:00:32, Info	DISM	DISM	DISM Manager: PID=8372 TID=1272 Successfully created the local image session and provider store. - CDISMManager::CreateLocalImageSession
2023-11-07 11:00:32, Info	DISM	DISM	DISM.EXE:
2023-11-07 11:00:32, Info	DISM	DISM	DISM.EXE: <----- Starting Dism.exe session ----->
2023-11-07 11:00:32, Info	DISM	DISM	DISM.EXE:
2023-11-07 11:00:32, Info	DISM	DISM	DISM.EXE: Host machine information: OS Version=10.0.19045, Running architecture=amd64, Number of processors=8
2023-11-07 11:00:32, Info	DISM	DISM	DISM.EXE: Dism.exe version: 10.0.19041.3570
2023-11-07 11:00:32, Info	DISM	DISM	DISM.EXE: Executing command line: dism  /Online /NoRestart /Cleanup-Image /ScanHealth /Logpath:"C:\logs\tron\raw_logs\dism_check.log"
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8372 TID=1272 Connecting to the provider located at C:\Windows\system32\Dism\FolderProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info	DISM	DISM	DISM Manager: PID=8372 TID=1272 physical location path: C:\ - CDISMManager::CreateImageSession
2023-11-07 11:00:32, Info	DISM	DISM	DISM Manager: PID=8372 TID=1272 Event name for current DISM session is Global\{B5FDD2EF-38EB-4B4C-9DC6-452A05D72DBE} - CDISMManager::CheckSessionAndLock
2023-11-07 11:00:32, Info	DISM	DISM	DISM Manager: PID=8372 TID=1272 Create session event 0x248 for current DISM session and event name is Global\{B5FDD2EF-38EB-4B4C-9DC6-452A05D72DBE}  - CDISMManager::CheckSessionAndLock
2023-11-07 11:00:32, Info	DISM	DISM	DISM Manager: PID=8372 TID=1272 Copying DISM from "C:\Windows\System32\Dism" - CDISMManager::CreateImageSessionFromLocation
2023-11-07 11:00:32, Info	DISM	DISM	DISM Manager: PID=8372 TID=1272 Successfully loaded the ImageSession at "C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B" - CDISMManager::LoadRemoteImageSession
2023-11-07 11:00:32, Info	DISM	DISM	DISM Image Session: PID=8952 TID=1128 Instantiating the Provider Store. - CDISMImageSession::get_ProviderStore
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Initializing a provider store for the IMAGE session type. - CDISMProviderStore::Final_OnConnect
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\OSProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info	DISM	DISM	DISM OS Provider: PID=8952 TID=1128 Defaulting SystemPath to C:\ - CDISMOSServiceManager::Final_OnConnect
2023-11-07 11:00:32, Info	DISM	DISM	DISM OS Provider: PID=8952 TID=1128 Defaulting Windows folder to C:\Windows - CDISMOSServiceManager::Final_OnConnect
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Attempting to initialize the logger from the Image Session. - CDISMProviderStore::Final_OnConnect
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\LogProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info	DISM	DISM	Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Found and Initialized the DISM Logger. - CDISMProviderStore::Internal_InitializeLogger
2023-11-07 11:00:32, Warning	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Failed to load the provider: C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\PEProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0x8007007e)
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Failed to get and initialize the PE Provider.  Continuing by assuming that it is not a WinPE image. - CDISMProviderStore::Final_OnConnect
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Finished initializing the Provider Map. - CDISMProviderStore::Final_OnConnect
2023-11-07 11:00:32, Info	DISM	DISM	Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 11:00:32, Info	DISM	DISM	Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 11:00:32, Info	DISM	DISM	DISM Manager: PID=8372 TID=1272 Image session successfully loaded from the temporary location: C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B - CDISMManager::CreateImageSession
2023-11-07 11:00:32, Info	DISM	DISM	DISM.EXE: Target image information: OS Version=10.0.19045.3570, Image architecture=amd64
2023-11-07 11:00:32, Info	DISM	DISM	DISM.EXE: Image session version: 10.0.19041.3570
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Getting the collection of providers from an image provider store type. - CDISMProviderStore::GetProviderCollection
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\CbsProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info	DISM	DISM	DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info	CSI	00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
2023-11-07 11:00:32, Info	CSI	00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS
2023-11-07 11:00:32, Info	DISM	DISM	DISM OS Provider: PID=8952 TID=1128 Determined System directory to be C:\Windows\System32 - CDISMOSServiceManager::get_SystemDirectory
2023-11-07 11:00:32, Info	DISM	DISM	DISM Package Manager: PID=8952 TID=1128 Finished initializing the CbsConUI Handler. - CCbsConUIHandler::Initialize
2023-11-07 11:00:32, Info	CSI	00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
```

2023-11-07 11:00:32, Info CSI 00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS
2023-11-07 11:00:32, Info DISM DISM Package Manager: PID=8952 TID=1128 CBS is being initialized for online use. More information about CBS actions can be located at: %windir%\logs\cbs\cbs.log - CDISMPackageManager::Initialize
2023-11-07 11:00:32, Info DISM DISM Package Manager: PID=8952 TID=1128 Loaded servicing stack for online use only. - CDISMPackageManager::CreateCbsSession
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\MsiProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\IntlProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\IBSProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\DmiProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info CSI 00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
2023-11-07 11:00:32, Info CSI 00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS
2023-11-07 11:00:32, Info DISM DISM Driver Manager: PID=8952 TID=1128 Further logs for driver related operations can be found in the target operating system at %WINDIR%\inf\setupapi.offline.log - CDriverManager::Initialize
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\UnattendProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\SmiProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Warning DISM DISM Provider Store: PID=8952 TID=1128 Failed to load the provider: C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\EmbeddedProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0x8007007e)
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\AppxProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\ProvProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\AssocProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\GenericProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\OfflineSetupProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\SysprepProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\TransmogProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Transmog Provider: PID=8952 TID=1128 Current image session is [ONLINE] - CTransmogManager::GetMode
2023-11-07 11:00:32, Info DISM DISM Transmog Provider: PID=8952 TID=1128 Audit Mode: [No] - CTransmogManager::Initialize
2023-11-07 11:00:32, Info DISM DISM Transmog Provider: PID=8952 TID=1128 GetProductType: ProductType = [WinNT] - CTransmogManager::GetProductType
2023-11-07 11:00:32, Info DISM DISM Transmog Provider: PID=8952 TID=1128 Product Type: [WinNT] - CTransmogManager::Initialize
2023-11-07 11:00:32, Info DISM DISM Transmog Provider: PID=8952 TID=1128 Product Type ServerNT : [No] - CTransmogManager::Initialize
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\0642C76F-3739-4CC0-B278-17A893AE434B\SetupPlatformProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM Provider Store: PID=8952 TID=1128 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 11:00:32, Info DISM DISM.EXE: Got the collection of providers. Now enumerating them to build the command table.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: DISM Log Provider
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: OSServices
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: DISM Package Manager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: DISM Package Manager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: MsiManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: MsiManager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: IntlManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: IntlManager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: IBSManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: DriverManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: DriverManager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: DISM Unattend Manager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: DISM Unattend Manager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: SmiManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: AppxManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: AppxManager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: ProvManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: ProvManager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: AssocManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: AssocManager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: GenericManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: GenericManager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: OfflineSetupManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: OfflineSetupManager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: SysprepManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: SysprepManager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: Edition Manager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: Edition Manager.
2023-11-07 11:00:32, Info DISM DISM.EXE: Attempting to add the commands from provider: SetupPlatformManager
2023-11-07 11:00:32, Info DISM DISM.EXE: Succesfully registered commands for the provider: SetupPlatformManager.
2023-11-07 11:00:32, Info DISM DISM Package Manager: PID=8952 TID=1128 Processing the top level command token(cleanup-image). - CPackageManagerCLIHandler::Private_ValidateCmdLine
2023-11-07 11:00:32, Info DISM DISM Package Manager: PID=8952 TID=1128 Attempting to route to appropriate command handler. - CPackageManagerCLIHandler::ExecuteCmdLine
2023-11-07 11:00:32, Info DISM DISM Package Manager: PID=8952 TID=1128 Routing the command... - CPackageManagerCLIHandler::ExecuteCmdLine
2023-11-07 11:00:32, Info DISM DISM Package Manager: PID=8952 TID=1128 CBS session options=0x100! - CDISMPackageManager::Internal_Finalize
2023-11-07 11:03:49, Info CSI 00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
2023-11-07 11:03:49, Info CSI 00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS

2023-11-07 11:03:49, Info DISM DISM Package Manager: PID=8952 TID=1128 Loaded servicing stack for online use only. - CDISMPackageManager::CreateCbsSession
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Found the OSServices. Waiting to finalize it until all other providers are unloaded. - CDISMProviderStore::Final_OnDisconnect
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Found the OSServices. Waiting to finalize it until all other providers are unloaded. - CDISMProviderStore::Final_OnDisconnect
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Found the PE Provider. Waiting to finalize it until all other providers are unloaded. - CDISMProviderStore::Final_OnDisconnect
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(DISM Package Manager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Package Manager: PID=8952 TID=1128 Finalizing CBS core. - CDISMPackageManager::Finalize
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: DISM Package Manager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(MsiManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: MsiManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(IntlManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: IntlManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(IBSManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: IBSManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(DriverManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: DriverManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(DISM Unattend Manager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: DISM Unattend Manager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(SmiManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: SmiManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(AppxManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: AppxManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(ProvManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: ProvManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(AssocManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: AssocManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(GenericManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: GenericManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(OfflineSetupManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: OfflineSetupManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(SysprepManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: SysprepManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(Edition Manager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: Edition Manager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Finalizing the servicing provider(SetupPlatformManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: SetupPlatformManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Releasing the local reference to OSServices. - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Disconnecting Provider: OSServices - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8952 TID=1128 Releasing the local reference to DISMLogger. Stop logging. - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Manager: PID=8372 TID=1272 Closing session event handle 0x248 - CDISMManager::CleanupImageSessionEntry
2023-11-07 11:03:49, Info DISM DISM.EXE: Image session has been closed. Reboot required=no.
2023-11-07 11:03:49, Info DISM DISM.EXE:
2023-11-07 11:03:49, Info DISM DISM.EXE: <----- Ending Dism.exe session ----->
2023-11-07 11:03:49, Info DISM DISM.EXE:
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8372 TID=1272 Found the OSServices. Waiting to finalize it until all other providers are unloaded. - CDISMProviderStore::Final_OnDisconnect
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8372 TID=1272 Disconnecting Provider: FolderManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 11:03:49, Info DISM DISM Provider Store: PID=8372 TID=1272 Releasing the local reference to DISMLogger. Stop logging. - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:46:07, Info DISM PID=2816 TID=1748 Scratch directory set to 'C:\Users\vboxuser\AppData\Local\Temp\'. - CDISMManager::put_ScratchDir
2023-11-07 14:46:07, Info DISM PID=2816 TID=1748 DismCore.dll version: 10.0.19041.3570 - CDISMManager::FinalConstruct
2023-11-07 14:46:07, Info DISM Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 14:46:07, Info DISM PID=2816 TID=1748 Successfully loaded the ImageSession at "C:\Windows\system32\Dism" - CDISMManager::LoadLocalImageSession
2023-11-07 14:46:07, Info DISM Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=2816 TID=1748 Found and Initialized the DISM Logger. - CDISMProviderStore::Internal_InitializeLogger
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=2816 TID=1748 Failed to get and initialize the PE Provider. Continuing by assuming that it is not a WinPE image. - CDISMProviderStore::Final_OnConnect
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=2816 TID=1748 Finished initializing the Provider Map. - CDISMProviderStore::Final_OnConnect
2023-11-07 14:46:07, Info DISM Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 14:46:07, Info DISM DISM Manager: PID=2816 TID=1748 Successfully created the local image session and provider store. - CDISMManager::CreateLocalImageSession
2023-11-07 14:46:07, Info DISM DISM.EXE:
2023-11-07 14:46:07, Info DISM DISM.EXE: <----- Starting Dism.exe session ----->
2023-11-07 14:46:07, Info DISM DISM.EXE:
2023-11-07 14:46:07, Info DISM DISM.EXE: Host machine information: OS Version=10.0.19045, Running architecture=amd64, Number of processors=8
2023-11-07 14:46:07, Info DISM DISM.EXE: Dism.exe version: 10.0.19041.3570
2023-11-07 14:46:07, Info DISM DISM.EXE: Executing command line: dism /Online /NoRestart /Cleanup-Image /ScanHealth /Logpath:"C:\logs\tron\raw_logs\dism_check.log"
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=2816 TID=1748 Connecting to the provider located at C:\Windows\system32\Dism\FolderProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Manager: PID=2816 TID=1748 physical location path: C:\ - CDISMManager::CreateImageSession
2023-11-07 14:46:07, Info DISM DISM Manager: PID=2816 TID=1748 Event name for current DISM session is Global\{CAC6A17D-8C18-403C-B52D-26E5D187667A} - CDISMManager::CheckSessionAndLock
2023-11-07 14:46:07, Info DISM DISM Manager: PID=2816 TID=1748 Create session event 0x22c for current DISM session and event name is Global\{CAC6A17D-8C18-403C-B52D-26E5D187667A} - CDISMManager::CheckSessionAndLock
2023-11-07 14:46:07, Info DISM DISM Manager: PID=2816 TID=1748 Copying DISM from "C:\Windows\System32\Dism" - CDISMManager::CreateImageSessionFromLocation
2023-11-07 14:46:07, Info DISM DISM Manager: PID=2816 TID=1748 Successfully loaded the ImageSession at "C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1" - CDISMManager::LoadRemoteImageSession
2023-11-07 14:46:07, Info DISM DISM Image Session: PID=1944 TID=2748 Instantiating the Provider Store. - CDISMImageSession::get_ProviderStore
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Initializing a provider store for the IMAGE session type. - CDISMProviderStore::Final_OnConnect
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\OSProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM OS Provider: PID=1944 TID=2748 Defaulting SystemPath to C:\ - CDISMOSServiceManager::Final_OnConnect
2023-11-07 14:46:07, Info DISM DISM OS Provider: PID=1944 TID=2748 Defaulting Windows folder to C:\Windows - CDISMOSServiceManager::Final_OnConnect
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Attempting to initialize the logger from the Image Session. - CDISMProviderStore::Final_OnConnect
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\LogProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Found and Initialized the DISM Logger. - CDISMProviderStore::Internal_InitializeLogger
2023-11-07 14:46:07, Warning DISM DISM Provider Store: PID=1944 TID=2748 Failed to load the provider: C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\PEProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0x8007007e)
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Failed to get and initialize the PE Provider. Continuing by assuming that it is not a WinPE image. - CDISMProviderStore::Final_OnConnect
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Finished initializing the Provider Map. - CDISMProviderStore::Final_OnConnect
2023-11-07 14:46:07, Info DISM Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 14:46:07, Info DISM Initialized Panther logging at C:\logs\tron\raw_logs\dism_check.log
2023-11-07 14:46:07, Info DISM DISM Manager: PID=2816 TID=1748 Image session successfully loaded from the temporary location: C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1 - CDISMManager::CreateImageSession
2023-11-07 14:46:07, Info DISM DISM.EXE: Target image information: OS Version=10.0.19045.3570, Image architecture=amd64
2023-11-07 14:46:07, Info DISM DISM.EXE: Image session version: 10.0.19041.3570
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Getting the collection of providers from an image provider store type. - CDISMProviderStore::GetProviderCollection
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\CbsProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info CSI 00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
2023-11-07 14:46:07, Info CSI 00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS
2023-11-07 14:46:07, Info DISM DISM OS Provider: PID=1944 TID=2748 Determined System directory to be C:\Windows\System32 - CDISMOSServiceManager::get_SystemDirectory
2023-11-07 14:46:07, Info DISM DISM Package Manager: PID=1944 TID=2748 Finished initializing the CbsConUI Handler. - CCbsConUIHandler::Initialize
2023-11-07 14:46:07, Info CSI 00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND

2023-11-07 14:46:07, Info CSI 00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS
2023-11-07 14:46:07, Info DISM DISM Package Manager: PID=1944 TID=2748 CBS is being initialized for online use. More information about CBS actions can be located at: %windir%\logs\cbs\cbs.log - CDISMPackageManager::Initialize
2023-11-07 14:46:07, Info DISM DISM Package Manager: PID=1944 TID=2748 Loaded servicing stack for online use only. - CDISMPackageManager::CreateCbsSession
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\MsiProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\IntlProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\IBSProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\DmiProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info CSI 00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
2023-11-07 14:46:07, Info CSI 00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS
2023-11-07 14:46:07, Info DISM DISM Driver Manager: PID=1944 TID=2748 Further logs for driver related operations can be found in the target operating system at %WINDIR%\inf\setupapi.offline.log - CDriverManager::Initialize
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\UnattendProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\SmiProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Warning DISM DISM Provider Store: PID=1944 TID=2748 Failed to load the provider: C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\EmbeddedProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0x8007007e)
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\AppxProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\ProvProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\AssocProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\GenericProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\OfflineSetupProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\SysprepProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\TransmogProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Transmog Provider: PID=1944 TID=2748 Current image session is [ONLINE] - CTransmogManager::GetMode
2023-11-07 14:46:07, Info DISM DISM Transmog Provider: PID=1944 TID=2748 Audit Mode: [No] - CTransmogManager::Initialize
2023-11-07 14:46:07, Info DISM DISM Transmog Provider: PID=1944 TID=2748 GetProductType: ProductType = [WinNT] - CTransmogManager::GetProductType
2023-11-07 14:46:07, Info DISM DISM Transmog Provider: PID=1944 TID=2748 Product Type: [WinNT] - CTransmogManager::Initialize
2023-11-07 14:46:07, Info DISM DISM Transmog Provider: PID=1944 TID=2748 Product Type ServerNT : [No] - CTransmogManager::Initialize
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\72DE162D-2081-4532-A386-004B1ACEAEF1\SetupPlatformProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM Provider Store: PID=1944 TID=2748 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:46:07, Info DISM DISM.EXE: Got the collection of providers. Now enumerating them to build the command table.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: DISM Log Provider
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: OSServices
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: DISM Package Manager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: DISM Package Manager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: MsiManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: MsiManager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: IntlManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: IntlManager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: IBSManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: DriverManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: DriverManager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: DISM Unattend Manager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: DISM Unattend Manager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: SmiManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: AppxManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: AppxManager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: ProvManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: ProvManager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: AssocManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: AssocManager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: GenericManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: GenericManager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: OfflineSetupManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: OfflineSetupManager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: SysprepManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: SysprepManager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: Edition Manager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: Edition Manager.
2023-11-07 14:46:07, Info DISM DISM.EXE: Attempting to add the commands from provider: SetupPlatformManager
2023-11-07 14:46:07, Info DISM DISM.EXE: Succesfully registered commands for the provider: SetupPlatformManager.
2023-11-07 14:46:07, Info DISM DISM Package Manager: PID=1944 TID=2748 Processing the top level command token(cleanup-image). - CPackageManagerCLIHandler::Private_ValidateCmdLine
2023-11-07 14:46:07, Info DISM DISM Package Manager: PID=1944 TID=2748 Attempting to route to appropriate command handler. - CPackageManagerCLIHandler::ExecuteCmdLine
2023-11-07 14:46:07, Info DISM DISM Package Manager: PID=1944 TID=2748 Routing the command... - CPackageManagerCLIHandler::ExecuteCmdLine
2023-11-07 14:46:07, Info DISM DISM Package Manager: PID=1944 TID=2748 CBS session options=0x100! - CDISMPackageManager::Internal_Finalize
2023-11-07 14:47:54, Info CSI 00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
2023-11-07 14:47:54, Info CSI 00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS

```
2023-11-07 14:47:54, Info                  DISM   DISM Package Manager: PID=1944 TID=2748 Loaded servicing stack for online use only. - CDISMPackageManager::CreateCbsSession
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Found the OSServices.  Waiting to finalize it until all other providers are unloaded. -
CDISMProviderStore::Final_OnDisconnect
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Found the OSServices.  Waiting to finalize it until all other providers are unloaded. -
CDISMProviderStore::Final_OnDisconnect
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Found the PE Provider.  Waiting to finalize it until all other providers are unloaded. -
CDISMProviderStore::Final_OnDisconnect
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(DISM Package Manager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Package Manager: PID=1944 TID=2748 Finalizing CBS core. - CDISMPackageManager::Finalize
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: DISM Package Manager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(MsiManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: MsiManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(IntlManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: IntlManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(IBSManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: IBSManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(DriverManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: DriverManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(DISM Unattend Manager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: DISM Unattend Manager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(SmiManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: SmiManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(AppxManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: AppxManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(ProvManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: ProvManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(AssocManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: AssocManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(GenericManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: GenericManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(OfflineSetupManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: OfflineSetupManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(SysprepManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: SysprepManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(Edition Manager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: Edition Manager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Finalizing the servicing provider(SetupPlatformManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: SetupPlatformManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Releasing the local reference to OSServices. - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Disconnecting Provider: OSServices - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=1944 TID=2748 Releasing the local reference to DISMLogger.  Stop logging. - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Manager: PID=2816 TID=1748 Closing session event handle 0x22c - CDISMManager::CleanupImageSessionEntry
2023-11-07 14:47:54, Info                  DISM   DISM.EXE: Image session has been closed. Reboot required=no.
2023-11-07 14:47:54, Info                  DISM   DISM.EXE:
2023-11-07 14:47:54, Info                  DISM   DISM.EXE: <----- Ending Dism.exe session ----->
2023-11-07 14:47:54, Info                  DISM   DISM.EXE:
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=2816 TID=1748 Found the OSServices.  Waiting to finalize it until all other providers are unloaded. -
CDISMProviderStore::Final_OnDisconnect
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=2816 TID=1748 Disconnecting Provider: FolderManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54, Info                  DISM   DISM Provider Store: PID=2816 TID=1748 Releasing the local reference to DISMLogger.  Stop logging. - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:47:54,53    Done.
2023-11-07 14:47:54,53    Launch job 'System File Checker'...
2023-11-07 14:47:55, Info                  CSI    00000008 [SR] Verifying 100 components
2023-11-07 14:47:55, Info                  CSI    00000009 [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:55, Info                  CSI    0000000a [SR] Verify complete
2023-11-07 14:47:56, Info                  CSI    0000000b [SR] Verifying 100 components
2023-11-07 14:47:56, Info                  CSI    0000000c [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:56, Info                  CSI    0000000d [SR] Verify complete
2023-11-07 14:47:56, Info                  CSI    0000000e [SR] Verifying 100 components
2023-11-07 14:47:56, Info                  CSI    0000000f [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:56, Info                  CSI    00000010 [SR] Verify complete
2023-11-07 14:47:56, Info                  CSI    00000011 [SR] Verifying 100 components
2023-11-07 14:47:56, Info                  CSI    00000012 [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:56, Info                  CSI    00000013 [SR] Verify complete
2023-11-07 14:47:56, Info                  CSI    00000014 [SR] Verifying 100 components
2023-11-07 14:47:56, Info                  CSI    00000015 [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:56, Info                  CSI    00000016 [SR] Verify complete
2023-11-07 14:47:56, Info                  CSI    00000017 [SR] Verifying 100 components
2023-11-07 14:47:56, Info                  CSI    00000018 [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:57, Info                  CSI    00000019 [SR] Verify complete
2023-11-07 14:47:57, Info                  CSI    0000001a [SR] Verifying 100 components
2023-11-07 14:47:57, Info                  CSI    0000001b [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:57, Info                  CSI    0000001c [SR] Verify complete
2023-11-07 14:47:57, Info                  CSI    0000001d [SR] Verifying 100 components
2023-11-07 14:47:57, Info                  CSI    0000001e [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:57, Info                  CSI    0000001f [SR] Verify complete
2023-11-07 14:47:57, Info                  CSI    00000020 [SR] Verifying 100 components
2023-11-07 14:47:57, Info                  CSI    00000021 [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:57, Info                  CSI    00000022 [SR] Verify complete
2023-11-07 14:47:57, Info                  CSI    00000023 [SR] Verifying 100 components
2023-11-07 14:47:57, Info                  CSI    00000024 [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:58, Info                  CSI    00000025 [SR] Verify complete
2023-11-07 14:47:58, Info                  CSI    00000026 [SR] Verifying 100 components
2023-11-07 14:47:58, Info                  CSI    00000027 [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:59, Info                  CSI    00000028 [SR] Verify complete
2023-11-07 14:47:59, Info                  CSI    00000029 [SR] Verifying 100 components
2023-11-07 14:47:59, Info                  CSI    0000002a [SR] Beginning Verify and Repair transaction
2023-11-07 14:47:59, Info                  CSI    0000002b [SR] Verify complete
2023-11-07 14:47:59, Info                  CSI    0000002c [SR] Verifying 100 components
2023-11-07 14:47:59, Info                  CSI    0000002d [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:01, Info                  CSI    0000002e [SR] Verify complete
2023-11-07 14:48:01, Info                  CSI    0000002f [SR] Verifying 100 components
2023-11-07 14:48:01, Info                  CSI    00000030 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:03, Info                  CSI    00000031 [SR] Verify complete
2023-11-07 14:48:03, Info                  CSI    00000032 [SR] Verifying 100 components
2023-11-07 14:48:03, Info                  CSI    00000033 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:09, Info                  CSI    00000034 [SR] Verify complete
2023-11-07 14:48:09, Info                  CSI    00000035 [SR] Verifying 100 components
2023-11-07 14:48:09, Info                  CSI    00000036 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:12, Info                  CSI    00000037 [SR] Verify complete
2023-11-07 14:48:12, Info                  CSI    00000038 [SR] Verifying 100 components
2023-11-07 14:48:12, Info                  CSI    00000039 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:13, Info                  CSI    0000003a [SR] Verify complete
2023-11-07 14:48:13, Info                  CSI    0000003b [SR] Verifying 100 components
2023-11-07 14:48:13, Info                  CSI    0000003c [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:13, Info                  CSI    0000003d [SR] Verify complete
2023-11-07 14:48:13, Info                  CSI    0000003e [SR] Verifying 100 components
2023-11-07 14:48:13, Info                  CSI    0000003f [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:13, Info                  CSI    00000040 [SR] Verify complete
2023-11-07 14:48:13, Info                  CSI    00000041 [SR] Verifying 100 components
2023-11-07 14:48:13, Info                  CSI    00000042 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:14, Info                  CSI    00000043 [SR] Verify complete
2023-11-07 14:48:14, Info                  CSI    00000044 [SR] Verifying 100 components
2023-11-07 14:48:14, Info                  CSI    00000045 [SR] Beginning Verify and Repair transaction
```

2023-11-07 14:48:14, Info CSI 00000046 [SR] Verify complete
2023-11-07 14:48:14, Info CSI 00000047 [SR] Verifying 100 components
2023-11-07 14:48:14, Info CSI 00000048 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:15, Info CSI 00000049 [SR] Verify complete
2023-11-07 14:48:15, Info CSI 0000004a [SR] Verifying 100 components
2023-11-07 14:48:15, Info CSI 0000004b [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:15, Info CSI 0000004c [SR] Verify complete
2023-11-07 14:48:15, Info CSI 0000004d [SR] Verifying 100 components
2023-11-07 14:48:15, Info CSI 0000004e [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:16, Info CSI 0000004f [SR] Verify complete
2023-11-07 14:48:16, Info CSI 00000050 [SR] Verifying 100 components
2023-11-07 14:48:16, Info CSI 00000051 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:17, Info CSI 00000052 [SR] Verify complete
2023-11-07 14:48:17, Info CSI 00000053 [SR] Verifying 100 components
2023-11-07 14:48:17, Info CSI 00000054 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:17, Info CSI 00000055 [SR] Verify complete
2023-11-07 14:48:17, Info CSI 00000056 [SR] Verifying 100 components
2023-11-07 14:48:17, Info CSI 00000057 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:17, Info CSI 00000058 [SR] Verify complete
2023-11-07 14:48:18, Info CSI 00000059 [SR] Verifying 100 components
2023-11-07 14:48:18, Info CSI 0000005a [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:18, Info CSI 0000005b [SR] Verify complete
2023-11-07 14:48:18, Info CSI 0000005c [SR] Verifying 100 components
2023-11-07 14:48:18, Info CSI 0000005d [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:19, Info CSI 0000005e [SR] Verify complete
2023-11-07 14:48:19, Info CSI 0000005f [SR] Verifying 100 components
2023-11-07 14:48:19, Info CSI 00000060 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:19, Info CSI 00000061 [SR] Verify complete
2023-11-07 14:48:19, Info CSI 00000062 [SR] Verifying 100 components
2023-11-07 14:48:19, Info CSI 00000063 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:20, Info CSI 00000064 [SR] Verify complete
2023-11-07 14:48:20, Info CSI 00000065 [SR] Verifying 100 components
2023-11-07 14:48:20, Info CSI 00000066 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:20, Info CSI 00000067 [SR] Verify complete
2023-11-07 14:48:20, Info CSI 00000068 [SR] Verifying 100 components
2023-11-07 14:48:20, Info CSI 00000069 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:21, Info CSI 0000006a [SR] Verify complete
2023-11-07 14:48:21, Info CSI 0000006b [SR] Verifying 100 components
2023-11-07 14:48:21, Info CSI 0000006c [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:21, Info CSI 0000006d [SR] Verify complete
2023-11-07 14:48:21, Info CSI 0000006e [SR] Verifying 100 components
2023-11-07 14:48:21, Info CSI 0000006f [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:22, Info CSI 00000070 [SR] Verify complete
2023-11-07 14:48:22, Info CSI 00000071 [SR] Verifying 100 components
2023-11-07 14:48:22, Info CSI 00000072 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:22, Info CSI 00000073 [SR] Verify complete
2023-11-07 14:48:22, Info CSI 00000074 [SR] Verifying 100 components
2023-11-07 14:48:22, Info CSI 00000075 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:22, Info CSI 00000076 [SR] Verify complete
2023-11-07 14:48:22, Info CSI 00000077 [SR] Verifying 100 components
2023-11-07 14:48:22, Info CSI 00000078 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:23, Info CSI 00000079 [SR] Verify complete
2023-11-07 14:48:23, Info CSI 0000007a [SR] Verifying 100 components
2023-11-07 14:48:23, Info CSI 0000007b [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:23, Info CSI 0000007c [SR] Verify complete
2023-11-07 14:48:23, Info CSI 0000007d [SR] Verifying 100 components
2023-11-07 14:48:23, Info CSI 0000007e [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:24, Info CSI 0000007f [SR] Verify complete
2023-11-07 14:48:24, Info CSI 00000080 [SR] Verifying 100 components
2023-11-07 14:48:24, Info CSI 00000081 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:24, Info CSI 00000082 [SR] Verify complete
2023-11-07 14:48:24, Info CSI 00000083 [SR] Verifying 100 components
2023-11-07 14:48:24, Info CSI 00000084 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:25, Info CSI 00000085 [SR] Verify complete
2023-11-07 14:48:25, Info CSI 00000086 [SR] Verifying 100 components
2023-11-07 14:48:25, Info CSI 00000087 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:26, Info CSI 00000088 [SR] Verify complete
2023-11-07 14:48:26, Info CSI 00000089 [SR] Verifying 100 components
2023-11-07 14:48:26, Info CSI 0000008a [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:27, Info CSI 0000008e [SR] Verify complete
2023-11-07 14:48:27, Info CSI 0000008f [SR] Verifying 100 components
2023-11-07 14:48:27, Info CSI 00000090 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:28, Info CSI 00000091 [SR] Verify complete
2023-11-07 14:48:28, Info CSI 00000092 [SR] Verifying 100 components
2023-11-07 14:48:28, Info CSI 00000093 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:29, Info CSI 00000094 [SR] Verify complete
2023-11-07 14:48:29, Info CSI 00000095 [SR] Verifying 100 components
2023-11-07 14:48:29, Info CSI 00000096 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:29, Info CSI 00000097 [SR] Verify complete
2023-11-07 14:48:30, Info CSI 00000098 [SR] Verifying 100 components
2023-11-07 14:48:30, Info CSI 00000099 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:31, Info CSI 0000009b [SR] Verify complete
2023-11-07 14:48:31, Info CSI 0000009c [SR] Verifying 100 components
2023-11-07 14:48:31, Info CSI 0000009d [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:31, Info CSI 0000009e [SR] Verify complete
2023-11-07 14:48:31, Info CSI 0000009f [SR] Verifying 100 components
2023-11-07 14:48:31, Info CSI 000000a0 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:31, Info CSI 000000a1 [SR] Verify complete
2023-11-07 14:48:31, Info CSI 000000a2 [SR] Verifying 100 components
2023-11-07 14:48:31, Info CSI 000000a3 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:32, Info CSI 000000a4 [SR] Verify complete
2023-11-07 14:48:32, Info CSI 000000a5 [SR] Verifying 100 components
2023-11-07 14:48:32, Info CSI 000000a6 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:32, Info CSI 000000a7 [SR] Verify complete
2023-11-07 14:48:32, Info CSI 000000a8 [SR] Verifying 100 components
2023-11-07 14:48:32, Info CSI 000000a9 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:33, Info CSI 000000aa [SR] Verify complete
2023-11-07 14:48:33, Info CSI 000000ab [SR] Verifying 100 components
2023-11-07 14:48:33, Info CSI 000000ac [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:34, Info CSI 000000ad [SR] Verify complete
2023-11-07 14:48:34, Info CSI 000000ae [SR] Verifying 100 components
2023-11-07 14:48:34, Info CSI 000000af [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:34, Info CSI 000000b0 [SR] Verify complete
2023-11-07 14:48:35, Info CSI 000000b1 [SR] Verifying 100 components
2023-11-07 14:48:35, Info CSI 000000b2 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:35, Info CSI 000000b3 [SR] Verify complete
2023-11-07 14:48:35, Info CSI 000000b4 [SR] Verifying 100 components
2023-11-07 14:48:35, Info CSI 000000b5 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:35, Info CSI 000000b6 [SR] Verify complete
2023-11-07 14:48:35, Info CSI 000000b7 [SR] Verifying 100 components
2023-11-07 14:48:35, Info CSI 000000b8 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:36, Info CSI 000000b9 [SR] Verify complete
2023-11-07 14:48:36, Info CSI 000000ba [SR] Verifying 100 components
2023-11-07 14:48:36, Info CSI 000000bb [SR] Beginning Verify and Repair transaction

2023-11-07 14:48:36, Info CSI 000000bc [SR] Verify complete
2023-11-07 14:48:37, Info CSI 000000bd [SR] Verifying 100 components
2023-11-07 14:48:37, Info CSI 000000be [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:37, Info CSI 000000bf [SR] Verify complete
2023-11-07 14:48:37, Info CSI 000000c0 [SR] Verifying 100 components
2023-11-07 14:48:37, Info CSI 000000c1 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:38, Info CSI 000000c2 [SR] Verify complete
2023-11-07 14:48:38, Info CSI 000000c3 [SR] Verifying 100 components
2023-11-07 14:48:38, Info CSI 000000c4 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:39, Info CSI 000000c5 [SR] Verify complete
2023-11-07 14:48:39, Info CSI 000000c6 [SR] Verifying 100 components
2023-11-07 14:48:39, Info CSI 000000c7 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:39, Info CSI 000000c8 [SR] Verify complete
2023-11-07 14:48:39, Info CSI 000000c9 [SR] Verifying 100 components
2023-11-07 14:48:39, Info CSI 000000ca [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:40, Info CSI 000000cb [SR] Verify complete
2023-11-07 14:48:40, Info CSI 000000cc [SR] Verifying 100 components
2023-11-07 14:48:40, Info CSI 000000cd [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:40, Info CSI 000000ce [SR] Verify complete
2023-11-07 14:48:40, Info CSI 000000cf [SR] Verifying 100 components
2023-11-07 14:48:40, Info CSI 000000d0 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:41, Info CSI 000000d1 [SR] Verify complete
2023-11-07 14:48:41, Info CSI 000000d2 [SR] Verifying 100 components
2023-11-07 14:48:41, Info CSI 000000d3 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:42, Info CSI 000000d4 [SR] Verify complete
2023-11-07 14:48:42, Info CSI 000000d5 [SR] Verifying 100 components
2023-11-07 14:48:42, Info CSI 000000d6 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:42, Info CSI 000000d7 [SR] Verify complete
2023-11-07 14:48:42, Info CSI 000000d8 [SR] Verifying 100 components
2023-11-07 14:48:42, Info CSI 000000d9 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:43, Info CSI 000000da [SR] Verify complete
2023-11-07 14:48:43, Info CSI 000000db [SR] Verifying 100 components
2023-11-07 14:48:43, Info CSI 000000dc [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:43, Info CSI 000000dd [SR] Verify complete
2023-11-07 14:48:43, Info CSI 000000de [SR] Verifying 100 components
2023-11-07 14:48:43, Info CSI 000000df [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:44, Info CSI 000000e0 [SR] Verify complete
2023-11-07 14:48:44, Info CSI 000000e1 [SR] Verifying 100 components
2023-11-07 14:48:44, Info CSI 000000e2 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:44, Info CSI 000000e3 [SR] Verify complete
2023-11-07 14:48:44, Info CSI 000000e4 [SR] Verifying 100 components
2023-11-07 14:48:44, Info CSI 000000e5 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:44, Info CSI 000000e6 [SR] Verify complete
2023-11-07 14:48:45, Info CSI 000000e7 [SR] Verifying 100 components
2023-11-07 14:48:45, Info CSI 000000e8 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:45, Info CSI 000000e9 [SR] Verify complete
2023-11-07 14:48:45, Info CSI 000000ea [SR] Verifying 100 components
2023-11-07 14:48:45, Info CSI 000000eb [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:45, Info CSI 000000ec [SR] Verify complete
2023-11-07 14:48:45, Info CSI 000000ed [SR] Verifying 100 components
2023-11-07 14:48:45, Info CSI 000000ee [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:46, Info CSI 000000ef [SR] Verify complete
2023-11-07 14:48:46, Info CSI 000000f0 [SR] Verifying 100 components
2023-11-07 14:48:46, Info CSI 000000f1 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:47, Info CSI 000000f2 [SR] Verify complete
2023-11-07 14:48:47, Info CSI 000000f3 [SR] Verifying 100 components
2023-11-07 14:48:47, Info CSI 000000f4 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:47, Info CSI 000000f5 [SR] Verify complete
2023-11-07 14:48:47, Info CSI 000000f6 [SR] Verifying 100 components
2023-11-07 14:48:47, Info CSI 000000f7 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:48, Info CSI 000000f8 [SR] Verify complete
2023-11-07 14:48:48, Info CSI 000000f9 [SR] Verifying 100 components
2023-11-07 14:48:48, Info CSI 000000fa [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:49, Info CSI 000000fb [SR] Verify complete
2023-11-07 14:48:49, Info CSI 000000fc [SR] Verifying 100 components
2023-11-07 14:48:49, Info CSI 000000fd [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:49, Info CSI 000000fe [SR] Verify complete
2023-11-07 14:48:49, Info CSI 000000ff [SR] Verifying 100 components
2023-11-07 14:48:49, Info CSI 00000100 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:50, Info CSI 00000104 [SR] Verify complete
2023-11-07 14:48:50, Info CSI 00000105 [SR] Verifying 100 components
2023-11-07 14:48:50, Info CSI 00000106 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:51, Info CSI 00000107 [SR] Verify complete
2023-11-07 14:48:51, Info CSI 00000108 [SR] Verifying 100 components
2023-11-07 14:48:51, Info CSI 00000109 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:51, Info CSI 0000010a [SR] Verify complete
2023-11-07 14:48:51, Info CSI 0000010b [SR] Verifying 100 components
2023-11-07 14:48:51, Info CSI 0000010c [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:52, Info CSI 0000010d [SR] Verify complete
2023-11-07 14:48:52, Info CSI 0000010e [SR] Verifying 100 components
2023-11-07 14:48:52, Info CSI 0000010f [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:53, Info CSI 00000110 [SR] Verify complete
2023-11-07 14:48:53, Info CSI 00000111 [SR] Verifying 100 components
2023-11-07 14:48:53, Info CSI 00000112 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:53, Info CSI 00000113 [SR] Verify complete
2023-11-07 14:48:53, Info CSI 00000114 [SR] Verifying 100 components
2023-11-07 14:48:53, Info CSI 00000115 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:54, Info CSI 00000116 [SR] Verify complete
2023-11-07 14:48:54, Info CSI 00000117 [SR] Verifying 100 components
2023-11-07 14:48:54, Info CSI 00000118 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:54, Info CSI 00000119 [SR] Verify complete
2023-11-07 14:48:55, Info CSI 0000011a [SR] Verifying 100 components
2023-11-07 14:48:55, Info CSI 0000011b [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:55, Info CSI 0000011d [SR] Verify complete
2023-11-07 14:48:55, Info CSI 0000011e [SR] Verifying 100 components
2023-11-07 14:48:55, Info CSI 0000011f [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:56, Info CSI 00000120 [SR] Verify complete
2023-11-07 14:48:56, Info CSI 00000121 [SR] Verifying 100 components
2023-11-07 14:48:56, Info CSI 00000122 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:56, Info CSI 00000123 [SR] Verify complete
2023-11-07 14:48:56, Info CSI 00000124 [SR] Verifying 100 components
2023-11-07 14:48:56, Info CSI 00000125 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:57, Info CSI 00000126 [SR] Verify complete
2023-11-07 14:48:57, Info CSI 00000127 [SR] Verifying 100 components
2023-11-07 14:48:57, Info CSI 00000128 [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:57, Info CSI 00000129 [SR] Verify complete
2023-11-07 14:48:57, Info CSI 0000012a [SR] Verifying 100 components
2023-11-07 14:48:57, Info CSI 0000012b [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:58, Info CSI 0000012c [SR] Verify complete
2023-11-07 14:48:58, Info CSI 0000012d [SR] Verifying 100 components
2023-11-07 14:48:58, Info CSI 0000012e [SR] Beginning Verify and Repair transaction
2023-11-07 14:48:59, Info CSI 0000012f [SR] Verify complete
2023-11-07 14:48:59, Info CSI 00000130 [SR] Verifying 100 components
2023-11-07 14:48:59, Info CSI 00000131 [SR] Beginning Verify and Repair transaction

2023-11-07 14:48:59, Info CSI 00000132 [SR] Verify complete
2023-11-07 14:48:59, Info CSI 00000133 [SR] Verifying 100 components
2023-11-07 14:48:59, Info CSI 00000134 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:00, Info CSI 00000135 [SR] Verify complete
2023-11-07 14:49:00, Info CSI 00000136 [SR] Verifying 100 components
2023-11-07 14:49:00, Info CSI 00000137 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:00, Info CSI 00000138 [SR] Verify complete
2023-11-07 14:49:00, Info CSI 00000139 [SR] Verifying 100 components
2023-11-07 14:49:00, Info CSI 0000013a [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:00, Info CSI 0000013b [SR] Verify complete
2023-11-07 14:49:00, Info CSI 0000013c [SR] Verifying 100 components
2023-11-07 14:49:00, Info CSI 0000013d [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:01, Info CSI 0000013e [SR] Verify complete
2023-11-07 14:49:01, Info CSI 0000013f [SR] Verifying 100 components
2023-11-07 14:49:01, Info CSI 00000140 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:02, Info CSI 00000141 [SR] Verify complete
2023-11-07 14:49:02, Info CSI 00000142 [SR] Verifying 100 components
2023-11-07 14:49:02, Info CSI 00000143 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:02, Info CSI 00000144 [SR] Verify complete
2023-11-07 14:49:02, Info CSI 00000145 [SR] Verifying 100 components
2023-11-07 14:49:02, Info CSI 00000146 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:03, Info CSI 00000147 [SR] Verify complete
2023-11-07 14:49:03, Info CSI 00000148 [SR] Verifying 100 components
2023-11-07 14:49:03, Info CSI 00000149 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:04, Info CSI 0000014a [SR] Verify complete
2023-11-07 14:49:04, Info CSI 0000014b [SR] Verifying 100 components
2023-11-07 14:49:04, Info CSI 0000014c [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:04, Info CSI 0000014d [SR] Verify complete
2023-11-07 14:49:04, Info CSI 0000014e [SR] Verifying 100 components
2023-11-07 14:49:04, Info CSI 0000014f [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:05, Info CSI 00000150 [SR] Verify complete
2023-11-07 14:49:05, Info CSI 00000151 [SR] Verifying 100 components
2023-11-07 14:49:05, Info CSI 00000152 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:05, Info CSI 00000153 [SR] Verify complete
2023-11-07 14:49:05, Info CSI 00000154 [SR] Verifying 100 components
2023-11-07 14:49:05, Info CSI 00000155 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:06, Info CSI 00000156 [SR] Verify complete
2023-11-07 14:49:06, Info CSI 00000157 [SR] Verifying 100 components
2023-11-07 14:49:06, Info CSI 00000158 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:06, Info CSI 00000159 [SR] Verify complete
2023-11-07 14:49:06, Info CSI 0000015a [SR] Verifying 100 components
2023-11-07 14:49:06, Info CSI 0000015b [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:07, Info CSI 0000015c [SR] Verify complete
2023-11-07 14:49:07, Info CSI 0000015d [SR] Verifying 100 components
2023-11-07 14:49:07, Info CSI 0000015e [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:07, Info CSI 0000015f [SR] Verify complete
2023-11-07 14:49:07, Info CSI 00000160 [SR] Verifying 100 components
2023-11-07 14:49:07, Info CSI 00000161 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:08, Info CSI 00000162 [SR] Verify complete
2023-11-07 14:49:08, Info CSI 00000163 [SR] Verifying 100 components
2023-11-07 14:49:08, Info CSI 00000164 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:09, Info CSI 00000165 [SR] Verify complete
2023-11-07 14:49:09, Info CSI 00000166 [SR] Verifying 100 components
2023-11-07 14:49:09, Info CSI 00000167 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:09, Info CSI 00000168 [SR] Verify complete
2023-11-07 14:49:09, Info CSI 00000169 [SR] Verifying 100 components
2023-11-07 14:49:09, Info CSI 0000016a [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:09, Info CSI 0000016b [SR] Verify complete
2023-11-07 14:49:09, Info CSI 0000016c [SR] Verifying 100 components
2023-11-07 14:49:09, Info CSI 0000016d [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:10, Info CSI 0000016e [SR] Verify complete
2023-11-07 14:49:10, Info CSI 0000016f [SR] Verifying 100 components
2023-11-07 14:49:10, Info CSI 00000170 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:10, Info CSI 00000171 [SR] Verify complete
2023-11-07 14:49:10, Info CSI 00000172 [SR] Verifying 100 components
2023-11-07 14:49:10, Info CSI 00000173 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:11, Info CSI 00000174 [SR] Verify complete
2023-11-07 14:49:11, Info CSI 00000175 [SR] Verifying 100 components
2023-11-07 14:49:11, Info CSI 00000176 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:12, Info CSI 00000177 [SR] Verify complete
2023-11-07 14:49:12, Info CSI 00000178 [SR] Verifying 100 components
2023-11-07 14:49:12, Info CSI 00000179 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:12, Info CSI 0000017a [SR] Verify complete
2023-11-07 14:49:12, Info CSI 0000017b [SR] Verifying 100 components
2023-11-07 14:49:12, Info CSI 0000017c [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:13, Info CSI 0000017d [SR] Verify complete
2023-11-07 14:49:13, Info CSI 0000017e [SR] Verifying 100 components
2023-11-07 14:49:13, Info CSI 0000017f [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:13, Info CSI 00000180 [SR] Verify complete
2023-11-07 14:49:13, Info CSI 00000181 [SR] Verifying 100 components
2023-11-07 14:49:13, Info CSI 00000182 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:14, Info CSI 00000183 [SR] Verify complete
2023-11-07 14:49:14, Info CSI 00000184 [SR] Verifying 100 components
2023-11-07 14:49:14, Info CSI 00000185 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:14, Info CSI 00000186 [SR] Verify complete
2023-11-07 14:49:14, Info CSI 00000187 [SR] Verifying 100 components
2023-11-07 14:49:14, Info CSI 00000188 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:15, Info CSI 00000189 [SR] Verify complete
2023-11-07 14:49:15, Info CSI 0000018a [SR] Verifying 100 components
2023-11-07 14:49:15, Info CSI 0000018b [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:15, Info CSI 0000018f [SR] Verify complete
2023-11-07 14:49:16, Info CSI 00000190 [SR] Verifying 100 components
2023-11-07 14:49:16, Info CSI 00000191 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:16, Info CSI 00000192 [SR] Verify complete
2023-11-07 14:49:16, Info CSI 00000193 [SR] Verifying 100 components
2023-11-07 14:49:16, Info CSI 00000194 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:16, Info CSI 00000195 [SR] Verify complete
2023-11-07 14:49:16, Info CSI 00000196 [SR] Verifying 100 components
2023-11-07 14:49:16, Info CSI 00000197 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:17, Info CSI 00000198 [SR] Verify complete
2023-11-07 14:49:17, Info CSI 00000199 [SR] Verifying 100 components
2023-11-07 14:49:17, Info CSI 0000019a [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:17, Info CSI 0000019b [SR] Verify complete
2023-11-07 14:49:17, Info CSI 0000019c [SR] Verifying 100 components
2023-11-07 14:49:17, Info CSI 0000019d [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:18, Info CSI 0000019e [SR] Verify complete
2023-11-07 14:49:18, Info CSI 0000019f [SR] Verifying 100 components
2023-11-07 14:49:18, Info CSI 000001a0 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:18, Info CSI 000001a1 [SR] Verify complete
2023-11-07 14:49:18, Info CSI 000001a2 [SR] Verifying 100 components
2023-11-07 14:49:18, Info CSI 000001a3 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:19, Info CSI 000001a4 [SR] Verify complete
2023-11-07 14:49:19, Info CSI 000001a5 [SR] Verifying 100 components
2023-11-07 14:49:19, Info CSI 000001a6 [SR] Beginning Verify and Repair transaction

2023-11-07 14:49:20, Info CSI 000001a7 [SR] Verify complete
2023-11-07 14:49:20, Info CSI 000001a8 [SR] Verifying 100 components
2023-11-07 14:49:20, Info CSI 000001a9 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:20, Info CSI 000001aa [SR] Verify complete
2023-11-07 14:49:20, Info CSI 000001ab [SR] Verifying 100 components
2023-11-07 14:49:20, Info CSI 000001ac [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:21, Info CSI 000001ad [SR] Verify complete
2023-11-07 14:49:21, Info CSI 000001ae [SR] Verifying 100 components
2023-11-07 14:49:21, Info CSI 000001af [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:22, Info CSI 000001b0 [SR] Verify complete
2023-11-07 14:49:22, Info CSI 000001b1 [SR] Verifying 100 components
2023-11-07 14:49:22, Info CSI 000001b2 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:23, Info CSI 000001b3 [SR] Verify complete
2023-11-07 14:49:23, Info CSI 000001b4 [SR] Verifying 100 components
2023-11-07 14:49:23, Info CSI 000001b5 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:23, Info CSI 000001b6 [SR] Verify complete
2023-11-07 14:49:23, Info CSI 000001b7 [SR] Verifying 100 components
2023-11-07 14:49:23, Info CSI 000001b8 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:24, Info CSI 000001b9 [SR] Verify complete
2023-11-07 14:49:24, Info CSI 000001ba [SR] Verifying 100 components
2023-11-07 14:49:24, Info CSI 000001bb [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:24, Info CSI 000001bc [SR] Verify complete
2023-11-07 14:49:24, Info CSI 000001bd [SR] Verifying 100 components
2023-11-07 14:49:24, Info CSI 000001be [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:25, Info CSI 000001c3 [SR] Verify complete
2023-11-07 14:49:25, Info CSI 000001c4 [SR] Verifying 100 components
2023-11-07 14:49:25, Info CSI 000001c5 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:26, Info CSI 000001c6 [SR] Verify complete
2023-11-07 14:49:26, Info CSI 000001c7 [SR] Verifying 100 components
2023-11-07 14:49:26, Info CSI 000001c8 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:26, Info CSI 000001c9 [SR] Verify complete
2023-11-07 14:49:26, Info CSI 000001ca [SR] Verifying 100 components
2023-11-07 14:49:26, Info CSI 000001cb [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:27, Info CSI 000001cc [SR] Verify complete
2023-11-07 14:49:27, Info CSI 000001cd [SR] Verifying 100 components
2023-11-07 14:49:27, Info CSI 000001ce [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:27, Info CSI 000001cf [SR] Verify complete
2023-11-07 14:49:27, Info CSI 000001d0 [SR] Verifying 100 components
2023-11-07 14:49:27, Info CSI 000001d1 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:28, Info CSI 000001d2 [SR] Verify complete
2023-11-07 14:49:28, Info CSI 000001d3 [SR] Verifying 100 components
2023-11-07 14:49:28, Info CSI 000001d4 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:29, Info CSI 000001d5 [SR] Verify complete
2023-11-07 14:49:29, Info CSI 000001d6 [SR] Verifying 100 components
2023-11-07 14:49:29, Info CSI 000001d7 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:30, Info CSI 000001d8 [SR] Verify complete
2023-11-07 14:49:30, Info CSI 000001d9 [SR] Verifying 100 components
2023-11-07 14:49:30, Info CSI 000001da [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:31, Info CSI 000001db [SR] Verify complete
2023-11-07 14:49:31, Info CSI 000001dc [SR] Verifying 100 components
2023-11-07 14:49:31, Info CSI 000001dd [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:31, Info CSI 000001de [SR] Verify complete
2023-11-07 14:49:31, Info CSI 000001df [SR] Verifying 100 components
2023-11-07 14:49:31, Info CSI 000001e0 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:32, Info CSI 000001e1 [SR] Verify complete
2023-11-07 14:49:32, Info CSI 000001e2 [SR] Verifying 100 components
2023-11-07 14:49:32, Info CSI 000001e3 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:32, Info CSI 000001e4 [SR] Verify complete
2023-11-07 14:49:33, Info CSI 000001e5 [SR] Verifying 100 components
2023-11-07 14:49:33, Info CSI 000001e6 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:33, Info CSI 000001e7 [SR] Verify complete
2023-11-07 14:49:33, Info CSI 000001e8 [SR] Verifying 100 components
2023-11-07 14:49:33, Info CSI 000001e9 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:33, Info CSI 000001ea [SR] Verify complete
2023-11-07 14:49:34, Info CSI 000001eb [SR] Verifying 100 components
2023-11-07 14:49:34, Info CSI 000001ec [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:34, Info CSI 000001ed [SR] Verify complete
2023-11-07 14:49:34, Info CSI 000001ee [SR] Verifying 100 components
2023-11-07 14:49:34, Info CSI 000001ef [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:34, Info CSI 000001f0 [SR] Verify complete
2023-11-07 14:49:34, Info CSI 000001f1 [SR] Verifying 100 components
2023-11-07 14:49:34, Info CSI 000001f2 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:35, Info CSI 000001f3 [SR] Verify complete
2023-11-07 14:49:35, Info CSI 000001f4 [SR] Verifying 100 components
2023-11-07 14:49:35, Info CSI 000001f5 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:36, Info CSI 000001f6 [SR] Verify complete
2023-11-07 14:49:36, Info CSI 000001f7 [SR] Verifying 100 components
2023-11-07 14:49:36, Info CSI 000001f8 [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:36, Info CSI 000001f9 [SR] Verify complete
2023-11-07 14:49:36, Info CSI 000001fa [SR] Verifying 75 components
2023-11-07 14:49:36, Info CSI 000001fb [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:37, Info CSI 000001fc [SR] Verify complete
2023-11-07 14:49:37, Info CSI 000001fd [SR] Repairing 0 components
2023-11-07 14:49:37, Info CSI 000001fe [SR] Beginning Verify and Repair transaction
2023-11-07 14:49:37, Info CSI 000001ff [SR] Repair complete
2023-11-07 14:49:37,58 Done.
2023-11-07 14:49:37,58 Launch job 'chkdsk'...
2023-11-07 14:49:37,58 Checking C: for errors...
2023-11-07 14:49:53,44 No errors found on C:. Skipping full chkdsk at next reboot.
2023-11-07 14:49:53,44 Done.
2023-11-07 14:49:53,44 ! SKIP_TELEMETRY_REMOVAL (-str) set. Disabling instead of removing.
Operace byla dokoncena špesne.
Operace byla dokoncena špesne.
Operace byla dokoncena špesne.
Operace byla dokoncena špesne.
Operace byla dokoncena špesne.
ERROR: Pr˘stup byl odepren.
ERROR: Pr˘stup byl odepren.
Operace byla dokoncena špesne.
Operace byla dokoncena špesne.
Operace byla dokoncena špesne.
Operace byla dokoncena špesne.
Operace byla dokoncena špesne.
2023-11-07 14:49:53,50 Launch job 'Disable silent installation of 3rd-party apps'...
2023-11-07 14:49:53,50 Done.
2023-11-07 14:49:53,50 Launch job 'Disable NVIDIA telemetry'...
2023-11-07 14:49:53,55 Done.
2023-11-07 14:49:53,55 Launch job 'Network repair'...
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
Ok.
Sucessfully reset the Winsock Catalog.
You must restart the computer in order to complete the reset.
2023-11-07 14:49:53,69 Done.

```
2023-11-07 14:49:53,69    Launch job 'Repair file extensions'...
2023-11-07 14:49:53,74    Done.
2023-11-07 14:49:53,74   stage_4_repair complete.
2023-11-07 14:49:53,86   stage_5_patch begin...
2023-11-07 14:49:56,41    7-Zip detected, updating...
2023-11-07 14:49:56,41    Launch job 'Update 7-Zip'...
2023-11-07 14:49:57,58    Done.
2023-11-07 14:49:57,59    Updating Windows Defender...
Signature update started . . .
ERROR: Signature Update failed with hr=80240022
CmdTool: Failed with hr = 0x80240022. Check C:\Users\vboxuser\AppData\Local\Temp\MpCmdRun.log for more information
2023-11-07 14:50:01,30    Done.
2023-11-07 14:50:01,31 !  SKIP_WINDOWS_UPDATES (-swu) set. Skipping all Windows Update methods.
2023-11-07 14:50:01,31    Launch job 'DISM base reset'...
d'»ž2023-11-07 14:50:01, Info                  DISM   PID=1088 TID=3120 Scratch directory set to 'C:\Users\vboxuser\AppData\Local\Temp\'. - CDISMManager::put_ScratchDir
2023-11-07 14:50:01, Info                  DISM   PID=1088 TID=3120 DismCore.dll version: 10.0.19041.3570 - CDISMManager::FinalConstruct
2023-11-07 14:50:01, Info                  DISM   Initialized Panther logging at C:\logs\tron\dism_base_reset.log
2023-11-07 14:50:01, Info                  DISM   PID=1088 TID=3120 Successfully loaded the ImageSession at "C:\Windows\system32\Dism" - CDISMManager::LoadLocalImageSession
2023-11-07 14:50:01, Info                  DISM   Initialized Panther logging at C:\logs\tron\dism_base_reset.log
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=1088 TID=3120 Found and Initialized the DISM Logger. - CDISMProviderStore::Internal_InitializeLogger
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=1088 TID=3120 Failed to get and initialize the PE Provider.  Continuing by assuming that it is not a WinPE image. -
CDISMProviderStore::Final_OnConnect
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=1088 TID=3120 Finished initializing the Provider Map. - CDISMProviderStore::Final_OnConnect
2023-11-07 14:50:01, Info                  DISM   Initialized Panther logging at C:\logs\tron\dism_base_reset.log
2023-11-07 14:50:01, Info                  DISM   DISM Manager: PID=1088 TID=3120 Successfully created the local image session and provider store. - CDISMManager::CreateLocalImageSession
2023-11-07 14:50:01, Info                  DISM   DISM.EXE:
2023-11-07 14:50:01, Info                  DISM   DISM.EXE: <----- Starting Dism.exe session ----->
2023-11-07 14:50:01, Info                  DISM   DISM.EXE:
2023-11-07 14:50:01, Info                  DISM   DISM.EXE: Host machine information: OS Version=10.0.19045, Running architecture=amd64, Number of processors=8
2023-11-07 14:50:01, Info                  DISM   DISM.EXE: Dism.exe version: 10.0.19041.3570
2023-11-07 14:50:01, Info                  DISM   DISM.EXE: Executing command line: Dism  /online /Cleanup-Image /StartComponentCleanup /ResetBase /Logpath:"C:\logs\tron\dism_base_reset.log"
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=1088 TID=3120 Connecting to the provider located at C:\Windows\system32\Dism\FolderProvider.dll. -
CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Manager: PID=1088 TID=3120 physical location path: C:\ - CDISMManager::CreateImageSession
2023-11-07 14:50:01, Info                  DISM   DISM Manager: PID=1088 TID=3120 Event name for current DISM session is Global\{6DCD13BE-8793-47F9-B344-6702F2EE9AB7} -
CDISMManager::CheckSessionAndLock
2023-11-07 14:50:01, Info                  DISM   DISM Manager: PID=1088 TID=3120 Create session event 0x220 for current DISM session and event name is Global\{6DCD13BE-8793-47F9-B344-
6702F2EE9AB7}  - CDISMManager::CheckSessionAndLock
2023-11-07 14:50:01, Info                  DISM   DISM Manager: PID=1088 TID=3120 Copying DISM from "C:\Windows\System32\Dism" - CDISMManager::CreateImageSessionFromLocation
2023-11-07 14:50:01, Info                  DISM   DISM Manager: PID=1088 TID=3120 Successfully loaded the ImageSession at "C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A" - CDISMManager::LoadRemoteImageSession
2023-11-07 14:50:01, Info                  DISM   DISM Image Session: PID=3432 TID=2440 Instantiating the Provider Store. - CDISMImageSession::get_ProviderStore
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Initializing a provider store for the IMAGE session type. - CDISMProviderStore::Final_OnConnect
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\OSProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM OS Provider: PID=3432 TID=2440 Defaulting SystemPath to C:\ - CDISMOSServiceManager::Final_OnConnect
2023-11-07 14:50:01, Info                  DISM   DISM OS Provider: PID=3432 TID=2440 Defaulting Windows folder to C:\Windows - CDISMOSServiceManager::Final_OnConnect
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Attempting to initialize the logger from the Image Session. - CDISMProviderStore::Final_OnConnect
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\LogProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   Initialized Panther logging at C:\logs\tron\dism_base_reset.log
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Found and Initialized the DISM Logger. - CDISMProviderStore::Internal_InitializeLogger
2023-11-07 14:50:01, Warning               DISM   DISM Provider Store: PID=3432 TID=2440 Failed to load the provider: C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\PEProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0x8007007e)
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Failed to get and initialize the PE Provider.  Continuing by assuming that it is not a WinPE image. -
CDISMProviderStore::Final_OnConnect
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Finished initializing the Provider Map. - CDISMProviderStore::Final_OnConnect
2023-11-07 14:50:01, Info                  DISM   Initialized Panther logging at C:\logs\tron\dism_base_reset.log
2023-11-07 14:50:01, Info                  DISM   Initialized Panther logging at C:\logs\tron\dism_base_reset.log
2023-11-07 14:50:01, Info                  DISM   DISM Manager: PID=1088 TID=3120 Image session successfully loaded from the temporary location: C:\Users\vboxuser\AppData\Local\Temp\27321D39-
47C8-4A86-AD29-C00BEBEC602A - CDISMManager::CreateImageSession
2023-11-07 14:50:01, Info                  DISM   DISM.EXE: Target image information: OS Version=10.0.19045.3570, Image architecture=amd64
2023-11-07 14:50:01, Info                  DISM   DISM.EXE: Image session version: 10.0.19041.3570
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Getting the collection of providers from an image provider store type. -
CDISMProviderStore::GetProviderCollection
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\CbsProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. -
CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  CSI    00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
2023-11-07 14:50:01, Info                  CSI    00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS
2023-11-07 14:50:01, Info                  DISM   DISM OS Provider: PID=3432 TID=2440 Determined System directory to be C:\Windows\System32 - CDISMOSServiceManager::get_SystemDirectory
2023-11-07 14:50:01, Info                  DISM   DISM Package Manager: PID=3432 TID=2440 Finished initializing the CbsConUI Handler. - CCbsConUIHandler::Initialize
2023-11-07 14:50:01, Info                  CSI    00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
2023-11-07 14:50:01, Info                  CSI    00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS
2023-11-07 14:50:01, Info                  DISM   DISM Package Manager: PID=3432 TID=2440 CBS is being initialized for online use. More information about CBS actions can be located at:
%windir%\logs\cbs\cbs.log - CDISMPackageManager::Initialize
2023-11-07 14:50:01, Info                  DISM   DISM Package Manager: PID=3432 TID=2440 Loaded servicing stack for online use only. - CDISMPackageManager::CreateCbsSession
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\MsiProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. -
CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\IntlProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. -
CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\IBSProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. -
CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\DmiProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. -
CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  CSI    00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
2023-11-07 14:50:01, Info                  CSI    00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS
2023-11-07 14:50:01, Info                  DISM   DISM Driver Manager: PID=3432 TID=2440 Further logs for driver related operations can be found in the target operating system at
%WINDIR%\inf\setupapi.offline.log - CDriverManager::Initialize
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\UnattendProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. -
CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\SmiProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. -
CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Warning               DISM   DISM Provider Store: PID=3432 TID=2440 Failed to load the provider: C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-
C00BEBEC602A\EmbeddedProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0x8007007e)
```

2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-C00BEBEC602A\AppxProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-C00BEBEC602A\ProvProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-C00BEBEC602A\AssocProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-C00BEBEC602A\GenericProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-C00BEBEC602A\OfflineSetupProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-C00BEBEC602A\SysprepProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-C00BEBEC602A\TransmogProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Transmog Provider: PID=3432 TID=2440 Current image session is [ONLINE] - CTransmogManager::GetMode
2023-11-07 14:50:01, Info DISM DISM Transmog Provider: PID=3432 TID=2440 Audit Mode: [No] - CTransmogManager::Initialize
2023-11-07 14:50:01, Info DISM DISM Transmog Provider: PID=3432 TID=2440 GetProductType: ProductType = [WinNT] - CTransmogManager::GetProductType
2023-11-07 14:50:01, Info DISM DISM Transmog Provider: PID=3432 TID=2440 Product Type: [WinNT] - CTransmogManager::Initialize
2023-11-07 14:50:01, Info DISM DISM Transmog Provider: PID=3432 TID=2440 Product Type ServerNT : [No] - CTransmogManager::Initialize
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Connecting to the provider located at C:\Users\vboxuser\AppData\Local\Temp\27321D39-47C8-4A86-AD29-C00BEBEC602A\SetupPlatformProvider.dll. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Encountered a servicing provider, performing additional servicing initializations. - CDISMProviderStore::Internal_LoadProvider
2023-11-07 14:50:01, Info DISM DISM.EXE: Got the collection of providers. Now enumerating them to build the command table.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: DISM Log Provider
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: OSServices
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: DISM Package Manager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: DISM Package Manager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: MsiManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: MsiManager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: IntlManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: IntlManager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: IBSManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: DriverManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: DriverManager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: DISM Unattend Manager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: DISM Unattend Manager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: SmiManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: AppxManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: AppxManager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: ProvManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: ProvManager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: AssocManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: AssocManager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: GenericManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: GenericManager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: OfflineSetupManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: OfflineSetupManager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: SysprepManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: SysprepManager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: Edition Manager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: Edition Manager.
2023-11-07 14:50:01, Info DISM DISM.EXE: Attempting to add the commands from provider: SetupPlatformManager
2023-11-07 14:50:01, Info DISM DISM.EXE: Succesfully registered commands for the provider: SetupPlatformManager.
2023-11-07 14:50:01, Info DISM DISM Package Manager: PID=3432 TID=2440 Processing the top level command token(cleanup-image). - CPackageManagerCLIHandler::Private_ValidateCmdLine
2023-11-07 14:50:01, Info DISM DISM Package Manager: PID=3432 TID=2440 Attempting to route to appropriate command handler. - CPackageManagerCLIHandler::ExecuteCmdLine
2023-11-07 14:50:01, Info DISM DISM Package Manager: PID=3432 TID=2440 Routing the command... - CPackageManagerCLIHandler::ExecuteCmdLine
2023-11-07 14:50:01, Info DISM DISM Package Manager: PID=3432 TID=2440 CBS session options=0x10400100! - CDISMPackageManager::Internal_Finalize
2023-11-07 14:50:01, Info CSI 00000001 Shim considered [l:126]'\??\C:\Windows\Servicing\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_OBJECT_PATH_NOT_FOUND
2023-11-07 14:50:01, Info CSI 00000002 Shim considered [l:123]'\??\C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3562_none_7e0523f67c93b82a\wcp.dll' : got STATUS_SUCCESS
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Found the OSServices. Waiting to finalize it until all other providers are unloaded. - CDISMProviderStore::Final_OnDisconnect
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Found the OSServices. Waiting to finalize it until all other providers are unloaded. - CDISMProviderStore::Final_OnDisconnect
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Found the PE Provider. Waiting to finalize it until all other providers are unloaded. - CDISMProviderStore::Final_OnDisconnect
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(DISM Package Manager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Package Manager: PID=3432 TID=2440 Finalizing CBS core. - CDISMPackageManager::Finalize
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: DISM Package Manager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(MsiManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: MsiManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(IntlManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: IntlManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(IBSManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: IBSManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(DriverManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: DriverManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(DISM Unattend Manager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: DISM Unattend Manager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(SmiManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: SmiManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(AppxManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: AppxManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(ProvManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: ProvManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(AssocManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: AssocManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(GenericManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: GenericManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(OfflineSetupManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: OfflineSetupManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(SysprepManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: SysprepManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(Edition Manager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: Edition Manager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Finalizing the servicing provider(SetupPlatformManager) - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info DISM DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: SetupPlatformManager - CDISMProviderStore::Internal_DisconnectProvider

```
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Releasing the local reference to OSServices. - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Disconnecting Provider: OSServices - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=3432 TID=2440 Releasing the local reference to DISMLogger.  Stop logging. - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info                  DISM   DISM Manager: PID=1088 TID=3120 Closing session event handle 0x220 - CDISMManager::CleanupImageSessionEntry
2023-11-07 14:50:01, Info                  DISM   DISM.EXE: Image session has been closed. Reboot required=no.
2023-11-07 14:50:01, Info                  DISM   DISM.EXE:
2023-11-07 14:50:01, Info                  DISM   DISM.EXE: <----- Ending Dism.exe session ----->
2023-11-07 14:50:01, Info                  DISM   DISM.EXE:
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=1088 TID=3120 Found the OSServices.  Waiting to finalize it until all other providers are unloaded. -
CDISMProviderStore::Final_OnDisconnect
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=1088 TID=3120 Disconnecting Provider: FolderManager - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01, Info                  DISM   DISM Provider Store: PID=1088 TID=3120 Releasing the local reference to DISMLogger.  Stop logging. - CDISMProviderStore::Internal_DisconnectProvider
2023-11-07 14:50:01,77    Done.
2023-11-07 14:50:01,78   stage_5_patch complete.
2023-11-07 14:50:01,78   stage_6_optimize begin...
2023-11-07 14:50:01,78    Resetting page file settings to Windows defaults...
Updating property(s) of '\\VMTESTINGENVIRO\ROOT\CIMV2:Win32_ComputerSystem.Name="VMTESTINGENVIRO"'
Property(s) update successful.
2023-11-07 14:50:01,81    Done.
2023-11-07 14:50:01,83    Launch job 'ngen .NET compilation'...
Microsoft (R) CLR Native Image Generator - Version 4.8.9093.0
Copyright (c) Microsoft Corporation.  All rights reserved.
All compilation targets are up to date.
2023-11-07 14:50:01,84    Done.
2023-11-07 14:50:01,84    Virtual Machine detected. Skipping defrag of C:.
2023-11-07 14:50:01,84   stage_6_optimize complete.
2023-11-07 14:50:01,86   stage_7_wrap-up begin...
2023-11-07 14:50:01,86 !  PRESERVE_POWER_SCHEME (-p) set to "yes", skipping power settings reset.
2023-11-07 14:50:01,86    Calculating post-run results for summary logs...
2023-11-07 14:50:17,51    Done. Summary logs are at "C:\logs\tron\summary_logs\"
2023-11-07 14:50:17,51    Saving misc logs to "C:\logs\tron\raw_logs\"...
2023-11-07 14:50:17,51    Done.
2023-11-07 14:50:17,51    Uninstalling Malwarebytes...
2023-11-07 14:50:17,51    Done.
2023-11-07 14:50:17,53   stage_7_wrap-up complete.
2023-11-07 14:50:17,53 ! SKIP_CUSTOM_SCRIPTS (-scs) set to "yes", skipping...
2023-11-07 14:50:17,54    Doing miscellaneous clean up...
2023-11-07 14:50:17,56    Done.
2023-11-07 14:50:17,57   TRON RUN COMPLETE. Use \resources\stage_9_manual_tools if further action is required.
2023-11-07 14:50:17,57   Auto-reboot (-r) not selected. Reboot as soon as possible.
2023-11-07 14:50:17,64 ! WARNINGS were detected (yes_check_update_skipped). Recommend reviewing the log file.
--------------------------------------------------------------------------------
 Tron v12.0.6 (2023-10-17) complete
                Windows 10 Home (AMD64)
                Executed as VMTESTINGENVIRO\vboxuser on VMTESTINGENVIRO
                Command-line switches:
                Time zone: Stredn˜ Evropa (bezny cas)
                Safe Mode: yes NETWORK
                Logfile: C:\logs\tron\tron.log
                Warnings detected?:   yes_check_update_skipped
                Debug logs uploaded?: no
                Free space before Tron run: 39 MB
                Free space after Tron run:  41 MB
                Disk space reclaimed:       2 MB *
   * If you see negative disk space don't panic. Due to how some of Tron's
     functions work, actual space reclaimed will not be visible until after
     a reboot.
--------------------------------------------------------------------------------
```

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2021/2022

Studijní program: Aplikovaná informatika
Forma studia: Prezenční
Obor/kombinace: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení:	**Jiří Hladík**
Osobní číslo:	**I1900184**
Adresa:	Nerudova 1101, Kostelec nad Orlicí, 51741 Kostelec nad Orlicí, Česká republika
Téma práce:	Analýza nástrojů pro automatizovanou analýzu a ošetření operačního systému Windows v případě napadení malware
Téma práce anglicky:	Analysis of tools for automated logging and treatment of the Windows operating system in case of malware infection
Jazyk práce:	Čeština
Vedoucí práce:	Ing. Tomáš Svoboda, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Cílem práce je provést analýzu současného stavu využívání serverových a desktopových operačních systémů rodiny Microsoft Windows. V teoretické části budou popsány operační systémy Windows, kybernetické hrozby a typy kybernetických útoků s důrazem na možnosti obrany proti napadení systému. V praktické části autor demonstruje použití nástrojů a postupy pro automatizovanou analýzu a ošetření operačního systému Windows v případě napadení malware.

Seznam doporučené literatury:

BETTANY, Andrew a Mike HALSEY. *Windows Virus and Malware Troubleshooting* [online]. Berkeley, CA: Apress, 2017 [cit. 2022-03-17]. ISBN 978-1-4842-2606-3. Dostupné z: doi:10.1007/978-1-4842-2607-0

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: