Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Ochrana výpočetní techniky před viry

Petr Javorovský

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Petr Javorovský

Informatika

Název práce

Ochrana výpočetní techniky před viry

Název anglicky

Protecting Information Technology before viruses.

Cíle práce

Cílem bakalářské práce je na základě zpracované literární rešerše, navrhnout a analyzovat ochranu výpočetní techniky v operačních systémech Windows před nežádoucími útoky počítačových virů a navrhnout řešení pro zvýšení bezpečnosti.

Metodika

Metodika bakalářské práce zahrnuje ve své teoretické části studium odborné literatury, aktuálních vědeckých článků a zdrojů na internetu a to jak českých, tak i světových. V analytické části práce bude zpracována historie a typy virů, detekce virů a srovnání vybraných typů antivirů. Výsledky, zpracované analýzy budou využity pro návrh možné ochrany informačních a komunikačních technologií.

Doporučený rozsah práce

60 stran

Klíčová slova

Bezpečnost, viry, útoky, antiviry, výpočetní technika, ochrana, detekce

---

Doporučené zdroje informací

BAUDIŠ, P. – ZELENKA, J. *Antivirová ochrana*. Praha: Plus, 1996. ISBN 80-85297-74-4.

Comodo. Dostupné z WWW https://www.comodo.com

Čepský Pavel Antiviry online: Hodně muziky za málo peněz? Dostupné z WWW http://www.lupa.cz/clanky/antiviry-online-hodne-muziky-za-malo-penez/

Eset. Dostupné z WWW http://www.eset.com

Heineige, Karel. Viry a počítače. Praha: Mobil Media, 2001. ISBN 80-86593-02-9

Jalůvka, Josef. Moderní počítačové viry: podstata, prevence, ochrana. 2. aktualizované vydání. Praha: Computer Press, 2000. ISBN 80-7226-402-8

Kubeš Radek. Pět nejlepších antivirů, které jsou zdarma. Dostupné z WWW http://technet.idnes.cz/pet-nejlepsich-antiviru-ktere-jsou-zdarma-fis-/software.aspx?c=A090124_225810_software_vse

Microsotf. Tipy pro ochranu počítače před viry. Dostupné z WWW http://windows.microsoft.com/cs-cz/windows7/tips-for-protecting-your-computer-from-viruses

Požár, Josef. Základy teorie informační bezpečnosti. 1. vydání. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8

Szor, Peter. Počítačové viry: analýza útoku a obrana. 1. vydání. Brno: Zoner Press, 2006. ISBN 80-86815-04-8

Předběžný termín obhajoby

2017/18 ZS – PEF (únor 2018)

Vedoucí práce

Ing. Edita Šilerová, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 8. 3. 2017

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 8. 3. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 05. 11. 2017

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Ochrana výpočetní techniky před viry" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29.11.2017 _____

Poděkování

Rád bych touto cestou poděkoval vedoucí mé bakalářské práce, Ing. Editě Šilerové za její cenné rady, věcné připomínky a vstřícnost při zpracování této bakalářské práce.

Ochrana výpočetní techniky před viry

Abstrakt

Tato bakalářská práce má pomocí svého obsahu uživatele přesvědčit o tom, proč by neměl ochranu výpočetní techniky brát na lehkou váhu. Na začátku je vysvětleno, co je to počítačový virus a na jaké skupiny ho rozdělujeme. U jednotlivých skupin se pak uživatel seznámí s tím, jak se tyto jednotlivé viry šíří, kde mohou být obsaženy a co mu mohou způsobit. V dalších kapitolách jsou pak vyjmenované dnes nejčastěji používané typy virů, po kterých následuje kapitola prevence před nakažením. V praktické části, která navazuje na kapitolu prevence před nakažením, jsou porovnány různé programy pro ochranu výpočetní techniky.

Klíčová slova: bezpečnost, viry, útoky, antiviry, výpočetní technika, ochrana, detekce

Protecting information technology from viruses.

Abstract

This bachelor thesis is aiming to convince its reader not to underestimate safety of information technology and consider using protection. At the beginning it is explained, what is computer virus and what groups are divided. After that there is a description of each group, how they infect, where they can be located and what they could do. In the next chapters there are named most used types of viruses and how to prevent infection. In the practical part, there is comparison of programs for protection of information technology.

Keywords: security, viruses, attacks, anti-viruses, information technology, protection, detection

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Od doby, kdy vznikl první osobní počítač, uběhlo již přes více než 30 let. Za tuto dobu se počítače staly nejen velice populárními a žádanějšími, ale i o dost technologicky vyspělejšími. Bohužel se však spolu s rozvojem a oblíbeností výpočetní techniky, která je dnes na jiné (vyspělejší) technické úrovni než před 30 lety, začaly objevovat také první počítačové viry, tedy škodlivé programy a kódy, které mají za úkol znepříjemňovat a znesnadňovat práci s výpočetní technikou.

Tyto viry byly z počátku vytvářeny jako neškodné vtipy programátorů a uměly jen pouze zobrazovat nežádoucí či blikající text, nebo dokázaly obracet obrazovku. S postupem času však lidé (útočníci) začaly viry zdokonalovat a využívat je jako nebezpečné nástroje, které mohly mít za následek i nefunkčnost celého systému. Dnes se viry především používají k zašifrování pevného disku či dat a k získání osobních údajů, hesel apod. Díky tomu si potom útočník může přijít i k nemalé finanční částce.

Naštěstí spolu s rozvojem výpočetní techniky a těchto nebezpečných kódů, začaly vznikat i takzvané antivirové programy, které mají zajistit ochranu před těmito nebezpečnými kódy (viry).

Dnes však řada uživatelů nevěnuje ochraně a ani těmto programům moc velkou pozornost. Někteří z nich ani nevědí, k čemu takovéto programy slouží a zda je vůbec mají nainstalované na jejich osobním počítači, nehledě na to, zda fungují či nikoliv.

Pro takovéto uživatele však představují tyto škodlivé kódy značnou míru potencionálního nebezpečí. Mnoho z nich si však toto nebezpečí ani neuvědomuje, a vystavují jak sebe, tak i výpočetní techniku bezpečnostnímu riziku, které tyto nebezpečné kódy přinášejí.

Proto bych se tomuto tématu rád věnoval na dalších stránkách podrobněji, a zdůraznil, jak je ochrana výpočetní techniky důležitá, nejen pro obyčejné uživatele.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem bakalářské práce je na základě zpracované literární rešerše, navrhnout a analyzovat ochranu výpočetní techniky v operačních systémech Windows před nežádoucími útoky počítačových virů a navrhnout řešení pro zvýšení bezpečnosti.

2.2 Metodika

Metodika bakalářské práce zahrnuje ve své teoretické části studium odborné literatury, aktuálních vědeckých článků a zdrojů z internetu, a to jak českých, tak i světových. V analytické části bude zpracována historie a typy virů, detekce virů, a srovnání vybraných typů antivirů. Výsledky zpracované analýzy budou využity pro návrh možné ochrany informačních a komunikačních technologií.

3 Teoretická východiska

3.1 Co je to počítačový virus

Pojem počítačový virus se do povědomí lidí nejvíce zapsal jako veškerá škodlivá havěť, která napadá jejich počítače, znesnadňuje jim práci, či jim škodí nějak jinak, a to bez ohledu na to, zda se jedná o vir, trojského koně, červa nebo o speciální typ této škodlivé havěti. Takováto škodlivá havěť potom představuje nebezpečné kódy či programy, které se šíří pomocí různých metod a které v sobě ukrývají mnoho nebezpečných vlastností. Takovou to škodlivou havěť pak označujeme jedním slovem jako **Malware**[1]. Ten v sobě ukrývá nebezpečné vlastnosti, které při spuštění nebezpečného kódu či programu mohou způsobit: poškození počítače a informací v něm uložených, krádež přihlašovacích údajů a hesel, zasílání spamu, mazání a přepisování souborů, získání plné kontroly nad napadeným počítačem, zobrazování různého textu, nebo zašifrování souborů či zablokování přístupu do počítače. Každý škodlivý kód či program potom v sobě může ukrývat výše zmíněné vlastnosti, a to včetně jejich kombinací.

Obrázek 1 – Malware. [3]

Škodlivé kódy a programy se ale dají také používat k odposlouchávání či sledování uživatelů, viz případ ze začátku čtvrtletí roku 2017, kdy byly z CIA (Central Intelligence Agency) ukradeny a zveřejněny přísně tajné informace o tom, že tato špionážní služba mimo jiné používá sadu nástrojů, které slouží pro tvorbu malwaru na míru v operačních systémech Windows. Pomocí nich potom měla CIA údajně odposlouchávat a sledovat některé potencionálně nebezpečné uživatele.

Tato část je zpracovaná podle [1] a [2].

[1] Zkratka od anglického spojení **Mal**icious Soft**ware** - tedy zákeřný či škodlivý program.

3.2 Základní dělení malwaru

Jak již bylo zmíněno, malwarem označujeme skupinu nebezpečných kódů a programů, do kterých spadají viry, trojské koně, červi a speciální případy škodlivých kódů.

Škodlivé kódy a programy dále můžeme rozdělit do jakých si podkategorií, například podle toho, zda dokáží jen upravovat či mazat soubory, zda si dokáží uchovat a odeslat přihlašovací údaje (jména a hesla) útočníkovi, zda dokáží zašifrovat data, či umožňují plnou kontrolu nad napadeným počítačem apod.

Vlastnosti škodlivých kódů a programů se však mohou navzájem kombinovat a nelze je tedy jednoduše přesně zařadit. To, co například dokáže vir, může dokázat také trojský kůň či červ nebo naopak. Následující dělení je tedy jen z jednou mnoha variant.

3.2.1 Viry

Název počítačových virů je odvozen díky jistým podobnostem s biologickými viry. Tak jako se biologické viry dokáží šířit vkládáním svého kódu do živých buněk, počítačové viry se šíří vkládáním svého kódu do jiných spustitelných souborů či dokumentů. Tím postupně infikují všechny spustitelné soubory a dokumenty, se kterými potom uživatel ztratí možnost pracovat. Počítačový virus je tedy schopen sebe-replikace neboli množení sebe sama, které probíhá za přítomnosti vykonatelného hostitele (soubory, dokumenty) a to bez vědomí uživatele. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel.

Jak již bylo řečeno, počítačové viry se ukrývají ve spustitelných souborech, které představují sadu dat, jenž ve většině případů, umožňují uživateli manipulaci s programem. Může se například jednat o program pro úpravu fotek či videí, ale i o počítačovou hru. Jelikož je nebezpečný kód uložen v těle samotného programu (kódu), tak není skoro možné nebezpečný program rozeznat. Program se uživateli může i normálně spustit a pracovat tak, jako pracoval před nakažením. Při spuštění napadeného programu se však spustí i virus, který v sobě tento program ukrýval a začne dělat neplechu. Může například začít upravovat či mazat soubory, nebo v horším případě může mít za následek i znemožnění startu systému počítače.

Viry však nenapadají a nejsou obsaženy jen ve spustitelných souborech ale i dokumentech. Především se jedná o dokumenty programu Microsoft Office, což je kancelářský nástroj, který slouží pro tvorbu prezentací, tabulek, databází a psaní různých textů (bakalářských prací, smluv apod.). Tento program má v sobě zakomponované tzv.

makra, což je jaký si podprogram, tedy sled příkazů, který slouží pro ulehčení práce s těmito kancelářskými nástroji. Tento sled příkazů se dá však upravit i do formy nebezpečného kódu, který se při spuštění napadeného dokumentu spustí. Nebezpečná makra pak mohou například použít kameru na PC ke sledování uživatele, zpřístupňovat historii prohlížeče či zajistit přístup k heslům a šifrovacím klíčům.

Tato část je zpracována podle [2], [4] a [5].

3.2.2 Trojské koně

Trojské koně dostaly označení podle staré řecké báje o starověkém městě Trója, které se Řekové marně snažili dobýt. Za hradby tohoto města se jim však 9 let nepodařilo dostat, a proto vymysleli lest v podobě dřevěného koně, do kterého se ukryli. Po ukrytí v tomto dřevěném koni pak čekali a doufali, že si ho Trojané vezmou za své hradby. Jelikož Trojané žili v domnění, že se jedná o dar, vzali si tohoto koně skutečně za hradby a Řekové ještě večer toho dne mohli využít moment překvapení a město dobýt.

Na tomto principu tedy pracuje i typ škodlivého kódu typu trojské koně. Nemaskuje se však za dřevěného koně, ale za užitečný program, který má uživateli usnadňovat či jinak pomáhat s prací ve výpočetní technice. Pokud pak takovýto program v sobě ukrývá trojského koně a uživatel jej spustí, spustí spolu s ním i škodlivý kód v něm ukrytý. O tomto škodlivém kódu pak uživatel nemusí ani vědět – pokud ho tedy předtím neupozorní jeho antivirový program. Aby takovéto nebezpečné programy nebyly snadno rozeznatelné, přidávají do svého obsahu loga známých firem (Microsoft, Eset, Adobe apod.), pomocí kterých se pak snaží maskovat. Uživatele to tedy potom může lehce zmást a může si skutečně myslet, že se jedná o software těchto důvěryhodných firem.

Trojský kůň se však nemusí ukrývat pouze v programech, ale stejně tak i jako viry se může ukrývat v dokumentech. Škodlivý kód, který je pak ukrytý v takto napadeném programu či dokumentu, v sobě může obsahovat obdobné nebezpečné charakteristiky jako viry. To znamená, že třetí strana může získat třeba čísla kreditních karet, přihlašovací jména a hesla, či jiné osobní údaje. Trojský kůň pak stejně jako viry, dokáže mazat obsah pevných disků, vypínat antivirový program, nebo může umožnit útočníkovi aktivovat vlastní komponenty a tím mu zajistit vzdálený přístup k počítači.

Oproti virům se však trojské koně nedokázali dlouhou dobu šířit sami. To znamená, že pokud byl napadený dokument či program spuštěn, škodlivý kód se spustil bez následku toho, že by se sám replikoval i do dalších jiných dokumentů či programů. Dnes se však již

objevují i sofistikovanější verze trojských koňů, kteří v sobě ukrývají další komponenty pro možnosti jejich šíření.

Trojské koně můžeme na základě jejich charakteristik dále rozdělit na: password-stealing koně, destruktivní koně, backdoor koně a downloader koně.

Tato část je zpracována podle [6] a [7].

3.2.2.1 Password - stealing koně

Tato skupina trojských koní sleduje jednotlivé stisky kláves (key-loggers), které uživatel zadává. Ty se potom skládají z písmen a čísel, které si tento škodlivý kód uloží a odešle je na předem danou e-mailovou adresu, která patří tvůrci tohoto škodlivého kódu. Díky této technice potom útočník může získat například přihlašovací údaje (do e-mailů, bankovnictví, sociálních sítí, síťových uložišť atd.), kopie odeslaných zpráv, seznam navštívených webových stránek, a zkrátka vše, co uživatel zadá na klávesnici. Pomocí těchto získaných údajů, poté může útočník získat například finanční obnosy, osobní údaje, a také pomocí nich může odesílat třeba další škodlivé dokumenty, čímž je může šířit dále. Tyto odcizené informace však nemusí posloužit pouze útočníkovi. Odcizené informace se dají také prodat na černém trhu, čímž útočník může získat i nemalou finanční částku.

Tato část byla zpracována podle [2] a [8].

3.2.2.2 Destruktivní koně

Tento typ trojských koní se zaměřuje na vymazávání a přepisování dat, která jsou uložena na pevném disku a která mohou být dále uložena na jiných paměťových zařízeních (USB Flash disk, externí HDD, síťový disk apod.).

Destruktivní trojský kůň pak v tom nejhorším případě dokáže klidně vymazat i veškerá uložená data, která se nachází na pevném disku, čímž může způsobit i nemožnost startu operačního systému. V lepším případě dokáže „pouze“ vymazat či upravit soubory, čímž je znehodnotí a nedají se tak použít pro další práci. Pokud je tedy takovýto trojský kůň spuštěn, uživatel může přijít i o velice cenná data. Na druhou stranu, se tento typ trojských koňů dá poměrně lehce rozeznat – pokud si tedy uživatel včas všimne, že mu sami od sebe mizí soubory či mu sami od sebe mění svůj obsah.

Tato část byla zpracována podle [9].

3.2.2.3 Backdoor koně

Backdoor trojské koně poskytují tvůrci škodlivého kódu vzdálený přístup k napadenému počítači. To znamená, že pokud je počítač napaden tímto koněm, útočník se na něj může skrze počítačovou síť vzdáleně připojit a zcela ho neoprávněně ovládat, a to až na vzdálenost několika stovek kilometrů. Na takto napadeném počítači může poté například sledovat to, co uživatel právě dělá, provádět operace s jeho soubory (mazat, upravovat, přeposílat), instalovat další škodlivé kódy apod.

Backdoor trojské koně pak ve svém těle (kódu) často obsahují také přídavné komponenty, jako jsou programy na rozpoznání stisku kláves (key-loggers), nebo škodlivé kódy, které jsou určeny pro poškození či zašifrování souborů nebo celého disku. Tím pak uživatel přijde o možnost práce s těmito daty či o úplný přístup do systému.

Tato část byla zpracována podle [2] a [10].

3.2.2.4 Downloader koně

Downloader trojské koně májí ve svém těle ukrytou cestu na vzdálený server. Pokud se tedy počítač, který byl napadený tímto trojským koněm, připojí k internetu, začne tento kůň stahovat další nebezpečné kódy, které jsou uloženy na tomto serveru. K tomuto serveru má potom přístup i útočník, který tento škodlivý kód vytvořil. Může tedy nebezpečné kódy poměrně snadno upravovat, a to bez ohledu na to, že by si toho uživatel byl vědom. Pomocí downloader trojského koně pak tyto kódy může nadále stahovat do napadeného počítače a tím na něm způsobovat ještě větší neplechu.

Tato část byla zpracována podle [11] a [12].

3.2.3 Červi

Červi jsou díky svému chování velmi podobní virům. Oproti virům však nešíří své kopie pomocí spustitelných souborů či dokumentů, ale prostřednictvím počítačové sítě, a to ve formě síťových paketů[2]. Aby mohli sebe sama přenést až do cílového (napadnutelného) počítače, využívají bezpečnostních děr operačních systémů, programů a kódů. Tyto bezpečností díry jim potom umožňují infikovaný kód propašovat až do uživatelova počítače, a to bez jeho vědomí. Proto je tedy vhodné, aby uživatel své

[2] Blok dat, který je přenášen skrze počítačovou síť.

programy a operační systém udržoval pravidelně aktualizovaný, a aktualizace zbytečně neoddaloval.

Počítačové červi však nevyužívají pouze zranitelnosti programů a operačních systémů, ale také webových stránek, které mají obsaženy chyby v kódu, jsou nedostatečné zabezpečené a využívají nezabezpečené porty.

Počítačové červi, můžeme dále zařadit do kategorií podle toho, jak se pomocí počítačové sítě šíří. Tedy na červy, které se šíří prostřednictvím komunikačních služeb (chat a e-mail červi) a na červy, které využívají ke svému šíření sdílených složek (file-sharing červi).

Tato část je zpracována podle [2] a [13].

3.2.3.1 E-mail červi

Jak už z názvu vyplývá, tito červi se po počítačové síti přenáší pomocí e-mailových zpráv. Nejčastěji se pak šíří pomocí odkazů na podvodné webové stránky, které se však tváří jako stránky neškodné a důvěryhodné. Mohou pak mít například podobu přihlašovací stránky do bankovnictví, e-mailu, sociální sítě či jiné webové služby. Pokud pak uživatel vyplní přihlašovací okno na takto podvodné přihlašovací stránce a odešle jej, tak se jeho přihlašovací údaje dostanou až k útočníkovi, kterému tato podvodná stránka patří – jedná se o tzv. **Phising** (více o Phisingu v kapitole „Aktuální hrozby“ na straně 22).

Tato část je zpracována podle [2], [14] a [15].

3.2.3.2 Chat červi

Chat červi jsou svým způsobem šíření velmi podobní e-mailovým červům. Oproti nim se však šíří pomocí komunikačních programů (ICQ, Skype) a sociálních sítí jako je například Facebook, a to jak ve formě odkazů na nebezpečné webové stránky, tak i v podobě nebezpečných doplňků.

Nebezpečné doplňky pak mohou být například uloženy ve videu, které může být umístěno na sociální síti. Pokud pak uživatel chce toto video spustit a klikne na něj, vyskočí na něj hláška: „*Pro přehrání tohoto videa prosím nainstalujte přiložený doplněk.*“ O doplněk se samozřejmě nejedná, a pokud je uživatel v oblasti počítačové bezpečnosti nezkušený, stáhne si do počítače škodlivého červa, který je v tomto doplňku obsažen. Tento červ pak může ve většině případů dále odesílat toto video kontaktům, které má poškozený uživatel uloženy v kontaktech, sdílet jej na uživatelově profilu a označovat u ní jeho přátele či jej sdílet ve skupinách, ve kterých je poškozený uživatel členem – tím se

tedy tento nebezpečný červ dostává k dalším a dalším lidem. To je však pouze vedlejší efekt. Dále v sobě může obsahovat nebezpečné komponenty, které mohou sledovat jednotlivé stisky kláves, aktivitu uživatele, otevírat zadní vrátka do systému, a mnoho dalších jiných nebezpečných komponent. Náhled videa pak zobrazuje svým způsobem něco zajímavého, co má uživatele nalákat k tomu, aby toto video přehrál. Může se například jednat o náhled krásné nahé ženy apod.

Doplněk však může být také obsažen například i v pdf souboru, který útočník může zaslat pomocí komunikačních služeb, a u kterého pak může například tvrdit, že se jedná o nějakou smlouvu apod. Při otevření takovéhoto souboru pak program hlásí, že potřebuje nejnovější aktuální verzi, kterou si uživatel může stáhnout na přiložené adrese. Přiložená adrese je však pochopitelně podvodná a nabídne uživateli falešný program. Ten pak v sobě ukrývá mnoho nebezpečných metod.

Tato část je zpracována podle [2] a [16].

3.2.3.3 File-sharing červi

File-sharing červi využívají ke svému šíření sdílených složek, které se používají jako uložiště souborů v rámci počítačové sítě. Díky tomu, že jsou tyto složky dostupné prostřednictvím počítačové sítě, mohou se k nim dostat i počítačoví červi - tedy v tomto případě file-sharing červi. Do těchto sdílených složek pak ukládají své kopie v podobě původních souborů, a může si je potom tedy stáhnout kdokoliv, kdo do těchto složek má přístup. Kopie jsou pak velice chytře pojmenovány a na první pohled je skoro nelze rozeznat od původních souborů. Nezkušený uživatel pak potom tedy může tento neškodně vypadající soubor stáhnout, přičemž spolu s ním stáhne i počítačového červa, který je v něm ukrytý. Pokud pak uživatel takovýto soubor spustí či otevře, spustí místo souboru tohoto nebezpečného červa, který v sobě může ukrývat mnoho nebezpečných vlastností.

Tato část je zpracována podle [17].

3.2.4 Speciální případy malwaru

O tom, co je to počítačový virus, trojský kůň či červ jsme si již řekli v předchozích kapitolách. V oblasti výpočetní techniky však ještě existuje jedna kategorie nebezpečného malwaru, která se na rozdíl od ostatních již zmíněných zaměřuje především na špehování uživatele, zobrazování nechtěných reklam, získávání osobních informací pomocí podvodných e-mailů, šifrování jednotlivých souborů, dokumentu a celého pevného disku, těžení tzv. kryptoměny a zasílání falešných poplašných zpráv.

V této kapitole se zmíním o speciálních škodlivých kódech, které zařazujeme do kategorie: Spyware, Adware a Hoax. V kapitole „Aktuální hrozby“ se pak zmíním o dalších případech speciálního malwaru a naleznete ji na straně 22.

3.2.4.1 Spyware

Spyware je typ škodlivého kódu, který pomocí počítačové sítě odesílá data z uživatelova počítače, a to bez jeho vědomí. Jedná se tedy o typ škodlivého programu, který je určen pro špehování uživatele – odtud také dostal své jméno (**SPY** – špehovat, **WARE** – zkratka pro malware). Při takovéto špionáži může poté například získat informace o prohlížených webových stránkách, seznam otevíraných souborů, IP adresu počítače, informace o softwaru a multimediálních souborech apod.

Spyware však v sobě může ukrývat také techniky, které mu umožní převzít kontrolu nad tímto napadeným počítačem či techniky pro odposlouchávání toho, co uživatel zadává na klávesnici. Pomocí těchto technik pak může získat přihlašovací údaje do bankovnictví, čísla kreditních karet či jiné osobní údaje, které poté zasílá autorovi tohoto škodlivého kódu.

Zajímavostí může být, že se někteří autoři spywaru hájí tím, že jejich program odesílá pouze data o navštívených webových stránkách či data z nainstalovaných programů, a to za účelem zjištění potřeb nebo zájmů uživatele. Takto získané informace prý potom mohou využít pro cílenou reklamu.

Tato část je zpracována podle [19] a [20].

3.2.4.2 Adware

Adware je označení pro malware, který znepříjemňuje práci na počítači tím, že zobrazuje nechtěné a otravné reklamy. Může však také například nainstalovat legitimní panel nástrojů (toolbar) do prohlížeče, který pak velmi často změní i výchozí vyhledávač (např. z googlu na ask) a domovskou stránku uživatele.

Adware pak obsahují především tzv. freeware programy, které jsou uživateli nabízeny zcela zdarma. Oproti jiným škodlivým programům či kódům a také hlavně díky licenčnímu ujednání je však uživateli při instalaci takovéhoto programu sděleno, že obsahuje větší počet reklam, a má tedy tak na výběr, zda takovýto program chce doopravdy nainstalovat či nikoliv. V průběhu instalace má pak také uživatel na výběr, zda chce nainstalovat přiložený toolbar či nikoliv. Mnoho uživatelů však průběhu instalace nevěnuje dostatečnou pozornost, a tak se v jejich internetovém prohlížeči projeví nechtěné změny.

Díky většímu počtu reklam, které tyto programy zobrazují, pak mohou vývojáři financovat další svůj program, či vydávat nové aktualizace, záplatovat bezpečností díry, a program tak neustále vylepšovat. Na druhou stranu se uživatel těchto otravných reklam občas může zbavit tím, že si zdarma dostupný program zakoupí.

Adware se však objevuje také i na webových stránkách. Webové stránky, které adware obsahují, pak v drtivé převaze nabízejí zhlédnutí filmů, poslech hudby a další jiné zdarma dostupné služby. Při manipulaci s takovýmito službami se občas uživateli otevře nové okno, a to s úplně jinou webovou stránkou. Nově otevřená okna s webovými stránkami pak ve většině případů nabízejí nějaké placené služby a produkty. Nechtěné reklamy potom tedy uživateli znepříjemňují práci s internetovými službami tím, že tu a tam záměrně vyskočí. Za každou zhlédnutou reklamu pak autor webové stránky obdrží určitý peněžní obnos.

V poslední době také stále přibývá stránek, které nabízejí za zhlédnutí reklam malý počet jednotek krypto-měny[3]. Díky tomuto zhlédnutí si pak autor webové stránky, která reklamy obsahuje, může vydělat i poměrně slušné peníze – pochopitelně o dost vyšší než ti, co na reklamy koukají. Webové stránky, na které tyto reklamy odkazují, tím pak získávají větší počet zhlédnutí a větší počet potencionálních zákazníků.

Oproti jinému malwaru se tedy dá říci, že adware je takřka neškodný a jen znepříjemňuje práci na počítači tím, že zobrazuje větší počet nežádoucích reklam.

Tato část je zpracována podle [19] a [20].

3.2.4.3 Hoax

Hoaxem označujeme veškeré falešné zprávy, mystifikace, novinářské kachny, poplašné zprávy, výmysly a žerty, které mohou být šířeny prostřednictvím e-mailových zpráv, sociálních sítí či jiných komunikačních prostředků. Takovéto zprávy se pak postiženého uživatele nejčastěji snaží přesvědčit pomocí nepravdivých informací, a to ve formě nového nebezpečí, naléhavé pomoci či šokující informace. Pomocí svého obsahu potom žádají o další rozesílání této falešné zprávy mezi přátele, případně na co největší množství dalších adres, díky čemuž se hoax šíří dále. Falešná zpráva potom operuje s efektivním využitím jazyka v kombinaci s efektivním působením na city příjemce, a svůj obsah se často snaží potvrdit „osobními důkazy“ a „logickými argumenty“. Často je také

[3] Virtuální měna, která se používá pro elektronické platby. Ve většině případů pak bývá anonymní a nelze jí proto tedy vystopovat.

tvrzení pisatele doprovázeno velmi názornými obrázky (tělesná postižení, oběti autonehody, nebezpečná zvířata apod.).

Přibližně 80 procent dětí ve věku od 6-15 let, pak hoaxy přeposílá dále, čímž umožnují jejich šíření. Děti si rovněž hoaxy velmi často čtou a jejich obsah v nich potom vyvolává strach, obavy, nedůvěru a působí tedy na jejich psychiku. Obsah takového hoaxu pak může mít například následující podobu: pokud tuto zprávu nepošlete dalším 10 lidem, stane se Vám něco špatného, infikované jehly v tramvaji, AIDS z kontaminovaných potravin, jedovatí pavouci v koupených palmách apod. Hoax však nešíří pouze jen děti, ale také i dospělí jedinci. Příkladem toho mohou být hoaxy, které se dnes ve velké míře objevují na sociálních sítích.

Z výše uvedených vlastností tedy vyplývá, že hoax není typickým malwarem, který by prováděl škodlivé operace v počítači. Za to však uživatelům škodí pomocí falešných zpráv, kterými je obtěžuje, poskytuje jim nebezpečné rady, nadbytečně zatěžuje linky a servery, přetěžuje konkrétní cílové e-mailové schránky („*Za každý odeslaný e-mail na tuto adresu, dostane děvčátko 1 cent*“), a pokud je uživatel přeposílá dále, ztrácí díky nim na důvěryhodnosti.

Tato část je zpracována podle [21].

3.3 Aktuální hrozby

V dnešním světě informačních technologií se útočníci zaměřují především na tvorbu a využití nebezpečných kódů, pomocí kterých si mohou přijít i na velice slušné peníze. Nebezpečné kódy, které dokáží zajistit přístupy k penězům, jsou pak pro útočníky mnohem lákavější a zajímavější než kódy, které například dokáží pouze upravovat či mazat soubory. Proto se tedy dnes tyto kódy ve velké míře čím dál více používají a neustále zdokonalují.

Malware, kterým si útočník může přijít i k nemalým finančním částkám pak zařazujeme do katogerie Phising, Ransomware, Minig viry a Botnety. Každá kategorie těchto nebezpečných kódu se pak šíří pomocí různých metod, a také se jinak projevuje. Jedno však mají vždy společné – snaží se z uživatele či jeho počítače vydolovat co nejvíce peněž.

3.3.1 Phising

Phisingem označujeme všechny podvodné techniky, které se z uživatele snaží vylákat důvěrné informace, a to pomocí podvodných webových stránek, či odkazů, které

sice směřují na oficiální webové stránky, avšak v sobě ukrývají nebezpečné kódy. Nejčastěji pak mezi tyto důvěrné informace patří údaje k platebním kartám nebo přihlašovací údaje k účtům (bankovní, e-mailové atd.). Nemusí se však jednat pouze o bankovní účty, ale také o účty k ostatním organizacím, ve kterých dochází k manipulaci s penězi (Ebay, PayPal).

Aby útočníci z uživatelů vylákali tyto důvěrné informace, rozesílají podvodné e-mailové zprávy, pomocí kterých se snaží vyvolat dojem, že byly odeslány z příslušné organizace (AirBank, PayPal, Amazon, Microsoft atd.). Toho se snaží docílit grafickou podobou e-mailu a zfalšováním adresy odesílatele. Text, který je potom v takovýchto podvodných e-mailech napsán, pak může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu, výzkum klientské spokojenosti, informace o nové aktualizaci, a mnoho dalšího. V textu této zprávy je pak přidělen ještě odkaz na podvodnou webovou stránku, která na první pohled vypadá jako oficiální stránka příslušné organizace. Pokud ho pak nezkušený uživatel rozklikne, je přesměrován na stránku, která na první pohled vypadá jako stránka, kam se běžně přihlašuje, či jako stránka, která žádá o vyplnění osobních údajů, čísel kreditních karet apod. Ve skutečnosti se pak jedná o podvod a grafická iluze má pouze zajistit, aby zde uživatel zadal a odeslal své přihlašovací údaje. Pokud by tedy útočník chtěl například získat přihlašovací údaje do bankovnictví, stačilo by mu, aby tato stránka vypadala přesně jako ta, do které se uživatel běžně přihlašuje - to by potom uživatele dokonale zmátlo. Pokud by uživatel na takto podvodné stránce poté zadal a odeslal heslo včetně přihlašovacího jména, tak by se tyto údaje dostaly až do rukou útočníka, tedy majiteli této podvodné webové stránky. Pomocí získaných údajů by si poté například mohl z účtu odeslat nějakou finanční částku, zjistit osobní informace, nebo rozesílat další škodlivý malware.

Tato část je zpracována podle [22].

3.3.2 Ransomware

Ransomware je typ vyděračského škodlivého kódu, který využívá techniky pro zašifrování dat, jež jsou uloženy na pevném disku a jiných paměťových zařízeních. Tato data pak mohou být i velice cenná, a například v rámci firem, mohou obsahovat osobní údaje o zaměstnancích a zákaznících, účetní záznamy, licencovaný software třetích stran, vlastní software firem, interní dokumenty firem a mnoho dalších souborů a dokumentů,

které firmy používají a potřebují pro svůj chod. Samotné šifrování je pak velice důkladně provedeno pomocí šifrovacího algoritmu, a odšifrování dat může být někdy i velice tvrdý oříšek, a ne vždy se může povést. Některé šifrovací algoritmy pak mohou být velice složitě napsané, a přístup k dešifrovacímu klíči může tedy vlastnit pouze autor viru.

Šifrovací malware se však nesoustředí pouze jen na jednotlivé soubory či dokumenty, ale rovněž i na celý disk, čímž zapříčiní nemožnost práce s napadeným počítačem. Pokud tedy zašifruje pevný disk, uživatel nemá možnost se do systému vůbec dostat, a místo přihlašovací obrazovky se mu zobrazí výzva k zaplacení určité peněžní částky, a to nejčastěji ve formě elektronické měny. Po zaplacení této částky, prý pak údajně obdrží dešifrovací klíč, jenž mu umožní zašifrovaný pevný disk odšifrovat. V drtivém množství případů, je pak nebezpečný kód velice sofistikovaný a přidává například hlášení od policie či autorskoprávní organizace, ve kterém požaduje tisíce korun za údajné porušení autorského práva. Často je pak také přidán odpočet času, do kterého má uživatel možnost zaplatit. Pokud uživatel zaplatit nestihne, útočníci vyhrožují, že veškerá uložená data budou smazána. To pak některé uživatele může vystrašit a podvědomě donutit k tomu, aby tuto částku zaplatili.

Takovýto postup však není zaručen a ani odborníky doporučen. Jednak tím, že uživatel bude touto peněžní částkou dále podporovat útočníky v jejich vyděračských aktivitách a za druhé, neexistuje vůbec žádná záruka, že uživatel dešifrovací klíč vůbec obdrží. Pokud by se stalo, že by uživatel dešifrovací program obdržel, mohl by v sobě ukrývat také další nebezpečné kódy, které by celou situaci mohli ještě zhoršit. Z nedávného výzkumu například vyplývá, že v případě firem, které se s těmito vyděračskými aktivitami setkaly, tak každá pátá firma, která výkupné zaplatila, svá data zpět nezískala. Útočníci přitom chtějí nemalé peněžní částky, a to až v hodnotě 15 000 Kč.

Jednou z největších hrozeb tohoto roku byl pak ransomware jménem WannaCry, o kterém řada z vás, již určitě slyšela. Tento nebezpečný kód se velmi dobře šířil, jelikož vedle typické ruční nákazy (manuální spuštění viru), mohl zneužít ke svému šíření i bezpečnostních děr v operačních systémech Windows (XP,7). Tímto způsobem se potom nejspíše nakazily i velké podniky, jako byly například britské nemocnice, některé drážní systémy v zahraničí a také automobilová firma značky Renault. Zajímavé je, že za hlavní viníky byla označena NSA. Tato národní bezpečností agentura prý údajně měla přispět tomuto ransomwaru tím, že ve svých laboratořích napsala programy pro zneužití

zranitelnosti systému Windows, které potom byly ukradeny a kvůli kterým se pak mohl hotový virus lépe šířit lokálními sítěmi a internetem.

Tato část je zpracována podle [23], [24] a [25].

Obrázek 2 – WannaCry. [25]

3.3.3 Mining virus

Mining virus je malware, který využívá techniky k „těžení“ (dolování) tzv. krypto-měny (Bitcoin, Monero, ZCash)[4], což je digitální měna, která se skládá z počítačového kódu a lze ji využít k elektronickým transakcím, a to bez prostřednictví bank[5].

Těžení je pak prováděno pomocí matematického výpočtu, které ve velké míře využívá výkonu grafických karet. Jelikož náklady na výpočetní techniku, která by dostatečně rychle tuto měnu těžila, jsou vysoké, a někteří jedinci se nespokojí jen se svými výpočetními zdroji, tak se útočníci snaží využívat i výpočetních zdrojů cizích počítačů. Aby mohli využívat výpočetních zdrojů cizích počítačů, mění je pomocí škodlivého kódu v zařízení pro dolování této digitální měny. Pochopitelně se však zaměřují na větší počet počítačů, kam by tento nebezpečný kód mohli propašovat. Platí, že čím více počítačů, tím více výpočetního výkonu, tím více těžení, a tedy logicky více peněz.

[4] Cena za jednu jednotku krypto-měny se pak pohybuje i okolo částky přesahující 150 000 Kč.
[5] Díky tomu, že banky nezpracovávají takovéto transakce a také díky anonymitě odesílatele a příjemce, se tato měna stává velice populární, a není divu, že toho využívají i počítačový piráti.

Člověk by si řekl, že odhalit takovýto virus může být díky velkému obsazování výpočetních zdrojů lehké odhalit. Podle odborníku však tento nebezpečný kód prý naplno pracuje pouze ve chvíli, kdy uživatel svůj počítač nepoužívá. V opačném případě se snaží nebrat si moc výpočetního výkonu, z důvodu jeho utajení.

Tato část je zpracována podle [26], [27] a [28].

3.3.4 Botnet

Za jednu z největších hrozeb současnosti je považován nebezpečný malware, který označujeme jako **Botnet**. Pokud bychom botnet měli nějak definovat, jednalo by se o skupinu napadených počítačů nic netušících uživatelů. Napadený počítač, který je součástí tohoto botnetu, se potom stává tzv. botem (od slova robot), a má za úkol vykonávat příkazy, které mu tvůrce škodlivého kódu zasílá pomocí internetových protokolů a služeb (IRC[6], e-maily, twitter).

Příkazy pak představují různé úkoly a mohou provádět DDoS[7] útoky, rozesílat spam, těžit bitcoiny, klikat na reklamy, krást soukromá data a samozřejmě pomáhat s šířením dalšího malwaru, díky čemuž jejich počet dále roste. Právě v jejich počtu je největší síla. Desítky či stovky tisíc počítačů připojených k centrálnímu prvku, který ovládá útočník, pak disponují nejen obrovským výpočetním výkonem. Napadený počítač se pak nejčastěji může stát botem pomocí jiných škodlivých kódu, které jsem již zmiňoval v předchozích kapitolách (viry, červi, trojské koně apod.).

Nejčastějším důvodem tvorby botnetů jsou samozřejmě peníze. Zajímavé ale je, že jejich tvůrci je nevyvíjí přímo pro sebe. Místo toho je pronajímají dalším lidem, což je často velký problém. Bezpečnostní experti potom netuší, co daný botnet bude dělat další den. Cena za botnet se pak odvíjí podle doby pronájmu, počtu pronajatých botů, a rozmístění botů po světě (viz. „tabulka 1“ na další stránce). Pak už je tedy pouze jen na nájemci, jak tyto počítače využije.

[6] Protokol určený pro textovou komunikaci
[7] Útok, pomocí kterého dojde k přetížení služby (internetové stránky), a to za pomocí několika najednou zaslaných žádostí. Přetížení má pak za následek zpomalení nebo nefunkčnost/nedostupnost služby.

	Počet počítačů		
	1000	5000	10 000
Umístění infikovaných počítačů	**Cena**		
Světový mix	25 USD	110 USD	200 USD
Evropský mix	50 USD	225 USD	400 USD
Německo, Kanada, Británie	80 USD	350 USD	600 USD
Spojené státy	120 USD	550 USD	1000 USD

Tabulka 1 - Ceny za pronájem botnetu. [29]

Momentálně patří mezi největší hrozbu botnetu malware jménem Reaper. Objevila ho bezpečnostní firma Check Point Research a tvrdí, že se jedná o rychle rostoucí a rozvíjející se hrozbu, u které dokonce věří, že by jednou mohla shodit internet. Údajně prý již tato hrozba nakazila více než deset tisíc zařízení a další dva milióny prý čekají ve frontě.

Reaper pak využívá slabá místa domácích routerů vyráběných firmami Linksys a D-Link, dále slabých míst IP kamer a síťových video přehrávačů od firem TP-Link, AVTECH, NETGEAR, MikroTik, Synology a mnoho dalších, které se dají zakoupit i v České republice. Některá tato slabá místa již byla opravena nově vydanými aktualizacemi softwaru, avšak mnoho uživatelů nikdy neprovede potřebné kroky k aktualizacím těchto zařízení. Díky tomuto pak může mít útočník k dispozici i několik desetitisíců zařízení, kterými pak může provádět nebezpečné útoky.

Tato část je zpracována podle [29], [30] a [31].

3.4 Prevence před nakažením

O tom, jaké máme typy malwaru a co všechno mohou způsobit, jsme si již řekli v přechozích kapitolách. Nikde jsme však nepoukázali na to, jaká je vůbec preventivní ochrana před takovouto škodlivou havětí, která by nám mohla napadnout, poškodit a zneužít naše počítače. Bylo by tedy vhodné, vypsat si jednotlivé způsoby, jak se malware může dostat do našich počítačů, a na základě toho udělat návod, jak tomuto napadení předejít.

3.4.1 Nebezpečné přílohy

Internetová síť se dnes mimo jiné využívá i k přenášení souborů mezi lidmi, a to v rámci celého světa. Můžeme tak velice snadno odesílat a přijímat dokumenty, hudbu,

programy, videa a podobně, aniž bychom musely tyto soubory fyzicky donést až k dotyčné osobě.

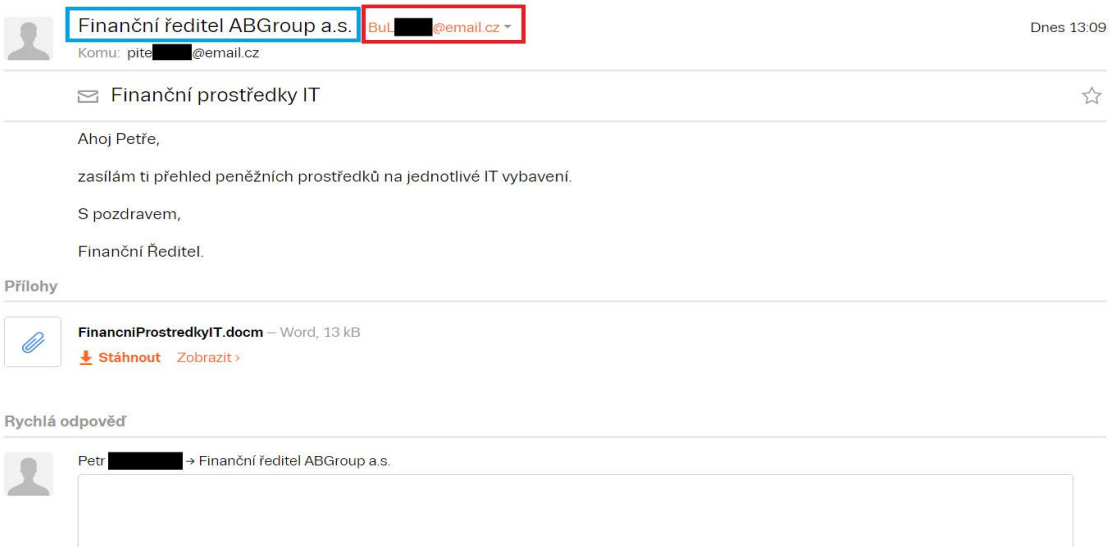
Tohoto způsobu přenosu si však jsou vědomi i počítačový útočníci, kteří díky tomu využívají nepozornosti uživatelů. Každý soubor je totiž zařazen do jakési kategorie, podle toho, co představuje (obrázek, video, program, skript, hudba, dokument atd.) a nazýváme to typem souboru. Některé soubory však mohou být útočníky velice fikaně přejmenovány, a to co na první pohled vypadá třeba jako dokument, obrázek či pdf soubor, může být ve skutečnosti spustitelný skript[8], ve kterém se potom ukrývá nebezpečný kód. Takovéto předělané soubory, pak nejčastěji útočníci zasílají ve formě příloh, a to prostřednictvím e-mailových zpráv.

Některé e-mailové služby a programy (Outlook, Seznam) však odesílání příloh s potencionálně nebezpečnými typy souboru nedovolují. Útočníci jsou však velice vychytralí, a přidávají tyto nebezpečné soubory do archivů (ZIP, RAR), které zablokované nejsou. Nebezpečná příloha (archiv) se pak tedy může dostat až k uživateli.

Ochrana před takovýmito nebezpečnými přílohami je však velmi jednoduchá – neotevírat přílohy, které nám přijdou prostřednictvím komunikačních služeb (e-maily, skype, faceboook) od zdrojů, které neznáme.

Útočníci si však svá e-mailová jména mohou měnit a může se na první pohled zdát, že zprávu zasílá třeba finanční ředitel nebo nějaký náš kamarád. Pokud se však na email podíváme důkladněji, zjistíme, že e-mailová adresa ve skutečnosti patří někomu úplně jinému. Mnoho uživatelů si však všimne pouze e-mailového jména, nikoliv samostatné e-mailové adresy. Pro názornost využijme obrázku „Nedůvěryhodný adresát“ na další stránce.

[8] Soubor, který obsahuje instrukce, pomocí kterých počítač provede určitou činnost.



Obrázek 3 - Nedůvěryhodný adresát. [4]

Jak si na obrázku můžeme všimnout, adresát je přejmenovaný na finančního ředitele firmy ABGroup a.s. (vyznačeno modře), což může mnohé uživatele lehce zmást. Pokud se však podíváme důkladněji, můžeme si všimnout, že e-mailová adresa ve skutečnosti patří někomu úplně jinému (vyznačeno červeně). V e-mailu je pak přiložen nebezpečný dokument, a pokud by se uživatel nechal zmást a spustil ho, nebezpečný kód by mu na počítači mohl nadělat pěknou paseku. Aby tato e-mailová zpráva nabyla ještě na větší důvěryhodnosti, mohl by útočník ještě přidat podpis a logo firmy.

Může se však také stát, že zdroj, od kterého přílohu obdržíme, považuje za důvěryhodný, avšak může být pod správou někoho, kdo se za něj pouze vydává (ukradl mu přihlašovací údaje a odesílá pod ním nebezpečný obsah). Pokud si pak tedy nejste jisti tím, zda se jedná o důvěryhodný zdroj nebo zda se nejedná o škodlivou přílohu, soubor raději neotevírejte

Abychom si udělaly přehled o tom, jaké přílohy jsou bezpečné a které mohou být potencionálně nebezpečné, můžeme se podívat na následující tabulku, ve které jsou vypsané některé typy souborů a rozdělené podle toho, zda se v nich může skrývat nebezpečný kód či nikoliv.

Bezpečné typy souborů	Potencionálně nebezpečné typy souborů
JPEG, PNG, BMP, BPG, GIF - **obrázky**	BAT, VBS, CMD, JS, VB – **spustitelné skripty** – mohou usnadňovat práci X mohou být napsány do škodlivé podoby
MKV, AVI, WMV, MPG, MP4 - **videa**	EXE, COM, MSI, MSP – **spustitelné programy** – mohou být vytvořeny pro práci s PC X mohou být ve formě nebezpečného programu
XLSX, DOCX, PPTX, – **kancelářské typy souborů** (tabulky, dokumenty, prezentace, databáze)	XLSM, DOCM, PPTM – **kancelářské typy souborů, které obsahují makra** - mohou usnadňovat práci X mohou být napsány do škodlivé podoby

Tabulka 2 - Typy souborů

Tato část je zpracována podle [32], [33] a [34].

3.4.2 Nebezpečné doplňky.

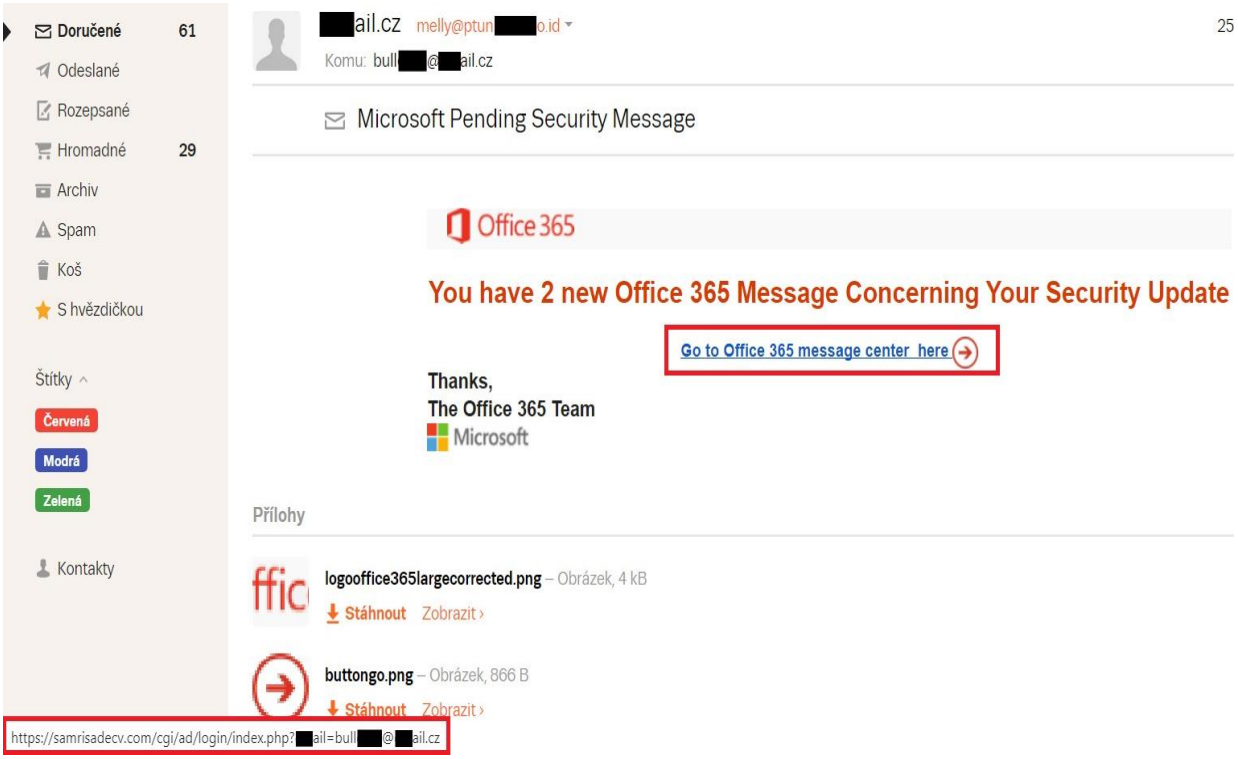
Dalším nebezpečím, které na nás v oblasti výpočetní techniky číhá, jsou nebezpečné „doplňky“. Ty představují jakýsi podpůrný program, který slouží třeba pro přehrání videí (flash player) nebo otevření dokumentů (PDF).

V případě doplňku pro videa, vypadá proces nakažení zhruba takto: Útočník vytvoří video, které svým způsobem obsahuje něco zajímavého (svlékající se atraktivní nahá žena, rychlý přístup k penězům atd.), a do kterého vloží falešný doplněk, který se tváří jako doplněk z oficiálních stránek výrobce. Pokud se mu pak zadaří a uživatele na toto video naláká, tak jej uživatel pochopitelně spustí, přičemž na něj vyskočí upozornění: *„Pro přehrání tohoto videa je vyžadována aktuální verze Adobe Flash Player. Prosím stáhněte si přiloženou aktuální verzi.“* Leckomu už může dojít, že je tento doplněk podvodný a maskuje se za známý doplněk pro přehrávání videí. Bohužel tomu řada uživatelů mnoho kdy naletí. Upravený doplněk pak v sobě obsahuje nebezpečné charakteristiky a může provést i opravdu škodlivé věci. Pokud tedy na vás někdy takovýto doplněk vyskočí a bude se chtít hned začít stahovat a instalovat, nestahujte jej. Raději přejděte na oficiální stránky výrobce, kde rovnou zjistíte, zda máte tento doplněk nainstalovaný a aktuální.

3.4.3 Nedůvěryhodné stránky.

V poslední době také stále více přibývá podvrhnutých a nedůvěryhodných stránek, které se tváří buď jako stránky přihlašovací, nebo stránky, které se z uživatele snaží vylákat třeba osobní informace, čísla kreditních karet, bezpečnostní otázky a podobně (tzv. Phising). Na takovéto stránky potom můžeme narazit jak v běžném e-mailu, tak i na samostatném internetu (ve vyhledávači).

Na nebezpečný e-mail včetně odkazu na podvodnou webovou stránku, se můžeme podívat na obrázkách níže. Tento e-mail byl zaslán přímo mé osobě, a proto je tedy dobrým a názorným příkladem tohoto způsobu nakažení.

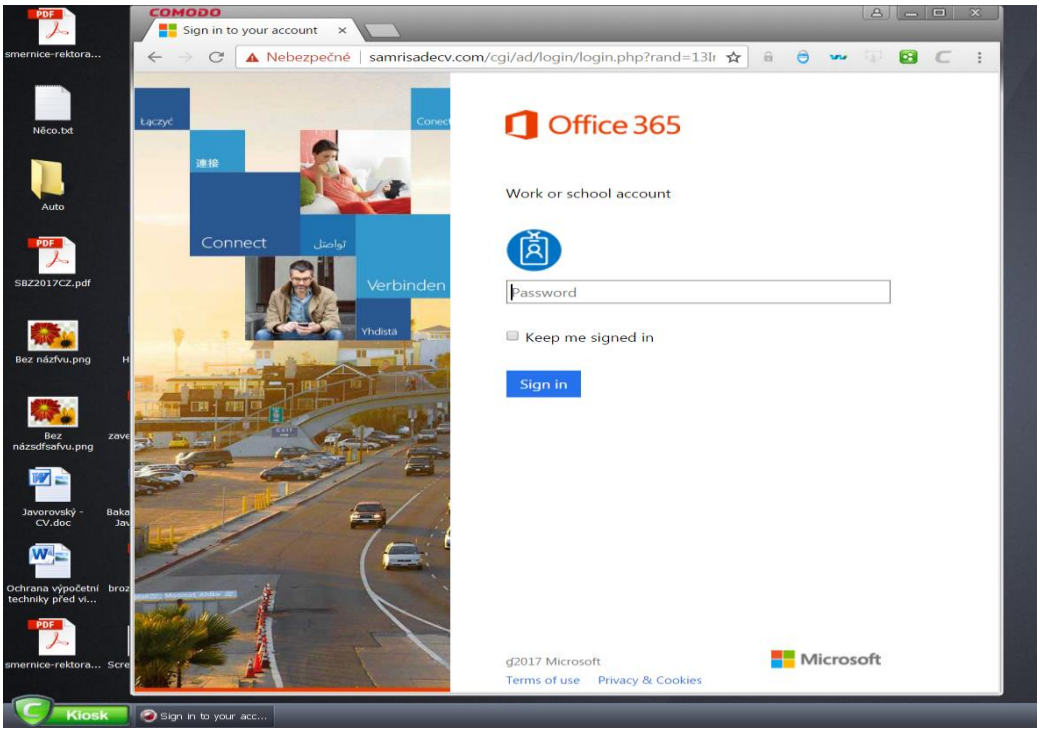


Obrázek 4 - Nebezpečný e-mail

První, čeho si můžeme všimnout, je rozdílné jméno adresáta a e-mailová adresa, ze které byl e-mail odeslán. Ve jméně máme jako doménu[9] uvedenou CZ a v adrese je zase uvedena CO.ID, což už může napovídat tomu, že se jedná o nějaký podvod. V mém případě se pak také jedná o adresu, kterou vůbec neznám a nikdy jsem si s ní nepsal. Dalším vodítkem je i obsah této e-mailové zprávy - Proč by mi společnost Microsoft

[9] Unikátní adresa internetu, která se například používá pro webové stránky. E-mailové služby jí pak používají v e-mailových jménech: pepadvorak@**abcd.com**

odesílala e-mail z jiné domény, když používají svojí vlastní? Třetím vodítkem, které je spojené také s obsahem, je přesměrování na adresu, která má údajně patřit Microsoftu – Společnosti by po nikom nikdy neměly chtít přihlášení či změnu osobních údajů, nebo stáhnutí aktualizací pomocí zaslaných e-mailových zpráv, které obsahují přesměrování na „jejich“ stránky. Z toho vyplývá, že bychom vždy měli přihlášení či změny osobních údajů, provádět přes oficiální webové stránky, které můžeme najít ve webovém prohlížeči. Dalším, a i nejdůležitějším vodítkem je pak adresa, na kterou zpráva odkazuje. Když na ní najedeme myší, můžeme si v levém dolním rohu všimnout (vyznačeno červeně), že odkazuje na stránky Samrisadecv.com., což už je tedy třetí doména, kterou tento e-mail obsahuje (CZ, CO.ID). Když jsem tuto adresu potom zadal do prohlížeče, zjistil jsem, že obsahem těchto stránek jsou hotely. Moje otázka tedy byla: *„Proč by mě Microsoft odkazoval na firmu, která poskytuje hotely? Není to trochu podezřelé?“* Podezřelé to samozřejmě je, a následně jsem rozklikl i přímý odkaz, který mě přesměroval na podvodnou přihlašovací stránku, která vypadala přesně jako ta od společnosti Microsoft (viz obrázek na další stránce). Doména však byla stále původní, tedy Samrisadecv.com., a navíc se mi zde zobrazilo i upozornění na nebezpečí – pokud by webová stránka nebyla ještě detekována jako nebezpečná, toto upozornění by se zde nezobrazilo.



Obrázek 5 - Podvodná stránka

Pokud bych pak zde zadal své heslo a odeslal ho, dostalo by se až do rukou útočníka, a ten by potom měl přístup do mé e-mailové schránky.

3.4.4 Nedůvěryhodné programy, a bezpečnostní díry

Dalším způsobem nebezpečí, kterým se škodlivý kód může dostat do našeho počítače, jsou bezpečnostní díry, které se objevují v programech a operačních systémech. Ty představují, jaké si slabé místo, kterým útočník může škodlivý kód propašovat do uživatelova počítače, a to bez jeho vědomí. Je tedy vhodné pravidelně stahovat aktualizace na programy a také na samostatný operační systém.

Programy je pak vhodné stahovat nebo zakupovat pouze z oficiálních stránek výrobce, kde uživatel vždy najde nejaktuálnější verzi, a je zde malé riziko toho, že se nebude jednat o neoriginální software. Na jiných síťových uložištích (uloz.to, slunecnice.cz, stahuj.cz, apod.), nemusí být uživateli vždy nabídnuta aktuální verze programu, a může pak tedy v sobě obsahovat staré bezpečnostní díry, které byly v novějších verzích (pomocí aktualizací) opraveny. Také zde není žádná záruka toho, že se bude jednat o skutečný program firmy – může se například jednat o nebezpečný program útočníka, který se pouze tváří jako originální software firmy, avšak ve skutečnosti tomu tak není. Zakoupené programy a operační systémy, mají pak vždy k dispozici nově vydané aktualizace, které si uživatel může bezplatně stáhnout, což se však nedá říct o neoriginálním softwaru či systému.

4 Analytická část

4.1 Jak se bránit před malwarem

Prevence před nakažením nebezpečnými kódy může být sice velmi užitečná, avšak uživateli nezaručuje úplné bezpečí, které by ho stoprocentně ochránilo před těmito nebezpečnými kódy. Občas se prostě může stát, že bude nějaké nebezpečné příloze, stránce či souboru důvěřovat, ale ten neřád v sobě bude mít ukrytý nebezpečný kód.

Mnohem častějším způsobem však bývá nakažení prostřednictvím nelegálního softwaru, kteří si uživatelé velmi často stahují do svých počítačů. Takovýto software je pak tedy zdarma, a je pochopitelné, že si ho uživatel chce nainstalovat do svého počítače, a tím ušetřit i několik tisíc korun. Toho však využívají počítačoví útočníci, kteří jsou si takovýchto nepoctivců vědomi. Do originálního softwaru přidávají své nebezpečné kódy a nabízejí ho na internetových uložištích. Aby těmto nahraným programům přidali na věrohodnosti, dopisují si u nich v recenzích kladné hodnocení, a zaručují stoprocentní funkčnost programu. Pokud pak takovéto nelegální programy uživatel stahuje, měl by být velice obezřetný.

Těmito způsoby a mnoha dalšími se však může malware dostat do uživatelova počítače, a to i v případě že si bude dávat pozor. Jak ale takovéto nebezpečí potom rozeznat, když si uživatel nemůže být stoprocentně jistý, jakým souborům důvěřovat a jakým nikoliv? Nabízí se jednoduché řešení – Aby se uživatel mohl před potencionálním nebezpečím bránit ještě efektivněji, měl by spolu s prevencí a selským rozumem, používat i antivirové programy.

Antivirový program ale nemusí být pro některé uživatele lehké vybrat. V počítačové bezpečnosti však existují naštěstí organizace, které se zabývají testováním antivirových programů, a tím mohou uživateli pomoc při výběru. Jednou z nejlepších organizací pro srovnání antivirových programů je AV Comparatives (https://www.av-comparatives.org).

Tato organizace vydává každý měsíc report z testování několika antivirových programů, a to i programů z českých a slovenských firem (AVG, Avast, Eset). Kritériem pro jednotlivá testování jsou pak: detekce malwaru, odstranění malwaru, anti-phishingové testy, zátěž systémových prostředků, falešné detekce a mnoho dalšího. Ke každému jednotlivému kritérii, je pak vyhotovena kompletní zpráva v PDF souboru, která je dostupná prostřednictvím internetu široké veřejnosti. Ve vyhotovené zprávě z testu, je pak

možné najít jaké antivirové programy a jakým způsobem byly testovány, kolik bylo na test použito souborů a jak v jednotlivých testech dopadly. Na konci roku pak organizace vydává celkový přehled, kde hodnotí úspěšnost jednotlivých programů pomocí několika různých kritérií a na základě toho jim uděluje ohodnocení. Hodnotí se úspěšnost v hledání infikovaných souborů, výkonnost, ochrana v reálném nasazení a odstraňování malwaru. Uživatel si potom tedy může lehce udělat představu o tom, jaký antivirový program je dobrý a který nikoliv. Schválně zde píšu dobrý, nikoliv nejlepší. Pro každého uživatele může být lepší něco jiného, a organizace AV Comparatives sama říká, že nejlepší hodnocení dostává antivirový program, jehož testy zůstaly v průběhu roku stálé a neporažené ostatními antivirovými programy. V testech pak nejsou taky zahrnuty další faktory, které by měl uživatel zhodnotit při výběru těchto programů – uživatelské prostředí, jazyk programu, cena, či možnost podpory. Jedinou nevýhodou těchto stránek je omezení na anglický jazyk, což by některým uživatelům mohlo vadit. Existuje však i alternativa ve formě českého jazyku, a to například na webové stránce antivirovecentrum.cz. – nenabízí však takové srovnání jako AV Comparatives.

Tato část je zpracována podle [35] a [36].

V následujících kapitolách budou srovnané různé typy programů, které by na základě analýzy mohl či by naopak neměl uživatel použít pro ochranu výpočetní techniky. Jednotlivé programy jsou pak vybrané na základě autorova rozhodnutí, a to podle toho, s jakými typy programů se již setkal, či je vybral na základě doporučení nebo jiného usouzení.

4.2 Real-time Antiviry

Jednou z možností, jak uživatel může chránit svoji výpočetní techniku před nebezpečnými kódy, jsou tzv. real-time antivirové programy. Ty zajišťují ochranu výpočetní techniky v reálném čase, což znamená, že počítač je chráněn po celou dobu jeho spuštění. Tato ochrana pak tedy zajišťuje bezpečnost před všemi nebezpečnými soubory, dokumenty, webovými stránkami, přílohami a kódy, a to po celou dobu běhu operačního systému.

4.2.1 Comodo Antivirus 10

Testována verze: 10.0.2.6420

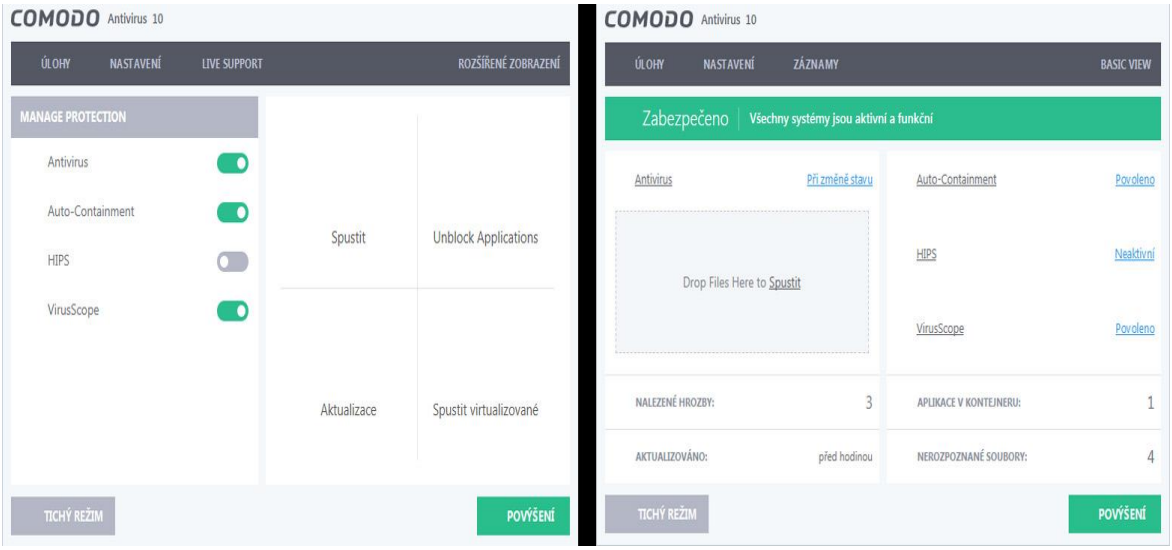
Jako první antivirový program, který zajišťuje ochranu v reálném čase, jsem zvolil Comodo Antivirus 10, jehož výběr nebyl náhodný. Osobně ho na svém počítači používám již cca 5 let (ve verzi Internet Security), a za tu dobu jsem si ho velice oblíbil. Má oblíbenost u něho vznikla díky jednoduchému uživatelskému rozhraní, a také především díky jeho vynikající kontrole. Zatím mě dokázal ochránit před všemi nebezpečnými hrozbami, se kterými jsem se za dobu 5 - ti let setkal.

Díky mé spokojenosti, bych ho tedy rád představil i čtenářům této bakalářské práce, kteří ho díky mé analýze, a svého vlastního uvážení, mohou zařadit do výběru jednoho z možných programů na boj proti nebezpečnému malwaru.

4.2.1.1 První spuštění

Program po svém spuštění uživatele přivítá přátelským a jednoduchým uživatelským rozhraním, ve kterém ihned může provést aktualizaci virové databáze a programu. Dále zde může také spustit antivirovou kontrolu, odblokovat zablokované programy, či spustit nějaký program v tzv. kontejneru. Vysvětlení, co jednotlivé tlačítka dělají, naleznete níže.

- **Tlačítko spustit** – umožňuje uživateli spustit následující typy kontrol:
  - **Rychlá kontrola –** zkontroluje nejčastěji infikované oblasti a paměť.
  - **Úplná kontrola –** zkontroluje všechny soubory a adresáře v počítači.
  - **Hodnotící kontrola –** zkontroluje nejčastěji infikované oblasti a paměť, a pomocí cloudu ověří reputaci souborů.
  - **Vlastní kontrola –** umožní kontrolu souborů a adresářů, vybraných na základě uživatele.
- **Tlačítko Unblock Applications** - umožňuje odblokovat zablokované programy, které nebyly nalezeny v databázi důvěryhodných programů, a jež byly zablokovány uživatelem.
- **Tlačítko spustit virtualizované –** umožnuje potencionálně nebezpečné programy zapnout ve virtualizovaném okně (Containment) a to tedy bez následku toho, že by nebezpečné kódy mohly ohrozit reálný systém – veškeré věci provedené ve virtualizovaném prostředí se pak nepropíší do reálného systému.



Obrázek 6 - Comodo - Uživatelské rozhraní

V uživatelském rozhraní se pak dále také nachází tlačítko, které umožňuje přepínat mezi Basic View (na levé straně) - to poskytuje zjednodušené grafické podání, a „Rozšířené zobrazení“ (na pravé straně) – to poskytuje rozšířené textové zobrazení. V Basic View pak má uživatel možnost rychle zapínat jednotlivé funkce. V Rozšířeném zobrazení má pak možnost tyto funkce ihned nastavovat. Mezi těmito dvěma módy lze pak jednoduše přepínat, a uživateli to tedy může usnadnit a urychlit práci s tímto antivirovým program. Jednotlivé funkce jsou pak popsány v samostatné kapitole „Nastavení“, a najdete ji na další stránce.

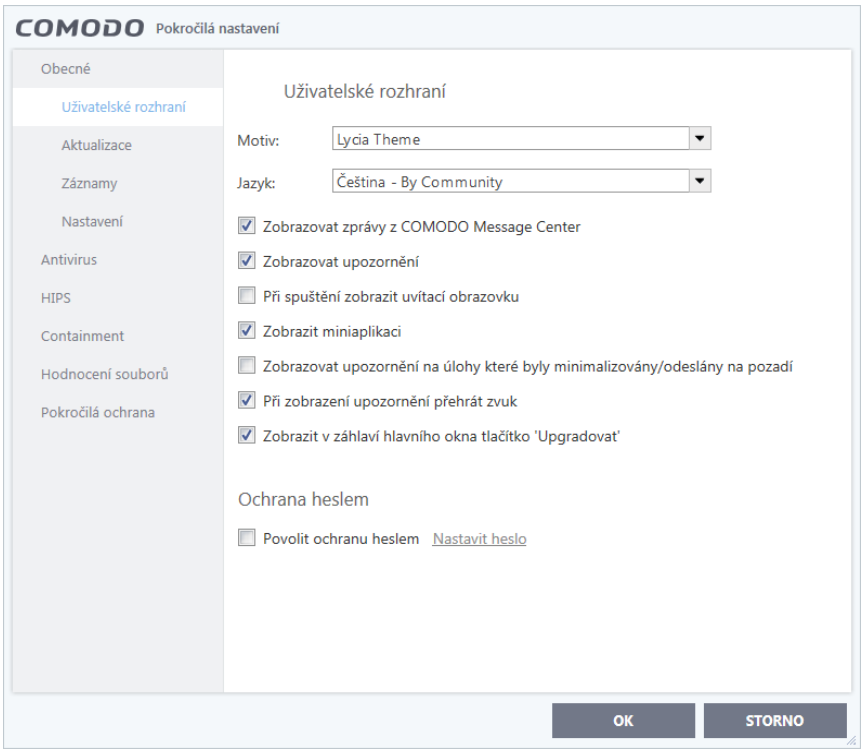
Na panelu nahoře má potom uživatel možnost spustit procesy ve virtualizovaném prostředí, či spustit virtuální plochu, a to pomocí tlačítka Úlohy. Při spuštění procesu či plochy ve virtuálním prostředí, se žádné provedené změny, které byly během procesu vykonány, nepropíši do reálného systému – tím se tedy předejde riziku nakažení. Osobně však nevidím v těchto funkcích moc velké využití pro obyčejného uživatele, a tak se tímto nastavením nebudu dále zabývat. Tlačítko Záznamy pak zobrazuje protokoly o událostech antivirového programu.

Velice zajímavé tlačítko je však Live Support. To umožní uživateli nainstalovat vedlejší software, který slouží pro komunikaci s firemním technikem. Tento technik je pak uživateli dostupný 7 dní v týdnu, a oproti jiným programům, které online podporu také nabízejí, uživateli pomůže takřka s čímkoliv - od vytvoření e-mailové schránky, pomoci při formátování dokumentů, nastavení tiskárny, až po odstranění malwaru z počítače. Tato služba je pak zdarma dostupná po 60 dní od instalace, a uživatel má tak možnost ji bezplatně vyzkoušet. Licence na rok pak stojí 1000Kč, což si myslím, že za přiděleného

technika, který uživateli bude nápomocen 7 dní v týdnu a pomůže mu takřka s čímkoliv, je opravdu slušná nabídka.

4.2.1.2 Nastavení

Nejdůležitějším tlačítkem je pak tlačítko nastavení, které obsahuje kompletní nastavení antivirového programu. Tedy například vzhled programu, kdy se budou vyhledávat aktualizace, automatické kontroly systému, a nastavení jednotlivých zabezpečovacích funkcí antiviru, hipsu, containmentu a viruscopu. Jednotlivé zabezpečovací funkce, by pak uživatele měli zajímat nejvíce – osobně však doporučuji je nechat nastaveny tak jak jsou – zajišťují dostatečnou ochranu před malwarem.



Obrázek 7 - Comodo - Pokročilé nastavení

- **Záložka Antivirus** – Uživatel zde má možnost povolit či zakázat rezidentní kontrolu, která zajišťuje prověření souborů při jejich použití a umožňuje tak předejít nakažení systému – doporučuji mít zapnuto.

  Umožňuje nastavení ohledně detekce - uživatel by měl dbát zvýšené pozornosti především na možnost „Nezobrazovat upozornění antiviru“ – pokud je vypnuto, na každý nebezpečný soubor bude uživatel vždy upozorněn, a bude mít možnost s ním provést vymazání, přesun do karantény (kód nebude moct škodit), nebo ho přidat do

výjimek. Nezkušenému uživateli doporučuji mít tuto funkci zapnutou a nastavenou na „Blokovat hrozby“ – každá zjištěná hrozba pak bude vymazána.

Obsahuje možnosti jednotlivých kontrol (úplná kontrola, rychlá kontrola atd.), včetně možnosti nastavení kontroly vlastní, a pravidelné (např. každý den v 6 večer).

Obsahuje možnost povolit či zakázat použít při kontrole souborů heuristickou analýzu – kromě porovnání souborů s virovou databázi, v sobě zahrnuje také logickou analýzu, která posuzuje, co testovaný kód v praxi dělá – například kontroluje to, zda soubor nechce zapisovat svůj vlastní kód do jiných souborů – doporučuji zapnout. Kontrola sice bude trvat déle, ale zajistí lepší ochranu před nebezpečnými kódy.

- **Záložka Hips** – Obsahuje možnost zapnutí / vypnutí procesu, který sleduje kritické oblasti operačního systému, a zajišťuje ochranu před změnami provedenými malwarem (defaultně vypnuto). Pokud je tato funkce zapnuta, bude při každém spuštění programu, který není podepsán digitálním certifikátem (není v databázi důvěryhodných programů), zobrazeno hlášení, co se s takovýmto programem má udělat (přidat ho do důvěryhodných programů, spustit ho či ho zablokovat) – doporučuji zapnout.
- **Záložka Containment –** obsahuje nastavení ohledně virtualizace

  Pokud je nastavení Containmentu zapnuto (defaultně ano), některé programy (na základě vyhodnocení) budou automaticky spuštěny ve virtualizovaném prostředí. Takovéto programy pak mají zvýrazněný okraj oken, a to pomocí zelené barvy. Barva však není dobře viditelná, a poměrně často lze takovýto okraj lehce přehlédnout – doporučuji vypnout - ostatní funkce by vás před možnými hrozbami měli zabezpečit a popřípadě je zarazit.
- **Záložka Hodnocení souborů** - Umožňuje zobrazení důvěryhodných vydavatelů softwaru, včetně možnosti přidaní či odebrání vydavatele, a také nastavení jak bude jeho software vyhodnocován.
- **Záložka pokročilá ochrana** - Umožňuje zapnout VirusScope - slouží pro vyhodnocování běžících procesů, a v případě, že by nějaký proces mohl narušit soukromí či bezpečnost uživatele, umožňuje takovýto proces (běžící program) ukončit a vymazat.

4.2.1.3 Zatížení systému při kontrole

Obrázek níže nám ukazuje, jak byl systém zatížen při kontrole 80 GB disku.

Pro kontrolu souborů pak byla použita vlastní kontrola (obdobná kontrola jako u dalšího testovaného produktu) včetně heuristické analýzy.

Disk byl rozdělen na dva samostatné oddíly C a D. Oddíl C byl pak zaplněn 50 GB velkých a malých souborů, včetně adresáře s operačním systémem. Oddíl D byl pak zaplněn 30 GB převážně souborů malých.

Pro zjištění zatížení systému, byl použit program ProcessMonitor, který umožňuje generovat vytížení jednotlivých systémových prostředků za jednotlivé procesy, a to v podobě grafů.

Poznm. - Obrázek zde není přidělen jelikož 3 ze 4 měření vykazovalo špatné hodnoty, a obrázek se správnými hodnotami byl špatně pořízen – měření pak bylo otestováno pomocí jiných dostupných prostředků. Jsou zde tedy alespoň vypsány průměrné hodnoty zatížení systémových prostředků.

Dostupné systémové prostředky: Operační systém – Windows 7 - 64bit
Operační paměť – 8 GB RAM
Procesor – Intel Core i7 – 3612QM, 2,7 GHz

Naměřené průměrné zatížení systémových prostředků: HDD – 50%
CPU - 20%
RAM 720 MB

4.2.1.4 Klady a zápory

- **Klady**
  - Virová databáze obsahuje přes 50 000 000 nebezpečných definic.
  - Přehledné uživatelské prostředí, které zajišťuje snadný přístup k běžným funkcím.
  - Pokročilé technologie a funkce (HIPS, virusscope, virtualizované prostředí, hodnotící kontrola).
  - Komunitou vytvořený český jazyk (až na některá místa funguje perfektně).

- Možnost neomezeného zaslání souborů k vyhodnocení do společnosti Comodo.
- Pravidelné aktualizace virové databáze (i několikrát týdně).
- Umožnuje v programu tzv. drag and drop – uživatel nemusí provádět kontrolu souboru přímo na něm, ale stačí jej přetáhnout do programu.
- Obsahuje databázi důvěryhodných vydavatelů softwaru.
- Je nenáročný na běh systému.
- Dokáže zajistit ochranu před nebezpečnými webovými stránkami.
- Plná technická podpora na 60 dní zdarma.
- Umožňuje detekci potencionálně nechtěných programů.
- Jedná se o zdarma dostupný program.
- Při kontrole souboru zobrazuje, kolik % souborů již bylo zpracováno.
- Instalace programu netrvá příliš dlouho (cca 25 min).

- **Zápory**
  - V defaultním nastavení, zapíná automaticky některé programy ve virtualizovaném prostředí.
  - Velmi široké možnosti nastavení pravidel, které může běžný uživatel špatně nastavit.
  - Skoro žádné vysvětlení některých složitějších kontrol a funkcí (oproti jiným programům).
  - Neobsahuje v sobě příručku s nápovědou k programu.
  - Větší počet falešných detekcí.

4.2.1.5 Celkové hodnocení

Antivirový program od společnosti Comodo nabízí velice slušnou ochranu před nebezpečnými škodlivými kódy. Tuto ochranu umožňuje provádět hlavně díky několika funkcím, které v sobě obsahuje a které mají zajistit odhalení potencionálních nebezpečných hrozeb. Pokud se pak uživatel prokousá jednotlivými nastaveními, rozhodně bych ho doporučil jako dobrý antivirový program pro ochranu výpočetní techniky.

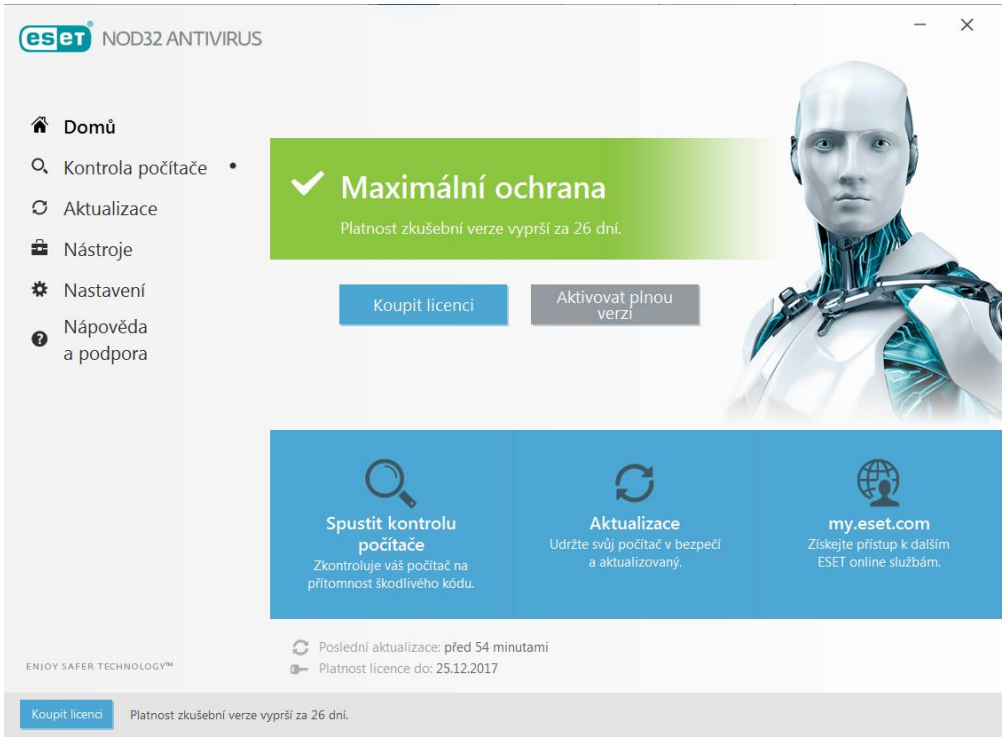
4.2.2 Eset NOD32

Testována verze: 11.0.149.0

Jako druhý antivirový program jsem vybral produkt od slovenské společnosti Eset, a to na základě několika doporučení mých přátel a internetových recenzí. Všichni si ho velice chválí, a organizace AV Comparatives ho dokonce zvolila jako nejlépe hodnocený produkt roku 2016, a rovněž mu udělila zlaté ocenění za málo falešných detekcí a velice přátelské uživatelské rozhraní. Osobně jsem tedy i já sám zvědavý, jak si povede v mé analýze.

4.2.2.1 První spuštění

Program po svém spuštění, uživatele přivítá velice přátelským a opravdu jednoduchým uživatelským rozhraním, ve kterém je velice jednoduché se zorientovat. Uživatel zde má možnost spustit kontrolu počítače, provést aktualizaci programu a virové databáze, a možnost přejít na stránky výrobce. Dále mu je zde sdělena informace o tom, kdy byla provedena poslední aktualizace, a platnost zakoupené licence. Po levé straně pak má uživatel možnost přepínat mezi jednotlivými záložkami, které obsahují nastavení a funkce programu.



Obrázek 8 - Eset - Uživatelské rozhraní

4.2.2.2 Jednotlivé záložky

- **Kontrola počítače** – obsahuje informace o poslední provedené kontrole, a umožňuje spustit následující typy kontrol:
  - **Smart kontrola** – rychlá kontrola počítače, která léčí infikované soubory, bez potřeby zásahu uživatele. Kromě souborů, které se mají zkontrolovat, v sobě obsahuje také kontrolu operační paměti, boot sektoru a archivů. Kromě toho spouští také heuristickou analýzu. Dále je tato kontrola spuštěna s nízkou prioritou, což znamená, že pokud uživatel během kontroly pracuje s programy, které mají vysoké nároky na systém, tak se sníží výpočetní zdroje, které byly přiděleny této kontrole. Kontrola pak používá tzv. smart optimalizaci, která používá předdefinované nastavení pro dosažení nejefektivnější ochrany systému a rychlosti kontroly.
  - **Kontrola počítače z kontextového menu** – na rozdíl od předchozí kontroly, nekontroluje operační paměť a boot sektor – osobně nedoporučuji používat - je lepší, když do kontroly počítače bude vždy zahrnuta operační paměť a boot sektor.
  - **Hloubková kontrola počítače** – oproti předchozím kontrolám nepoužívá smart optimalizaci – pomalejší než smart kontrola, ale za to důkladnější. Doporučuji používat, pokud chce uživatel dosáhnout co nejefektivnější kontroly.

    Poznm. - Jednotlivé typy kontrol jdou pak detailněji nastavit (v záložce nastavení) a lze u nich ještě provést kontrolu poštovní schránky, léčení souborů, či zápis všech zkontrolovaných souborů do protokolu.
- **Aktualizace -** Obsahuje informace o aktuální verzi programu, poslední aktualizaci a o jejich poslední kontrole dostupnosti. V rozšířeném nastavení lze pak nastavit zálohování modulů před každou aktualizací (defaultně zapnuto), zda se má program sám aktualizovat, a zda se má před stažením aktualizací uživatele vždy dotázat.
- **Nástroje -** Obsahují informace o důležitých událostech programu ESET (blokované soubory, zachycené hrozby, události apod.), statistiky ochrany, informace o souborech v karanténě a plánovač úloh. Dále také obsahuje pomocné nástroje, které

sledují spuštěné procesy, či umožňují podezřelý soubor odeslat k analýze do společnosti ESET.

- **Nastavení** – obsahuje nastavení počítačové a internetové ochrany
  - Umožňuje zapnout / vypnout rezidentní ochranu souborového systému – ochrana souborů používaných programy a operačním systémem.
  - Umožňuje zapnout / vypnout HIPS – odhaluje a zabraňuje nežádoucímu chování aplikací.
  - Umožňuje zapnout / vypnout ochranu přístupu na web – blokuje přístupy na stránky se škodlivým obsahem.
  - Umožňuje zapnout / vypnout ochranu poštovních klientů – kontroluje odeslané a přijaté e-maily prostřednictvím poštovních klientů (Outlook, Thunderbird).
  - Umožňuje zapnout / vypnout anti-phisingovou kontrolu – blokuje přístup na podvodné webové stránky.
  - **Umožňuje vstup do rozšířeného nastavení –** zde má uživatel možnost zapnout detekci potencionálně nechtěných a zneužitelných programů (generátory licenčních klíčů, software pro vzdálený přístup nebo ovládání počítače apod.), a také možnost vypnutí odesílání anonymních statistik, a podezřelých souborů a procesů – defaultně zapnuto. Dále je zde možnost nastavení kontroly počítače při nečinnosti systému (např. když je uživatel odhlášen, či je zamknutá nebo vypnutá obrazovka) a nastavení uživatelského rozhraní. Rozšířené nastavení pak také obsahuje nastroj, který uživatele upozorní na chybějící aktualizace operačního systému Windows, a to od úrovně volitelné aktualizace, až po úrovně aktualizace kritické.
- **Nápověda a podpora** - Obsahuje nápovědu pro antivirový produkt ve formě internetových odkazů. Jednotlivé odkazy pak směřují na ESET databázi znalostí, řešení nejčastějších problémů, a včetně nápovědi k programu. Nápověda je pak dostupná přímo i v samostatném programu, a i velice nezkušenému uživateli dobře vysvětlí jednotlivé funkce programu. Nápověda dále obsahuje virovou encyklopedii, ve které uživatel může najít aktuální i staré bezpečnostní hrozby.

4.2.2.3 Zatížení systému při kontrole

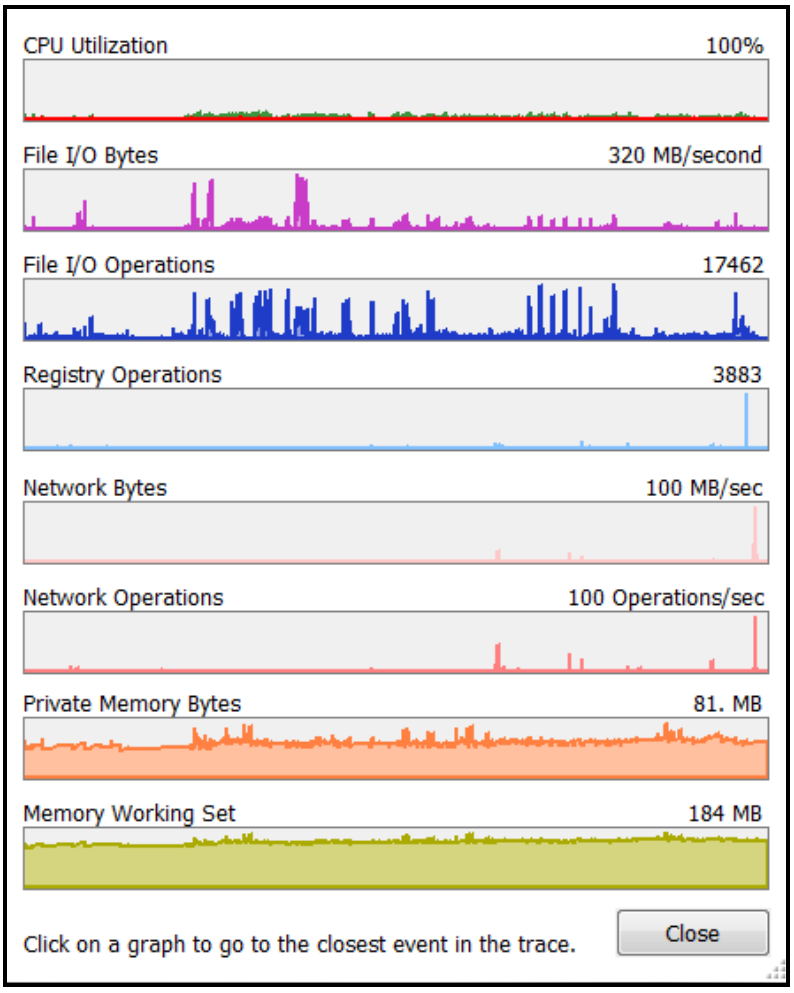
Obrázek níže nám ukazuje, jak byl systém zatížen při kontrole 80 GB disku.

Pro kontrolu souborů pak byla použita kontrola: Kontrola počítače z kontextového menu.

Disk byl rozdělen na dva samostatné oddíly C a D. Oddíl C byl pak zaplněn 50 GB velkých a malých souborů, včetně adresáře s operačním systémem. Oddíl D byl pak zaplněn 30 GB převážně souborů malých.

Pro zjištění zatížení systému, byl použit program ProcessMonitor, který umožňuje generovat vytížení jednotlivých systémových prostředků za jednotlivé procesy, a to v podobě grafů.

Dostupné systémové prostředky: Operační systém – Windows 7 - 64bit
Operační paměť – 8 GB RAM
Procesor – Intel Core i7 – 3612QM, 2,7 GHz



Obrázek 9 - Eset - Zatížení výpočetních prostředků při kontrole

Vysvětlivky: **CPU Utilization** - zobrazuje vytížení procesoru – průměr 10%

File I/O Bytes a Operation - zobrazuje vytížení pevného disku - pruměr 30%

Private Memory Bytes a Memory Working Set – zobrazuje kolik bylo použito paměti RAM – průměr 300 MB

4.2.2.4 Klady a zápory

- Klady
  - Možnost kontroly počítače při nečinnosti systému (např. když je uživatel odhlášen, či je zamknutá nebo vypnutá obrazovka).
  - Velice přátelské a přívětivé rozhraní programu.
  - Pokročilé technologie a funkce (HIPS, ochrana přístupu na web, ochrana poštovních klientů, anti-phisingová kontrola, …).
  - Dokáže uživateli velice jednoduše vysvětlit veškeré funkce, nastavení, kontroly apod.
  - Ochrana před potencionálně necjtěnými a nebezpečnými programy a procesy
  - Je nenáročný na běh systému.
  - Obsahuje nástroj, který uživatele upozorní na chybějící aktualizace.
  - Získané ocenění od organizace AV Comparatives.
  - Český jazyk
- Zápory
  - Poměrně dlouhá doba instalace (cca 60 min)
  - Jedná se o placený software – cena však není nijak závratná - 1 209 Kč za rok
  - Odesílá anonymní statistiky – lze vypnout
  - Odesílá vzorky podezřelých souborů a procesů – lze vypnout

4.2.2.5 Celkové hodnocení

Antivirový program od slovenské společnosti Eset mě velice mile překvapil. Obsahuje velice příjemné a přehledné uživatelské rozhraní, ve kterém se musí zorientovat i naprostý laik. Jeho skvěle nastavení kontroly nebezpečných kódů, potencionálně

nebezpečných či nechtěných programů, e-mailových klientů …, by i nezkušenému uživateli mělo zajistit velice velkou ochranu před nakažením. Běžnému uživateli je pak antivirový program také velice nápomocný, a vysvětlí mu takřka všechny funkce, nastavení, kontroly, zkrátka vše, co v programu uživatel může nalézt. Jedinou jeho nevýhodou pak může být pouze jen cena, ale ta je k poměru všech výhod velice zanedbatelná, a proto mi nezbývá nic jiného než vřele doporučit tento skvělý antivirový program od slovenské společnosti.

4.3 Porovnání vybraných programů

Níže můžeme najít kriteriální tabulku. Je založena na bodovací metodě, a má za úkol pomoci při vybrání finálního vítěze.

Kritéria / Antivirové programy	Comodo Antivirus	Eset NOD32
Vytížení CPU při kontrole	8	10
Vytížení RAM při kontrole	4	10
Vytížení HDD při kontrole	5	8
Doba testované kontroly	5	11
Typy kontroly	9	11
Ochrana před nebezpečnými web. stránkami	8	11
Detekce potencionálně nechtěných programů	11	11
Doba instalace programu	8	6
Falešné detekce	7	11
Nápověda k programu	5	11
Cena	11	6
Celkem	81	106

Tabulka 3 - Kriteriální tabulka

Na základě analýzy, celkového hodnocení a této kriteriální tabulky, musím označit za jasného vítěze antivirový produkt Eset NOD32. Uživateli je tedy doporučeno zvolit antivirový program Eset NOD32, před antivirovým programem Comodo Antivirus 10.

4.4 Jiné způsoby ochrany

Další možností, jak výpočetní techniku dále ochránit před nebezpečnými kódy, poskytují tzv. online antivirové programy. Oproti real-time antivirovým programům však nenabízejí ochranu v reálném čase, a slouží pouze pro jednorázové kontroly. Online antivirové programy jsou pak rozdělné na webové antiviry, které se používají pro kontroly souborů a dokumentů, pomocí webové stránky, a na online antiviry, které ke svému spuštění potřebují podpůrný program.

Webové antiviry pak umožňují uživateli nahrát soubor či dokument na určitou webovou stránku, kde je pak uložena databáze několika antivirových programů. Určitý soubor či dokument je pak zkontrolován pomocí těchto databází, a na jejich základě potom provede vyhodnocení – pokud je soubor či dokument nakažený, nedokáže ho však smazat, jelikož ho uživatel pouze nahrál, a soubor či dokument je tedy testován přímo na příslušné webové adrese – nikoliv v uživatelově počítači.

Podpůrné programy pak slouží pro jednorázovou kontrolu počítače či jednotlivých souborů, a neinstalují se. Pouze se jen spustí, a nastaví se u nich možnosti kontroly (bootsektrou, operační paměti, potencionálně nechtěných programu …), tak jako u real-time antivirových programů.

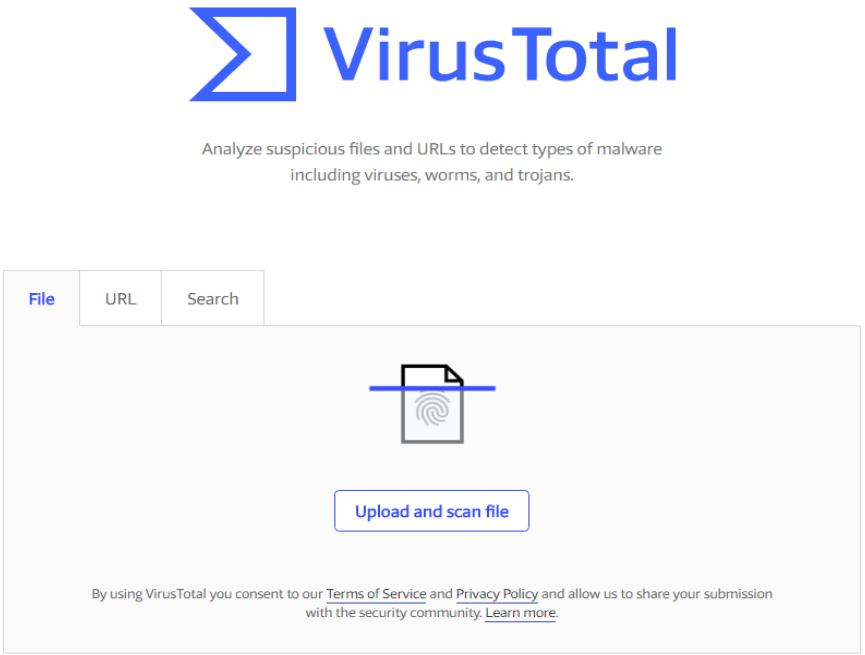
Webové a online antivirové programy pak tedy slouží jen k jednorázové kontrole určitých souborů, dokumentů, či celého PC, po které potom ukončí svoji činnost - a právě v tom je jejich hlavní nevýhoda – nedokáží uživatele chránit v reálném čase.

Osobně doporučuji tyto antiviry používat tedy jako dodatečnou kontrolu, pokud si uživatel není jistý tím, zda daný soubor, program nebo webová stránka neobsahuje něco podezřelého, či si není jistý výsledkem kontroly svého antivirového programu.

4.4.1 VirusTotal

Jako jednu z možností webového antivirového programu jsem vybral dnes již poměrně známy VirusTotal od společnosti Google. Osobně ho znám přibližně 7 let, a za tu dobu jsem ho již několikrát použil, a to převážně ke kontrole souborů, u kterých jsem si nebyl jistý, zda obsahují nějaký nebezpečný kód či nikoliv.

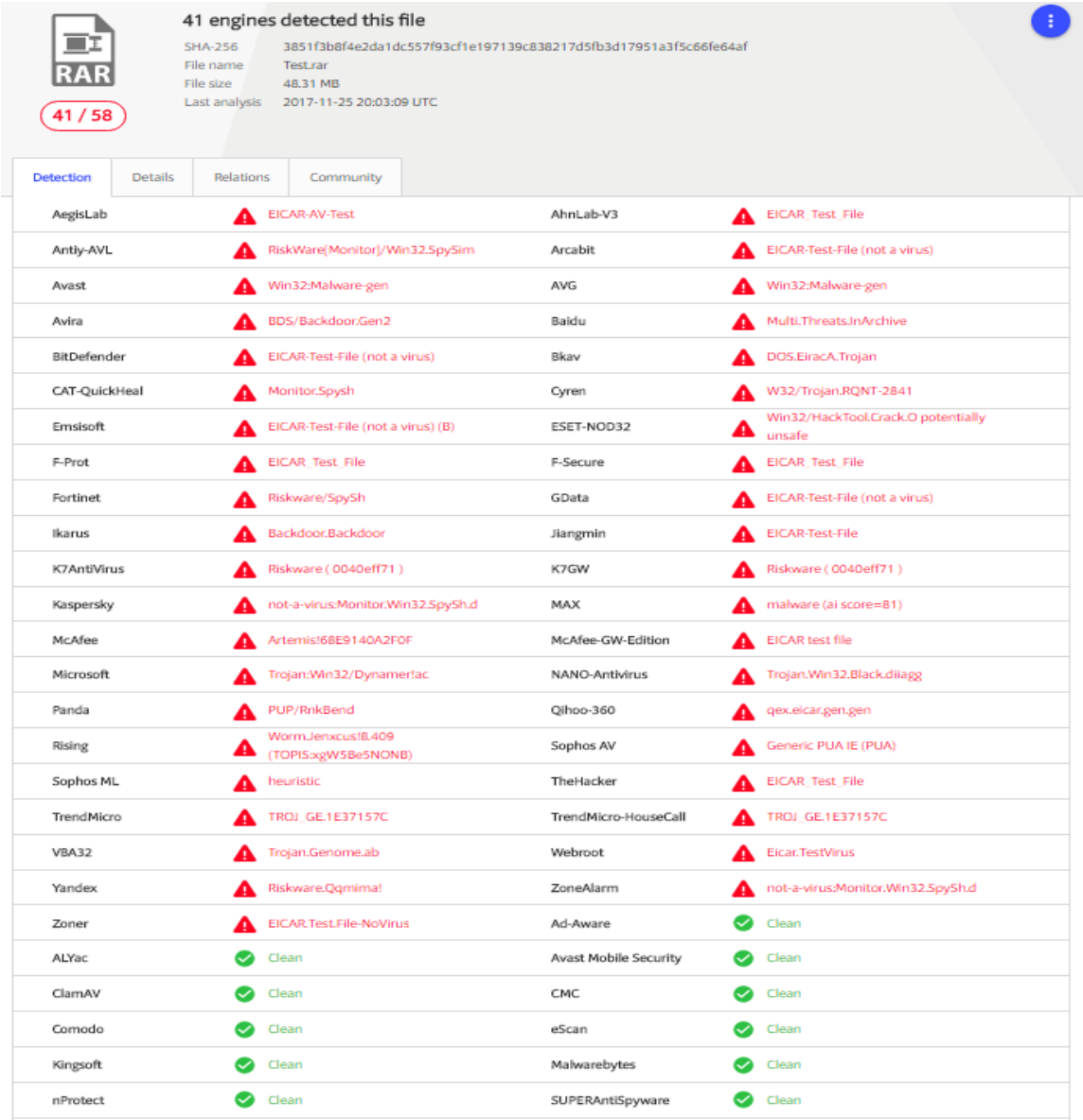
VirusTotal je pak dostupný prostřednictvím webové stránky, a to na adrese https://www.virustotal.com. Pokud se ho tedy uživatel rozhodne použít, webová stránka ho přivítá velice jednoduchým a přátelským prostředím. Dovolím si i říci, že by ho byl schopný použít i velice nezkušený uživatel. Na úvodní stránce má potom uživatel možnost nahrání a následné kontroly jednotlivých souborů či dokumentů, a to až ve velikosti 256 MB. Soubory a dokumenty pak musí uživatel nahrávat pouze jednotlivě – nelze tedy nahrát například dva či více souborů a dokumentů najednou. Doba nahrání a následné kontroly pak závisí na velikosti jednotlivých dat a rychlosti internetového připojení. Pokud již byl někdy v minulosti nahraný obsah kontrolován, následná kontrola je provedena mnohem rychleji. Kromě kontroly souborů a dokumentů, nabízí VirusTotal také kontrolu webových stránek. Pokud se tedy uživatel domnívá, že určitá webová stránka obsahuje malware, může jí pomocí VirusTotalu prověřit. VirusTotal dále také nabízí možnost vyhledávání již v minulosti nahraných souborů, dokumentů či webových stránek, a to včetně jejich vyhodnocení a podrobnějších informací.



Obrázek 10 - VirusTotal - Úvodní stránka

Kontrola jednotlivých souborů a dokumentu je pak provedena pomocí několika antivirových programů (70). Ty prověřují obsah kódu nahraných objektů, a pokud se kus kódu shoduje s tím, co mají antivirové programy zapsané ve své virové databázi, vyhodnotí soubor či dokument jako škodlivý. V případě webových stránek pak ještě navíc kontrolují, zda již není zařazena do seznamu nebezpečných stránek (např. v databázi

Googlu). Každý antivirový program pak vypíše, jaký malware v nahraném souboru či dokumentu našel. Po vyhodnocení jednotlivými antivirovými programy, má uživatel možnost zkontrolovat hlášení ještě podle ostatních lidí, kteří zde občas dopíšou, že se jedná pouze o falešné hlášení.



Obrázek 11 - VirusTotal - Kontrola pomocí několika antivirů

4.4.1.1 Klady a zápory

- **Klady**

  Funkční čeština, porovnání nahraného obsahu pomocí několika antivirových programů, možnost kontroly webových stránek, nezatěžuje operační systém (zatěžuje server), zdarma dostupný, jednoduché uživatelské rozhraní, možnost

vyjádření komunity a expertů k hodnoceným souborům, pravidelně aktualizované virové databáze, sdílí výsledky kontrolovaných souborů s ostatními uživateli, je dostupný na různých operačních systémech, neinstaluje se, rychlá reakce na nový malware

- **Zápory**

  Potřeba internetové připojení, nemožnost kontroly obsahu celých složek, nemožnost kontroly celého disku, PC a paměti, nedokáže uživatele chránit v reálném čase, mohou ho zneužít počítačový útočníci, kteří na něm testují svůj kód – zjistí, kolik antivirových programů ho odhalilo, a následně se jej snaží přepsat do podoby, kterou by antivirový program neodhalil.

4.4.1.2 Celkové hodnocení

VirusTotal je velice šikovným webovým antivirovým programem, který by uživatel měl v případě nejistoty před nebezpečím, rozhodně využít. Umožní mu potenciálně nebezpečný soubor či webovou stránku vyhodnotit, a to během několika minut. Na základě vyhodnocení se pak uživatel dozví, zda soubor či webová stránka obsahují nějaký nebezpečný kód. Může se tak tedy preventivně chránit před potencionálním nakažením.

Osobně ho však nedoporučuji používat jako jediný „antivirový program“, který uživateli může zajistit ochranu před nebezpečnými kódy. VirusTotal pracuje totiž na straně serveru, nikoliv uživatele, a nechrání ho tedy před hrozbami v reálném čase.

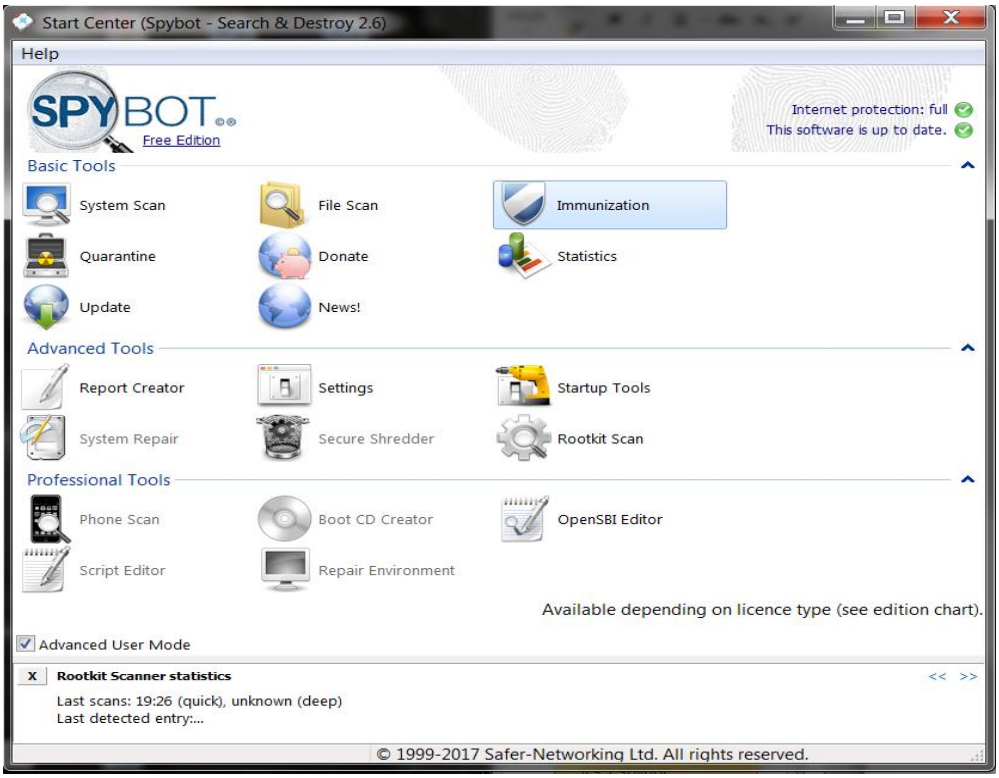
Virus Total tedy doporučuji jako doplňkový nástroj v případě potřeby, pokud si uživatel není jist tím, zda webová stránka či soubor neobsahuje něco škodlivého.

4.4.2 Spybot

Testována verze: 2.6. Free

Jako další podpůrný program, který již není online a slouží také na rozeznání malwaru, jsem vybral program Spybot, který mi byl doporučen cca před 3 roky. Dá se tedy předpokládat, že program za tu dobu prošel velikými změnami a mohl by se vyrovnat mnoha konkurenčním programům.

Po instalaci programu, která trvala přibližně necelé 2 minuty, jsem program zapnul a přivítal mě velice obstarožním uživatelským rozhraním.



Obrázek 12 - Spybot - Rozhraní programu

Orientace v obstarožním prostředí však byla jednoduchá a takřka ihned jsem našel tlačítko pro aktualizaci virové databáze. Očekával jsem, že to zabere i několik minut a šel jsem se tedy mezitím věnovat jiné práci. Jaké překvapení však bylo, když ani ne po 3 minutách byla aktuální virová databáze stažena. V domnění, že se jedná o nějakou chybu programu, jsem tedy dal virovou databázi stahovat znovu. Program však zahlásil, že stažená virová databáze je již aktuální. Podíval jsem se tedy do protokolu o stažené virové databázi a byl jsem nemile zklamán. Dostupná virová databáze obsahovala pouze 100 nebezpečných kódů, což je v dnešní době, kde nebezpečí číhá na každém rohu, opravdu velice málo. Dovolím si tedy tvrdit, že tento program je na boj proti nebezpečnému malwaru velice neúčinný.

Na jednom českém webu (stahuj.centrum.cz) jsem také zjistil, že navzdory tomu, že nedokáže rozeznat skoro žádný malware, si ho stejně během 7 dnů stáhlo již 300 uživatelů, což je poměrně velké číslo, pokud bychom brali fakt, že by všechny tyto počítače, které jsou chráněny pouze tímto softwarem, mohl při splnění více kritérií zneužít počítačový útočník.

Testová verze je však 2.6 Free a je zdarma dostupná komukoliv. Firma však nabízí ještě verzi Home a Professional Plus, která nabízí stažení většího obsahu virové databáze, které by tedy mohly zvednout ochranu systému i o 100 %. Tyto verze jsou pak postaveny

na enginu antivirového programu Bitdefender, který mimo jiné dostal i ocenění vynikajícího produktu za rok 2016. Tyto verze si však uživatel nemůže zdarma vyzkoušet, a proto jsem je v testování nemohl zohlednit. Licence se pak kupuje na rok, a cena se pohybuje v přívětivém rozmezí 300 – 600 Kč, v závislosti na verzi a měny, ve které se bude program kupovat (dolary nebo eura).

4.4.2.1 Celkové hodnocení

Jelikož testovaná verze velmi neuspěla v obsahu virové databáze, což je jeden z nejdůležitých faktorů, nebudu zde vypisovat žádné klady – osobně mě nic ani kladného nenapadá. Zmíním jen tedy jeho obrovskou nevýhodu – neobsahuje aktuální virové definice, a obsah virové databáze je velice malý.

Na základě toho zjištění nedoporučuji uživateli stahovat verzi 2.6 Free, jelikož ho nedokáže ochránit před možnými hrozbami malwaru.

5 Závěr

Kvůli neustálému vývoji výpočetní techniky, rostoucímu počtu uživatelů a rostoucímu počtu nebezpečných kódů a podvodných technik, je dnes ochrana výpočetní techniky a bezpečnost uživatele, velice aktuální téma. Mnoho uživatelů se však poměrně moc ochraně a bezpečnosti nevěnuje, a tak vystavují výpočetní techniku a také hlavně sebe riziku napadení.

Proto bylo cílem mé bakalářské práce seznámit uživatele s možnou ochranou a prevencí, a to jak sebe sama, tak i výpočetní techniky, kterou využívají. Dílčím cílem poté bylo srovnání vybraných možných programů, které mohou či nemusí zajistit ochranu uživatele a výpočetní techniky.

Běžný uživatel by pak měl využít slovenského produktu Eset NOD32, který zajišťuje vynikající ochranu a bezpečnost, před možnými možnosti napadení. Pro dodatečnou kontrolu souboru či dokumentů, by pak měl použít webového antivirového programu VirusTotal. Ten však oproti Eset NOD32 neumožňuje ochranu v reálnem čase.

S rostoucím počtem nebezpečných kódů a technik, vznikají stále nové antivirové programy, které před těmito hrozbami chrání. Je tedy doporučeno používat spolu se selským rozumem a prevencí, také příslušné nástroje, které zajistí bezpečnost a ochranu výpočetní techniky a uživatele.

6 Seznam použitých zdrojů

1. ČÍŽEK, Jakub. Skupina Wikileaks zveřejnila další úniky ze CIA. Popisují tvorbu virů pro Windows. *Živě.cz – O počítačích, IT a internetu* [online]. Brno: CN Invest, 2017, 10. dubna 2017 [cit. 2017-04-10]. Dostupné z: http://www.zive.cz/bleskovky/skupina-wikileaks-zverejnila-dalsi-uniky-ze-cia-popisuji-tvorbu-viru-pro-windows/sc-4-a-187117/default.aspx
2. HÁK, Bc. Igor. Moderní počítačové viry, třetí vydání. *Fakulta stavební VUT v Brně* [online]. (PDF). Brno: Fakulta Stavební VUT, 15. září 2005 [cit. 2017-04-10]. Dostupné z: http://www.fce.vutbr.cz/aiu/vojkuvka.m/u3v/vyuka/Kniha-o-virech.pdf
3. CANBEDONE. Hand highlighting Malware tag cloud clear glass isolated on white. *Hand Highlighting Malware Tag Cloud Clear* [online]. New York City: Shuttlerstock Inc., © 2003-2017 [cit. 2017-04-10]. Obrázek ve formátu JPEG. Dostupné z: https://www.shutterstock.com/cs/image-photo/hand-highlighting-malware-tag-cloud-clear-577481197?src=y5yuZ2F54lPunkc7jDXVPQ-1-6
4. What is a Computer Virus? *Norton - Antivirus Software and Spyware Removal* [online]. United States: Symantec Corporation, ©1995-2017 [cit. 2017-04-10]. Dostupné z: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html
5. SOBOTKA, Jakub. Pozor! První škodlivé makro pro Apple MacOS objeveno. *Techbrain* [online]. Techbrain.cz, ©2016-2017 [cit. 2017-04-10]. Dostupné z: https://techbrain.cz/pozor-prvni-skodlive-makro-apple-macos-objeveno/
6. BITTO, Ondřej. Trojské koně: co jsou zač a jak se bránit. *Živě.cz – O počítačích, IT a internetu* [online]. Brno: CN Invest, ©2017 [cit. 2017-04-10]. Dostupné z: https://www.zive.cz/clanky/trojske-kone-co-jsou-zac-a-jak-se-branit/sc-3-a-123708/
7. KIGUOLIS, Linas. Co je to trojské koně a jak jej odstranit. *Bezpečnost a novinky o virech* [online]. Odstranitvirus.cz, ©2001-2017, 26. dubna 2016 [cit. 2017-04-15]. Dostupné z: https://odstranitvirus.cz/trojske-kone/
8. BRADLEY, Mitchell. What Is a Keylogger and Key Logging Software? *Lifewire* [online]. Lifewiere.com, [cit. 2017-15-10]. Dostupné z: https://www.lifewire.com/definition-of-keylogger-817998

9. JANSSEN, Cory a Dale. Destructive Trojan. *Techopedia - Where Information Technology and Business Meet* [online]. Techopedia Inc., ©2017 [cit. 2017-04-15]. Dostupné z: https://www.techopedia.com/definition/53/destructive-trojan
10. KIGUOLIS, Linas How to remove backdoors. *Security and spyware news* [online]. 2-spyware.com, ©2001-2017, 11. května 2017 [cit. 2017-04-21]. Dostupné z: https://www.2-spyware.com/backdoors-removal
11. Trojan-Downloader. *F-Secure | Cyber Security Solutions for your Home and Business* [online]. F-Secure, ©2017 [cit. 2017-04-21]. Dostupné z: https://www.f-secure.com/v-descs/trojan-downloader.shtml
12. What is a Trojan Downloader? *Server Intellecet The Windows Server Experts* [online]. SingleHop Company, ©2017 [cit. 2017-04-21]. Dostupné z: https://www.serverintellect.com/support/techfaq/trojan-downloader/
13. Co je to virus, červ a trojský kůň? *Srpenec* [online]. Srpenec.cz, 19. února 2011 [cit. 2017-04-21]. Dostupné z: http://www.srpenec.cz/internet/bezpecnost/co-je-to-virus-cerv-a-trojsky-kun
14. Email-Worm. *Securelist* [online]. Securelist.com, ©2017 [cit. 2017-04-21] Dosutpné z: https://securelist.com/threats/email-worm/
15. Worm. *Wikia* [online]. Malware Wiki, ©2009 [cit. 2017-05-10]. Dostupné z: http://malware.wikia.com/wiki/Worm
16. KIGUOLIS, Linas. Facebook video virus. How to remove? *2-spyware* [online]. 2-spyware.com, ©2001-2017, 11. ledna 2017 [cit. 2017-05-10]. Dostupné z: https://www.2-spyware.com/remove-facebook-video-virus.html
17. BIJALWAN, Abhishek. Which are the different types of Computer Worms?. *Quora* [online]. Quora, 2016 [cit. 2017-05-17]. Dostupné z: https://www.quora.com/Which-are-the-different-types-of-Computer-Worms
18. Spyware. *Správa sítě - slovník pojmů: správa sítě, zabezpečení sítě, outsourcing IT* [online]. Praha: Aira GROUP, ©2016 [cit. 2017-05-17]. Dostupné z: http://www.sprava-site.eu/spyware/
19. Viry, adware, spyware, rootkity a další malware. *Západočeská univerzita* [online]. Plzeň: Západočeská univerzita, ©1991-2017 [cit. 2017-05-17] Dostupné z: http://home.zcu.cz/~koderova/

20. MORELI, Olivia. Co je to adware a jak jej odstranit. Bezpečnost a novinky o virech [online]. Odstranitvirus.cz, ©2001-2017, 26. dubna 2016 [cit. 2017-05-17]. Dostupné z: https://odstranitvirus.cz/adware/
21. KOPECKÝ, Dr. Kamil. Co je hoax. *Projekt E-bezpečí* [online]. Olomouc: Univerzita Palackého, ©2008 – 2017, 18. května 2008 [cit. 2017-05-17]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25
22. DŽUBÁK, Josef. Phishing: Co je to Phising. *Hoax* [online]. Hoax.cz, ©2000-2017 [cit. 2017-05-24]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing
23. ALI. Jak funguje ransomware? *CIO Business World.cz | IT strategie pro manažery* [online]. Praha: IDG, 30. listopadu 2016 [cit. 2017-05-24]. Dostupné z: http://businessworld.cz/bezpecnost/jak-funguje-ransomware-13282
24. Ransomware. *Trend Micro Eastern Europe - Securing Your Journey to the Cloud* [online]. Irsko: Trend Micro, ©1989-2017 [cit. 2017-05-24]Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/ransomware
25. ČÍŽEK, Jakub. WannaCry se neměl vůbec rozšířit. Stačilo, abychom používali Windows Update. *Živě.cz – O počítačích, IT a internetu* [online]. Brno: CN Invest, 2017, [cit. 2017-05-24]. Dostupné z: https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx
26. EKB, Info.cz. WannaCry je slabý odvar. Šíří se nový virus, který zotročí vaše PC a nechá ho těžit obdobu bitcoinů. *Info.cz* [online]. CZECH NEWS CENTER, ©2001 – 2017, 18. května 2017 [cit. 2017-06-10]. Dostupné z: http://www.info.cz/svet/wannacry-je-slaby-odvar-siri-se-novy-virus-ktery-zotroci-vase-pc-a-necha-ho-tezit-obdobu-bitcoinu-9815.html
27. ADK, Info.cz. Bitcoin jako zbraň teroristů. Anonymitu kryptoměn využívá nejen Islámský stát. *Info.cz* [online]. CZECH NEWS CENTER, ©2001-2017, 19. srpna 2017 [cit. 2017-06-26]. Dostupné z: http://www.info.cz/svet/bitcoin-jako-zbran-teroristu-anonymitu-kryptomen-vyuziva-nejen-islamsky-stat-14605.html
28. DOEVAN, Jake. Bitcoinový virus. Jak ho odstranit? (Průvodce odinstalace). *Bezpečnost a novinky o virech* [online]. Odstranitvirus.cz, ©2001-2017, 17. října 2017 [cit. 2017-06-10]. Dostupné z: https://odstranitvirus.cz/bitcoinovy-virus/
29. KRČMÁŘ, Petr. Pronajmu botnet, ceník přiložen… aneb jak se dělá DDoS. *Root.cz - informace nejen ze světa Linuxu* [online]. Internet Info, ©1998-2017, 8. Března 2013

[cit. 2017-06-26]. Dostupné z: https://www.root.cz/clanky/pronajmu-botnet-cenik-prilozen-aneb-jak-se-dela-ddos/

30. Co je to botnet. *Jak na webové stránky - Zvyšování výkonu a bezpečnost webových stránek* [online]. Timehosting.cz, 18. února 2015 [cit. 2017-06-26]. Dostupné z: http://timehosting.cz/co-je-botnet/
31. PEREZ, Carlos. Reaper IoT Botnet. *Tenable™ - The Cyber Exposure Company* [online]. Tenable.com, ©2017 26. října 2017 [cit. 2017-06-26]. Dostupné z: https://www.tenable.com/blog/reaper-iot-botnet
32. HOFFMAN, Chris. *50+ File Extensions That Are Potentially Dangerous on Windows* [online]. How To Geek, ©2006-2017, 12. února 2013 [cit. 2017-07-10]. Dostupné z: https://www.howtogeek.com/137270/50-file-extensions-that-are-potentially-dangerous-on-windows/
33. HOFFMAN, Chris. How To Spot A Danger Email Attachmanet. *MakeUseOf - Technology, Simplified* [online]. Makeusof.com, ©2017 [cit. 2017-07-10]. Dostupné z: http://www.makeuseof.com/tag/spot-dangerous-email-attachment/
34. Pozor na nebezpečné přílohy ve formátu ZIP! *mBank – internetová banka, z které vyřídíte téměř vše online | osobní finance* [online]. Praha: mBank, ©2015, 9. září 2014 [cit. 2017-07-10]. Dostupné z: https://www.mbank.cz/blog/post,521,pozor-na-nebezpecne-prilohy-ve-formatu-zip.html
35. Independt Test of Anti-Virus Sofrware. *AV-Comparatives Independent Tests of Anti-Virus Software - AV-Comparatives* [online]. AV-comparatives.org, ©2017 [cit. 2017-07-20]. Dostupné z: https://www.av-comparatives.org
36. Antivirové centrum. *Antivorve centrum* [online]. Praha: Amenit s.r.o., ©2017 [cit.2017-07-20]. Dostupné z: https://www.antivirovecentrum.cz