VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2019 Miluše Havlová

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

VIRTUÁLNÍ PROSTŘEDÍ PRO ZAJIŠTĚNÍ DŮKAZNÍHO MATERIÁLU
EVIDENCE SECURING IN VIRTUAL ENVIRONMENT

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

Miluše Havlová

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Zdeněk Martinásek, Ph.D.

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Informační bezpečnost**
Ústav telekomunikací

Studentka: Miluše Havlová ***ID:*** 195827
Ročník: 3 ***Akademický rok:*** 2018/19

NÁZEV TÉMATU:

Virtuální prostředí pro zajištění důkazního materiálu

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je návrh vhodného prostředí pro zajištění důkazního materiálu v trestním řízení ve smyslu ustanovení zákona 141/1961Sb., trestní řád. Pracovní prostředí pro bezpečné zajištění důkazu by ve vztahu k samotnému důkaznímu materiálu mělo být inertní tzn. neumožnit jiné nakládání s důkazem, než jeho zajištění, odborné prozkoumání, vyhodnocení a zpracování odborné zprávy. Elektronickým důkazem se pro účely zpracování rozumí záznam komunikace (PCAP) / systémová hlášení, škodlivý kód, případně nástroje sloužící k obcházení bezpečnostních prvků, případně zneužití zranitelnosti. Toto pracovní prostředí by zároveň nemělo umožnit šíření malware a mělo umožnit evidenci přístupů a způsobu nakládání s elektronickým důkazem. Zanalyzujte možnosti a popište požadavky na vytvoření tohoto prostředí. Prostředí navrhněte a vytvořte. Simulujte bezpečnostní incident a využijte vytvořené prostředí pro sběr důkazů k simulovanému incidentu. Průběh a závěry simulace popište a prezentujte.

DOPORUČENÁ LITERATURA:

[1] PEARCE, Lauren. Malware analysis in a nutshell. Los Alamos National Lab.(LANL), Los Alamos, NM (United States), 2016.

[2] GUARNIERI, Claudio, et al. The Cuckoo Sandbox (2012). URL https://www. cuckoosandbox. org, 2012.

Termín zadání: 1.2.2019 ***Termín odevzdání:*** 27.5.2019

Vedoucí práce: Ing. Zdeněk Martinásek, Ph.D.
Konzultant: Ing. Jaroslav Rus (ANECT a.s.)

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Tato práce pojednává o tématu elektronických důkazů. V rámci práce jsou popsány právní postupy zajišťování a analýzy elektronických důkazů. Dále je navrženo a popsáno virtuální prostředí a nástroje vhodné k bezpečnému zajištění elektronických důkazů. Pomocí vybraných nástrojů je zajištěn vzorek malwaru, který je analyzován a popsán. Tento vzorek je následně použit k simulování bezpečnostního incidentu. Navržené prostředí je použito k sběru důkazů v rámci simulovaného bezpečnostního incidentu.

KLÍČOVÁ SLOVA

android, elektronický důkaz, forenzní analýza, malware, RAT, trojan, virtuální prostředí, zajištění důkazního materiálu

ABSTRACT

The bachelor thesis deals with evidence securing in virtual environment. The main goal is to suggest suitable virtual environment for evidence securing which can be used in prosecution. As the next the tools that are suitable for safe securing of evidence are described. With the help of selected tools the sample of malware is secured and then the sample is analyzed and described. The suggested environment is used to evidence gathering within the frame of simulated security incident.

KEYWORDS

android, electronic evidence, forensic analysis, malware, RAT, trojan, virtual environment, evidence securing

HAVLOVÁ, Miluše. *Virtuální prostředí pro zajištění důkazního materiálu*. Brno, 2019, 56 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Zdeněk Martinásek, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Virtuální prostředí pro zajištění důkazního materiálu“ jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autorky

PODĚKOVÁNÍ

Na tomto místě bych ráda poděkovala vedoucímu mé bakalářské práce panu Ing. Zdeňkovi Martináskovi, Ph.D. za odborné vedení práce, konzultace, trpělivost a věcné připomínky k práci. Dále chci poděkovat panu Ing. Jaroslavovi Rusovi za odborný dohled, konzultace a ochotu, kterou mi při zpracování bakalářské práce věnoval.

Brno ....

podpis autorky

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Informační bezpečnost se stává čím dál tím více důležitější v souvislosti s technologickým vývojem. Tak jako jsou vyvíjena lepší a sofistikovanější řešení zabezpečení operačních systémů, přístupů a dat vůbec, jsou zároveň vytvářeny i nové mechanismy k obcházení těchto bezpečnostních ochran. Současně s vývojem se do internetové prostředí přesouvá i kriminalita a přibývá trestních řízení, kdy je nutné dokazovat něco, co se stalo v kybernetickém prostoru.

K tomu, aby bylo možné dokázat trestný čin, který se stal prostřednictvím počítače nebo jiných chytrých zařízeních, je nutné z dotčených systémů získat důkazní materiál. Odborníci, kteří provádějí analýzu, využívají speciálních forenzních nástrojů k analyzování dat a sbírání digitálních stop. Aby elektronický důkaz měl u soudu co největší důkazní hodnotu, nebo aby byl vůbec uznán, musejí činit velmi obezřetně a dodržovat správné postupy. Důležité je analýzu neprovádět s originálním důkazním materiálem, ale až s jeho bitovou kopií. Tím se zajistí, že originální materiál nebude změněn a výsledek analýzy bude reprodukovatelný. Rovněž je důležité po analýze zpracovat dokumentaci, která je následně použita jako listinný důkaz před soudem.

Cílem bakalářské práce je seznámit se s právními i technickými postupy zajištění a analýzy elektronického důkazního materiálu. Seznámit se s možnostmi návrhu prostředí vhodného k analýze důkazního materiálu a toto prostředí vytvořit. V praktické části simulovat bezpečnostní incident a provést sběr důkazů v navrženém prostředí. Nakonec o zajištěném důkazu sepsat zprávu.

1 Elektronický důkazní materiál

Stále rychlejší rozvoj moderních technologií se neodráží pouze v technickém odvětví, ale čím dál tím víc prostupuje i do dalších oborů jakým je například právo. Za poslední léta došlo k rozsáhlým posunům v soudních řízeních, především, co se týče způsobů dokazování a možných důkazů. V právnické praxi se mnohem častěji vyskytují elektronické důkazy a právníci tak musí řešit věrohodnost elektronických dokumentů, která je často sporná [1].

1.1 Vývoj informatiky v kriminalistice

1.1.1 Historický vývoj informatiky

Největší a dynamický rozvoj je v informatice zaznamenán na přelomu 20. století. Pro úspěšnou kriminalistickou práci je stěžejní analýza informačních potřeb, klasický i operativní sběr informací, jejich shromažďování, archivace a poté efektivní využití, kterým se dosáhne vypátrání obecné pravdy, zjištění motivů trestných činů, způsobů jejich provedení, zanechaných stop a důsledků směřující k odhalení a usvědčení pachatele. Pro tuto činnost je využití informatiky nevyhnutelné, a to nejen obecné informatiky, ale také informatiky velmi specifické – kriminalistické.

Ještě v 70. letech 20. století byly informační technologie veřejnosti zcela nepřístupné, jelikož byly nejen složité, ale také velmi nákladné. Proto byly vyvíjeny a využívány především pro bezpečností složky. Tato informatika, která se využívala pro kriminalistickou práci se nazývala informatikou kriminalistickou.

Masového rozšíření informační technologie i pro běžné obyvatelstvo bylo dosaženo v 80. a 90. letech 20. století. Sálové počítače byly nahrazeny kompaktnějšími technologiemi. Svět počítačových technologií prostoupil až na globální trh a vyvíjený software byl použitelný ve všech odvětvích, včetně kriminalistiky. Dnes se již vyvíjí menší množství specializovaných technologií, které by byly přímo určené jen pro policejní složky, avšak ty, které se dnes vyvíjí, jsou mnohem specializovanější a robustnější.

V 21. století je informatika již na vysoké úrovni výpočetní síly. Informace jsou díky rozsáhlým počítačovým sítím (interním i externím) a dalším technologiím jako jsou GSM/GPS dostupné v podstatě odkudkoliv [2].

1.1.2 Hrozby současnosti

S rapidním rozvojem technologií a jejich zabezpečovacích mechanizmů se objevují stále nové formy kriminality, a to především té počítačové. Informační kriminalita

je v současnosti jednou z nejvýnosnějších odvětví organizovaného zločinu. Mezi nejvýnosnější strategie dnes patří investice do exploit kitu a následné vydírání oběti pomocí ransomware. Podle studie společnosti Trustwave dosahuje návratnost investic do malware útoků až 1425 % [3].

Ransomware je druh počítačového softwaru, pomocí kterého útočníci blokují počítačové prostředky oběti a za odblokování požadují výkupné. Přitom ani není jisté, zda při zaplacení požadované částky útočník opravdu poskytne přístup k systému a odepíraným souborům. Počítačových softwarů typu ransomware jsou dnes stovky, ale všechny mají podobný koncept. Nenápadně se dostat do počítače nic netušícího uživatele, zablokovat uživateli možnost provádět v počítači jakoukoliv činnost a následně jej vydírat zaplacením výkupného. Často se při nasazování ransomware využívá sociálního inženýrství. To vypadá tak, že útočník si vytipuje, na jakou skupinu uživatelů se zaměřit. Většinou se jedná o stránky s nevhodným obsahem nebo stránky jejichž tématika je trestná. Oběť pak ze strachu z trestu raději zaplatí výkupné, než aby se obrátila na policii.

Pro názornější příklad uvedu popis ransomwaru zvaný Locky. Tento program se šíří prostřednictvím nakažených souborů s příponou .doc, které jsou jako příloha v emailu. Tyto soubory obsahují makro, které je spuštěno, pokud má uživatel makra povolena ve Wordu. Pomocí makra je stažen .exe soubor a dojde k zašifrování souborů. Název souborů je změněn na 16 místnou alfanumerickou kombinaci s příponou .locky. V tuto chvíli již nepomůže ani reboot počítače, jelikož ransomware je spuštěn hned po spuštění systému. Po startu je zobrazena hláška s informacemi, že k šifrování souborů jsou využity algoritmy RSA-2048 a AES-1024 a k získání privátního klíče a programu, který je potřebný k dešifrování je nutné útočníkovi zaplatit částku 5 BitCoinů. Dále je uveden návod, jak a kam uvedenou částku zaplatit, přičemž je uživatel nucen k potřebným akcím využít prohlížeč Tor. Podobných ransomwarů se na internetu vyskytuje velmi mnoho např. CryptoWall, TeslaCrypt nebo DMA-Locker [4].

Znepokojivým trendem dnešní doby je, že ransomware je poskytovaný jako služba. Tato skutečnost způsobuje, že i začínající hacker může uskutečnit spoustu útoků, když si koupí za poměrně nízkou částku balík nástrojů k webovým útokům. Někdy je to dokonce tak snadné, že k vytvoření ransomware stačí vyplnit formulář.

Ransomware bohužel není jediná služba na trhu kyberkriminality. Další moderní záležitostí provádění útoků je DDoS (Distributed Denial of Services). Cílem útoku není získat data nebo vymáhat peníze, ale omezit dostupnost služeb. Na cílový server jsou generovány desetitisíce paketů za sekundu a tím je vyčerpána jeho výpočetní kapacita a dosaženo toho, že nemůže obsluhovat ostatní žádosti odesílané na server. Na rozdíl od DoS (Denial of Services) pakety pocházejí z různých zdrojů, a tak je identifikace útočníka podstatně náročnější [5]. Největším problémem je, že poža-

davky kladené na server, i když je jich mnoho, nejsou v podstatě nelegální a je těžké rozhodnout, kdy se jedná o trestný čin dle ustanovení § 230 TZ a kdy ne.

I přes zavedení čipových karet je stále oblíbený a výdělečný Carding. Ten spočívá v tom, že pachatel prostřednictvím speciálního vybavení (např. pomocí použití skimmerů na bankomatech) získá údaje z karet a k nim i potřebné PINy. Vytvoří balíček těchto údajů a ty posléze nabízí na specializovaných e-shopech. Např. e-shop s informacemi o platebních kartách obsahuje v doméně termín „DUMPS“, čímž kriminálníci označují databázi odcizených platebních údajů. Na různých internetových fórech jsou i další informace k zneužití, např. kopie dokladů, informace o zaměstnání, platebních účtech a další. Ty jsou dále využívány k podvodům či vydírání. Právě různé zneužitelné osobní informace jsou získávány infikováním počítače oběti trojským koněm. Ten potom nasbírané informace odesílá útočníkovi. Dnes existuje již řada trojských koní, kteří dovedou přeposílat takřka cokoliv (aktivitu uživatele, úhozy klávesnice, vytvářet screenshoty). Jeden ze stále oblíbených je trojský kůň Trickbot, který při přístupu na internetové bankovnictví přidá do webové stránky kód (předloží podvrhnutou stránku) a díky tomu jsou potom přihlašovací údaje odcizeny [6].

Dále jsou používány také minery. Některé weby mohou obsahovat skript – JS miner [7], který při návštěvě webových stránek vytěžuje prostředky počítače, např. CoinHive/SMMCH. Nebo klasické minery, které pracují přímo v infikovaném počítači a snižují jeho výkon, např. XMRig.

1.2 Důkaz, důkazní prostředek a pramen důkazu

Trestní řád v ustanovení § 89 odst. 2 TŘ předkládá demonstrativní výčet důkazních prostředků sloužících k dokazování skutečností v trestním řízení. Jelikož ale pojmy jako je *důkaz, důkazní prostředek a pramen důkazu* nejsou v trestním řádu dostatečně rozlišeny, dochází často k jejich záměně [8]. Nejlépe podle mého tyto pojmy vystihují následující citace.

„Důkazem se rozumí výsledek činnosti orgánu činného v trestním řízení při dokazování (např. obsah výpovědi vyslýchané osoby, obsah listiny, výsledek znaleckého zkoumání – obsah znaleckého posudku a odpověď znalce na položené otázky, výsledek získaný ohledáním atd.)” [8]. Jedná se tedy o informace, které je možné použít přímo při dokazování v trestním řízení. Zároveň jsou to data, která byla podrobena analýze či byla nějakým způsobem interpretována, aby měla smysl pro dokazování v trestním řízení. Elektronickým důkazem jsou informace o důkazní hodnotě uložené nebo přenášené v digitální podobě.

„Důkazním prostředkem je procesní činnost orgánu činného v trestním řízení nebo oprávněné strany trestního řízení, která slouží k poznání skutečnosti, jež má být zjiš-

těna“ [8]. Elektronický důkazní prostředek je tedy zdrojem této informace. Prakticky to může být cokoliv, co má náležitý význam k objasnění věci v trestním řízení a je uchováno v elektronické podobě. Jsou to především data, která nebyla ještě analyzována ani interpretována (data je potřeba pomocí nějakého dalšího elektronického zařízení převést do podoby, ve které jsou pro člověka čitelná).

„Pramenem důkazů jsou nositelé informace, z níž se čerpá poznatek, který je předmětem dokazování. Prameny důkazů jsou buď osoby, nebo věci a podle tohoto hlediska lze důkazní prostředky rozdělit na osobní (výslech obviněného, svědků, znalců, ohledání osoby) a věcné (ohledávané věci, listiny, místo činu)“ [8]. Pramenem elektronických důkazů se rozumí např. datové úložiště, které obsahuje důkazní prostředek.

1.3 Digitální stopy

Pojem počítačová stopa se v kriminalistice začal objevovat již na počátcích 80. let, kdy se využívaly ještě sálové počítače. Postupný vývoj technologií měl za následek miniaturizaci zařízení do tzv. smart, jako jsou smartphony, tablety, notebooky, čtečky apod. Miniaturní procesory a paměti prostupují nejen v počítačovém odvětví, ale i v automobilovém, v lékařství, sportovních pomůckách a dalších. A tak se pojem počítačová stopa postupně nahradil pojmem digitální stopa, který je v dnešní technologicky vyspělé době univerzálnější.

Na počítačové stopy působí určité faktory, jimiž jsou objekt, způsob, jakým je na počítačové stopy působeno a odrážené vlastnosti objektu. Jedním z prvotních objektů je člověk, který modifikuje techniku nebo provádí změny v datech, a to přímo nebo nepřímo. Zároveň mohou být prováděny změny ze strany systémových či programových dat, a to buď v závislosti na člověku nebo nezávisle na člověku. Technika samotná může být také objektem, avšak rozdíl je v tom, že nemůže provádět změny sama na sobě.

Člověk obsluhující vstupně-výstupní zařízení svou aktivitou působí na data nebo techniku a tím mění data v operačním systému. To má za následek změnu informací, která jsou uložena na datovém nosiči. Obstojně technicky zdatný uživatel provede většinou to, co přesně chce, a to se projeví i v operačním systému. Méně zdatný uživatel často provede sice to, co chce, avšak zároveň provede v systému i další akce, o kterých třeba ani neví.

Programová data a technika jsou na tom obdobně. Např. programy v podobě virů mají dynamický kód, který se podle potřeby mění. Takové viry mohou třeba měnit nebo mazat informace uložené na médiu, a veškerá jejich činnost probíhá na pozadí. Technika může měnit své funkční vlastnosti, které jsou ovlivněny např. teplotou nebo mechanickým poškozením. Z toho vyplývá, že: *Počítačová stopa je stopou, která obsahuje vnitřní, funkční, dynamickou a jinou (významovou) informaci odráženého*

objektu. Objekty, které zanechávají v počítačových stopách uvedené vlastnosti jsou člověk, data a technika.

Počítačové stopy je nutné pro přehlednost zařadit, a tak jsou děleny na technické a datové.

Technické stopy jsou veškerá elektronická zařízení, která jsou součásti počítače, sítě a k nim připojených periférií. Jsou to např. procesor, sběrnice, klávesnice, monitor, modemy, pevné disky, atd.

Datové stopy jsou především informace, které jsou uložené na datových nosičích. Tato data je možné dále rozdělit podle toho, kdo je vytvořil nebo změnil.

Dělení datových stop:

- stopy vytvořené člověkem,
- stopy vytvořené systémovými daty,
- stopy vytvořené programovými daty,
- stopy vytvořené jiným způsobem.

Počítač již dnes není jediné zařízení, které pracuje s digitálními daty, a tak zařízeních, která dokážou přenášet digitální data a zanechávat o své aktivitě informace, je celá řada. V závěru podkapitoly jsou tedy digitální stopy veškeré informace, které jsou uloženy a přenášeny v digitální podobě a mají nějakou významovou hodnotu [2].

1.4 Zajištění elektronických dat

Při zajišťování elektronických důkazů je důležité dbát na zákonem dané postupy a podrobnou dokumentaci, aby důkaz mohl být použit k dokazování v trestním řízení. V opačném případě se totiž může stát, a v praxi se také často stává, že pokud nebyl správně dodržen postup zajištění elektronického důkazu, důkaz se stává nepoužitelným pro dokazování a nemá tedy žádnou důkazní hodnotu.

Trestní řád bohužel přes všechny své novelizace neobsahuje správný postup pro nakládání s elektronickými důkazy, a to potom často vede k tomu, že je v praxi nutné za určitých okolností realizovat „vlastní“ postup, který se ve finále může ukázat jako neplatný a tím se důkaz stane nevyužitelným. Jeden z jasně daných limitů je uveden v § 89 odst. 3 TŘ. Podle něj je platný pouze takový důkaz, který byl získán zákonnou cestou.

Počítačová data, která mohou být použita při dokazování před soudem, lze získat následujícími způsoby:

- zajištěním zařízení nebo datových nosičů, které počítačová data uchovávají (počítače, mobilní telefony, datové nosiče atd.),

- získáním přímého přístupu k počítačovým datům, jež jsou uchována v počítačových systémech (volně dostupným, pomocí poskytnutých přístupů, pomocí přihlášeného zařízení atd.),
- získáním počítačových dat od poskytovatelů služeb (uživatelská data nebo provozní a lokalizační údaje uchovaná u poskytovatele) [8].

Z procesního hlediska není složité zajistit věci, jako je počítačový systém či nosič dat, jelikož se na ně vztahuje § 78 TŘ, podle nějž ten, kdo má u sebe věc, která může v trestním řízení sloužit jako důkaz, je povinen ji v přípravném řízení vydat na vyzvání státního zástupce nebo policejního orgánu. Policie může vyžadovat informace od poskytovatele informačního systému dle §66 odst. 4 zákona 273/2008Sb. a zajišťovat věcné důkazy dle §34 téhož zákona v přípravném řízení, kdy ještě nejsou formálně zahájeny úkony trestního řízení dle trestního řádu. Údaje o uskutečněném telekomunikačním provozu a odposlechy (od operátora) lze vyžadovat pouze dle §88 a §88a trestního řádu.

V rámci této práce se jedná především o data, která jsou uchována na datových nosičích (soubory typu PCAP, systémová hlášení či škodlivý kód). Takovéto důkazní prostředky je třeba při zajišťování důsledně zaprotokolovat a zapečetit do antistatického vaku. Dále by měly být uchovány takovým způsobem, aby data, která nesou, nemohla být nikým pozměněna do doby, než k nim bude mít přístup znalec.

1.5 Analýza dat

Po správném zajištění dat nastává čas k jejich analýze. V době před analýzou nemají data jako taková ještě téměř žádnou vypovídající hodnotu. Protože jsou zatím pouhou binární posloupností, je nutné je nějakým způsobem interpretovat. Až poté je možné z nich získat užitečné informace, které mohou být použity jako důkaz. K takovéto analýze se využívají více či méně technicky náročné nástroje.

Získat důkazy z elektronických důkazních prostředků lze vícero způsoby. Zatímco někdy není k získání důkazu zapotřebí znalce, jindy je to nezbytné. V takových případech, kdy se jedná o věci technicky náročnější, je zapotřebí postupovat opatrně a dbát na správné zajištění elektronického důkazního materiálu. Pokud by byl zajištěn chybně, mohlo by dokonce dojít k jeho znehodnocení. Proto je nutné před samotnou analýzou vytvářet takzvané bitové kopie (např. kopie disku bit po bitu, která je totožná s originálem) a pracovat až s touto kopií. O tom, zda je k případu potřeba využít odborných vědomostí znalce, rozhoduje podle ustanovení § 105 odst. 1 TŘ orgán činný v trestním řízení. Pokud se jedná o jednodušší případy, je možné vyžádat pouze vyjádření znalce.

1.5.1 Analýza dat pomocí vstupních a výstupních periférií

Zatímco tato práce se zaměřuje na analýzu pomocí speciálních nástrojů, je dobré zmínit, že tento postup není vždy nutný. Běžným způsobem, jak získat data z elektronického zařízení, je základní ohledání elektronického zařízení a dat v něm obsažených pomocí vstupních a výstupních periférií (klávesnice, myš, monitor atd.). Jedná se o běžnou práci s počítačem a průzkum uložených dat. I tento postup je nutné zpracovat do protokolu. Ačkoliv je tento postup rychlejší a technicky nenáročný, má jistou nevýhodu a tou je slabá důkazní síla. Ta může být vzhledem k povaze počítačových systémů zpochybněna. Další nevýhoda je, že takto obyčejným průzkumem není možné odhalit všechna data. Mohou být totiž skryta a poté je k získání takovýchto dat zapotřebí sofistikovanějších nástrojů.

1.5.2 Forenzní analýza

Při používání technologických zařízení jako jsou počítač, chytrý telefon a další zařízení, zůstávají v systému digitální stopy. Tyto informace souvisí s provozem systému, zápisem a čtením dat a různými akcemi, které uživatel během svého užívání vyvolá. Nejedná se však o informace, z kterých by bylo jednoznačně možné určit původce těchto informací. Proto je potřeba pomocí speciálních forenzních nástrojů digitální stopy uložené na paměťovém nosiči extrahovat do čitelného formátu.

Základem každé analýzy, pokud je to možné, je před samotnou analýzou opatřit bitovou kopii zkoumaných dat. Pokud by se tak nestalo a pracovalo se s originálním datovým nosičem či daty, mohlo by dojít k nechtěné modifikaci obsahu, což by zapříčinilo znehodnocení důkazu, a to je nežádoucí. K vytvoření bitové kopie je zapotřebí forenzních nástrojů. Kromě samotného vytvoření bitové kopie je nutné pomocí kontrolního součtu ověřit, jestli zkopírovaná data skutečně odpovídají originálu.

Analýzu může provést i vyšetřovatel, ale pro zvýšení důkazní síly je doporučeno, aby analýzu provedl znalec. Ten zpracuje znalecký posudek, který je dále u soudu užíván jako listinný důkaz.

Aby mohly být výsledky analýzy použity jako důkaz u soudu, musí splňovat následující podmínky:

- *legalita*, všechny důkazní materiály musí být získány legálními prostředky,
- *integrita*, veškeré úkony musí být prováděny tak, aby nedošlo ke změně dat,
- *opakovatelnost/přezkoumatelnost*, používání takových metod, kterými se při opětovné analýze dospěje ke stejným výsledkům,
- *nepodjatost*, osoba provádějící analýzu musí být nestranná a nezaujatá k posuzované věci.

1.6 Hodnocení elektronických důkazů

Součástí soudního řízení je předložení důkazů a jejich provedení. Dokazování pomocí elektronických důkazů je ale problematičtější. Jelikož v současné době není reálné, aby byl důkaz před soudem předveden kupříkladu zdrojovým kódem, je nutné vyžádat vyjádření odborníka. Odborné vyjádření může poskytnout kdokoliv, kdo disponuje odbornými znalostmi. Často se využívá uznávaných lidí z praxe nebo znalců. Znalec po důkladné analýze zpracuje podrobnou dokumentaci a ta je poté jako listinný důkaz použita před soudem. Jsou ale situace, kdy je obtížné elektronický důkaz zaznamenat do podoby listinného dokumentu a vhodnější by bylo použít důkazy přímo (třeba pomocí simulace). Vzhledem k tomu, že technická úroveň soudů není v současné době příliš dobrá, nemůže být důkaz takto předveden. V budoucnu lze ale s přibývající technikou očekávat větší tlak na tyto možnosti dokazování.

2 Analytické prostředky

S důkazním materiálem je potřebné nakládat obezřetně. Jak z hlediska toho, aby byly dodrženy správné postupy, tak i v tom smyslu, že může být nebezpečný pro testovací stanici. Proto se využívá prostředí izolované od operačního systému (sandbox), který je instalovaný přímo na hardware. Důvodem, proč využívat specializované forenzní nástroje je ten, že máme k dispozici kromě analýzy dat jako takových i logy přístupů a zacházení s daty. K tomu může být použit software a hardware popsaný v následujících podkapitolách.

2.1 Software

2.1.1 Pracovní prostředí GNU/Linux

V dnešní době existuje celá řada operačních systémů speciálně upravených pro forenzní analýzu. Některé jsou komerční, ale spousta z nich je volně dostupná na internetu. Jedná se především o operační systémy založené na unixovém jádře. Tyto systémy obsahují předinstalované speciální nástroje pro forenzní analýzu. Jedna z nesporných výhod využívání linuxových systémů je ta, že se dá systém docela snadno upravovat podle potřeby uživatele. Kromě toho má linuxový systém řadu dalších praktických výhod a to, že je méně automatizovaný než např. MS Windows, a tak lze očekávat, že nám na pozadí nepoběží nějaké neočekávané nebo nepochopitelné procesy. Dále Linux podporuje spousty souborových systémů, což umožňuje analyzovat více druhů systémů. Užitečnou výhodou pro vyšetřování a analýzu je, že v Linuxu je všechno bráno jako soubor, což usnadňuje monitorování a umožňuje lépe zkoumat logování aktivních operací. Linux také obsahuje zařízení zvaná *loopback*. Jedná se o soubor, se kterým lze pracovat jako s diskem a který lze připojit a provést následnou analýzu. Konkrétně se v Linuxu jedná o soubory /dev/loopX, kde X zastává číslo připojeného souboru (např. /dev/loop0).

2.1.2 Sandbox

Elektronický důkazní materiál může být v podobě různých formátů. Může se jednat o obrazové formáty, audio soubory, textové soubory, ale také o zachycenou komunikaci či škodlivý kód. Právě při analyzování škodlivého kódu je potřeba chránit fyzická zařízení. K tomu slouží takzvaný *sandbox*. Sandbox je prostředí, které umožňuje omezit přístup ke zdrojům hostitelského počítače a mít tak kontrolu nad procesy běžícími uvnitř. Sandbox je užíván zejména k testování nového softwaru nebo ke spouštění nedůvěryhodného kódu.

Při analýze elektronických důkazních materiálů dochází často k situacím, kdy je potřeba spouštět neznámé kódy a sledovat jejich chování v systémů. Tyto programy pak mohou napáchat v systému nenapravitelné škody. Pokud je takový program spuštěn v sandboxu, nemůže zapisovat mimo odkládací prostor na disku, který je mu vyhrazen.

2.1.3 Virtualbox

Virtualbox je multiplatformní virtualizační nástroj, který je od roku 2009 vyvíjen firmou Oracle. Distribuován je pro operační systémy Windows, Linuxové systémy i Mac OS.

Mezi jeho základní funkce patří vytváření tzv. snímků (snapshots). Pomocí této funkce je možné ukládat přesné obrazy virtuálního stroje včetně operačního systému, konfigurace, spuštěných aplikací atd. Tato funkce je dobře využitelná především při testování neověřeného softwaru, kdy může dojít k situaci, že selže celý systém a bude nenávratně poškozen. V takové situaci stačí jen nahrát předem uložený obraz a systém je během několika vteřin uveden do původního stavu.

Další užitečná funkce je podpora přenosu obsahu schránky. Umožňuje tak kopírovat odkazy či soubory z hostitelského systému a vkládat je do virtuálního systému a naopak. Kopírování probíhá stejným způsobem, jako by se pracovalo v jednom a tom samém systému. Následně je možné nastavit přenos obsahu schránky z hostitelského do virtuálního, z virtuálního do hostitelského anebo obousměrně.

V rámci sdílení je možné nastavit i sdílenou složku, aniž by bylo nutné nastavovat síťové prostředí. ‘ Dále nástroj disponuje podporou hardwarové virtualizace (Intel VT a AMD-V) a paravirtualizace [10].

2.1.4 CAINE

CAINE je GNU/Linux live distribuce, jehož nejnovější verze je založená na systému Ubuntu 18.04. Systém je upravený pro potřeby počítačové forenzní analýzy a zároveň již obsahuje nástroje a balíčky k těmto úkonům. Zachovává myšlenku open source softwaru a jeho použití je tedy zcela zdarma. Systém obsahuje velké množství forenzních nástrojů a je možné jej dále rozšiřovat. CAINE poskytuje vhodnou softwarovou podporu během všech fází vyšetřování a také poloautomatické reportování závěrečné zprávy. Výhodou je i intuitivní uživatelské prostředí [11].

2.1.5 Tails

Jedná se o Debian GNU/Linux live distribuci založenou na systému Debian. Její nejnovější verze je Tails 3.13.2. Využívá se zejména pro anonymizaci na Internetu

a zajištění soukromí. Veškeré spojení do Internetu je směrováno přes síť Tor. Zároveň nezanechává v použitém počítači elektronické stopy, pokud to není vynuceno. Tails je nakonfigurován tak, že neukládá žádná data na pevný disk a jeho jediným úložištěm je tedy RAM. To má za následek, že po vypnutí počítače jsou všechna data smazána. Data, která jsou potřebná pro další využití je samozřejmě možné uložit na externí úložiště mimo systém a tím nedojde k jejich ztrátě. Systém Tails také obsahuje šifrovací nástroje k ochraně dat [12].

2.2 Hardware

Kromě softwarového vybavení je potřeba mít i příslušný hardware. Za běžných podmínek stačí k analýze i standardní počítačové vybavení. Existují však i specializované zařízení od mobilních zařízení po laboratorní stanice. Tato zařízení disponují vysokou škálou různých portů a dokáží přečíst všechna dostupná média.

2.3 Nástroje pro forenzní analýzu

2.3.1 Autopsy

Autopsy je volně dostupný nástroj pro forenzní analýzu. Je možné ho získat z oficiálních stránek Sleuthkit (https://www.sleuthkit.org/autopsy/). Nástroj je v prostředí CAINE již předinstalovaný.

Případy (Cases)

Ještě před tím, než je možné začít s analýzou, je potřeba vytvořit případ. Případ může obsahovat jeden nebo více datových zdrojů. Datové zdroje mohou být z více disků nebo dokonce i z více počítačů. Každý případ je uložen ve vlastním adresáři, který je obvykle pojmenován stejně jako případ. V adresáři jsou obsaženy konfigurační soubory s koncovkou .aut.

Datové zdroje (Data sources)

Datové zdroje jsou data, která se budou analyzovat. Mohou to být obrazy disků, logické soubory, lokální disk apod. Aby bylo možné s datovými zdroji pracovat, je nutné mít otevřený předem vytvořený případ a do něj poté tyto datové zdroje přidat. Autopsy podporuje celkem čtyři typy datových zdrojů:

1. Obraz disku, soubor či soubory, které jsou bitovou kopií fyzického disku nebo paměťové karty nebo obraz disku virtuálního počítače. Autopsy podporuje následující formáty:

- raw single (např. *.img, *.dd, *.raw, *.bin),
- raw split (např. *.001, *.002, *. aa, *. ab),
- enCase (např. *. e01, *. e02),
- virtuální stroje (např. *. vmdk, *.vhd).

2. Lokální disk, lokální úložiště a připojené nosiče dat jako je interní a externí HDD nebo USB flash disk.
3. Logické soubory, lokální soubory a složky.
4. Nepřiřazené místo na disku, jakýkoliv typ souboru, který neobsahuje souborový systém.

Techniky vyhledávání důkazů

Výpis souborů: Provádí analýzu souborů a složek včetně názvů již smazaných souborů

Obsah souborů: Obsah souborů je možné prohlížet ve formátu raw, hex nebo extrahovat řetězce ASCII.

Hash databáze: Rychlá identifikace dobrých a špatných souborů pomocí vyhledávání v hash databázi. Autopsy využívá NIST National Software Reference Library (NSRL), popřípadě i databáze dobrých a špatných souborů vytvořené uživatelem.

Třídění typů souborů: Třídí soubory podle jejich vnitřních známých atributů.

Činnost souborů v čase: Časová osa aktivity souboru usnadňuje určit části v systému, které mohou obsahovat elektronické stopy. Pomocí Autopsy je možné vytvořit časovou osu nad datovými zdroji a zaznamenávat jejich úpravy, přístupy a změny, a to jak pro alokované soubory, tak pro nealokované soubory.

Hledání klíčových slov: V souborovém systému lze vyhledávat pomocí ASCII textových řetězců. Vyhledávat lze v celém souborovém systému disku nebo pouze v nealokovaném prostoru. Pro rychlejší vyhledávání je možné nastavit indexaci. Pokud jsou některé výrazy často hledány, je možné nastavit, aby je Autopsy vyhledával automaticky.

Analýza meta dat: Meta data obsahují podrobnosti souborů a složek a Autopsy umožňuje zobrazit podrobnosti jakékoli struktury meta dat v souborovém systému. To je užitečné pro obnovení smazaného obsahu.

Analýza datových jednotek: Na datových jednotkách je uložen obsah souborů a pomocí Autopsy je možné zobrazit obsah jakékoliv datové jednotky v několika formátech včetně ASCII, hexdump a textových řetězců.

Detaily disku: Mohou být zobrazeny informace o souborovém systému, jako je rozložení disku nebo časy aktivity na disku. Takovéto informace jsou užitečné především k obnovování dat na disku [13].

Moduly (Ingest Modules)

Ingest moduly analyzují data datových zdrojů. Veškerá analýza souborů a jejich obsahů je prováděna těmito moduly v reálném čase. Jsou to například vyhledávání a výpočty hashů, vyhledávání klíčových slov a extrakce webových artefaktů. Ingest moduly se konfigurují poté, co jsou přidány do případu datové zdroje. Jakmile se provede konfigurace, moduly jsou spuštěny na pozadí a jsou připraveny podávat výsledky v reálném čase, pokud najdou důležité informace. Při konfiguraci je možné vybrat, který z ingest modulů bude zapnutý, a která data budou analyzována.

2.3.2 Ghidra

Ghidra je program pro softwarové reverzní inženýrství (SRE). Jejím tvůrcem je americká tajná služba NSA, která ho veřejnosti poskytla v březnu 2019 pod licencí open source Apache 2. Ghidra obsahuje širokou škálu možností při analýze zkompilovaného kódu, které je dále možné rozšiřovat i o své vlastní nástroje. Umožňuje například jeho dekompilaci, grafické zobrazení funkcí, přehled proměnných, předpřipravené skripty a zpětnou kompilaci. Díky tomu, že je Ghidra psána v programovacím jazyku Java, je možné ji spustit jak na systémech Windows a Linux, tak i MacOS [14]. Ghidra podporuje následující formáty:

- Common Object File Format (CoFF),
- Debug Symbols (DBG),
- Executable and Linking Format (ELF),
- Ghidra Data Type Archive Format,
- GZF Input Format,
- Intel Hex,
- Mac OS X Match-O,
- Module Definition (DEF),
- Motorola Hex,
- New Executable (NE),
- Old-style DOS Executable (MZ),
- Portable Executable (PE),
- Preferred Executable Format (PEF),
- Program Mapfile (MAP),
- Raw Binary,
- XML Input Format.

Nástroje

K podrobnější analýze programů lze využít různé nástroje, díky kterým je možné získat komplexnější znalost analyzovaného programu. Nástroje je možné importovat, upravovat nebo vytvářet vlastní, které je poté možné exportovat a poskytnout k užívání dalším analytikům.

Ghidra obsahuje ve výchozím nastavení dva již integrované nástroje. Jsou to CodeBrowser a Version Tracking.

Pomocí **CodeBrowseru** je možné zanalyzovat strukturu programu. Nejdříve je nutné importovat program nebo jeho části (například třídu). Následně je nutné vybrat, jaké funkce analyzátoru se mají aplikovat při prvotní automatické analýze. Tímto jsou zjištěny základní informace o samotném analyzovaném programu, např. kde se nachází spustitelný soubor, velikost adresování, použitý procesor, verze Javy (u programů psaných v jazyce Java), atd. Jakmile je analýza dokončena, je možné procházet mapování v paměti a zobrazit si dekompilované funkce. Funkce jsou čitelné v jazyce C a je možné je zobrazit i graficky. Zároveň je možné analyzovat dvě verze programů najednou a hledat mezi nimi spojitosti nebo rozdíly.

K tomu už ale lépe slouží nástroj **Version Tracking**. Tento nástroj porovná dvě verze programů a zobrazí jejich shody. Nejprve je nutné vytvořit novou relaci. Jako vstup je nutné přidat soubory, které chceme porovnat. Při porovnání dvou verzí programu se jako zdrojový soubor zvolí starší verze programu a jako cílový soubor novější verze programu. Ještě před samotným porovnáváním verzí je dobré (lze přeskočit) spustit test předpokladů. Tento test vyhodnotí, zda budou analytické funkce mezi těmito dvěma zdroji fungovat úspěšně, popřípadě oznámí, kde je problém, který je nutné před analýzou odstranit, aby byl výsledek co nejlepší. Následně už je možné programy dekompilovat a spouštět korelační algoritmy, které vyhledávají podobnosti, resp. rozdíly mezi verzemi programu. Tato funkce je velmi užitečná právě při analýze malwaru. Pokud se k analytikovi dostane originální verze malwaru a poté třeba její upravená verze, lze pomocí nástroje Version Tracking odhalit změny, které byly provedeny.

2.3.3 QuickHash

QuickHash je další z řady open source nástrojů a je již součástí operačního systému Caine. Nástroj byl původně vyvinut pro Linux, ale dnes je již dostupný i pro Windows a MacOS. QuickHash nabízí rozšířené možnosti práce s otisky souborů, řadu formátů a hashovacích funkcí. Otisk je možné vytvořit např. pro řádek textu, soubor či složku. Dále je možné přímo porovnat dva soubory nebo dvě složky. K dispozici jsou ještě další funkce, např. kopírování, při kterém je před provedením kopie spočítán hash, poté je provedeno kopírování a následně je hash proveden znovu. Ve všech

funkcích je možné použít algoritmy MD5, SHA-1, SHA256, SHA512 a xxHash.

2.3.4 Wireshark

Wireshark je open source software vydávaný pod licencí GPL. Umožňuje odposlouchávat síťový provoz, který je následně možné analyzovat. Zachycené pakety je možné filtrovat podle různých kritérií (např. podle protokolu, IP adresy, apod.). Síťový provoz je možné ukládat (nejčastěji ve formátu *.pcap), popřípadě nahrát ze souboru. Wireshark podporuje mnoho formátů, takže je možné importovat i data zachycená jiným síťovým analyzátorem. Nástroj má řadu využití, např. odstraňování síťových problémů, přezkoumání zabezpečení sítě, testování síťových aplikací nebo odladění implementace protokolů.

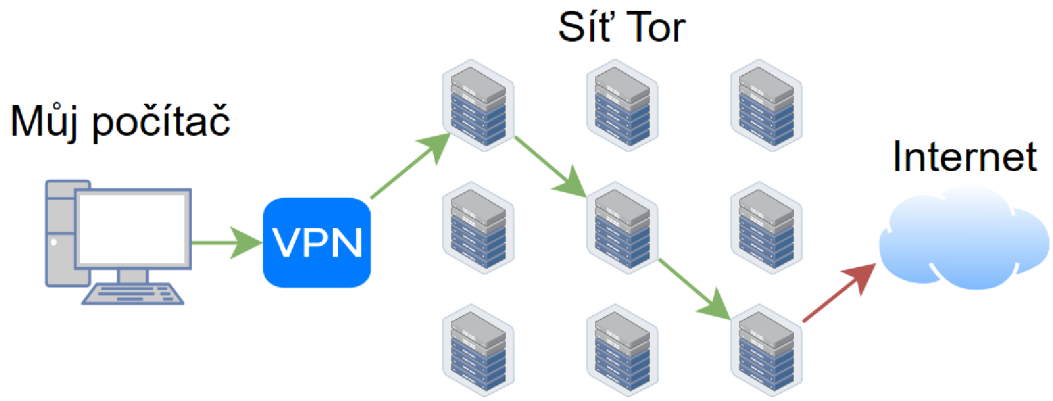
3 Zajištění vzorku a jeho analýza

Při manipulaci s potencionálně škodlivými nástroji je důležité dbát hlavně na svoji bezpečnost a anonymitu. Častokrát samotní tvůrci nebo ti, kteří škodlivé nástroje upravují, přetvářejí a zveřejňují, zapomínají skrýt své elektronické stopy. Na druhé straně, analýza malwaru nebo jeho vyhledávání za účelem analýzy vyžaduje také určité zabezpečení anonymity a skrývání elektronických stop. Pro svou práci jsem se rozhodla zajistit vzorek škodlivého nástroje, který bude naplňovat podmínku protizákonné činnosti. Za těchto okolností mohu narazit i na potencionálně nebezpečné weby, kde by mohlo dojít k získání osobních informací o návštěvnících, informací o poloze apod. Proto je z bezpečnostních důvodů nutné využít anonymizující služby.

3.1 Anonymizace

Pro zvýšení anonymity jsem zvolila kombinaci služby **VPN** a sítě **Tor**. Jako poskytovatele VPN jsem zvolila AirVPN. K připojení používám AirVPN klienta Eddie, který je open source software založený na OpenVPN integrující AirVPN služby. První je nutné standardním způsobem vytvořit účet. Poté zakoupit plán a následně je možné vybrat konfiguraci klienta ke stažení, podle typu systému (Windows či Linux) a architektury (32bit či 64bit), na kterém VPN klient poběží. Na výběr je ještě možnost vybrat formát instalačního souboru a možnost grafického prostředí.

Instalace přes grafické prostředí je jednoduchá a obsahuje základní věci jako licenční podmínky a cílové umístění instalace. Po dokončení instalace je klient připraven k použití a je možné ho spustit. Po spuštění je nutné se přihlásit. Dále už jsou na výběr desítky serverů, ke kterým se lze připojit. Eddie nabízí i připojení k doporučenému serveru, který vybere podle aktuálních parametrů (tzn. vytížení serveru, odezva, počet připojených uživatelů). Pokud chci přistupovat na konkrétní darkweby, je vhodné dle toho vybrat server manuálně podle lokace, protože mnohé weby umožňují přístup pouze z některých zemí. Klient dále obsahuje informace o rychlosti downloadu a uploadu, statistiky připojení (latenci, IP adresy, protokol, port, atd.) a logy událostí. Zaznamenány jsou informace jako použité šifrování, certifikáty, provedení autentizace, změny serverů, apod. Souběžně s VPN využívám cibulové sítě Tor. Do sítě Tor se připojuji z virtuálního prostředí Tails, který mám nainstalovaný ve Virtualboxu a jehož specifika jsou již popsána výše. Aby bylo docíleno dvojité vrstvy šifrování, nejprve je nutné se připojit do VPN z hostujícího počítače, a až poté spustit Tails a v něm prohlížeč Tor. Schéma je znázorněno na obrázku 3.1.



Obr. 3.1: Princip použití služby VPN + Tor

3.2 Analýza darkwebů

Fóra, která obsahují malware, exploity a nástroje k obcházení bezpečnostních prvků je nespočet. Lze je vyhledávat různými způsoby. Nejjednodušší je vyhledávání pomocí běžných vyhledávačů (Google, Bing, apod.). Dále je možné vyhledávat pro síť Tor pomocí TORCH (*xmh57jrznw6insl.onion.to*) nebo *eepsites.i2p* pro vyhledávání na i2p.

Při vyhledávání vzorků k zajištění jsem se zaměřila spíše na tzv. skript kiddie fóra. Většina těchto webů vyžaduje k přístupu na fórum pouze registraci. Někdy stačí registrace i k tomu, aby mohly být z fóra staženy soubory, jindy je požadována aktivita (např. komentování příspěvku) nebo minimální doba registrace (např. 14 dní po registraci je již umožněno stahovat soubory). Hlavní důvod, proč jsem k práci zvolila tento typ fór je ten, že na kriminální fórum je vstup většinou pouze na pozvání a k tomu je nutné vytvořit již nějaký malware nebo získat doporučení od již stávajících členů komunity kriminálního fóra.

Z řady fór jsem pro analýzu vybrala *devilteam.su*. Jedná se o funkční fórum s denně aktivními uživateli. Objevují se na něm nejrůznější témata a nástroje k obcházení bezpečnostních prvků. Z velké části fórum obsahuje návody k používání různých nástrojů k administrativní činnosti, nastavení sítě či programování. Uživatelé zde také přidávají příspěvky se svým softwarem a kontaktem a tímto způsobem nabízejí své služby.

3.3 Zajištění vzorku

K zajímavějším oblastem webu *devilteam.su* patří kategorie **Virus**, která obsahuje podkategorie **RATs** a **Trojan**. V podkategorii **RATs** jsem narazila na nástroj ke

vzdálené správě zařízení se systémem Android. Nástroj se nazývá Droidjack a na fóru *devilteam.su* byla zveřejněna jeho cracknutá verze. Bohužel odkaz ke stažení Droidjacku již nefungoval, protože Droidjack byl nahrán na dočasném úložišti, kde došlo buď k vypršení doby uložení a nebo k jeho odstranění z úložiště.

Přesto, že Droidjack nebyl k dispozici na *devilteam.su*, zkusila jsem najít nástroj na jiných webech, což se podařilo. Zjistila jsem, že Droidjack je stále poměrně rozšířený a najít další zdroje ke stažení cracknutého nástroje bylo poměrně jednoduché. Četnost vzorků dokládá snahu šířit tento malware pravděpodobně v úmyslu poškodit prodej DroidJacku na stránkách *droidjack.net*. Následující seznam je příklad webů, na kterých je Droidjack aktuálně dostupný:

- https://www.xup.in,
- http://easyupload.net,
- https://www.ethicalhackingtutorials.com,
- https://dfiles.eu,
- https://hageektools.blogspot.com,
- https://haxf4rall.com.

Z povahy věci neuvádím přímé odkazy ke stažení Droidjacku, ale pouze adresy webů. Většina nalezených vzorků má totožný otisk, avšak občas se objevují i vzorky s otiskem jiným. Tyto vzorky byly pravděpodobně upraveny vícero uživateli a je možné, že kód byl upraven nebo rozšířen v jejich prospěch. Další kapitoly budou věnovány vzorku zajištěnému z *haxf4all.com*. Zmíněný web obsahuje článek o funkcích nástroje Droidjack, odkaz na video tutoriál a odkaz na fileserver *https://upload.ac*, kde lze nástroj stáhnout. Před stažením bylo nutné projít ověřením Captcha, jinak stahování probíhalo standardním způsobem.

3.4 Analýza vzorku

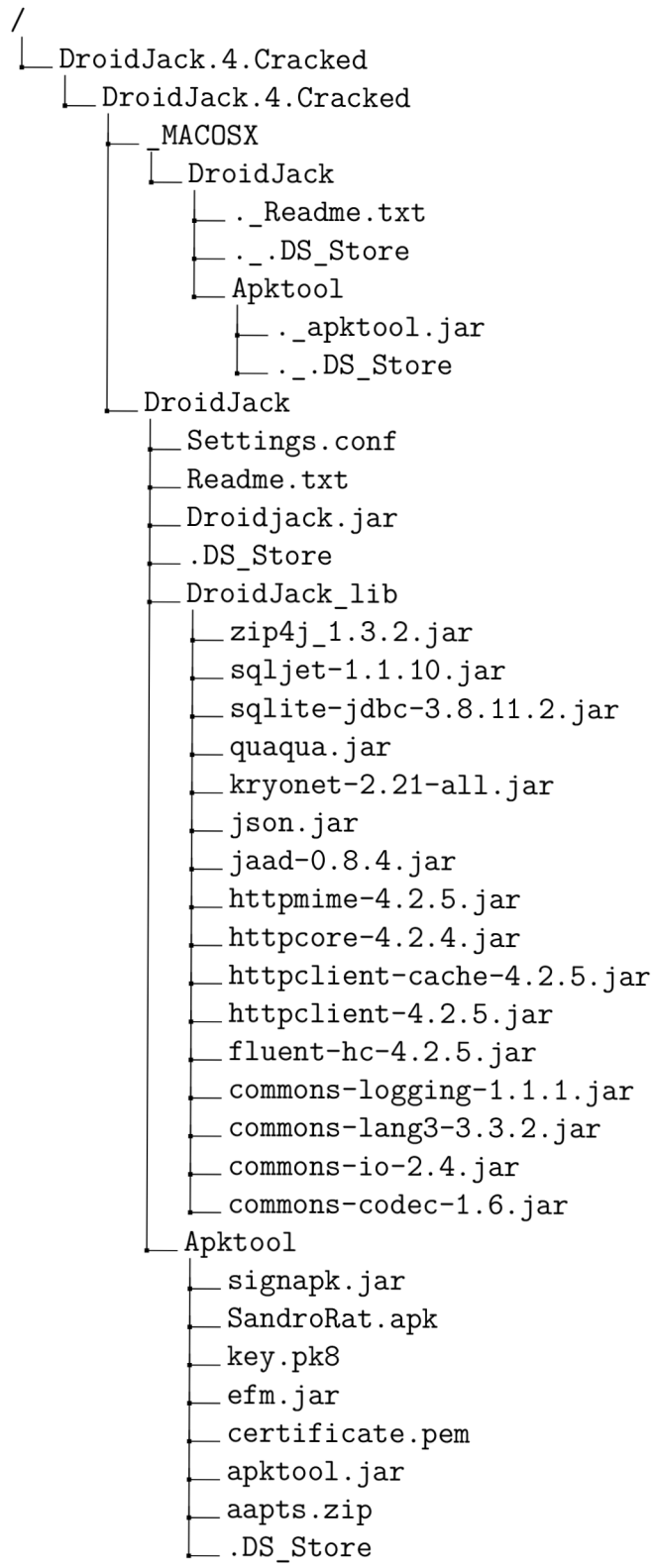
DroidJack je trojan založený na SandroRAT, který původně vznikl z nástroje Sandroid. Původně byl nástroj roku 2013 nabízen na Google Play Store jako nástroj, který uživatelům umožní kontrolu počítače. Nezaznamenal však značný úspěch a tak se tvůrce zaměřil na jiné uživatele a nástroj začal nabízet na fóru *hackforums.net* [19]. Roku 2015 byl tento nástroj využit k útokům na mobilní bankovnictví v Polsku. O rok později byl použit v souvislosti s vydáním populární hry Pokemon GO. Uživatelé, kteří na hru čekali a neměli ji zatím k dispozici přes oficiální Obchod Play, ji začali shánět neoficiální cestou, a tak narazili na infikovanou verzi Pokemon GO, která obsahovala DroidJack [20]. I přesto, že byla vedena extenzivní kampaň orgánů činných v trestním řízení proti uživatelům RAT DroidJack, nebyl chod portálu a pravděpodobně ani další vývoj nijak narušen.

3.4.1 Jak začít s analýzou

Postup při prvotní analýze je následující: Připravit si ve virtuálním prostředí analyzační stanici s veškerým potřebným softwarem, nástroji, atd. a poté vytvořit snímek takto připravené stanice. K tomuto snímku se lze vždy vrátit, pokud při analýze dojde k nevratné chybě. Výhodou je, že lze provádět i více analýz najednou (stejný vzorek s jinými nástroji nebo odlišný vzorek, ale současně). Většina virtuálních prostředí totiž umožňuje i klonování snímků. Snímky lze vytvářet i v různých fázích analýzy, tudíž je možné se vrátit tam, kam je třeba.

3.4.2 Vytváření otisků

Analýza byla provedena ve virtuálním počítači s operačním systémem Caine 10. Při analýze škodlivého či neznámého softwaru je nezbytné ihned po zajištění vytvořit hashe souborů a archivů. Tyto hashe je pak možné porovnat s již existující databází hashů a snáze tak identifikovat, o jaký software, nástroj či malware se jedná. K tomu jsem použila výše zmiňovaný nástroj QuickHash, který je součástí operačního systému Caine 10. Po spuštění nástroje jsem zvolila záložku **File**, vybrala SHA256 a vybrala originální archiv vzorku **Droid_Jack.4.4[breachthesecurity.com].rar**. Poté jsem vytvořila hashe i pro obsažená data. Přesunula jsem se tedy na záložku **FileS**. Zde je možné vybrat celou složku a libovolně zahrnout i podsložky a vytvořit hashe pro všechna data. Archiv obsahuje 32 souborů a jeho struktura je následující:



Hlavní adresář Droidjack obsahuje spustitelný soubor *Droidjack.jar*. Při provádění analýzy programu jsou klíčové právě spustitelné soubory. Dále archiv obsahuje návod od samotného autora v textovém souboru *Readme.txt*, jak nástroj používat a rady na nejčastější komplikace s nástrojem. V adresáři se také nachází složka s kon-

figuračními soubory pro server *DroidJack_lib* a konfigurační soubor *Settings.conf*. Dále obsahuje složku *Apktool*, ve které jsou soubory potřebné pro vygenerování DroidJack klienta ve formátu APK. Také obsahuje samotný trojan *SandroRat.apk*, na kterém je DroidJack založen. Právě ten tvoří základ generované aplikace.

Otisk archivu **Droid_Jack.4.4 [breachthesecurity.com].rar** pomocí algoritmu SHA256 je následující:

- 4C0C10FE8EA03E2B46A78810792486902E3EA1FBAF2E7439029BEAF77B32BF4A

Otisky obsahujících souborů jsou zobrazeny v tabulkách 3.1 a 3.2.

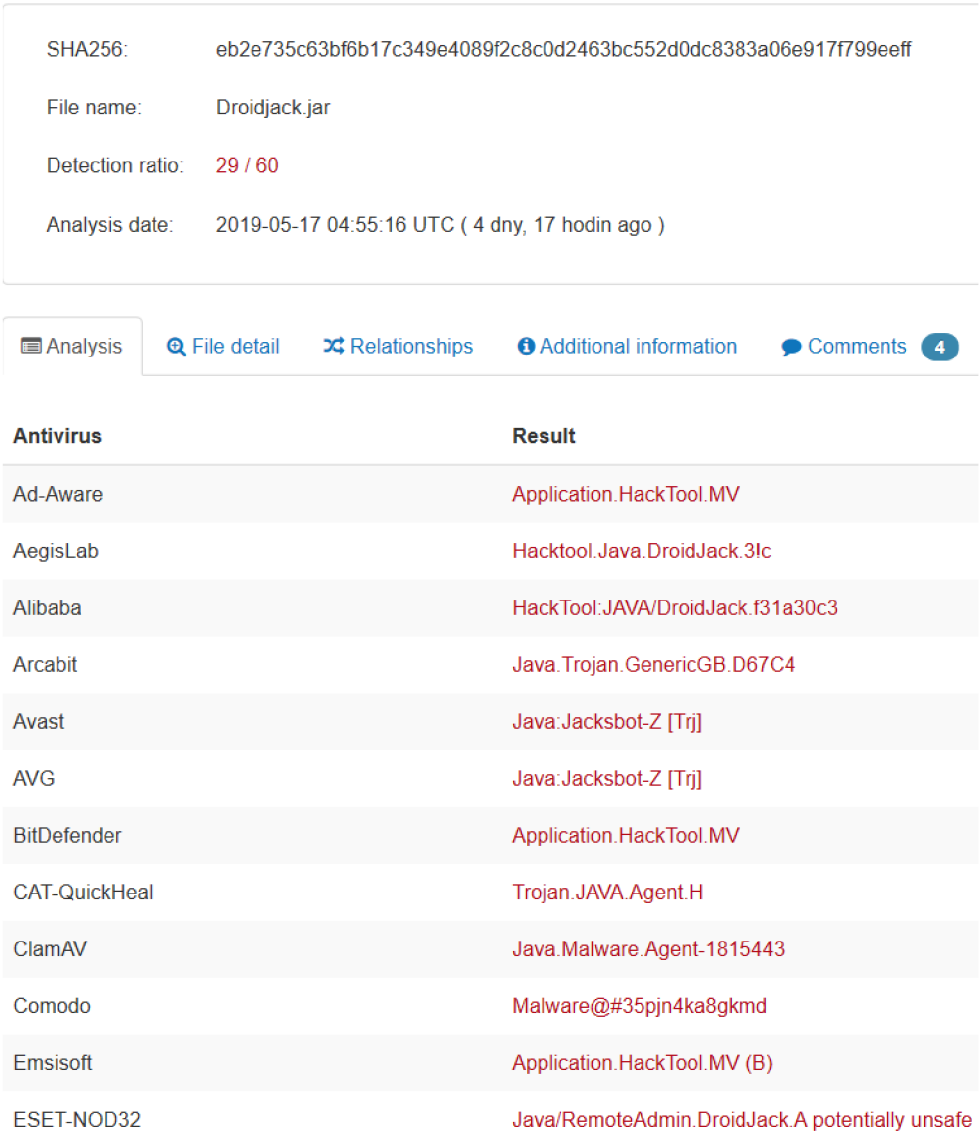
Pomocí těchto hashů je možné vyhledávat v databázích škodlivého softwaru a získat tak bližší informace o analyzovaném vzorku. Příkladem těchto online nástrojů jsou **virustotal.com** a **hybrid-analysis.com**. Pokud byl již vzorek někdy nástrojem analyzován, je dohledatelný právě pomocí hashe. Pokud ne, je možné nahrát přímo soubor (v případě analyzovaného vzorku se jedná o soubor *Droidjack.jar* nebo i *SandroRat.apk*) a nástroj poté provede analýzu. Pomocí podobných nástrojů lze často nalézt i další verze vzorku, popřípadě související soubory (třídy, knihovny, apod.). Výpis z VirusTotal je zobrazen na obrázku 3.2. Právě pomocí VirusTotal bylo zjištěno, že existují svazky s dalšími desítkami souborů oskenovaných pomocí tohoto nástroje.

Soubor	**Hash (SHA256)**
._Readme.txt	D77E265E4E35C81D17761BFBC47C7FAE3D45141B55 FE63A407E4BF92D69FFBB3
._.DS_Store	74694443E1068DDA8CB89E61B380EA27BCF410293B B68B4680E9D1253DA73D4D
._apktool.jar	E5AC3A87C6D3F093A9BC5C3CA4CC6227FB4B9F8B 46FB04D154C40FFE2E2CFE71
._.DS_Store	74694443E1068DDA8CB89E61B380EA27BCF410293B B68B4680E9D1253DA73D4D
Droidjack.jar	EB2E735C63BF6B17C349E4089F2C8C0D2463BC552D 0DC8383A06E917F799EEFF
.DS_Store	923211913F3C80FB88E966BE6301E7965C28785E91137 2ABA7CB4ADFFAC305A2
Settings.conf	74EF3785B09777D3937B3B8889455761BF613E2848793 04B2B1D0ACEC964732C
Readme.txt	0FC45CF966832A54A4783F71DC02511A22FB28144B1 4737E3EB6C37CF4E14159
key.pk8	A07CE769D17334F803A499C520D4A7D88478CEB1A9 CF740FAF296F8F54616E82
apktool.jar	C15CF1B87486D83DBC9E5CE64A03178A64EEEECF6 2CF08637193BA759F61419B
aapts.zip	9BA477194B6BEE993D26D1051A4E02143540F6B12CF 93D498F380EA0E40E1A1A
signapk.jar	B17534E89A5B58D5E343BA54A49DA579CF9213988F4 BEEAE24FE4582A0C226BB
.DS_Store	8C7D7C53AF7189A9235E4A43ED2694F874C20CE061 CE23B1F271436E8404A64D
certificate.pem	B2E32152E7972032FD64AD351323F50008602C60FEB1 9522B1AADD414BF1F7B4
SandroRat.apk	30AA2EEEB8401E4A312A7E99462432769A7C56911418 0AAEDBFCBEF18B6DB268
efm.jar	91D79633B19D62B0EA71341B1692F49B2B59F9535E30 A181D66FC4E83B0A2660

Tab. 3.1: Tabulka hashů (první část)

Soubor	**Hash (SHA256)**
kryonet-2.21-all.jar	EAB8C51E0E3A11BB1411ACE21D9876184D5084FDE 82EE298DA03CA0627499151
sqljet-1.1.10.jar	DF7463424E3560F5E8C8003E1816C0A6EA6E84673921 CA5AF05B90B0892B3C97
httpclient-cache- 4.2.5.jar	A67C50B74286766BDBB397088C4A78F1008D2AB17D F7562DB76439778C90430A
httpclient-4.2.5.jar	56B4AAE1BD9C66E1F890279DDE75E81D226C97E302 DE97DAFC081ADEAB956BBC
quaqua.jar	04C1725622CA16461436EF1D35D9992F82680997761FC 76116E37F2347EE03D4
sqlite-jdbc-3.8.11.2.jar	F30968B896AF52BAAEDA4A901F6EF2629319168FA3 04E9747C7CFABEF6C476EC
httpmime-4.2.5.jar	2EF409C599C532CA1E692013582695231BDB9F3956D4 EC9BA3AC71300728B382
commons-lang3- 3.3.2.jar	46D24EA8D0771655AEC5FDF203CA4BFAB4CC1A458 7B8A15901D385F80263DD36
commons-logging- 1.1.1.jar	CE6F913CAD1F0DB3AAD70186D65C5BC7FFCC9A99 E3FE8E0B137312819F7C362F
commons-codec- 1.6.jar	54B34E941B8E1414BD3E40D736EFD3481772DC26DB 3296F6AA45CEC9F6203D86
httpcore-4.2.4.jar	BDA2B9E0464F7A0E122D5E9BFF7B384F3BC3A91AF 18AD51E029DEAAA599E5DB3
jaad-0.8.4.jar	BE6BA7919A20F602703536E343860C2AE74AD18DA19 5FD845743B877DBB379F7
commons-io-2.4.jar	CC6A41DC3EAACC9E440A6BD0D2890B20D36B4EE4 08FE2D67122F328BB6E01581
fluent-hc-4.2.5.jar	E13070F38957FC1C063895105AB64C810A3FD8B4B6A B5D45CE2D508C8D5FA192
json.jar	38C21B9C3D6D24919CD15D027D20AFAB0A019AC92 05F7ED9083B32BDD42A2353
zip4j_1.3.2.jar	92524AA1BF716F1D15E75FB66C2212EE903E118677C A625506F94487628317F7

Tab. 3.2: Tabulka hashů (druhá část)



SHA256:	eb2e735c63bf6b17c349e4089f2c8c0d2463bc552d0dc8383a06e917f799eeff
File name:	Droidjack.jar
Detection ratio:	29 / 60
Analysis date:	2019-05-17 04:55:16 UTC (4 dny, 17 hodin ago)

Analysis | File detail | Relationships | Additional information | Comments 4

Antivirus	Result
Ad-Aware	Application.HackTool.MV
AegisLab	Hacktool.Java.DroidJack.3!c
Alibaba	HackTool:JAVA/DroidJack.f31a30c3
Arcabit	Java.Trojan.GenericGB.D67C4
Avast	Java:Jacksbot-Z [Trj]
AVG	Java:Jacksbot-Z [Trj]
BitDefender	Application.HackTool.MV
CAT-QuickHeal	Trojan.JAVA.Agent.H
ClamAV	Java.Malware.Agent-1815443
Comodo	Malware@#35pjn4ka8gkmd
Emsisoft	Application.HackTool.MV (B)
ESET-NOD32	Java/RemoteAdmin.DroidJack.A potentially unsafe

Obr. 3.2: Scan souboru Droidjack.jar z VirusTotal

3.4.3 Zachycení komunikace

Prostřednictvím **hybrid-analysis.com** jsem zjistila, že vzorek se snaží kontaktovat droidjack.net s IP adresou 162.251.80.24 port 80, což je oficiální stránka tohoto nástroje, kde je nástroj nabízen jako legální software a je možné zde koupit jeho licenci za 210$. Originální nástroj je pravděpodobně schopný ověřit licenci a povolit užívání pouze autorizovaným uživatelům.

Dále jsem se rozhodla odchytit síťovou komunikaci DroidJacku pomocí programu Wireshark, takže jsem si nástroj Wireshark spustila přes příkazovou řádku příkazem *sudo wireshark*. Wireshark musí být pod systémem Caine spuštěn s administrátorským oprávněním, aby mohl přistupovat k síťovému rozhraní. Po spuštění jsem

vybrala rozhraní *enp0s3* a zvolila *Start*. Při pokusu spustit zajištěný vzorek ve virtuálním prostředí Caine s nastavenou vnitřní sítí bez přístupu k Internetu došlo k chybě *NullPointerException* a spouštěcí proces byl zastaven. Zachycenou chybu nebylo možné bez zdrojového kódu identifikovat a odstranit, proto jsem síťové připojení virtuální stanice nastavila na síťový most s přístupem do Internetu. Navíc bylo zjištěno, že vzorek nelze spustit standardním příkazem *java -jar Droidjack.jar* pomocí příkazové řádky. Když jsem se ho pokoušela spustit tímto způsobem, opět byl proces spouštění přerušen. DroidJack bylo tedy nutné spustit pouze přes grafické rozhraní (pravým tlačítkem kliknout na soubor *Droidjack.jar* a zvolit *Otevřít pomocí Java 8*. Poté se již nástroj spustil bez problémů.

Zachycená komunikace na obrázku 3.3 potvrzuje, že nástroj se opravdu snaží komunikovat s droidjack.net a patrně to je důvodem, proč nastala chyba při spouštění v uzavřené síti. Požadavky na IP adresu 162.251.80.24 se snaží odesílat několikrát za sebou. Pokud má k adrese přístup, vyžádá si soubor *Terms.html*, který obsahuje licenční ujednání, které je nutné potvrdit pro pokračování aplikace.

Time	Source	Destination	Proto	Lengt	Info
74.542010	192.168.0.59	192.168.0.1	DNS	77	Standard query 0x79ec A www.droidjack.net
74.872262	192.168.0.1	192.168.0.59	DNS	107	Standard query response 0x79ec A www.droidjack.net CNAME droidjack.net A 162.251.80.24
74.872679	192.168.0.59	192.168.0.1	DNS	77	Standard query 0xa3c9 AAAA www.droidjack.net
75.048774	192.168.0.1	192.168.0.59	DNS	155	Standard query response 0xa3c9 AAAA www.droidjack.net CNAME droidjack.net SOA ns1.cp-13.webhostbox.net
75.052402	192.168.0.59	162.251.80.24	TCP	66	49557 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
75.215189	162.251.80.24	192.168.0.59	TCP	66	80 → 49557 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1420 SACK_PERM=1 WS=128
75.215427	192.168.0.59	162.251.80.24	TCP	54	49557 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
75.293783	192.168.0.59	162.251.80.24	HTTP	221	GET /Terms.html HTTP/1.1
75.463114	162.251.80.24	192.168.0.59	TCP	1474	80 → 49557 [ACK] Seq=1 Ack=168 Win=15744 Len=1420 [TCP segment of a reassembled PDU]
75.464359	162.251.80.24	192.168.0.59	TCP	1474	80 → 49557 [ACK] Seq=1421 Ack=168 Win=15744 Len=1420 [TCP segment of a reassembled PDU]
75.464368	162.251.80.24	192.168.0.59	HTTP	1021	HTTP/1.1 200 OK (text/html)
75.464528	192.168.0.59	162.251.80.24	TCP	54	49557 → 80 [ACK] Seq=168 Ack=3808 Win=66560 Len=0
75.467543	192.168.0.59	162.251.80.24	TCP	54	49557 → 80 [FIN, ACK] Seq=168 Ack=3808 Win=66560 Len=0
75.631293	162.251.80.24	192.168.0.59	TCP	54	80 → 49557 [FIN, ACK] Seq=3808 Ack=169 Win=15744 Len=0
75.631486	192.168.0.59	162.251.80.24	TCP	54	49557 → 80 [ACK] Seq=169 Ack=3809 Win=66560 Len=0

Obr. 3.3: Odchycená komunikace programem Wireshark

Dále jsem zjistila, že nástroj je určen pro operační systém Windows. Lze sice spustit i na systému založeném na Ubuntu 18.04, ale nefunguje správně. Generování aplikace vykazuje chybu hned v počátku. Další aktivní analyzování nástroje bylo prováděno na operačním systému Windows 7, kde nástroj funguje spolehlivě.

3.4.4 Funkčnost vzorku

Po spuštění nástroje DroidJack vyskočí okno s přihlášením vyžadující jméno a heslo. Tato pole je možné nechat zcela prázdná a pokračovat potvrzením tlačítka zámku. Nástroj umožňuje generovat klienta, pomocí kterého je následně možné vzdáleně ovládat zařízení, které má klienta nainstalováno. S klientem lze nastavit komunikaci jak přes síť LAN, tak i přes síť WAN (Internet). Co se týče konfigurace, v síti LAN postačí IP adresa zařízení, které bude naslouchat. Při konfiguraci přes síť WAN autor nástroje doporučuje registrovat dynamické DNS a forwardovat porty 1334 a 1337 (nebo cokoliv v rozmezí 1024 - 65535, co není využíváno nějakou aplikací). K těmto

portům se poté připojuje vygenerovaný klient DroidJacku. Ve chvíli, kdy je aplikace spuštěna, jsou otevřeny porty 1334 a 1337 pro UDP a TCP spojení. Aplikace si vyžádá v podstatě všechna oprávnění a po jejich potvrzení je umožněno vzdálené ovládání.

Díky možnosti šifrování je usnadněno skrytí trojského koně v legitimní aplikaci. Trojan injektovaný do aplikace nemusí být rozpoznatelný ani antivirovým programem. Navíc lze nastavit tzv. *skrytý mód*, kdy se aplikace v grafickém prostředí nezobrazuje jako spuštěná, ačkoliv stále naslouchá a čeká na příkazy ze vzdáleného zařízení.

Jakmile je klient spuštěn, je vzdáleně možné provádět následující akce:

- procházet a spravovat soubory (nahrávat a stahovat),
- procházet SMS, posílat SMS,
- procházet správce volání,
- spravovat zprávy prostřednictvím aplikace WhatsApp,
- procházet, přidávat a mazat kontakty,
- procházet historii internetového prohlížeče,
- procházet instalované aplikace,
- použít GPS lokátor a zjistit tak polohu zařízení,
- pořizovat snímky a pořizovat video,
- použít mikrofon k odposlouchávání zařízení a pořizovat nahrávky,
- otevírat v prohlížeči webové stránky,
- zobrazovat vyskakovací zprávy,
- ovládat hlasitost.

V rámci připojení je zobrazováno telefonní číslo (pokud je registrované v síti), model a architektura telefonu. Je možné dodatečně konfigurovat následující nastavení aplikace:

- měnit dynamickou DNS a port,
- zapnout skrytý mód,
- zapnout mobilní data, když je voláno zvolené číslo,
- zapnout WiFi, když je voláno zvolené číslo,
- zapnout spouštění zároveň se zvolenou aplikací,
- aktualizovat aplikaci nebo instalovat novou,
- nastavit aplikaci jako systémovou,
- navždy odpojit od klienta.

Výše vyjmenované funkce svědčí o tomu, že nástroj je určen především pro nelegální účely a jeho užitím se uživatel může dopustit rozsáhlých škod na majiteli infikovaného zařízení, jak už majetkových (krádež peněz z bankovního účtu), tak i porušování práv (např. neoprávněné nakládání s osobními údaji). Všechny mechanizmy nejsou schopny detekovat malware a při použití s populární aplikací bude

schopnost detekce ještě snížena. Přesto že jde o prozkoumaný malware, může být phishingová kampaň s payloadem DroidJack velmi efektivní právě kvůli možnosti zneužít populární placené aplikace jako vektor útoku. Jedná se tedy o extrémně nebezpečný malware, který může být efektivně zneužit i proti chráněnému zařízení.

4 Simulace bezpečnostního incidentu

Cílem práce je vytvořit prostředí pro zajištění elektronického důkazního materiálu. V rámci práce nasimulovat bezpečnostní incident a poté ve vytvořeném prostředí provést jeho analýzu. V rámci simulace bude blíže prozkoumáno prostředí a možnosti zajištěného nástroje Droidjack. Nástroj je typu RAT, který je zaměřený na systém Android, a proto bude tento systém cílem útoku. V rámci simulace bude zajištěn disk útočníka, který bude následně analyzován.

Nástroj narušující bezpečnost uživatelům se systémem Android byl vybrán záměrně, jelikož se v dnešní době jedná o jeden z velmi častých a poměrně snadných útoků. Může za to pravděpodobně rozšířenost tohoto systému, ale také jeho otevřenost. Prakticky kdokoliv může do obchodu Google Play (obchod s aplikacemi pro Android) nahrát téměř cokoliv. Na druhé straně jsou zvědaví uživatelé, kteří si stáhnou kdejakou aplikaci např. jen proto, že má pěknou ikonku a popis. Dále všechny požadavky aplikace přijmou, aplikaci bez rozmýšlení instalují a spouští. Podobný scénář jsem vybrala pro mou simulaci. Důvodem simulace bezpečnostního incidentu a následné analýzy je ukázat, jak snadné je stát se obětí útoku a jak lehkovážné chování na Internetu vede k přibývajícím případům narušení bezpečnosti systému. Ukázat jednu z možností, proč se kyberkriminalita stává jedním z nejvýdělečnějších zločinů.

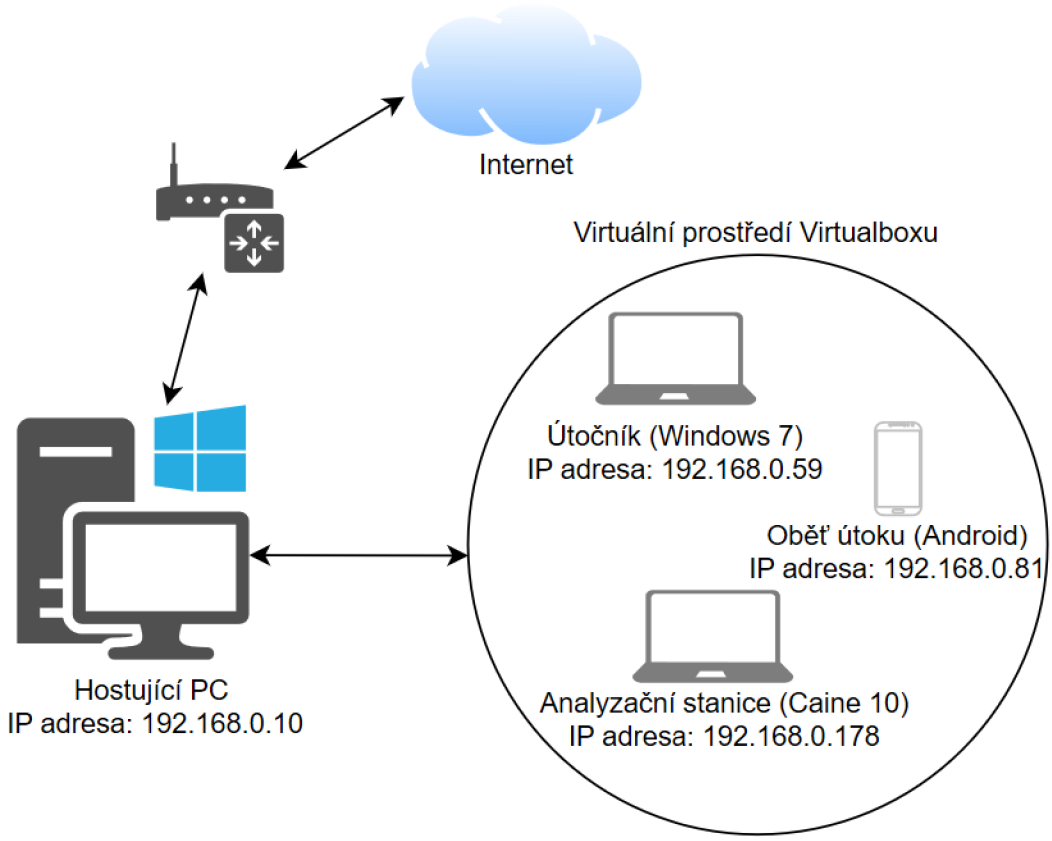
4.1 Hostující stanice

Jelikož navržené virtuální prostředí, které je popsáno níže, není až tak výpočetně náročné, je spuštěno na běžném počítači. Zařízení disponuje operační pamětí 8GB a mikroprocesorem Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz. Na zařízení je nainstalovaný 64bitový operační systém Windows 10 Home.

4.2 Virtuální prostředí pro simulaci bezpečnostního incidentu

Jak vyplývá z teoretické části, virtuální prostředí má nesmírné výhody k simulaci incidentů a analyzování aktivity v zařízení, proto je virtuální prostředí využito i při tvorbě této práce. Jako virtualizační software jsem zvolila Virtualbox verze 6.0.8, který je volně dostupný ke stažení z https://www.virtualbox.org/wiki/Downloads. Instalace je jednoduchá, k výběru je pouze výběr složky, kam se má Virtualbox a jeho funkce nainstalovat a popřípadě vytvoření zástupců (např. na ploše). Po dokončení instalace je Virtualbox možné ihned používat.

Do Virtualboxu jsem si nainstalovala tři virtuální stanice,a to Android 7.1 r2, který je obětí útoku, Windows 7 Home, který je použit k útoku a Caine 10, na kterém je provedena analýza. Systém Windows byl zvolen kvůli nástroji Droidjack. Ačkoliv byla práce s ním odzkoušena i na linuxovém systému, ukázalo se, že na systému Windows pracuje nejspolehlivěji. Blokové schéma zapojení virtuálních strojů je zobrazeno na obrázku 4.1.



Obr. 4.1: Schéma zapojení virtuálních stanic

4.2.1 Android

Operační systém Android je dostupný přímo z oficiálních stránek Androidu, konkrétně z http://www.android-x86.org/. Je nutné zmínit, že se jedná o „rootnuté“ systémy, které se využívají při různém testování či vyvíjení softwaru a lze je nainstalovat do Virtualboxu jako standardní desktopový systém. Pro svou práci jsem zvolila Android-x86 7.1-r2 released.

Postup pro přidání do Virtualboxu je následující. Ve Virtualboxu zvolím *Nový*. Do kolonky *Název* vepíšu název virtuálního stroje, v nabídce *Typ* vyberu *Linux* a verzi *Ostatní Linux (64 bit)*. Odkliknu tlačítko *Další*. V následujícím okně zvolím

velikost paměti RAM. Pro příjemnější práci zvolím velikost paměti RAM minimálně *2 GB*. Odkliknu tlačítko *Další*. Vyberu *Vytvořit* nyní virtuální pevný disk a zvolím *Další*. Typ virtuálního pevného disku zvolím *VDI* a zvolím *Další*. Disk zvolím *dynamicky alokovaný* a zvolím *Další*. Určím maximální velikost *16 GB* a umístění, odkud se virtuální stroj bude spouštět (možno nechat výchozí). Nakonec kliknu na *Vytvořit*.

Jelikož je systém Android modifikovaný linuxový systém, instalace probíhá podobně jako u linuxových systémů. Na výběr jsou standardní možnosti instalace jako rozdělení disku, výběr souborového systému, instalace GRUB, atd. Protože je systém Android navržen především pro dotyková zařízení, bylo nutné jej restartovat a v nastavení virtuálního počítače v záložce *Systém* nastavit ukazovací zařízení na *PS/2 myš*.

4.2.2 Windows

Operační systém Windows 7 je komerčním produktem společnosti Microsoft. Oproti použitým linuxových systémům má zcela odlišnou architekturu a i správa systému je rozdílná. Systémy Windows jsou nejčastěji používány nejen na osobní počítače, ale především také ve firemní sféře, proto je také většina útoků stále ještě situována právě na uživatele se systémem Windows.

Přidání Windows 7 do Virtualboxu je obdobné jako u výše popsaného Androidu s tím rozdílem, že typ operačního systému vyberu *Windows* a verzi *Windows 7 (64bit)*. Další parametry zvolím tak, aby splňovaly alespoň minimální požadavky systému. Pro 64bitový operační systém to je rychlost taktu procesoru minimálně 1 GHz, velikost RAM 2 GB, a virtuální disk o velikosti alespoň 20 GB.

Instalace systému je standardní a nevyžaduje zvláštní specifické znalosti. Po instalaci je již systém možné použít k simulaci, avšak je nutné doinstalovat ještě dva programy. Prvním je nějaký nástroj, který umí pracovat s archivy. Já jsem zvolila 7-Zip, jelikož je volně dostupný a pro běžnou práci je dostačující. A druhým je Java 8, která je nutná ke spuštění nástroje DroidJaku. Java je volně dostupná z webových stránek *https://www.oracle.com/*.

4.2.3 Caine

Caine je live distribuce a její instalace je trochu odlišná, avšak velmi snadná. Ve Virtualboxu jsem si opět přidala virtuální stroj a připojila iso soubor s distribucí Caine, která je dostupná ke stažení z https://www.caine-live.net/page5/page5.html. Při spouštění jsem zvolila *Boot Live in safe graphics mode*. Po startu systému je na ploše několik ikon. Aby bylo Caine možné využít nejen jako live distribuci, je nutná jeho instalace. Ještě před tím je ale nutné povolit zápis na disk pomocí nástroje

UnBlock. To se provede tak, že se program spustí, zvolí se disk, kterému chceme změnit mód zápisu a potvrdíme volbou *OK*. Pokud je mód zápisu *Read-Only*, změní se na *Writable* a naopak. Instalaci systému spustíme dvojklikem na *Instal 18.04*. Následně jsem zvolila jazyk a rozložení klávesnice. V dalším okně je k vybrání možnost stahovat aktualizace při instalaci systému, kterou doporučuji zaškrtnout, protože ušetří čas. Dalším krokem je vybrání typu instalace. Pokud nepotřebujeme specifické rozdělení disku, je nejlepší variantou *Vymazat disk a instalovat 18.04*. V dalším okně vybereme časovou zónu. Poslední volbou nastavení jména uživatele, login a jména hostitele na *caine* a heslo pro roota. Poté je možné spustit instalaci. Po jejím dokončení je Caine připraven k použití jako běžná stanice (tzn. nemusí se spouštět pouze jako live cd).

4.2.4 Použití vzorku k vytvoření bezpečnostního incidentu

DroidJack jsem přenesla do operační stanice s Windows 7, kterou jsem si předem připravila. Všechny použité virtuální stanice jsem zapojila do sítě přes síťový most, aby každé virtuální zařízení v síti mělo jednoznačnou IP adresu a konfigurace nástroje DroidJack byla tak snazší. Ve virtuální síti je povolen DHCP server a tak virtuální stroje dostaly následující IP adresy:

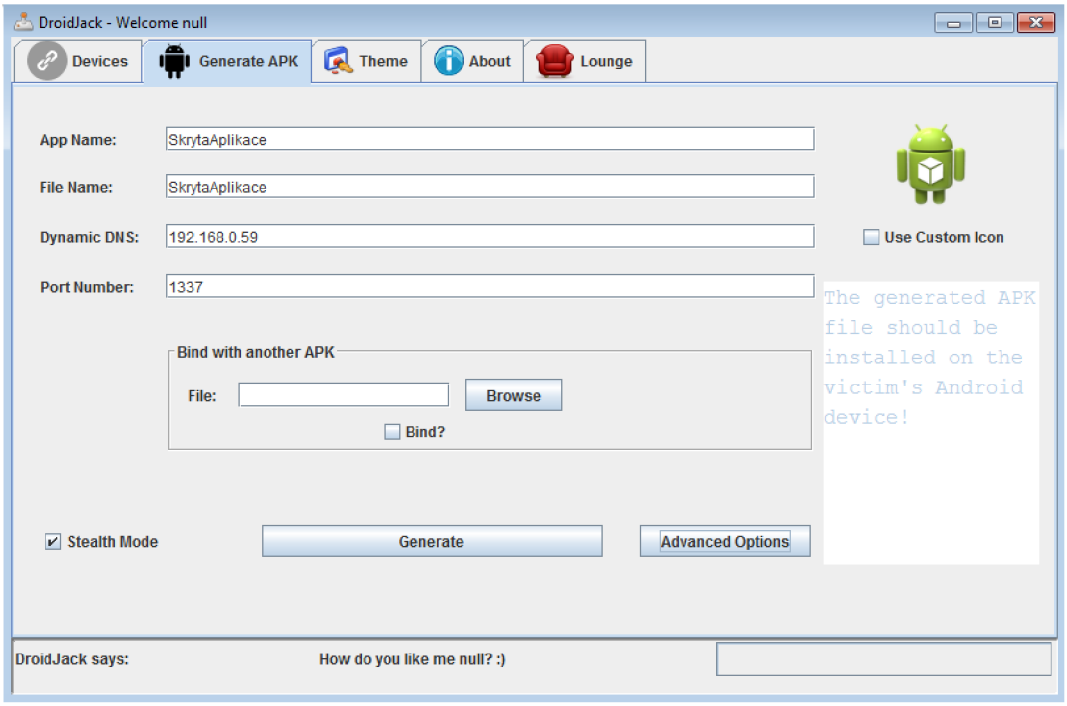
- Windows 192.168.0.59,
- Android 192.168.0.81,
- Caine 192.168.0.178.

Ve virtuálním stroji Windows jsem spustila nástroj DroidJack. Potvrdila jsem licenční podmínky a potvrdila přihlášení s prázdnými údaji. V nástroji jsem vybrala položku **Generate APK**. Do textového pole **App Name** jsem vložila název *CistaAplikace*, do pole **File Name** také *CistaAplikace*. Další kolonka je **Dynamic DNS**, do které v LAN síti stačí dát IP adresu zařízení, které bude vzdálenou správu provádět (bude na něm spuštěn DroidJack). V tomto modelovém případě to je virtuální stroj Windows s IP adresou 192.168.0.59. Další pole vyžaduje **Port Number**. Podle doporučení autora se má zvolit port 1337 nebo větší než 1024. Zvolila jsem tedy port *1337*. Dále nástroj umožňuje přidat aplikaci, do které bude trojan schován. Na výběr je ještě možnost *Skrytého módu*. Libovolně lze z klienta odstranit některé funkce, jako přístup ke kontaktům, k SMS, GPS, správci souborů, a další.

Pokud jsou některé funkce odstraněny, vygenerovaná aplikace nepožaduje všechna oprávnění, což může snížit podezření z potencionálně škodlivé aplikace. Dnes již existuje řada chytrých zařízení (např. chytré hodinky), která komunikují s telefonem pomocí aplikací a je zcela běžné, že vyžadují oprávnění k hovorům nebo SMS, aby mohla splňovat svoji funkci (např. zobrazení příchozí SMS). Proto dnes podobná oprávnění nejsou neobvyklá a může snadno dojít k zneužití dat.

Posledním možným nastavením je výběr šifrování. Pokud ho zvolíme, je na výběr ze šifrovacích algoritmů AES, DES, TripleDES a Blowfish.

Aplikaci jsem ponechala ve výchozím nastavení, tzn. povolené všechny funkce, bez šifrování, bez skrytého módu tak, jak lze vidět na obrázku 4.2.



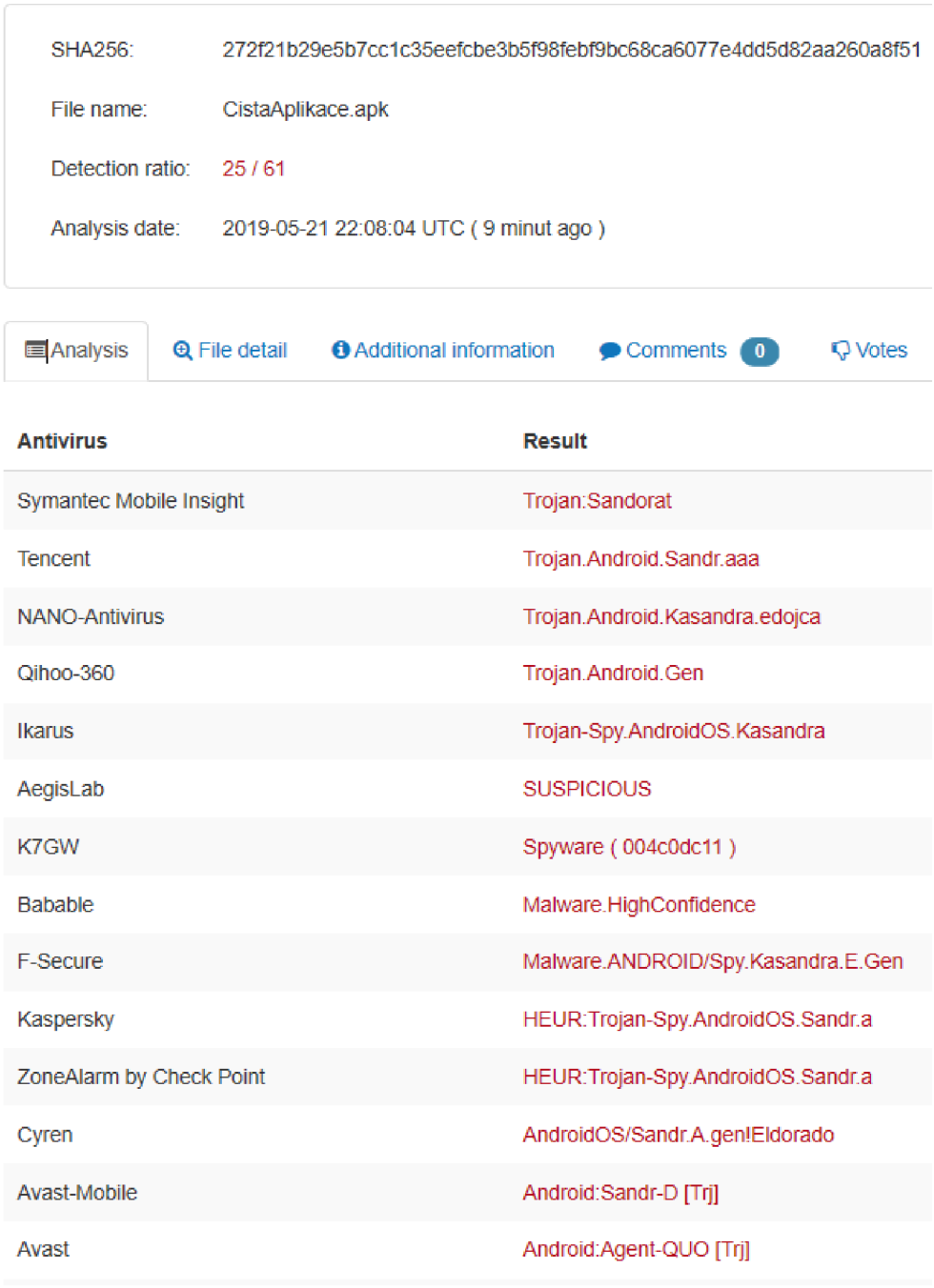
Obr. 4.2: Nastavení generovaného klienta DroidJacku

Poté jsem potvrdila tlačítko **Generate**. Protože jsem nezvolila nějakou aplikaci, s kterou bych DroidJack klienta spojila, byl vygenerován čistý klient ve formátu APK. Tento soubor jsem nahrála na dočasné úložiště *leteckaposta.cz* a poté jej pomocí prohlížeče Chrome stáhla do virtuální stanice Android. Jelikož ke stažení došlo prostřednictvím prohlížeče Chrome, bylo nutné ještě povolit instalace z neznámých zdrojů. Útočníci však často své aplikace nahrají přímo do Obchodu Play, který je brán jako důvěryhodný zdroj aplikací. Nakonec je možné spustit instalaci aplikace, potvrdit vyžadovaná oprávnění a aplikaci spustit.

Pouze klient DroidJacku při spuštění vykazuje jen prázdné okno (pokud je povolen *skrytý mód*, okno jen problikne a již se nezobrazuje), avšak na pozadí již čeká na spojení a na požadavky. Oběť útoku nemusí ani tušit, že došlo ke kompromitaci zařízení.

Pomocí VirusTotal jsem provedla analýzu vygenerované aplikace *CistaAplikace* a výpis ze skenování je na obrázku 4.3. Dle VirusTotal aplikaci jako škodlivou detekuje 29 z 61 nástrojů na rozeznávání škodlivého softwaru. Základní informace o souboru jsou na obrázku 4.4.

Mimo jiné byl na VirusTotal nalezen soubor *livecamera.apk*, který obsahuje shodné prvky jako vygenerovaná aplikace a jde tudíž také o trojan SandroRAT. Například vyžaduje stejná oprávnění a obsahuje shodně s vygenerovanou aplikací 12 souborů. Také obsahuje stejné stringy, viz obrázek 4.5. Patrně se jedná o dalšího generovaného klienta nástroje DroidJack. Detekční hodnota je téměř stejná jako u generované aplikace a výsledky z analýzy velmi podobné. Informace o *livecamera.apk* z VirusTotal jsou na obrázcích 4.6 a 4.7.



SHA256: 272f21b29e5b7cc1c35eefcbe3b5f98febf9bc68ca6077e4dd5d82aa260a8f51

File name: CistaAplikace.apk

Detection ratio: 25 / 61

Analysis date: 2019-05-21 22:08:04 UTC (9 minut ago)

Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result
Symantec Mobile Insight	Trojan:Sandorat
Tencent	Trojan.Android.Sandr.aaa
NANO-Antivirus	Trojan.Android.Kasandra.edojca
Qihoo-360	Trojan.Android.Gen
Ikarus	Trojan-Spy.AndroidOS.Kasandra
AegisLab	SUSPICIOUS
K7GW	Spyware (004c0dc11)
Babable	Malware.HighConfidence
F-Secure	Malware.ANDROID/Spy.Kasandra.E.Gen
Kaspersky	HEUR:Trojan-Spy.AndroidOS.Sandr.a
ZoneAlarm by Check Point	HEUR:Trojan-Spy.AndroidOS.Sandr.a
Cyren	AndroidOS/Sandr.A.gen!Eldorado
Avast-Mobile	Android:Sandr-D [Trj]
Avast	Android:Agent-QUO [Trj]

Obr. 4.3: Scan vygenerované aplikace z VirusTotal

File identification

MD5	da0f362505436d162c88e78c8bd6293b
SHA1	aba57faa9f5f190a03623f2b3aee06ab7c5d0326
SHA256	272f21b29e5b7cc1c35eefcbe3b5f98febf9bc68ca6077e4dd5d82aa260a8f51
ssdeep	6144:FyWL4oLNHoYbkb4tttghDqsQcYZG70o7ONLpkHX8RIIPlb:0FG1bo4tttg9VaC0o7OpIX8CIp
File size	254.9 KB (260998 bytes)
File type	Android
Magic literal	Zip archive data, at least v2.0 to extract
TrID	Android Package (91.3%) ZIP compressed archive (6.9%) PrintFox/Pagefox bitmap (var. P) (1.7%)
Tags	apk android

Obr. 4.4: Informace o souboru vygenerované aplikace z VirusTotal

Interesting strings

```
http://www.droidjack.net/Access/DJ6.php
http://www.droidjack.net/storeReport.php
```

Obr. 4.5: Souvislost se stránkou www.droidjack.net

APK

30 / 58

30 engines detected this file

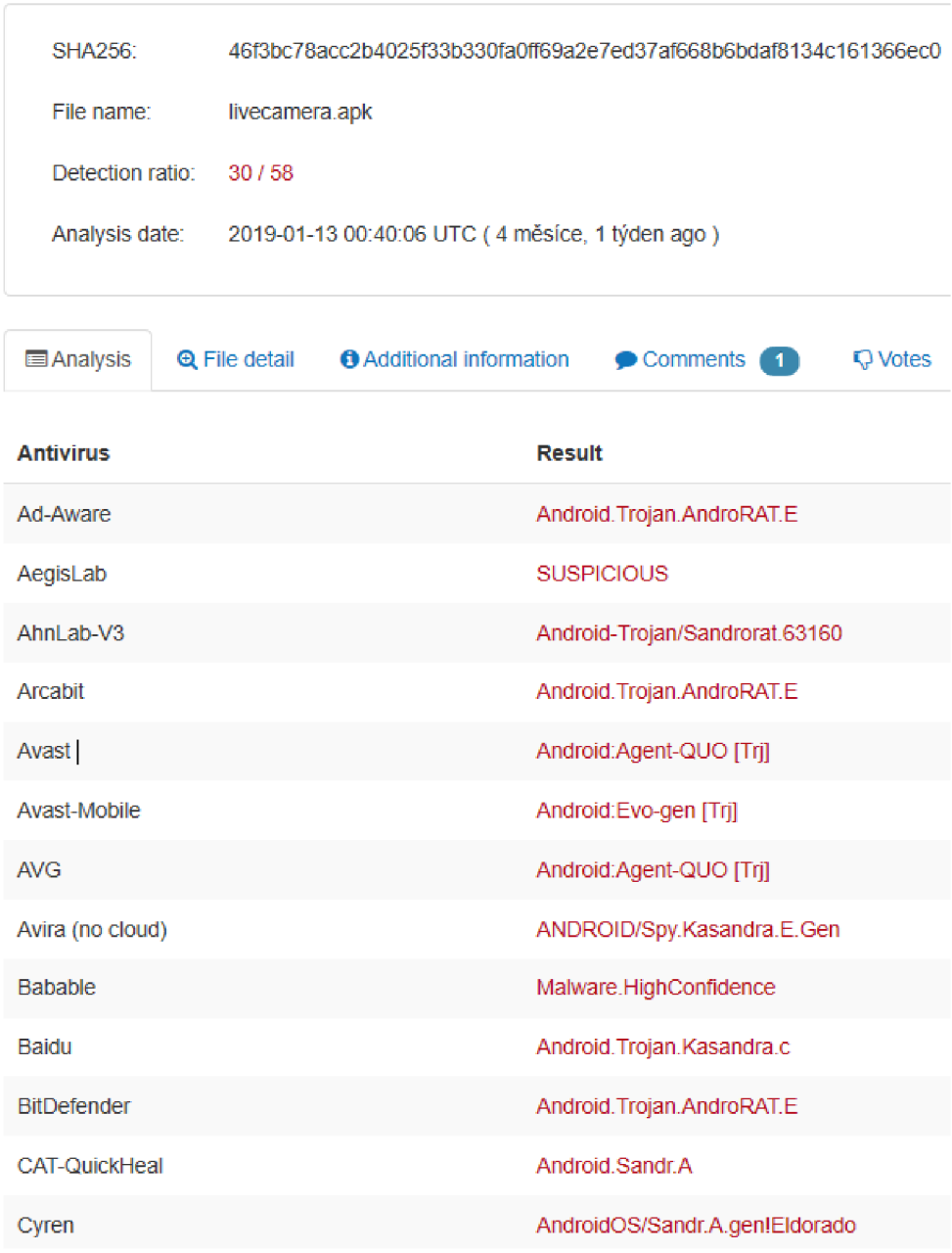
SHA-256	46f3bc78acc2b4025f33b330fa0ff69a2e7ed37af668b6bdaf8134c161366ec0
File name	livecamera.apk
File size	253.3 KB
Last analysis	2019-01-13 00:40:06 UTC
Community score	-27

Detection | Details | Relations | Behavior | Community 1

Basic Properties

MD5	d169cc61fce40d6333c9fb1971446eda
SHA-1	c3b3f5332f14198b2123df00fdba37d6c58012d9
File Type	Android
Magic	Zip archive data, at least v2.0 to extract
SSDeep	6144:kNV0Zc/w0WDpsqR3I6WRNLpRUEHlQCHajDCQ:80iwvp/pIlRJpRUEDHE
TRiD	Android Package (91.3%) ZIP compressed archive (6.9%) PrintFox/Pagefox bitmap (var. P) (1.7%)
File Size	253.3 KB

Obr. 4.6: Informace o souboru livecamera.apk z VirusTotal



SHA256: 46f3bc78acc2b4025f33b330fa0ff69a2e7ed37af668b6bdaf8134c161366ec0

File name: livecamera.apk

Detection ratio: 30 / 58

Analysis date: 2019-01-13 00:40:06 UTC (4 měsíce, 1 týden ago)

Analysis | File detail | Additional information | Comments 1 | Votes

Antivirus	Result
Ad-Aware	Android.Trojan.AndroRAT.E
AegisLab	SUSPICIOUS
AhnLab-V3	Android-Trojan/Sandrorat.63160
Arcabit	Android.Trojan.AndroRAT.E
Avast	Android:Agent-QUO [Trj]
Avast-Mobile	Android:Evo-gen [Trj]
AVG	Android:Agent-QUO [Trj]
Avira (no cloud)	ANDROID/Spy.Kasandra.E.Gen
Babable	Malware.HighConfidence
Baidu	Android.Trojan.Kasandra.c
BitDefender	Android.Trojan.AndroRAT.E
CAT-QuickHeal	Android.Sandr.A
Cyren	AndroidOS/Sandr.A.gen!Eldorado

Obr. 4.7: Scan souboru livecamera.apk z VirusTotal

5 Výsledky simulace

Simulovaný incident měl následující scénář. Útočník vytvořil aplikaci s injectovaným trojským koněm prostřednictvím zajištěného vzorku DroidJack. Uživatel zařízení se systémem Android si tuto aplikaci stáhl do svého zařízení a nainstaloval. Útočník poté vzdáleně ovládal zařízení uživatele Androidu. Protože se jedná o simulaci incidentu a zajištění důkazů v trestním řízení, byl analyzován zajištěný disk útočníka. Postup a výsledky sběru důkazů budou následně popsány.

Pro zajištěný disk útočníka *Windows7_DJ* jsem v hostitelském systému vytvořila otisk pro kontrolu dat. Hash byl vytvořen pomocí nástroje **Total Commander** a pro výpočet byl zvolen algoritmus SHA256. Otisk disku *Windows7_DJ.vdi* je následující:

- 52c39cd9f5cbdd178a048347e0768ba5d18f614040cf5fb6e9e15fed98deda427.

Poté jsem pomocí *WinSCP* nakopírovala disk *Windows7_DJ* do virtuální stanice. Program *WinSCP* je SFTP a FTP klient pro Microsoft Windows. Jeho hlavním účelem je bezpečné kopírování mezi vzdálenými systémy, ale dobře poslouží i pro kopírování mezi hostitelským a hostujícím systémem.

Postup kopírovaní mezi hostitelským a hostujícím systémem je následující: Po otevření programu *WinSCP* se zobrazí okno, kde je potřeba vyplnit protokol, IP adresu systému, ke kterému se připojujeme a číslo portu. Následně ještě uživatelské jméno a heslo. Protokol jsem zvolila **SCP**, IP adresu **192.168.0.178**, číslo portu **22** a uživatelské jméno a heslo **caine**. Po stisknutí tlačítka *Login* dojde k autentizaci a k připojení. Poté je možné mezi oběma souborovými systémy provádět standardní operace jako na hostitelském počítači.

Poté, co jsem disk *Windows7_DJ.vdi* nakopírovala do virtuální stanice Caine, provedla jsem opět kontrolní součet pomocí nástroje *QuickHash* a algoritmu SHA256. Kontrolní součet odpovídal a to znamená, že při kopírování nedošlo k chybě. Následně jsem virtuální disk *Windows7_DJ.vdi* musela převést do formátu **.vmdk**, protože program *Autopsy* formát **.vdi** nepodporuje. K tomu jsem musela doinstalovat utilitu **qemu-img**. Tento nástroj jsem vybrala, protože práce s ním je jednoduchá a převedení disku i instalaci postačí následující dva řádky:

- apt-get install qemu-utils.
- qemu-img convert Windows7_DJ.vdi -O vmdk Windows7_DJ.vmdk

Prvním příkazem se nainstaluje nástroj qemu-utils a druhým se virtuální disk *Windows7_DJ.vdi* převede do formátu *Windows7_DJ.vmdk*. Nyní by už bylo možné disk analyzovat pomocí programu *Autopsy*. Než jsem ale analýzu zahájila, vytvořila jsem nový kontrolní součet opět nástrojem *QuickHash* a algoritmem SHA256 tentokrát pro disk *Windows7_DJ.vmdk*, který je následující:

- 323878CE222AB52ECA65BEC393042602E6151D1D9B312B17147E78810F27

1CD8.

Dále jsem spustila program **Autopsy 4.9.1** a založila nový případ. Do pole *Case Name* jsem vložila **DroidJackv4.4** a pole *Base Directory* jsem ponechala výchozí /. Dále jsem nastavila případ jako nesdílený označením políčka **Single-user**. V dalším okně je možné nastavit číslo případu a informace o vyšetřovateli případu např. jméno, telefonní číslo, email, atd. Jedná se o ukázkový případ, proto jsem do kolonky čísla případu vložila číslo **1** a jméno vyšetřovatele **caine**.

Po vytvoření případu je možné přidat datové zdroje. Zvolila jsem tedy *Add Data Source* a v souborovém adresáři jsem vybrala disk *Windows7_DJ.vmdk* a nastavila časovou zónu na **(GMT+1:00) Europe/Prague**. Zároveň při přidávání datového zdroje je možné vybrat moduly, které budou použity k analýze, např. modul, který extrahuje nedávnou aktivitu uživatele. Moduly je možné dodatečně nastavit, např. přidat slovo **droidjack** do modulu pro vyhledávání klíčových slov. Jakmile je datový zdroj přidán, začne probíhat analýza. Moduly můžeme spouštět i dodatečně a s různým nastavením.

Z analýzy vyplývá, že operační systém byl přihlášen pod uživatelem **student** a že se nedávno pracovalo se soubory **Droidjack.lnk** a **CistaAplikace.apk.lnk** (viz obrázky 5.1 a 5.2. Soubory s příponou *.lnk* jsou v podstatě odkazy na originální spustitelné soubory.

Type	Value	Source(s)
Path	C:\Users\student\Downloads\DJ_samples_04\DroidJack.4.4.Cracked\DroidJack.4.4.Cracked\DroidJack	RecentActivity
Path ID	12975	RecentActivity
Date/Time	2019-05-21 21:00:27	RecentActivity
Source File Pat	/img_Windows7_DJ.vmdk/vol_vol3/Users/student/AppData/Roaming/Microsoft/Windows/Recent/DroidJack.lnk	
Artifact ID	-9223372036854772151	

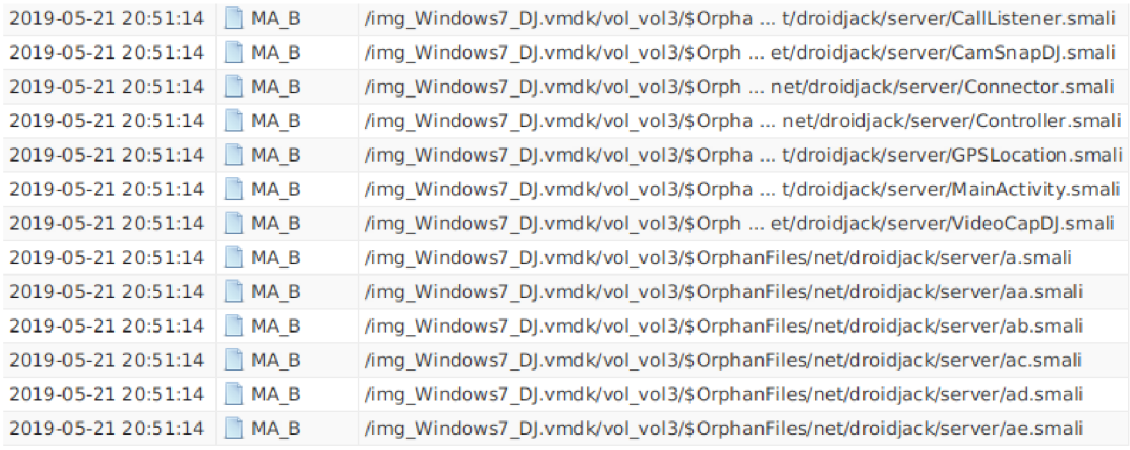
Obr. 5.1: Nedávná aktivita souboru Droidjack

Type	Value	Source(s)
Path	C:\Users\student\Downloads\DJ_samples_04\DroidJack.4.4.Cracked\DroidJack.4.4.Cracked\DroidJack\CistaAplikace.apk	RecentActivity
Path ID	13003	RecentActivity
Date/Time	2019-05-21 21:00:27	RecentActivity
Source File Pat	/img_Windows7_DJ.vmdk/vol_vol3/Users/student/AppData/Roaming/Microsoft/Windows/Recent/CistaAplikace.apk.lnk	
Artifact ID	-9223372036854772152	

Obr. 5.2: Nedávná aktivita souboru CistaAplikace.apk

Pomocí funkce *Timeline*, kdy jsou shromážděny činnosti a zápisy v systému, jsem nalezla aktivitu nástroje DroidJack, která je možná vidět na A.1.

Pro přesné určení jsem v souborovém systému Windows 7 nalezla soubor odpovídající soubor *Droidjack.jar* a extrahovala jej. K tomuto souboru jsem poté vytvořila hash pomocí algoritmu SHA256 a ověřila původ tohoto souboru na VirusTotal. Hash i výpis z VirusTotal (viz obrázek 3.2) odpovídal vzorku popsaném v kapitole 3. V



2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orpha ... t/droidjack/server/CallListener.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orph ... et/droidjack/server/CamSnapDJ.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orph ... net/droidjack/server/Connector.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orpha ... net/droidjack/server/Controller.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orpha ... t/droidjack/server/GPSLocation.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orpha ... t/droidjack/server/MainActivity.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orph ... et/droidjack/server/VideoCapDJ.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/a.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/aa.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/ab.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/ac.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/ad.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/ae.smali

Obr. 5.3: Činnost nástroje DroidJack

adresáři *Droidjack* byl také soubor *CistaAplikace.apk*, který byl podle předchozích výsledků také aktivní. Proto jsem jej opět extrahovala a porovnala na VirusTotal (viz obrázek 4.3. Bylo potvrzeno, že soubor *CistaAplikace.apk* pochází z nástroje DroidJack.

Informace posbírané z disku *Windows7_DJ.vmdk* prostřednictvím navrženého prostředí **Caine** a nástroje **Autopsy** prokazatelně dokazují, že v zařízení byly použity nástroje, které slouží k nelegálním účelům (viz příloha A).

6 Závěr

Splnění hlavního cíle spočívalo ve vytvoření vhodného prostředí k analýze elektronického důkazního materiálu a provedení analýzy jednoho bezpečnostního incidentu v navrženém prostředí. Důležitým faktem je, že analýza musela být provedena tak, aby nebyla narušena integrita originálních dat a musely být použity takové postupy, aby mohla být analýza opakovatelná se stejným výsledkem.

V první části mé práce popisuji problematiku definice elektronického důkazu a jeho zajišťování. Oblast týkající se elektronických důkazů a jejich zajišťování není v českém právním systému dostatečně specifikována. České právo nedisponuje dostatečnou právní úpravou včetně metodiky zajišťování elektronických důkazů.

V další části popisuji analytické prostředky, které lze využít pro zajištění, zkoumání a vyhodnocení elektronických důkazů. K tomu může být použit software, který v mé práci popisuji, avšak nejdůležitějšími jsou právě nástroje pro forenzní analýzu, které umožní bezpečné zajištění elektronického důkazu tak, aby byly splněny podmínky pro použití důkazu v trestním řízení.

V praktické části mé bakalářské práce jsem s pomocí vybraných nástrojů zajistila vzorek malwaru, který naplňuje skutkové podstaty nelegálních činností, a následně jsem jej analyzovala. K zajištění takového vzorku bylo potřeba provést kroky k zajištění vlastní ochrany v kybernetickém prostoru, k čemuž slouží anonymizace uživatele pomocí služeb jako je VPN a Tor. Poté bylo možno samotné prozkoumání webů s ilegálním obsahem včetně návodů k jejich používání. Na zajištěném vzorku jsem provedla analýzu, ze které vyplynulo, že se jedná o extrémně nebezpečný malware, který může být efektivně zneužit i proti chráněnému zařízení. Tento vzorek byl použit v následné simulaci bezpečnostního incidentu. Poté jsem zajistila disk útočníka a s pomocí navrženého prostředí a nástrojů jsem provedla analýzu a sběr důkazů tak, aby splňovaly podmínky použitelnosti v trestním řízení.

Navržené prostředí je podle mého mínění vhodné k zajištění a analýze důkazního materiálu. Prostředí je kromě analýzy malwaru či disku možné využít k analýze řady dalších elektronických důkazů.

Literatura

[1] PINKAVOVÁ, A.: *Používání elektronických důkazů v řízení* [online]. 2014 [cit. 2018-10-19]. Dostupné z URL: <https://www.epravo.cz/top/clanky/pouzivani-elektronickych-dukazu-v-rizeni-95131.html>

[2] PORADA, V.: *Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016.* ISBN 978-80-7380-589-0.

[3] *New Trustwave Report Reveals Criminals Receive 1,425 Percent Return on Investment from Malware Attacks* [online]. 2015 [cit. 2018-11-12]. Dostupné z URL: <https://www.trustwave.com/Company/Newsroom/News/New-Trustwave-Report-Reveals-Criminals-Receive-1,425-Percent-Return-on-Investment-from-Malware-Attacks/>

[4] *Locky Ransomware* [online]. 1. 6. 2016 [cit. 2018-11-12]. Dostupné z URL: <https://www.pcrisk.cz/odstraovaci-piruky/7540-locky-ransomware>

[5] *DDoS – sofistikovaný útok nebo služba na objednávku?* [online]. duben 2015 [cit. 2018-11-12]. Dostupné z URL: <https://www.systemonline.cz/it-security/ddos-sofistikovany-utok-nebo-sluzba-na-objednavku.htm>

[6] OSBORNE, Ch.: *Old banking Trojan TrickBot has been taught new tricks* [online]. 22. 3. 2018 [cit. 2018-11-21]. Dostupné z URL: <https://www.zdnet.com/article/old-trickbot-trojan-taught-new-tricks/>

[7] *Jak odstranit Js Miner* [online]. 6. 10. 2018 [cit. 2018-11-21]. Dostupné z URL: <http://www.2-remove-virus.com/cz/js-miner-odstranit/>

[8] POLČÁK, R., PÚRY, F., HARAŠTA, J.: *Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, 2015.* ISBN 978-80-210-8073-7.

[9] *Subjekty trestního řízení. Nejvyšší státní zastupitelství* [online]. 2012 [cit. 2018-10-29]. Dostupné z URL: <http://www.nsz.cz/index.php/cs/prubeh-rizeni-v-trestnich-a-netrestnich-vecech/subjekty-trestniho-izeni>

[10] *VirtualBox: Technical documentation* [online]. [cit. 2018-12-09]. Dostupné z URL: <https://www.virtualbox.org/>

[11] *CAINE: Computer Forensics Linux Live Distro* [online]. [cit. 2019-05-08]. Dostupné z URL: <https://www.caine-live.net/>

[12] *About. Tails* [online]. 2009 [cit. 2019-05-08]. Dostupné z URL: <https://tails.boum.org/about/index.en.html>

[13] *Autopsy User Documentation* [online]. 2017 [cit. 2018-10-29]. Dostupné z URL: <https://sleuthkit.org/autopsy/docs/user-docs/4.3/>

[14] *CIMPANU, Catalin. NSA releases Ghidra, a free software reverse engineering toolkit. Zero Day* [online]. 6. 3. 2019 [cit. 2019-05-09]. Dostupné z URL: <https://www.zdnet.com/article/nsa-release-ghidra-a-free-software-reverse-engineering-toolkit/>

[15] GRUNDY, B.,J.: *TT Law EnforcTmTnt and ForTnsic ExaminTr's Introduction to Linux: A ComprThTnsivT BTginnTr's GuidT to Linux as a Digital ForTnsic Platform* [online]. Version 4.31. 2017 [cit. 2018-10-29]. Dostupné z URL: <https://linuxleo.com/Docs/linuxintro-LEFE-4.31.pdf>

[16] HOLOVOVÁ, S.: *Virtualizace virtualizačního softwaru. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2018. 52 s. Vedoucí práce: Ing. Tomáš Lieskovan.*

[17] KADLEC, Bc. J.: *Forenzní analýza unixových systému* [online]. Hradec Králové, 2006 [cit. 2018-11-05]. Dostupné z URL: <https://i.iinfo.cz/files/root/k/Digitalni_forensni_analyza_unixovych_systemu.pdf.Diplomovápráce.UniverzitaHradecKrálové,FakultaInformatikyamanagementu,Katedrainformačníchtechnologií.VedoucípráceIng.MiloslavFeltl.>

[18] WRIGHT, C.: *A Step-by-Step introduction to using the AUTOPSY Forensic Browser* [online]. 2009 [cit. 2018-11-07]. Dostupné z URL: <https://digital-forensics.sans.org/blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser>

[19] COOGAN, P.: *DroidJack RAT: A tale of how budding entrepreneurism can turn to cybercrime* [online]. 25. 11. 2014 [cit. 2019-05-19] Dostupné z URL: <https://www.symantec.com/connect/blogs/droidjack-rat-tale-how-budding-entrepreneurism-can-turn-cybercrime>

[20] *DroidJack Uses Side-Load... It's Super Effective! Backdoored Pokemon GO Android App Found* [online]. 7. 6. 2016 [cit. 2019-05-19] Dostupné z URL: <https://www.proofpoint.com/us/threat-insight/post/droidjack-uses-side-load-backdoored-pokemon-go-android-app>

Seznam symbolů, veličin a zkratek

AES	Advanced Encryption Standard (symetrická bloková šifra)
APK	Android application package
Blowfish	Symetrická bloková šifra
CAINE	Computer Aided INvestigative Environment
DES	Data Encryption Standard (symetrická bloková šifra
DHCP	Dynamic Host Configuration Protocol (protokol z rodiny TCP/IP pro automatickou konfiguraci sítě)
DNS	Domain Name System
FTP	File Transfer Protocol
GPL	General Public Licence
GPS	Global Positioning System
HDD	Hard Disk Drive (pevný disk)
IP	Internet Protocol
JAR	Java Archive
NSA	National Security Agency (vládní kryptologická organizace USA)
RAM	Random Access Memory (vyrovnávací paměť počítače)
RAT	Remote Administration Trojan
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SMS	Short Message Service
SRE	Software Reverse Engineering (softwarové reverzní inženýrství)
TCP	Transmission Control Protocol
TŘ	Zákon o trestním řízení soudním (trestní řád) č. 141/1961 Sb., ve znění pozdějších předpisů
Triple DES	Triple Data Encryption Standard (zesílená symetrická bloková šifra)
TZ	Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších
UDP	User Datagram Protocol
USB	Universal Seriál Bus (přenosné úložiště velikosti klíčenky)
WiFi	Wireless Fidelity (komunikační standard pro bezdrátový přenos dat)

Seznam příloh

A Zpráva o bezpečnostním incidentu

Dne 21. 05. 2019 byla na zajištěném disku zaznamenána aktivita ilegálního nástroje DroidJack, který slouží ke vzdálenému ovládání zařízení. Umožňuje generovat klienta pro zařízení se systémem Android, prostřednictvím kterého přebírá plnou moc nad zařízením, ve kterém je klient instalován a je umožněno exportovat veškerá data od systémových aktivit až po citlivé údaje o uživateli zařízení. Dále byl nalezen soubor CistaAplikace.apk, který je právě klientem nástroje DroidJack. Tento klient byl vytvořen na zajištěném disku lokálním uživatelem student.

2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orpha ... t/droidjack/server/CallListener.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orph ... et/droidjack/server/CamSnapDJ.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orph ... net/droidjack/server/Connector.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orpha ... net/droidjack/server/Controller.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orpha ... t/droidjack/server/GPSLocation.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orpha ... t/droidjack/server/MainActivity.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$Orph ... et/droidjack/server/VideoCapDJ.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/a.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/aa.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/ab.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/ac.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/ad.smali
2019-05-21 20:51:14	MA_B	/img_Windows7_DJ.vmdk/vol_vol3/$OrphanFiles/net/droidjack/server/ae.smali

Obr. A.1: Záznam ze zajištěného disku

Activities

net.droidjack.server.MainActivity

net.droidjack.server.CamSnapDJ

net.droidjack.server.VideoCapDJ

Obr. A.2: Aktivity nástroje DroidJack podle VirusTotal

Services

net.droidjack.server.Controller

net.droidjack.server.GPSLocation

net.droidjack.server.Toaster

Obr. A.3: Služby nástroje DroidJack podle VirusTotal

B Obsah přiloženého CD

Na přiloženém CD je uložena elektronická verze této bakalářské práce ve formátu PDF.