VŠB TECHNICKÁ UNIVERZITA OSTRAVA
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Spyware - jeho možnosti a omezení

Spyware - its Use and Limits

Jan Faltýnek

Diplomová práce

Vedoucí práce: prof. Ing. Ivan Zelinka, Ph.D.

Ostrava, 2021

Abstrakt

Práce se zabývá spywarem na počítačovém systému Windows. V této práci je popsána základní struktura a chování takovéhoto programu. Také je zmíněna historie těchto programů a jejich aktuální zástupci, včetně současných statistik. Mimo jiné je rozepsána problematika sociálních sítí a jejich vliv na bezpečnost osobních dat. Hlavní důraz je pak kladen na aplikaci, která má simulovat reálné nasazení a ovládání útočníkem. Na této aplikaci je demonstrováno, kde mohou být slabá místa operačního systému Windows a na co by si uživatelé měli dávat pozor. Aplikace obsahuje funkce, jako je čtení paměti z jiného procesu, keylogger, vytváření snímku obrazovky, kopírování souborů z cílového počítače a další základní prvky spyware. Velká část je pak věnována funkcím diagnostiky systému, jelikož díky tomuto se dá získat mnoho informací o počítači. Výsledná aplikace je pak testována pomocí antivirového programu, zda ji rozpozná jako hrozbu.

Klíčová slova

Spyware; Malware; bezpečnost; Windows; C#; diagnostika

Abstract

This thesis is focused on spyware on Windows computer system. Basic structure and behavior of such a program is described in the thesis. History of these programs and their current representatives including current statistics are also mentioned. Besides others, possible issues with social networks and their influence on personal data safety is written down. The main part of the thesis is an application, which should simulate real deployment and attacker control. It is demonstrated, where weak sides of Windows operating system could be and to what users should pay attention. The application consists of functions as reading of other process memory, keylogger, screenshot creation, files copying from a targeted computer and other elementary spyware features. Important part of the thesis is dedicated to system diagnostics functions, because thanks to this, it is possible to gain a lot of information about a computer. The final application is tested using antivirus program, whether it recognize the application as a threat.

Keywords

Spyware; Malware; security; Windows; C#; diagnostics

Poděkování

Rád bych na tomto místě poděkoval prof. Ing. Ivanovi Zelinkovi, Ph.D., který mi s prací pomáhal.

Obsah

Seznam použitých zkratek a symbolů

API	–	Application Programming Interface
BIOS	–	Basic Input-Output System
BSSID	–	Basic Service Set Identifiers
CD	–	Compact Disc
CD-ROM	–	Compact Disc Read Only Memory
DHCP	–	Dynamic Host Configuration Protocol
DLL	–	Dynamic-Link Library
DNS	–	Domain Name System
DVD	–	Digital Versatile Disc
EULA	–	End User License Agreement
FB	–	Facebook
GPS	–	Global Positioning System
HTML	–	Hyper Text Markup Language
HTTPS	–	Hypertext Transfer Protocol Secure
HW	–	Hardware
IoT	–	Internet of Things
IP	–	Internet Protocol
MAC	–	Media Access Control
MMS	–	Multimedia Messaging Service
NAT	–	Network Address Translation
OS	–	Operační Systém
PDF	–	Portable Document Format
PID	–	Process Identifier
P2P	–	Peer-to-peer
RAM	–	Random Access Memory
SMS	–	Short message service
TCP	–	Transmission Control Protocol
USB	–	Universal Serial Bus

VPN	–	Virtual Private Network
WMI	–	Windows Management Instrumentation
XOR	–	Exclusive Or

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Dnešní doba je ve znamení počítačů. Neexistuje snad odvětví, ve kterém by nebylo potřeba využívat tento vynález. Přináší nám mnoho ulehčení jak v osobním tak i firemním životě. Bez této technologie si už většina z nás ani nedokáže představit život a u mladších generací je tento fakt několikanásobně umocněn.

Je potřeba si však uvědomit, že každá věc, ač byla vynalezena či objevena s těmi nejlepšími úmysly, se dá zneužít. Například oheň, který může sloužit jako zdroj tepla a nezbytná součást k přípravě pokrmu, tak na druhé straně se může stát to, že nám díky němu vyhoří celý dům, nebo shoří celý les. Případně někdo úmyslně založí požár, aby někomu jinému uškodil. Podobně můžeme nahlížet na počítače a nejznámější počítačovou síť – internet. Internet je určitě místo, kde se dá získat nespočet užitečných informací, ale také je to místo, které nás v jistých situacích ohrožuje.

V naprosté drtivé většině případů se bude jednat o ublížení spíše majetkové (finanční), avšak v dnešní době se můžeme už bavit i o fyzickém ublížení a rozhodně o psychickém. Téměř každý dopravní prostředek je ovládán více či méně nějakým elektrickým zařízením. V případě neočekávané chyby to může vést k fatálním následkům. Kdybychom se bavili o záměrném narušení systému proto, aby jiný člověk utrpěl nějaké zranění, tak bychom se nejspíše v dnešní době zaměřili na velmi populární téma, kterým je autonomní vozidlo. Zde si jistě každý dokáže představit situaci, převzetí kontroly neoprávněnou osobou nad takovýmto vozidlem, která by vedla ke zranění. Ale to jsou problémy nejspíše následujícího desetiletí.

Psychická újma je rozhodně téma, které je již aktuální a týká se také samotné podstaty této práce. Nejčastěji je spojena s kyberšikanou [3] a ta se dotýká dětí. Případně si děti mohou brát špatně to, že nemají na sociálních sítích takovou pozornost, jakou by si přály. Když už se náhodou s těmito problémy svěří rodičům, tak ti jim mnohdy nedokážou pomoct, jelikož se sami s tímto problémem nikdy nesetkali. Důvod, proč se tato problematiky týká také této práce, je to, že předmětem těchto "vtípků" může být obrázek či text, který měl být soukromý, ale nějakým způsobem, ať už to špatnou bezpečnostní politikou, nebo chybnou důvěrou v další osobu, se dostal do rukou někoho jiného.

Jak již bylo řečeno, nejběžnějším ohrožením, které můžeme čekat od digitálního světa, je materiální ztráta. Ať už nám někdo znemožní práci na daném počítačovém systému, nebo nám ukradne citlivá data.

Tato práce vznikla ze dvou důvodů. V kontextu současné situace bezpečnostních útoků práce poukazuje na běžné problémy s bezpečnostní, které se týkají uživatelských dat. Vysvětluje základní principy škodlivého kódu, tak aby je pochopil i člověk, který není z bezpečnostního oboru a podpořil tak kritické myšlení nad daným tématem. Druhý důvod je pak ukázka toho, jak se dají získat určitá data z operačního systému Windows, což by mělo pomoct budoucím studentům bezpečnostního oboru, aby věděli, na které části systému se mohou zaměřit, aby vylepšili jejich ochranu, případně aby více analyzovali zmíněný problém.

V kapitole Spyware bude zmíněno, jak se dělí tento škodlivý software, jak se šíří, jeho stručná historie, funkcionalita a jak postupovat, abychom se nestali snadným cílem. Také zde bude zmíněn aktuální stav spyware a jeho typičtí zástupci. V další části se řeší problém bezpečnosti osobních dat v rámci moderních technologií a sociálních sítí. Praktickou částí je pak aplikace, ve které jsou ukázaný všechny základní techniky spywaru.

Kapitola 2

Malware

Jedná se o složeninu dvou anglických slov, malicious (škodlivý) a software, kterou se označují programy, které mají za úkol [1] upravovat chování operačního systému, aby útočník mohl získat například přístup k danému systému, ukrást data, případně znepřístupnit data a služby. Většina těchto programů se snaží být co nejvíce nenápadná a ideálně vůbec nedetekovatelná, aby oběť neměla ponětí, že se něco děje a tím pádem nijak nereagovala na vzniklý problém.

Malware se může dělit podle svého zaměření na několik kategorií (Adware, Počítačový červ, Ransomware, Rootkit, Spyware, Trojský kůň, Vir), avšak v dnešní době se málo kdy setkáme s tím, že škodlivý kód obsahuje čistě jen jednu kategorii. Většinou se skládá z kombinací těchto typů, proto se raději označují souhrnně jako malware. Důvod proč se ještě objeví programy, které obsahují právě jednu zmíněnou kategorii, je nejčastěji ten, že takto psané programy mohou být méně nápadné pro antivirové společnosti.

2.1 Adware

Jedná se o programy, které nemají většinou přímo ublížit cíli (jestliže nejsou kombinovány například se spywerem), jelikož mají za následek to, že uživatel uvidí nevyžádanou formou reklamy, například jako pop-up okno, nebo otevření konkrétní webové stránky. Tohle je pro většinu uživatelů nepříjemné vyrušení od jejich běžné činnosti, ale jinou újmu z toho nemají, když se bavíme o PC, avšak na mobilních zařízeních to může být úplně něco jiného, jelikož starší stroje to bude výrazně zpomalovat.

2.2 Počítačový červ

Nepotřebují ke spuštění jiný program, do kterého by se uložili jako počítačový virus. Vyznačují se tím, že se šíří prostřednictvím sítě. V okamžiku, kdy je jeden počítač napaden, snaží se dostat dál. V minulosti se tak dělo hlavně na základě e-mailů, které byly rozeslány všem kontaktům v napade-

ném počítači. Proto dochází k zahlcení sítě a to je i identifikátorem toho, že dané počítače mohou být napadeny.

2.3 Ransomware

Jedná se o velmi populární škodlivý software, který cílí na důležitá data v počítači, které pak zašifruje. Následně se ve většině případů objeví zpráva, že byly zašifrované data a pokud chceme klíč, musíme poslat určitý obnos peněz (nejčastěji v podobě nějaké kryptoměny). Poté by měl přijít zmíněný klíč, který zpřístupní ztracené data. Existuje nemálo případů, kdy se oběti i po zaplacení nedočkaly obnovy ztracených souborů, proto je nezbytné si zálohovat důležité soubory.

2.4 Rootkit

Tyto programy slouží k tomu, aby zamaskovaly to, že na daném systému se nachází nějaký virus či spyware. Mění chování operačního systému tak, aby uživatel nebo antivirus nebyl schopen odhalit přítomnost malwaru. Samy o sobě nejsou škodlivé, ale připravují půdu pro další hrozby.

2.5 Spyware

Jsou to programy, které sbírají data od uživatelů, které jsou následně nejčastěji pomocí internetu zaslány zpět ke zdroji. Cílem může být třeba nastavení počítače, což slouží jako počáteční informace pro budoucí sofistikovanější útok, případně vytipování oběti. Mnohem častěji spyware míří na osobní informace, jako jsou hesla a čísla platebních karet. Do této kategorie lze řadit i keylogger, což je program, který zaznamenává stisky kláves, ve kterých se následně nejčastěji hledají uživatelská jména a hesla. Podrobněji bude popsán spyware v následující kapitole.

2.6 Trojský kůň

Je to typ malware, který se maskuje tím, že je součástí nějakého užitečného programu, který opravdu využijeme. Tento typ si proto nejčastěji samotní uživatelé dobrovolně nainstalují, ale nemají ponětí, že daná aplikace dělá další věci, které si nepřejí, jako například otvírání síťových portů.

2.7 Vir

Počítačové viry jsou programy, které se připojí k existujícímu spustitelnému souboru, tohle se stane po otevření již infikovaného souboru či dokumentu. Díky tomuto chování se může schovat na více místech v počítači, nebo se jen přesouvat z jednoho souboru do druhého. Chování tohoto viru

zůstane nejspíše stejné, takže jestli jej jednou detekoval antivir, tak by měl být schopen projít zbylé programy a označit ty, které slouží jako hostitelské.

Kapitola 3

Spyware

Opět se jedná o složeninu dvou anglických slov, spy (špion) a software. Jak již bylo zmíněno, tento malware slouží k tomu, aby sbíral data uživatelů. Počítačová data jsou podle Úmluvy o počítačové kriminalitě [1], která byla uzavřena 23. listopadu 2001, definovány takto: "počítačová data znamenají jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem"[4]. Útočníci hlavně cílí na data, které pro ně mají nějakou hodnotu, primárně to jsou přihlašovací údaje a informace o kreditních kartách, ale také to mohou být plány výrobků, nebo firemní citlivá data.

Spyware tedy jako takový neovlivní chod systému tím způsobem, že by se začal chovat nepředvídatelně a nebylo možné na daném systému pracovat, ale snaží se nás ve výsledku materiálně okrást. Je důležité vnímat tento typ malwaru jako velkou hrozbu pro firmy, stejně jako je vnímán ransomware a útoky zaměřené na odstavení služeb (Denial of service attack [1]) poskytovatele.

3.1 Historie

V říjnu 1995 se pojem "spyware" poprvé objevil na veřejném fóru s názvem Usenet [9], což byla distribuovaná internetová diskuse, kde uživatelé posílali zprávy ve stylu připomínající e-mail. Tento název se objevil v článku, který analyzoval obchodní model. Následně tento pojem přebrala společnost Microsoft.

Veřejnost se poprvé významně setkala s tímto pojmem v roce 1999, kdy byl objeven dodatečný software v populární freewarové hře Elf Bowling [24], který získával informace od uživatelů. Ve stejném roce Steve Gibson [9] z Gibson Research objevil formu spywaru, který se tvářil jako reklama, ale ve skutečnosti okrádal uživatelé o důvěrné informace. Z tohoto historického důvodů se často řádí mezi spyware i adware, který úplně nesplňuje podmínku toho, že vždy sleduje nějakým způsobem uživatele. V reakci na to Gibson vyvinul OptOut [7], první anti-spywarový program.

Podle studie [9] AOL a Národní aliance pro kybernetickou bezpečnost z listopadu 2004 bylo 80 % počítačů nakaženo nějakou formu spywaru. 89 % dotazovaných uživatelů uvedlo, že nevěděli o jeho přítomnosti.

Od roku 2006 se spyware stal jednou z hlavních bezpečnostních hrozeb pro počítačové systémy s operačními systémy Microsoft Windows. Podle průzkumu [9], založeném na datovém logu zákazníku společnosti Webroot Software, se zjistilo, že je infikováno 9 z 10 počítačů připojených k internetu. Počítače, kde byl výchozím prohlížečem Internet Explorer, byly vůči těmto útokům zranitelné, protože jeho těsná integrace s Windows umožňovala přístup spywaru k důležitým částem operačního systému.

3.1.1 Významný spyware historie

Za relativně krátkou dobu existence programů, které kradou uživatelské data, se do historie nechvalně zapsalo již několik zástupců. Mnoho z nich je tu stále, jelikož jejich úkol přetrvává pořád, jen je museli útočníci přepsat do novějších počítačových jazyků, případně pozměnit jejich strukturu, aby byly tyto programy sofistikovanější a mohly se lépe schovávat před moderními metodami antivirových společností.

3.1.1.1 CoolWebSearch

Je to velmi známý nežádoucí program [10], který se zapsal do historie kybernetické bezpečnosti. Objevil se v roce 2003. Jedná se o malware typu hijacker [8], tedy nějakým způsobem modifikuje chování webového prohlížeče. Mířil jak na prohlížeč Internet Explorer, tak také Google Chrom. Jeho primárním cílem bylo přesměrovat všechna vyhledávání na Coolwebsearch.com nebo na jiné pochybné stránky, avšak zároveň kradl i citlivá data. Nebezpečný program už byl vydán v několika různých verzích (přesněji 107), všechny používají jiný kód, ale chovají se velmi podobně. Nejvíce ohrožoval kybernetický svět v roce 2005, kdy jim bylo nakaženo více než 8 % počítačů po celém světě.

3.1.1.2 DyFuCa

Jedná se o malware [12], který se skládá ze dvou částí, které jsou downloader a doplněk do prohlížeče. Při návštěvě infikované stránky se instalují bez souhlasu uživatele a umožňují spuštění ovládacích prvků ActiveX [23]. Program také přesměrovává webové stránky na jiné, tak aby z toho měl někdo třetí prospěch. V internetovém prohlížeči začnou vyskakovat obtěžující reklamy a pomoci aplikace Outlook rozpošle různé e-maily. Downloader stáhne následně do počítače keylogger. DyFuCa je také známý jako Internet Optimizer.

3.1.1.3 Morpheus

Morpheus [11] byl program pro sdílení a vyhledávání souborů přes P2P síť v operačním systému Microsoft Windows, vyvinutý a distribuovaný společností StreamCast. Morpheus byl vydán v několika verzích v letech 2001 až 2007. Jeho pravidelnou součástí byl spyware, který získával data uživatelů, za což byl kritizován analytiky.

3.1.1.4 Look2Me

Look2Me [13] program pracuje na pozadí a zobrazuje nadměrné množství vyskakovacích reklam. Nejvíce tímto malwarem trpěl Internet Expolrer. Některé reklamy nabádaly uživatele k instalaci WinFixer [13], což byl antivirový program. K odstranění Look2Me je potřeba speciální nástroj. Look2Me infikuje pouze Windows 2000, XP a 2003.

3.2 Současnost

Díky Koronavirové krizi [22] ve světě bylo potřeba přesunout mnoho zaměstnanců z kanceláří do jejich domovů. To mělo za následek, že vzniklo mnoho prostoru pro potencionální bezpečnostní díry, kterých se snažili útočníci využít. Tento trend neunikl bezpečnostním analytikům, kteří vypozorovali větší nárůst útoků.

Na základě výzkumu společnosti IBM, kterého se účastnilo 524 organizací, byl vypracován tento dokument [53], který popisuje bezpečnostní situaci v roce 2020. Tyto organizace byly cílem útoku, který vedl ke krádeži dat. Byly ze 17 různých odvětví průmyslu a stejně tak ze 17 různých zemí. Vyčíslená průměrná ztráta díky takovému útoku byla necelé 4 milióny $. Nejpostiženějším odvětvím bylo zdravotnictví a nejpostiženějším státem byly Spojené státy americké. Průměrná doba potřebná pro odhalení a nápravu způsobených škod byla 280 dní. Za 52 % těchto útoků mohl nějaký malware, ve 23 % případů za únik dat mohla lidská chyba a ve zbylých 25 % se jednalo o systémovou chybu. V 19 % případů mohl být tento útok proveden, jelikož došlo k odcizení přihlašovacích údajů. Dalších 19 % pak bylo provedeno na základě špatného nastavení Cloudového [30] úložiště. Velké zastoupení (16 %) pak měly chyby v aplikacích třetích stran. 53 % těchto útoků bylo motivováno finančním ziskem.

Společnost Varonis zveřejnila vlastní "Data Risk Report"[54]. Jejich cílová skupina byl finanční a bankovní sektor. Do statistik bylo zařazeno 56 různých organizací. Podle tohoto průzkumu má v průměru každý zaměstnanec firmy přístup k 11 miliónům souborů. Téměř dvě třetiny firem mají více jak 1000 citlivých dokumentů přístupných každému zaměstnanci. Součástí práce je i analýza toho, jaké množství a typů souborů vychází na jeden terabyte dat. Pro střední firmy (500 - 1500 zaměstnanců) je to 1,5 miliónů souborů a z toho je 12 tisíc souborů citlivého charakteru. Složek, které mají restrikce pro přístup, je pak 9,5 tisíc. Všechny tyto čísla jsou průměrný výsledek.

Tabulka 3.1: Tabulka spyware hrozeb v roce 2020 v České Republice

Pořadí	Jméno
1.	MSIL/Spy.Agent.AES trojan
2.	Win32/PSW.Fareit trojan
3.	Win32/Formbook trojan
4.	MSIL/Autorun.Spy.Agent.DF worm
5.	MSIL/Spy.Agent.CTW trojan

V roce 2016 byly ukradeny data uživatelů společnosti Uber [34]. Ta přišla s oficiálním vyjádřením až rok poté a ujišťovala své klienty, že již udělala vše proto, aby k takovému incidentu nikdy nedošlo a snažila se kompenzovat možné ztráty. Bylo zveřejněno přes 57 miliónů záznamů uživatelů. Společnost uklidňovala své klienty, že byly odcizeny jen jména, telefonní čísla a e-mailové adresy, že nemusí mít strach o své bankovní účty. Tohle je ukázka toho, že zabezpečení firem někdy nemusí být dostatečné a přestože uživatel plní veškeré zásady bezpečného chování v kyberprostoru, tak samotná bezpečnost aplikace na úrovní databáze, kterou samotný uživatel nemá vůbec ve své moci, selže.

Tabulka 3.1 znázorňuje pět největších hrozeb v České Republice ke konci roku 2020, které nějakým způsobem kradly data českých uživatelů. Data [35] byly poskytnuty společností Eset.

3.2.1 Aktuální zástupci ohrožující uživatele

3.2.1.1 CopperStealer

Nový spyware [16], který nepřichází s žádnou inovativní změnou ve svém odvětví. Jen poukazuje na trend, že se snaží útočníci nachytat uživatele, kteří se nějakým způsobem snaží ušetřit na nakupování her od oficiálních distributorů a raději hledají neoficiální aktivační klíče. Výskyt této aplikace byl právě zaznamenán na takovýchto stránkách.

3.2.1.2 FickerStealer

Je to [16] další případ aplikace, která se snaží odcizit přihlašovací údaje od uživatele. Jelikož již byla známá, tak změnila svůj způsob infikace a to tak, že se nyní tváří jako instalační soubor hry, takže domnělí hráči, kteří si mysleli, že ušetří nějaké peníze, nakonec mohou přijít o ještě větší obnos.

3.2.1.3 Fureball

První varianta [16] se objevila v roce 2017, ale nyní přichází s novou formou napadení a to je pomocí SMS, když v ní je odkaz na infikovanou stránku. Jeho cílem jsou data uživatele.

3.2.1.4 Ramnit

Objevuje [14] se již od roku 2010. Existuje ve více variantách – Virus, Trojský kůň, Červ. První verze tohoto programu infikovaly Exe, DLL a HTML soubory na počítači. Pozdější varianty už obsahovaly funkce, které sloužily k odcizení dat z napadeného počítače. Může se vyskytovat i ve variantě, kdy je součástí botnetu [17]. V roce 2015 na rozsáhlou síť nakažených počítačů reagoval Europol, který jej citelně oslabil.

3.2.1.5 RedLineStealer

Jedná se o relativně nový spyware [16], který byl zachycen počátkem roku 2020. Zaměřuje se na kradení hesel a přihlašovacích údajů včetně těch na kryptoměny. Pravidelně zasílá informace o napadeném počítači.

3.2.1.6 Remote Admin Tool (RAT)

RAT [16] byl v posledních měsících mířen primárně na uživatele v Anglii a Americe, jak uvádí společnost Symantec. Obsahuje komponentu, která zachytává stisky kláves a umí vytvářet snímky obrazovky. Je možné ho ovládat na dálku pomocí příkazů. Umožňuje také spustit a ukončit procesy na daném zařízení.

3.2.1.7 Xcsset

Tento spyware [16] je zvláštní v tom, že se zaměřuje hlavně na uživatele, kteří využívají zařízení s MacOS. Je však schopný se spustit i v jiné verzi na systému Windows.

3.2.1.8 Zbot

Je [15] typicky distribuován za pomocí e-mailové pošty, kdy je přibalen jako příloha. Další cestou jak může být nakažen počítač tímto spywarem je ten, když se navštíví specifický odkaz, který zapříčiní stažení Zbotu do systému. Primárně se zaměřuje na krádež kreditních čísel, které jsou vyplňovány na internetu, včetně jejich ověřovacích kódů. V roce 2011 unikly zdrojové kódy a ostatní útočníci toho zneužili a kusy kódu využili k vytvoření vlastní napodobeniny Zbotu. Další verze Zbotu následně vytvářely botnet [17], který byl znám jako GameOverZeuS. Tento botnet byl dále využíván k šíření aplikací, které kradly uživatelské účty k bankovnictví. Měl i omezené možnosti vzdáleného přístupu v podobě spouštění již nainstalovaných aplikací, případně aktualizací sebe sama.

3.2.1.9 Další

Jednou z dalších hrozeb, na kterou společnost Symantec upozorňuje tyto měsíce, je podvodný e-mail [16], který obsahuje přílohu "Covid-19 reports.iso". Existuje ve třech jazykových variantách

(angličtina, korejština, vietnamština). Další hrozby, které se vyskytovaly v posledních měsících, jsou BlackNET Remote Access Trojan [16] a IcedID [16].

3.2.2 Legální placený spyware

Existují firmy, které programují aplikace, které mají monitorovat oficiálním způsobem počítače. To může vyžadovat například nějaká organizace, aby věděla, co jejich zaměstnanci provádí na počítačích, ovšem tento fakt musí být jasně zmíněn v pracovní smlouvě.

3.2.2.1 FinFisher (FinSpy)

Jedním takovým veřejně známým zástupcem je právě tento spyware [18]. Je dostupný pro všechny desktopové i mobilní systémy. Jeho cílem je dostat se k datům na daném zařízení a monitorovat, co se na něm děje.

3.2.2.2 Společnost Cellebrite

Jedná se o společnost [19], která dodává bezpečnostním složkám některých zemí software, který má za úkol obcházet bezpečnostní opatření. Tyto nástroje slouží například k získávání dat z uzamknutých telefonů, když mají policisté oprávnění k tomuto úkonu.

3.2.3 Kali Linux

Je to open-source operační systém [20], který je vyvíjen pro bezpečnostní analytiky. Obsahuje řadu nástrojů, které dopomáhají k testování jiných systémů a aplikací. Je to ideální bezplatný vstup do světa bezpečnosti, který si může každý osahat. Jsou zde programy, které mohou sloužit právě taky jako jednoduchá ukázka síly aplikací, kterými mohou útočníci disponovat. K většině aplikací je i dokumentace, takže to ulehčí první kroky s tímto systémem. Jelikož je to dobře známý systém, tak mnoho antivirových společností mají většinu těchto aplikací na svém seznamu a automaticky je blokují, když můžou.

Pro základní testování sítě je tu například Nmap [21] nebo Wireshark [21]. Metasploit Framework [21] se dá pak třeba využít k základním možnostem získávání informací z daného zařízení, ale umí toho mnohem víc.

3.3 Dělení spywaru

Je několik kategorií [1] [9] [24], do kterých lze spyware rozdělit. Úplně to nejzákladnější dělení je na softwarový a hardwarový. Mezi hardwarový se řadí takové elektronické produkty, které slouží ke sběru dat nebo k odposlouchávání cíle. Tady spadají věcí pro pořizování multimediálních záznamů, ovšem za podmínky, že jsou nelegálně využívány k pořizování nahrávek, které slouží ke špe-

hování jiné osoby. Dalším zástupcem mohou být zařízení podobné datovým rozbočovačům, které se umístí přímo u zdroje dat (například před router v domácí síti) a jelikož tímto zařízením následně prochází veškerá komunikace, tak si útočník může procházet uživatelská data, která nebyla šifrována. Existuje celá řada těchto elektronických vychytávek, které se musí patřičně vložit mezi zdroj a cíl. Velkou nevýhodou těchto zařízení je to, že se útočník musí dostat fyzicky ke své oběti. Oproti tomu softwarový spyware je pro útočníka mnohem snadnější na nasazení do zařízení oběti, jelikož to může udělat z jakéhokoliv místa na světě. Zde spadají počítačové programy. Dalším kritériem pro dělení je jejich chování, případně jaký způsob využívají ke sběru dat.

3.3.1 Systémové monitory

Tento typ spywaru se nainstaluje tajně nebo jako tajná část jinak legitimně vypadajícího bezpečného softwaru. Slouží k tomu, aby zaznamenávaly aktivitu uživatele, jako je vyhledávání na internetu, instalované programy, uložené kreditní karty a hesla, ale také vykonaná práce na daném zařízení. Vyhledávají e-mailové kontakty a jejich korespondenci. Významných osobních dat se na každém počítači nachází víc, než si člověk může uvědomovat.

3.3.2 Keylloger

Další kategorií jsou programy, které slouží k tomu, aby zaznamenávaly veškeré stisky kláves uživatelem. Útočník předpokládá, že se zde budou nacházet důležité informace jako je například heslo. Nad těmito daty musí být provedena analýza (velikost takto získaných dat může být až v desítkách MB, což na čistě textové dokumenty je už velký obsah textu), která následně lépe odhalí, zda se zde nacházejí užitečné informace pro útočníka. Tento typ spyware musí být přítomen v systému co nejdelší dobu, aby mohl nasbírat co nejvíce adekvátních dat, takže se útočník snaží, aby byl program co nejméně nápadný.

3.3.3 Cookies Spyware

Cookies [25] jsou soubory uchovávané internetovým prohlížečem, aby se zde ukládaly data vztahující se k jednotlivým webovým stránkám. Mohou obsahovat osobní informace včetně hesel, proto existuje spyware vyloženě zaměřený na tento konkrétní typ dat. Tento typ by se dal zařadit do systémového monitoringu, avšak mnohé statistky jej již uvádějí samostatně.

3.3.4 Adware

Jak již bylo uvedeno, z historických důvodů mnoho autorů jako jednu z možných variant uvádějí Adware, což jsou programy, které obtěžují uživatelé tím, že mu zobrazují reklamy. Dalším důvodem, proč jsou zde občas zařazeny, je ten, že využívají neoprávněně cookies prohlížeče, aby mohly ukazovat cílenou reklamu.

3.3.5 Mobile Spyware

Opět by se tento typ spyware mohl řadit do kategorie systémový monitoring, jelikož se jedná o programy, které získávají data z operačního systému mobilních zařízení, avšak tyto data se liší oproti počítačovým, jelikož obsahují GPS souřadnice a další podobné informace, které může mobilní zařízení získávat oproti počítači. Také možnost šíření pomocí SMS a MMS odděluje tyto typy od běžných monitorovacích aplikací.

3.4 Infikace

Způsobů, jak se může dostat do systémů spyware, je mnoho [1] a jsou stejné i pro všechny ostatní typy malware, proto je i prevence téměř identická proti všem škodlivým aplikacím.

3.4.1 Přenosná paměťová media

Tento typ přenosu je z historického hlediska nejstarším možným, kdy pomocí disket se mohly přenášet škodlivé programy a následně spouštět. Podobně jako diskety, tak v dnešní době už i CD jsou historií. DVD na tom začíná být podobně, jelikož stolní počítače si sice stále uchovávají DVD mechaniku, ale firmy začaly vyrábět notebooky ve velkém právě bez těchto mechanik, aby ušetřily místo a tímto i celkovou hmotnost zařízení.

Co zůstává a určitě brzy nevymizí, jsou USB disky a externí disky. Na nich se mohou nacházet infikované soubory a ty si pak můžeme nakopírovat sami do počítače. Za nakažení tímto způsobem si mohou většinou uživatelé sami, jelikož je to z nepozornosti nebo nedostatečné kontrole přenosového média. Je velmi ojedinělé, aby se útočník dostal fyzicky k počítači, kdyby to však nastalo a chtěl využít spyware, tak raději udělá bitovou kopii harddisku. Ovšem v dnešní době Cloudových služeb [30] už ani toto nemusí být účinný útok, jelikož data, která by mohla útočníka zajímat, nemusí být vůbec přítomna na harddisku počítače.

3.4.2 E-mail

Jedna z velmi oblíbených metod útočníků, jak šířit malware. Úplně nejtriviálnější způsob je, že příloha je nakažený soubor, který se může tvářit jako PDF dokument, který nás může svým názvem (vyplaty2020) lákat k nahlídnutí a tím se spustí. Samotný e-mail může obsahovat skript, který se vykoná v prostředí internetového prohlížeče. Běžnou praxí jsou internetové odkazy, které nás mohou přesměrovat na jinou stránku, která bude obsahovat další hrozby.

3.4.3 Kancelářské dokumenty

Balík Office pro kancelářskou práci od společnosti Microsoft je mocný nástroj, ale také tím jak moc je pokročilý, může přinášet nebezpečí. Je možné pomocí jeho maker [31] dělat omezené operace

nad počítačem, ale i to stačí, aby se mohl proměnit ve zbraň. To samé platí o PDF souborech, které mohou být také hrozbou.

3.4.4 Stažením z internetu

Zde je potřeba si definovat pojem internet - "Technicky se jedná o celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem." [1]. Internet je obrovským zdrojem dat, takže je jasné, že zde bude existovat velké množství hrozeb.

Počátky internetu se datují k projektu ARPANET [32], což byl projekt sponzorovaný americkou armádou, aby mezi sebou mohly na větší vzdálenost komunikovat počítače bez centrálního řízení. Technické možnosti nedovolovaly v té době tak obrovské přenosy dat jako dnešní moderní technologie, takže při návrhu se s tím počítalo, že je potřeba šetřit prostředky (výpočetní i přenosové) kde se dá, proto šla hodně bezpečnost stranou a o šifrování se nemělo ani smysl bavit. Bohužel nyní se musíme potýkat s tím, že nebylo všechno ideálně navrženo, odhalené chyby řešili lidé záplatami, a proto se zde objevuje mnoho bezpečnostních zranitelností. Ale tímto problémem trpí i projekty, které mají pětiletou životnost, natož takový který má 50 let historie za sebou.

Při prohlížení webových stránek [56] se uživatel vystavuje nebezpečí. Existuje mnoho adres, které lákají svým obsahem. Nejčastěji to jsou stránky, které nabízejí ke zhlédnutí fotky, videa a hudbu. Při navštívení takovéto stránky musíme být na pozoru a ideálně se takovým, které vypadají dost pochybně, vyhnout. Tyto stránky mohou vydělávat z reklam, ale klidně mohou obsahovat skripty, které se spustí při navštívení stránky. V lepším případě budou obsahovat kód, který bude jen využívat výpočetní zdroje počítače pro těžení kryptoměny, v tom horším to bude kód, který se bude pokoušet způsobit finanční škody.

Avšak i webová stránka, kterou provozuje poctivý člověk a nemá žádné zlé úmysly, může představovat riziko. Technologie se dostaly opravdu daleko, a proto už je možné naprogramovat neuvěřitelné webové aplikace, avšak mnohdy je hodně kladen důraz na rychlost a tohle ve většině případů odskáče bezpečnost. Při vývoji se můžou využívat aplikace třetích stran (tohle platí nejen pro webové aplikace, ale i pro běžné programy na operačním systému), které mohou obsahovat neplánovanou či záměrnou chybu. Naprostým symbolem těchto problémů byl v minulosti Adobe Flash Player [33]. Dalším častým problémem je neadekvátní udržování aktualizací webu samotného, což vede ke vzniku bezpečnostních děr.

Nejběžnějším způsobem nákazy je to, že si malware uživatel sám stáhne. Myslí si, že stahuje program, který mu bude například přehrávat hudbu, ale po instalaci zjistí, že se nic takového neděje a jeho počítač se začal chovat podivně. Tady je alespoň patrné, že je zle a je s tím potřeba něco dělat. Sofistikovanější malware, v podobě trojského koně, by opravdu přehrál hudbu a uživatel by neměl nejmenší ponětí, že daný program mu zároveň doluje důležité informace z počítače.

Tohle vše byly nelegální způsoby. Ovšem smutnou pravdou je, že těžit informace o počítači a uživateli jde i do značné míry legálně a to při souhlasu uživatele s EULA (End-User-License-Agreement)[2]. Jedná se o druh licence pro uživatele software, se kterou musí souhlasit, aby daný produkt mohli využívat. Píše se zde o tom, jak uživatel může s daným programem nakládat, ale mimo to se zde mohou objevit kapitoly, které upozorňují, že při souhlasu s touto licencí bude software zasahovat nějakým způsobem do vašeho soukromí. Většinou je to nějak zaobaleno tím, že to potřebují pro statistické účely.

Většina lidí naprosto ignoruje EULA podmínky a nezajímá se o tyto informace, pak se však diví, že daná firma o nich ví víc, než by si přáli. Na druhou stranu lidé nemají moc na výběr, když chtějí daný produkt využívat. Tohle je i případ technologického giganta Google. Jejich smluvní podmínky [1] v rámci EULA jsou místy alarmující, ale uživateli nezbývá, než je přijmout.

3.5 Prevence

Nejdůležitějším pravidlem je to, aby uživatel měl vždy aktuální verze všech aplikací a samotného operačního systému. Nové chyby se objevují denně a s těmi je spojen Zero day attack [2], což je typ útoků, kdy útočník odhalí bezpečnostní chybu v aplikaci, která je již nasazena. Taková to chyba se může nacházet i roky v počítačovém kódu, když si jí pak firma všimne, snaží se ji opravit a nasazení proběhne pomocí aktualizace. Některé firmy se zpožděním popisují nalezené chyby, ovšem tohle může sloužit jako manuál pro útočníka, jestliže cílí na počítač, který nemá právě aplikovanou tuhle aktualizaci.

Druhým důležitým bodem je antivirus, popřípadě anti-spyware, bezpečnostní společnosti je již nabízejí většinou jako jeden kompletní balíček. V rámci operačního systému Windows 8.1 (nejnižší podporovaná verze systému od společnosti Microsoft v současnosti [5]) a výš je nainstalovaný Microsoft Defender, což je základní bezpečnostní prvek, ovšem vyplatí se investovat do antiviru od společnosti (ESET, Avast, Kaspersky atd.), která se primárně zaměřuje na bezpečnost. Mít však více než jeden antivir těchto společností na jednom počítači se nedoporučuje. Často se navzájem omezují a tím se jejich účinnost velmi snižuje.

Určitě je tedy nezbytné to, aby se uživatel počítače choval obezřetně a to ne jen, když si prohlíží webové stránky na internetu. Měl by si pozorně číst hlášky, kterými ho může operační systém varovat před možným napadením.

Využíváním webové stránky VirusTotal [49], což je webová stránka, která umožňuje nahrát soubor, který je pak prověřen pomocí několika antivirů od různých bezpečnostních firem. Následně je ukázán výsledek, jak vyhodnotil daný soubor každý antivirus a uživatel si podle toho může udělat svůj názor. Když je soubor označen jako škodlivý, tak je zde možnost dohledat další informace, které objasňují, proč byl označen jako malware. Velmi užitečná je také utilita, kdy se zde dá vložit celý internetový odkaz webové stránky a proběhne podobné hodnocení.

Vytváření záloh nechrání před počítačovými hrozbami přímo, ale může v mnoha případech pomoct, pakliže se nedostane i do těchto záloh malware, pak by to znamenalo, že s obnovou dat by se vrátila i hrozba. Pro uživatele může být v mnoha případech nejjednodušší řešení při napadení jeho počítače to, že obnoví data a systém do stavu, kdy věděl, že vše bylo v pořádku.

Vytváření logů o tom, co daný operační systém a aplikaci dělají při jejich činnosti, je dobrý způsob, jak ulehčit následně analýzu [55] toho, co napáchal malware na počítači. Bezpečnostní experti to ocení v případě, že jim předáte nakažený počítač a budete chtít přijít na to, jak se vlastně přihodilo, že jste byl cílem útoků a antivirus nezvládnul odvést svou práci. Tohle často vede také k tomu, že experti ve firmě následně ví, co mají hledat na ostatních zařízeních.

Mnohé firmy, které investují nemalé peníze do počítačové bezpečnosti, jdou až tak daleko, že jejich zaměstnanci nedostávají počítače s USB porty ani žádným jiným externím vstupem, jelikož to jsou slabá místa v bezpečnosti. Síťovou infrastrukturu si následně mohou správci ohlídat a nastavovat pravidla tak, aby co nejlépe bránili svou firmu.

Kapitola 4

Moderní trendy ohrožující soukromí

Stejně jako tomu bylo na počátku internetu, kdy bylo potřeba naučit se zacházet s novou technologií, odhalit její bezpečnostní rizika, vyladit nedokonalosti, tak podobně je potřeba přistupovat k aktuálním trendům, které s sebou přinášejí nové problémy. Uživatel by proto měl vědět o možných komplikacích a nástrahách, aby se jim mohl co nejlépe vyhnout.

4.1 Sociální sítě

Sociální síť [26] je webová aplikace, kterou využívají lidé ke kontaktu s přáteli, rodinou, kolegy, zákazníky nebo klienty. Sociální sítě mohou mít mimo jiné sociální účel, obchodní účel nebo obojí prostřednictvím webů, jako je Facebook, Twitter, LinkedIn a Instagram. Sociální sítě se staly významnou základnou pro obchodníky, kteří se snaží zaujmout zákazníky.

Je pravdou, že tento trend poskytl mnoho nových a inovativních pracovních příležitostí, o kterých se nám ještě před 15 lety ani nezdálo. Ovšem všechno tohle má i své nevýhody a tím hlavním jsou data, které společnosti od nás získávají. Není cílem zde polemizovat, zda dané společnosti nakládají s našimi daty naprosto legálně, ale upozornit na to, že každý uživatel by si měl dávat pozor na to, co na sociálních sítích zveřejňuje, jelikož jednou z nejdražších komodit současné společnosti jsou informace. Podle chování lidí na internetu lze například vytvořit pravděpodobností model a podle něj určit zda jisté akcie firem porostou či nikoliv. Takže je to nakonec vše o penězích.

Téma jak se má každý uživatel chovat na internetu, aby se nevystavoval nebezpečí nebo někoho jiného, je rozebíráno odborníky a podsouváno veřejnosti už několik let. Avšak podle světových průzkumů to nezabírá, jelikož statistiky [53] [54] okradených lidí na internetu se nelepší. Teď ještě nastal nový trend, kdy dobrovolně o sobě dáváme spoustu informací na internet.

Sociální síť není spyware v pravém slova smyslu, avšak je to aplikace, která sbírá data od miliónů lidí a nabízí jejich obsah zase jiným lidem, ovšem všechno tohle dělá se souhlasem jednotlivých uživatelů. Na tento fakt upozorňují bezpečnostní experti a jednotlivé firmy se s tím snaží něco dělat, aby alespoň trochu v tomto ohledu zmírnily tlak společnosti a zlepšilo se veřejné mínění

o nich. V posledních letech velmi zapracovali na možnosti nastavení u jednotlivých uživatelských profilů, tak aby měl právo vidět obsah uživatele třeba jen uživatel, který je "přítel". Velký problém však je, že této možnosti využije naprosté minimum uživatelů, ať už z důvodu, že jsou líní, nevědí o této možnosti, nebo jen prostě nechtějí skrývat před ostatními své informace, aby mohli dostávat "like"na své obrázky a přiblížili se tak k vysněné práci internetového influencera.

4.1.1 Facebook

Na začátku roku 2004 Mark Zuckerberg [27] spustil nový projekt, kterým byla webová aplikace pro studenty a učitelé z Harvardu. Po založení vlastního profilu mohli uživatelé sdílet své data včetně fotek. Postupně se přidávaly i jiné školy, až nakonec v roce 2006 byl Facebook zpřístupněn všem lidem s podmínkou, že musejí mít emailovou adresu a věk nad 13 let.

Při hledání konkrétního člověka v dnešní době je velmi jednoduché otevřít internetový vyhledávač Google a zadat nějaké jméno. Jestliže to bylo jméno běžného člověka a žádné známé celebrity, tak jeden z prvních odkazů bude právě na Facebook, jestliže existuje jeho profil. Nyní lze najít spoustu informací podle toho, jak si dotyčná osoba cení svého soukromí, ale běžně se zde nachází místo bydliště, rok narození, zaměstnání případně škola. O takovéto možnosti se například bezpečnostním složkám v osmdesátých letech mohlo jen zdát a nyní to může využít každý člověk na světě.

Ovšem co je alarmující, je to, že i když má uživatel správně nastavené zobrazování informací a fotek jen "přátelům", tak stačí, aby měl jeden z těchto přátel špatně nastavené bezpečnostní opatření a následně označil jakýmkoliv způsobem fotku původního uživatele, tak se z této fotky stane veřejně přístupný záznam, protože se to zobrazí ne na profilu vlastníka, ale toho uživatele, který jej označil. Podobně se dá přes "přátele" hledat konkrétní lidi. Když člověk ví, že daná osoba se kamarádí s někým, tak podle seznamu přátel toho dotyčného se dá dohledat.

Další možností, jak využít Facebook k získání informací, je vytvořit si falešný profil s cizím jménem a vydávat se za něj. Díky tomuto může útočník získat důvěrné informace, ke kterým by se jinak nemusel dostat. Cílem tohoto útoku jsou hlavně děti, ale ani dospělí nejsou výjimkou.

Velkým nebezpečím je také to, že se někdo dostane do profilu jiného uživatele a způsobí jeho jménem nějaké problémy. Ale ještě horší věc, kterou může kdokoliv udělat během chvíle, když se dostane na profil někoho jiného, je to, že si stáhne kompletní informace o tom, co dotyčný kdy dělal na FB, s kým si psal (včetně obsahu) a další metadata, které o uživateli FB získal. Všechno tohle je dostupné přes "Nastavení a soukromí/Nastavení/Vaše informace na Facebooku/Stažení vašich informací"4.1. Stažený soubor bude mít velikost v řádech stovek MB, podle toho, jak moc je uživatel aktivní na sociální síti a jestli využil nějaké filtry obsahu. Tahle ta možnost tu je už několik let, avšak při testu v roce 2021, se objevila novinka v tom, že Facebook uživatele upozorní přes e-mail, že si stahoval tyto data. Na ukradených datech to nemění nic, ale dává to možnost reakce uživateli, aby pachatele vystopovat, jestliže se to stalo na jeho vlastním zařízení, když se třeba jen chvilku nedíval a nezamkl si ho.

Obrázek 4.1: Ukázka stažení osobních dat z Facebooku

Když se dostanou tyto data uživatele do rukou někoho jiného, tak to jistě může využít k vydírání. Pravděpodobnost, že za 10 let a více využívání této aplikace, by se uživatel alespoň jednou neunáhlil a nenapsal něco o někom, čeho by mohl litovat, nebo neposlal nějakou nevhodnou fotku, je hodně malá. Je pravda, že aby se někdo probral takovým množstvím dat, je potřeba nějakého času, ale s rozvojem technologií a moderní umělé inteligence je jen otázka času, kdy bude existovat aplikace, které přesně takovéto data bude požadovat jako vstupní parametr. Ona následně podle naučených vzorů najde všechny choulostivé data v krátkém čase.

4.1.2 Instagram

Za touto aplikací [28] stojí pánové Kevin Systrom a Mike Krieger. Ti na počátku experimentovali s jinou aplikací, která se jmenovala Burbn [28] a byla mnohem komplikovanější, jelikož nabízela mnohem více funkcí, což se ukázalo jako její velký problém. Následně se rozhodli, že se soustředí jen na jednu hlavní funkci a tou bude nahrávání a sdílení fotek s přáteli. Aplikace dostala nové jméno (Instagram) a byla uvedena na trh v říjnu 2010. Stále se velmi úspěšnou, a proto ji v roce 2012 odkupuje společnost Facebook za 1 miliardu dolarů.

Zde je namístě upozornit, že některé fotografie o nás mohou nepřímo říkat informace, které bychom jen tak nesdělovali všem neznámým lidem. Nejtradičnější ukázková situace vzniká v létě, kdy samotná policie varuje, aby uživatelé nedávali na internet fotografie z letiště, že odjíždějí na dovolenou. Toto může být jasným signálem pro zloděje, že mohou navštívit nemovitost a nikdo se v ní nebude nacházet. Takže podle neuvážených veřejných fotek je možné lidi sledovat, na jakém místě se nejspíše nacházejí, nebo naopak nemohou nacházet.

Z dlouhodobého hlediska je zde možná hrozba toho, že tím, jak uživatel bude dostatečně často sdílet fotografie své postavy a hlavně obličeje, bude zde možnost využít umělou inteligenci, která

na základě těchto fotografií bude moct vytvořit fotografie, které nebudou mít vůbec reálný základ, ale budou mít za cíl zesměšnit oběť, která pak bude mít plné ruce práce s dokazováním, že tohle není skutečnost. Je to teoretická ukázka toho, jak zničit dobré jméno konkurenční firmy.

Dalším takovým typickým příkladem je rozpoznávání obličeje pro odemčení zařízení. Už nyní se snaží tvůrci mobilních telefonů implementovat různá opatření, aby nebylo možné vzít jen obyčejnou fotku něčího obličeje a tu využít jako klíč. Ovšem i tohle hloupé řešení fungovalo na velmi starých modelech, takže je jen otázkou, do jaké míry zloději budou vynalézaví a schopni obejít moderní zabezpečení. Jistě jim však uživatelské fotky, přístupné všem, pomůžou.

4.2 Internet of Things

Internet věci [29], zkráceně IoT, je pojem popisující oblast komunikace a řízení věcí, které užíváme běžně každý den. Tyto zařízení pak komunikují mezi sebou navzájem a to hlavně pomocí bezdrátového přenosu dat a internetu, kde jedno zařízení pomocí čidla například zjistí teplotu v domě a tím dá vědět jinému, že by mělo začít vytápět. Vše je to tedy o sbírání dat a správném vyhodnocení, aby se mohla vykonat adekvátní odpověď.

Jelikož se ve většině případů jedná o velmi malá zařízení, které musejí mít minimální požadavky na energii, protože jsou často jen napájeny z baterie a nejsou zapojeny přímo v sítí. Toto vede k tomu, že mnoho zařízení není přizpůsobeno, aby mohly získaná data a celou jejich komunikaci s okolím nějakým způsobem šifrovat. Takže kdokoliv, kdo má přístup k jejich společnému komunikačnímu kanálu, si může v datech číst, ovšem může posílat i falešné zprávy, jestliže zná protokol, který by měl být popsán a dostupný na internetu. Falešné zprávy pak mohou zařídit to, že byt se bude vytápět i přesto, že je třeba léto a teplota 25 stupňů Celsia.

Dalším důvodem, proč je někdy v těchto zařízeních bezpečnost opomíjena je ten, že se výrobci snaží udělat maximálně levný produkt a jak už bylo zmíněno několikrát, to často na úkor bezpečnosti. Následně pak zákazník, který si vybírá mezi produktem za 200 Kč a 1000 Kč na to doplatí, jelikož si logicky zvolí levnější produkt, ale bez hlubších znalostí nezjistí, jaké potíže to může obnášet.

4.2.1 IP Kamery

Jsou jedním z nejběžnějších zástupců IoT zařízení, které jsou primárně využívány ke kontrole majetku. Takže se jedná o bezpečnostní zařízení, proto je zarážející, že se zde mnohdy nakonec šetří také na bezpečnostních prvcích.

Podle statistik [36], kdy v roce 2013 byl výskyt IP kamer celosvětově něco kolem 0,4 miliónů kusů, tak v roce 2019 je to již 25,1 miliónů. Jak lze vidět, je to moderní trend a jelikož nejlevnější kusy se dají nakoupit již kolem 800 Kč, tak se není moc čemu divit.

Odborníci se shodují na tom, že největším problémem je často uživatelské rozhraní, které je děláno pomocí webové stránky. Zde je hlavní problém v tom, že se nepřistupuje přes port 443, tedy

šifrovanou verzi, ale využívá se jen klasická nešifrovaná, která poslouchá na portu 80. Další častý problém je, že majitel nastaví špatně své zařízení, proto následně má možnost se díky této chybě každý dívat na to, co daná kamera snímá, jelikož stačí mít správný internetový odkaz, který je schopen indexovat pomocí svých algoritmů Google.

Tohle je tedy největší nebezpečí, které skýtá samotná kamera, místo toho, aby chránila majetek, nakonec slouží jako špión, pomocí kterého může sledovat někdo naše soukromí.

4.2.2 Chytré náramky

Na tento módní doplněk se také často zaměřují bezpečnostní specialisté a opět upozorňují na to, že mnoho z těchto zařízení má bezpečnostní díry právě v komunikaci, která je prováděna přes mobil. Tím mimo jiné je v ohrožení i samotné mobilní zařízení, jelikož aplikace, která je potřebná pro stažení dat z náramku může být sama o sobě bezpečnostní hrozbou. Tohle je pěkný příklad toho, jak mohou IoT zařízení degradovat bezpečnost jiného zařízení.

4.2.3 Hlasový asistent

Nejspíše technologie, která se bude v budoucnu nacházet v každé domácnosti a řídit ji. Je však potřeba uvědomit si, co taková technologie s sebou musí přinášet a tím je neustálý odposlech, jestliže bude uživatel chtít využívat její primární účel a tím je reagovat na hlasové povely. Proto by si každý měl důsledně přečíst licenční podmínky, aby věděl, s čím souhlasí při využívání této technologie.

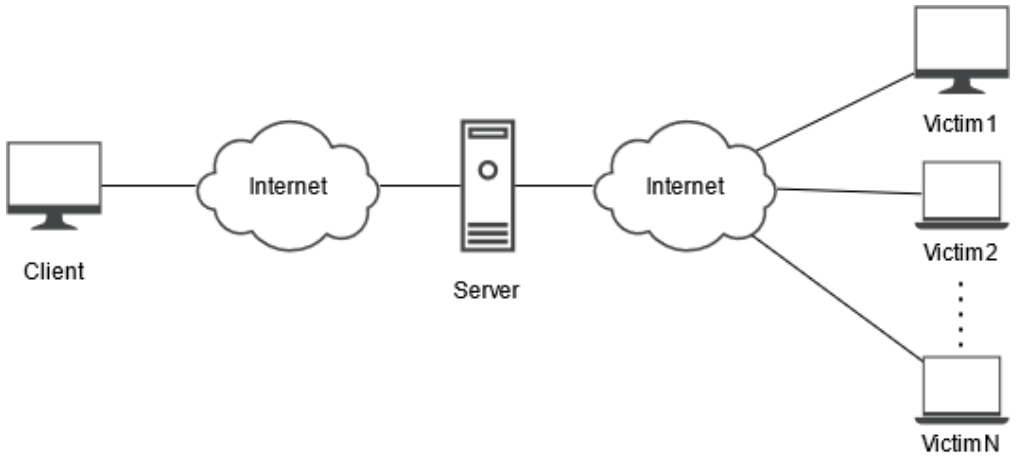
Kapitola 5

Praktická část

V praktické části bude popsána implementace tří aplikací, které spolu navzájem komunikují a představují teoretický scénář, jak by mohlo vypadat reálné nasazení spywaru a jeho ovládání útočníkem na dálku. Tato kapitola obsahuje popis základních komponent spywaru a taky zdroje informací, které by mohly útočníky zajímat.

5.1 Síťová komunikace

Informace a data, které jsou získané pomocí naprogramované aplikace, je potřeba dostat z napadeného počítače zpátky k útočníkovi, aby s nimi nakonec mohl nějak naložit.



Obrázek 5.1: Schéma síťové komunikace

Přenos dat je zajištěn pomocí síťové komunikace. Základní schéma je znázorněno na obrázku 5.1. Celý proces se skládá ze tří různých částí. Obyčejný způsob klient-server zde nebyl použit z toho důvodu, aby bylo možné demonstrovat částečně i možnosti maskování komunikace v síti. Takto může nastrčený server stále poslouchat na portu, ke kterému se přihlašují postupně jednotlivé oběti

a samotný útočník se může přihlásit z klientské aplikace, klidně za použití VPN služby, aby maskoval svou IP adresu.

5.1.1 Klientská část

Jedná se o konzolovou aplikaci, která se připojuje na server. Pomocí tohoto rozhraní je možné posílat požadavky na server. Při spuštění se hledá konfigurační soubor, jestliže nebude nalezen, aplikují se výchozí hodnoty pro port a IP adresu, na které se nachází server.

5.1.2 Serverová část

Slouží k propojení mezi klientem a obětí. Server stále poslouchá na dvou portech. Ve výchozím nastavení je to port 6666 pro Klient aplikaci a port 6667 pro Victim aplikaci. Opět při startu aplikace se hledá konfigurační soubor, ve kterém se tyto hodnoty mohou změnit.

Hlavním úkolem serveru je vyhodnocovat požadavky od klientské aplikace a následně je přeposílat na jednotlivé oběti, které příkaz zpracují a pošlou přes server výsledek zpět do klientské aplikace.

Ke komunikaci se využívá TCP [37] spojení. Zpráva má jednoduchou formu textu. Mezi klientem a serverem se využívá tento formát "GET::FFFF3015CCCC::LOCATION0023". "GET" je klíčové slovo pro získávání informací, "FFFF3015CCCC" je identifikátor (Pro unikátní identifikaci jednotlivých obětí se využívá jejich MAC adresa. Ta byla zvolena z toho důvodu, že IP adresy mohou být přidělovány DHCP serverem nebo prostřednictvím NATu. Takhle by mělo být možné skládat k sobě jednotlivé získané informace od jednoho stroje, přestože změní pozici v síti.) a "LOCATION0023" je název funkce, která se bude volat ve Victim aplikaci. Tuto komunikaci je možné šifrovat, ale schválně byl zvolen jen obyčejný XOR způsob, aby nebylo potřeba přidávat a volat funkce pokročilého šifrování, které by mohly upozorňovat antivirus. Funkce XOR stačí k tomu, aby se v přenášených paketech nevyskytovala klíčová slova v čitelné podobě, a zároveň nevytěžuje zbytečně moc aplikaci.

Komunikace mezi Klientem a Serverem funguje asynchronně, tedy Klient může posílat více požadavků a Server je zpracovává zároveň, avšak mezi Serverem a Victim části funguje jen synchronní komunikace na principu Request-Response. Zde musí nejprve vykonat první požadavek Victim aplikace a následně může až další. Je to částečně i kamuflážní mechanismus, aby spyware nespotřebovával více hardwareových prostředků, než je nutné.

Přemostění mezi hlavním vláknem, které obsluhuje spojení s klientem a vlákny, které obsluhují jednotlivé spojení mezi oběťmi (jedno vlákno na každou připojenou oběť), je zařízeno pomocí sdílené kolekce "List<string> RequestFromClient". Pro výhradní právo zápisu jednotlivými vlákny do této proměnné se pak využívá "lock".

5.1.3 Victim část

Tohle je nejdůležitější část, jelikož se jedná o samotný spyware. Jak již bylo zmíněno výše, reaguje na požadavky od Klientské aplikace, které zprostředkovává Server. Opět při spuštění se snaží nahrát aktuální konfiguraci.

Když se tato aplikace spustí, snaží se připojit na server, jestliže se jí to nepovede, tak využije další komunikační kanál a tím je e-mail. Google nabízí API [38], pomoci kterého je možné skrze aplikace posílat poštu. Touto formou se však dá odeslat jen omezené množství dat a proto je potřeba zvážit, co jsou nejpotřebnější informace.

5.2 Hlavní bloky aplikací

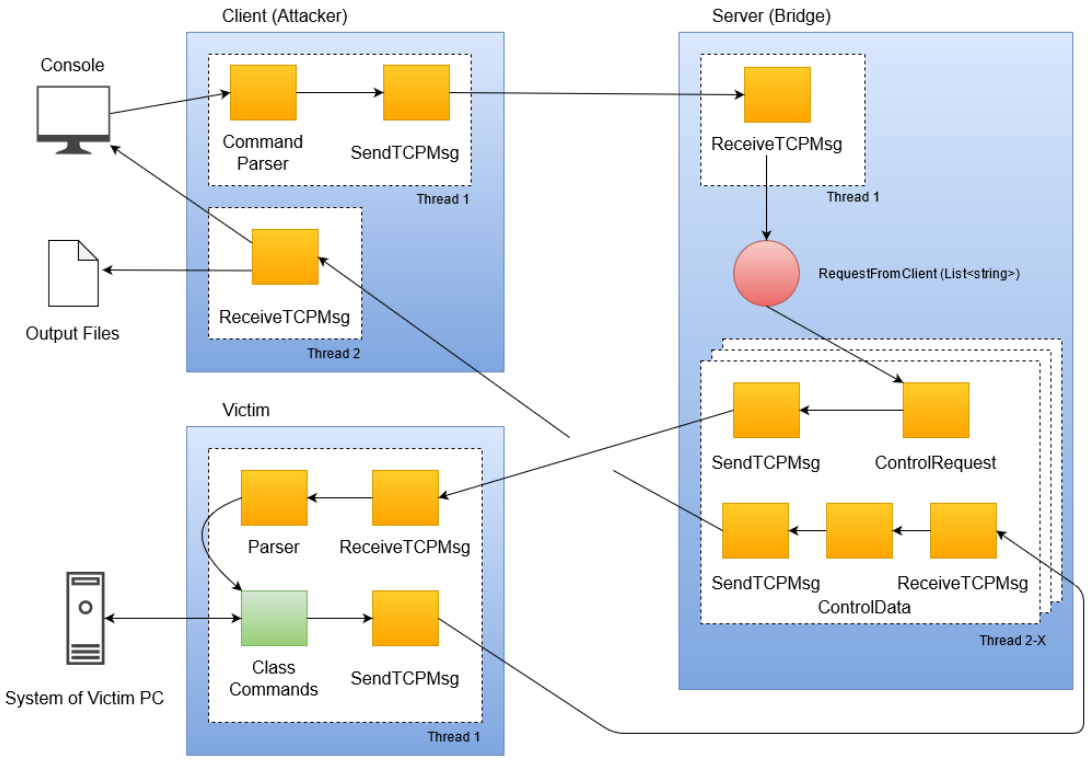
V předchozích odstavcích bylo stručně popsáno, jak funguje tok dat mezi jednotlivými částmi. Podrobnější popisek jednotlivých částí lze vidět na obrázku 5.2. Modré obdélníky znázorňují jednotlivé aplikace. Bílé obdélníky s tečkovaným okrajem pak mají vyjadřovat bloky, které běží v rámci jednoho vlákna v dané aplikaci. Oranžový obdélník znázorňuje logické bloky pro konkrétní činnost. Zelený obdélník má specifikovat to, že na daném místě se volá třída "Commands", která zprostředkovává veškeré akce pro získávání dat. Červené kolečko pak vyjadřuje datovou strukturu, která je potřeba proto, aby bylo možné dostat příkazy z hlavního vlákna k vláknům, které komunikují s Victim aplikací.

Na Klientovi běží vždy dvě vlákna. Jedno hlavní, které zpracovává příkazy, které byly zadány útočníkem z konzole, a následně je pošle na Server. Druhé vlákno pak zařizuje příjem dat. Při běhu serveru existují vždy minimálně dvě vlákna. Jedno přijímá příkazy od Klienta a následně jej dává do "RequestFromClient". Druhé se stará o to, když se připojí nějaká Victim aplikace, tak vytvoří nové vlákno, které se stará o komunikaci s tímto zařízením. Samotná Victim aplikace běží pak jen v rámci jednoho vlákna. Výjimkou je pak jen volání některých funkcí v rámci "Commands" třídy, kde se například pro běh keyloggeru volá funkce v novém vlákně.

5.3 Kopírování souborů

Jednou ze základních funkcí spyware by měla být možnost získání souborů z napadeného počítače. Toho lze docílit velmi jednoduše a to tak, že požadovaný soubor načteme v binárním formátu (byte[] bytes = File.ReadAllBytes(path)) a pak si jej aplikace pošle přes internet byte po bytu. Klient pak tyto získané data opět zapíše binárně do souboru a tím vznikne kopie u samotného útočníka.

V běžném posílání řídicích zpráv je využíváno kódování pomocí "ASCIIEncoding.ASCII.Get Bytes()", jenže toto kódování využívá jen 7 bitů z 8, což by zapříčinilo znehodnocení souboru, proto je nutné k těmto zprávám přiložit čistě pole bytů, které obsahu načtený soubor.



Obrázek 5.2: Diagram propojení jednotlivých komponent

Hlavička řídící zprávy nese i informaci o velikosti samotného souboru, aby bylo možné jej následně správně oddělit od zbytku zprávy.

Aplikace, která představuje spyware, obsahuje metodu jménem "SendFile", která obstarává toto posílání. Využívá se jak ke kopírování souborů z napadeného počítače, tak i k posílání vytvořených souborů, které jsou výsledkem jiných funkcí spywaru.

5.4 Snímek Obrazovky

Při pořízení snímku obrazovky (printscreen), se mohou v tomto obrázku nacházet informace, které by mohly být jinak těžce dostupné. Nikde však není garantováno to, že tato situace musí nastat vždy. S větším počtem takto vytvořených snímků, pak tedy roste pravděpodobnost, že se podaří zachytit něco zásadního.

Následující metoda 5.1 slouží k vytváření snímků obrazovky a jejich uložení do souboru.

```
public void TakeScreen()
    {
        Rectangle resolution = Screen.PrimaryScreen.Bounds;
```

```
        Bitmap bmpScreenshot = new Bitmap(resolution.Width, resolution.Height,
            PixelFormat.Format32bppArgb);
        Graphics gfxScreenshot = Graphics.FromImage(bmpScreenshot);
        Size s = new Size(resolution.Width, resolution.Height);
        gfxScreenshot.CopyFromScreen(0, 0, 0, 0, s, CopyPixelOperation.SourceCopy)
            ;
        bmpScreenshot.Save("ScreenCapture.jpg", ImageFormat.Jpeg);
    }
```

Listing 5.1: Metoda pro vytvoření snímku obrazovky

Takto vytvořený obrázek následně jen binárně přenese již implementovaná funkce pro kopírování souborů.

5.5 Seznam souborů

Metoda pro získávání souborů byla již představena, takže je potřeba získat informace o tom, které soubory by mohly být zajímavé. K tomu slouží metoda "FindAllFilesIn" (obrázek 5.3).

Jsou potřeba dva vstupní parametry. První je kořenový adresář (odkud se má začít prohledávat) a ten druhý je hledané klíčové slovo v názvu souboru. Metoda je konstruovaná tak, aby vrátila seznam cest například obrázků, PDF, nebo Microsoft Word dokumentů.

Informace o adresářích se získávají pomocí třídy "DirectoryInfo", která pak obsahuje užitečné metody jako "GetDirectories" a "GetFiles".

```
C:\Users\jfalt\Desktop\Diploma\CzechThesisExample\FiguresAssignment1.jpg
C:\Users\jfalt\Desktop\Statistika\test4\resenireseniStrana2Zoom.jpg
C:\Users\jfalt\Desktop\FAL0046.jpg
C:\Users\jfalt\Desktop\faltynek.jpg
C:\Users\jfalt\Desktop\IMG_20200401_175125.jpg
```

Obrázek 5.3: Ukázka výpisu pro FindAllFilesIn s parametry "C:\Users\jfalt\Desktop\" a ".jpg"

5.6 Záznam zvuku

Využití mikrofonu od počítače k odposlouchávání dané místnosti je také jednou z funkcí napsané aplikace. Mnoho metod, které umožňují práci s mikrofonem, jakožto zdroj dat, jsou doprovázený tím, že uživatel musí na začátku spuštění programu souhlasit s tím, že tato aplikace bude mít přístup k mikrofonu, což je velká komplikace pro útočníka.

Při využívání této DLL knihovny 5.2 se však nevyžaduje žádný souhlas uživatele. Což je tedy zásadní výhodou a důvod, proč byla nakonec použita. Nevýhody jsou však také. První a mnohem

důležitější je to, že kvalita takto získaného zvukového záznamu nebyla příliš dobrá a obsahovala vždy v pozadí šum. Druhou nevýhodou je to, že aplikace potřebuje nahrát další DLL knihovnu, díky čemuž na sebe může upozornit a antivirus ji s větší pravděpodobnosti označí za škodlivou.

```
[DllImport("winmm.dll", EntryPoint = "mciSendStringA", ExactSpelling = true,
    CharSet = CharSet.Ansi, SetLastError = true)]
private static extern int record(string lpstrCommand, string lpstrReturnString,
    int uReturnLength, int hwndCallback);
```

Listing 5.2: Import DLL knihovny pro záznam zvuku

5.7 Keylogger

Aby měla aplikace přístup k informaci o stisku jakékoliv klávesy i ve chvíli, kdy uživatel nevyužívá kontext dané aplikace, je potřeba využít systémové volání. K tomu je využita knihovna "User32.dll" a metoda (GetAsyncKeyState) z ní.

Při volání funkce, která se stará o naprogramovaný keylogger, je potřeba vytvořit vlákno, jelikož tělo metody je v nekonečném cyklu a stále se doptává na stav kláves v jistém časovém intervalu.

Tato funkce 5.3 znázorňuje, jak vypadá ten nejjednodušší kód pro získání stisknutých kláves. Projdou se všechny klávesy, a jestliže se potvrdí, že byly stisknuty, tak se přidají do bufferu. Tady může nastat problém. Celá funkce předpokládá, že za jeden časový interval (např. 40 ms), uživatel použije jednu klávesu, případně jednu obyčejnou (a, b, c, 1, 2, 3, +, -, atd.) a k tomu nějakou kontrolní (<CTRL>, <ALT>, <SHIFT>). Jestliže by to tak nebylo, tak pak mohou být zaznamenané znaky ve špatném pořadí. Případně jestliže by držel jednu klávesu delší dobu, tak tam jistě nebude správný počet znaků. Tohle však nehrozí u většiny uživatelů, když zadávají hesla, jelikož nespěchají, aby se nevytvořil překlep.

Z výše zmíněného jde odvodit další problém a to ten, že získáme jen informaci o tom, že bylo například sfiknuta klávesa se znakem "B", ale už nevíme, jestli by mělo být velké nebo malé, což je pro hesla zásadní problém. V aplikaci je to vyřešeno takto, jestliže je stisknuta nějaká obyčejná klávesa, tak zároveň se aplikace doptává, zda je zmáčkla i nějaká kontrolní klávesa (<CTRL>, <ALT>, <SHIFT>). Díky tomuhle řešení je pak samotný stisk kontrolní klávesy ignorován, aby se ve výpise nenacházela zbytečně dvakrát.

Zjištění, zda je potřeba vzít v potaz to, že je CapsLock zapnut, je ošetřeno pomocí metody "Control.IsKeyLocked(Keys.CapsLock)". Takto jde ošetřit i NumLock.

```
public string GetBuffKeys() {
    string buffer = "";
    foreach (System.Int32 i in Enum.GetValues(typeof(Keys)))
```

```
    {
        if (GetAsyncKeyState(i) == -32767)
            buffer += Enum.GetName(typeof(Keys), i);
    }
    return buffer;
}
```

Listing 5.3: Ukázka kódu pro zachycení klávesy

Na obrázku 5.4 lze vidět, jak bude vypadat výsledek keyloggeru pro daný výraz. "předloha" jsou klávesy, které byly stisknuty. Pro lepší přehlednost jsou zde mezery, ale ty nejsou součásti zápisu. V hranatých závorkách jsou vždy složené příkazy, případně klávesy, které nejde přímo zaznamenat, jako je například Enter. <NP1> je klávesa NumPad1 atd. "input" je pak výstup, jak to vypadá například v kolonce prohlížeče, když se mačkaly klávesy podle předlohy. Výsledek reprezentace programu je pak vidět v "keylogger".

```
předloha: <CTRL+SHIFT+C> + ě š 1 2 3 a b <SHIFT+C> <SHIFT+D> <NP1> <NP2> <NP+> <NP-> <CTRL+V> <ENT>
input: +ěš123abCD12+-
keylogger: <CTRL>C<D1><D2><D3><SHIFT><D1><SHIFT><D2><SHIFT><D3>abCD12+-<CTRL>v<ENT>
```

Obrázek 5.4: Ukázka výsledku pro keylogger

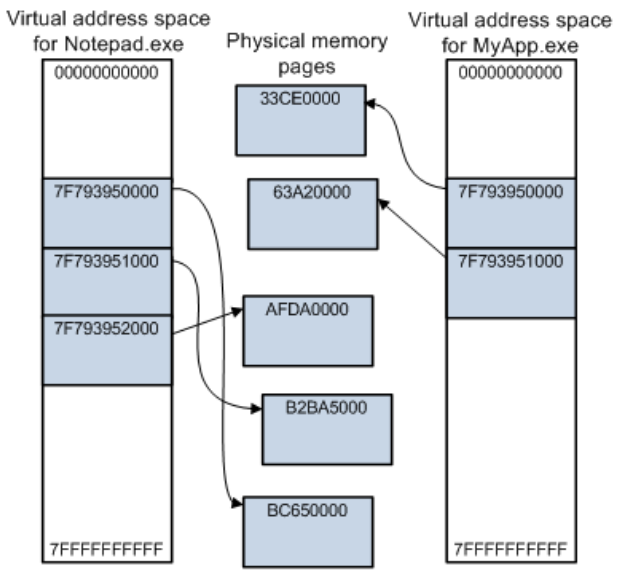
5.8 Čtení paměti jiného procesu

V paměti programu se nacházejí veškerá data, se kterými daná aplikace pracuje, proto je cílem každého útočníka se zde nějak podívat. Tohle však není vůbec jednoduché, jelikož tento fakt je velice dobře znám a proto se i samotný Microsoft snaží dělat všechno proto, aby byly aplikace v bezpečí jedna před druhou a i antiviry si dobře hlídají tyto přístupy.

Základní ochranou před manipulací s pamětí je tzv. virtuální paměť [47]. Ta slouží primárně k tomu, aby daná aplikace měla větší adresní prostor, než by mohl mít, kdyby využíval jen adresy fyzické RAMky. Ale díky tomu je i každá aplikace izolovaná před jinou, jelikož nesdílí tento virtuální prostor. Takže jedna aplikace může mít na adrese 0x7777FFFF hodnotu X, ale jiná aplikace na téže adrese, avšak ve svém přiděleném prostoru, bude mít úplně jinou hodnotu Y. Na stránkách Microsoftu [47] je k této problematice vystaven obrázek 5.5, který znázorňuje tuto mechaniku.

Další bezpečnostní prvek, který má chránit paměť programu, je to, že se program při každém spuštění alokuje na jinou adresu. Jinými slovy, paměť programu při každém spuštění je úplně jiná, jelikož na jednotlivých adresách mohou být úplně jiné hodnoty než při minulém spuštění.

Jelikož přímo z jedné aplikace není možné číst paměť té druhé, protože spolu nesdílí adresní prostor, je potřeba využít funkcí systému. K tomu slouží knihovna "kernel32.dll" 5.4.



Obrázek 5.5: Znázornění adresace ve virtuální paměti

```
[DllImport("kernel32.dll")]
public static extern IntPtr OpenProcess(int dwDesiredAccess, bool bInheritHandle,
    int dwProcessId);

[DllImport("kernel32.dll")]
public static extern bool ReadProcessMemory(int hProcess, int lpBaseAddress, byte
    [] lpBuffer, int dwSize, ref int lpNumberOfBytesRead);
```

Listing 5.4: Import funkcí z kernel32.dll

Implementovaná metoda v odevzdaném řešení pracuje jen s aplikacemi v 32bit režimu. Proto je zde "int lpBaseAddress", jinak by bylo potřeba nahradit "int" za "Int64", aby dané číslo mohlo reprezentovat celou velikost adresního prostoru. Důvod, proč byla nakonec zvolena jen 32bit verze je ten, že pro demonstraci použití to stačí a při využívání 64bit verze je potřeba procházet mnohem větší adresní prostor. Nelze totiž předpokládat, když má fyzicky daný počítač velikost RAMky například 16 GB, tak že tohle je i velikost virtuální paměti. Virtuální paměť může využívat celý rozsah 2^{64} adres, což je obrovský prostor pro hledání.

Jestliže hledáme informace v paměti, chtělo by to nějaké místo, od kterého bychom začali prohledávat. Toto místo se dá získat pomocí "process.MainModule.BaseAddress". Takto lze získat adresu, kde začíná hlavní modul programu, který obsahuje i PE hlavičku [40]. Pro 32bit aplikace to pomůže primárně se správným zarovnáním v paměti, ale v 64bit aplikaci to slouží k alespoň částečné lokalizaci dat. Nikde však není garantováno, že před touto adresou nemohou být taky nějaká data.

Důležitá poznámka je to, že 64bit aplikace může sahat do paměti 32bit aplikaci, ale naopak to nefunguje a program při takovémto pokusu spadne.

Funkcionalita samotného programu je taková, že stáhne obsah paměti 32bit procesu buďto jako proud bytů, nebo je transformuje rovnou na Char. Následně se nad binární verzí dá využít nějaký nástroj pro analýzu binárního kódu. Jednou z možností je například aplikace Strings [48], která vrátí řetězce, které se v binárních datech ukrývají.

5.9 Geolokace pomocí WiFi karty

Díky informacím, které se dají získat z operačního systému (jazyková sada, časové pásmo) nebo hardwaru, lze předpokládat, že daný stroj se nachází v nějaké dané lokaci, ale většinou se jedná o plochu o velkém rozměru. Pro přesnější lokalizaci zařízení je možné využít například WiFi kartu.

Teorie je velmi jednoduchá. Když bude existovat dostatečně velká databáze statických (věci, které nebudou měnit v čase svou geografickou polohu) zařízení (ve většině případů se jedná o routery) o jejich identifikátoru a jejich lokaci, bude možné díky tomu určit lokaci jiného zařízení s jistou přesností, jestliže budou spolu moci nějak tyto zařízení komunikovat.

Zmíněnou komunikací se myslí, že všechny routery vysílají kolem sebe základní informace o sobě, včetně svého identifikátoru BSSID, což je vlastně jejich MAC adresa. To bychom měli statická zařízení a ještě je potřeba určit jejich polohu. K tomu stačí, aby se kolem routeru prošel člověk se smartphonem, který obsahuje jak WiFi adaptér, aby mohl chytat tyto zprávy, tak GPS lokalizátor, aby právě mohl udat polohu tohoto zařízení. Nebude náhoda, že přesně takovou databázi vlastní společnost Google a nabízí API [39], pomoci kterého je možné určit právě zeměpisné souřadnice díky blízkých WiFi routerů.

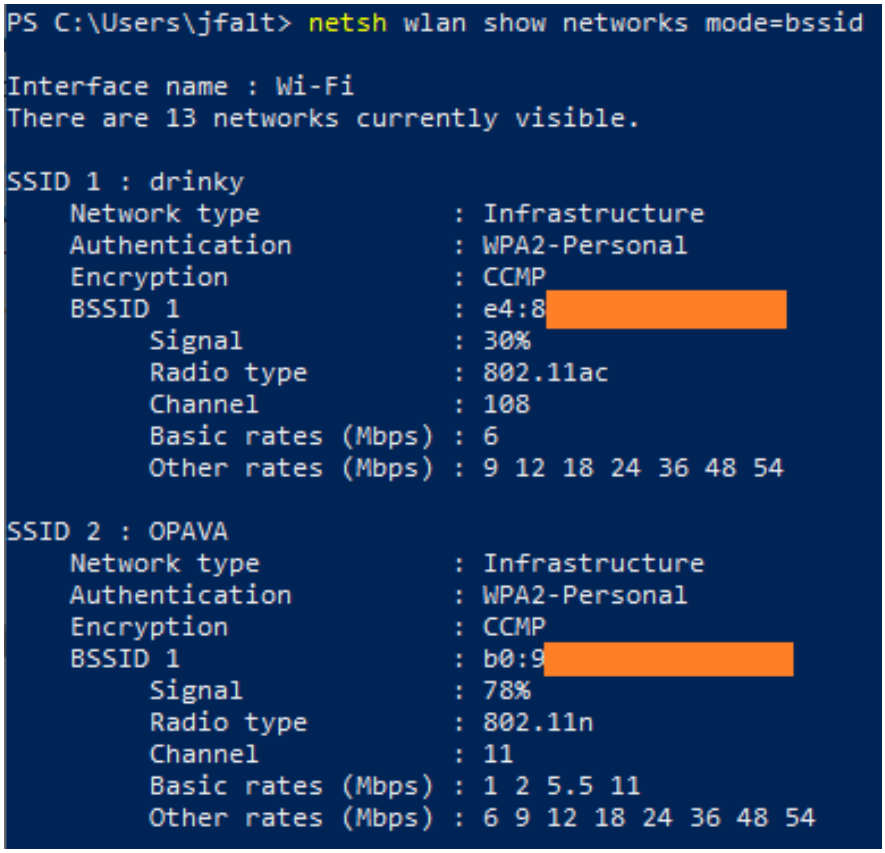
Jestliže počítač s operačním systémem Windows má WiFi adaptér, je možné pomocí příkazu (netsh wlan show networks mode=bssid) v Powershellu získat všechny okolní sítě a jejich informace. Výsledek pak vypadá takto 5.6. Jeho užití v C# aplikaci lze vidět na této funkci 5.5, která vrátí všechny BSSID routerů v okolí.

```
static List<string> GetIDs()
{
    List<string> resultsList = new List<string>();
    var script = $"netsh wlan show networks mode=bssid";
    var powerShell = PowerShell.Create().AddScript(script);

    foreach (dynamic item in powerShell.Invoke().ToList()){
        string line = Convert.ToString(item);
        if (line.Contains("BSSID")){
            var res = line.Substring(30, 17); //BSSID - 17 znaku
```

```
            resultsList.Add(res);
        }
    }
    return resultsList;
}
```

Listing 5.5: Ukázka funkce na získání BSSID routerů v okolí



Obrázek 5.6: Ukázka výsledku BSSID v okolí

Nyní jsou dostupně všechny potřebné informace k tomu, aby bylo možné vytvořit dotaz na API od Googlu a on nám vrátí lokaci, jestliže bude mít informace o zaslaných routrech. Je možné využít i jiné databáze, ale od Googlu byla veřejně dostupná a zdokumentovaná.

Je potřeba si vytvořit účet, aby bylo možné dostat klíč, který je potřeba k využívání tohoto API. Celý postup je popsán na stránkách společnosti Google, které již byly zmíněny.

Pomocí následujícího příkazu 5.6 lze jednoduše otestovat, po získání klíče, možnosti tohoto API. Za "key=" je pak potřeba doplnit získaný klíč. Jsou zde možnosti pro lokalizaci i pomocí přijímačů pro mobilní zařízení.

```
curl -d @test.json -H "Content-Type: application/json" -i "https://www.googleapis.
    com/geolocation/v1/geolocate?key= "
```

Listing 5.6: Příkaz pro otestování Google API

Ve zdrojových kódech k této práci pak bude jak ukázkový json soubor, tak implementované C# rozhraní pro spojení přes HTTPS k této službě.

Je nutné upozornit, že během testování tohoto API, služba měla časté výpadky a ani jejich vlastní ukázkový příklad nefungoval. Vracel se json s odpovědí – notFound 404 "The request was valid, but no results were returned".

5.10 Informace z internetových prohlížečů

Mnoho zajímavých informací o uživateli se dá zjistit pomocí jeho internetového prohlížeče. Největší hodnotu mají uložená hesla. Tato část je zaměřená na to, jak moc těžké je například získat právě hesla, jestliže si je uživatel uložil v prohlížeči. Budou zde zmíněny i další zajímavé zdroje dat, které se plní při využívání prohlížeče.

5.10.1 Mozilla Firefox

Nejjednodušší způsob získání jakýchkoliv dat je ten, že se opět někdo dostane k počítači, na kterém je přihlášený uživatel a tak si může spustit samotný prohlížeč. Na pár kliků si může stáhnout všechny uložené přihlašovací údaje v čitelné podobě pomocí samotného prohlížeče. Z tohoto důvodu samotná společnost varuje, aby si uživatelé dodatečným opatřením (hlavní heslo k prohlížeči [44]) zabezpečili, jestliže sdílí počítač s jinou osobou. Tuhle obranu však využívá minimum uživatelů, jelikož se jim nechce pamatovat ani zadávat další heslo, případně o této možnosti ani netuší.

Nyní přejděme tedy k tomu, že nemáme fyzický přístup k počítači, takže je potřeba najít soubory, které obsahují informace lehce dostupné právě pomocí rozhraní v prohlížeči. Tyto soubory se nacházejí ve složce AppData, což je skrytá složka systému, do které si všechny programy zapisují některá svá data. Takže obsah této složky bude jistě zajímavý i pro útočníka. Do této složky se dá dostat pomocí průzkumníka ve Windows, když se nechá hledat výraz "%AppData%". V C# se pak dá získat cesta k této složce takto 5.7.

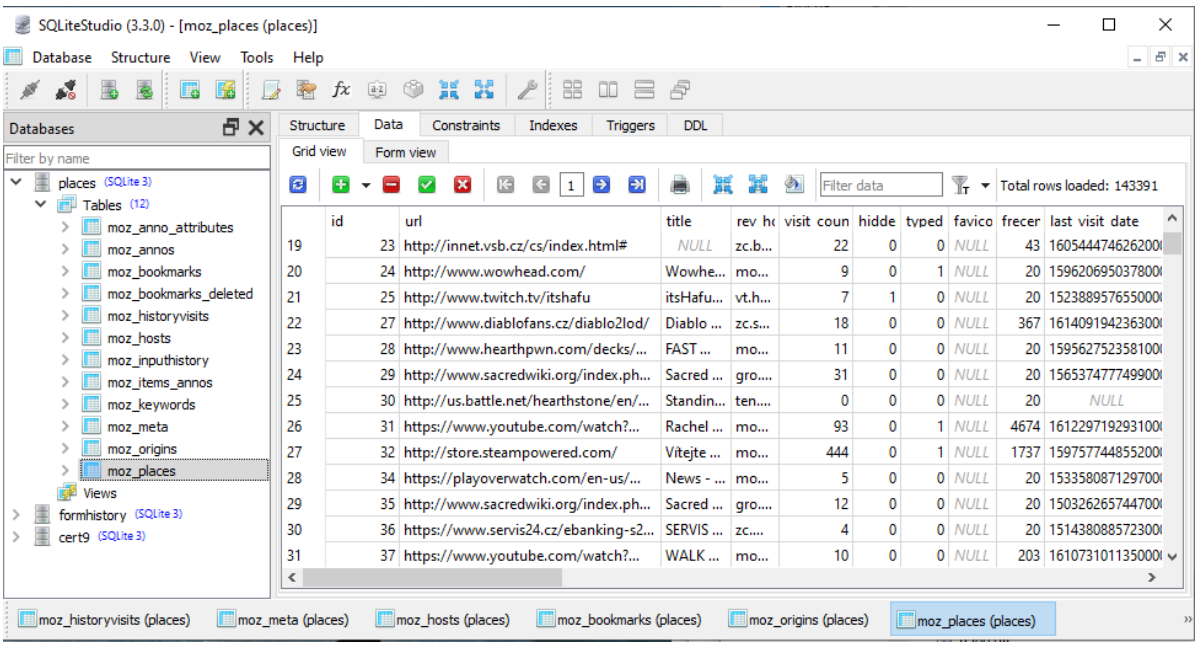
```
string location = @"%AppData%";
string path = Environment.ExpandEnvironmentVariables(location);
Console.WriteLine(path);
```

Listing 5.7: Kód pro získání cesty k AppData

Pakliže je nalezena cesta ke složce AppData, tak v ní už je jen potřeba přejít do "C:\Users\user01\AppData\Roaming\Mozilla\Firefox\Profiles\yfw4ve15.default". V této složce se nacházejí všechny zajímavé soubory [45].

Nelze zde najít hesla a přihlašovací údaje v čitelné podobě, ale přesto se dají velmi jednoduše získat. Jakmile někdo získá soubory "key4.db" a "logins.json", tak má přístup ke všem uloženým heslům v daném profilu. Pomocí key4.db se dají dešifrovat uložené informace v logins.json a to velmi triviální metodou. Útočník jen nahradí tyto dva získané soubory ve svém adresáři s Mozillou a při spuštění prohlížeče uvidí všechny ukradené hesla, jako by byly jeho vlastní. Tak jednoduché to je, jestliže nejsou chráněny tyto soubory nějakým pokročilejším nastavením.

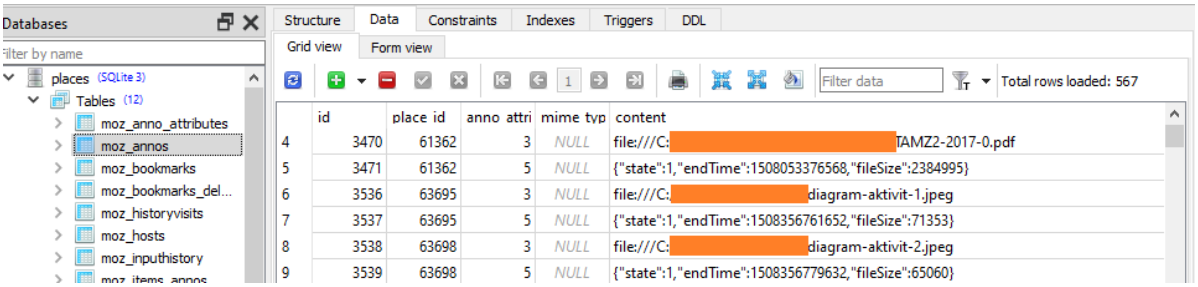
Další zajímavý soubor je "places.sqlite". Tento soubor obsahuje všechny záložky a seznam všech stažených souborů a navštívených webových stránek. Díky těmto informacím 5.7 se dá stopovat, kde uživatel trávil svůj čas, případně se zde mohou nacházet nějaké citlivé informace. Je zde zaznamenáno, kdy byly staženy soubory 5.8 a kam se uložily.



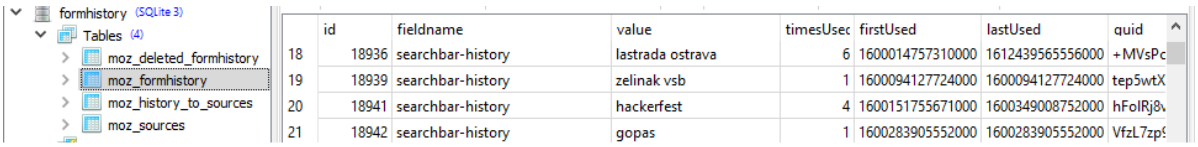
Obrázek 5.7: Ukázka obsahu places.sqlite - navštívené stránky

Soubor "formhistory.sqlite" pak obsahuje data o tom, co uživatel zadával do vyhledávajících polí a formulářů. Během procházení zde nebyly odhaleny žádná hesla, avšak i tak se zde nacházejí informace, jako je třeba vyhledávání pomocí Googlu 5.9. Webové stránky které by měly například ve formuláři na vyplnění místo a čas konání schůzky, by bylo možné tímto způsobem obejít a získat tyto informace.

Soubory "cookies.sqlite" a "webappsstore.sqlite" uchovávají metadata jednotlivých serverů, které uživatel navštívil. Zde už pak záleží, jaké servery daný uživatel navštěvuje a jestli tyto servery mají naimplementováno vše bezpečně, nebo je možné, že ukládají pomocí těchto úložišť citlivá data.



Obrázek 5.8: Ukázka obsahu places.sqlite - stažené soubory



Obrázek 5.9: Ukázka obsahu formhistory.sqlite - vyhledávač

5.10.2 Google Chrome

Hesla uživatelů tohoto prohlížeče jsou ve větším bezpečí. Není možné se k nim jednoduše dostat ani tehdy, jestliže se útočník dostane k přihlášenému účtu na systému Windows. Kdyby si chtěl zobrazit nebo zkopírovat veškerá hesla v čitelné podobě pomocí samotného prohlížeče, potřeboval by znát Windows heslo pro daný účet, jelikož je vyžadováno při provádění této akce samotným prohlížečem.

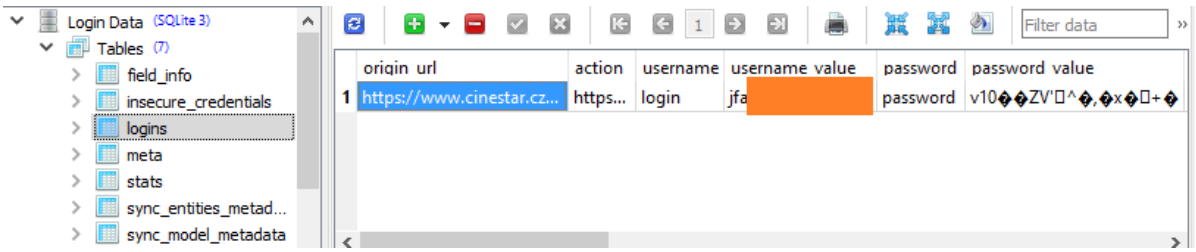
Chrome si uchovává své data ve složce AppData (C:\Users\user01\AppData\Local\Google\Chrome\User Data\Default) jednotlivých uživatelů. Nedají se získat hesla v čitelné podobě, ale i tak se zde nacházejí informace o uživateli, které útočník může hledat, jako například, co dělá uživatel na internetu.

Soubor "Login Data" obsahuje informace o uložených uživatelských heslech a jménech k jednotlivým stránkám, které si uživatel uložil. Na obrázku 5.10 je vidět, že hesla jsou šifrovaná a nedá se zde praktikovat metoda, že se tento soubor zkopíruje do nově instalovaného prohlížeče Chrome. Když by to někdo udělal, bude vidět jen na daných stránkách loginy, ale hesla se neobjeví. Šifrování hesel má na starosti Windows pomocí funkce "CryptProtectData", takže dešifrování lze praktikovat jen na počítači, který provedl šifrování. Tohle je informace získaná z fóra [46], kde je popsána i celá technická stránka věci.

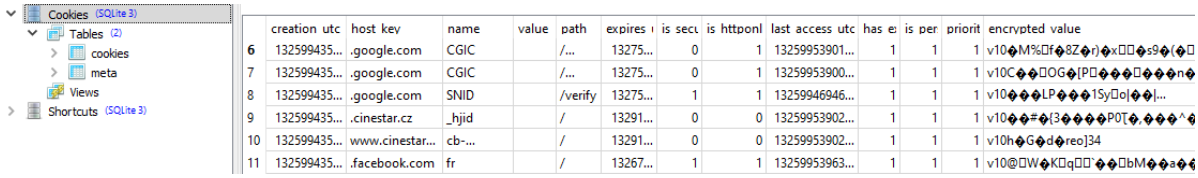
Soubor "Cookies" obsahuje soubory Cookie jednotlivých navštívených serverů. Nedají se zde však získat žádné zásadní informace, jelikož jak lze vidět na obrázku 5.11, tak veškerý obsah samotného Cookie souboru je šifrovaný. Takže se zde nacházejí jen informace o tom, že daný uživatel navštívil nějaké stránky a kdy byl daný záznam vytvořen, případně kdy se k němu naposledy přistupovalo.

Informace, které už mohou být relevantní pro útočníka, se nacházejí v souboru "Shortcuts". Zde 5.12 lze najít klíčová slova, která uživatel zadával do vyhledávače. Je tady záznam toho, jak se

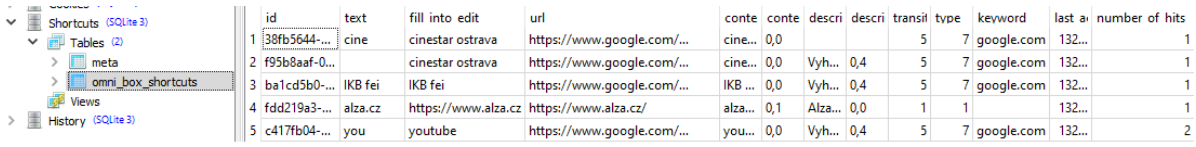
klíčové slovo nakonec přeložilo pro vyhledání i kolikrát bylo použito.



Obrázek 5.10: Ukázka obsahu Login Data - uživatelské účty



Obrázek 5.11: Ukázka obsahu Cookies



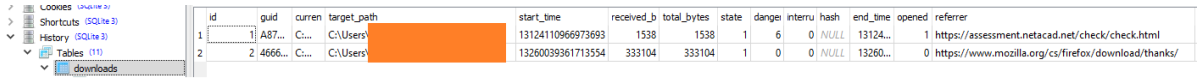
Obrázek 5.12: Ukázka obsahu Shortcuts - vyhledávaná klíčová slova

Data o navštívených stránkách jsou uložené v "History". Všechny navštívené stránky jsou uložené v tabulce s názvem "urls" 5.13. Je možné vyčíst, kolikrát byla navštívena daná stránka a kdy to bylo naposledy. Tabulka se jménem "downloads" 5.14 obsahuje všechny stažené soubory a informace (začátek stahování, cesta ke staženému souboru, velikost, zda byl soubor už otevřen, z jaké stránky byl stažen) k těmto záznamům. Vyhledávaná klíčová slova se nacházejí v tabulce "keyword_search_terms".

id	url	title	visit_count	typed_cou	last_visit_time
46	https://www.google.com/search?...	vsb - Hledat Googlem	2	0	13259953444139673
47	https://www.vsb.cz/	VŠB - Technická univerzita Ostrava - VŠB-TUO	1	0	13259953445043252
48	https://www.vsb.cz/cs/	VŠB - Technická univerzita Ostrava - VŠB-TUO	1	0	13259953445043252
49	https://www.vsb.cz/cs/student/	Informace pro naše studenty - VŠB-TUO	1	0	13259953448621995

Obrázek 5.13: Ukázka obsahu History - tabulka urls

Podrobnější informace o přehrávaných videozáznamech, hudbě a obrázcích jsou uloženy v souboru "Media history" 5.15.



Obrázek 5.14: Ukázka obsahu History - tabulka downloads

id	origin_id	url	duration_ms	position_m:	last_updated_	title	artist	album	source_title
1	1	https://www.youtube.com/watc...	86741	34693	13260039045	Harry Potter a zavřená škola 1	SMRTIJED		youtube.com
2	3	https://www.twitch.tv/	1073741824000	125	13260042944	Twitch			twitch.tv
3	3	https://www.twitch.tv/xnapycz	1073741824000	28018	13260042977	Xnapycz - Twitch			twitch.tv

Obrázek 5.15: Ukázka obsahu Media history - videa

"Web Data" je soubor, ve kterém se nacházejí další metadata jednotlivých navštívených webových stránek. Je možné zde najít e-mailovou adresu nebo adresu bydliště, jestliže ji uživatel vyplňoval v nějakém formuláři na internetu a tento formulář obsahoval tyto klíčová slova.

5.11 Užití System.Management v C#

Tato knihovna umožňuje přístup k informacím o správě systému, aplikacích a zařízeních, které jsou instrumentované v infrastruktuře služby WMI (Windows Management Instrumentation) [41]. Což je rozhraní pro správu dat a operací v operačních systémech Windows. Pomocí tohoto rozhrání se mohou psát skripty nebo aplikace pro automatizaci administrativních úkolů na vzdálených počítačích. WMI také dodává data pro správu do jiných částí operačního systému a produktů.

V aplikaci se využívá abstraktních tříd "Win32*"[43], které poskytují právě potřebné informace. Podrobnější seznam jmen, který obsahuje přes 340 různých těchto tříd, je možné najít zde [42]. V této kapitole budou popsány jen některé z nich (ty nejzajímavější z pohledu získaných informací) a jejich nejužitečnější atributy. Celá podrobná dokumentace je dostupná na stránkách Microsoftu [43].

Nejdůležitější je způsob, jakým je vůbec možné přistupovat k těmto strukturám. Následující kód 5.8 popisuje základní postup.

```
string MyKey = win32Class;
ManagementObjectSearcher searcher = new ManagementObjectSearcher("select * from "
    + MyKey);
foreach (ManagementObject share in searcher.Get()){
    foreach (PropertyData PC in share.Properties){
        if (PC.Value != null){
            if ((PC.Value.GetType().ToString()) == "System.String[]"){
                    Console.WriteLine(" " + PC.Name + " (System.String[]):");
                    String[] pole = (String[])PC.Value;
                    foreach (string item in pole){
                        Console.WriteLine("  " + item);
```

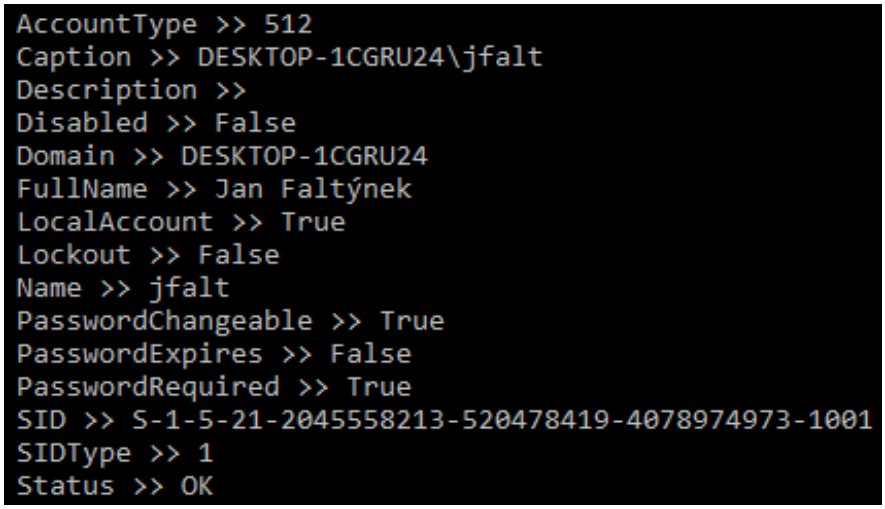
```
                    }
                }
                else{
                    Console.WriteLine(" " + PC.Name + " >> " + PC.Value);
                }
            }
        }
    }
```

Listing 5.8: Ukázka kódu na získání informací z Win32 třídy

Nyní budou následovat jednotlivé třídy a ukázky získaných informací z nich. Je nutné upozornit, že ne vždy bude ukázán celý výpis a tedy některé informace mohou chybět, jelikož se nezdály až tak užitečné, případně jejich hodnota byla Null.

5.11.1 Win32_Account

Tato abstraktní WMI třída obsahuje informace o účtech, které se nacházejí na operačním systému Windows.



Obrázek 5.16: Ukázka získaných dat z Win32_Account

Významné atributy:

- AccountType – identifikuje typ účtu (512 je číslo pro obyčejné uživatele, ale také admina a Guesta)
- Caption – popisek (jak je vidět, i z něho jde získat nějaká infromace)
- Domain – název domény Windows, do které skupina nebo uživatel patří
- FullName – jméno

- Lockout – jestli je uživateli zakázáno přistupovat k OS
- Name – uživatelské jméno (to, které se také používá v cestách k souborům)
- SID - security identifier je hodnota řetězce proměnné délky, která se používá k identifikaci důvěryhodnosti uživatele. Každý účet má jedinečný identifikátor SID, který vydá orgán, například doména Windows

Zde 5.16 se tedy dá zjistit, kteří uživatelé využívají počítač, nějaké jejich osobní informace a identifikátor SID, pomocí kterého by mělo být možné následně jednotlivé uživatele spojovat s jejich provedenými akcemi.

5.11.2 Win32_BaseService

Win32_Service zastupuje služby (service) v počítačovém systému Windows.

```
AcceptPause >> False
AcceptStop >> False
Caption >> Avast Antivirus
DisplayName >> Avast Antivirus
PathName >> "C:\Program Files\AVAST Software\Avast\AvastSvc.exe" /runassvc
ProcessId >> 3812
StartMode >> Auto
```

Obrázek 5.17: Ukázka získaných dat z Win32_BaseService

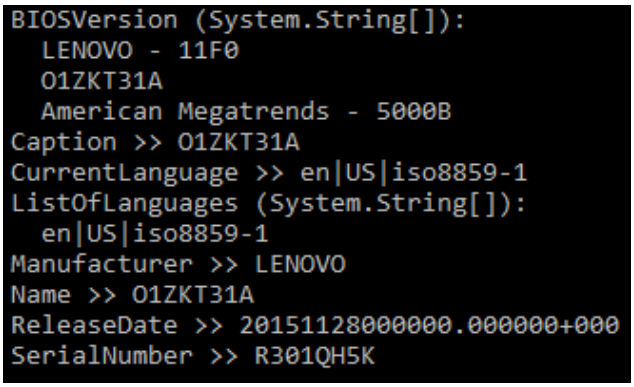
Významné atributy:

- AcceptPause – zda lze zastavit tento proces
- AcceptStop - zda lze vypnout tento proces
- Caption – popisek
- DisplayName – popis, co má služba dělat
- PathName – cesta k souboru
- ProcessID – ID procesu, pod kterým běží služba
- StartMode – jak se služba zapíná

Pomocí této třídy se dá zjistit informace 5.17 o všech službách, které jsou registrovány na daném zařízení a pomocí atributu DisplayName se většinou dá odvodit, za co daná služba odpovídá. Takhle se dají najít některé antivirové programy případně zálohovací nástroje. Pomocí ProcessID se dá například vynutit ukončení služby přes aplikaci, nebo dohledat další informace o tomto procesu.

5.11.3 Win32_BIOS

Reprezentuje atributy základních vstupních a výstupních služeb (BIOS) počítačového systému, které jsou nainstalovány v počítači.



Obrázek 5.18: Ukázka získaných dat z Win32_BIOS

Významné atributy:

- BIOSVersion – verze BIOSu
- Caption – popisek
- CurrentLanguage – využívaný jazyk
- ListOfLanguages – podporované jazyky
- Manufacturer – výrobce
- Name – jméno
- ReleaseDate - datum vydání systému BIOS ve formátu UTC
- SerialNumber – sériové číslo

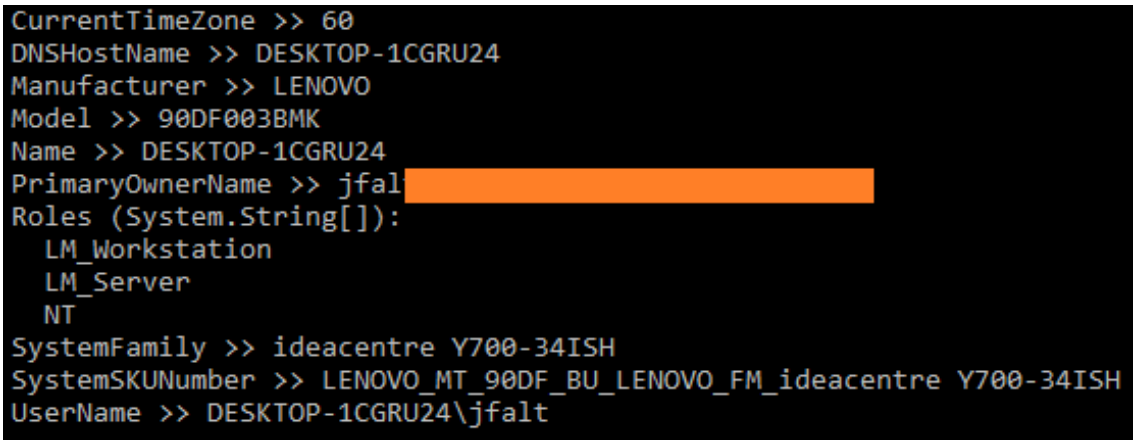
Lze zde získat základní informace 5.18 o BIOSu, tedy možná identifikace zařízení v síti na základě výrobce a sériového čísla, včetně jeho možného umístění podle podporovaných jazyků.

5.11.4 Win32_ComputerSystem

Základní informace o běžícím systému.

Významné atributy:

- CurrentTimeZone – časová zóna (0 + počet min)
- DNSHostName – název místního počítače podle DNS
- Manufacturer – výrobce
- Model – název produktu, který výrobce udal. Musí zde být vždy nějaká hodnota
- Name – název systému
- PrimaryOwnerName – vlastník
- Roles – jakou roli může zastávat tento systém
- SystemFamily – rodina produktů do které konkrétní počítač patří
- SystemSKUNumber – identifikuje konkrétní konfiguraci počítače k prodeji
- UserName – jméno přihlášeného uživatele

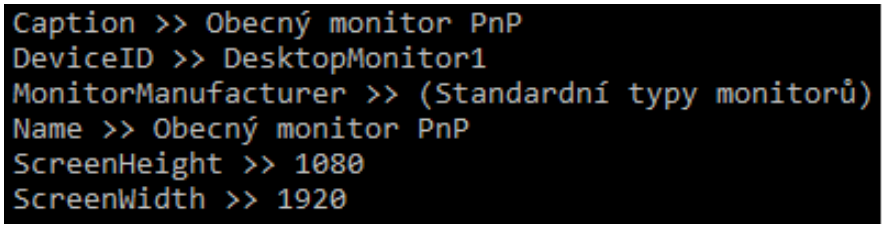


Obrázek 5.19: Ukázka získaných dat z Win32_ComputerSystem

Opět tu jsou informace 5.19, které dokážou určit, o jaké zařízení by se mělo jednat. Nejdůležitější informací však je, že se zde vyskytuje e-mailová adresa uživatele, který je označen jako vlastník. To vychází z nynějšího trendu Microsoftu, že se k přihlášení využívá právě e-mailová adresa.

5.11.5 Win32_DesktopMonitor

Popisuje monitor nebo display, který je připojen k počítačovému systému.



Obrázek 5.20: Ukázka získaných dat z Win32_DesktopMonitor

Významné atributy:

- Caption – popisek
- DeviceID – unikátní identifikátor monitoru z pohledu systému
- MonitorManufacturer – jméno výrobce
- Name – jméno
- ScreenHeight – rozlišení monitoru (výška)
- ScreenWidth – rozlišení monitoru (šířka)

Zde se dá zjistit 5.20, kolik monitorů je připojeno k počítači. Když se ve výpisu nebude vyskytovat žádný monitor, dá se předpokládat, že se jedná o server, což je indikace toho, že se na stroji mohou nacházet další důležitá data.

5.11.6 Win32_DiskDrive

Popisuje fyzické disky, které se nacházejí na počítači.

```
Caption >> ST2000DX001-SSHD-8GB
Description >> Disková jednotka
DeviceID >> \\.\PHYSICALDRIVE1
Manufacturer >> (Standardní diskové jednotky)
MediaType >> Fixed hard disk media
Model >> ST2000DX001-SSHD-8GB
SerialNumber >>             Z4Z3MNLF
Size >> 2000396321280

Caption >> WD My Passport 0730 USB Device
Description >> Disková jednotka
DeviceID >> \\.\PHYSICALDRIVE2
Manufacturer >> (Standardní diskové jednotky)
MediaType >> External hard disk media
Model >> WD My Passport 0730 USB Device
SerialNumber >> WXH1E31LTR81
Size >> 750120860160
```

Obrázek 5.21: Ukázka získaných dat z Win32_DiskDrive

Významné atributy:

- Caption – popisek
- Description – popis produktu
- DeviceID – unikátní identifikátor disku z pohledu systému
- Manufacturer – výrobce
- MediaType – udává typ zařízení
- Model – název modelu
- SerialNumber – sériové číslo
- Size – velikost disku

Díky této třídě se dá zjistit 5.21, kolik pevných disků se nachází na daném zařízení. Výpis obsahuje jak pevné disky, tak i externí disky a USB Flash disky. Což tedy dává informaci o tom, že jsou zde i další místa, kde by se mohly nacházet užitečná data.

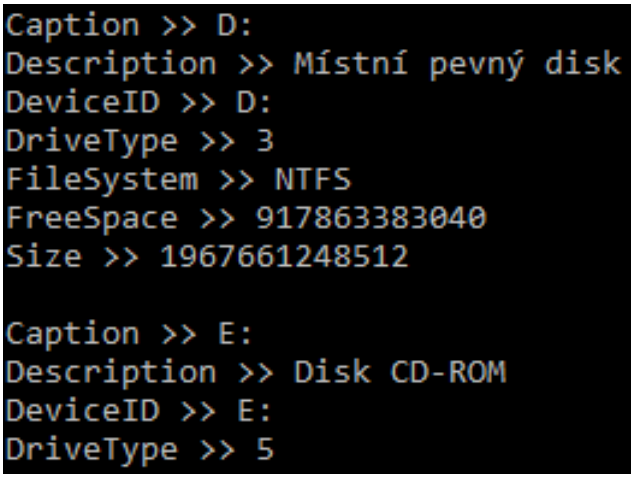
5.11.7 Win32_LogicalDisk

Obsahuje informace o logických discích na počítači.

Významné atributy:

- Caption – popisek
- Description – popis zařízení
- DeviceID – unikátní identifikátor logického disku z pohledu systému
- DriveType – informace o jaké zařízení se jedná
- FilySystem – jméno užívaného souborového systému diskem

- FreeSpace – volné místo
- Size – velikost disku

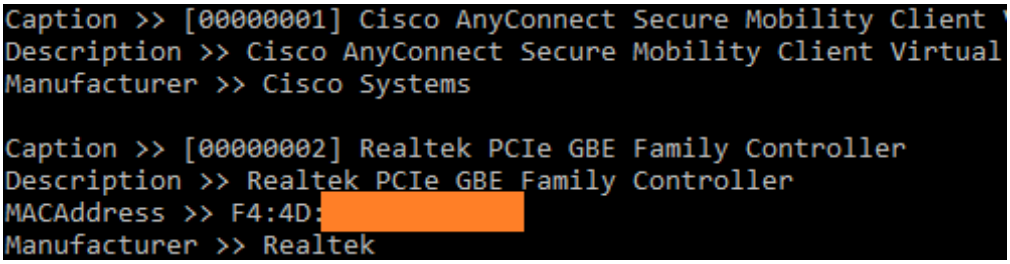


Obrázek 5.22: Ukázka získaných dat z Win32_LogicalDisk

Další informace 5.22 které pomohou zjistit, že jsou připojeny k počítači i jiná zařízení. Jsou zde informace jak o jejich cestě, tak se zde nachází jejich velikost a obsazení. Díky tomu se dá vyhodnotit, zda je potřeba procházet tato zařízení. V případě CD-ROM se dá dohledat, jestli je právě nějaké médium uvnitř.

5.11.8 Win32_NetworkAdapter

Umožňuje přístup k informacím o síťových adaptérech na zařízení.



Obrázek 5.23: Ukázka získaných dat z Win32_NetworkAdapter

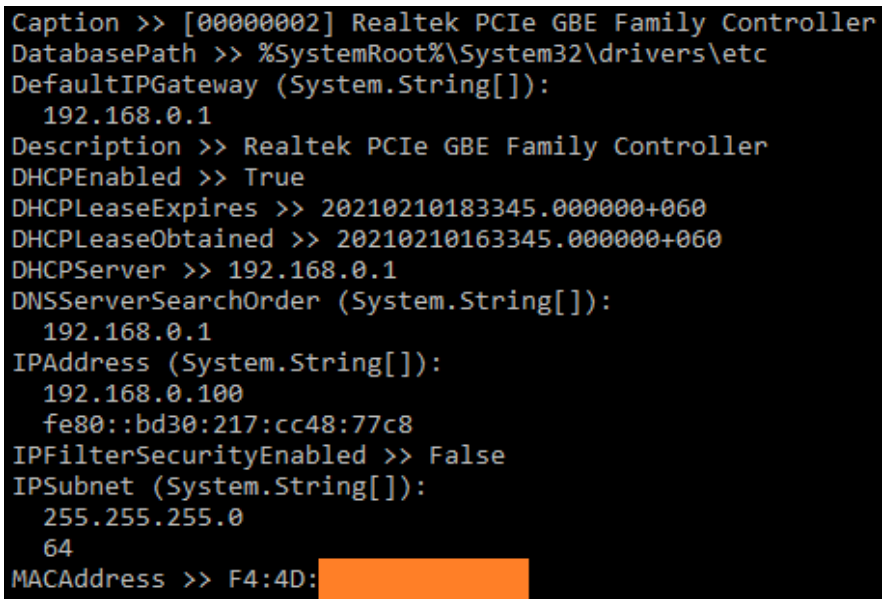
Významné atributy:

- Caption – popisek
- Description – popis produktu
- MACAddress – MAC Adresa zařízení
- Manufacturer – výrobce

Za pomocí informací 5.23 z této třídy se dá zjistit, jaké připojení (WiFi/kabel) k internetu dané zařízení využívá a jakou má MAC adresu. Také se zde vypíšou VPN adaptéry, takže se dá zjistit, jestli uživatel počítače využívá těchto služeb. Mimo jiné se zobrazí i rozhraní pro internet virtuálních strojů z aplikací, jako je například VirtualBox.

5.11.9 Win32_NetworkAdapterConfiguration

Popisuje atributy a chování jednotlivých síťových adaptérů.



Obrázek 5.24: Ukázka získaných dat z Win32_NetworkAdapterConfiguration

Významné atributy:

- Caption – popisek
- DatabasePath – cesta k internetovým databázovým souborům (HOSTS, LMHOSTS, NETWORKS a PROTOKOLY)
- DefaultIPGateway – výchozí IP adresa brány
- Description – popis produktu
- DHCPEnabled – zda je povoleno DHCP
- DHCPLeaseObtained – čas získání záznamu z DHCP
- DHCPLeaseExpires – platnost záznamu
- DHCPServer – IP adresa DHCP serveru
- DNSServerSearchOrder – Seznam DNS serverů
- IPAddress – IP adresa zařízení
- IPFilterSecurityEnabled – zda je na zařízení povolen IPSecPermit
- IPSubnet – v jakém subnetu se nachází IP adresa

- MACAddress – MAC Adresa zařízení

Je zde mnoho zajímavých informací 5.24, které se týkají síťového připojení. IP adresy DHCP a DNS serveru společné s bránou mohou prozradit hodně o sítí, jestliže by se jednalo například o firemní síť. Kdyby byl zapnut filtr, který využívá IPSecPermit, tak by se například mohl program adaptovat podle toho, jaký provoz by byl povolen, jelikož tato informace by se zde také nacházela.

5.11.10 Win32_NTEventlogFile

Obsahuje informace o souborech, které jsou známé jako Event logy [52].

```
Caption >> C:\WINDOWS\System32\Winevt\Logs\Application.evtx
Compressed >> True
CompressionMethod >> Compressed
Encrypted >> False
FileSize >> 20975616
LastAccessed >> 20210210181454.356166+060
LastModified >> 20210210181454.356166+060
Path >> \windows\system32\winevt\logs\
Sources (System.String[]):
  Application
  .NET Runtime
  .NET Runtime Optimization Service
  Application Error
```

Obrázek 5.25: Ukázka získaných dat z Win32_NTEventlogFile

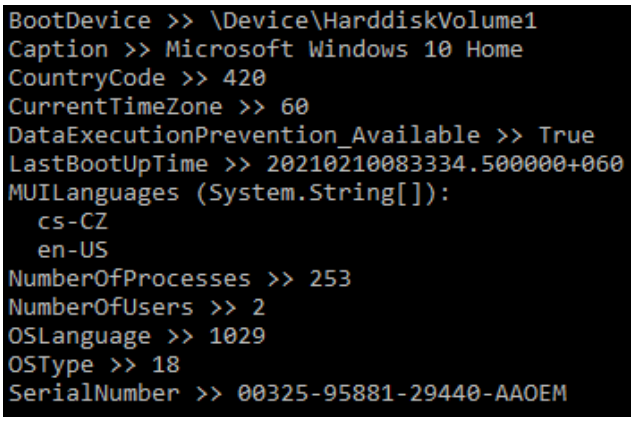
Významné atributy:

- Caption – popisek
- Compressed – zda jsou data komprimována
- CompressionMethod – jaká komprimační metoda byla využita
- Encrypted – jestli jsou data šifrována
- FileSize – velikost dat
- LastAccessed – poslední přístup k souboru
- LastModified – poslední modifikace souboru
- Path – cesta k souboru
- Sources – které aplikace zapisují do tohoto logu

Zde 5.25 se dá najít cesta k souborům, které obsahují různé chování jak uživatele samotného, tak i počítačového systému. Lze zjistit, zda se dá přistupovat k tomuto souboru a jaké aplikace do něj zapisují. Těchto souborů se v počítači nachází několik. Jeden je například speciálně pro Powershell.

5.11.11 Win32_OperatingSystem

Poskytuje informace od samotného operačního systému.



Obrázek 5.26: Ukázka získaných dat z Win32_OperatingSystem

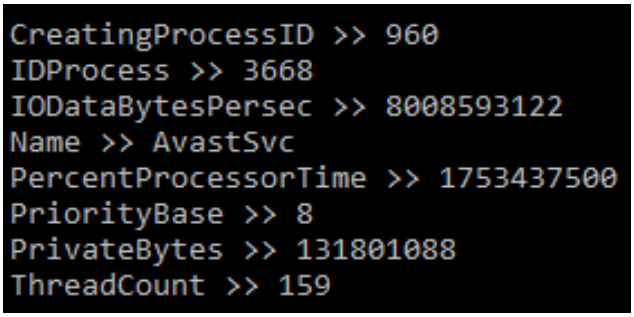
Významné atributy:

- BootDevice – místo ze kterého systém bootuje
- Caption – popisek
- CountryCode – kód země, ve které je registrován
- CurrentTimeZone – časová zóna (0 + počet min)
- DataExecutionPrevention_Available – když je hodnota True, tak je zaplá HW ochrana před Buffer Overrun útokem
- LastBootUpTime – čas posledního spuštění systému
- MUILanguages – instalované jazyky na počítači
- NumberOfProcesses – počet běžících procesů
- NumberOfUsers – počet uživatelů pro které nyní ukládá operační systém informace
- OSLanguage – jazyková verze operačního systému
- OSType – typ operačního systému
- SerialNumber – sériové číslo

Poskytuje mnoho informací 5.26, které naznačují, že by uživatel měl být z České Republiky, takže tu jsou data, které určitým způsobem lokalizují uživatele. Také jsou zde informace o nějakém bezpečnostním opatření (mohou být vypsány i další příznaky, které říkají, jestli je zapnuta nějaká další ochrana, tyhle však nejsou součástí ukázkového výpisu). Další zajímavá informace může být to, o jaký typ Windows se jedná. Jestli se nejedná o nějaký typ serveru.

5.11.12 Win32_PerfRawData_PerfProc_Process

PerfRawData poskytuje data o stavu systému a běžících aplikacích. V tomto případně jsou informace hlavně zaměřena na běžící procesy.



Obrázek 5.27: Ukázka získaných dat z Win32_PerfRawData_PerfProc_Process

Významné atributy:

- CreatingProcessID – ID procesu, které vytvořilo tento proces
- IDProcess – ID procesu
- IODataBytesPersec – průtok dat v bytech za sekundu
- Name – název procesu
- PercentProcessorTime – je to čas, po který všechna vlákna tohoto procesu používala procesor k provedení příkazů za 100 nanosekund
- PriorityBase – priorita procesu
- PrivateBytes – počet alokovaných bytů, které nesdílí s jiným procesem
- ThreadCount – počet vláken

Všechny procesy pod daným uživatelem lze na základě této třídy vidět 5.27. Jde získat povědomí o tom, které jsou důležité, případně na jakou aplikaci se dále zaměřit.

Velkou část duplicitních dat, které mají informace o aktuálních procesech lze najít i pomocí Win32_Process, obsahuje jen nepatrně víc dat a ty nejsou nijak zvlášť užitečné v tomto případě.

5.11.13 Win32_Processor

Obsahuje informace o procesoru.

Významné atributy:

- Caption – popisek
- L2CacheSize – velikost L2 cache v kB
- L3CacheSize – velikost L3 cache v kB
- Manufacturer – výrobce
- MaxClockSpeed – maximální rychlost procesrou v MHz

- Name – název
- NumberOfCores – počet jader
- SerialNumber – sériové číslo
- VirtualizationFirmwareEnabled – zda je zaplá podpora virtualizace

```
Caption >> Intel64 Family 6 Model 94 Stepping 3
L2CacheSize >> 1024
L3CacheSize >> 6144
Manufacturer >> GenuineIntel
MaxClockSpeed >> 3312
Name >> Intel(R) Core(TM) i5-6600 CPU @ 3.30GHz
NumberOfCores >> 4
SerialNumber >> To Be Filled By O.E.M.
VirtualizationFirmwareEnabled >> True
```

Obrázek 5.28: Ukázka získaných dat z Win32_Processor

Takhle se dají získat základní informace 5.28 o procesoru na daném systému Windows. Další informací je to, že systém podporuje virtualizaci, takže se na něm může nacházet virtuální stroj a to je potencionální zdroj informací k nalezení.

Taky je důležité si všimnout, že i u produktu, od kterého by uživatel čekal vysoký standart, není schopen systém načíst sériové číslo, takže se nedá vždy počítat s tím, že se sériová čísla objeví ve výpisu.

5.11.14 Win32_Product

Lze vyhledat informace o produktech, které byly instalované pomocí Windows Installeru. Takže se zde nemusí nacházet úplně každá nainstalovaná aplikace, například Mozilla Firefox se neobjevila mezi těmito položkami.

```
Description >> Cisco AnyConnect Secure Mobility Client
IdentifyingNumber >> {C1F2A6F4-89D5-459A-B39A-EF5BE4472CB9}
InstallDate >> 20200109
InstallSource >> C:\WINDOWS\TEMP\Cisco\Installer\4472CB9\
Name >> Cisco AnyConnect Secure Mobility Client
URLInfoAbout >> http://www.cisco.com
Vendor >> Cisco Systems, Inc.
```

Obrázek 5.29: Ukázka získaných dat z Win32_Product

Významné atributy:

- Descripition – popis produktu
- IdentifyingNumber – něco jako sériové číslo pro SW
- InstallDate – datum, kdy se daný produkt nainstaloval
- InstallSource – místo, odkud se instaloval SW

- Name – jméno produktu
- URLInfoAbout – odkaz na informace o produktu
- Vendor – prodejce produktu

Na základě informací 5.29 o tom, jaké produkty jsou nainstalované, se dá například následně vyhledat, jestli mají na nějaké verzi známé bezpečnostní díry, případně jestli nesbírají samy o sobě data, které by měly hodnotu. Taky je to jedna z cest, jak zjistit, zda je přítomen antivirus na daném zařízení.

5.11.15 Další zajímavé Win32 třídy

Jak bylo již zmíněno, existuje zde mnoho těchto tříd, které se dají procházet zmíněnou metodou. Některé však nemusí být tolik zajímavé, ale přesto bude o nich malá zmínka, co se v nich dá najít.

- Win32_MotherboardDevice – informace o základní desce
- Win32_NetworkLoginProfile – informace o uživatelích, co mohou dělat (diskové kvóty, omezení časového přístupu), jestliže se jedná o server a oni využívají vzdáleného připojení
- Win32_NTLogEvent – lze získat informace o logu (jen některé typy), včetně jejich celé zprávy (čeho se událost týkala, jak byla vyřešena)
- Win32_PerfRawData_PerfDisk_PhysicalDisk – informace o vytížení a rychlosti disků
- Win32_PerfRawData_PerfOS_Objects – počet aktuálních vláken, procesů a semaforů v systému
- Win32_PerfRawData_Tcpip_NetworkInterface – informace o jednotlivých interface, kolik jimi protéká dat
- Win32_PhysicalMemory – informace o RAMce
- Win32_Printer – informace o tiskárně, často včetně IP adresy
- Win32_QuickFixEngineering – obsahuje informace o HotFixech (velké aktualizace nikoliv), avšak i tak se dá poznat, jestli se daný stroj udržuje aktualizovaný
- Win32_SoundDevice – informace o zvukových zařízeních
- Win32_SystemEnclosure – informace o skříni počítače
- Win32_VideoController – informace o grafické kartě

5.11.16 Velikost získaných dat

Základem dobrého spyware je nenápadnost a toho se týká jak využití výpočetních prostředků daného systému, tak i velikost přenášených dat.

Během testu žádná z komponent (informace získaných z jednotlivých tříd), které obsahovali informace o HW, nepřekročila hranici 10 MB v paměti a procesor vytěžovala na jedno procento. Soubor, který pak obsahuje všechny základní informace o HW, měl velikost 4,1 kB.

Velikost souboru, který obsahoval navíc informace o uživatelích, síťový interface, počítačovém systému a širší informace o HW měl pak 51 kB, ale výpočetní požadavky zůstaly stejné.

Ovšem když se začaly získávat navíc i informace o jednotlivých procesech, službách a hlavně nainstalovaných produktech, tak paměťové nároky šly výrazně nahoru, místy bylo potřeba až 200 MB v RAMce a to byl nárok jen pro čtení a zápis získaných informací, žádné posílání dat přes síť, nebo jejich analýza. Výsledný soubor pak měl velikost 1,5 MB. Alespoň procesor byl stále minimálně vytěžován.

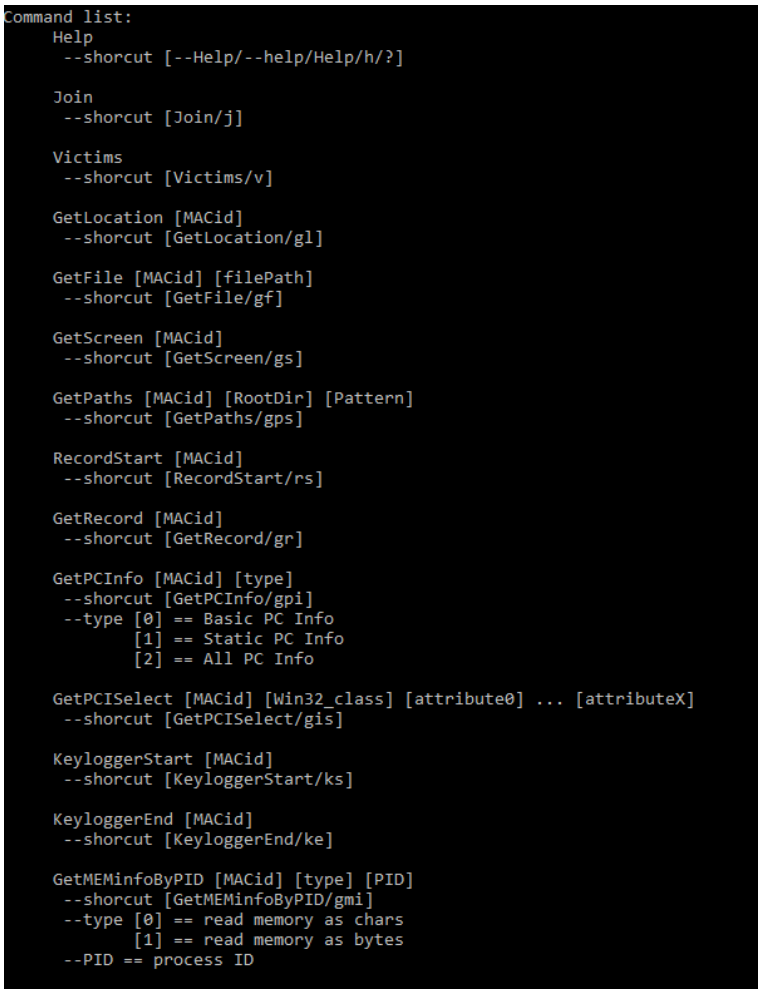
5.12 Příkazy pro Klientskou část

Zde budou popsány příkazy, které mohou být prostřednictvím aplikace požadovány. Na obrázku 5.30 je vidět výpis "Help" ze samotné aplikace. Všechny příkazy mají svou zkratku, která je vždy popsána za klíčovým slovem "shorcut". Například příkaz "Victim" jde zkrátit jen na "v" při zápisu do konzole. Dále pak obsahují v hranatých závorkách potřebné parametry, aby se mohly vykonat. Všechny příkazy, které mají ovládat nějakým způsobem vzdálené stroje, mají jako první parametr "MACid", aby bylo možné určit, pro který stroj je tento příkaz platný.

5.12.1 Příkazy

- Help – vypíše list příkazů
- Join – úvodní příkaz, aby se aplikace připojila k serveru
- Victims – vrátí seznam MAC adres, které jsou zaregistrované na serveru, a tím pádem je možné jim zadávat příkazy
- GetLocation – vrátí seznam ID routerů v okolí napadeného počítače, jestliže má WiFi kartu
- GetFile – stáhne zadaný soubor
- GetScreen – pořídí snímek obrazovky a stáhne jej do adresáře útočníka
- GetPaths – vytvoří seznam souborů, který odpovídá parametrům
- RecordStart – začne nahrávat zvuk
- GetRecord – zastaví nahrávání a vrátí soubor se zvukovou stopou
- GetPCInfo – vrátí informace o počítači dle předdefinovaných pravidel
- GetPCISelect – vrátí informace o počítači podobně jako GetPCInfo, ale je zde možnost vlastní konfigurace
- KeyloggerStart – začne sledování zmáčknutých kláves

- KeyloggerEnd – zastaví sledování kláves a vrátí soubor, který obsahuje záznam stisknutých kláves
- GetMEMinfoByPID – vrátí obsah paměti pro daný proces



Obrázek 5.30: Výpis helpu z Klient aplikace

5.13 Problémy a návrhy zlepšení

Implementované řešení záměrně neobsahuje žádný způsob toho, aby Victim část byla schopna sama sebe spustit při spuštění systému. Jeden důvod je ten, že v kombinaci s metodami, které jsou využívány pro zisk dat, by to jistě zapříčinilo to, že by je díky tomu antivirus označoval za spyware. Druhým důvodem je nutnost si uvědomit, že celá "Command" třída, může být třeba jen součástí nějaké knihovny, která může být následně využita naprosto neškodnou aplikací. Tímto způsobem jde zařídit, že díky jiné aplikaci se bude spouštět i škodlivý kód.

Důležitější část, která nebyla implementována, je zametání stop na operačním systému. Jak již bylo řečeno, operační systém si dělá poznámky do logovacích souborů o tom, která aplikace co dělá během jejího běhu, aby bylo právě možné zjistit, jestli se neděje něco, co není zamýšleno.

Chybí také větší samostatnost Victim části. Téměř všechny akce se dějí na popud útočníka, což bylo cílem, ovšem mohlo by zde být rozšíření, které například na základě zjištěných informací bude pouštět další moduly naprosto samo a až po nějakém čase zašle výsledky.

5.13.1 Užití neuronových sítí

Právě při vytváření části, která by se měla rozhodovat podle získaných dat, by se mohla využívat neuronová síť [50]. Ta by na základě natrénovaných vstupů mohla ovládat celý chod tohoto modulu. Spouštět například keylogger tehdy, když by modul získal informaci o tom, že jeden z běžících procesů je internetový prohlížeč. Nebo spouštět náročnější metody jen tehdy, když není plně vytěžován počítač jinou aplikací. Hodně zajímavé by mohlo být to, že na základě zjištění jaký antivirus se nachází na daném zařízení, by se spouštěly jen ty metody, které byly otestovány, že je daný antivir nezachytí.

Další typickou úlohou na využití neuronových sítí by byly právě snímky obrazovky. Aplikace obsahuje metodu pro získání snímku obrazovky, ale jak bylo upozorněno, ne vždy se na něm musí nacházet něco zajímavého a s tím by mohly právě pomoct tyto sítě.

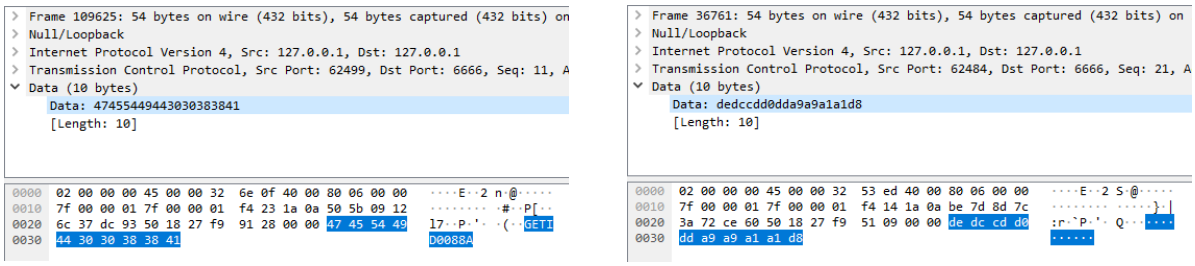
Kapitola 6

Testování aplikací

První test je zaměřen na komunikaci mezi jednotlivými částmi a na jejich šifrovanou formu. Pomocí aplikace Wireshark [51] byly otestovány jednotlivé pakety a na obrázku 6.1b jde vidět, že šifrování zpráv fungovalo, když bylo zapnuté. Ve druhém případě 6.1a jde přečíst celý příkaz "GETID0088A". V obou případech byla zaslána totožná zpráva.

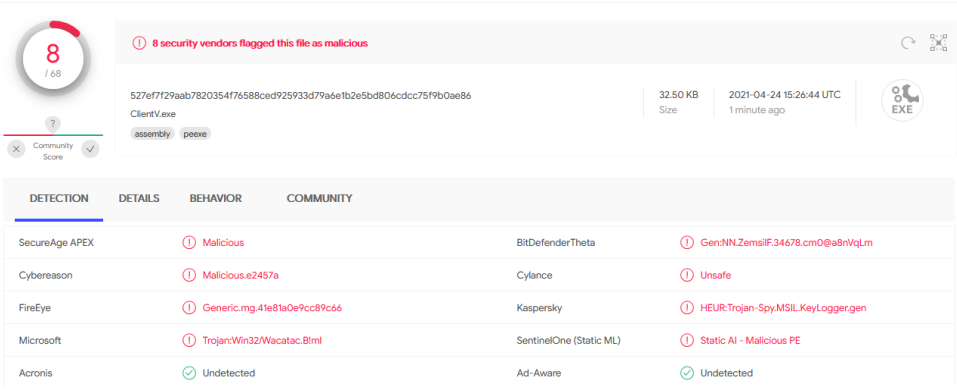
Další sada testů byla zaměřena na kontrolu, které antivirové programy vyhodnotí implementovanou aplikaci "Victim" jako hrozbu. Na obrázku se objevuje jméno souboru "ClientV" namísto Victim, což je z toho důvodu, aby jej neoznačovaly antiviry za malware jen na základě jména. Mnoho proměnných v samotném kódu je upraveno tak, aby nepoutaly pozornost. Veškeré tyto testy byly vytvořeny za pomoci stránky Virustotal [49].

Na obrázku 6.2 je vidět analýza naprogramovaného řešení, které obsahuje všechny moduly, které byly popsány v této práci. Jak je vidět, tak 8 antivirů z 68 možných nakonec vyhodnotily celé řešení za hrozbu. Tohle bylo kompletně funkční řešení. Pak byla provedena jen malá změna v hlavním modulu a to ta, že jediné co se zavolalo, byl výpis textu do konzole a aplikace se ukončila. Žádný pokus o spojení ani snaha o získání dat. Ale kód stále obsahoval všechny implementované metody, jen se tedy nevolaly. Tady bylo 6 pozitivních z 68. To může znamenat, že jednotlivé antivirové programy buď různě testují, nebo rozdílně vyhodnocují.



(a) Vyplé šifrování (b) Zaplé šifrování

Obrázek 6.1: Ověření šifrování zpráv ve Wiresharku



Obrázek 6.2: Testování výsledné aplikace na Virustotal

Tabulka 6.1: Tabulka reprezentující výsledky na stránce Virustotal pro jednotlivé příkazy

Příkaz	Počet pozitivních	Počet negativních
GetFile	1	67
GetLocation	1	67
GetMEMinfoByPID	3	65
GetPaths	1	67
GetPCInfo + GetPCISelect	3	65
GetScreen	1	67
KeyloggerStart + KeyloggerEnd	7	61
RecordStart + GetRecord	2	66

V této tabulce 6.1 jsou porovnány výsledky, jak užití různých implementovaných metod ovlivňuje výsledek testu. Součásti testovaného řešení byla vždy plně funkční komunikace plus jedna vybraná metoda. Úplně jako první byla vyzkoušena aplikace, která byla schopná jen komunikace, ale neobsahovala žádnou metodu pro získání dat. Na tuto verzi reagoval pozitivně jeden antivirus, a proto je výsledek malinko zkreslen, jelikož tento antivirus se díky této situaci objevoval při každém testu jako pozitivní.

Všechny antivirové programy nemusí být úplně aktuální na stránce Virustotal, případně nemusí obsahovat všechny své funkcionální moduly. Ale i tak poskytuje tabulka přehled o tom, jak by nasazení takovéhoto spywaru mohlo dopadnout.

Kapitola 7

Závěr

První část práce se zabývala seznámením se spywarem. Byly popsány jeho základní typy, způsoby jakými se může dostat do počítače, současní zástupci a jak maximálně snížit riziko, aby se takový program dostal do systému.

Následovala sekce, která se zabývala sociálními sítěmi a IoT zařízeními. Tato témata byly zmíněné proto, že se jich taky dotýká ochrana osobních dat a je důležité, aby si uživatelé těchto služeb uvědomovali rizika.

Největší důraz pak byl kladen na demonstraci principů spyware pomocí implementovaných tří aplikací, které společně spolupracují. Do první aplikace se zadávají příkazy, které putují přes serverovou část, kde jsou následně přeposlány na cílovou oběť podle MAC adresy. Když přijde příkaz do třetí aplikace (spyware), ta na jeho základě získá požadovaná data a pošle je zpět do první aplikace přes server.

Spyware aplikace má několik základních funkcí. Nejdůležitější je schopnost posílat z napadeného počítače soubory. Tohle umožňuje krást například kancelářské dokumenty. Dále se tato funkcionalita využívá, když je výstupem implementovaného modulu soubor. Pak se tento získaný soubor pošle stejnou metodou útočníkovi. Dále aplikace obsahuje nástroje pro odposlech zvuku a získání snímku obrazovky. V rámci keyloggeru je řešen problém rozpoznání velkého a malého písmene při stisknutí klávesy. Je zde metoda pro získání geografické polohy na základě informací z WiFi karty. Spyware je schopen číst paměť jiného procesu na daném zařízení. Součástí je i modul, který umožňuje zisk informací ze tříd, které využívají Windows Management Instrumentation rozhraní. Díky tomuto modulu má útočník přístup k velkému množství informací, které jsou statické (HW komponenty) i dynamické (běžící procesy, instalované programy, připojená zařízení atd.). Problémy a návrhy zlepšení jsou popsány zde 5.13.

V minulých letech byla již napsána práce [57], která se zabývala spywarem. Její teoretická část se zabývala mimo jiné právními normami, které umožňují některým státům nasazovat tento druh softwaru jako obranou zbraň. Oproti tomu tato práce se v teoretické rovině zaměřila na sociální sítě a IoT zařízení. Aplikace, která je implementována v rámci této práce, obsahuje několik funkcí (zís-

kání geografické polohy za pomocí WiFi karty, čtení paměti jiného procesu), které nebyly ve zmíněné práci implementovány. Tato práce obsahuje navíc popisy souborů internetových prohlížečů (Mozilla Firefox , Google Chrome) a správu jejich uložených hesel. Přínos této práce je také v popisu jednotlivých tříd, které je možné využít k zisku informací o systému Windows.

Možnosti Spywaru jsou velké, jelikož to jsou ve finále aplikace, které využívají toho, že musí existovat způsob, jak se ke všem zdrojům dat na počítač dá přistoupit. Kdyby tomu tak nebylo, tak ani obyčejné aplikace, které mají třeba právě funkci diagnostiky, by nemohly fungovat. Rozdíl mezi aplikací, která je užitečná a žádaná, oproti aplikaci, která funguje jako spyware může být z pohledu kódu velmi malý. Například aplikace, která zprostředkovává informace o hardwaru počítače a zároveň obsahuje nějakou síťovou komunikaci v případě, že dojde k chybě v programu, aby mohla být tato chyba odstraněna. Takováto aplikace získává informace a dokonce posílá v jistých případech někam přes internet zprávy, ale pořád se nejedná o spyware. Stačí, aby se přidala do těchto zpráv o chybách informace, která není nutná pro řešení problému a najednou se může jednat o spyware. Tady tato úvaha mimo jiné ukazuje, jak to mohou mít antivirové společnosti těžké, aby určily, která aplikace je škodlivá a která nikoliv.

Omezení Spywaru jsou pak tedy hlavně na straně uživatele. Jestliže bude například spouštět bez rozmyšlení každou aplikaci jako správce, když to vyžaduje, tak najednou se otevřela velmi jednoduchá cesta do celého systému a nebylo potřeba žádným zásadním způsobem obcházet zabezpečení, které mají implementované operační systémy. Další velkou překážkou může být antivirus, ale jestliže to bude nějaký cílený útok, jak šlo vidět i z výsledků testů 6.1, tak i ten nemusí stačit.

Literatura

[1] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.

[2] KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČOVÁ a Martin KUNC. CyberSecurity. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

[3] Kyberšikana. Internetem bezpečně [online]. [cit. 2021-4-27]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/

[4] Sdělení č. 104/2013 Sb. m. s. ZÁKONY PRO LIDI [online]. [cit. 2021-4-27]. Dostupné z: https://www.zakonyprolidi.cz/ms/2013-104

[5] Lifecycle FAQ - Windows. Microsoft [online]. 2016 [cit. 2021-4-27]. Dostupné z: https://docs.microsoft.com/cs-cz/lifecycle/faq/windows

[6] The Past and Present State of Spyware. Finjan [online]. 2016 [cit. 2021-4-27]. Dostupné z: https://blog.finjan.com/the-past-and-present-state-of-spyware/

[7] OptOut. Gibson Research Corporation [online]. [cit. 2021-4-27]. Dostupné z: https://www.grc.com/optout.htm

[8] What are browser hijackers? Norton [online]. [cit. 2021-4-27]. Dostupné z: https://us.norton.com/internetsecurity-malware-what-are-browser-hijackers.html

[9] Spyware. Mcgill [online]. [cit. 2021-4-27]. Dostupné z: https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/s/Spyware.htm

[10] DOEVAN, Jake. Remove CoolWebSearch. 2-spyware [online]. [cit. 2021-4-27]. Dostupné z: https://www.2-spyware.com/remove-coolwebsearch.html

[11] KOMÁREK, Josef. Morpheus 3 Beta. Technet [online]. 2003 [cit. 2021-4-27]. Dostupné z: https://www.idnes.cz/technet/software/morpheus-3-beta-bastl-pro-sit-gnutella-preplneny-spywarem-recenze.A030305_5203587_software

[12] DOEVAN, Jake. Remove DyFuCa. 2-spyware [online]. 2018 [cit. 2021-4-27]. Dostupné z: https://www.2-spyware.com/remove-dyfuca.html

[13] Look2Me. F-Secure [online]. [cit. 2021-4-27]. Dostupné z: https://www.f-secure.com/sw-desc/look2me.shtml

[14] Ramnit. F-Secure [online]. [cit. 2021-4-27]. Dostupné z: https://www.f-secure.com/v-descs/virus_w32_ramnit.shtml

[15] Trojan-Spy:W32/Zbot. F-Secure [online]. [cit. 2021-4-27]. Dostupné z: https://www.f-secure.com/v-descs/trojan-spy_w32_zbot.shtml

[16] Protection Bulletin. Broadcom [online]. [cit. 2021-4-27]. Dostupné z: https://www.broadcom.com/support/security-center/protection-bulletin

[17] Botnet. Internetem bezpečně [online]. [cit. 2021-4-27]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/

[18] FinFisher. FinFisher [online]. [cit. 2021-4-27]. Dostupné z: https://finfisher.com/FinFisher/index.html

[19] Cellebrite [online]. [cit. 2021-4-27]. Dostupné z: https://www.cellebrite.com/en/law-enforcement/

[20] Kali Linux. Kali [online]. [cit. 2021-4-27]. Dostupné z: https://www.kali.org/

[21] Kali Linux Tools Listing. Kali [online]. [cit. 2021-4-27]. Dostupné z: https://tools.kali.org/tools-listing

[22] SVOBODA, Jakub a Martin PROCHÁZKA. Home office: nový standard. Novinky.cz [online]. 2020 [cit. 2021-4-27]. Dostupné z: https://www.novinky.cz/finance/clanek/home-office-novy-standard-40328602

[23] STRÁNSKÝ, Petr. Co se skrývá za magickou formulí ActiveX. Computerworld [online]. 1998 [cit. 2021-4-27]. Dostupné z: https://computerworld.cz/archiv/co-se-skryva-za-magickou-formuli-activex-10566

[24] GILLIS, Alexander. Spyware. TechTarget [online]. 2019 [cit. 2021-4-27]. Dostupné z: https://searchsecurity.techtarget.com/definition/spyware

[25] BITTO, Ondřej. Cookies: Co jsou a jak na ně? Živě.cz [online]. 2012 [cit. 2021-4-27]. Dostupné z: https://jnp.zive.cz/cookies-co-jsou-a-jak-na-ne

[26] KENTON, Will. Social Networking. Investopedia [online]. 2021 [cit. 2021-4-27]. Dostupné z: https://www.investopedia.com/terms/s/social-networking.asp

[27] PRINDÍK, Jan. Facebook-a-jeho-strucna-historie. Proexperty [online]. [cit. 2021-4-27]. Dostupné z: http://www.proexperty.cz/web-2-0/socialni-site/105-5-1-facebook-a-jeho-strucna-historie

[28] PTÁČEK, Michal. Jak vznikl a následně uspěl Instagram. Czechcrunch [online]. 2015 [cit. 2021-4-27]. Dostupné z: https://www.czechcrunch.cz/2015/07/jak-vznikl-a-nasledne-uspel

[29] Co je IoT? IoT Portál [online]. [cit. 2021-4-27]. Dostupné z: https://www.iot-portal.cz/co-je-iot/

[30] Co je cloud? Microsoft Azure [online]. [cit. 2021-4-27]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-the-cloud/

[31] Vytvoření a uložení všech maker do jednoho sešitu. Microsoft [online]. [cit. 2021-4-27]. Dostupné z: https://support.microsoft.com/cs-cz/office/vytvo%C5o%99eno%C3o%AD-a-uloo%C5o%BEeno%C3o%AD-vo%C5o%A1ech-maker-do-jednoho-seo%C5o%A1itu-66c97ab3-11c2-44db-b021-ae005a9bc790

[32] ARPANET, předchůdce internetu, byl spuštěn před 50 lety. ITBIZ [online]. [cit. 2021-4-27]. Dostupné z: https://www.itbiz.cz/zpravicky/arpanet-predchudce-internetu-byl-spusten-pred-50-lety

[33] STRNAD, Michal. Třetí zranitelnost v Adobe Flash Player za poslední měsíc. Root.cz [online]. 2015 [cit. 2021-4-27]. Dostupné z: https://www.root.cz/zpravicky/treti-zranitelnost-v-adobe-flash-player-za-posledni-mesic/

[34] KHOSROWSHAHI, Dara. 2016 Data Security Incident. Uber [online]. [cit. 2021-4-27]. Dostupné z: https://www.uber.com/en-CA/newsroom/2016-data-incident/

[35] FIŠER, Miloslav. Čechy terorizuje spyware. Jak se bránit? Novinky.cz [online]. 2021 [cit. 2021-4-27]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/cechy-terorizuje-spyware-jak-se-branit-40354675#seq_no=8&dop_ab_variant=0&dop_source_zone_name=novinky.web.nexttoart&dop_req_id=bFlL3x67iBR-202103220957&source=article-detail

[36] Smart home IP camera shipments worldwide from 2012 to 2019. Statista [online]. [cit. 2021-4-27]. Dostupné z: https://www.statista.com/statistics/486027/smart-home-ip-camera-shipments-worldwide/

[37] TCP. Root.cz [online]. [cit. 2021-4-27]. Dostupné z: https://www.root.cz/slovnicek/tcp/

[38] Gmail API. Google [online]. [cit. 2021-4-27]. Dostupné z: https://developers.google.com/gmail/api/quickstart/dotnet

[39] Geolocation API. Google [online]. [cit. 2021-4-27]. Dostupné z: https://developers.google.com/maps/documentation/geolocation/overview

[40] Obecná struktura PE souboru. Builder.cz [online]. 2001 [cit. 2021-4-27]. Dostupné z: https://www.builder.cz/rubriky/assembler/obecna-struktura-pe-souboru-155818cz

[41] Windows Management Instrumentation. Microsoft [online]. 2018 [cit. 2021-4-27]. Dostupné z: https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

[42] SHIRAZI, Alireza. How To Get Hardware Information. Codeproject [online]. 2008 [cit. 2021-4-27]. Dostupné z: https://www.codeproject.com/Articles/17973/How-To-Get-Hardware-Information-CPU-ID-MainBoard-I

[43] Build desktop Windows apps using the Win32 API. Microsoft [online]. [cit. 2021-4-27]. Dostupné z: https://docs.microsoft.com/en-us/windows/win32/

[44] Ochrana uložených přihlašovacích údajů pomocí hlavního hesla. Mozilla [online]. [cit. 2021-4-27].https://support.mozilla.org/cs/kb/ochrana-ulozenych-prihlasovacich-udaju-pomoci-hlav

[45] Profily – místo, kde Firefox uchovává záložky, hesla a další data uživatele. Mozilla [online]. [cit. 2021-4-27]. Dostupné z: https://support.mozilla.org/cs/kb/profily-misto-kde-firefox-uchovava-zalozky-hesla-d?redirectslug=Profiles&redirectlocale=en-US

[46] How does Google Chrome store passwords? Superuser [online]. 2010 [cit. 2021-4-27]. Dostupné z: https://superuser.com/questions/146742/how-does-google-chrome-store-passwords

[47] Virtual address spaces. Microsoft [online]. 2020 [cit. 2021-4-27]. Dostupné z: https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/virtual-address-spaces

[48] RUSSINOVICH, Mark. Strings v2.53. Microsoft [online]. 2016 [cit. 2021-4-27]. Dostupné z: https://docs.microsoft.com/en-us/sysinternals/downloads/strings

[49] VirusTotal [online]. [cit. 2021-4-27]. Dostupné z: https://www.virustotal.com/gui/

[50] DURČÁK, Pavel. Neuronové sítě a princip jejich fungování. Builder.cz [online]. 2017 [cit. 2021-4-27]. Dostupné z: https://www.napocitaci.cz/33/neuronove-site-a-princip-jejich-fungovani

[51] Wireshark [online]. [cit. 2021-4-27]. Dostupné z: https://www.wireshark.org/

[52] HOFFMAN, Chris. What Is the Windows Event Viewer, and How Can I Use It? Howtogeek [online]. [cit. 2021-4-27]. Dostupné z: https://www.howtogeek.com/123646/htg-explains-what-the-windows-event-viewer-is-and-how-you-can-use-it/

[53] Cost of a Data Breach Report 2020: IBM Security [online]. In: . 2020, s. 0-81 [cit. 2021-4-27]. Dostupné z: https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[54] 2021 DATA RISK REPORT FINANCIAL SERVICES: Varonis [online]. In: . 2021, s. 1-8 [cit. 2021-4-27]. Dostupné z: https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf?utm_content=146358482&utm_medium=social&utm_source=twitter&hss_channel=tw-21672993

[55] EGELE, Manuel, Christopher KRUEGEL, Engin KIRDA, Heng YIN a Dawn SONG. Dynamic Spyware Analysis [online]. 2007 [cit. 2021-4-27]. Dostupné z: https://www.researchgate.net/publication/220881097_Dynamic_Spyware_Analysis

[56] GRIBBLE, Steven, Alex MOSHCHUK, Tanya BRAGIN a Henry LEVY. A Crawler-based Study of Spyware on the Web. NDSS Symposium 2006 [online]. 2006 [cit. 2021-4-27]. Dostupné z: https://www.ndss-symposium.org/ndss2006/crawler-based-study-spyware-web/

[57] KAFKA, Radim. Spyware: design, struktura a funkcionalita [online]. Ostrava, 2020 [cit. 2021-4-27]. Dostupné z: http://hdl.handle.net/10084/140536. Diplomová práce. Vysoká škola báňská - Technická univerzita Ostrava.

Seznam příloh

Příloha A

Příloha v IS EDISON

Adresářová struktura souborů v příloze v IS EDISON vypadá takto.

```
KlientApp
    examples.txt
    OutputBasicHWinfo.txt
    Program.cs
    test.json
ServerApp
    Program.cs
VictimApp
    Commands.cs
    ComputerInfo.cs
    Keyboard.cs
    Program.cs
    ReadM.cs
```

Ve složce KlientApp se nachází zdrojový kód (Program.cs) pro tuto apliakci. Následně ukázkový výsledek (OutputBasicHWinfo.txt) pro získání informací za pomoci příkazu GetPCInfo. Soubor (examples.txt) ukazuje vzorové příkazy pro užití aplikace. Soubor (test.json) je pro počáteční otestování Google API.

Ve složce ServerApp je jen zdrojový kód (Program.cs) pro Server aplikaci.

Poslední složka (VictimApp) obsahuje zdrojové kódy (Commands.cs, ComputerInfo.cs, Keyboard.cs, Program.cs, ReadM.cs) potřebné pro sestavení Victim aplikace.