Bezpečnosť a možnosti zachovania anonymity na Internete

Filip Mazúr

Bakalářská práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Filip Mazúr**
Osobní číslo:	**A13235**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost a možnosti zachování anonymity na Internetu**
Téma anglicky:	**Security and Anonymity on the Internet**

Zásady pro vypracování:

1. **Proveďte rešerši na téma bezpečnosti na Internetu, zaměřte se na zachování anonymity.**
2. **Prozkoumejte a popište nejzranitelnější místa v počítači.**
3. **Analyzujte nejčastější hrozby, které mohou vézt ke ztrátě osobních údajů.**
4. **Popište nejčastější chyby, které uživatelé dělají na Internetu vedoucí ke ztrátě osobních údajů.**
5. **Popište a prakticky otestujte nástroje, které se dají použít pro zachování anonymity na Internetu.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. První vydání. Praha: Grada Publishing, a.s., 2015, 183 stran. ISBN 978-80-247-5453-6.**
2. **SZOR, Peter. Počítačové viry: analýza útoku a obrana. Vyd. 1. Brno: Zoner Press, 2006, 608 s. ISBN 80-86815-04-8.**
3. **PETROWSKI, Thorsten. Bezpečí na internetu: pro všechny. Vyd. 1. Liberec: Dialog, 2014, 243 s. ISBN 978-80-7424-066-9.**
4. **SINGER, P. Cybersecurity and cyberwar: what everyone needs to know. Oxford: Oxford University Press, 2014, viii, 306 s. ISBN 978-0-19-991811-9.**
5. **BAILEY, Matt. Complete Guide to Internet Privacy, Anonymity & Security: Fully updated and revised for 2015. 23.12.2014. USA: Nerel publication, 2011, 304 s. ISBN 978-3-9503093-3-1.**

Vedoucí bakalářské práce: **doc. Ing. Jiří Vojtěšek, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **5. února 2016**

Termín odevzdání bakalářské práce: **1. června 2016**

Ve Zlíně dne 5. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 16.5.2016

.....
podpis diplomanta

ABSTRAKT

Prvá časť obsahuje možné nástrahy dnešného Internetu a príčiny ktorými prichádzame o anonymitu, súkromie či citlivé dáta. Presne definuje najrozličnejšie útoky, vírusy a spôsoby, ktorými disponujú moderní kyber-kriminálnici. V druhej časti zase zhŕňa a preveruje spôsoby na zachovanie bezpečnosti a anonymity. Od jednoduchých nástrojov umožňujúce čiastočnú anonymitu až po tie komplexnejšie sľubujúce vysokú mieru bezpečnosti a ochrany súkromia, či už pri komunikácii cez Internet alebo počas prehliadania ľubovoľných stránok. Zároveň publikácia odpovie na otázku či je dnes ešte vôbec možné dosiahnuť úplnej neviditeľnosti na Internete za použitia voľne dostupných prostriedkov.

Kľúčové slova: anonymita, bezpečnosť, internet, počítačové siete, identita, ochrana údajov

ABSTRACT

The first part contains possible different threats of today Internet, which causes loss of anonymity, privacy and sensitive data. It precisely defines many different attacks, malwares and ways which are used by the modern kyber-criminals. The second part includes and examines different ways to preserve the security and anonymity. From the simplest tools allowing partial anonymity, we will go through the most comprehensive, promising the complex anonymity and security, either when communicating over the Internet or while browsing any website. Also, the publication will answer the question if it's still even possible to achieve complete "invisibility" on the Internet, by only using a freely available tools.

Keywords: anonymity, security, internet, computer networks, identity and data protection

Poďakovanie

Ďakujem pánu doc. Ing. Jiřímu Vojteškovi Ph.D. za odborné rady, pomoc a trpezlivosť pri tvorbe tejto bakalárskej práce. Taktiež ďakujem nášmu oddeleniu počítačových sietí UTB za overenie správností faktov, ktoré tvora hlavné piliere tejto práce.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Internet dosiahol za posledné desaťročie nebývaných rozmerov. Mnohonásobne sa zväčšil objem prenesených dát, zvýšila sa miera komunikácie, svetlo sveta uzreli služby bez ktorých si dnes nevieme predstaviť život na Internete. Mnohé z nich sú dnes voľne dostupné, úplne zadarmo, čakajúce len na stiahnutie a využívanie. Staré príslovie však hovorí, že nič nie je zadarmo. Všetko je na úkor niečoho, a v mene Internetu je to na úkor straty anonymity či súkromia. Poplatky za využívanie programov či služieb sú takmer prekonané. Dnes sa totiž platí súkromím. S tým sú žiaľ spájané aj možnosti krádeže identity, vírusy rabujúce bankové účty, biznis s predávaním údajov tretím stranám a mnohé iné nebezpečenstvá.

Táto práca vznikla s úmyslom vysvetliť a pomôcť pochopiť bežnému užívateľovi použitie Internetu tak, aby si uvedomoval riziká siete, a zanechával za sebou čo najmenšiu možnú digitálnu stopu a to aj s pomocou programov tu spomenutých. Publikácia prevedie čitateľa

- možnosťami ochrany proti sledovaniu, profilovaniu či kyber-kriminálnikom
- spôsobmi ako ostať anonymný, ako prehliadať a sťahovať z Internetu bez obáv
- praktickými radami na zabezpečenie si počítača a všetkých jeho dát
- používaniami overených a funkčných programov zameraných na ochranu súkromia

Treba však na začiatku zdôrazniť, že dosiahnutie absolútnej anonymity je už v dnešnej dobe prakticky utópia. Nič nie je 100% bezpečné ani nepriestrelné. Všetko má svoje slabiny, zadné vrátka alebo priestor pre zneužitie. Rizík na Internete je stále viac a spôsoby krádeže identít sú stále rafinovanejšie a prepracovanejšie. Odhliadnuc od toho, počas posledných desiatich rokoch vznikol úplne nový fenomén – zber a zhromažďovanie údajov o každom pripojenom užívateľovi. Či už sa jedná o zber zastrešovaný Národným agentúrami alebo súkromnými webovými stránkami ktoré dennodenne navštevujeme, je táto činnosť mimoriadny zásah do nášho súkromia. Je to ako žiť s vysielačom na chrbte a pravidelne posielať informácie o svojej činnosti niekomu, pre koho sú tieto údaje iba obchodnou komoditou.

Je na čase sa pozrieť aké najčastejšie riziká so sebou prináša Internet a ako možno sa úspešne proti tomu brániť a ochrániť si to najcennejšie čo na Internete máme: anonymitu.

I. TEORETICKÁ ČÁST

1 MALWARE

Ako prvá vec s ktorou by sa mal užívateľ zoznámiť a vedieť rozpoznať je malware. Tento druh záškodníckeho softwaru je označenie pre všetky druhy počítačových hrozieb ktoré prináša so sebou internetové pripojenie. Označenie zahŕňa najmä vírusy, červy a trójske kone. Z nich tu dominujú práve trojské kone, najmä pre ich všestrannosť a rozmanitosť.

1.1 Definícia malwaru

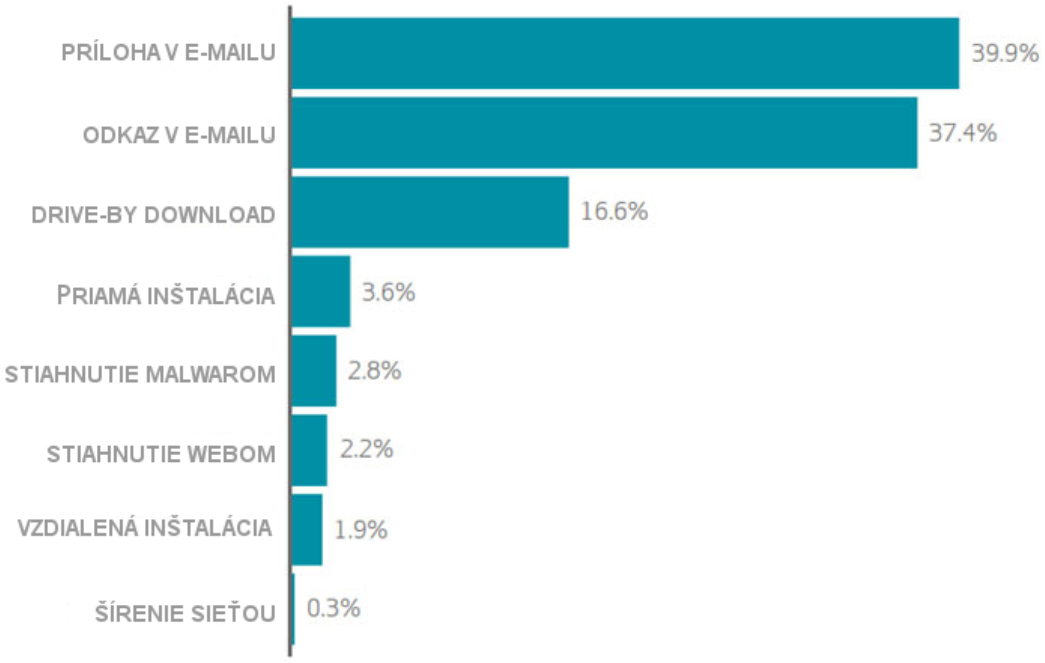
Zo skúseností spoločnosti Kaspersky [1] vyplýva, že mnoho užívateľov nerozoznáva medzi malwarom a generalizuje ich do jedného zaužívaného pojmu. Je dôležité si pritom uvedomiť, že každý druh malwaru sa vyznačuje odlišným chovaním. Zatiaľ čo prioritou počítačových vírusov je čo najviac rozmnožiť svoj kód na disku a pokračovať v nainfikovaní ďalších počítačov, červ sa nainštaluje len raz, a potom hľadá ďalší počítač na vykonanie rovnakej akcie. Rovnako ako počítačový vírus sa šíri automaticky, ale drvivou väčšinou býva spúšťačom práve neobozretný užívateľ. Inou kategóriou sú trójske kone. Jedná sa o škodlivé programy maskujúce sa ako niečo neškodné, dokonca užitočné. Sú spúšťané buď užívateľmi alebo nainštalované na pozadí webovej stránky. Na rozdiel oproti vírusom či červom sa trójske kone na infikovanom počítači nerozmnožujú, ale spoliehajú sa na pripojenie do Internetovej siete. Nie je tomu tak dávno, čo sa začali objavovať aj takzvané hybridné hrozby – malware ktorý kombinuje funkcie vírusov, červov a trójskych koní, všetko v jednom balíku, poskytujúci kyber-kriminálnikovi oveľa väčšie možnosti v útoku. Čo sa však stane keď sa útočník zmocní nášho počítača? Zoznam je nekonečný, môže ísť o zhromaždenie citlivých údajov, posielanie spamu, vymazanie určitých súborov, či poškodenie samotného počítača. Najčastejšie sa stáva, že takto infikovaný počítač sa pripojí do siete s ostatnými infikovanými počítačmi. Takáto sieť sa nazýva Botnet a býva riadená pomocou malých programov (botov) ktoré opakujú zadanú činnosť. Botnet môže byť zneužitý na činnosti ako sú rozposielanie spamu alebo zúčastňovanie sa cielených útokov. To všetko bez vedomia užívateľa. Ten si zatiaľ môže prezerať recepty na halušky a pritom ani netušiť, že sa jeho infikovaný počítač zúčastňuje útoku na nejakú organizáciu či jednotlivca. Najbežnejší spôsob takého zneužitia je potom prostredníctvom DDoS útokov (distributed denial of service – hromadné riadené odmietnutie služby). Je to útok pri ktorom tisíce počítačov botnetu zašle malý kúsok dát jednému cieľu (serveru na ktorú prebieha útok) aby obmedzili normálne fungovanie chodu stránky, e-mailu, služby alebo iného servisu ktorý momentálne beží na danom serveri.

1.2 Vývoj malwaru

Keď sa malware prvý krát objavil, slúžil na jednoduché účely ako napríklad spôsobiť vymazanie, premenovanie či premiestnenie súborov, znefunkčniť počítač a podobne, bez akéhokoľvek finančného obohatenia sa na strane kyber-kriminálnika. Týmto činom sa zvyklo hovoriť kyber-vandalizmus. Niektoré druhy malwaru dokonca nerobili vôbec nič, len zaberali miesto alebo zahlcovali RAM. Takéto vírusy boli typické pre 90tie roky.

Kým vírusy nemusia byť jasne viditeľné že sú spustené, užívateľ môže občas „cítiť“, že niečo nie je v poriadku. Počítač sa správa spomalene alebo pripojenie má nízku rýchlosť.

Dnes sa zmysel malwaru zmenil natoľko, že drvivá väčšina je tvorená len za účelom nelegálneho sa obohacovania. To je často dosahované buď zhromažďovaním dôverných dát z infikovaných počítačov alebo dokonca vďaka vydieraniu, kedy sa uzamknú všetky dáta v počítači a kyber-kriminálnik za ich odomknutie požaduje vysoké výkupné. Aby bolo niečo také možné vykonať, sú najnovšie malwary naprogramované tak aby sa nainštalovali čo najdiskrétnejšie s nulovým dopadom na výkon infikovaného počítača. Poškodený, alebo počítač v režime off-line nemá pre kyber-kriminálnika žiadnu cenu.



Obr. 1. Najčastejšie spôsoby šírenia malwaru podľa Verizon DBIR 2015[2]

1.3 Zmysel malwaru

Od roku 2003 bol malware využívaný pre kyber-kriminálne účely zahrňujúce rovnako fyzické či právnické osoby. Hlavným zmyslom dnešnej kyber-kriminality je obohacovanie sa. Malware ktorý je na to používaný útočníkmi má zväčša rovnaké, známe ciele:

1. **Vykonávať zisk kradnutím citlivých informácií** – bankové účty, čísla kreditných kariet, krádež duševného vlastníctva. Toto sa dokopy nazýva krádež identity. Ide o proces pri ktorom kyber -kriminálnik predstiera, že je niekto iný, zneužijúc pri tom osobné údaje obeti na rôzne nelegálne a nekalé činnosti. V takto infikovanom počítači môže kyber-kriminálnik zneužiť rôzne účty na krádež, digitálne pranie peňazí alebo predať údaje o daných účtoch ďalším kyber-kriminálnikom.
2. **Vydieranie** – najčastejšie je dosahované zašifrovaním užívateľských dát heslom a pýtaním si peňazí za ich odomknutie. Táto metóda je známa pod názvom ransomware, a ide o mimoriadne výnosnú a zákernú metódu. Za ďalší vydieračský spôsob možno označiť takzvané podvodné antivírové programy. Ich úlohou je v podstate presvedčiť užívateľa, aby si myslel, že je jeho počítač nedostatočne chránený. Potom už je len užívateľova nerozvážnosť, že zaplatí za odstránenie vírusu, ktorý sa vlastne v jeho počítači ani nikdy nenachádzal, čím ešte kyber-kriminálnikovi poskytne svoje údaje o platobnej karte. Aby si daný program vydobyl vyžadovanú pozornosť, upozorňuje na seba veľkými bannermi a neuzatvoriteľnými správami ktoré klamlivo indikujú prítomnosť falošného malwaru.

1.4 Šírenie malwaru

Existuje niekoľko spôsobov akými sa dokáže škodlivý malware šíriť. Užívateľ si môže nainfikovať počítač hoci aj návštevou bezpečnej alebo známej stránky. Kyber-kriminálnici neustále hľadajú bezpečnostné diery na webových serveroch kde schovávajú svoj škodlivý kód, pekne implementovaný medzi stránkami na serveri, čakajúc na svoju obeť. Ak si užívateľ zobrazí stránku z daného serveru, malware sa premiestni (nakopíruje) do úložiska, schovaný v paketoch ktoré počítač očakáva z danej stránky. Ide o populárny proces nazývaný drive-by download. Tento spôsob šírenia nie je zďaleka jediný. Malware sa výborne šíri aj prostredníctvom príloh alebo neznámych odkazov v e-maile. Zavírované odkazy sa rýchlo šíria aj na sociálnych sieťach ako je Facebook alebo Twitter.

Ďalším spôsobom je šírenie pomocou prenosných médií ako je CD alebo USB, ale vzhľadom na to, že ide o fyzické média, takéto šírenie je omnoho pomalšie. Malware si samozrejme nezakladá na rozširovaní sa iba za pomoci užívateľa, ale sám aktívne hľadá zraniteľné miesta v softwari. Takéto miesta sa môžu nachádzať buď v operačných systémoch alebo v populárnych programoch ako je Adobe Reader, Adobe Flash, Java či Microsoft Office a ďalšie s tým súvisiace doplnky [1],[3].

Skvelý príklad šírenia malwaru sa stal vo februári 2013, kedy sa domovská stránka súkromnej americkej televízie NBC stala obeťou kyber-kriminálnikov. Čo sa vlastne udialo?

- Ako prvé sa útočníci zamerali na webovú stránku vysoko sledovaného kabaretu Jimmyho Fallona, Late Night, kde za pomoci bezpečnostnej chyby upravili stránku tak, aby sa po otvorení návštevníkom rozbehol upravený JavaScrypt.
- Ten aktivoval vložený HTML komponent známy ako IFRAME.
- IFRAME nadviazal spojenie so stránkami ktoré už boli predtým nainfikované exploit kitom známym ako RedKit. Exploit kit je program na údržbu webových serverov, najmä na vyhľadávanie ich slabých miest. Upravené exploit kity sú bežným nástrojom kyber-kriminálnikov.
- Po získaní spojenia sa exploit kit diaľkovo pokúsil prebrať kontrolu nad prehliadačom pomocou zraniteľnosti v Jave alebo chybe v zabudovanom PDF prehliadači.
- Ak bol exploit kit úspešný, nainštaloval sa do počítača program určený na získanie finančných údajov. Tento program bol mimoriadne nebezpečný vzhľadom na to, že ho v tom čase boli schopné úspešne detegovať len 3 zo 40 antivírových programov.

Tento príklad je dokonalou ukážkou drive-by downloadu, kde kyber-kriminálnici používajú celú kaskádu trikov cez sťahovanie, inštalovanie či spúšťanie, bez akéhokoľvek vedomia či už užívateľa alebo jeho antivírového programu. Ten by sa práve stal obeťou odcudzenia identity, a veľmi pravdepodobne aj obeťou finančnej krádeže [4].

1.5 Druhy malwaru

Je možné, že predchádzajúca kapitola obsahovala pojmy, ktoré ešte neboli vysvetlené. Na nasledujúcich stranách preto uvádzam stručný prehľad najbežnejšieho malwaru, s ktorým môže užívateľ prísť do kontaktu. Subjektívne som sa snažil na základe literatúry či informácií poskytnutých spoločnosťou Kaspersky [2] ohodnotiť ich dopad na systém či stratu súkromia užívateľa. Podotýkam, že toto hodnotenie nie je záväzné a slúži iba ako pomôcka pre čitateľa ľahšie sa zorientovať. Hodnotiaca tabuľka sa nachádza v kapitole 1.5.9.

1.5.1 Vírusy

Počítačové vírusy sa dajú definovať ako typ kódu ktorý sa rekurzívne šíri pomocou svojej upravenej kópie. Takéto programy sú zväčša tvorené za účelom spôsobiť škody. Štandardne vírus pracuje bez toho aby o ňom užívateľ vôbec tušil. Najčastejšie sa vírus dostane do počítača neopatrným sťahovaním neznámych súborov či otváraním nedôveryhodných e-mailových príloh. Keď je infikovaný súbor alebo program otvorený, vírus sa rozmnoží a nainfikuje ostatné súbory či programy. Škody spôsobené počítačovými vírusmi sa líšia. V drvivej väčšine je posolstvo vírusov v poškodení čo najviac súborov a pokiaľ by to bolo možné tak aj vo vyradení daného počítača z prevádzky. Niekedy môže mať užívateľ šťastie a natrafí na vírus ktorého úlohou je iba sa nekontrolovane množiť a spomaliť tým celé PC, bez toho aby niečo poškodil. Samotné víri nezvyknú vynášať von údaje. Fungujú nezávisle od svojho stvoriteľa, šíriac sa najmä v pornografickom alebo pirátskom obsahu, čakajúc na svoje obete [5],[6].

1.5.2 Červy

Pod pojmom červ (z ang. worm) si možno predstaviť škodlivý program ktorého hlavnou doménou je šírenie sa z počítača do počítača prostredníctvom siete. Na rozdiel od bežných vírusov, sa červy šíria automaticky a jeden infikovaný počítač zapojený do siete je schopný nainfikovať zvyšné. Rovnako ako u vírusov, je aj šírenie červa podmienené sťahovaním neznámych súborov či otváraním nedôveryhodných e-mailových príloh. Bežnou formou červov sú takzvané e-mailové červy, ktoré sú schopné lokalizovať užívateľovu e-mailovú adresu a posielať hromadné e-maily. Tak isto červ dokáže vytvoriť bezpečnostnú dieru v sieti a umožniť tým kyber-kriminálnikovi sa zmocniť osobných údajov inštaláciou zadných vrátok alebo keyloggerov (viď kapitolu 2.1.5) rovnako ako poškodiť, premenovať alebo vymazať údaje, či zastavovať dôležité procesy v počítači [5],[6].

1.5.3 Trójske kone

Ako už samotný názov napovedá, jedná sa o program ktorý sa snaží tváriť užitočne. Kyber-kriminálnici často pribaľujú trójske kone spoločne s nejakým neškodným programom alebo rovno v danom programe. Je preto veľmi nepravdepodobné, aby sa trójsky kôň dostal do počítača inou formou, než sťahovaním neznámych súborov či otváraním nedôveryhodných e-mailových príloh. Väčšina trójskych koní je vo forme spustiteľných programov. Môžu vyzerať ako hra, film alebo iné médium. Pretože operačný systém Windows nezobrazuje úplne všetky informácie o danom súbore, často sa stáva, že nevedomý užívateľ si infikovaný súbor stiahne, spustí a vystaví svoj počítač hrozbe. Aktivovaný trójsky kôň sa nereplikuje a nešíri po sieti. Vo svojej 100% podobne je pre antivírové programy mimoriadne ľahko identifikovateľný, preto si kyber-kriminálnici dávajú záležať na ich úprave a implementácií do programov. Aj vďaka tomu vzniklo ich niekoľko druhov [5],[6].

Backdoor

Druh trójskeho koňa ktorý umožní kyber-kriminálnikovi ovládať počítač na diaľku. Umožňuje svojmu autorovi urobiť prakticky čokoľvek, vrátane posielania, prijímania, zapínania či modifikácií súborov. Backdoor trójske kone sú často používané na zhromažďovanie infikovaných počítačov do Botnetu alebo takzvanej Zombie siete ktorá rovnako dobre môže slúžiť napríklad ako už spomínaná forma DDoS útoku.

Trojan-Banker

Trójsky kôň designovaný na krádež účtov pre online bankovníctvo, e-platby či informácie o platobných kartách.

Trojan-Downloader

Druh trójskeho koňa ktorého úlohou je sťahovať a inštalovať najnovšie malware programy vrátane ďalších trójskych koní či programov ktoré by útočníkovi generovali zisk.

Trojan-Dropper

Trojan špeciálne upravený na maskovanie ostatných vírusov a trójskych koní. Tento druh je náročný na lokalizovanie aj pre pokročilé antivírové programy.

Trojan-FakeAV

Trojan tváriaci sa ako užitočný antivírový program, podávajúci falošné hlásenia a vyžadujúci peniaze za odstránenie víru. Toto už bolo spomenuté pri definícii malwaru.

Trojan-Spy

Trójsky kôň ktorý nespôsobuje žiadne škody ani nespomaľuje počítač, avšak pravidelne sleduje a odosiela dáta o užívateľovi, či už vďaka keyloggeru, snímkam obrazovky alebo posielaním vzoriek paketov kyber-kriminálnikovi [7].

Do rodiny trójskych koní sa podľa niektorej literatúry radí aj exploit, ransomware a rootkit.

1.5.4 Spyware

Program vytvorený pre nelegálnu špionáž. Spyware prehľadáva počítač a zneužíva všetky údaje ktoré nájde. Konštantne beží na pozadí, a v niektorých extrémnejších prípadov spôsobuje spomalenie siete či vyššiu konzumáciu operačnej pamäte. Spyware sa dostane do počítača najčastejšie vo forme užitočne sa tváriaceho programu, preto ho niektoré literárne pramene priradzujú do rodiny trójskych koní. Prioritou spywaru je filtrovanie údajov ako

- prístupové údaje a heslá ku mailovým službám
- údaje o platobných kartách
- osobné informácie – faktúry, zmluvy atď.
- sériové a registračné čísla softwaru [5]

1.5.5 Exploit

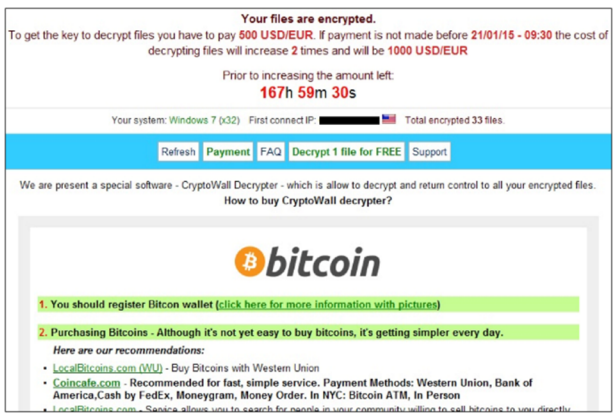
Za exploit sa dá označiť cielené využívanie bezpečnostných medzier v systéme a pašovanie škodlivého softwaru cez nich. Exploit sa do počítača dostáva najčastejšie formou súborov Microsoftu Office. Ten umožňuje používanie programovateľných súborov – makier, ktoré sa spustia po otvorení daného dokumentu. Táto medzera predstavovala pre Office nebezpečie a od verzie 2010 začal kancelársky program hlásiť ak bolo ku súboru pripojené dané makro, a požadovať dodatočné povolenie. Kyber-kriminálnici nikdy nespia a ihneď ako nájdu slabinu v sieti, programe či webovej stránke, sú schopný do nej prepašovať exploit. Paradoxne, by sa tento druh malwaru dal považovať za hnací motor pre bezpečnostné updaty, ktoré výrobcovia v snahe bojovať s útočníkmi pravidelne vydávajú [8].

1.5.6 Rootkit

Ide o zbierku takmer nedetekovateľných programov ktoré sa do počítača dostanú spolu so stiahnutým softwarom z internetu alebo prezeraním infikovaných webových stránok. Cieľom rootkitov je získať administrátorské práva na danom zariadení pomocou modifikácie kódu v operačnom systéme. Rootkit sa tým vlastne stane jeho súčasťou. Ako ďalší krok väčšinou vytvorí zadné vrátka, zaisťujúce plný prístup kyber-kriminálnikovi do užívateľského počítača. To zahŕňa možnosti ako vymazanie či poškodenie súborov, nainštalovania spywaru, kompletné sledovanie aktivity za počítačom či odcudzenie účtov alebo informácií o kreditných kartách. Rootkity sa ťažko hľadajú a ešte ťažšie odstraňujú. Pri nájdenom rootkite sa odporúča formátovať harddisk a nainštalovať operačný systém nanovo. Moderné antivírusové programy už umožňujú odstrániť rootkit bez možnosti reinštalácie, ale môj názor je taký, že maximálne bezpečie sa dosiahne jedine reinštaláciou [5].

1.5.7 Ransomware

Nepríjemný druh malwaru, založený na zašifrovaní dát silnou 256 bitovou asymetrickou šifrou AES a ich opätovnom sprístupnení až po zaplatení výkupného. (ransome=výkupné). Najčastejšie sa objavuje vo forme neuzatvoriteľných správ, varovaní o porušení autorských práv či iných falošných hlásení. Do počítača sa vie dostať buď z infikovanej stránky alebo pri spustení neznámeho súboru či prílohy. Po zablokovaní dát ponúkne užívateľovi možnosť ich odblokovať jedine ak zaplatí požadovanú čiastku, najčastejšie v anonymnej kryptomene Bitcoin [8]. O nepodceňovaní ransomwaru svedčí aj fakt, že Americký Federálny úrad pre vyšetrovanie (FBI) prekvapil tým, že dotknutým odkázal, že im nemá ako pomôcť a jediným východiskom je zaplatenie. Za najrozšírenejší a najúspešnejší ransomware sa momentálne považuje Cryptowall, ktorý už zarobil autorom stovky miliónov dolárov [9].



Obr. 2. Cryptowall na nainfikovanom PC

1.5.8 Adware, pornware a riskware

Tieto tri programy stoja na hrane legálnosti. Do počítača sa síce vedia dostať nelegálnou cestou a to nainštalovaním upraveného programu či formou návštevy infikovanej stránky, ale aj s legálnym súhlasom nepozorného užívateľa pri inštalovaní freeware programov.

- **Adware** sa vyznačuje pop-up oknami s reklamou, vložením ďalšej reklamy do prehliadača či zhromažďovaním informácii o navštívených webových stránkach.
- **Pornware** sa vyznačuje sťahovaním či zobrazovaním morálne otáznych médií za ktoré môžu byť účtované užívateľovi poplatky.
- **Riskware** programy nie sú vyslovene škodlivé, ale majú vysoký potenciál viac uškodiť ako pomôcť. Ide hlavne o rôzne sťahovače, dialery, čističe pozostatkov, programy na „zvyšovanie výkonu“ počítača alebo programy ktoré by radi spravovali užívateľove heslá [7].

1.5.9 Prehľad jednotlivých vírusov a ich dopad na systém a anonymitu

Tabuľka hodnotení funguje na princípe, že čím je číslo väčšie, tak tým je hrozba silnejšia. Pri trójskych koňoch hrozba závisí od typu daného trojského programu.

DRUH VÍRUSU	DOPAD NA SÚKROMIE	DOPAD NA SYSTÉM
Vírusy	2 / 10	8 / 10
Červy	5 / 10	7 / 10
Trójske kone	2-8 / 10	2-8 / 10
Spyware	10 z 10	3,5 / 10
Exploit	5 / 10	5 / 10
Rootkit	9 / 10	6 / 10
Ransomware	4 / 10	10 / 10
Adware, pornware, riskware	3 / 10	3 / 10

Tab. 1. Prehľad jednotlivých vírusov a ich dopad na systém a anonymitu

2 OHROZENIE IDENTITY

Malware a kyber-kriminálnici nie je to jediné, čo by malo trápiť užívateľa Internetu. Je to práve už v úvode spomínane komplexné sledovanie aktivít a zber dát za rôznym účelom. Problémom dnešného Internetu podľa viceprezidenta Googlu Philipa Justusa nie je ani to, že by firmy vedeli príliš mnoho informácií, ale skôr skutočnosť, či ľudia vedia kto a aké dáta o nich získava, a či majú na výber a možnosť povedať nie [10]. Ja osobne mu dávam za pravdu. Mnoho ľudí nevie a ani nechce vedieť aké množstvo informácií zanechávajú za sebou. Veľké množstvo ľudí to ani nerieši, vyhovárajú sa na „bezvýznamnosť v dave". Faktom však ostáva, že takýto prístup či apatia voči vlastnému súkromiu bude viesť len ku intenzívnejšiemu sledovaniu alebo zberu dát. Tu si dovolím citovať írskeho filozofa a politika, Edmunda Burka:

„Aby zlo zvíťazilo, stačí aby dobrí ľudia neurobili vôbec nič [11]."

Počiatkom roku 2010, sociálne siete zažili nevídaný rozmach. Dnes by sa zdalo, že ten kto nie je minimálne na dvoch sociálnych sieťach ako keby neexistoval. Ľudia začali postupne otupovať v ostražitosti a nechávajú si zdieľať takmer každý údaj zo svojho života. V spojení so slabo informovanou verejnosťou ohľadom bezpečnostných rizík vznikajú bezradné situácie, kedy sú ľudia schopný dobrovoľne uverejniť informácie ako číslo kreditnej karty alebo fotografiu občianskeho preukazu. Sociálne média nie sú ani zďaleka jediné kde sa užívatelia dobrovoľne, v duchu hesla „ja nemám čo skrývať" vzdávajú svojho súkromia. Rozmach chytrých telefónov otvoril úplne novú kapitolu možnosti sledovania zo strany či už poskytovateľa aplikácií alebo tvorcu operačného systému. Masívne sledovanie vládnymi agentúrami potvrdili uniknuté dokumenty bývalého zamestnanca NSA, Edwarda Snowdena, ktorý poodhalil gigantickú spyware chobotnicu ukrytú za exabajtami prúdiacích dát. To čo sa považovalo iba za konšpiračné teórie sa potvrdilo. Z Edwarda Snowdena sa razom stal politický disident, ktorý bol nútený ujsť z Ameriky do Moskvy v Rusku [12].

Táto rozsiahla kapitola sa začína charakteristikou od najnelegálnejších praktík ako sú rôzne krádeže identity či spoofing dát, až po tie legálne, teda súkromné alebo národné analýzy, profilovanie, či zbery a zhromažďovanie dát od všetkých užívateľov, v údajnom záujme zlepšenia produktu alebo boju s terorizmom.

2.1 Nelegálny zber dát

V tejto kategórii sa nachádzajú programy a činnosti ktoré vedú buď na sledovanie užívateľa s cieľom získať mená, heslá, prístupové informácie do účtov alebo odfiltrovať všetku komunikáciu, ktorá prebieha medzi sledovanými. Takéto informácie si potom kyberkriminálnici predávajú medzi sebou alebo tretím stranám. V priemere trvá viac než 12 mesiacov kým si dotyčný/dotyčná uvedomí, že jeho identita bola odcudzená [5]. Medzitým mohli poškodenému vzniknúť zbytočné škody a výdavky s tým spojené. Získať späť raz ukradnutú identitu je beh na dlhé trate zahrnujúci nekonečné upovedomovanie orgánov v trestnom konaní či správcov webových stránok kde sa nachádzajú údaje o poškodenom. Dôležitá je v tomto prípade prevencia a obozretnosť. Najčastejšími zbraňami kyberkriminálnikov sú dôverčivosť, neskúsenosť a nevedomosť užívateľov.

2.1.1 Hoax

Ide o poplašné a veľmi často klamlivé správy, napríklad varujúce pred počítačovými vírusmi, nebezpečenstvom zneužitia mobilných telefónov, e-mailové petície, prosby o darovanie krvi a mnoho ďalšieho. Väčšinou nie sú škodlivé pre počítač, ale nepozorný užívateľ im môže naletieť a prísť o peniaze alebo o iné prostriedky [13],[14].

2.1.2 Phishing

V podstate ide o pokročilejší Hoax. E-maily využívajúce sociálne inžinierstvo, ktoré vyzerajú na prvý pohľad oficiálne a často obsahujú varovnú správu. Príkladom sú e-maily, ktoré vyzývajú na zmenu hesla k bankovému účtu. V takomto e-maile je umiestnený odkaz, na ktorý sa dá prihlásiť a zmeniť si heslo. Odkaz však nesmeruje na stránku banky, ale na jej dokonalú napodobeninu. Takéto stránky sú väčšinou veľmi prepracované a nebudia žiadne podozrenie. Preto netreba naletieť. Pri každej podobnej správe sa musí spozornieť, keďže banky nikdy nevyzývajú na podobné operácie e-mailom. Dobrým signálom upozorňujúcim na phishing býva chýbajúci protokol HTTPS a s tým spojený overovací certifikát organizácie. Vždy pred každým prihlásením do banky je dôležité skontrolovať či daná webová stránka sa začína protokolom HTTPS a či certifikát ktorý overuje stránku je platný. Odporúčam si zapísať aj názov certifikačnej autority. Niekedy sa totiž stáva, že kyberkriminálnici dokážu vytvoriť falošné HTTPS s falošným certifikátom [13],[14].

2.1.3 Pharming

Táto metóda spočíva v presmerovaní názvu www stránky na inú adresu. Každej mennej adrese, napríklad ultrabanka.sk príslušní daná IP adresa, napríklad 165.25.210.51.Kyber-kriminálnici však dokážu presmerovať danú adresu buď napadnutím DNS servera (server ktorý sa stará o preklad IP adresy na jej čitateľnú formu), alebo zmenou súboru hosts priamo v počítači užívateľa. Po takomto zásahu je užívateľ po zadaní danej adresy stránky banky presmerovaný na jej predpripravenú napodobeninu. Ak užívateľ na to včas nepríde, a zadá tam svoje prihlasovacie údaje, okamžite ich získa, ten kto danú stránku vytvoril. Proti tejto hrozbe sa dá brániť rôznym spôsobom. Najjednoduchší spôsob je si uložiť stránku do záložiek alebo skontrolovať či stránka obsahuje platný HTTPS certifikát vydaný známou certifikačnou autoritou [13],[14].

2.1.4 Spoofing

Metóda, ktorá sa používa na zmenu totožnosti odosielaných správ. Jednou z týchto metód je aj náhrada e-mailovej adresy pri phishingu. Ďalšia spočíva v podvrhu IP adresy, na stránky, ktoré takýmto spôsobom overujú totožnosť prihlasujúceho. Najviac nebezpečnou je však metóda nazývaná man-in-the-middle. Tato metóda spočíva v narušení komunikácie medzi klientom a serverom, pri ktorej útočník naruší šifrovací systém verejného a súkromného kľúča, ktorý sa používa pri komunikácií [13],[14].

2.1.5 Keylogger

Ide o software alebo hardware využívaný tretími stranami na získanie citlivých informácií (prihlasovacie údaje, heslá, informácie o kreditných kartách, atď.) tým, že zaznamenávajú stlačenia jednotlivých kláves. Keylogger sa do počítača môže dostať zabudovaný v trójskom koni, teda napríklad pri sťahovaní programov z neznámych zdrojov. Po aktivácií začne odosielať nazbierané údaje kyber-kriminálnikovi. Bežnými súčasťami a funkciami keyloggerov sú v dnešnej dobe aj odchytávanie snímok z obrazovky, fotenie fotiek pomocou webkamery alebo osobitné zaznamenávanie a rozpoznávanie textu v komunikačných programoch a internetových prehliadačoch. Keyloggery sa inštalujú do počítačov bez vedomia užívateľa a v kombinácií s dodatočným zberom paketov ide o závažnú stratu súkromia pri používaní počítača [13],[14].

2.1.6 Falošný prístupový bod

Falošný prístupový bod (ďalej len FPB) je zákerná a relatívne jednoduchá metóda na získanie hesiel a dát od pripojených užívateľov. Podstata je vytvoriť bezdrôtový prístupový bod do siete za použitia WiFi, na ktorý by sa mohol každý pripojiť za vidinou bezdrôtového Internetu zadarmo. V skutočnosti sa však pripoja na sieť, ktorá je plne pod kontrolou kyber-kriminálnika. Na túto činnosť sa využíva špeciálna distribúcia Linuxu Kali, ktorá obsahuje nástroje ako **sslstrip** a **ettercap** ktoré dokážu otvárať a spracovávať jednotlivé pakety prenesené touto sieťou. Tieto pakety obsahujú údaje ako MAC adresy, IP adresy stránok ktoré si obeť prezerá, heslá a prihlasovacie údaje, či iné mimoriadne citlivé informácie. S týmto zariadením je možné odfiltrovať celú komunikáciu. Funguje to nasledovne:

- Užívateľ sa pripojí na FPB
- Následne celá jeho internetová komunikácia je prenášaná cez útočníkov počítač.
- Internetová komunikácia sa následne spracuje pomocou sslstripu a ettercapu.
- Zistené údaje ako heslá, IP adresy, kontá sa zapíšu do logov.
- Útočník následne prenáša internetovú komunikáciu na ďalší router.
- Router pošle dané údaje na Internet a odozvu pošle opäť útočníkovi ktorí ju po spracovaní prenesie užívateľovi do jeho počítača.

2.1.7 Wireshark

Wireshark je paketový analyzér, ktorý funguje podobne ako Kali od Linuxu, ale s tým rozdielom, že nepotrebuje FPB aby získaval užívateľské dáta. Wireshark jednoducho prepne útočníkovu sieťovú kartu do takzvaného promiskuitného režimu, ktorý umožňuje prijímanie všetkých paketov v pripojenej sieti. Takže v podstate stačí, aby si kyber-kriminálnik vzal notebook, nainštaloval Wireshark, prihlásil sa do nezabezpečenej Wi-Fi alebo LAN siete a bez problémov dokáže odchytávať najmä nešifrovanú komunikáciu, vrátane hesiel, IP adries či rôznych užívateľských účtov. To je asi jediná nevýhoda oproti FPB, keďže ten dokáže spracovať a otvoriť aj šifrovanú HTTPS komunikáciu. Proti tomuto je veľmi zložité sa ubrániť. Je treba poriadne zvážiť kde je bezpečné sa pripojiť na Internet a kde nie. Najlepšie je mať so sebou vlastný mobilný Internet [15].

2.2 Legálny zber dát

Pod pojmom legálny zber možno rozumieť zhromažďovanie údajov za účelom zlepšenia produktu, poskytovania presnejšej reklamy alebo v rámci boja proti terorizmu či extrémizmu. Často však za tým stojí aj možnosť obchodovania s týmito údajmi. Zber dát sa už dávno netýka len počítačov. Stačí si kúpiť nový smartphone, pripojiť sa do siete, a ako prvé vyskočí okno z oznámením, že spoločnosť XY (závisí od výrobcu OS) má v rámci zlepšenia produktu záujem o zhromažďovanie dát typu poloha, výsledky vyhľadávania či spôsob užívania. Takto ostanú len dve možnosti: dobrovoľne prísť o súkromie na úkor lepšej konektivity, alebo vrátiť chytrý telefón späť do predajne a vystačiť si s „hlúpym“. Dalo by sa povedať, že človek prichádza o súkromie hneď ako začne používať Internet. Každou jednou činnosťou nechránený jedinec zanecháva digitálne odtlačky. Tie sú v podstate stopy na sieti, ktoré obsahujú celú škálu informácií o činnosti užívateľa. Môže ísť o údaje IP adresy, cookies, informácie o polohe, systéme či prehliadača. Signálom toho, že sme boli zaznamenaný sú zmeny v reklamách. Býva to naozaj nepríjemné vidieť ako reklamy čírou náhodou zobrazujú informácie o produktoch ktoré sme prednedávnom vyhľadávali alebo nakúpili [5]. Ako je to možné?

Existuje mnoho spoločností ktoré sa zaoberajú online inzerciou a online marketingom. Tieto spoločnosti ponúkajú za finančnú kompenzáciu možnosť umiestniť si na webových stránkach sledovacie zariadenia, takzvané sledovače. Úlohou týchto sledovačov je zhromažďovať dáta ako čas strávený na stránke, počet kliknutí na danú kategóriu, či prebehol nákup a tým vytvárať na základe unikátnej IP adresy profil každého užívateľa. Tento profil v kombinácií s polohou ktorú nesie každá IP adresa, potom slúži na lepšie zobrazenie cielených reklám. Precíznosť tohto systému naháňa hrôzu. Napriek tomu, že inzerčné spoločnosti by nemali spájať nazbierané údaje s konkrétnym menom a priezviskom, nazbieraný objem a presnosť dát úplne postačujú na jednoznačnú identifikáciu daného užívateľa. Výborným príkladom je istá americká inzerčná spoločnosť, ktorá dokázala predpovedať na základe zmien vo vyhľadávaní a prezeraní webu, že užívateľka je tehotná ešte pred tým, než o tom vedela jej rodina. Začalo to zobrazovaním reklám na detskú výbavu, odkazmi na detské fóra a pokračovalo až zasielaným zľavených kupónov na detské potreby priamo domov. Keďže išlo o mladé dievča, zdesenie jej rodiny bolo na mieste [16].

2.2.1 Princíp a dôvod fungovania

Za prvé je potrebné si uvedomiť, čo nás dokáže v sieti jednoznačne identifikovať. Je to práve naša IP adresa. Tá so sebou nesie celú škálu informácií a zanecháva najviac stôp v sieti. IP adresu je možné zachytiť pri žiadosti o zobrazenie stránky vykonávanej naším prehliadačom, v súboroch cookies, v histórii prehliadania, v e-mailových správach, na sociálnych sieťach, pri používaní Torrentov alebo aj pri preberaní RSS správ.

Ak už raz niekto získa užívateľovu IP adresu a zamiera sa na ňu pomocou všetkých nazhromaždených dát, dokáže jednoducho vyskladať užívateľský profil. Takáto činnosť sa nazýva profilovanie. Najčastejšie sa používa za menej vážnejším, komerčným účelom, ako poskytovanie informácií tretím stranám ktorý sledujú a využívajú dáta pre reklamu. Nikto však nezaručí, že takéto dáta nebudú zneužité. Môže sa stať, že dôjde ku závažnejším spôsobom ich využívania a to formou sledovania čo si užívateľ prezerá a sťahuje, alebo tvorbou cielených útokov na zariadenie daného užívateľa [5],[8].

Spoločnosti zaoberajúce sa zberom dát vyvíjajú svoje vlastné sledovacie nástroje. Tie si následne nechávajú umiestňovať na rôzne webové stránky za poplatok prevádzkovateľovi. Hodnota takto nazbieraných dát je však niekoľkonásobne väčšia. Dáta potom analyzujú, vytvoria profil užívateľa a predajú inzerčným spoločnostiam.

- **Analytyká** - sledovače ktoré sa zaoberajú výskumom a analýzou činnosti na webových stránok. Sledujú aktivitu každej IP adresy a následne posielajú štatistiky.
- **Majáky** - sledovače slúžiace výhrade ku sledovaniu konkrétnej činnosti na webe
- **Cookies** – vzhľadom na fakt, že protokol HTTP si neukladá predchádzajúce činnosti užívateľa, boli vyvinuté súbory cookies. Tie sa uložia do počítača a slúžia na ukladanie informácií o užívateľovi, kde potom po prihlásení na server je schopný rozpoznať o koho ide. Problém však nastáva, keď si navštevovaný web začne postupne takto analyzovať záujmy konkrétneho užívateľa. Hlavne ktoré stránky navštevuje, aké informácie vyhľadáva, ako často chodí na tú a tú stránku a podobne. Tieto informácie sa dajú neskôr bez vedomia užívateľa využiť pre cielenú reklamu alebo štatistické vyhodnocovanie správania. Cookies možno vyložene zneužiť vtedy, ak získa útočník prístup do počítača užívateľa, pretože cookies na počítači nie sú nijako chránené. Potom je možné predstierať aj cudzie ID [17].

2.2.2 Pokročilejšie možnosti legálneho zberu dát

Technológia používaná na sledovanie online aktivít sa pomaly odbremeňuje od používania IP adries a blížili sa ku používaniu oveľa viac sofistikovanejších metód. Tento trend bol podmienený túžbou sledovať nie len jedno užívateľské zariadenie, ale rovno všetky. Faktom ostáva, že sledovanie zariadení ako sú napríklad chytré telefóny, už nezávisí až tak od IP adresy. Je pravda, že tam princíp funguje trochu ináč, a síce už pri obyčajnej inštalácií danej aplikácie musí užívateľ odsúhlasiť možný zber dát či prístup do citlivých priečinkov. Medzi zariadeniam kde na IP adrese závisí, teda počítače či notebooky tento nový spôsob sledovania dané IP adresy prakticky úplne vylúčil a dokáže analyzovať aj bez nich. Ide o kombináciu prehliadača, doplnkov, aplikácií a fontov ktoré sú nainštalované v zariadení a slúžia ako unikátny identifikátor rovnako dobre ako IP adresa. Táto technológia sa nazýva Fingerprinting. Pravdaže ak sa skombinuje s IP adresou, výsledky sú ešte presnejšie [5].

2.2.3 Sociálna sieť Facebook

Z doposiaľ uvedených informácií vyplýva, že užívateľ príde takmer o kompletnú anonymitu len tým, že si nechránene prezerá Internetový obsah. Čo ak sa ku tomu ešte pridá používanie sociálnej siete? Miestu kde človek dobrovoľne vydáva informácie o sebe , o svojich známych, o svojich pocitoch či rôznych želaniach? Nasledujúca časť sa zameriava na zber a analýzu dát v najpoužívanejšej sociálnej sieti na Slovensku či Česku – na Facebooku.

Pred zaregistrovaním sa do tejto siete je potrebné opýtať samého seba ako veľmi chceme o sebe dať vedieť. Licenčné podmienky Facebooku hovoria jasne, že akékoľvek vydávanie sa za toho kto nie sme, je jasným porušením pravidiel užívania. Facebook vyžaduje od nás e-mailovú adresu, a pri registrácií si dokonca pýta jej prístup. Tento krok sa dá preskočiť, ale hneď nasleduje ďalší ako pridanie si XY citlivých údajov či profilový obrázok. To by mala byť naša fotografia. Tu je nutné pripomenúť, že Facebook kúpil softwarového výrobcu ktorý sa špecializuje na rozpoznávanie tvári. Facebook je teda schopný skenovať všetky nahrané fotografie a podľa našej profilovej nájsť ďalšie, hoci aj tie ktoré boli nahrané u niekoho iného. Ku tomu ak sa pridá vyznačená poloha (či už z metadát danej fotografie alebo pridaná užívateľom), tváre ďalších ľudí či druh vykonávanej činnosti, vznikajú tak dokonalé podmienky pre profilovanie, kde predaj týchto údajov tretím stranám znamená vysoko presnú, cielenú reklamu.

Facebook však prichádza s niekoľkými možnosťami úpravy súkromia. Ich nastavenia mávajú určitý pozitívny dopad na anonymitu, a je len na užívateľovi koľko informácií si o sebe želá nechať zobraziť. Samotný Facebook sa s týmto krokom ponúka hneď o začiatku registrácie a ide o odporúčanú jednorazovú záležitosť. Ignorovanie nastavení súkromia môže viesť ku prístupu cudzích ľudí na užívateľský profil a dôležitosť tohto kroku potvrdzuje aj nedávno zrušená možnosť ostať na tejto sieti nevyhľadatelným.

Treba si uvedomiť, že Facebook nie je charita a jeho príjem tvorí predávanie nazbieraných informácií tretím stranám. Sledovanie Facebookom je už tak pokročilé, že užívateľ sa nemusí nachádzať ani na danej stránke aby o ňom Facebook bol schopný zhromažďovať údaje. Stačí iba navštíviť stránku na ktorej je umiestnený Facebookovský doplnok (tlačidlo páči sa mi to, zdieľať...) a už sa zaznamenáva čas na stránke, ID užívateľa, počet kliknutí a tak ďalej. Je absolútne nepotrebné, aby užívateľ daný doplnok použil. Dokonca nemusí mať ani účet na Facebooku. V podstate tieto doplnky fungujú ako vyššie spomínané sledovače. Samotný Facebook sa spolu s týmito doplnkami ktoré sa už nachádzajú na takmer každej stránke správa ako obrovský supercookie. Zhromažďuje IP adresy spoločne s Fingerprintom daného užívateľa a porovnáva to s miliónmi ostatných dát získaných za účelom poskladania kompletného profilu o užívateľovi [5],[8].

Výborným príkladom bol nedávny súdny spor, kedy americký študent práv podal na súd žiadosť o získanie všetkých údajoch ktoré Facebook o ňom za celý čas využívania nazbieral. Obdržal 1222 stranový dokument, a to iba za 3 roky aktivity na Facebooku. Dokument bol rozdelený do 57 skupín vrátane vymazaných príspevkov, súkromných správ, kamarátov, kontaktov, vyhľadávaní, či informácií ako IP adresy odkiaľ sa prihlasoval, polohy, či časové známky. Dokument obsahoval dokonca aj zoznam telefónnych čísiel z mobilu na ktorom mal taktiež aplikáciu Facebook. V kombinácii so spomenutou možnosti rozlišovania a zberu biometrických dát – teda fotografií, je dobrovoľné používanie sociálnej siete Facebook opozitom súkromia a anonymity na Internete [18].

Nechcem týmto nikoho odhovárať od využívania spomenutej siete. Je to výborný nástroj na komunikáciu s okolím, len si treba uvedomiť, že jediný dôvod prečo si Facebook nič neúčtuje za svoje využívanie je ten, že už bol zaplatený našim súkromím.

2.2.4 Zber dát nadnárodnými spoločnosťami

Nadnárodné spoločnosti zaoberajúce sa výpočtovou technikou ako sú Google alebo Windows kladú vysoký dôraz na využívanie svojich produktov. Pre ich vylepšovanie a predpovedanie ďalších predajov si dali za cieľ nazhromaždiť o používateľovi tak veľa dát ako sa len bude dať. Všetko to zabalili a predniesli vo forme „zlepšovania kvality produktov“. Nejde tu však len o to. Toto množstvo nazbieraných dát môže byť kedykoľvek posunuté represívnym či vyšetrovacím národným zložkám. Človek nikdy netuší ako sa môže zmeniť vládny režim. Viete si predstaviť situáciu kedy by sa demokracia v priebehu pár rokov zmenila na totalitu a pomocou týchto nástrojov by boli vyhľadaný potencionálne nepohodlní ľudia? Už teraz sa stáva, že legálne odsúdia niekoho kto napíše alebo uverejní nevhodný príspevok na verejnej diskusii. Čo sa bude diať ďalej nechávam len na predstavivosti čitateľa. Nasledujúca kapitola je venovaná práve tejto problematike.

Microsoft

Spoločnosť Microsoft na svojich stránkach tvrdí, že používa celý rad metód a technológií na zhromažďovanie a analýzu údajov ako napríklad:

- internetové funkcie v softvéri a službách programu, ktoré odosielajú informácie na servery Microsoftu za účelom ich ďalšieho spracovania
- technológie ako súbory cookie a beacony, tie sa môžu využívať napríklad na uloženie preferencií a nastavení používateľa, zhromažďovanie údajov o používaní, overenie používateľa alebo zistenie podvodu (napríklad nelegálna verzia systému)

Microsoft od uvedenia operačného systému Windows 10 na trh však začal s masívnym zhromažďovaním dát o činnosti užívateľov. Podobným spôsobom sa snažil dostať aj do starších Windows 7 formou updatov ktoré prinášali telemetriu, sledovanie zobrazovaného obsahu alebo odosielanie histórie Internetu Exploreru na analýzu do Microsoftu. V domácej verzii Windows 10 je vypnutie updatov zakázané, čo znamená, že užívateľovi môže byť predhodený akýkoľvek update ktorý s opravami či stabilitou nebude mať nič spoločné. Dokonca už aj šifrovanie harddisku nástrojom od Microsoftu sa stalo pri Windows 10 kontraproduktívne, keďže Microsoft začal uchovávať na svojich serveroch dešifrovací kľúč. Nechcem si radšej ani predstaviť, čo by sa stalo keby o tieto citlivé údaje prišli [5].

Štandardne sa v domácej verzii Windows 10 nachádzajú zapnuté nastavenia ako

- zdieľanie užívateľského ID pre lepšie zobrazovanie reklám
- posielanie do Microsoftu užívateľom napísane texty (toto je typický keylogger)
- prístup ku polohe a jej zdieľanie pre lepšiu reklamu
- posielanie webovej histórie do Microsoftu
- posielanie vzoriek súborov a nainštalovaných programov do Microsoftu

zapnuté a pripravené odosielať dáta hneď ako sa počítač pripojí do siete Internetu, čo je pri Windows 10 už prakticky povinnosť. Microsoft ďalej tvrdí, že spolupracuje so zložkami národného či represívneho charakteru, teda nemá žiaden problém im poskytnúť všetky nazhromaždené dáta o užívateľovi [19],[20].

Skype

Populárny internetový komunikačný nástroj ktorý sa vyznačuje najmä posielaním správ, prijímaním hovorov a video hovorov alebo zdieľaním obrazovky. Nie je tam toho veľa čo by sa dalo zneužiť alebo odhaliť o danom užívateľovi. V roku 2011 odkúpila Skype spoločnosť Microsoft a nastalo pár zmien. Začali sa ukladať kompletné informácie a dialógy medzi užívateľmi. Tieto informácie nie sú našťastie určené tretím stranám, ale represívnym zložkám či národným sledovacím agentúram. Sledovanie komunikácie pomocou Skype bolo doteraz pre políciu veľmi ťažké, predovšetkým kvôli zložitému kódovaniu programu a tiež pretože v ňom počítače užívateľov komunikovali priamo, bez toho, aby využívali sprostredkujúce servery. Microsoft však začal ukladať dané správy a umožnil prístup vládnym agentúram nielen do archívov ukladaných správ, ale priamo medzi práve rozposielané správy. Najviac toho využila americká NSA ktorá pomocou svojej obrovskej analyzačnej databázy PRISM (viď kapitolu 2.2.5) je schopná odfiltrovať a prečítať takmer každú správu či hovor v USA a vo významných partnerských krajinách [21].

Google

Internetový gigant ktorý určite netreba predstavovať. Začínal ako internetový prehliadač, no dnes zastrešuje obrovské portfólio webových služieb a riešení. Google dnes zhromažďuje množstvo informácií vrátane mena, priezviska, polohy či IP adresy.

Medzi zhromažďované údaje patrí činnosť v službe Google, pod je možné rozumieť všetky

- hľadané výrazy
- webové stránky, ktoré užívateľ navštevuje
- sledované videá (služba Youtube tiež patrí pod Google)
- reklamy na ktoré užívateľ klikne
- polohy zariadení
- informácie o zariadení
- adresy IP a údaje súborov cookie.

Zhromažďujú sa aj osobné údaje (rovnako aj fakturačné údaje, čísla platobných kariet atď.)

- meno,
- e-mailovú adresu a heslo,
- dátum narodenia,
- pohlavie,
- telefónne číslo,
- krajinu.

Tak isto sa analýze nevyhnú ani vytvorené dokumenty či dáta v službách od Google, ako

- e-mailové správy, ktoré užívateľ posiela a prijíma pomocou Gmailu;
- kontakty, ktoré si pridá
- udalosti kalendára
- fotky a videá, ktoré nahraje
- všetky dokumenty, tabuľky a prezentácie na Disku (cloudové riešenie Googlu)

Všetky tieto informácie sa ukladajú a analyzujú na serveroch spoločnosti Googlu za účelom lepšej cielenej reklamy, predaja informácií tretím stranám alebo môžu byť veľmi ľahko s požehnaním vládnych agentúr použité proti užívateľovi [22].

2.2.5 Zber dát vládnymi agentúrami

Neexistuje žiaden komplexnejší a viac prešpekulovanejší program ako je ten na sledovanie užívateľov Internetu z dielne americkej NSA. Táto vládna agentúra ktorá spôsobom sledovania už prakticky spĺňa všetky kritéria čínskeho totalitného režimu má iba jediný zmysel existencie – kompletná eliminácia súkromia obyvateľov USA a partnerských krajín v mene „boja proti terorizmu“. NSA nestačí len monitorovanie hovorov, alebo Internetu. Táto agentúra prakticky sleduje celý svet, a stojí za mnohými kauzami [23]. V rýchlosti spomeniem známu chybu v SSL protokole, označovanú ako Heartbleed. NSA túto chybu beztrestne dlhé roky využívala, bez najmenšieho premyslenia, že tým ohrozuje dáta užívateľov. Ďalšími kauzami sú napríklad zadné vrátka v šifrovacom RSA algoritme umožňujúce rýchle dešifrovanie komunikácie, či zadné vrátka v takmer každom Cisco routeri opäť umožňujúce ľahké filtrovanie a posielanie vzoriek komunikácie [24]. Za spomenutie stojí aj alebo silný tlak na organizáciu TrueCrypt ktorá nakoniec prestala aktualizovať svoj produkt. Počet všetkých káuz kde bola zapletená NSA by asi nestačil ani na 5 takýchto prác.

PRISM

Takéto obrovské množstvo dát, ktoré je schopné NSA denne nazbierať musí byť nejako zatriedené a rozanalyzované. Na to slúži program PRISM. Jeho zmyslom je uchovávanie dát s cieľom ich následnej analýzy. Tento program posúva profilovanie na úplne novú úroveň. Pokrýva viac ako 75% celkovej komunikácie v USA. Funguje v obrovskom komplexe dátových úložísk v Salt Lake, v štáte Utah. Celý projekt stojí desiatky miliónov ročne. S NSA spolupracuje Facebook, Windows, Apple, Twitter, Google a mnohé ďalšie IT firmy. Spoločne umožňujú programu PRISM monitorovať a zbierať akékoľvek informácie, v prípade Windowsu už aj samotné užívateľské dáta uložené na harddisku [25].

XKeyscore

Pokiaľ budeme chápať PRISM ako jednu obrovskú databázu, tak program XKeyscore sa stará o zatrieďovanie, analyzovanie a vyberanie dát z tejto databázy. Rovnako ako samotný PRISM, tak aj Xkeyscore bol odhalený vďaka odvahe Edwarda Snowdena [26].

II. PRAKTICKÁ ČÁST

3 OBRANA A OCHRANA SÚKROMIA A DÁT

Ak ešte niekoho zaujímala otázka, či Internet sám o sebe poskytuje dostatočnú anonymitu, dúfam, že už pozná odpoveď. Internet bol sám o sebe anonymný zhruba tak do polovice 90.tych rokov. Potom sa začalo postupne s analýzami IP adries, zberom jednoduchých dát a dopracovali sme sa až do fázy, kedy takmer každý jeden paket odoslaný Internetom môže byť potenciálne podrobený preskúmaniu či už vládnou agentúrou, reklamným sledovačom alebo samotným kyber-kriminálnikom. Netrúfam si povedať čo je horšie.

Našťastie vždy existuje riešenie. Nie každému je totiž po vôli keď ho niekto sleduje a potom na základe aktivity na Internete vyhodnocuje štatistiky alebo ich ďalej predáva. Nasledujúca praktická časť obsahuje overené a účinné programy pomocou ktorých si je možné aj v dnešnej dobe celkom úspešne ochrániť súkromie. Začína sa od jednoduchých doplnkov do prehliadačov, cez blokovače, servery proxy až ku špeciálne upraveným operačným systémom alebo prehliadačom, ktoré umožňujú prístup do anonymizujúcej siete.

Dôležité je si však uvedomiť jedno. Nič nie je 100% nepriestrelné. Dosiahnutie absolútnej anonymity je zložitý a náročný proces plný kompromisov zo strany užívateľa. Nestačí si nainštalovať prístup do anonymizujúcej sieti a myslieť si, že na nás teraz nikto nemá. Je treba nájsť správne vyváženie, medzi použiteľnosťou a primeranou ochranou súkromia. Nie každý má možnosť zmeniť operačný systém, a nie každý má dostatočné znalosti o tom aby pochopil fungovanie nasledujúcich programov. Jedno je však isté, bez akejkoľvek ochrany je užívateľ vydaný prakticky na milosť či nemilosť Internetu a opäť so zabarikádovaním sa v tejto sieti môže na seba privolať nechcenú pozornosť. Treba myslieť na to, že ak by si rôzne národné agentúry našli určitý spoločný cieľ s veľkým záujmom o jeho prelomenie, predpokladám, že nič, ale absolútne nič čo by bolo v tom momente pripojené na Internete by nebolo pred nimi v bezpečí.

Rady obsiahnuté v tejto praktickej časti umožnia užívateľovi sa v prvom rade úspešne zabezpečiť pred stratou identity, a možnosti profilácie reklamnými spoločnosťami. Pravdaže používanie nasledujúcich programov bude mať aj mimoriadne pozitívny dopad na samotnú anonymitu a citlivé údaje užívateľa.

3.1 Level 0 – Základné zabezpečenie

Ako úplne základné zabezpečenie pre bežných užívateľov, ktorý sa nechcú vzdať používania operačného systému Windows sa odporúča niekoľko jednoduchých krokov, ktoré dokáže zvládnuť ktokoľvek. Nasledujúce kroky nemajú dopad na zvýšenie anonymity na Internete, ale ide skôr na bezpečnosť pred jeho hrozbami.

3.1.1 Používanie silného hesla

Najbanálnejší, a predsa tak podceňovaný krok. Výber správneho hesla je dôležitá vec ktorá sa nesmie zanedbať. Platí jednoduché motto – čím je heslo dlhšie, tým dlhšie trvá kyber-kriminálnikom jeho prelomenie. Odporúča kombinácia malých a veľkých písmen, čísel a špeciálnych znakov. V žiadnom prípade by sa nemalo používať všade rovnaké heslo, nech je akejkoľvek kvality. Stačí jedna zle zabezpečená stránka bez šifrovania svojej databázy hesiel na ktorú sa dostanú kyber-kriminálnici a je to len otázka času kedy si podľa registračného e-mailu vyskúšajú aj Vaše konto. Pre lepšie pochopenie sily hesla, odporúčam navštíviť stránku na jeho otestovanie *howsecureismypassword.net*.

POZOR: V žiadnom prípade netestujte svoje skutočné heslo, ale iba jemu podobné.

Pravidelné obmieňane hesla je ďalším dôležitým krokom. Nič nie je 100% bezpečné, ani stránky využívajúce HTTPS protokoly. Pripomína to nedávna kauza Heartbleed. Išlo o masívnu zraniteľnosť v OpenSSL knižnici ktorá šifruje heslá a citlivé údaje uložené na každej stránke kde je možnosť mať účet. OpenSSL využíva väčšina webových serverov. Medzi napadnuté weby patrili aj *seznam.cz* alebo *sme.sk*. Ihneď po objavení chyby začali prvé on-line služby varovať používateľov a odporúčať im zmenu hesla. Tá mala pomôcť po tom, čo administrátori webov implementovali opravenú verziu OpenSSL na server. Samotná záplata ale zrejme nestačí. Magazín The Verge napísal, že sa hackerom podarilo s využitím zraniteľnosti Heartbleed získať i privátny SSL kľúč. To znamená, že útočník dokáže odchytiť šifrované dáta aj po tom, čo na serveri bola nainštalovaná opravená verzia OpenSSL a používateľ si zmenil svoje heslo [27]. Weby využívajúce OpenSSL teda musia navyše zmeniť aj privátne SSL kľúče. Bežný používateľ tak prakticky nemá reálnu možnosť ovplyvniť bezpečnosť svojich dát.

3.1.2 Windows účty

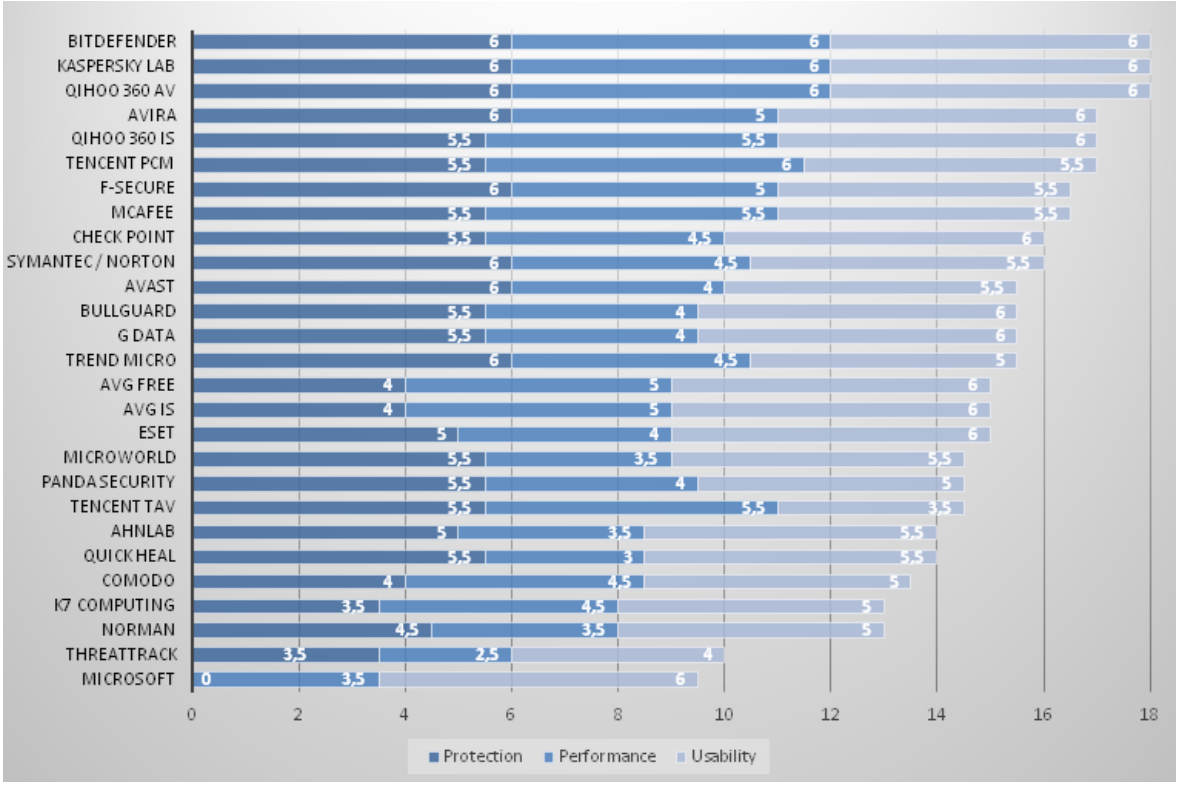
Drvivá väčšina užívateľov na svojom zariadení využíva administrátorský účet na všetky aktivity za počítačom. Lenže používanie administrátorského účtu prináša aj určité riziká. Administrátorský účet je v podstate účet s plným oprávnením na zmeny bezpečnostných nastavení, zmeny parametrov hardwaru, inštalovaní programov či plnému prístupu do všetkých položiek. Už len jednoduché premenovanie názvu administrátorského účtu môže trochu zvýšiť bezpečnosť. Ideálne je vytvorenie štandardného užívateľského účtu s limitovanými právomocami na prehliadanie internetu a bežnú prácu. Premenovaním tohto účtu na „administrátorský“ môže zmiasť neskúseného kyber-kriminálnika. Ďalej sa odporúča vypnúť, alebo odstrániť hosťovský účet, keďže často práve zapnutý hosťovský účet je slabinou a bránou do systému. Prirodzene odporúča sa používať na všetky účty silné heslo na spôsob predošlej kapitoly [5]. Okrem triku s účtami je vhodné si inštalovať najnovšie aktualizácie. Nemusí ísť o úplne každú jednu, no je mimoriadne dôležité si nainštalovať aspoň kritické a bezpečnostnú záplaty. Operačný systém najmä od Microsoftu stále obsahuje plno bezpečnostných medzier ktoré môžu byť skôr či neskôr zneužité, tak prečo to kyber-kriminálnikovi uľahčovať ignorovaním najdôležitejších aktualizácií?

3.1.3 Antivírové programy

Na druhej strane veriť, že iba aktualizovaný operačný systém so zapnutou ochranou Firewall nás uchráni pred všetkými nástrahami Internetu je zase celkom naivné. Antivírové programy sa dnes stali nevyhnutným doplnkom potrebným na bezpečný pohyb na Internete. Tie naozaj kvalitné dokážu odchytiť drvivú väčšinu už spomenutých malware programov, alebo upozorniť na nebezpečné stránky ešte pred tým, než na ne užívateľ vstúpi. Bez kvalitného antivírového programu by som neodporúčal sa ani pripájať do siete. Dnes sú na trhu stovky druhov antivírových riešení, od tých menej kvalitných až po tie naozaj dobré ktoré pravidelne obsadzujú popredné priečky.

Užívateľ by mal pri výbere správneho antivírového programu zvážiť jeho účinnosť, dopad na súkromie a náročnosť na výpočtové zdroje. Momentálne medzi najlepšie antivírové riešenia patria programy od spoločností ako sú Bitdefender alebo Kaspersky. Na druhej strane uvádzam porovnanie antivírových programov za rok 2015 známym magazínom PCWorld [28].

Tmavomodrá farba znázorňuje stupeň ochrany, svetlejšia náročnosť na výpočtové zdroje (tu platí vyššie číslo = menšia náročnosť) a najsvetlejší pásik znázorňuje kvalitu UI.



Obr. 3. Porovnanie účinnosti rôznych antivírusových systémov pre rok 2015 [28]

3.1.4 Ochrana portov

Sieťový port je špeciálne číslo od 0 až 65535 ktoré slúži pri komunikácií v počítačových sieťach. Každý port je pridelený na rôznu činnosť pomocou ktorej komunikuje náš počítač so serverom. Niektoré porty sú rezervované na rozličné typy sieťových činností ako prehliadanie webu, posielanie e-mailov, chatovanie atď. Vo všeobecnosti platí, že prvých 1024 portov bolo vytvorených pre špecifické potreby internetovej prevádzky. Napríklad port 21 slúži na zdieľanie súborov (FTP), port 25 je SMTP e-mailový protokol, port 80 je HTTP, port 443 je zase HTTPS slúžiace na prezeranie webu pri používaní SSL šifrovania.

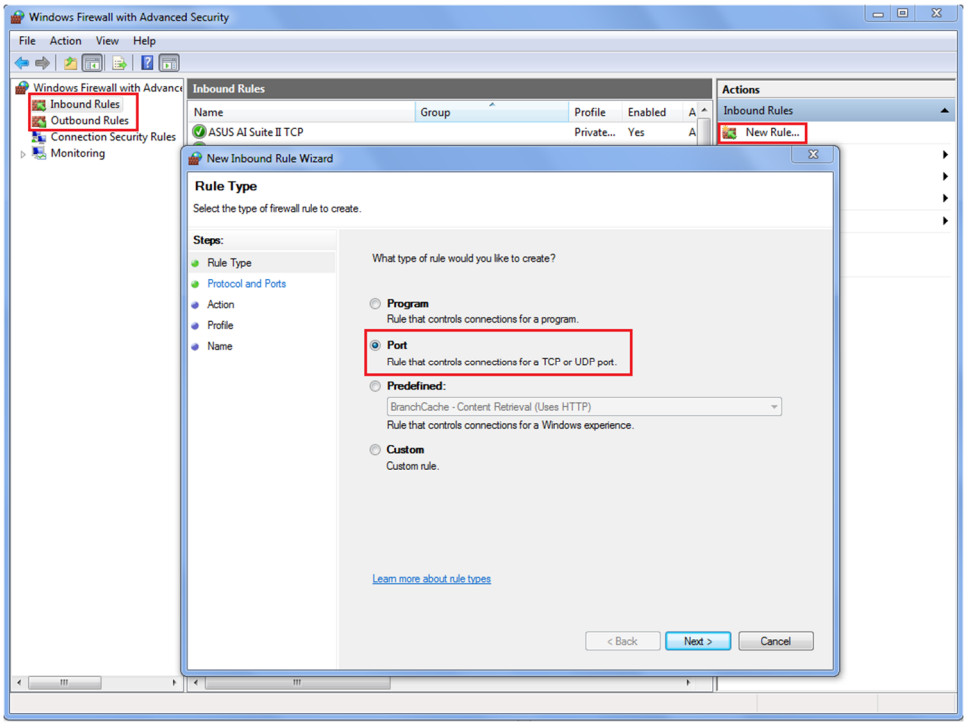
Takto by som mohol pokračovať ďalej. Zvyšné porty, teda 1024 a vyššie neboli vyvíjané na špecifické účely a tým pádom môžu byť využívané ľubovoľne. Porty s číslom 49152 až 65535 sa považujú za dynamické porty. Niekedy práve tieto porty sú zdrojom problémov keďže z času na čas ich využívajú backdoor trójske kone či spyware programy na komunikáciu s kyber-kriminálnikom [5].

Zistenie potencionálne nebezpečných portov a ich zablokovanie

Neznamená to, že teraz musíme zablokovať ručne takmer 20 000 portov. Porty sa dajú predstaviť ako dvere. Pokiaľ sa nepoužívajú, sú zatvorené. Na detegovanie portov ktoré sú otvorené, slúži táto stránka *grc.com*.

Obr. 4. Webová stránka grc.com

Povedzme, že nám stránka identifikovala port 51750 ako otvorený, a aktivita ktorá na ňom prebieha nám nič nehovorí. Zablokovať daný port sa dá jednoducho pomocou nového pravidla v pokročilých nastaveniach Windows Firewall [5].



Obr. 5. Návod ako zablokovať port v systéme Windows 7

3.2 Level 1 – Prehliadače a bezpečnostné doplnky

Výber správneho prehliadača je dôležitá vec ktorá taktiež môže prispieť ku lepšej bezpečnosti užívateľa. V súčasnosti sú k dispozícií desiatky prehliadačov. Každý sa odlišuje či už jadrom alebo funkciami. Lenže netreba zabúdať aj na mieru súkromia a anonymity.

3.2.1 Google Chrome

Vo všeobecnosti sa neodporúča používanie Google Chrome. Tento closed-source prehliadač nielenže odosiela telemetriu priamo centrále, ale prednedávnom mal problémy s doplnkami, ktoré robili snímky obrazovky alebo sledovali pohyb na Internete. Následne zistené informácie predávali tretím stranám [29].

3.2.2 Mozilla Firefox

Open-source prehliadač ktorý kladie dôraz na anonymitu a bezpečnosť. Obsahuje vstavanú webovú ochranu pred sledovačmi alebo vylepšený anonymný režim. Necháva na samotnom užívateľovi aby si vybral množstvo a druh dát ktorý by sa odosielal do centrály. Firefox si výborne rozumie s internetovým vyhľadávačom ako je napríklad DuckDuckGo alebo Disconnect Search, ktoré oproti tradičnému Google vyhľadávaču nezbierajú údaje o užívateľoch. Nutné je však pripomenúť, že dôležitým sponzorom organizácie Mozilla Foundation je práve Google, a bolo by naivné si myslieť, kebyže za to nič nechcel [30].

3.2.3 Project Chromium

Open-source prehliadač založený na rovnakom jadre ako jeho príbuzný Chrome, je vynikajúcou alternatívou pre tých ktorý sa nechcú vzdať Chromu, a zároveň nechcú aby ich správanie sledoval Google. Stále však nemožno zaručiť 100% nezávislosť od tejto spoločnosti.

3.2.4 Epic Privacy Browser

Prehliadač založený na WebKit jadre (Chrome, Chromium) so zabudovanými doplnkami ako je šifrovanie komunikácie medzi klient-serverom, odstraňovanie cookies, blokovanie sledovačov na webových stránkach a celkom vydarená funkcia šifrovaného proxy pripojenia. Je síce nutné podotknúť, že základňa proxy sa nachádza na území USA, čo znamená, že vládne agentúry majú bez problémov dosah na všetko čo ňou prejde, ale ako nástroj ochrany proti tretím stranám obchodujúcimi s našimi údajmi je tento prehliadač výborný. Jedinou nevýhodou je absencia možnosti nainštalovania ďalších bezpečnostných doplnkov.

3.2.5 Bezpečnostné doplnky prehliadača

Samotný prehliadač však nie je všetko. Po tom ako si užívateľ vyberie ten správny, je vhodné zvážiť inštaláciu doplnkov ktoré budú blokovať sledovače a nevyžiadané reklamy.

Disconnect

Vynikajúca open-source ochrana proti sledovacím prvkom na internetových stránkach. Disconnect je v podstate filter ktorý blokuje vyše 2000 rôznych sledovačov patriacich tretím stranám čím znižuje objem prenesených dát a zvyšuje anonymitu. Disconnect taktiež ponúka aj možnosť použiť svoj anonymný internetový vyhľadávač Disconnect Search.

NoScript

Doplnok blokujúci Javu ako takú, JavaSript a Flash rozšírenia. Doplnok výrazne obmedzuje použitie webovej stránky, avšak prehliadanie sa stane oveľa bezpečnejším. Obsahuje Anti-XSS a Anti-Clickjacking ochranu pre prehliadač. NoScript obsahuje aj možnosti udeliť výnimku, kde sa dajú nataviť bezpečné stránky ktorá nebude nijako obmedzovať. Je odporúčaný Edwardom Snowdenom [31].

Ghostery

Doplnok ktorý má rovnaké poslanie ako vyššie spomínaný Dissconnect. Líši sa používateľským rozhraním a širšími možnosťami blokovať obsah stránok. Ghostery dokáže blokovať okrem sledovačov aj majáky, widgety a rôzne pop-up reklamy. Výrazne tým prispieva na ochrane identity. Problémom je fakt, že organizáciu ktorá vyvíjala Ghostery prednedávnom kúpila reklamná spoločnosť Evidion, ktorá sa zaoberá zberom a predávaním dát ostatným reklamným spoločnostiam [32].

HTTPS Everywhere

Doplnok ktorý šifruje komunikáciu pomocou HTTPS protokolu aj na stránkach ktoré začínajú prefixom HTTP. Využíva fakt, že mnohé stránky podporujú pripojenie HTTPS, len ho štandardne nevyužívajú. Tento doplnok prakticky donúti prehliadač použiť šifrovaný prenos vždy pokiaľ to daný web podporuje.

Adblock

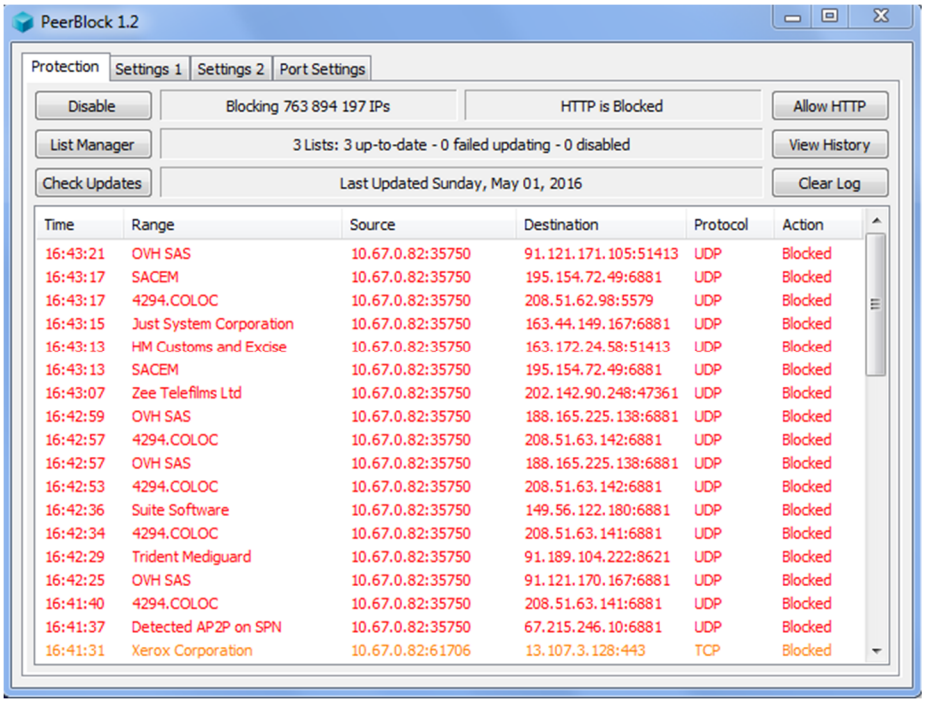
Jednoduchý a známy doplnok na blokovanie a filtrovanie nechcenej reklamy a domén ktoré obsahujú malware. Šetrí prenesené dáta a čas pre načítanie webovej stránky.

3.3 Level 2 - Programy na ochranu identity a údajov

Do tejto kategórie spadajú špeciálne programy ktoré sa už oveľa výraznejším spôsobom podieľajú na ochrane anonymity a zvýšenej internetovej bezpečnosti než obyčajné doplnky do prehliadačov. Všetky uvedené programy sú dostupné zadarmo až na ProxySwitcher.

3.3.1 PeerBlock

Jednoduchý open-source filtrovací program ktorého úlohou je blokovať škodlivé peer-to-peer spojenia s počítačom. Tento program vlastne zablokuje akúkoľvek komunikáciu s potencionálne nebezpečnými a neznámymi servermi. Vždy pri spustený si zaktualizuje čiernu listinu IP adries ktorým následne odoprie prístup do počítača. Negarantuje to však nepriestrelnú anonymitu. Listina nemusí byť vždy aktuálna, avšak výrazne napomáha pri ochrane identity najmä proti spyware, keyloggermi, a firmami živiacimi sa odchytávaním seederov na Torrentoch. Je možnosť používať aj vlastné listiny nebezpečných IP adries.

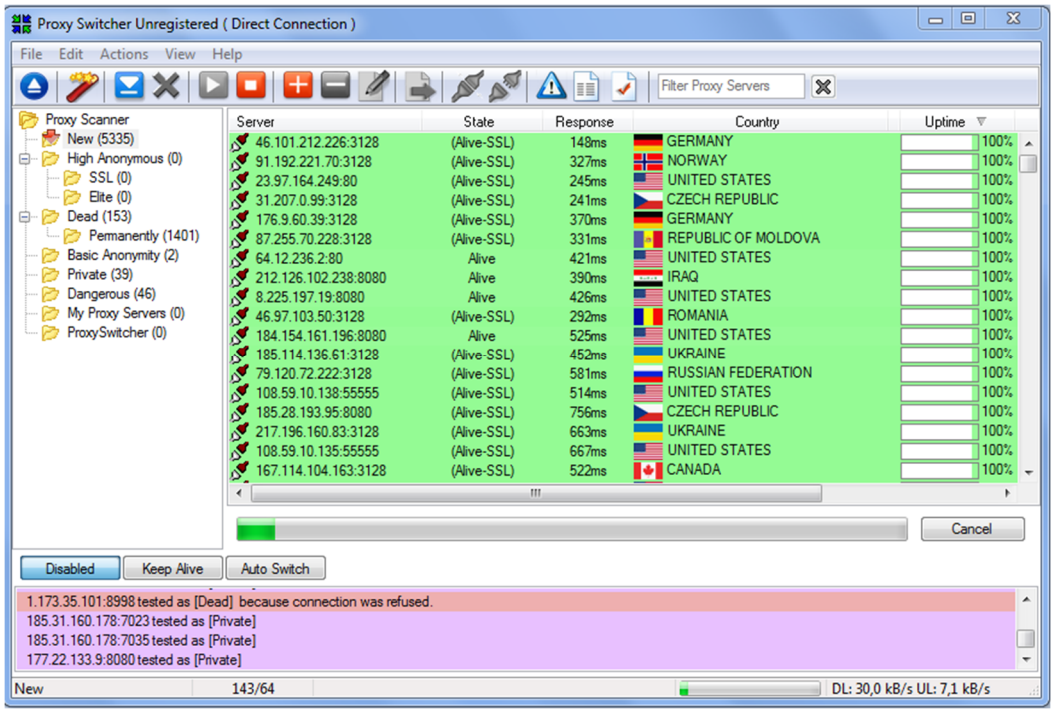


Obr. 6. PeerBlock 1.2 počas blokovania rôznych IP adries

Všimnite si obrovské množstvo potencionálne nebezpečných IP adries ktoré tento program v reálnom čase blokuje. Samozrejme stane sa, že môže blokovať aj neškodnú IP adresu (v mojom prípad začal blokovať komunikáciu s poskytovateľom pripojenia CESNET). Našťastie program ponúka možnosť zaradiť ľubovoľnú IP adresu do bielej listiny [33].

3.3.2 ProxySwitcher

O zraniteľnosti IP adresy a o tom koľko rôznych citlivých informácii dokáže webovej stránke o užívateľovi poskytnúť sa už spomínalo v teoretickej časti. Tu je návod ako tomu zabrániť. Štandardne moja pridelená IP adresa o mne prezrádza presnú polohu, poskytovateľa pripojenia, hostname, či názov inštitúcie na ktorej študujem. Toto je dostatočné množstvo informácií aby spoločnosti zaoberajúce sa zebrom dát si o mne urobili celkom presný obraz. Riešenie? Používanie proxy servera.



Obr. 7. ProxySwitcher

Server proxy je sprostredkovateľ medzi klientom a cieľovým serverom ktorý umožňuje klientom nepriame pripojenie k inému serveru. Prekladá požiadavky klienta a oproti cieľovému serveru vystupuje ako klient. Prijatú požiadavku potom odosiela naspäť klientovi.

Štandardne sa počítač pripája na webový server priamo, čím odhaľuje svoju pravú IP adresu. Program ProxySwitcher obsahuje overené proxy servery cez ktoré automaticky smeruje celé pripojenie na daný webový server. Čo robí tento program výnimočným je jeho funkcia meniť predom vybrané proxy servery vo zvolených časových intervaloch a tým pádom zmiasť potencionálneho kyber-kriminálnika či sledovače. ProxySwitcher podporuje Socksv5 a elitné proxy servery, ktoré okrem samotnej IP adresy zamaskujú aj poskytovateľa siete, operačný systém, a všetky metadáta spojené s užívateľom. Štandardne sa však

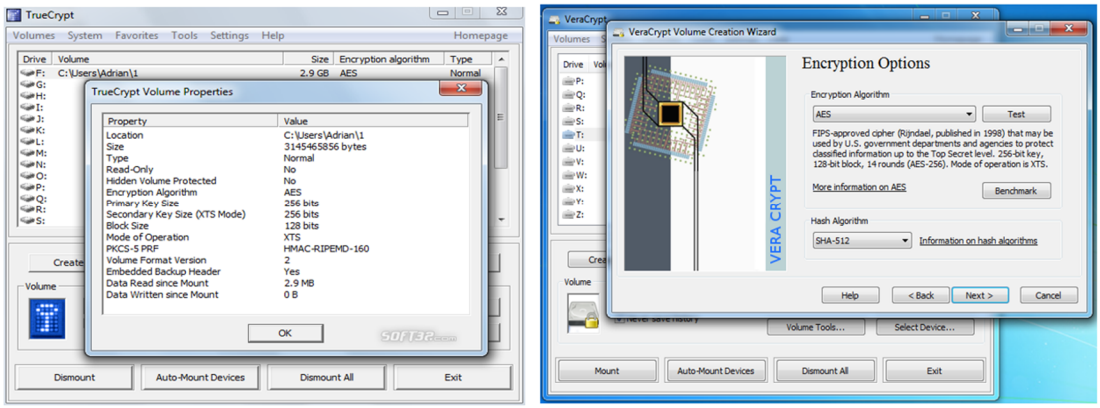
najčastejšie používajú Alive-SSL servery ktoré podporujú SSL pripojenia a tým pádom fungujú aj pre HTTPS protokol [34].

3.3.3 TrueCrypt

Napriek ukončenej podpore kvôli škandálu so zadnými vrátkami pre NSA, TrueCrypt sa naďalej teší vysokej popularite medzi bežnými užívateľmi. Používa sa hlavne na šifrovanie súkromných dát a súborov silnými šiframi ktoré okrem spomínaných vládnych agentúr bežný užívateľ či kyber-kriminálnik nemá šancu prelomiť. Súbory sa môžu schovávať napríklad aj do poznámkového bloku, ktorý sa po pripojení na TrueCrypt správa ako odnímateľný externý disk. Jedinou nevýhodou je, že takýto súbor je manipulovateľný a môže sa ho hocikto jednoducho zmocniť prostým skopírovaním, napríklad na vlastnú flashku.

3.3.4 VeraCrypt

V podstate ide rovnaký o program ktorý je založený na tom istom princípe ako TrueCrypt, len s tým rozdielom, že autori VeraCryptu tvrdia, že chyby ktoré sa vyskytovali v TrueCrypte, tak isto aj zadné vrátka NSA, sa už v tomto programe nevyskytujú a tím pádom by mal byť bezpečnejší. Užívateľské prostredie je iba zľahka odlišné, takže závisí čisto len na užívateľovej preferencii aký program sa rozhodne pre svoju potrebu využívať. S použitím programu TrueCrypt alebo VeraCrypt odporúčam zašifrovať rovno celý externý harddisk. Takto zašifrovaný harddisk je pre bežného smrteľníka prakticky nemožné dešifrovať a užívateľ si môže byť istý, že jeho dáta aj napriek odcudzení fyzického média ostanú neprečítané. Pozor si len treba dať na heslo. Zabudnuté heslo sa už nedá obnoviť a jediný spôsob ako znova použiť daný externý harddisk je iba jeho sformátovaním [35].



Obr. 8. TrueCrypt a VeraCrypt

3.4 Level 3 – Anonymný pohyb Internetom

Riziká používania proxy serverov spočívajú v tom, že nevieme s istotou povedať, že daný server proxy je 100% bezpečný. Je síce pravda, že spomínaný program ProxySwitcher pred pripojením sa na daný server najprv overí a až potom nadviaže spojenie, stále tu však hrozí určité riziko. Medzi to najväčšie rozhodne patrí spoofing, teda sledovanie kompletne celej sieťovej aktivity vrátane otvárania paketov či čítania citlivých údajov alebo dokonca presmerovanie pripojenia na záškodné webové servery. Toto nebezpečie hlavne hrozí pri používaní neznámych „Free Proxy“ ktoré sú voľne dostupné na Internete. Nasledujúce spôsoby bezpečného pripojenia kladú dôraz jak na anonymitu tak aj na bezpečnosť užívateľa.

3.4.1 VPN Tunel

Virtual Private Network, alebo VPN sa správa v podstate rovnako ako proxy server, čo znamená, že pakety smerujú z počítača cez VPN a z neho na požadovaný webový server. Teda rovnako ako u proxy, webový server vidí IP adresu daného VPN a nie našu skutočnú. Hlavným rozdielom oproti proxy je fakt, že VPN využíva šifrovanú komunikáciu čím môže trochu spomaliť pripojenie, ale zato je bezpečnejšie. Tak isto väčšina kvalitných VPN tunelov je spoplatnená. Je vhodné si nevyberať VPN služby ktoré sú lokalizované na území USA kvôli možnostiam sledovania tunajších vládnych agentúr a kvôli faktu, že mnohé VPN servery robia logy ktoré môžu byť neskôr použité/zneužité práve danými agentúrami [36],[37].

3.4.2 SSH Tunel

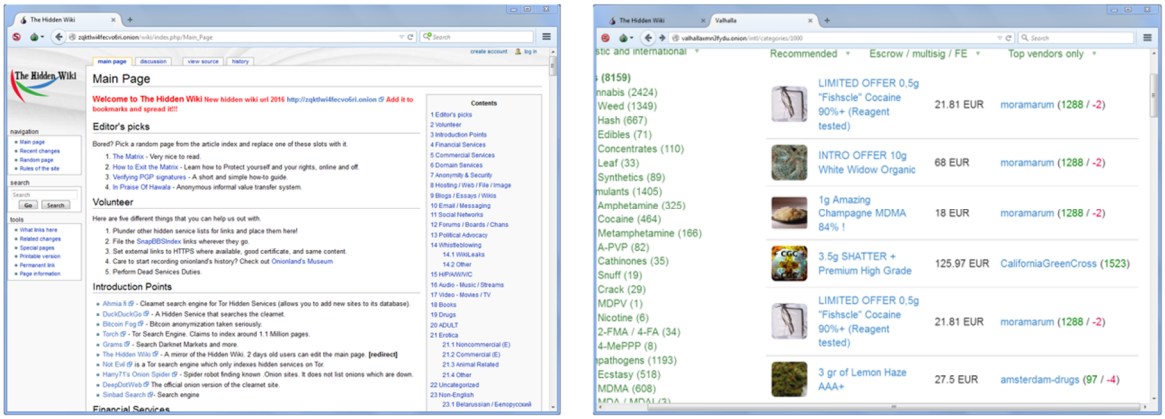
Tento spôsob pripojenia je vhodný pre diaľkové ovládanie terminálu na rôznych serveroch alebo ako bezpečný spôsob transferu dát na súkromné vzdialené úložisko. Skratka SSH znamená secure shell, alebo zabezpečený prístup ku príkazovému interpretovaču. Pre neskúseného užívateľa môže byť používanie SSH tunela oveľa zložitejšie než VPN, pretože na rozdiel od VPN, na používanie SSH je treba nastaviť zvlášť každú jednu aplikáciu. Samotné SSH nebolo ani nikdy dizajnové výhradne iba na prenos internetovej komunikácie aj keď je možné ho nastaviť ako proxy server využívajúci SSH na šifrované pripojenie [36],[37].

3.4.3 Anonymizujúca sieť TOR

TOR (skratka The Onion Router – cibuľový smerovač) je špeciálny druh anonymizujúcej sieťovej služby ktorá je podobná službám VPN. Rozdiel medzi TOR a VPN je ten, že TOR sa správa ako viacreťazové VPN, pretože dáta cestujú zašifrované cez početné uzly situované v rôznych lokalitách na svete, čím zabezpečuje vysokú ochranu pred sledovaním.

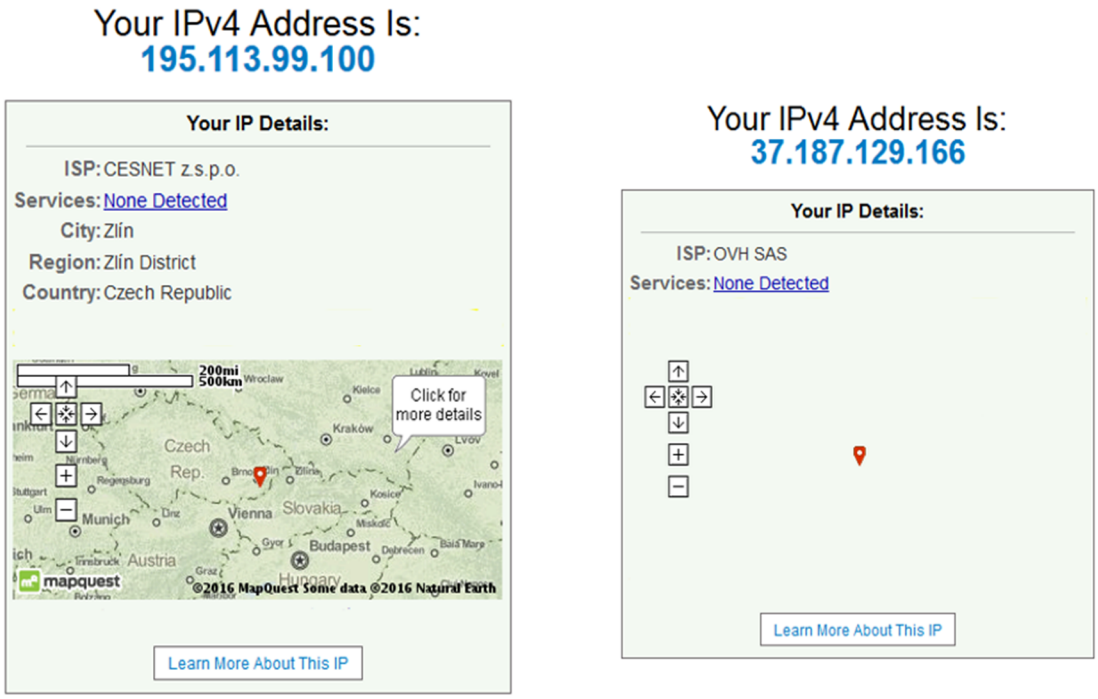
Aby sme mohli využívať túto anonymizujúcu sieť, potrebujeme špeciálny nástroj – TOR prehliadač. Vychádza z moderného Firefoxu a umožňuje používanie jak bežného indexovaného webu v anonymnom režime, tak aj neindexovaného Temného webu. Tento web sa vyznačuje vysokou mierou anonymity užívateľov a absolútnej slobody, čo sa odráža vo zvýšenej kriminalite typu obchody s drogami, zbraňami či ľuďmi.

Užívateľ po prihlásení sa do siete TOR obdrží určitú IP adresu. Tá sa potom mení každým prechodom cez uzol. Daný uzol vidí len IP adresu predchádzajúceho uzla a žiaden uzol nepozná kompletnú cestu. Výsledkom je teda niekoľko vrstiev ochrany a značné zvýšenie anonymity a nemožnosť odchytiť sledované dáta tretími stranami. Edward Snowden tvrdí, že TOR je stále kráľom anonymných sietí. Je využívaný novinármi alebo politickými väzňami či disidentmi. Nutné je však podotknúť, že po roku 2011 už ani TOR nie je to čo býval. Miera anonymity sa zmenšila pretože sa ním začali zaoberať národné bezpečnostné agentúry. Pomocou chyby vo Firefoxe ktorý je oficiálnym prehliadačom TOR, dokázala FBI zistiť pravé IP adresy užívateľov a 17 ľudí skončilo za mrežami. Táto chyba je už opravená, ale istota, že sa podobný incident viac nestane nemôže nikto garantovať [38].



Obr. 9. The Hidden Wiki a rôzne stránky predávajúce drogy sú typické pre TOR

Samotný prehliadač prichádza s predinštalovanými doplnkami. Tieto doplnky je odporúčané ich používať. Ide o známe NoScript a HTTPS Everywhere, ktorý dodatočne šifruje komunikáciu na stránkach Temného webu. Služba TOR spolu s doplnkami nielenže dokáže úspešne schovať užívateľa, ale dokonca danú IP adresu nedokážu rozoznať a lokalizovať ani stránky zamerané na odhalenie IP adries a ich užívateľov (obr. 10). Pri prezeraní Temného Webu treba byť opatrný, pretože mu chýba DNS a tak každá adresa stránky vyzerá ako zhluk čísel a písmen zakončená *.onion*. Pharming je tu teda naozaj jednoduchý.



Obr. 10. IP adresa užívateľa pred a po pripojením sa do TOR siete

Medzi ďalšie nevýhody používania TOR-u patrí, že proces prechádzania cez spomínané uzly je časovo náročnejší, takže sieť je výrazne pomalšia. Potom je hrozba presmerovania na skompromitovaný sever, kde je nebezpečenstvo infikovania sa tzv. majákom, ktorý po skončení používania služby TOR a prihlásení sa do normálnej siete, vyšle už skutočné informácie o danom užívateľovi. Opäť pripomínam, nikto nevie na 100% povedať, či všetky uzly ktoré využíva sieť TOR na presmerovanie dát sú vždy bezpečné. Pre vládne agentúry v reálnom čase nemusí byť až také zložité skompromitovať dostatočné množstvo uzlov až do takej miery, že budú schopný porovnať vstupný a výstupný uzol siete. Vtedy už dokážu nielenže odfiltrovať prenesené dáta, ale aj určiť skutočnú IP adresu a s ním spojeného užívateľa. Preto rozhodne neodporúčam nainštalovanie a pripájanie sa do TOR siete vo vlastnom domácom počítači kde máme svoje dáta a využívame ho na každodennú prácu [5],[8].

3.4.4 Anonymizujúca sieť I2P

Ide o špeciálny druh anonymizujúcej siete ktorá funguje na báze prídavných sieťových bezpečnostných vrstiev ktoré môžu aplikáciám a programom využívať na vzájomnú komunikáciu. Tá potom prebieha cez end-to-end šifrovane (komunikácia pri ktorej sú vzájomné správy schopný prečítať iba dvaja jej účastníci) až štyrmi pridanými vrstvami a na rozdiel od siete TOR, sú používané výstupné uzly zabezpečené sériou verejných kľúčov. Sieť I2P je určená na ochranu pred národným dohľadom a sledovaním poskytovateľov internetových služieb. Je ťažko presne povedať či je lepšie I2P alebo TOR. Každá služba prináša určité výhody a nevýhody. TOR má širšiu užívateľskú základňu, viac zdrojov na opravy bezpečnostných hrozieb a je omnoho jednoduchší na použitie. Zato I2P ponúka oveľa svižnejšie prenosové rýchlosti, hlavne vďaka odlišnému spôsobu fungovania prenášania paketov. Používanie I2P sa odporúča najmä pre tých, ktorý chcú spravovať vlastný obsah na Temnom webe [39].

3.4.5 Anonymná platobná mena Bitcoin

Nič neprezradí toľko o užívateľovi ako samotná platba cez Internet. Síce sa tieto informácie nesmú zdieľať ani predávať tretím stranám a v tomto sektore už platia naozaj prísne pravidlá, predstavme si, že užívateľ má určitý dôvod vykonať čisto anonymnú transakciu. Presne na takéto druhy platieb sa využíva kryptomena Bitcoin. Predstavuje decentralizovanú platobnú menu na ktorej obehu sa nepodieľajú žiadne banky, vládne inštitúcie, a ani nie je obmedzená hranicami. Ide o peer-to-peer zdieľanú technológiu medzi užívateľmi. Je to lacný, bezpečný a veľmi rýchly spôsob platobnej transakcie. Po tom ako si užívateľ zriadi na oficiálnej stránke *bitcoin.org* účet a nainštaluje si open-source program, tzv. peňaženku, získa unikátnu adresu pomocou ktorej môže prijímať svoje Bitcoiny. Každá peňaženka obsahuje privátny kľúč ktorý sa používa ako identifikácia daného užívateľa. Takýto spôsob zabraňuje opakovaniu rovnakej transakcie niekým iným. Všetky transakcie sú sprostredkovávané užívateľmi ktorý sú pripojený v danej sieti. Tento proces sa nazýva ťažba. Ide o systém slúžiaci na potvrdenie a overovanie čakajúcich transakcií zahrnutím ich do hlavnej reťaze v ktorej sa spracujú. Ako motiváciu systém postupne uvoľňuje voľné emisie Bitcoinov, ktoré nie sú viazané žiadnou platobnou transakciou. Ak má užívateľ šťastie a práve jeho počítač spracúva danú emisiu, pripíše sa mu na účet [40].

Nevýhodou Bitcoinov je nestabilný kurz, riziko technických problémov, chýbajúca ochrana spotrebiteľov a fakt, že je stále veľmi málo obchodných miest kde sa dá s nimi zaplatiť.

3.5 Level 4 – Šifrovaná komunikácia

Je potrebné si uvedomiť, že drvivá väčšina všetkých komunikačných nástrojov cez Internet môže byť zneužitá alebo odpočúvaná. Je jedno o aký typ messengeru sa jedná. Každé prináša určitú formu straty anonymity. Pri ICQ je to náchylnosť na spoofing a programy podobné WireSharku, Skype servíruje dáta priamo NSA a pri používaní instantných messengerov na mobilných telefónoch sa otvárajú možnosti ako ukladanie polohy, zapnutie fotoaparátu či mikrofónu, alebo prístup do kontaktov, priečinku SMS správ či galérie. Tie pri slabom šifrovacom mechanizme môžu byť odpočúvané kyber-kriminálnikmi alebo mimo to jednoducho ukladané na server vývojára a predávané tretím stranám.

3.5.1 OTR

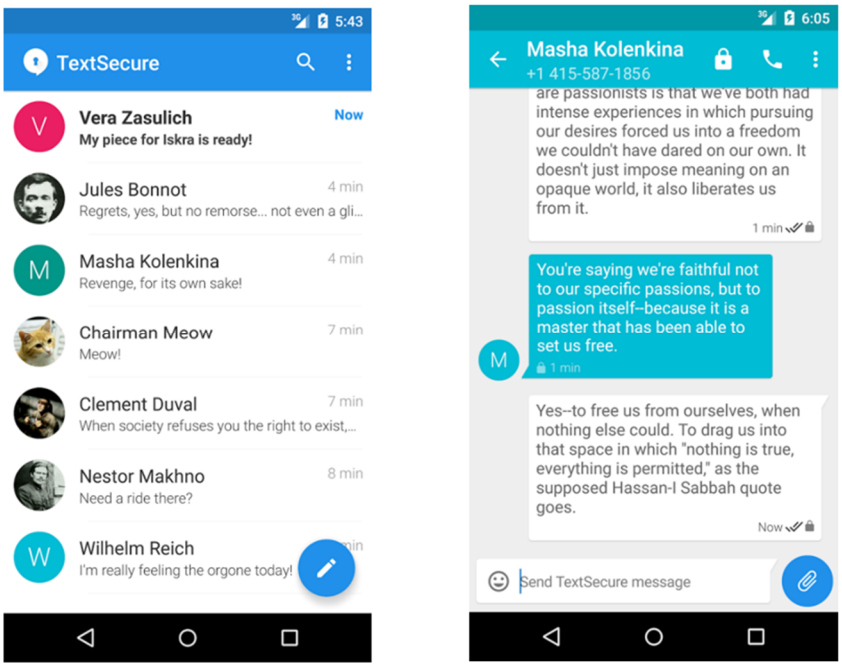
Jedná sa o open-source protokol ktorý umožňuje instantnú šifrovanú komunikáciu medzi dvoma užívateľmi. Skratka OTR znamená Off-the-record (mimo záznam) a pravdivosť tohto názvu potvrdzuje fakt, že vládnej agentúre NSA sa tento spôsob komunikácie stále nedarí úspešne dešifrovať [31]. OTR bol vytvorený ako sťahovateľný doplnok pre open-source messengery ako Pidgin, Jitsi či Adium. V podstate ide o knižnicu ktorá obsahuje nástroje na kompletné zašifrovanie akejkoľvek komunikácie prebiehajúcej cez XMPP server, ktorý využíva drvivá väčšina dnešných messengerov. Užívatelia si na začiatku vymenia dešifrovacie kľúče ktoré im umožnia prečítať správu a kyber-kriminálnik bez kľúča uvidí iba zhluky znakov [41].

3.5.2 PGP

Možnosti ochrany e-mailovej komunikácie je tiež niekoľko. Z môjho pohľadu medzi najlepšiu z nich patrí PGP. Skratka vznikla zo slovného spojenia pretty good privacy (celkom slušné utajenie). Podobne ako OTR, aj PGP funguje ako end-to-end šifrovací doplnok ktorý sa dodatočne inštaluje do e-mailových klientov. Ako klient sa odporúča Thunderbird. PGP je v tomto prípade obsiahnuté v programe **Gpg4win**. Tento program zaistí end-to-end šifrovanie. Pred začatím používania šifrovania, je potrebné získať súkromný a verejný kľúč. Na to sa používa doplnok **Enigmail**, ktorý slúži na výmenu kľúčov medzi komunikujúcimi, taktiež podpisuje odchádzajúce e-maily, čím ich zašifruje súkromným kľúčom ktorý sa da dešifrovať iba s verejným kľúčom odosielateľa. V jednoduchosti sa dá povedať, že PGP sa stará o šifrovanie dát a Enigmail o jednoznačnú autentifikáciu odosielateľa [42].

3.5.3 Signal

Ak už z nejakého dôvodu musíme využívať komunikáciu aj cez mobilné telefóny, tak tento komunikačný klient je asi to najbezpečnejšie čo Android a iOS ponúka. Ako aj vyššie spomenuté, aj táto aplikácia funguje na princípe end-to-end šifrovania. Jedná sa o open-source program ktorý je založený na asymetrickom šifrovaní AES 256, SHA256 a Curve25519. Ide o veľmi silné bezpečnostné hashe, ktorými je zakódovaná správa tak, aby ju dokázal prečítať len odosielateľ a príjemca. Tí si pred začatím konverzácie vymenia dešifrovacie kľúče ktoré im správy budú schopné dešifrovať. Program je vytvorený tak, aby nikto, ani prevádzkovateľ nemohol odchytiť a otvoriť dešifrovať správu [43].



Obr. 11. Užívateľské prostredie aplikácie Signal

Protokoly ako OTR a PGP odporúčam používať pod iným operačným systémom ako je Windows. Úplne postačuje aj základné Ubuntu. Problémom môže byť samotná inštalácia doplnkov a programov, ktorá je pod Linuxom pre neskúseného užívateľa náročnejšia. Všetky spomenuté programy sú vyskúšané a odporúčané Edwardom Snowdenom [31].

3.6 Level 5 – Bezpečnostné operačné systémy

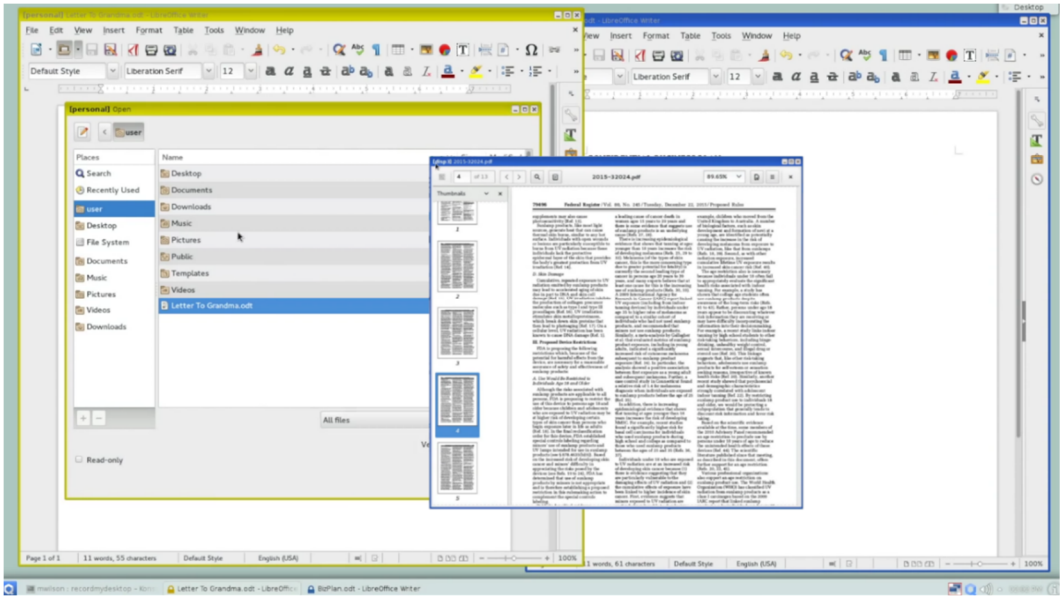
Nie je tajomstvo, že postupom času sa z operačného systému Windows stal nástroj kontroly pre NSA (konkurenčný operačný systém OSX na tom tiež nie je o nič lepšie). O tom, ako Microsoft doslova špehuje užívateľov svojho najnovšieho systému Windows 10, už bolo spomenuté v teoretickej časti. Teraz je na rade si predstaviť operačné systémy, ktoré boli vyvíjané iba pre jednu vec – a tou je bezpečnosť a anonymita užívateľa. Prirodzene sú všetky open-source a založené na Linuxovom jadre. Opäť sa jedná o sériu softwaru ktorý odporúča a aktívne využíva Edward Snowden či zakladateľ investigatívnej webovej stránky Wikileaks.org, Julian Assange [31].

3.6.1 TAILS Live OS

Jednoduchý operačný systém ktorý môže byť rýchlo spustený na akomkoľvek počítači bez potreby inštalácie, a to z médií ako je SD karta alebo USB kľúč. Jeho hlavným účelom je vytvoriť z akéhokoľvek zariadenia bezpečné miesto na komunikáciu či odoslanie citlivých údajov. Všetok software obsiahnutý v tomto operačnom systéme ja nakonfigurovaný na používanie siete TOR alebo I2P. Systém nezanecháva žiadne stopy na hostiteľskom počítači a používa výkonné šifrovacie nástroje (mnohé z nich už tu boli spomenuté) na sieťovú komunikáciu, e-mailovú komunikáciu, alebo na zašifrovanie celého média na ktorom je nainštalovaný. Tails je založený na Debiane a je zadarmo na stiahnutie [44].

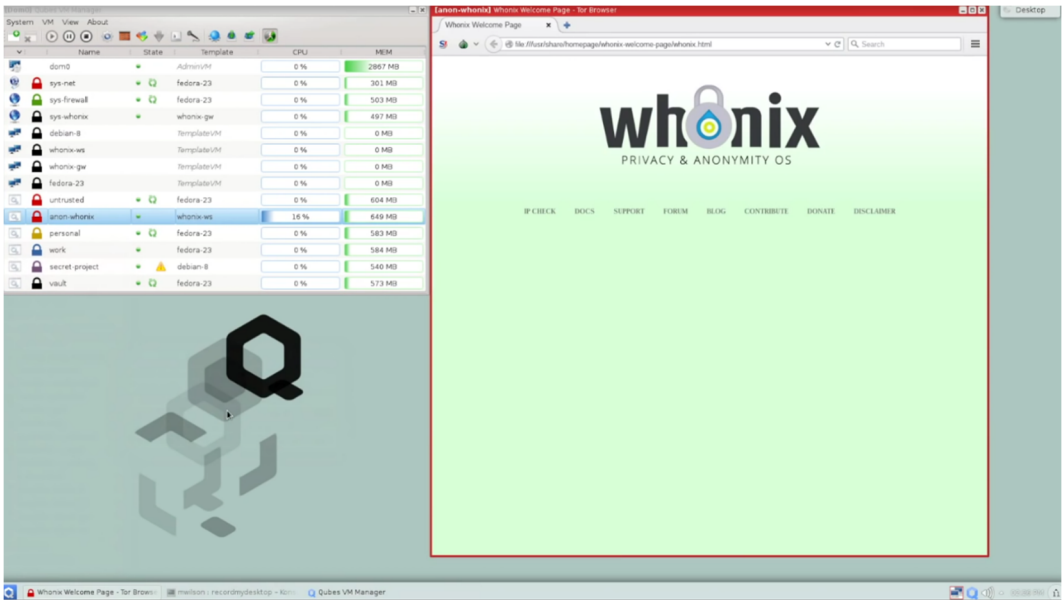
3.6.2 Qubes OS

Momentálne asi jeden z najbezpečnejších operačných systémov súčasnosti. Hlavnou výhodou tohto systému je virtualizácia jednotlivých procesov. Každý jeden program pracuje izolovane bez možnosti vzájomného vplyvu. Dáta a procesy sú od seba kompletne izolované, každé vo svojom vlastnom virtuálnom prostredí. Tým pádom ak užívateľ stiahol škodlivý materiál z Internetu, ostane iba v danom virtuálnom prostredí bez možnosti sa šíriť ďalej. Takto je možno používať niekoľko virtuálnych prostredí naraz, napríklad na prácu, na bankovníctvo alebo na správu citlivých či nebezpečných dokumentov. Výbornou vlastnosťou je aj okamžité vytvorenie dočasného virtuálneho prostredia napr. pre stiahnutý súbor z neznámeho zdroja. Nech ide o akokoľvek škodlivý súbor, zo svojho prostredia sa už viac nedokáže šíriť.



Obr. 12.Jednotlivé virtualizácie sú oddelené farebne

Qubes prichádza taktiež s predinštalovaným operačným systémom Whonix, ktorý pracuje rovnako v oddelenom virtuálnom prostredí. Whonix slúži ako zabezpečený prístupový bod do TOR siete. Šifruje komunikáciu, nezanecháva stopy, a je navrhnutý tak, že ani malware s root oprávneniami nie je schopný zistiť skutočnú IP adresu užívateľa [45].



Obr. 13. Whonix ako prístupová brána do TOR-u

ZÁVĚR

Anonymita je dôležitá, a málokto si to uvedomuje, Mnohí ľudia v mene pohodlia obetujú svoje súkromie, a potom neveria vlastným očiam keď sa stanú obeťami profilácie alebo kyber-kriminálnika. Ochrana súkromia a anonymity ale naozaj nie je žiadna veda. Stačí len trochu rozmýšľať kam sa vybrať na Internete, čo si z neho stiahnuť, komu zverejniť svoje údaje a ako s nimi daná organizácia naloží.

Moje odporúčanie pre bežného užívateľa je nasledujúce – kombinovať uvedené spôsoby. Používanie prehliadaču Mozilla Firefox alebo Chromium so zabudovaným vyhľadávačom DuckDuckGo a so všetkými spomenutými doplnkami, ktorý beží na bezpečnom operačnom systéme Qubes OS. Vysoko odporúčam aj pripájať sa do siete cez kvalitné VPN mimo USA, alebo nejaký bezpečný proxy server. Dodatočným používaním programov ako PeerBlocker či VeraCrypt sa jednak zvýši bezpečnosť systému a tak isto sa vyrieši väčšina strastí či už so s odcudzeným fyzickým úložným priestorom alebo s kyber-kriminálnikmi.

Ale čo ak ani to nestačí? Potom odporúčam jedine prístup na Internet z cudzích, ale zabezpečených prístupových bodov a počítačov. Presne na to slúži Tails Live OS ktorý je možné nabootovať na hocijakom zariadení pre bezpečný prístup na Internet.

A čo ak sa niekto nemôže vzdať používania systému Windows? Tak vtedy odporúčam sa vrátiť na Windows 7, najmä pre možnosť správy aktualizácií čo pri Windowse 10 chýba, a nainštalovať si všetky spomenuté bezpečnostné opatrenia okrem TOR-u, a sledovať a hlavne čítať si popis a druh aktualizácií ktoré si užívateľ inštaluje.

Zaručiť 100% anonymitu je mimoriadne zložitý a finančne veľmi náročný krok, vyžadujúci mnohé ústupky zo strany užívateľa. S programami ktoré sú zadarmo, je možné dosiahnuť slušnú, nie však úplne celkovú anonymitu. Treba si aj uvedomiť, že vládne agentúry ako NSA, nemajú rady keď ľudia používajú neprirodzené bezpečnostné opatrenia a siete ako je TOR, pretože je relatívne zložité v nich dolovať informácie. Technicky, TOR by mal byť používaný iba ak je to naozaj nutné, keďže okrem anonymity na seba pútame aj pozornosť už spomínaných vládnych agentúr. No napriek tomu, ak sa ku tomu ešte pripočíta operačný systém z rodiny Linux, anonymné platby vo forme Bitcoinov, či náhodné zmeny IP adresy napríklad každých 20 sekúnd, môžeme si byť celkom istý, že našu identitu sa len tak ľahko nikto nedozvie. Problémom už len ostáva stále nízka prenosová rýchlosť a relatívne slabé užívateľské rozhranie.

SEZNAM POUŽITÉ LITERATURY

[1] Malware Fundamentals. *Youtube* [Youtube video]. Kaspersky Lab, 27.07.2012 [cit. 2016-05-14]. Dostupné z: https://www.youtube.com/watch?v=afzkoB_lYNk

[2] *Verizon Data Breach Investigations Reports: Cybersecurity's most comprehensive investigations report.* [online]. Verizon, 2015 [cit. 2016-05-14]. Dostupné z: http://www.verizonenterprise.com/verizon-insights-lab/dbir/

[3] *Malware Classifications* [online]. Kaspersky lab, 2012 [cit. 2016-05-14]. Dostupné z: http://www.kaspersky.com/internet-security-center/threats/malware-classifications

[4] NBC website hacked and distributes malware – here's what happened. DUCKLIN, Paul. *Nakedsecurity by Sophos* [online]. 22.02.2013 [cit. 2016-05-14]. Dostupné z: https://nakedsecurity.sophos.com/2013/02/22/nbc-website-hacked-and-distributes-malware/

[5] BAILEY, Matthew. *Complete Guide to Internet Privacy, Anonymity & Security*. 2. vydanie. United States: Nerel Online, 2015, 260 s. ISBN 3950309349.

[6] SZOR, Peter. *Počítačové viry: analýza útoku a obrana*. Brno: Zoner Press, 2006, 608 s. Encyklopedie Zoner Press. ISBN 8086815048.

[7] Internet Security Threats [online]. Kaspersky Lab, 2015 [cit. 2016-05-14]. Dostupné z: http://www.kaspersky.com/internet-security-center/threats/all-articles

[8] PETROWSKI, Thorsten. Bezpečí na internetu: pro všechny. Liberec: Dialog, 2014, 243 s. Tajemství. ISBN 9788074240669.

[9] Ransomvér CryptoWall 3.0 zarobil stovky miliónov. Jedinej skupine. *Zive.sk* [online]. 02.11.2015 [cit. 2015-12-18]. Dostupné z: http://www.zive.sk/clanok/109653/ransomver-cryptowall-3-0-zarobil-stovky-milionov-jedinej-skupine

[10] *Google: Sběr dat na internetu? Zásadní je možnost říct ne* [online]. Praha: Česká Televize, 2015, 28.06.2015 [cit. 2016-05-14]. Dostupné z: http://www.ceskatelevize.cz/ct24/ekonomika/1540310-google-sber-dat-na-internetu-zasadni-je-moznost-rict-ne

[11] EXLEY, Helen. *Večné hodnoty*. Bratislava: Slovart, 2005, 135s. ISBN 80-8085-025-9

[12] Edward Snowden Biography [online]. [cit. 2016-05-15]. Dostupné z: http://www.biography.com/people/edward-snowden-21262897

[13] Malware. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 23.11.2015 [cit. 2015-12-18]. Dostupné z: https://sk.wikipedia.org/wiki/Malware

[14] HÁK, Igor. *Moderní počítačové viry*. Tretí vydáni. Brno, 2005, 110 s.

[15] About Wireshark. *Wireshark* [online]. [cit. 2016-05-15]. Dostupné z: https://www.wireshark.org/#learnWS

[16] HILL, Kashmir. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. *Forbes* [online]. 2012 [cit. 2016-05-15]. Dostupné z: http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#1de4b3dd34c6

[17] Tracker Basics: What You Need to Know About Trackers. *Ghostery.com* [online]. [cit. 2016-05-15]. Dostupné z: https://www.ghostery.com/intelligence/tracker-basics/

[18] User's Facebook Data Request Produces 1222 Pg PDF on CD. *Tomsguide.com* [online]. 2011 [cit. 2016-05-15]. Dostupné z: http://www.tomsguide.com/us/Facebook-Max-Schrems-EU-Directive-Privacy-Data-Collection,news-13529.html

[19] RASHID, Fahmida. Windows 7, 8, and 10: Now all collecting user data for Microsoft. InfoWorld [online]. 2015 [cit. 2016-05-15]. Dostupné z: http://www.infoworld.com/article/2979054/windows-security/windows-7-8-10-now-all-collecting-user-data-for-microsoft.html

[20] Prehlásenie o ochrane osobných údajov: Zhromažďované údaje. *Microsoft: Windows* [online]. 2015 [cit. 2016-05-15]. Dostupné z: http://windows.microsoft.com/sk-sk/windows/preview-privacy-statement

[21] Už i na Skypu může uživatele sledovat policie a úředníci. TechNet.cz [online]. 2012, 26.02.2012 [cit. 2016-05-15]. Dostupné z: http://technet.idnes.cz/skype-policii-snadneji-zpristupnuje-chat-a-udaje-o-uzivatelich-psg-/sw_internet.aspx?c=A120726_153725_sw_internet_kuz

[22] Aké údaje Google zhromažďuje? Google [online]. 2016 [cit. 2016-05-15]. Dostupné z: https://privacy.google.com/

[23] Cieľ NSA? Eliminácia súkromia jednotlivca. Živé.sk [online]. 2013 [cit. 2016-05-15]. Dostupné z: http://www.zive.sk/clanok/71013/ciel-nsa-eliminacia-sukromia-jednotlivca

[24] NSA vraj využívala chybu Heartbleed, zmena hesla nestačí. *Živé.sk* [online]. 2014 [cit. 2016-05-15]. Dostupné z: http://www.zive.sk/clanok/94958/nsa-vraj-vyuzivala-chybu-heartbleed-zmena-hesla-nestaci

[25] NSA Prism program slides. The Guardian [online]. 2013 [cit. 2016-05-15]. Dostupné z: http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

[26] SNOWDEN, Edward. *XKeyScore*. NSA, 2008.

[27] NEWTON, Casey. Hacker successfully uses Heartbleed to retrieve private security keys [online]. 2014 [cit. 2016-05-15]. Dostupné z: http://www.theverge.com/us-world/2014/4/11/5606524/hacker-successfully-uses-heartbleed-to-retrieve-private-security-keys

[28] HACHAMN, Mark. BitDefender, Kaspersky top list of best Windows 8.1 antivirus software. PCWorld [online]. 2015 [cit. 2016-05-15]. Dostupné z: http://www.pcworld.com/article/2901447/bitdefender-kaspersky-top-list-of-best-windows-81-antivirus-software.html

[29] Rozšírenie Awesome screenshot vás špehuje. *CItadelo.sk* [online]. 2014 [cit. 2016-05-15]. Dostupné z: https://www.citadelo.sk/rozsirenie-awesome-screenshot-vas-spehuje/

[30] MURPHY, David. Google Paying Mozilla Almost $1B for Firefox Search: Why? *PCMag.com* [online]. 2011 [cit. 2016-05-15]. Dostupné z: http://www.pcmag.com/article2/0,2817,2398046,00.asp

[31] ARMASU, Lucian. These Are Edward Snowden's Favorite Security Tools. *Tom's Hardware US* [online]. 2015 [cit. 2016-05-15]. Dostupné z: http://www.tomshardware.com/news/edward-snowden-favorite-security-tools,30507.html

[32] SIMONITE, Tom. A Popular Ad Blocker Also Helps the Ad Industry. MIT Technology Review [online]. 2013 [cit. 2016-05-15]. Dostupné z: https://www.technologyreview.com/s/516156/a-popular-ad-blocker-also-helps-the-ad-industry/

[33] *What is peerblock* [online]. 2013 [cit. 2015-12-18]. Dostupné z: http://www.peerblock.com/docs/faq#what_is_peerblock

[34] *ProxySwitcher: Knowledge base* [online]. [cit. 2015-12-18]. Dostupné z: https://www.proxyswitcher.com/kb.html

[35] *What does VeraCrypt bring to you?* [online]. 2016 [cit. 2016-05-15]. Dostupné z: https://veracrypt.codeplex.com/

[36] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, a.s., 2015, 184 s. Průvodce. ISBN 9788024754536.

[37] HOFFMAN, Chriss. VPN vs. SSH Tunnel: Which Is More Secure? Howtogeek.com [online]. 2012 [cit. 2016-05-15]. Dostupné z: http://www.howtogeek.com/118145/vpn-vs.-ssh-tunnel-which-is-more-secure/

[38] WARRE, Conrade. How Tor Works. *Massachusetts Institute of Technology* [online]. 2014 [cit. 2016-05-15]. Dostupné z: http://video.mit.edu/watch/how-tor-works-502/

[39] *The Invisible Internet Project* [online]. 2015 [cit. 2016-05-15]. Dostupné z: https://geti2p.net/en/

[40] How does Bitcoin work?: The basics for a new user. *Bitcoin.org* [online]. 2014 [cit. 2016-05-15]. Dostupné z: https://bitcoin.org/en/how-it-works

[41] *Off-the-Record Messaging* [online]. 2016 [cit. 2016-05-15]. Dostupné z: https://otr.cypherpunks.ca/

[42] *How to: Use PGP for Windows* [online]. Surveillance Self Defense, 2015 [cit. 2016-05-15]. Dostupné z: https://ssd.eff.org/en/module/how-use-pgp-windows

[43] *Private messaging* [online]. Open Whisper Systems, 2016 [cit. 2016-05-15]. Dostupné z: https://whispersystems.org/#encrypted_texts

[44] About. *Tails* [online]. 2016 [cit. 2016-05-15]. Dostupné z: https://tails.boum.org/about/index.en.html

[45] *Qubes OS: A reasonably secure operating system* [online]. 2016 [cit. 2016-05-15]. Dostupné z: https://www.qubes-os.org/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
Atď.	A tak ďalej
DNS	Domain Name System
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
I2P	Invisible Internet Project
Napr.	Napríklad
NSA	National Security Agency
OTR	Off The Record messaging
OS	Operating System
PC	Personal Computer
RSA	Rivest-Shamir-Adleman algorithm
RSS	Rich Site Summary
SD	Secure Digital
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TOR	The Onion Router
Tzv.	Takzvané
VPN	Virtual Private Network
URL	Unifrom Ressource Locator
USB	Universal Serial Bus
XMPP	Extensible Messaging and Presence Protocol

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

CD s elektronickou verziou tejto bakalárskej práce vo formáte PDF