Monitorování uživatelů zásuvnými moduly pro Internetové prohlížeče

Filip Kotásek

Bakalářská práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav počítačových a komunikačních systémů

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Filip Kotásek**
Osobní číslo:	**A17127**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**Prezenční**
Téma práce:	**Monitorování uživatelů zásuvnými moduly pro Internetové prohlížeče**
Téma práce anglicky:	**Spying on Users Using Plugins for Internet Browsers**

Zásady pro vypracování

1. Vyjmenujte základní informace a rizika související s monitoringem uživatelů.
2. Specifikujte cílovou skupinu, pro kterou jsou uživatelské informace určeny a popište význam uživatelských informací.
3. Vysvětlete pojem anonymita v prostředí internetu a uveďte prostředky, kterými ji lze dosáhnout.
4. Definujte způsoby identifikace uživatele.
5. Proveďte rozbor alespoň tří internetových doplňků do prohlížečů, které by mohly odesílat informace o uživatelích.

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

Seznam doporučené literatury:

1. SCHNEIER, Bruce. *Data and Goliath: the hidden battles to collect your data and control your world*. New York: W. W. Norton & Company, [2015]. ISBN 978-0-393-24481-6.
2. KISSELL, Joe. *Take Control of Your Online Privacy*. Second Edition. New York: TidBITS Publishing, 2015. ISBN 978-1-61542-454-2.
3. JADALI, Sam. *DataSpii: The catastrophic data leak via browser extensions* [online]. USA: Jadali, 2019 [cit. 2019-11-13]. Dostupné z: https://securitywithsam.com/2019/07/dataspii-leak-via-browser-extensions/
4. *OWASP Foundation* [online]. US: OWASP Foundation, 2019 [cit. 2019-11-22]. Dostupné z: https://www.owasp.org/index.php/Main_Page
5. NADER, Youssef. Top 10 Open Source Security Testing Tools for Web Applications. In: *Hackr.io* [online]. hackr.io, 2019, listopad 2019 [cit. 2019-11-22]. Dostupné z: https://hackr.io/blog/top-10-open-source-security-testing-tools-for-web-applications

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **19. prosince 2019**
Termín odevzdání bakalářské práce: **27. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. Ing. Martin Sysel, Ph.D.
garant oboru

Ve Zlíně dne 19. prosince 2019

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 diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a 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 – diplomovou/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 bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 3. 8. 2020

Filip Kotásek, v.r.
……..
podpis diplomanta

ABSTRAKT

Bakalářská práce s názvem *Monitorování uživatelů zásuvnými moduly pro In-ternetové prohlížeče* podává informace o soukromí, anonymitě uživatelů, které významným způsobem ovlivňují bezpečí uživatelů na internetu. Práce je členěna do dvou částí, první teoretická část informuje o základních hrozbách zneužití informací na základě monitoringu lidí, definuje hodnotu informací a sděluje základní pravidla pro zachování uživatelského soukromí či anonymity. Druhá praktická část je zaměřena na konkrétní výzkum deseti pluginů do internetových prohlížečů, kde hlavním kritériem je, zda zkoumané pluginy jsou vhodné k běžnému používání bez nadměrného sběru informací o uživatelích.

Klíčová slova: internet, anonymita, soukromí, plugin do prohlížeče, VPN, monitoring uživatelů

ABSTRACT

This bachelors thesis with the name *Spying on Users Using Plugins for Internet Browsers* provides information on privacy and on the anonymity of users, which in an immense way influences the safety of users on the internet. The study is divided into two parts, first being theoretical and second practical. The first part familiarizes the basic threats that come with abusing information acquired by monitoring people. It also defines the value of information and shares the basic rules for maintaining user privacy and anonymity. The second part, practical, focuses on a specific study on 10 plugins within the Internet browsers, with the main criteria being if the studied plugins are appropriate for common use without collecting an excessive amount of information about its users.

Keywords: internet, anonymity, privacy, browser extension, VPN, user monitoring

Poděkování, motto a čestné prohlášení, že odevzdaná verze bakalářské práce a verze elektronická, nahraná do IS/STAG jsou totožné ve znění:

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

OBSAH

ÚVOD

Bakalářská práce s názvem Monitorování uživatelů zásuvnými modely pro internetové prohlížeče se zabývá problematikou soukromí, anonymity, bezpečnosti a monitoringu uživatelů pohybujících se v prostředí internetu. Internet jako světová síť nabízí obrovské množství příležitostí jak jej využívat a to jak pro dobré účely, tak i pro ty špatné. V naší práci se nezabýváme přímo nelegálními záležitostmi, jako jsou například hackerské útoky, krádeže bankovních účtů apod. Spíše se snažíme proniknout do oblastí, které jsou ve světě internetu tzv. „na hraně“. Na této hranici je postaveno právě monitorování uživatelů. Pro některé z nás může být přirozené, pro jiné naopak představuje zásah do soukromí, který je pro ně velmi obtěžující.

V naší práci rozebíráme tématiku monitorování, kterou dále zužujeme až k monitoringu skrz pluginy do prohlížečů, které si tisíce lidí po celém světě doinstalovávají a nemusí ani vědět, že právě tento doplněk je může sledovat.

Práce je členěna do dvou částí. První, teoretická část, odpovídá na základní otázky ohledně monitoringu uživatelů, jinými slovy vysvětluje, proč se to tak děje a jak nebezpečné to může být. Dále popisuje hodnotu uživatelských dat a definuje ty základní, která by si měl každý z nás chránit. Dalším tématem, kterého se v teoretické části práce dotýkáme, je anonymita na internetu. Zajímají nás způsoby, kterými lze svou anonymitu zvýšit. V poslední kapitole podáváme informace o prostředcích, pomocí nichž lze cílového uživatele identifikovat.

Praktická část se zaměřuje na pluginy do prohlížečů a zjišťuje, zda jsou bezpečné k použití vzhledem k uživatelskému soukromí či nikoliv. Celkově tato práce obsahuje rozbor deseti doplňků.

I. TEORETICKÁ ČÁST

1 MONITORING UŽIVATELŮ

V dnešní době se každý člověk, alespoň v trochu moderní společnosti, ať chce nebo nechce, setkává s různými technologiemi. Právě rozmach nových digitálních a počítačových technologií stojí za monitoringem uživatelů. Obchodovat se dá téměř se vším a uživatelská data nejsou výjimkou. [1]

Každý z nás vlastní mobilní telefon, který uživatelům umožňuje využívat jeho funkce. Ale taky za to každý něčím platí, sice nepřímo, ale platí. Telefonní operátor nebo kdokoliv jiný komu je povoleno sledovat polohu, může přesně vědět, kde se daná osoba nachází, jak často a s kým je v kontaktu. Dokáže zmapovat místa, kde se často pohybuje, do jaké restaurace chodí na jídlo, zda navštěvuje kostel, jak často, dokonce i druh vyznání. Dříve na zjištění těchto informací museli policisté nebo jiní vyšetřovatelé trávit hodiny sledováním, aby cokoliv zjistili, ale v dnešní době stačí používat telefon. A my jako uživatelé bohužel nemůžeme přesně vědět, co se s těmito daty dále děje. [1] [2]

1.1 Každá technologie tvoří data

Každý počítač pracuje s daty a ty jsou jeho vstupem i výstupem. Data počítače tvoří, data se dají dále využívat, data jsou vedlejší produkt počítačů. Data jsou zkrátka nutné pro fungování všech systémů a může docházet k jejich sběru. Jakmile se uskuteční připojení na internet, tak se dat začne tvořit mnohem víc. Tvoří se data o tom, jaká stránka byla navštívena, jaká slova vyhledávána, na jakou reklamu bylo kliknuto atd. Kombinací těch všech informací je možné jedinečně identifikovat počítač. [2] [3]

Moderní auta jsou dnes řízena počítačem, tudíž také produkují data, počítače jsou i u kol, kde se hlídá tlak pneumatik. Pokud nastane nějaká porucha, tak první věc, jež technik v servisu udělá je, že připojí auto k dalšímu počítači, ten vezme všechna data, která byla shromažďována v daném autě a pak diagnostikuje problém. [2] [4]

Využíváním komunikačních prostředků a sociálních sítí, jako je email, Facebook, Instagram, Snapchat a dalších, data vytváříme. Všechny tyto služby si o nás ukládají informace.

Proto platí jedno zlaté pravidlo: to co je na internet nahráno, tam někde pořád bude a je možné, že je veřejně dohledatelné. Pokud budou nějaká data uložena třeba na cloudu a poté jsou z toho cloudu smazána, tak nám nikdo nedá jistotu, že to není uloženo někde jinde nebo to někdo jiný nezkopíroval. [1] [5]

Můžeme být svědky toho, že se vše mění na počítač, chytré hodinky jsou vlastně počítač, jenž udává čas a může také pomocí senzorů tvořit data o zdravotním stavu. Mobil je počítač, co zprostředkovává hovory, auto je počítač, co řídí motor a kola. [2]

I přes obrovské množství produkovaných dat to nemusí nutně znamenat nedůvěru ze strany toho, o kom jsou informace shromažďovány. Většina dat je prostě přirozeným vedlejším produktem moderních technologií. [1] [2]

1.2 Pod masovým dohledem

Vlády a velké firmy shromažďují, ukládají a analyzují obrovské množství dat. Shromažďování těchto dat o uživateli vypoví dostatek informací, ze kterých mohou být vyvozovány závěry o sledovaných. Ať chceme nebo ne, každý je pod masovým dohledem. [2] [6]

1.2.1 Google

Data z webového vyhledávání jsou dalším zdrojem osobních informací. Webovému vyhledavači člověk sděluje víc informací, než třeba kamarádům a blízkým. Vyhledavači se nelže, uživatel mu vždycky sdělí, na co myslí a formuluje tyto informace ve slovech. Google ví, jaké auta se uživateli líbí, může vědět, za co se uživatel stydí a z čeho má obavy. Google si pamatuje všechno dokonale a navždy. [2]

Sám CEO Googlu Erik Schmidt v roce 2010 řekl: *„My víme, kde jste, víme, kde jste byli a můžeme víceméně vědět, na co myslíte.“* A to řekl před deseti lety, teď to mohlo přejít ještě dál. [7]

Google není jenom vyhledávač, ale je to také poskytovatel spousty ostatních služeb. Google využívá vše, co ví, aby uživateli nabídl reklamu, jež ho zaujme. Takovým způsobem Google vydělává peníze. Čím více služeb používáme, tím více toho Google ví. [1] [8]

Dokonce se lze na adrese takeout.google.com podívat, co Google ví za informace a stáhnout si je. Podobná možnost je i na Facebooku. [8]

Teď se nabízí otázka, zda Google dokáže naše data chránit napořád a před všemi. A kdo dá uživatelům jistotu, že se s daty zachází, jak by se mělo a jsou shromažďovány pouze kvůli vylepšování svých služeb a reklamě. Na druhou stranu Google nechce nějakým způsobem poškozovat uživatele, ale jedná se o obří firmu a primárně se zaměřuje na zisk a jiné ekonomické ukazatele, nejvyšší prioritou není chránit uživatelské soukromí. [1] [2] [8]

Ale není to jenom u Googlu, dělají to i jiné společnosti se srovnatelnými službami (Microsoft, Yahoo atd.) Čím více údajů o vás jakákoli společnost vlastní, tím větší jsou rizika pro soukromí v jejich rukou. [1] [2]

Ale není to tak negativní, jak se na první pohled zdá, ač Google informace o uživatelích sbírá, dává jim za to spoustu výhod jako například využívání jeho služeb. A nabízí možnost toto sledování omezit, ale nikdy nemáme stoprocentní jistotu.

1.2.2 Historie polohy Google

Jako příklad sledování uživatelů uvedu tuto službu od Googlu-historii polohy. Google sbírá data, kde jsme byli, jak dlouho, jak dlouho zabrala cesta atd. Je zde možnost vidět interaktivní mapu a prohlédnout si, kde uživatel byl, v přesném čase na přesném místě. [9] [10]

Google říká, že je možné toto sledování vypnout, ale není to tak úplně pravda. Po vypnutí této služby, se služba stane neaktivní, ale polohu stále Google snímá, přes jiné služby, a to například přes Google mapy nebo obyčejné vyhledávání. Problémem je, že jednoduše nejde vypnout sledování polohy a musí se to dělat složitěji přes více druhů nastavení. Působí to tak, jako by Google nechtěl umožnit uživatelům jednoduché vypnutí sledování, ale musí, tak to vymyslel velmi složitě. [9] [10]

1.2.3 Edward Snowden

Účelem této kapitoly nebylo nějak vystrašit čtenáře, ale uvést je do problému a poukázat na to, co je všechno možné podle získaných informací vědět.

Někomu to může znít jako pohádka a mně také tak zněla, ale po výpovědi Edwarda Snowdena se můj pohled na tuto problematiku změnil a uvědomil jsem si, že internet není prostor, kde nikdo neví, kdo jsme, ale ví se to moc dobře. [6]

Odhalení vyšlo roku 2013 a bylo zjištěno, že věci, jež byly dosud pokládané jako soukromé, byly masově shromažďovány. Jednalo se například o telefonní záznamy, e-maily, nahrávky konverzací Skype a další data. [1] [6]

To všechno se údajně děje za účelem prevence terorismu nebo odhalování zločinců. Někdo si to vykládá, že je to nějaká platba za větší bezpečí, někdo to chápe tak, že se jedná o zneužití moci a omezování svobody. Ať si každý souhlasí s tím, co považuje za sobě bližší, ale faktem zůstává, že došlo a stále dochází k masivnímu sběru údajů. [1] [6]

Problém vzniká tam, pokud sesbíraná data budou špatně vyložena. Pak to může mít neblahé následky. I filtr na spam v emailu není naprosto dokonalý a občas tam umí spadnout něco, co nechceme, tak i monitorovaná osoba, která nic neudělala, se může dostat do problémů a zcela bez viny. [1] [6]

Tento muž se zasloužil o odhalení nekalých praktik americké vlády, přesněji služby NSA, kde popisuje, co je všechno možné. Za toto odhalení musel uniknout z USA a v případě návratu mu hrozí doživotí, nyní pobývá v Rusku.

2 UŽIVATELSKÁ DATA A JEJICH HODNOTA

Ač si to člověk nemusí uvědomit, tak každá sebeméně osobnější informace je velmi cenná a tyto informace si potřebuje ochránit. Tato kapitola rozebere, jaká data jsou pro uživatele důležitá a měl by si je ochraňovat, stejně tak odpoví na otázku, kdo a k čemu tyto data může využívat.

2.1 Jaké data je důležité si chránit

Jako první je důležité si říct, že každý má co skrývat. Bavme se o spořádaném člověku, který dodržuje všechna pravidla, zákony a předpisy. Všichni mají svá tajemství, i když žijí obyčejný život a zažívají běžné problémy. Každý by měl o člověku vědět to, co o něm potřebuje znát. Tím myslím, že doktor by měl mít přehled o zdravotním stavu pacienta, ale neměl by ho znát kupříkladu zaměstnavatel, samozřejmě, pokud ho omezení nelimituje při práci či není zaměstnanec nějak infekční, to stejné může platit o tom, že by doktor nemusel znát příjem pacienta. A dalších příkladů by šlo uvést více. [1] [11]

Není asi v lidských silách, při využívání moderních technologií, skrývat všechno před všemi. Ale je možné si zachovat určité informace pro sebe, nebo pro toho, komu k něčemu budou.

2.2 Data, která by se měly chránit

V této podkapitole budou rozebrány typy dat, které by měly být chráněny, jsou uvedeny ty nejběžnější, ale jsou to příklady, každý je jiný a má jiné potřeby na prioritu ochrany dat. [1]

2.2.1 Kontaktní informace

Sem patří jméno, příjmení, telefon, adresa. Tyto informace jsou zadávány při každém nákupu online a každý, kdo tak nakupuje, by měl nakupovat pouze na prověřených webech. [1] [12]

2.2.2 Finanční informace

Internetové bankovnictví, posílání peněz, stav na bankovním účtu, číslo karty, různé pohyby a tak dále. Banky a jiné instituce mají potřebu vědět, jaký kdo má příjem, jakou hypotéku splácí atd. Ale tyto informace by měla mít pouze banka a majitel účtu. [1] [12]

2.2.3 Pohyb na internetu

O této problematice již něco napsáno bylo. Jsou to data, která o uživateli říkají, co vyhledával, jakou stránku navštívil, z jaké IP adresy atd. Je extrémně těžké se vyhnout nějakému monitoringu z této strany a nezanechávat stopy. [1] [2]

2.2.4 Nákupy

Pokaždé když je proveden nákup online, prodejce si o tom udělá záznam. Všechna data jsou uložena někde online, prakticky je nemožné provést nákup anonymně skrz internet. Pokud toužíme po anonymním nákupu, je nutné využívat kamenných obchodů a platit hotově, protože banka ví, kde bylo nakupováno. [1]

2.2.5 Lokace

Určitě si každý, kdo používal telefon, musí vzpomenout, kolikrát byl dotazován na povolení o sledování polohy při navštívení určitých webů či při používání či instalaci aplikací, občas se stává, že uživatel bez předešlého uvažování dotaz prostě „odklepne“ a je automaticky sledován, a to s vysokou přesností, to pak vede k možnosti zmapování pohybu uživatele, a dokonce předpovědi, kde bude v určitý čas. [1] [2] [13]

2.2.6 Zdravotní informace

Můžeme zde shrnout vše, co o pacientovi ví lékař. Od hmotnosti, přes výšku a váhu až k prodělaným nemocem či operacím. Informace o zdravotním stavu mohou doktoři ukládat v nějakém softwaru. Asi bychom nebyli nadšeni, kdyby tyto informace unikly a mohly by být zneužity. Ať už k chybě došlo lidským zaviněním nebo slabým zabezpečením či nějakou chybou v systému. [1] [13]

2.3 Kdo chce naše data?

Není problémem sdílet soukromé informace s rodinou, lékařem, právníkem atd. Ale problém může nastat, když se k uživatelským datům chce dostat někdo, kdo je úplně nepotřebuje znát. Tato podkapitola prozradí, kdo chce získat data o uživatelích a k čemu mu budou.

2.3.1 Inzerenti

Hodně webů se živí nabízením reklam a někde je jich dokonce více než skutečného obsahu. Weby nabízí svůj reklamní prostor a mají nějaký příjem. Než se na to bude nahlížet z té horší

stránky, je důležité uvést, že díky reklamám je spousta webových stránek zdarma, jinak řečeno na provoz si vydělávají právě reklamou. [1] [14]

Vzniká touha vytvořit reklamu takovou, aby byla maximálně zajímavá a povedla k nákupům. Nejúčinnější reklama je ta, která nabízí zákazníkovi, to, co chce. Reklamy se zobrazují zákazníkům na stránkách, kde spolu reklama a obsah vůbec nesouvisí. Například při návštěvě nějakého webu zabývajícím se sportovním zpravodajstvím, se zobrazuje reklama na televize, jelikož uživatel hledal nedávno televize. [1] [14]

Pak si můžou inzerenti na základě nějakých informací tvořit profily zájmů, může to být na základě IP adresy nebo třeba z profilů na Facebooku či Googlu a dalších. Možná to nebude nakonec tak špatné, přece jenom, je lepší dostávat reklamu na to, co je potřeba než na to, co není. [1] [14]

Ale všechno má své ale, ne vždy ta cílená reklama je dobrá. Inzerenti například mohou, pokud zjistí, že člověk je movitější nabízet produkty za vyšší cenu. Pokud více lidí používá jedno zařízení, pak se nabídky reklam směřované někomu jinému, mohou zobrazit někomu, kdo je vůbec nepotřebuje, ba dokonce můžou zobrazit něco, co mělo zůstat v soukromí. Takže stojí za uvážení, zda chceme, aby se nám tyto reklamy zobrazovaly či ne. [1]

2.3.2 Data brokeři

Data broker je někdo, většinou nějaká společnost, která sbírá informace za účelem prodeje. Tyto informace může prodávat třeba vládám či inzerentům, zkrátka tomu, kdo zaplatí. Inzerent taky může zároveň shromažďovat data, využívat je pro svoje reklamy a taky je dál prodávat. V Americe je situace horší, protože zákon o ochraně osobních údajů není příliš omezující. V EU se můžeme s data brokery setkat, ale často se nachází na hranici zákona, jelikož musí podléhat GDPR, proto je důležité číst to, co odsouhlasíme při návštěvě stránky. [1] [15]

2.3.3 Doxxing

Je založen na objevování a zveřejňování nových informací o někom jiném. Pomocí doxxingu se například zjišťují skutečné identity lidí, které jinak používají nějaký alias. K pozitivnímu využití může docházet při odhalování nelegálních činností. Ve větší míře však bývá využíván obráceně. Doxxing se nejvíc týká veřejně známých lidí, celebrit, politiků atd. [1] [16]

2.3.4 Hackeři

Hacking lze nazvat určitým uměním, pokud se děje v dobrém slova smyslu (etický hacking). Ale jsou tací, co své umění zneužívají pro získávání citlivých informací. Hackeři jsou většinou mladí lidé, kteří tvoří a distribuují viry, keyloggery, malware a zabývají se tvorbou phishingu. Některé to pouze baví, jiní si tím vydělávají. Informace, jež chtějí získat, jsou většinou finančního charakteru. [1]

2.3.5 Big data

Jako příklad může být Google, který již byl v této práci zmíněn. Je to jeden z největších nevládních sběračů dat na světě, spolu s Facebookem, Twittrem a mnoha dalšími. Tyto informace mohou být použity pro cílení reklamy, ale také Vás profilovat jako potencionálního zločince. [1] [17]

2.3.5.1 Big media

Za big media jsou označování ti, kteří jsou držiteli autorských práv, nejčastěji filmové a nahrávací společnosti. Ti si přejí sbírat data za účelem zjistit, kdo pirátsky zneužívá jejich obsah. Tyto firmy většinou kooperují s internetovými providery a dokáží zjistit, o koho se jedná. Problémem je, že všechno není dokonalé a objevily se i případy, kdy byli zažalováni lidé, kteří ani nevlastnili počítač. [1]

2.3.5.2 Big Money

Banky při poskytování hypoték, úvěrů a dalších finančních produktů, potřebují co nejvíce informací o zákazníkovi. Kromě klasických údajů o příjmech či zaměstnání je zajímají i jiné informace. Čím víc toho ví, tím lépe dokážou odhadnout člověka a dát mu úvěr. Pokud například zjistí, že zákazník příliš často a ve větším množství objednává alkohol, mohou mu zvýšit sazby, aby minimalizovali riziko. [1]

3 ANONYMITA NA INTERNETU

Anonymita má mnoho různých definic, ale všechny jsou si podobné. V pojetí internetové anonymity uživatele zajímá, zda je možné ho identifikovat. V práci už bylo nastíněno, kdo všechno sbírá informace a jak je těžké něco v internetové síti dělat bez toho, aby se uživatel nedal identifikovat. [1][[18]

3.1 Rozdíl mezi internetovým soukromím, anonymitou a bezpečností

Často se při uvažování o anonymitě předpokládá soukromí, ale nemusí to tak nutně být. Pojmy jako anonymita, bezpečnost a soukromí spolu souvisí, ale je potřeba říci, že anonymita není synonymem pro soukromí a naopak. [1]

- Soukromí by se dalo formulovat jako svoboda od sledování a pozorování.
- Anonymita je možnost být na internetu bez toho, aby někdo mohl uživatele identifikovat.
- Bezpečnost je ochrana před nebezpečím.

Tyto pojmy se dají velmi snadno zaměnit, tak budou vysvětleny ještě na příkladu. Soukromí, je tedy to, když nikdo neví, jaké maily uživatel odeslal a jaké stránky navštívil a co napsal. Pokud je uživatel v bezpečí před malwarem, viry, hackery a dalšími hrozbami, dá se říct, že je zabezpečen, je v bezpečí. Když uživatel navštíví nějakou stránku, pošle zprávu atd. a není možné ho identifikovat je to anonymita. Například když uživatel poslal zašifrovanou zprávu někomu druhému skrz nějakou aplikaci, v našem případě bude jako příklad použit Facebook, tak se bude jednat o anonymitu nebo soukromí? Bude to soukromí, jelikož Facebook ví, že k nějaké komunikaci došlo a mezi kým, tudíž tuto situaci nelze nazývat anonymitou. Zpráva je nakonec soukromá, protože Facebook neví, jak přečíst odeslanou zprávu, když je zašifrovaná, kdyby nebyla, tak se nejedná ani o zprávu soukromou, protože by jí Facebook rozuměl. [1] [18]

3.2 Jak docílit anonymity?

Jedinou stoprocentní cestou, jak zůstat anonymní a v bezpečí před různými hrozbami, je přestat používat moderní technologie. Ale to není úplně tím správným řešením, existují různé možnosti k docílení anonymity a je důležité vědět, že v dnešní době není řešení nepoužívání technologií, tím určitě ničeho nedosáhneme. Musíme se smířit s tím, že internet je obrovský prostor, kde stoprocentního úspěchu prostě nelze docílit.

V této podkapitole budou rozebrány možnosti pro zvýšení anonymity.

3.2.1 Odhlášení uživatelských účtů

Úplně nejjednodušší cesta, jak uživatele identifikovat je být přihlášen pomocí uživatelských účtů. Pokud chce uživatel zůstat skutečně anonymní, nesmí se nikam přihlašovat, popřípadě se přihlašovat pod falešnými účty. To znamená, nepřihlašovat se na Facebook, na Twitter, do Googlu a spousta dalších. Pokud chceme anonymně přistupovat k informacím, je důležité být odhlášen a dodržovat další doporučení uvedená níže.

3.2.2 Vhodné nastavení prohlížeče

Prohlížeč sám o sobě ví o uživatelích hodně, proto je důležité si prohlížeč nastavit tak, aby neukládal žádné informace. Mezi základní operace patří:

- Neukládat nebo často mazat internetovou historii
- Neukládat záložky
- Nebýt v prohlížeči přihlášen
- Využívat možnosti Do not Track
- Zablokovat cookies třetích stran
- Čas od času promazat cookies
- Neukládat hesla, bankovní karty, adresy
- Využívat anonymních oken [19] [20] [21] [22]

3.2.3 TOR

TOR neboli The Onion Routing je označení pro open-source software a počítačovou síť. Má sloužit k bezpečné a anonymní aktivitě na internetu. Je velice jednoduché začít komunikovat přes TOR, stačí si stáhnout prohlížeč TOR z oficiálních stránek a používat jej jako každý

jiný. Tento prohlížeč je i multiplatformní, takže jej lze používat na všech operačních systémech. Klasická komunikace na internetu pracuje na IP protokolu, jehož pakety obsahují zdrojovou i cílovou adresu, a to se bohužel příčí s anonymitou. TOR tento nedostatek odstraňuje, nabízí anonymní komunikaci a chrání uživatele před monitorováním na internetu. [23] [24] [25]

Servery, bez kterých by tato služba nemohla existovat, jsou provozovány dobrovolníky po celém světě. Bezpečnost spočívá v několikanásobném šifrování. TOR ošetřuje data dřív, než jdou do sítě, z paketů odebírá veškeré informace, které by mohly uživatele identifikovat (zdroj, velikost, cíl a čas) a až poté je paket odeslán. Díky několikanásobnému šifrování je pouze známo, odkud pochází a kam směřuje. Většinou se pro komunikaci využívají 3 náhodné TOR servery z celého světa, které vytvoří cestu mezi uživatelem a cílovým serverem, tato cesta je v pravidelných časových intervalech aktualizována, to znamená, že pozorovatel vidí, pouze to, že uživatel komunikuje s Tor serverem a cílový server vidí, že odesilatel je jeden z tor serverů, kdekoliv uprostřed cesty není zjistitelná IP adresa uživatele ani cílového serveru. Vysoká bezpečnost má za následek nízkou přenosovou rychlost. Po připojení k Toru prohlížeč naváže spojení s directory serverem, těchto serverů je více, jsou důvěrné a obsahují informace o ostatních tor serverech, přes něž prochází komunikace. Directory server vytvoří okruh, který povede ke komunikaci. První server jediný komunikuje s uživatelem napřímo. Dále je v okruhu prostřední server a výstupní server, jenž komunikuje s cílovým počítačem. Každý z těchto serverů má svůj šifrovací klíč a před odesláním paketu je odesilatelem zašifrován v několika vrstvách. Každý v okruhu bude tedy moci odebrat pouze jednu vrstvu šifrování a poté odeslat na další počítač v okruhu. Jakmile poslední v okruhu odebere poslední šifrování, je paket odeslán příjemci. Je však důležité myslet na to, že v případě připojení na cílový nezabezpečený server, je používání Toru naprosto zbytečné. [23] [24] [25] [26]

3.2.4 VPN

Dalším způsobem zajištění své anonymity je použití VPN neboli virtuální privátní sítě. Je to služba, jež uživatelům umožňuje přístup na požadované stránky skrz server, který zamaskuje původní IP adresu, za adresu právě zmíněného serveru. VPN není užitečná pouze z hlediska většího soukromí a anonymity, může být také využita ke stahování torrentů, navštěvování stránek určených pouze daným zemím, vyhnutí se cenzuře či ušetření peněz, jelikož pro různé země mohou být různé ceny. [1] [27] [28]

Mezi uživatelem a serverem se vytvoří zašifrovaný informační kanál. Takže pokud by poskytovatel internetu chtěl vědět, na jaké stránky uživatel chodí, tak za normálního stavu, vidí vše, kam se uživatel dostane, ale při použití VPN vidí pouze to, že se uživatel připojil na VPN server, jaká komunikace je za serverem, už poskytovatel nemůže vědět. Jediný, kdo v této komunikaci ví skutečnou IP adresu i historii procházení je VPN server. Může to působit tak, že je to kontraproduktivní, protože co věděl poskytovatel internetu předtím, tak teď to ví poskytovatel VPN. Je to pravda, ale poskytovatelé internetu musí tyto informace v případě nějakého podezření na něco nekalého vydat oprávněným složkám státu. Většina VPN tuto povinnost nemá, jelikož servery bývají lokalitou tam, kde se ctí právo na soukromí. [27] [28] [22]

Je mnoho poskytovatelů VPN a je důležité vybrat toho pravého, podle výše zmíněných informací, není příliš výhodné používat VPN, které je například lokalizováno např. v Rusku, USA, Číně atd. Všechny tyto země sbírají velké množství dat. Dalším důležitým faktorem je, zda sám provozovatel, i když má servery na správném místě, neshromažďuje informace sám. Takovým kvalitním příkladem VPN může být NordVPN, neukládá žádné informace o uživatelích a sídlí v Panamě, takže nepodléhá legislativám, kde se musí něco komukoliv sdělovat. [27] [28] [29]

3.2.5 Sdílení souborů anonymně

Bohužel běžné služby se k anonymitě i soukromí nestaví příliš přívětivě, takže opět nedoporučuju požívat Google Drive či Dropbox a ostatní. Podle Edwarda Snowdena je Dropbox doslova nepřátelský k soukromí. Ale opět existují varianty, jež jsou v tomto ohledu lepší, jednou z nich může být OnionShare. [21] [30]

3.2.6 Využití správného vyhledavače

Při používání vyhledávačů musíme myslet také na to, že většina opravdu ukládá, všechno, co se kdy vyhledá. Takže Google, Bing či Yahoo se určitě nehodí. Zato DuckDuckGo je skvělá volba. Je to internetový anonymní internetový vyhledavač, který má i mnoho jiných užitečných funkcí. [21] [19]

3.2.7 Zabezpečený email

I co se týká emailů, existují společnosti, které nabízejí jasné výhody oproti běžným poskytovatelům emailových účtů. Jedním z takových poskytovatelů je ProtonMail, tato společnost se zavazuje chránit soukromí a anonymitu uživatelů. Při registraci nejsou potřeba žádné

osobní informace. Sám ProtonMail nedokáže přečíst emailovou komunikaci, využívá end to end šifrování. ProtonMail využívá PGP(PrettyGoodPrivacy), kde není možné, aby si někdo jiný přečetl váš email, zprávy jsou šifrovány veřejným klíčem příjemce a pouze příjemce si tuto zprávu může dešifrovat svým soukromým klíčem. Bohužel pro tuto službu musí mít příjemce také ProtonMail. [1] [22] [31]

3.2.8 Vypnutí lokace

Pro zvýšení anonymity je potřeba vypnout zjišťování polohy, a to hned na několika místech, v operačním systému, v mobilním operačním systému a v prohlížečích. [21]

3.2.9 Platba pomocí kryptoměn

Pokud je prioritou zůstat anonymní, tak platba obyčejnou bankovní kartou je nepřípustná. Místo toho je lepší použít nějaké systémy pro online převod peněz, ale ty také vedou záznamy, proto je ideální platit pomocí kryptoměn, např. Bitcoinem, kde vystopovat, kdo to zaplatil, je značně komplikovanější. [30] [21]

3.2.10 Blokování Javascriptu

Pomocí Javascriptu toho jde o uživateli zjistit docela dost. Může zjistit velikost monitoru a spoustu dalších informací, pomocí nichž pak je možné jedinečně identifikovat počítač, tato technika se nazývá tzv. Fingerprinting, o které bude více v následující kapitole. [21]

3.2.11 Vyhnout se špatným doplňkům do prohlížečů

Bohužel sledovat uživatele je možné i přes doplňky do prohlížečů. V této práci v praktické části bude rozebráno, jaké z testovaných doplňků jsou z hlediska soukromí bezpečné. Naopak některé doplňky dokáží pomáhat při zvětšování uživatelského soukromí a anonymity. [21]

4 PODLE ČEHO JE MOŽNÉ IDENTIFIKOVAT UŽIVATELE

Existuje spousta způsobů, jak uživatele identifikovat nebo poznat jaké má zařízení atd. Tato podkapitola se zaobírá nejčastějšími způsoby identifikace uživatele.

4.1.1 Uživatelské účty

Nejjednodušší cestou, jak někoho identifikovat je pomocí uživatelských účtů, když se uživatel přihlásí. Daná služba ví, kdo je za počítačem a co na něm dělá (v aplikaci, do které je přihlášen). Existují i přihlášení přímo do prohlížeče například u Google Chrome.

4.1.2 IP adresa

IP adresa je tím nejzákladnějším způsobem, jak někoho identifikovat, celkem jednoduše se to dá obejít skrz VPN. Pomocí IP adresy lze zjistit přibližná poloha, avšak identifikace není tak přesná, aby bylo možné identifikovat uživatele na úrovni ulic, ale i taková základní informace stačí pro poskytování cílených reklam pro oblast, kde uživatel žije. Ale IP adresy se mohou poměrně často měnit, proto se využívají více sofistikované technologie. S nástupem IPv6 adres se předpokládá zvýšení přesnosti určení polohy uživatele, protože možná nebude potřeba technologie NAT a každý bude mít svou IP adresu. [32] [33]

Při navštívení adresy iplocation.net je možné zjistit, co o nás všechno IP adresa prozrazuje.

IP Address	Country	Region	City
195.113.99.101	Czech Republic	Zlinsky kraj	Zlin
ISP	**Organization**	**Latitude**	**Longitude**
Univerzita Tomase Bati ve Zline	Not Available	49.2167	17.6667

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
195.113.99.101	Czech Republic	Zlín	Zlín
ISP	**Organization**	**Latitude**	**Longitude**
CESNET z.s.p.o.	Tomas Bata University (utb.cz)	49.2264	17.6706

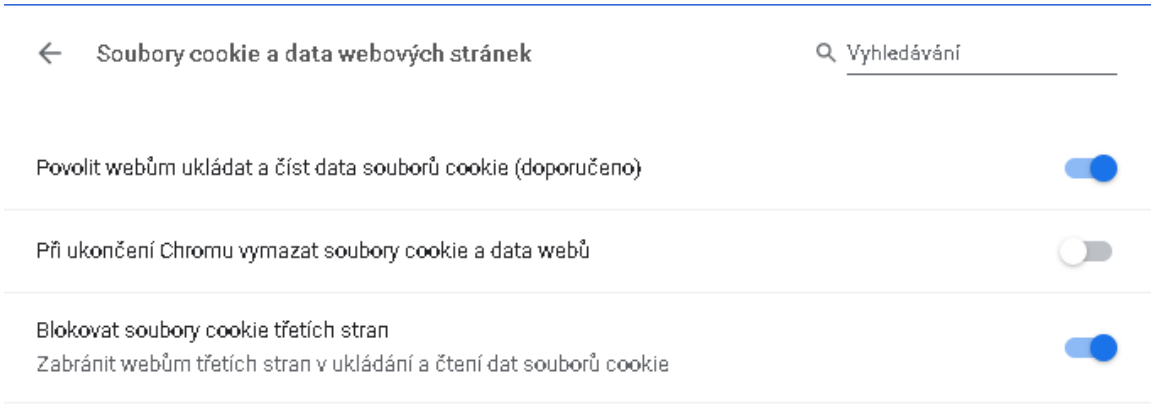
Geolocation data from DB-IP (Product: Full, 2019-11-1)

IP Address	Country	Region	City
195.113.99.101	Czech Republic	Zlín	Zlín
ISP	**Organization**	**Latitude**	**Longitude**
CESNET-TCZ	Tomas Bata University	49.2229	17.6669

Obrázek č. 1 Zjistitelné informace dle IP adresy

4.1.3 Cookies

Cookies jsou malé textové soubory, které se zaznamenávají při návštěvě stránek, samo o sobě není cookies nic špatného. Cookies například obsahují přihlašovací údaje, obsah košíku, nastavení webu, který se při každém navštívení uzpůsobí našemu nastavení. Ale pořád obsahují uživatelské informace. Horší jsou cookies třetích stran, které právě stojí za nabízením cílených reklam a monitoringem uživatelů. Naštěstí lze celkem jednoduše tyto cookies zakázat v nastavení prohlížeče, dokonce je možné si i všechna uložená cookies projít. [32] [33] [34]



Obrázek č. 2 nastavení cookies v Google Chrome

4.1.4 Super cookies

Jsou určitým vylepšením klasických cookies, obsahují jedinečný identifikátor a jsou schopné sledovat historii procházení a chování při procházení. Obyčejným smazáním cookies v prohlížeči se jich zbavit nelze. Klasickým příkladem je jsou Flash cookies, které fungují na Flash pluginu, tento druh cookies není časově nijak omezený. Lze ho smazat lokálně. Pokud chceme předejít ukládání tohoto druhu cookies je potřeba zakázat flash player, nebo ho nastavit tak, aby když web bude chtít tento plugin využít, tak ho musí uživatel pokaždé povolit. [32] [33] [34]

4.1.5 Evercookies

Evercookies je ty typ super cookies. Evercookies se vyznačují tím, že je problém se jich zbavit. Hlavně proto, že se ukládají na více místech a ve více formátech, například do souborů flash, místního úložiště HTML5 nebo do historie procházení. Jejich účelem je identifikovat uživatele i poté, co odstraní klasické soubory cookies, flash cookies atd. V případě odstranění cookies, jsou bezprostředně obnovena z jiného zdroje. [32] [33] [34]

4.1.6 Fingerprinting

Fingerprinting vznikl proto, aby bylo možné identifikovat uživatele i přesto, že zakázal cookies. Fingerpriting je další metodou identifikace uživatele. Využívá k tomu internetový prohlížeč. Dříve bylo možné toto obejít při používání více prohlížečů, ale fingerprinting používaný dnes, tento problém řeší a uživatele pozná, i když používá více prohlížečů. Princip fingerprintingu je takový, že se vytvoří jedinečný otisk, jež je identifikátorem. Otisk se skládá z obrovského množství informací, které ve své kombinaci sestaví již výše zmíněný identifikátor. [32] [33] [34]

Informace, jaké fingerprinting využívá:

- Nainstalované fonty
- Seznam nainstalovaných jazyků
- Rozlišení obrazovky
- Počet jader procesoru
- Renderování a anti-aliasing
- Vertex shader – každá grafická karta vykresluje jinak, další jedinečný údaj
- A spousta dalších [33] [35]

Základní obranou proti fingerprintingu je vypnoutí javascriptu v prohlížeči a spouštět ho na webech, kde to potřebujeme, bohužel javascript také ovlivňuje vzhled stránky a jeho funkčnost, některé weby nebudou vypadat a fungovat tak, jak by měly. Další možností je vypnout sledování v prohlížeči, ale tato metoda je sporná, jelikož právě to, že je využitá, dodává další informaci, s níž fingerprinting pracuje. V praktické části je rozebráno rozšíření, jež se právě zabývá problematikou vypínáním javascriptu a fungováním stránek - NoScript Security Suite. Na webu panopticlick.eff.org je možné si nechat otestovat prohlížeč a vidět, co se dá z prohlížeče přečíst. [33] [34]

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	5.8	55.78	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.97 Safari/537.36
HTTP_ACCEPT Headers	17.91	246830.0	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 gzip, deflate, br cs-CZ,cs;q=0.9,en;q=0.8
Browser Plugin Details	3.3	9.87	no javascript
Time Zone	3.3	9.87	no javascript
Screen Size and Color Depth	3.3	9.87	no javascript
System Fonts	3.3	9.87	no javascript
Are Cookies Enabled?	0.22	1.17	Yes
Limited supercookie test	3.3	9.87	no javascript
Hash of canvas fingerprint	3.3	9.87	no javascript
Hash of WebGL fingerprint	3.3	9.87	no javascript
DNT Header Enabled?	1.07	2.1	False
Language	3.3	9.84	no javascript
Platform	3.3	9.84	no javascript
Touch Support	3.3	9.87	no javascript

Obrázek č. 3 zjistitelné informace z prohlížeče

Jak jde vidět díky vypnutému javascriptu, je většina informací nezjistitelných.

4.1.6.1 Canvas fingerprinting

Po navštívení stránky se spustí skript, generuje tzv. canvas, jenž se načte na pozadí. Vykreslování obrázku se mírně liší dle operačního systému, grafické karty a grafického ovladače. I minimální rozdíly pomohou v identifikaci. [33] [34]

4.1.7 User agent

User agent je jedinečná informace o návštěvníkovi webu, přesněji obsahuje informace o operačním systému a prohlížeči. To pak umožňuje naprogramovat, aby se stránka chovala jinak v závislosti na operačním systému, využití má samozřejmě dobrou i špatnou stránku.

User agent lze změnit v prohlížeči, takže pak i uživatel může oklamat webovou stránku. Samozřejmě je to další údaj do fingerprintingu. [32] [36]

4.1.8 HTTP Referrer

HTTP referrer ukazuje navštívené stránce, odkud ji uživatel navštívil. Takže pokud uživatel přejde ze stránky A na stránku B, tak referrer, čitelný na stránce B, bude právě stránka A. Http referrer je taky používaný při načítání obsahu stránky, pokud je přítomný nějaký monitorovací skript, tak ví, na jakou stránku se uživatel zrovna dívá. Některé prohlížeče umí referrer vypnout například Opera nebo Firefox, u Google chrome je potřeba doinstalovat plugin. [32]

II. PRAKTICKÁ ČÁST

5 ROZBOR DOPLŇKŮ DO PROHLÍŽEČŮ

Praktická část se věnuje testování vybraných doplňků do prohlížečů. V této kapitole je vysvětleno, jakým způsobem se daná rozšíření vybírají, jaké softwarové prostředky budou použity pro testování, jak tyto prostředky nastavit a jak probíhá postup výzkumu. Poté již následují samotné výstupy z testování jednotlivých pluginů. V závěru této kapitoly je krátké a přehledné shrnutí vhodných doplňků z pohledu uživatelského soukromí.

5.1 Výběr testovaných doplňků

Jelikož testování probíhá na prohlížeči Mozille Firefox, tak doplňky jsou vybírány právě na tento prohlížeč. Aby byl výzkum co nejužitečnější, tak jsou zvolena určitá kritéria, podle nichž jsou doplňky zvoleny. Byl hledán kompromis mezi počtem uživatelů, kteří určité rozšíření do prohlížeče používají a dalším kritériem je užitečnost jednotlivých doplňků v závislosti na zvýšení soukromí, respektive ochranou před monitorováním, bezpečností a blokování reklam.

Původně bylo v plánu testovat pluginy odpovídající výše zmíněným kritériím na prohlížečích Google Chrome i Firefox, ale po provedení malého průzkumu bylo zjištěno, že doplňky, které používá nejvíce uživatelů na obou prohlížečích a zároveň mají nějakou souvislost s bezpečností nebo zvýšením soukromí, fungují jak na Google Chrome, tak také na Firefoxu. Z tohoto důvodu, pokud existoval doplněk na obou prohlížečích, tak je v této práci testován ve Firefoxu.

Je zřejmé, že počty uživatelů rozšíření se liší podle prohlížeče. Podle webu zd.net má pouze třináct pluginů na Google Chrome více než deset milionů uživatelů. Z těchto třinácti doplňků se výše uvedenými kritérii zabývají následující rozšíření:

- Avast Online Security
- Adblock Plus
- Adblock
- uBlock Origin [37]

Adblock a Adblock Plus je téměř totožný produkt, proto Adblock byl z testování vyloučen. Do každého žebříčku je přidán jeden plugin, který má hodně uživatelů, ale nezabývá se dalšími zmíněnými body a mohl by být běžnému uživateli užitečný. Z Firefoxu jsou vybrány následující doplňky:

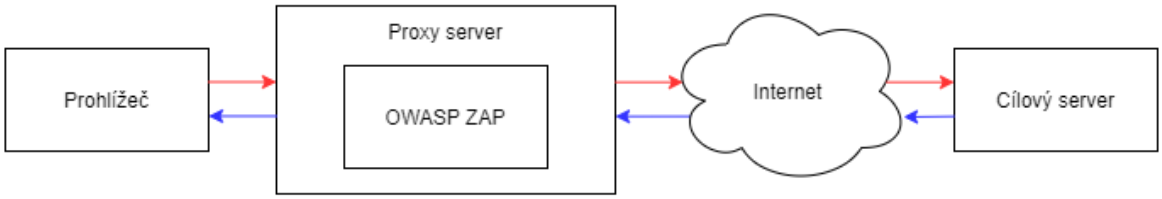
- Ghostery
- NoScript Security Suite
- Web of Trust
- Privacy Badger
- Facebook container
- VideoDownloaderHelper

Z Chromu jsou vybrány následující doplňky:

- Avast Online Security
- Adblock Plus
- uBlock Origin
- Avast Safe Price

5.2 Popis testovacího prostředí

Pro tento výzkum jsme použili hlavně dva programy. Prvním je prohlížeč, na kterém jsou doplňky reálně testovány a program Owasp ZAP, jenž pomáhá zjistit, zda doplněk nějaké informace odesílá či ne.



Obrázek č. 4 blokové schéma testovacího prostředí

Pro procházení internetu je potřeba prohlížeč, který se za normálního stavu připojuje přímo na internet. V tomto případě mezi internetem a prohlížečem stojí proxy server OWASP ZAPu. Dále se tento server připojuje na internet a dále na webovou stránku neboli cílový server. Tento proxy server je takový prostředník, veškerá komunikace musí protéct přes tento server směrem tam i zpět. Tudíž skrz OWASP ZAP se zachytává komunikace a následně je možné analyzovat odesílané zprávy, čehož je využito při prověřování vybraných pluginů.

5.2.1 Mozilla Firefox

Mozilla Firefox je multiplatformní webový prohlížeč, jeho první verze vyšla již v roce 2004. Produkt zprvu vyvíjela nezisková organizace Mozilla Foundation. Tato organizace v roce

2005 vytvořila dceřinu společnost Mozilla Corporation, která se od té doby stará o vývoj tohoto prohlížeče. [38]

Prohlížeč je využíván na hledání informací o pluginech, také na tento prohlížeč jsou pluginy instalovány a případně je využito jeho prostředí debuggingu.

5.2.2 Owasp ZAP

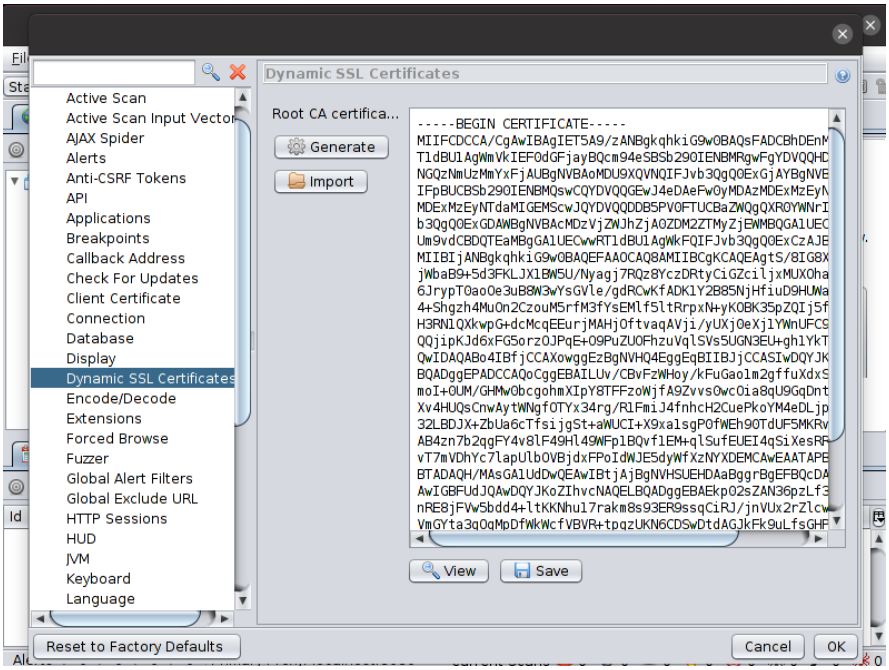
Podobných programů jako ZAP pár existuje a je zde několik možností, jaký program zvolit. Nakonec byl vybrán Owasp ZAP, jenž dopadl podle hodnocení hackr.io nejlépe. [39]

Aplikace je multiplatformní a open source, určená na testování bezpečnosti webových aplikací. Má velmi dobře vypadající a ovladatelné grafické prostředí a je napsána v Javě. ZAP je vyvíjen neziskovou organizací OWASP Foundation. V této práci bude sloužit jako zachytávač komunikace, jež proteče skrz prohlížeč. [40]

5.2.3 Nastavení programů

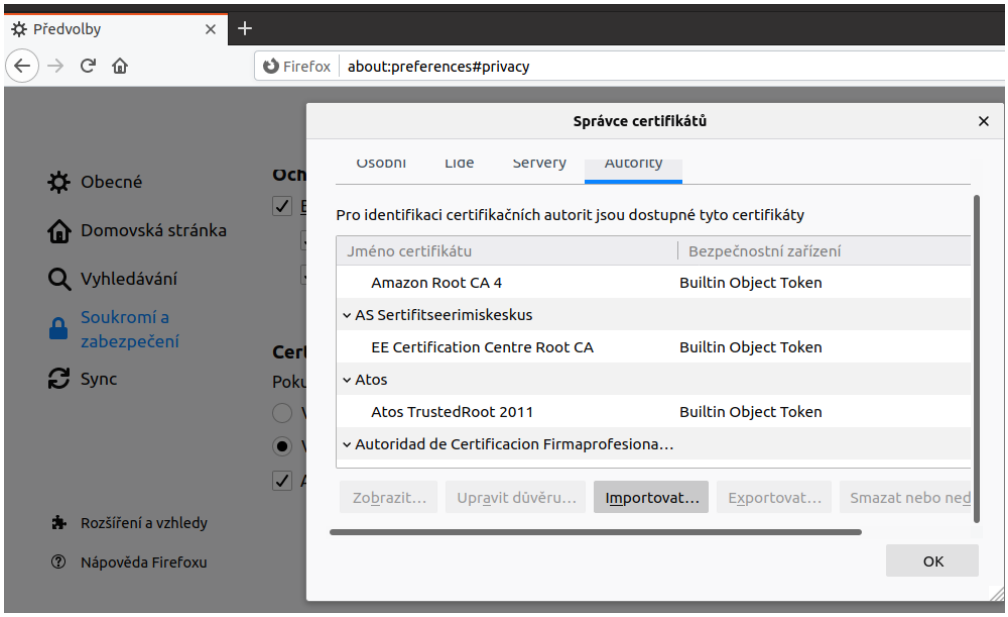
Po instalaci obou vybraných programů je potřebné správné propojení, aby dokázal Owasp ZAP zachytávat komunikaci.

Jako první je nutné stáhnout certifikát ze ZAPu. Tento certifikát se nachází v horní záložce pod názvem Tools a dále pod možností Options. Zde se nachází velká množství nastavení, která jdou nastavit individuálně podle potřeb uživatele. Pro nastavení proxy je potřeba stáhnout certifikát pod jménem Dynamic SSL Certifikates a potom ho uložit pomocí tlačítka save, jak je viditelné na obrázku níže. [41]



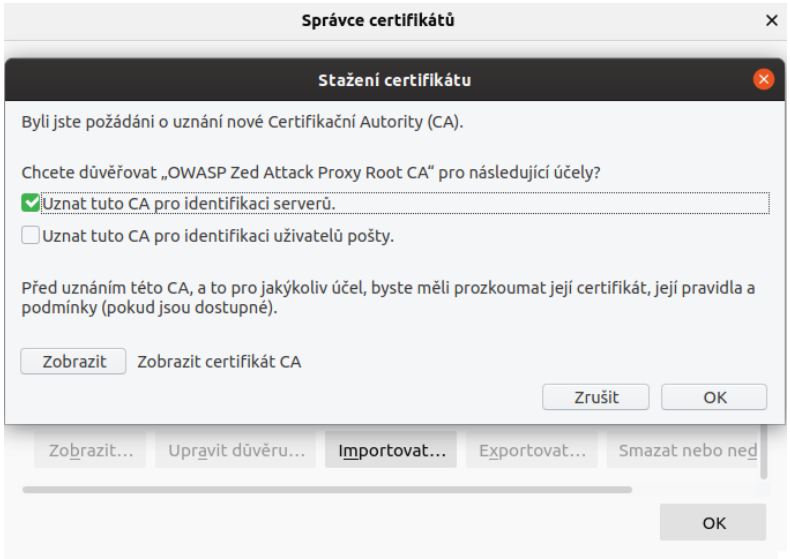
Obrázek č. 5 stažení certifikátu

Následujícím krokem je importování staženého certifikátu do prohlížeče. Tato možnost je ve Firefoxu lokalizována v možnostech a potom v záložce Soukromí a zabezpečení, kde úplně dole se nachází oblast, jež se jmenuje certifikáty. V této oblasti je tlačítko Zobrazit certifikáty, po kliknutí na něj se zobrazí okno viditelné na obrázku níže. [41]



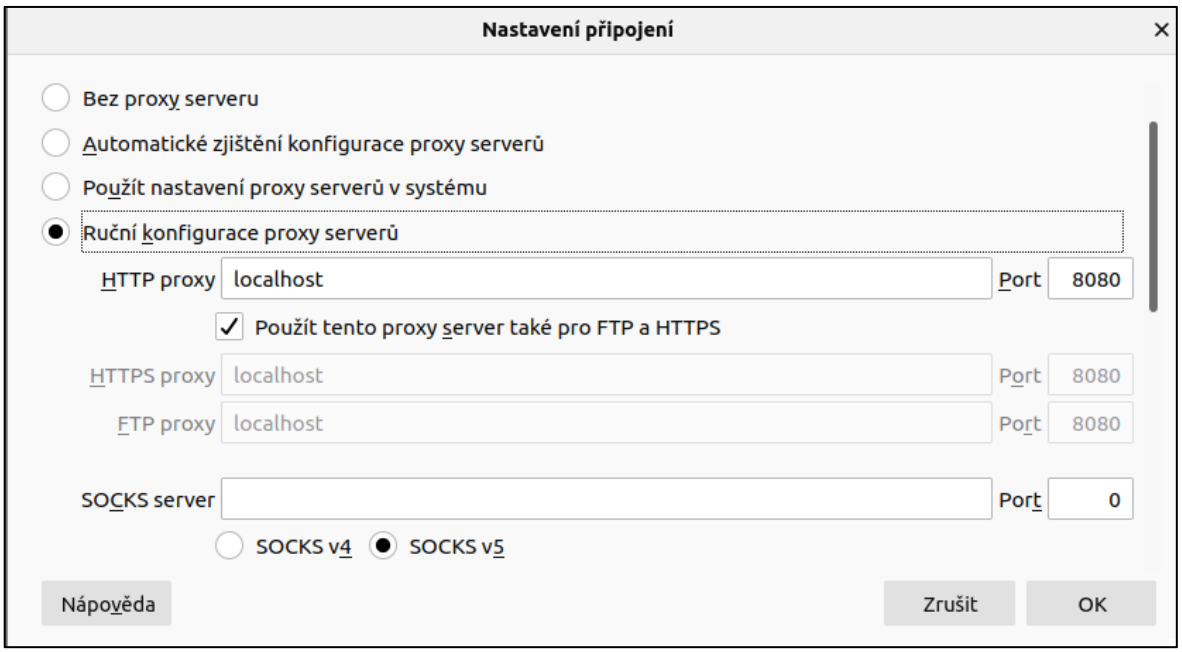
Obrázek č. 6 Importování cerfitikátu do prohlížeče

Dalším důležitým prvkem postupu je uznání tohoto certifikátu v prohlížeči. Pomocí možnosti importovat, je nutné sdělit programu, kde je uložen certifikát, který je stažen ze ZAPu. Poté se pouze uzná tento certifikát pro identifikací serverů a potvrdí pomocí OK. [41]



Obrázek č. 7 Uznání certifikátu

Posledním krokem v nastavení je nakonfigurovat proxy na localhost. Toto nastavení je umístěno v možnostech na záložce obecné a potom nastavení sítě, kde po klinutí na položku Nastavení se zobrazí okno nastavení připojení, kde je nutné nastavit toto připojení tak, jak je viditelné na obrázku pod tímto odstavcem. [41]



Obrázek č. 8 Nastavení proxy pro odesílání do ZAPu

Tímto je všechno nastaveno a je možné začít s testováním. [41]

5.3 Postup výzkumu

Zkoumání tohoto problému, má několik kroků, které na sebe plynule navazují a v konečném důsledku nemusí ani na poslední krok dojít, pokud nebude zachyceno nic podezřelého či nekalého.

Kroky výzkumu:

1. Hledání informací na webu
2. Testování v programu Owasp ZAP
3. Hledání odesílaných informací pomocí prohlížeče přes funkci nástroje pro vývojáře

První bod je nejméně odborný a v tomto kroku se zkoumá prostřednictvím internetového vyhledávání, zda se dají najít nějaké informace o monitoringu uživatelů. Informace se nebudou pouze hledat přímo o daném rozšířením, ale také o organizaci, jež tento produkt poskytuje. [42]

Na druhý bod je již použit software Owasp ZAP. Pomocí tohoto programu bude zjištěno, zda nějaká data zkoumané rozšíření do prohlížeče odesílá. Pokud se nic nezachytí, tak lze prohlásit, že doplněk nikoho nemonitoruje a tím pádem nic neodesílá a zkoumání tohoto doplňku můžeme ukončit. V případě, že dochází k odesílání, je potřeba zjistit co. Nemusí to nutně být za účelem monitorování, může to být nutné pro správné fungování doplňku. [42]

Třetí krok řeší problém, pokud je zjištěno, že nějaká data jsou odesílána a přes Owasp ZAP se k nim nelze dostat, to může znamenat, že jsou třeba šifrovaná. Potom začíná mravenčí práce a je nutné v kódu daného pluginu najít jeho část, která řeší právě odesílání dat a poté ji analyzovat, k tomuto problému je využit samotný prohlížeč a jeho prostředí pro debugging. [42]

6 TESTOVÁNÍ JEDNOTLIVÝCH PLUGINŮ

V této fázi výzkumu již dochází k samotnému zkoumání jednotlivých pluginu, dle uvedeného postupu. Každý doplněk má přehlednou tabulku se základními informacemi, tyto informace jsou aktuální k datu 4. 4. 2020.

6.1 Web of trust

Jako první doplněk byl testován plugin Web of trust, tento plugin by měl pomáhat uživatelům odhalovat nedůvěryhodné stránky a tím pádem doporučit, zda pohyb na nich není z nějakého důvodu nebezpečný. [43]

Tabulka č. 1 Web of trust

Testovaná verze:		20200226
Vývojář:		WOT services
Počet uživatelů:	Firefox	166 347
	Chrome	1 000 000+

[43] [44]

Již při první analýze při zadání následující fráze: „ *Web of trust spying on users*“ se objevilo hned několik odkazů, kde je nějakým způsobem naznačeno, že něco není úplně v pořádku.

Obrázek č. 9 Internetové hledání o WOT

Nezbývá nic jiného, než se na problém podívat důkladněji, do prohlížeče byla zadána adresa seznam.cz a pomocí ZAPu bylo zjištěno, že doplněk odesílá následující informace:

Obrázek č. 10 odesílané zakódované informace přes WOT

Na první pohled jsou počáteční pole poměrně nezajímavá a sdělují obecné informace, ale zajímavé naopak je dlouhé pole b64. Na první pohled není jasné, co je obsahem, z toho vyplývá, že je potřeba toto pole dekódovat, je využit terminál a příkaz k dekódování base64. Výsledkem dekódování bylo:

Kód 1 WOT – pole b64

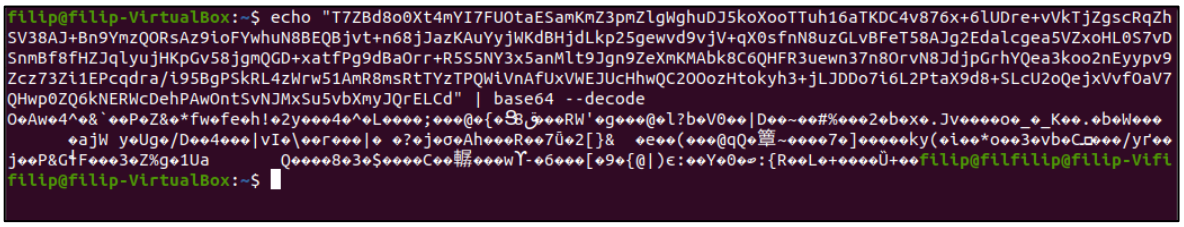
```
id=99ae416d37e0fbeeaab8187345e69af4684a2f8d&nonce=9aa5b84d04b811d54b9
355de6395c6b2886b9bb8&lang=cs&version=4.0.10.56beta-20170801-
3.2.2&target=T7ZBd8o0Xt4mYI7FUOtaESamKmZ3pmZlgWghuDJ5koXooTTuh16aTKDC
4v876x%2B6lUDre%2BvVkTjZgscRqZhSV38AJ%2BBn9YmzQORsAz9ioFYwhuN8BEQBjvt
%2Bn68jJazKAuYyjWKdBHjdLkp25gewvd9vjV%2BqX0sfnN8uzGLvBFeT58AJg2Edalcg
ea5VZxoHL0S7vDSnmBf8fHZJqlyujHKpGv58jgmQGD%2BxatfPg9dBaOrr%2BR5S5NY3x
5anMlt9Jgn9ZeXmKMAbk8C6QHFR3uewn37n8OrvN8JdjpGrhYQea3koo2nEyypv9Zcz73
Zi1EPcqdra%2Fi95BgPSkRL4zWrw51AmR8msRtTYzTPQWiVnAfUxVWEJUcHhwQC2OOozH
tokyh3%2BjLJDDo7i6L2PtaX9d8%2BSLcU2oQejxVvfOaV7QHwp0ZQ6kNERWcDehPAwOn
tSvNJMxSu5vbXmyJQrELCd
```

Výsledkem je opět nové pole a opět zakódované, jako první je opět dekódováno podle base64, ale bohužel to nejde, tak je dekódováno pomocí webového URL dekodéru. Dekódováno je pouze pole target.

Kód 2 WOT – pole target

```
T7ZBd8o0Xt4mYI7FUOtaESamKmZ3pmZlgWghuDJ5koXooTTuh16aTKDC4v876x+6lUDre
+vVkTjZgscRqZhSV38AJ+Bn9YmzQORsAz9ioFYwhuN8BEQBjvt+n68jJazKAuYyjWKdBH
jdLkp25gewvd9vjV+qX0sfnN8uzGLvBFeT58AJg2Edalcgea5VZxoHL0S7vDSnmBf8fHZ
JqlyujHKpGv58jgmQGD+xatfPg9dBaOrr+R5S5NY3x5anMlt9Jgn9ZeXmKMAbk8C6QHFR
3uewn37n8OrvN8JdjpGrhYQea3koo2nEyypv9Zcz73Zi1EPcqdra/i95BgPSkRL4zWrw5
1AmR8msRtTYzTPQWiVnAfUxVWEJUcHhwQC2OOozHtokyh3+jLJDDo7i6L2PtaX9d8+SLc
U2oQejxVvfOaV7QHwp0ZQ6kNERWcDehPAwOntSvNJMxSu5vbXmyJQrELCd
```

Tato změť znaků opět nic moc neřekne, zase následuje base64 dekódování.



Obrázek č. 11 Dekódování v terminálu

Jak můžeme vidět, tak terminál vyhodil nějaké divné znaky, zpráva je nečitelná a může se jednat o binární data. Nabízí se otázka proč?

Nyní nastává třetí část výzkumu. Po delší práci byl nalezen kus kódu, který začíná slovem encrypt v souboru WoTCrypto.js.

Teď už jenom stačilo dát zarážku na řádek, kde začíná nalezený kód.

Obrázek č. 12 WOT Mozilla debugging

Je nalezen zajímavý řádek, který ještě prošel URL dekódováním:

Kód 3 WOT – čitelné odesílané informace

```
subtrgt=https://www.seznam.cz/&kn=&sublast=&subref=&format=4&nt=link&
atm=exthead&epochtime=1583941096854&ch=6&sg=abb46fd76&id=ff5960e7160c
af16554e1a91d093ab80e295edb0&vmt=6&dm=21&vv=1&ver=20200226.0wot&delta
=AAEAAAAAAAQbCwAlMQAAAAAAAAAAAAAAAAAAAAAAAA=&host=seznam.cz
```

Všechno obsažené v kódu nahoře, je to, co WOT odesílá, tím pádem asi i shromažďuje, ne všechny informace lze snadno přečíst, těžko říct jakou informaci nese sg= abb46fd76 a některé další. Je načase tyto informace rozebrat:

- Subtrg – přesná adresa navštívené stránky
- Host – doména (seznam.cz)
- Sublast – poslední navštívená stránka
- Subref – referrer
- Version – verze rozšíření
- Epochtime – čas v unixovém formátu
- Id – identifikátor [42]

Je potřeba sdělit, že jediné informace, které tento doplněk potřebuje ke své funkci, jsou data o navštívené stránce, aby mohl říct, zda je bezpečné tuto stránku navštěvovat. Bohužel toto rozšíření toho odesílá daleko více, také si ukládá jakékoliv informace o výsledcích vyhledávání ve vyhledavačích, o této problematice je více napsáno v podkapitole o Avast Online Security.

6.2 Ghostery

Ghostery je doplněk, jež by měl zajišťovat soukromí uživatelů a bránit je před sledováním z různých webů a svou funkcí blokování sledovacích prvků na stránce by měl urychlovat načítání stránek, právě tím, že sledovací algoritmy nenačte. [43]

Tabulka č. 2 Ghostery

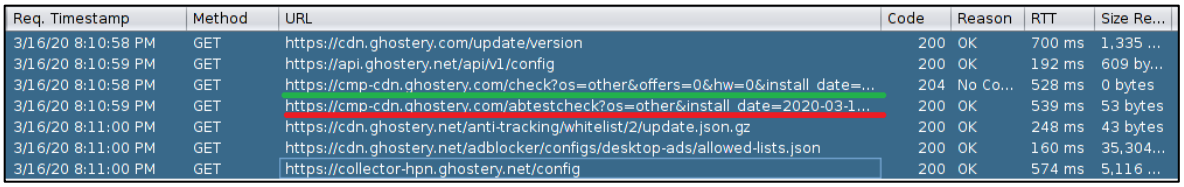
Testovaná verze:		8.4.6
Vývojář:		Ghostery
Počet uživatelů:	Firefox	1 613 169
	Chrome	2 000 000+

[43] [44]

Při hledání informací o sledování uživatelů prostřednictvím tohoto pluginu byly nalezeny zajímavé zprávy, třeba web lifehacker.com tvrdí, že Ghostery v minulosti sbíral a dále prodával uživatelská data, dělal to skrz funkci Ghostrank, která mapovala, jaké reklamy uživatel blokuje a pak je dále mohli inzerenti lépe zacílit. O dva roky později web extremetech.com zveřejnil rozhovor s Toddem Rubackem vedoucím oddělení ochrany osobních údajů a Ruback tvrdil, že data jsou sbírána pouze tehdy, pokud je povolena služba Ghostrank a tím je dovoleno doplňku sledovat sledovací algoritmy na stránkách. Ovšem tyto zprávy jsou staršího data, a to z roku 2013 a 2015, tak je potřeba důkladnějšího průzkumu. [45] [46]

Po instalaci verze 8.4.6 bylo zjištěno, že žádný Ghostrank již přítomný není. Po dalším pátrání byla nalezena informace, že Ghostrank byl odstraněn v roce 2018. Bude to znamenat, že informace se budou odesílat o všech?

Jakmile je spuštěn Zap, tak Ghostery zanedlouho odeslal sedm operací viditelných na obrázku níže.



Req. Timestamp	Method	URL	Code	Reason	RTT	Size Re...
3/16/20 8:10:58 PM	GET	https://cdn.ghostery.com/update/version	200	OK	700 ms	1,335 ...
3/16/20 8:10:59 PM	GET	https://api.ghostery.net/api/v1/config	200	OK	192 ms	609 by...
3/16/20 8:10:58 PM	GET	https://cmp-cdn.ghostery.com/check?os=other&offers=0&hw=0&install_date=...	204	No Co...	528 ms	0 bytes
3/16/20 8:10:59 PM	GET	https://cmp-cdn.ghostery.com/abtestcheck?os=other&install_date=2020-03-1...	200	OK	539 ms	53 bytes
3/16/20 8:11:00 PM	GET	https://cdn.ghostery.net/anti-tracking/whitelist/2/update.json.gz	200	OK	248 ms	43 bytes
3/16/20 8:11:00 PM	GET	https://cdn.ghostery.net/adblocker/configs/desktop-ads/allowed-lists.json	200	OK	160 ms	35,304...
3/16/20 8:11:00 PM	GET	https://collector-hpn.ghostery.net/config	200	OK	574 ms	5,116 ...

Obrázek č. 13 odesílané informace Ghostery

Při inspekci jednotlivých odeslaných zpráv bylo zjištěno, že odesílané informace nejsou nijak moc nebezpečné, jedná se o informace, které si Ghostery nasává po startu, jako je nějaká konfigurace nebo whitelist trackerů umístěných na webech či seznam povolených reklam.

Ale červeně podtržený řádek na obrázku výše odesílá následující:

Kód 4 Ghostery – odesílaná zpráva 1

```
https://cmp-cdn.ghostery.com/abtestcheck?os=other&install_date=2020-03-16&ir=9&gv=8.4.6&si=0&ua=firefox&v=0&l=enHTTP/1.1
```

A zeleně podtržený následující:

Kód 5 Ghostery – odesílaná zpráva 2

```
https://cmp-cdn.ghostery.com/check?os=other&offers=0&hw=0&install_date=2020-03-16&ir=9&gv=8.4.6&si=0&ua=firefox&lc=0&v=0&l=en HTTP/1.1
```

V těchto zprávách je hodně společných informací o:

- operačním systému,
- instalačním datu,
- verzi rozšíření,
- používaném prohlížeči
- a jazyku.

Ale vyskytují se zde informace, u kterých je těžké říct, co znamenají, jsou to položky jako:

- ir,
- si,
- v,
- lc,
- offers,
- hw.

Ale pokud se doplňku povolí v nastavení na záložce Opt In/Out položky:

- Sharing extention usage analytics,
- Sharing human web data.

Tak začne informací Ghostery posílat podstatně více, například bude odesílat, jakoukoli změnu v nastavení aplikace, pozastavení aplikace či označení stránky za důvěryhodnou.

Req. Timestamp	Method	URL	Code	Reason	RTT	Size R...
3/16/20 8:39:15 PM	GET	https://fonts.gstatic.com/s/opensans/v17/mem8YaGs126MiZpBA-UFVZ0b.woff2	200	OK	1 s	14,38...
3/16/20 8:39:16 PM	GET	https://fonts.gstatic.com/s/opensans/v17/mem8YaGs126MiZpBA-UFW50bbck.w...	200	OK	611 ms	11,31...
3/16/20 8:40:30 PM	GET	https://d.ghostery.com/trust_site/all?gr=-1&hw=1&v=8.4.6&ua=ff&os=other&l...	204	No Content	523 ms	0 bytes
3/16/20 8:41:27 PM	GET	https://d.ghostery.com/viewchange_from_simple/all?gr=-1&hw=1&v=8.4.6&ua...	204	No Content	507 ms	0 bytes
3/16/20 8:41:27 PM	GET	https://d.ghostery.com/viewchange_from_simple/daily?gr=-1&hw=1&v=8.4.6&u...	204	No Content	507 ms	0 bytes
3/16/20 8:41:31 PM	GET	https://d.ghostery.com/viewchange_from_detailed/all?gr=-1&hw=1&v=8.4.6&u...	204	No Content	517 ms	0 bytes
3/16/20 8:41:33 PM	GET	https://d.ghostery.com/hist_stats_panel/all?gr=-1&hw=1&v=8.4.6&ua=ff&os=...	204	No Content	125 ms	0 bytes
3/16/20 8:41:43 PM	GET	https://d.ghostery.com/viewchange_from_simple/all?gr=-1&hw=1&v=8.4.6&ua...	204	No Content	539 ms	0 bytes
3/16/20 8:41:50 PM	GET	https://d.ghostery.com/list_dash/all?gr=-1&hw=1&v=8.4.6&ua=ff&os=other&l...	204	No Content	499 ms	0 bytes
3/16/20 8:41:50 PM	GET	https://d.ghostery.com/list_dash/daily?gr=-1&hw=1&v=8.4.6&ua=ff&os=other...	204	No Content	496 ms	0 bytes
3/16/20 8:42:07 PM	GET	https://s3-eu-west-1.amazonaws.com/hokej.cz/scoreboard/2020-03-16.json	304	Not Modif...	245 ms	0 bytes

6 10 4 Primary Proxy: localhost:8080 Current Scans 0 0

Obrázek č. 14 odesílané informace Ghostery po povolení položek v nastavení

Taky je procházen kód, a to hlavně z důvodu, aby se objasnilo, co znamenají zkratky výše. V souboru background.js jsou nalezeny řádky začínající na *.ghostery.com/check* a *.ghostery.com/abtestcheck*. Tato část kódu poměrně jasně objasňuje, co zkratky znamenají.

```
.ghostery.com/abtestcheck
      ?os=${encodeURIComponent(ue.os)
}

      &install_date=${encodeURIComponent(I.a.install_date)
}

      &ir=${encodeURIComponent(I.a.install_random_number)
}

      &gv=${encodeURIComponent(Ie)
}

      &si=${I.a.account ? '1' : '0'
}

      &ua=${encodeURIComponent(ue.name)
}

      &v=${encodeURIComponent(I.a.cmp_version)
}

      &l=${encodeURIComponent(I.a.language)
}
```

Obrázek č. 15 .ghostery.com/abtestcheck

```
.ghostery.com/check
      ?os=${encodeURIComponent(k.os)
}
      &offers=${encodeURIComponent(I.a.enable_offers ? '1' : '0')
}
      &hw=${encodeURIComponent(I.a.enable_human_web ? '1' : '0')
}
      &install_date=${encodeURIComponent(I.a.install_date)
}
      &ir=${encodeURIComponent(I.a.install_random_number)
}
      &gv=${encodeURIComponent(0)
}
      &si=${encodeURIComponent(I.a.account ? '1' : '0')
}
      &ua=${encodeURIComponent(k.name)
}
      &lc=${encodeURIComponent(I.a.last_cmp_date)
}
      &v=${encodeURIComponent(I.a.cmp_version)
}
      &l=${encodeURIComponent(I.a.language)
}
```

Obrázek č. 16 .ghostery.com/check

V obrázcích se vyskytují nějaké položky na logickém principu, 0 znamená ne, 1 ano.

Vysvětlení zkratek:

- ir – náhodné číslo instalace,
- si – dává informaci, zda uživatel má účet,
- v – porovnání verzí,
- lc – porovnání posledního datumu,
- offers - zda bude uživatel dostávat nabídky od Ghostery,
- hw – Human web, funkce, která shromažďuje anonymní informace od uživatelů a snaží se vyvinout statistiku, která pomáhá této firmě k dalšímu vývoji. [47]

Tento plugin je jistě použitelný a má několik výhod. Jako pozitivum vidíme to, že i po povolení položek v nastavení aplikace, se neodesílá navštívená stránka. Ale ideální rozšíření to není, informace odesílá a je jich poměrně dost, když přijde na porovnávání tohoto doplňku

s pluginem Privacy Badger, tak oba nabídnou velmi podobnou službu, ale Ghostery nějaké informace odesílá, zatímco jeho konkurent ne. Na druhou stranu, pokud nebude povoleno větší monitorování, tak Ghostery neodesílá žádné citlivé informace o uživateli. Ale už je možné určité filtrování uživatelů podle jejich nastavení.

6.3 Adblock Plus

Adblock Plus velmi známý plugin do prohlížečů a funguje na několika platformách, jeho cílem je účinně blokovat reklamu a zpříjemnit tak čas strávený na internetu. Spolu s rozšířením uBlock Origin jsou nejvyužívanějšími blokátory reklam. [43]

Tabulka č. 3 Adblock Plus

Testovaná verze:		3.8.
Vývojář:		Adblock Plus
Počet uživatelů:	Firefox	9 715 811
	Chrome	10 000 000 +

[43] [44]

Při procházení internetových zdrojů jsou nalezeny pouze články o možné bezpečnostní díře v blokátorech reklam, při použití filtru rewrite. Dále na oficiálním webu adblockplus.org, lze dohledat informace o tom, že Adblock sbírá informace o technických vlastnostech pluginu i prohlížeče a další informace ukládá pouze na základě nějakého reportu či příspěvku ve fóru. [48] [49]

Po instalaci Adblocku ZAP jsou zachyceny tři velmi podobné zprávy, obsahující základní informace. Odesílaná informace je vždy stejná, liší se jen cílová adresa za posledním lomítkem.

Adblock po instalaci odeslal následující:

Kód 6 Ablock plus – odesílané informace po instalaci

```
GET https://easylist-downloads.adblockplus.org/abp-filters-anti-
cv.txt?addonName=adblockplusfirefox&addonVersion=3.8&application=fire
fox&applicationVersion=74.0&platform=gecko&platformVersion=74.0&lastV
ersion=0&downloadCount=0&firstVersion=0 HTTP/1.1
```

Z toho lze vyvodit tyto informace:

- addonName – jméno pluginu,
- addonVersion – verze pluginu,
- application – aplikace, v tomto případě Firefox,
- applicationVersion – verze aplikace (Firefoxu),
- platform – renderovací jádro aplikace (Gecko),
- platformVersion - verze platformy,
- lastVersion – poslední verze,
- downloadCount – počet stažení,
- firstVersion – první verze.

Je toho docela dost, ale jsou to informace, jež mohou být potřeba pro správné fungování, jsou to vlastně informace o pluginu samotném a o prohlížeči na jakém je nainstalován, ale například informace kolikrát je Adblock stažen, je navíc.

Při normálním používání jinak Adblock Plus nic neodesílá. I pokud je přes Adblock ručně nějaká reklama odstraněna, tak Adblock nic neodešle. Informace odesílá pouze tehdy, pokud je nahlášena chyba Adblocku přes odkaz nacházející se v tomto pluginu pod jménem nahlásit problém. To ovšem bylo naprosto v pořádku, jelikož je cíleně nahlášen problém.

Když se to shrne, tak Adblock plní svou funkci a kromě původní zprávy, tedy i avizovaných dat, která Adblock potvrdil i na oficiálních stránkách, nic navíc neodesílá.

6.4 uBlock Origin

Toto rozšíření se chlubí dobrým blokováním reklamy, a přitom nezatěžuje procesor ani paměť. Skládá se z filtrů, v základu aplikace jsou spuštěny čtyři, další lze přidat, ale čím více jich bude použito, tím více se bude toto rozšíření zpomalovat. [43]

Tabulka č. 4 uBlock Origin

Testovaná verze:		1.25.2.
Vývojář:		Raymond Hill
Počet uživatelů:	Firefox	5 927 899
	Chrome	10 000 000+

[43] [44]

Při procházení internetových zdrojů je nalezen článek upozorňující na bezpečnostní díru v aplikaci, bezpečnostní díra je stejná jako u výše zmíněného Adblocku Plus, ale nejsou nalezeny žádné informace o tom, že tento plugin něco odesílá, prověřován je i jeho vývojář a nalezené informace nenasvědčují tomu, že by měl tento plugin něco odesílat, ale je důležité to prověřit. [48]

Dokonce byly nalezeny informace, že tento doplněk, nemá žádný domovský server, kam by mohl data vůbec odesílat. [50]

Prověřování tohoto rozšíření trvá poměrně krátce, ZAP nezachycuje žádnou komunikaci, takže se dá prohlásit, že uBlock Origin nic neodesílá, a proto je z hlediska nějakého monitorování uživatelů přímo vhodný.

6.5 Privacy Badger

Privacy Badger je další rozšíření, které má chránit uživatelské soukromí a blokovat trackery umístěné na webu. [43]

Tabulka č. 5 Privacy Badger

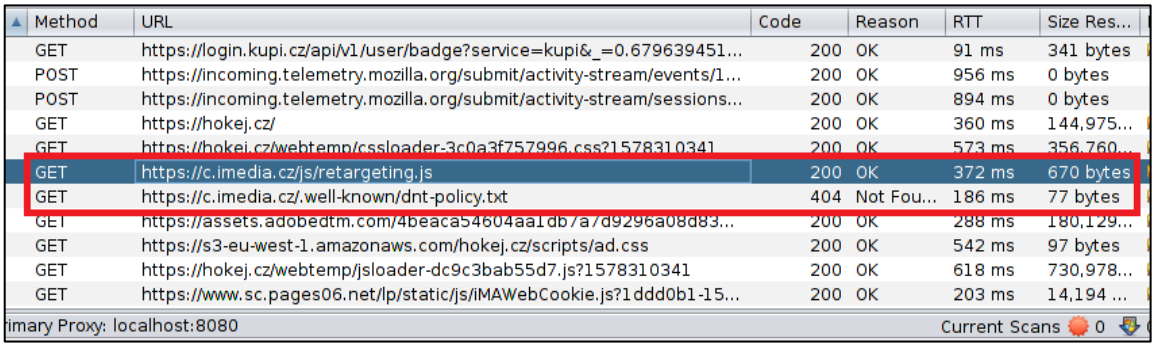
Testovaná verze:		2020.2.19.
Vývojář:		EFF Technologies
Počet uživatelů:	Firefox	1 281 178
	Chrome	1 000 000+

[43] [44]

Při hledání informací o tomto rozšíření žádné z nich nevypovídá o tom, že by mělo být rozšíření nějakým způsobem nedůvěryhodné nebo že by dokonce v minulosti mělo s něčím takovým problémy. Na první pohled vypadá všechno velice slušně.

Po stažení a instalaci tohoto pluginu je vyzkoušena jeho funkčnost, Privacy Badger zablokuje ty trackery, které zná, ty co nezná, tak dá uživateli možnost je zablokovat či ne.

Na ukázku je využit web hokej.cz, na tomto webu Privacy Badger zachytil 30 trackerů. Oproti tomu seznam.cz měl pouze 4, ale je potřeba říci, že právě seznam má svůj tracker na webu hokej.cz. Funkčnost byla demonstrována na trackeru c.media.cz. Pokud nebyl zablokovaný v Privacy Badgeru, ZAP zachytil komunikaci právě s tímto serverem.



Obrázek č. 17 Zachycená komunikace se c.media.cz

Následuje zapnutí blokování, v tomto rozšíření se již c.media.cz v ZAPu neobjevuje, Privacy Badger funguje opravdu dobře.

Při testování tohoto doplňku v ZAPu není zachycena žádná komunikace. Tento plugin nic neodesílá, což v tomto smyslu mu dává značnou výhodu před Ghostery, který toho odesílá více.

6.6 Video DownloaderHelper

Rozšíření usnadňuje uživatelům stahování mediálního obsahu, například videa či fotky z webu a ukládat je do lokálního úložiště. [43]

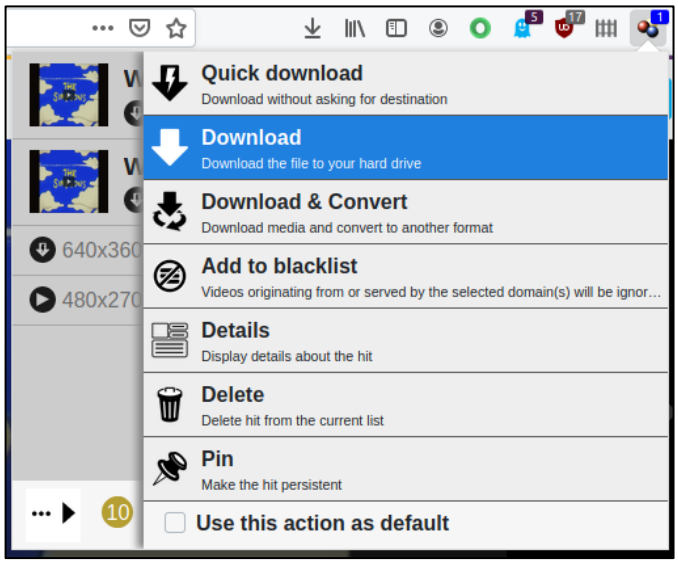
Tabulka č. 6 Video Downloader Helper

Testovaná verze:		7.3.7.
Vývojář:		mig
Počet uživatelů:	Firefox	3 099 976
	Chrome	_____

[43]

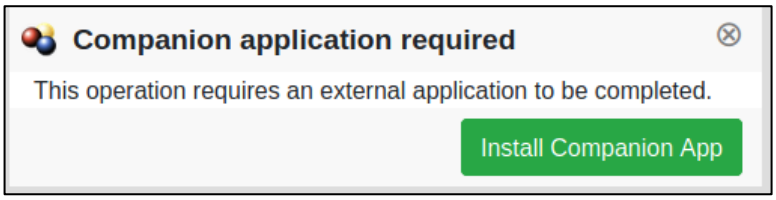
Při procházení internetových zdrojů není shledáno nijaké špatné chování tohoto doplňku. Ani hledání o jeho vývojáři není úspěšné, jeho přezdívka na webu addons.mozzila.org je pouze „mig“ a ani v různých kombinacích hledání není nic nalezeno.

Po instalaci pluginu a spuštěním prohlížeče tento doplněk nic neodesílá, ale je potřeba také otestovat to, zda nebude doplněk něco odesílat při stahování nebo po stažení videa. Pro tento účel byl využit web vimeo.com.



Obrázek č. 18 stažení videa přes VideoDownloader helper

Po kliknutí na download je stránka přesměrována a pro stažení videa je potřeba doinstalovat externí aplikaci.



Obrázek č. 19 instalace externí aplikace

Stále je kontrolováno, zda jsou nějaké informace odesílány a žádné odesílané informace nebyly zachyceny. Po instalaci potřebné aplikace je konečně staženo video. A ani po stažení žádné informace tento doplněk neodesílá.

6.7 NoScript Security Suite

NoScript Security Suite vznikl s cílem dát uživatelům větší bezpečí při pohybování na internetu. Malware se většinou objevuje při surfování jako javascript či flash. Jednoduše se dá říct, že se může zakázat javascript a uživatel bude v bezpečí, to je pravda, ale některé stránky mohou ztratit některou funkčnost nebo se vůbec nenačíst. Toto rozšíření se snaží najít kompromis mezi normálním chodem stránek a bezpečností. Rozšíření spouští javascript a flash pouze na ověřených doménách a těch, jaké si uživatel schválí. [43]

Tabulka č. 7 NoScript Security Suite

Testovaná verze:		11.0.19
Vývojář:		Giorgio Maone
Počet uživatelů:	Firefox	1 845 026
	Chrome	90 000+

[43] [44]

Do internetových vyhledávačů je zadáno několik různých kombinací hledání v souvislosti se špehováním uživatelů či prodejem jejich dat, také je prověřován autor tohoto rozšíření Giorgio Maone a nalezeny jsou pouze články, které nezpůsobují podezření.

Program Owasp ZAP nezachytil žádné zprávy, které by doplněk odesílal. Tudíž není potřeba zkoumat kód. Rozšíření NoScript Security Suite uživatele nemonitoruje a je bezpečné ho používat.

6.8 Facebook container

Facebook container nabízí uživatelům izolovat Facebook od jejich ostatních aktivit na internetu. Facebook se otvírá v containeru, kde se používá Facebook naprosto stejně jako při použití přímo. [43]

Tabulka č. 8 Facebook container

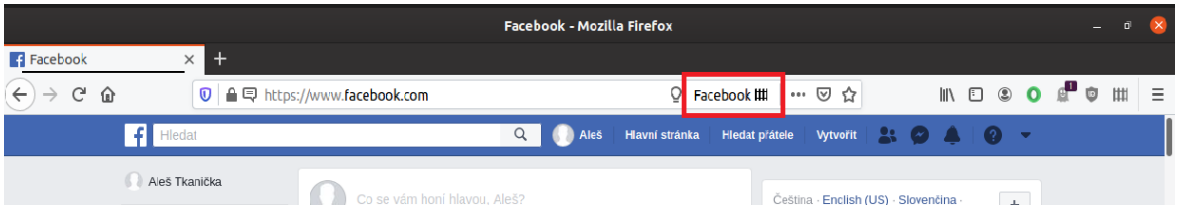
Testovaná verze:		2.1.0
Vývojář:		Mozilla Firefox
Počet uživatelů:	Firefox	2 067 024
	Chrome	_____

[43]

Při hledání informací na webu jsou nalezeny titulky pouze o tom, že toto rozšíření zamezí Facebooku monitoring uživatelů. Informace o tom, že tento plugin dělá něco špatně, nalezeny nejsou.

Pro plné otestování tohoto produktu bylo potřeba vytvořit si profil na Facebooku za účelem testování, po ukončení testování bude tento účet smazán.

Jako první je doplněk otestován, zda odesílá něco, i když uživatel není přihlášen. V tomto případě nic nalezeno není, plugin nic neposílá. Potom nastal čas otestovat plugin, když se někdo doopravdy přihlásí na Facebook. Po přihlášení se pod testovacím účtem a v adresním řádku prohlížeče zobrazila malá ikonu plotu.



Obrázek č. 20 Facebook Container

Tato ikona symbolizuje, že je přihlášeno přes Facebook container. Opět je provedena kontrola přes ZAP, zda rozšíření nezačalo informace odesílat ve chvíli, kdy se uživatel přihlásí. Opět tato kontrola nic špatného neodhalila.

6.9 Avast Online Security

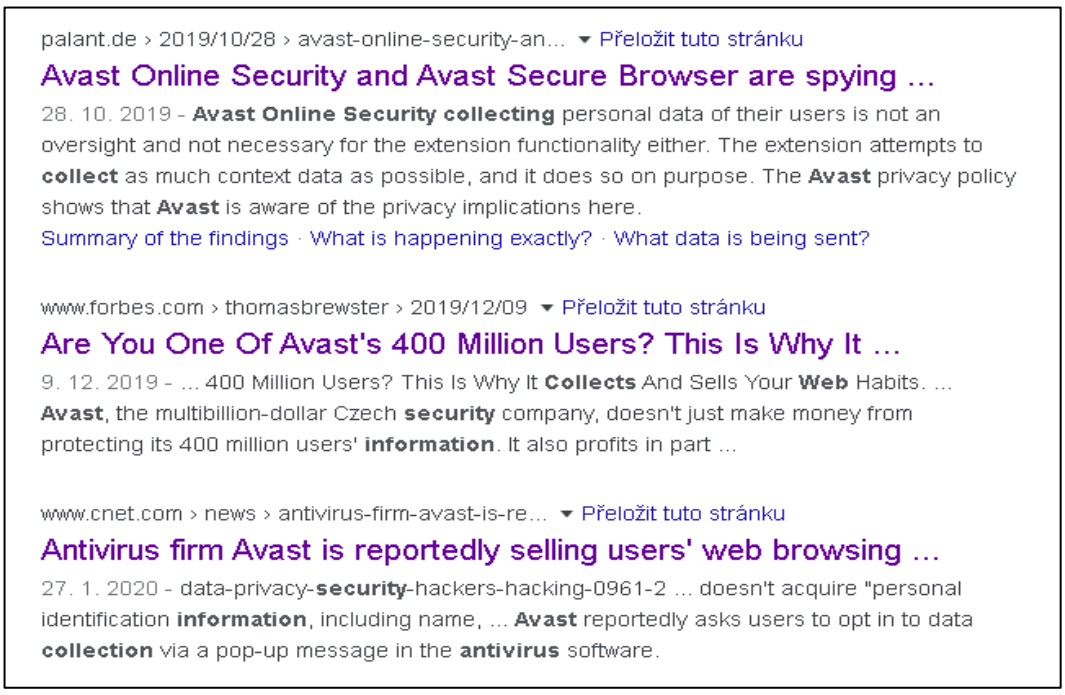
Avast Online Security obsahuje několik různých funkcí, jež mají zvýšit bezpečí uživatele. Jedná se například o funkce varování před vstoupením na stránky s potencionálně nebezpečným obsahem, hodnotí stránky, blokuje reklamu a chrání před sledováním. [43]

Tabulka č. 9 Avast Online Security

Testovaná verze:		20.1.480.
Vývojář:		Avast
Počet uživatelů:	Firefox	954 839
	Chrome	10 000 000+

[43] [44]

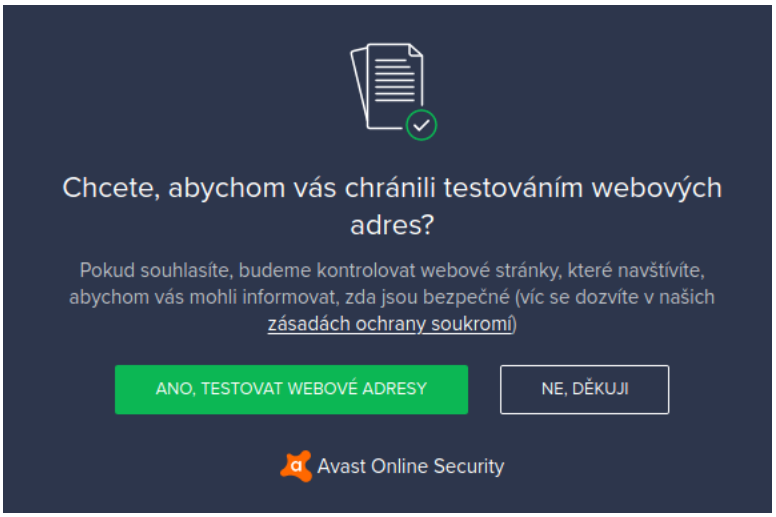
Při hledání informací o tomto rozšíření bylo nalezeno několik velmi zajímavých odkazů.



Obrázek č. 21 informace nalezené o Avastu

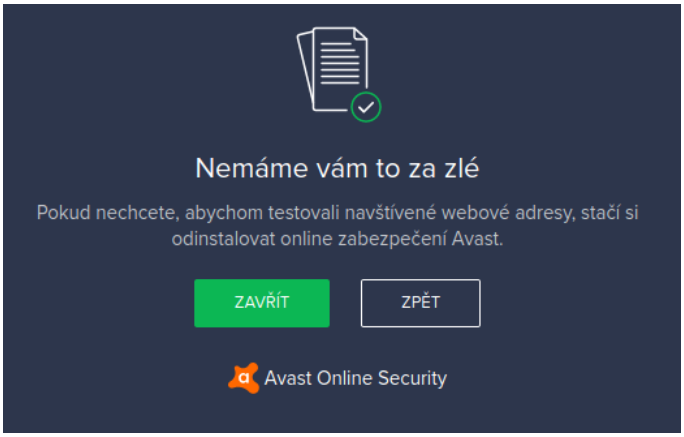
Podle Wladimira Palanta sbírá Avast masově velké množství uživatelských dat a jejich množství daleko překračuje meze únosného, shromažďuje data, která nejsou nutná pro fungování tohoto produktu. Zpráva byla vydána v říjnu roku 2019. Na tuto informaci reagovaly internetové obchody, které poskytují rozšíření a Avast Internet Security byl z těchto obchodů stažen pryč. Druhý nalezený článek je z ledna roku 2020, kde se píše, že Avast přehodnotil svůj přístup k této problematice a monitorování by nemělo probíhat. To dokážou tím, že zruší jejich dceřinou společnost Jumpshot, jež měla na svědomí prodej sesbíraných uživatelských dat. Jakmile Avast splnil požadavky portálů pro stahování pluginů, tak byl zařazen zpět. Z těchto informací, je jasné, že je důležité tento doplněk důkladně prověřit. Přestal Avast opravdu uživatele sledovat? [51] [52]

Hned po instalaci vyskočila hláška viditelná na obrázku níže.



Obrázek č. 22 Avast testování webových adres

V této chvíli jsou dvě možnosti, pokud je zvolena možnost ano, tak se pravděpodobně něco odesílat bude, pokud je zvoleno ne, nemělo by se tak dít. Jako první bude prověřena možnost ne. Při zvolení této možnosti Avast vyzývá, ať ho uživatel odinstaluje.

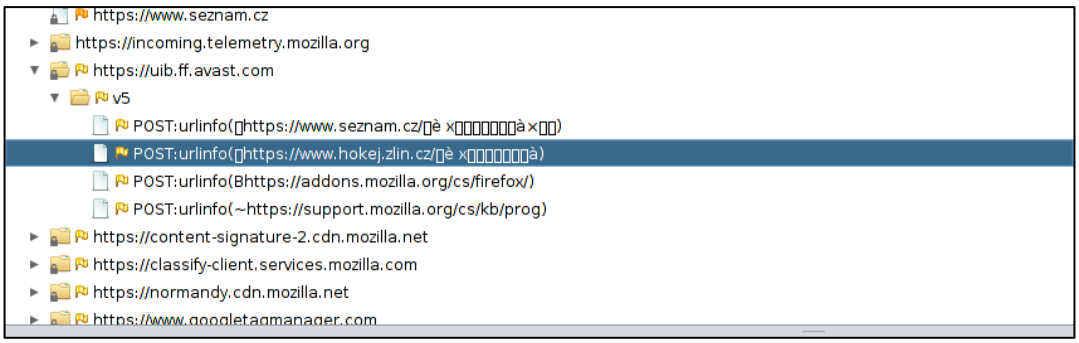


Obrázek č. 23 Avast výzva k oddinstalaci

Z této hlášky vyplývá, že Avast asi bez toho aniž by něco odesílal, fungovat nemůže, pokud se bude pokračovat dále a rozšíření se neodinstaluje, tak se jako ikona tohoto pluginu zobrazí červený křížek, který signalizuje, že doplněk v tuto chvíli nefunguje. ZAP žádnou komunikaci nezachycuje, ale taky Avast nefunguje. Je potřeba prozkoumat, co odesílá Avast, jakmile je povolena možnost testování webových adres.

Po zvolení této možnosti opravdu Avast začal odesílat, odesílá zprávu o každé navštívené stránce, dokonce odesílá i zprávu o přepnutí mezi panely v prohlížeči.

Analýza pomocí Zapu odhalila následující odesílání dat:



Obrázek č. 24 Avast odesílané informace

Avast odeslal data o každé stránce, jenž je navštívena, co přesně odesílá, při navštívení stránky hokej.zlin.cz je zaznačeno níže:

```
https://www.hokej.zlin.cz/
```

Obrázek č. 25 odeslané informace Avastem

Funkce tohoto pluginu je v hodnocení stránek, Avast by měl o stránce vždy říct, zda je bezpečná či ne, tak by odesílání veškerých adres nemuselo znamenat nijak závažný problém, ale není to jediné, co Avast odesílá, ostatní informace jsou nečitelné. Pokud je využito internetové vyhledávání, tak do Avastu se také odešlou všechny nalezené stánky, je to testováno na Googlu i českém Seznamu. Jako první se odešle klasická zpráva o pohybu, jako je znázorněno na obrázku 24. Potom Seznam odešle několik dotazů na svoje servery a načte stránku, následně se informace odešlou do Avastu. Toto jsou odeslané informace do Avastu při vyhledávané frázi „jak dělá pes“.

Kód 7 Avast Online Security - odesílané informace při hledání ve vyhledavači Seznam

```
https://www.seznam.cz/
0https://fungate.cz/co-dela-pes-kdyz-je-sam-doba/
>https://www.pesweb.cz/cz/1731.muj-pes-si-dela-co-chce-co-s-tim
Khttps://g.cz/58-situaci-ktere-dela-pes-schvalne-aby-pana-pripravil-
o-nervy/
:https://www.emimino.cz/diskuse/pes-dela-zakernosti-345653/
Chttps://www.ifauna.cz/psi/diskuse/detail/3361448/pes-dela-neporadek
;https://www.poradte.cz/zvirata/9786-pes-dela-naschvaly.html
}https://www.idnes.cz/hobby/mazlicci/zarlivy-pes-maltezak-dela-u-
pritele-louzicky-i-hromadky.A140413_092715_hobby-mazlicci_mce
1https://www.spokojenypes.cz/proc-to-ten-pes-dela/
Ahttps://cz.depositphotos.com/vector-images/kreslen%C3%BD-pes.html
 http://retriever-labradorsky.cz/
`https://search.seznam.cz/?q=jak%20d%C4%9Bl%C3%A1%20pes&count=10&pId=
dilOPDPcpC5nT8WhjF3J&from=10
`https://search.seznam.cz/?q=jak%20d%C4%9Bl%C3%A1%20pes&count=10&pId=
dilOPDPcpC5nT8WhjF3J&from=20
`https://search.seznam.cz/?q=jak%20d%C4%9Bl%C3%A1%20pes&count=10&pId=
dilOPDPcpC5nT8WhjF3J&from=30
`https://search.seznam.cz/?q=jak%20d%C4%9Bl%C3%A1%20pes&count=10&pId=
dilOPDPcpC5nT8WhjF3J&from=10
8https://napoveda.seznam.cz/cz/seznam/nastaveni-geolokace
https://www.seznam.cz/
:https://napoveda.seznam.cz/cz/fulltext-hledani-v-internetu
"https://www.seznam.cz/ochranaudaju
;https://search.seznam.cz/stats?q=jak%20d%C4%9Bl%C3%A1%20pes
'https://search.seznam.cz/pridej-strankuè x□à×□
```

Avast si ukládá vše, co internetový vyhledavač našel. Ukládá si všechny webové stránky, které odpovídají vyhledávání, dále si ukládá odkazy pro další seznam vyhledávaných položek na dalších číslovaných kartách. Tyto odkazy jsou zaznamenány tmavě šedě. Nakonec si uloží odkazy na nápovědu, ochranu údajů a další, zkrátka je uloženo vše, co někam odkazuje. Avast odesílá každou stránku dvakrát, tak duplikace jsou odstraněny, aby nebyl výpis příliš dlouhý, dále je trochu zkrácen o některé adresy odkazující na další karty vyhledávání.

Po prvním analyzování byl názor takový, že získané informace musí být Avastu zbytečné, že se jedná víceméně o to, co se vyhledá po zadání fráze do vyhledavače. Ale není tomu úplně tak. Internetové vyhledavače jsou propracované systémy (zejména Google), které dokážou uživateli vyhledat takovou sadu dat, která se vygeneruje dle zkušenosti s daným vyhledavačem či dle lokace, kde se vyhledává. Nakonec se tyto informace stávají velice citlivými. Uvedu na příkladu, pokud ve Zlíně vyhledáme výraz „restaurace“, tak Google vrátí výsledky s restauracemi ve Zlíně. Tímto způsobem dokáže Avast zjistit, kde se zhruba může uživatel nacházet, a to bez jakéhokoliv souhlasu. [53]

Při procházení kódu v debuggeru ve Firefoxu, lze v kódu najít, že Avast dokáže zjistit docela hodně, může to být například: operační systém, verze operačního systému, prohlížeč, verze prohlížeče, verzi rozšíření, navštívenou stránku, všechny otevřené panely v prohlížeči, lokalizaci a jistě to není vše. Ale otázka spíše zní, co odesílá. V kódu je nalezen callback:urlInfoChange a v položce request jsou zajímavé pouze informace:

- navštívená stránka
- verze rozšíření

A mohlo by to odpovídat, protože odesílaných informací opravdu není hodně. Na obrázku níže lze vidět, že zprávy se odesílají na adresu https://uib.avast.com přes port 443. Přesně tyto informace sedí k informacím z ZAPU, dá se tedy předpokládat, že tento kus kódu odesílá informace.

Obrázek č. 26 Avast – co odesílá

Pokud v nastavení je povoleno sdílení více dat, tak občas pošle zpráva na adresu https://analytics.ff.avast.com/v4/receive/gpb. Na tuto adresu se vždy odešle zpráva, pokud se udělá změna v nastavení.

Potom, co vyšlo najevo, že Avast sbíral data, tak udělal několik změn. Zrušil Jumpshot a přestal uživatele masivně sledovat a podle výzkumu už Avast odesílá informace, jež jsou důležité pro jeho funkci, ale taky odesílá výše zmíněné internetové vyhledávání. Avast, jakožto bezpečnostní firma, teď bude mít těžkou práci s novým budováním důvěry směrem k zákazníkům, ale základ už položili, odesílané informace z pluginu Avast Online security jsou minimální oproti původním, ale pořád se tu vyskytuje jisté ale.

6.10 Avast Safe Price

Avast Safe Price má pomáhat uživatelům s nakupováním. Porovnává nabídky různých obchodů a vyhledává nejlepší cenu. Také se dá použít na objevování aktuálních slevových kuponů. Chlubí se tím, že porovnává až 100 000 stránek. [43]

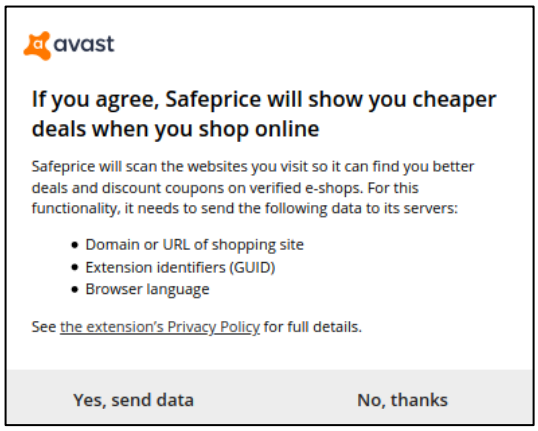
Tabulka č. 10 Avast Safe Price

Testovaná verze:		20.1.1611
Vývojář:		Avast
Počet uživatelů:	Firefox	268 272
	Chrome	10 000 000+

[43] [44]

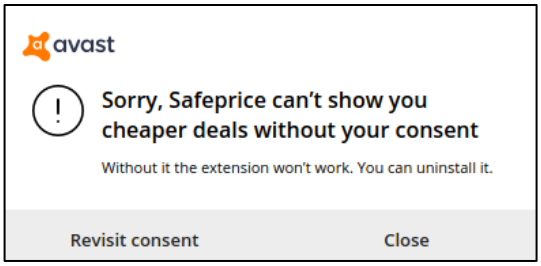
Při hledání informací jsou nalezené podobné informace jako o výše zmíněném pluginu od Avastu. Informace se týká toho, že Avast shromažďuje velké množství dat. [54]

Po instalaci se jako první objeví výzva k našemu souhlasu s tím, že se budou některé informace odesílat.



Obrázek č. 27 Avast Safe Price – výzva k povolení odesílání dat 1

Po vybrání možnosti nesouhlasu s odesíláním se objeví další výzva pro nové povolení nebo pro zavření, a to bohužel znamená to samé jako u Avast Online Secutity, rozšíření zůstane nainstalované, ale nebude funkční.

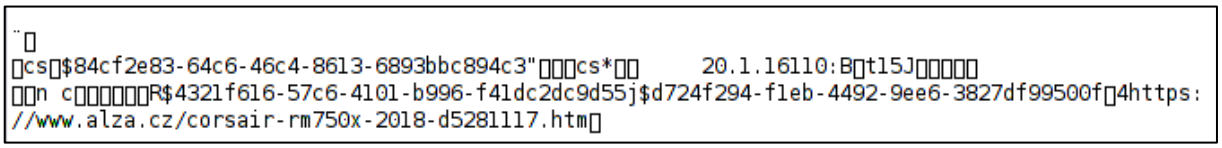


Obrázek č. 28 Avast Safe Price – výzva k povolení odesílání dat 1

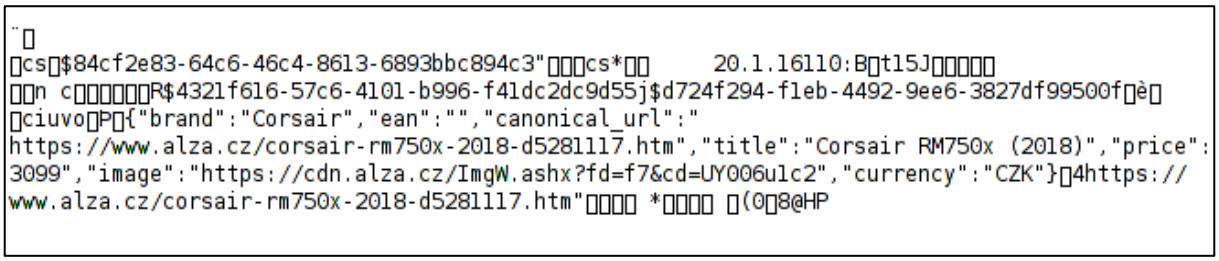
Jak se zdá, tak Avast Safe Price, tak jako jeho kolega od Avastu nedokáže pracovat bez odesílání dat, ale pro svou službu nějaké data potřebuje, zatím tedy není nic v nepořádku.

V ZAPU je zjištěno, že toto rozšíření odesílá informace o každé stránce, která je navštívena, tak jako odesílá Avast Online Security. Pokud je navštíven internetový obchod a je rozkliknuto přímo hledané zboží, tak tento doplněk najde stejný produkt v jiných obchodech za nejlepší cenu. Aby byla tato funkce schopná fungovat, musí Avast vědět, jaká stránka je navštívená. Ale problém je v tom, že tuto funkcionalitu nejde nijak vypnout, v nastavení lze vypnout pouze upozornění, ale doplněk dělá úplně to stejné co předtím. Pouze neupozorní na lepší nabídku. Tento doplněk zkrátka odesílá informace o každé navštívené stránce.

Ale to není všechno, co Avast odesílá. Navíc se odesílají i zprávy, na jejichž základě se načítají lepší nabídky daného produktu. První zpráva se odesílá na adresu: https://safeprice.ff.avast.com/v3/scrapers. A druhá zpráva se odesílá na adresu: https://safeprice.ff.avast.com/v3/offers.



Obrázek č. 29 Avast Safe Price – odesílaná data 1



Obrázek č. 30 Avast Safe Price – odesílaná data 2

Na první pohled je vidět, že odcházejí zprvu data, která jsou nečitelná a potom čitelný odkaz na stránku, jenž byla navštívena. Druhá zpráva obsahuje navíc informace o prohlíženém zboží, jako informace o:

- ceně,
- jméně výrobku,
- značce výrobku,
- měně,
- odkazu na obrázek, který je vystavovaný na dané stránce,
- stránce, jaká je právě navštěvována.

Stále ale jsou ve zprávách nečitelná data. Je nutné prozkoumat kód a pokusit se najít, co ta nečitelná data znamenají. Zpráva totožná se zprávou odesílanou doplňkem Avast Oline Security se testovat nebude, jelikož je stejná. Zkoumat se budou další dvě zprávy zmíněné v obrázcích výše.

V souboru query.js na řádku 126 byla nalezena část kódu, která odesílá požadavky na server.

Obrázek č. 31 zpráva odesílající se na https://safeprice.ff.avast.com/v3/scrapers

Zpráva se odesílá na adresu https://safeprice.ff.avast.com/v3/scrapers, což sedí se zprávou zachycenou přes ZAP. Druhá zpráva se odesílá na adresu https://safeprice.ff.avast.com/v3/offers

```
method: "post"
▶ notificationsFlag: {…}
▼ parserResults: (1) […]
  ▼ 0: {…}
    ▶ csl: {…}
      providerId: "ciuvo"
    ▼ query: {…}
        brand: "Corsair"
        canonical_url: "https://www.alza.cz/corsair-rm750x-2018-d5281117.htm"
        currency: "CZK"
        ean: ""
        image: "https://cdn.alza.cz/ImgW.ashx?fd=f7&cd=UY006u1c2"
        price: "3099"
        title: "Corsair RM750x (2018)"
      ▶ <prototype>: {…}
    ▶ <prototype>: {…}
    length: 1
  ▶ <prototype>: []
server: "https://safeprice.ff.avast.com:443/v3/offers"
▶ tab: {…}
timeout: 10000
url: "https://www.alza.cz/corsair-rm750x-2018-d5281117.htm"
▶ urlData: {…}
▶ <prototype>: {…}
▼ request: {…}
  message_type_: "AvastWRC.gpb.All.SafeShopOffer.OfferRequest"
▶ properties_: {…}
▼ values_: {…}
  ▶ available_template: {…}
  ▼ client_info: {…}
      message_type_: "AvastWRC.gpb.All.SafeShopOffer.ClientInfo"
    ▶ properties_: {…}
    ▼ values_: {…}
      ▶ browser: {…}
        campaign_id: "t2"
        client: 0
      ▼ extension: {…}
          message_type_: "AvastWRC.gpb.All.SafeShopOffer.ClientInfo.Extension"
        ▶ properties_: {…}
        ▼ values_: {…}
            type: 0
            version: "20.1.1611"
          ▶ <prototype>: {…}
        ▶ <prototype>: {…}
        extension_guid: "c86e63e4-f96f-4603-aa31-c2e69e4142d8"
        guid: ""
        language: "en"
        request_id: "625a1307-90d5-4cb5-aec3-23fb92f29495"
        transaction_id: "ea7c5e2e-b73f-4e96-86ab-74228c3b319f"
      ▶ user_settings: {…}
      ▶ <prototype>: {…}
    ▶ <prototype>: {…}
  ▶ notification_flags: {…}
  ▶ provider_query: {…}
    url: "https://www.alza.cz/corsair-rm750x-2018-d5281117.htm"
```


Obrázek č. 32 zpráva odesílající se na https://safeprice.ff.avast.com/v3/offers

Z výše uvedených obrázků a jejich informací se dá vyvodit, co se odesílá v nečitelných datech.

Z těchto zpráv lze vypíchnout pár zajímavých informací:

- request_id – id požadavku
- transaction_id – id transakce
- language - jazyk
- extension_guid – unikatní identifikátor rozšíření
- version – verze rozšíření

Dále po rozkliknutí položky user_settings se odesílají informace o tom, kolik nabídek se může maximálně zobrazit. Ale v nastavení žádná taková možnost nalezena nebyla.

Položky request_id a transaction_id, nepřidávají mnoho na důvěryhodnosti. Pokud něco má identifikační číslo, může být ukázkou toho, že se data někde skladují, nešlo by to udělat tak, aby se odesílal pouze název produktu, popřípadě výrobce a na základě toho dostat nějaké nabídky?

A hlavní věc, jež mi přijde navíc, je ověřování, zda je stránka důvěryhodná, to zní sice pěkně, ale ve výsledku to znamená to, že plugin, který má pomáhat nakupovat, odesílá všechny navštívené stránky. Tato funkčnost je samozřejmě nutná, pokud uživatel bude chtít automaticky načítat nabídky, ale samo o sobě pouze vyhledávání nejlevnějšího zboží nefunguje, tento doplněk přitom bude mapovat navštívené stránky. A ruku na srdce, jak často nakupujeme online, abychom využili tento plugin? Je to hodně individuální, ale pokud nenakupujeme, proč by mělo toto rozšíření vědět, co na internetu děláme a jaké stránky navštěvujeme?

6.11 Shrnutí výsledků

Tato poslední podkapitola přehledně shrne výsledky výzkumu, jednoduše řekne, zda je bezpečné plugin používat či ne.

	Název pluginu	Odesílá informace	Množství odesílaných dat
1.	Web of trust	Ano	Neúnosné jeho funkci.
2.	Ghostery	Ano	Únosné jeho funkci.
3.	Adblock Plus	Ano	Únosné jeho funkci.
4.	uBlock Origin	Ne	_____
5.	Privacy Badger	Ne	_____
6.	Video Downloader helper	Ne	_____
7.	NoScript Security Suite	Ne	_____
8.	Facebook Container	Ne	_____
9.	Avast Online Security	Ano	Neúnosné jeho funkci.
10.	Avast Safe Price	Ano	Neúnosné jeho funkci.

Únosnost odesílaných dat byla posouzena hlavně v souvislosti s funkcí jednotlivých doplňků. Jako příklad teď poslouží plugin Web of trust. Pro funkci tohoto doplňku je nutné odesílat pouze navštívenou stránku, ale tento plugin odesílá mnohem víc informací, tyto informace jsou navíc. Kvůli těmto důvodům bylo rozhodnuto, že odesílaná data jsou neúnosná jeho funkci.

Všechna rozšíření, která neodesílala žádné informace, jsou v pořádku, ale u doplňků, které něco odesílají, bylo třeba vyhodnotit, zda odesílané informace jsou potřebné k jeho funkci nebo ne. Avast Online Security doplatil na to, že si vyhledávání neukládá jako jeden odkaz, ale ukládá si všechny nalezené odkazy. A poslední Avast Safe Price bude sledovat pohyb uživatele i když nenakupuje. A to je dle mého pro takový doplněk nežádoucí. Další dva doplňky, co odesílaly data, jich mohly sice odesílat míň, ale tyto doplňky nemapují uživatelův pohyb, pouze při instalaci či zapnutí odešlou pár informací o prohlížeči a používaném doplňku, proto bylo rozhodnuto, že odesílaná data jsou únosná.

ZÁVĚR

Je potřeba si uvědomit, že lidé žijí ve vyspělém světě, kde se čím dál častěji setkávají s moderními technologiemi, které dokáží spoustu činností a procesů urychlovat a zjednodušovat, život by tím pádem z tohoto hlediska měl být lehčí. Dá se říct, že tomu tak opravdu je. Aplikace existují už téměř na cokoliv a v prostředí internetu lze najít nezměrné množství informací, jež se dají využít. Ale s tímto rozmachem moderních technologií a s nimi souvisejících možností, se otevírají také možná úskalí. Tím, že lidé mohli častým zjednodušováním zlenivět či prostě neznalostí se mohou dostat do problémů souvisejících s různými druhy malwaru, hackerských útoků atd. Tento problém se již ale dostává do povědomí lidí a existuje mnoho možností, jak se chránit. Ale tématem na hraně je monitorování uživatelů. Kam ho zařadit? Na tuto otázku není lehké odpovědět a právě touto otázkou se zabývá tato práce. Sledování lze tolerovat do určité míry, zda systém či aplikace tyto informace potřebuje ke své činnosti, pokud je tomu jinak, je to naprosto nepřípustné. A vůbec ubránit se sledování, i když není uživatel nikde přihlášen, je také velmi těžké, časem se většinou personalizované reklamy dostaví. Dosáhnout internetového soukromí je opravdu těžké a být anonymní je ještě těžší. A to je trn celého problému, běžný uživatel prostě nebude platit rychlou VPN službu, či používat pomalý TOR a dělat další omezení způsobené tím, aby nebyl sledován. Běžný uživatel chce zkrátka používat jednoduché, intuitivní a nové věci a nechce přemýšlet nad problémy tohoto typu. Je to nastavené obráceně, normální stav by měl být ten, že uživatel je na výchozím bodě nesledován a pokud by mu to nevadilo, mohla by nastat běžná praxe. Bohužel monitorování se může dít i přes malé věci, běžný člověk nepřemýšlí nad tím, že by obyčejný plugin do prohlížeče, který sice může vykonávat službu k ní primárně určenou, ale také může sbírat informace, by ho mohl sledovat. V této práci bylo rozebráno deset pluginů, z toho polovina odesílala informace. Z těchto pěti pluginů tři odesílaly více, než potřebovaly, a některé měly dokonce drzost nefungovat, pokud jim uživatel vysloveně nedovolil ho sledovat. Z deseti zkoumaných doplňků 33 % sbíralo nadměrné množství informací. Těžko předpovídat, jaké procento by bylo při prozkoumání všech dostupných pluginů, ale jako vzorek může stačit i toto. Testované pluginy používá dostatečné množství lidí a ty s menšími počty uživatelů mohou být ještě nebezpečnější, jelikož nejsou tak „na očích“. Tudíž by toto číslo mohlo zhruba odpovídat realitě.

Těžko se hledá vysvětlení, proč se tento masový sběr informací děje, můj názor je, že je to prostě trh, na kterém každý jeho účastník chce vydělat. Ale jak si má běžný člověk s těmito

informacemi poradit? Je důležité si uvědomit, že když člověk sedne za monitor, nezavře se ve své malé bublině, ale někdo může vědět, co přesně dělá.

Prostřednictvím sociálních sítí lidé sdílejí často ty nejintimnější osobní informace, s nimiž by se nesvěřili ani těm nejbližším. Ve většině případů si neuvědomují možné následky, které takové zveřejnění může způsobit.

Člověk si musí chránit své soukromí, a to nejlíp tak, že nebude ničemu a nikomu zadarmo svěřovat své informace, bude chodit na bezpečné stránky, bude dodržovat zásady bezpečnosti a zkrátka se bude chovat na internetu tak, jako by se sám nacházel někde na veřejnosti.

Svět moderních technologií bychom mohli přirovnat ke světu dopravy. Abychom mohli bez větší újmy v takovém světě přežít, potřebujeme nastudovat dopravní předpisy, naučit se orientovat v dopravním provozu. Nezbývá tedy nic jiného než doporučit všem uživatelům, aby v online prostředí vždy konali s rozumem a pokud možno nastudovali „dopravní předpisy světa moderních technologií“, získali pomyslný řidičský průkaz, jenž je bezpečně provede úskalími moderních technologií a vyhnou se tak možnosti úniku citlivých informací.

„Proč nám skvělá technika, která šetří práci a usnadňuje život, dosud přinesla tak málo štěstí? Odpověď je prostá: protože jsme se jí nenaučili rozumně užívat.“

Albert Einstain [55]

SEZNAM POUŽITÉ LITERATURY

[1] KISSELL, a JOE. *Take Control of Your Online Privacy*. 2. vydání. NewYork: TidBITS Publishing, 2015. ISBN 978-1-61542-454-2.

[2] SCHNEIER, a BRUCE. *Data and Goliath: the hidden battles to collect your data and control your world*. 1. vydání. NewYork: W. W. Norton & Company, 2015. ISBN 978-0-393-24481-6.

[3] ECKERSLEY, Peter. *How Unique Is Your Web Browser?*. Berlín: Springer, 2010. ISBN 978-3-642-14527-8.

[4] WOJDYLA, Ben. *How it Works: The Computer Inside Your Car* [online]. NYC: Popular mechanics, 2012 [cit. 2020-02-06]. Dostupné z: https://www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/

[5] YOUNG, Miles. *Google spies on you. What data does it collect?* [online]. USA: Business 2 community, 2013 [cit. 2020-02-06]. Dostupné z: https://www.business2community.com/social-media/how-long-do-your-online-posts-stay-on-the-internet-0474996

[6] SNOWDEN, a EDWARD. *Permanent Record*. 1.vydání. NewYork: Metropolitan Books/Henry Holt and Company, 2019. ISBN 978-0-393-24482-3.

[7] NICK, Saint. *Google CEO* [online]. NYC: Business Insider, 2010 [cit. 2019-11-17]. Dostupné z: https://www.businessinsider.com/eric-schmidt-we-know-where-you-are-we-know-where-youve-been-we-can-more-or-less-know-what-youre-thinking-about-2010-10

[8] NOVIKOV, Pavel. . *Google spies on you. What data does it collect?* [online]. Kypr: Screen lifer, 2019 [cit. 2020-02-06]. Dostupné z: https://screenlifer.com/en/trends/google-spies-on-you-what-data-does-it-collect/

[9] VÁCLAVÍK, Lukáš. *Google vás sleduje, i když to nechcete. Jak ukládání polohy vypnout?* [online]. Praha: cnews, 2018 [cit. 2020-02-06]. Dostupné z: https://www.cnews.cz/google-android-ios-vypnuti-sledovani-navod

[10] *Skutečně Google sleduje polohu uživatelů i poté, co si sledování vypnuli?* [online]. Praha: Lupa, 2018 [cit. 2020-02-06]. Dostupné z: https://www.lupa.cz/clanky/skutecne-google-sleduje-polohu-uzivatelu-i-pote-co-si-sledovani-vypnuli/

[11] DOHERTY, robin. *Why privacy is important, and having "nothing to hide" is irrelevant* [online]. Austrálie: Doherty, 2016 [cit. 2019-12-06]. Dostupné z: https://robindoherty.com/2016/01/06/nothing-to-hide.html

[12] BRIDGES, jennifer. *Top 10 reasons to keep your personal information private* [online]. Redwood city: Reputation defender, 2019 [cit. 2019-11-20]. Dostupné z: https://www.reputationdefender.com/blog/privacy/top-ten-reasons-keep-your-personal-information-private

[13] KONONOW, Piotr. *What is Personal Data Under GDPR - Definitions and Examples* [online]. Gdańsk: dataedo, 2018 [cit. 2019-12-14]. Dostupné z: https://dataedo.com/blog/what-is-personal-data-under-gdpr

[14] PUMPHREY, Clint. *How do advertisers show me custom ads* [online]. Atlanta: HowStuffWorks, 2012 [cit. 2019-12-20]. Dostupné z: https://computer.howstuffworks.com/advertiser-custom-ads.htm> 19 November 2019

[15] WLOSIK, Michal. *What Is a Data Broker and How Does It Work?* [online]. Polsko: Clearcode, b.r. [cit. 2019-11-25]. Dostupné z: https://clearcode.cc/blog/what-is-data-broker/

[16] GONIMAH, diana. *What is doxing* [online]. Londýn: Storyful, 2019 [cit. 2020-02-06]. Dostupné z: https://storyful.com/blog/what-is-doxing/

[17] HENRY, Alan. *What Is "Big Data," and Who's Collecting It?* [online]. New York: LifeHacker, 2014 [cit. 2020-01-07]. Dostupné z: https://lifehacker.com/what-is-big-data-and-whos-collecting-it-1595798695

[18] EDMUN, Annie. *I Don't Think Internet Anonymity Means What You Think It Means* [online]. Alexandria: LIBERTARIANISM, 2018 [cit. 2020-11-19]. Dostupné z: https://www.libertarianism.org/building-tomorrow/i-don%27t-think-internet-anonymity-means-what-you-think-it-means

[19] ATHOW, Desire. *How to become anonymous online* [online]. New York: TechRadar, 2018 [cit. 2020-04-07]. Dostupné z: https://www.techradar.com/how-to/how-to-become-anonymous-online

[20] *Internet Browser Privacy Tips: In-Browser Settings* [online]. USA: TechSafety, 2015 [cit. 2020-04-07]. Dostupné z: https://www.techsafety.org/internetbrowserprivacytips

[21] *17 steps to being completely anonymous online* [online]. USA: CSO, 2018 [cit. 2020-02-06]. Dostupné z: https://www.csoonline.com/article/2975193/9-steps-completely-anonymous-online.html?page=2

[22] GEBHARDT, Patrick. *How to Become Anonymous on the Internet - Part 1/2* [online]. Nürnberg: PAESSLER, 2019 [cit. 2020-02-06]. Dostupné z: https://blog.paessler.com/how-to-become-anonymous-on-the-internet-1

[23] SKERRITT, Brandon. *How does Tor actually work?* [online]. San Francisco & Colorado: Hackernoon, 2019 [cit. 2020-02-06]. Dostupné z: https://hackernoon.com/how-does-tor-really-work-5909b9bd232c

[24] KROHN, David. *Prohlížeč Tor – ucelená příručka prohlížeče Tor 2020* [online]. VpnMentor, 2020 [cit. 2020-02-06]. Dostupné z: https://cs.vpnmentor.com/blog/tor-prohlizec-ucelena-prirucka/

[25] SCHAMBERGER, Pavel. *Způsoby využívání anonymizační sítě Tor*. Praha, 2017.. Diplomová práce. Univerzita Karlova v Praze. Vedoucí práce Mgr. Vít Šisler, PhD.

[26] BOŠKOVIČ, Šimon. *Možnosti komunikace klient-server v TOR sítích*. Zlín, 2018.. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.

[27] KUČERA, Josef. *Soukromí na síti: Jak funguje VPN* [online]. Praha: Univerzita Karlova, 2019 [cit. 2020-02-06]. Dostupné z: https://www.matfyz.cz/clanky/1409-soukromi-na-siti-jak-funguje-vpn

[28] BENNET, John. *What Is a VPN? The Complete Beginner's Guide to VPNs in 2020* [online]. WizCase, 2020 [cit. 2020-02-06]. Dostupné z: https://www.wizcase.com/blog/what-is-a-vpn-a-beginners-guide/

[29] REZEK, Tomáš. *10 nejlepších VPN pro ČR pro rok 2020 dle rychlosti a zabezpečení* [online]. VpnMentor, 2020 [cit. 2020-02-06]. Dostupné z: https://cs.vpnmentor.com/

[30] BUTLER, Sydney. *How to Stay Anonymous Online – 15 Steps To Your Complete Digital Freedom!* [online]. Tamil Nadu: TechNadu, 2018 [cit. 2020-02-06]. Dostupné z: https://www.technadu.com/how-to-stay-anonymous-online/6898/

[31] GEBHARDT, Patrick. PAESSLER. *How to Become Anonymous on the Internet - Part 2/2* [online]. Nürnberg: PAESSLER, 2019 [cit. 2020-02-06]. Dostupné z: https://blog.paessler.com/how-to-become-anonymous-on-the-internet-2

[32] HOFFMAN, chris. *The Many Ways Websites Track You Online* [online]. Potomac Falls: How to geek, 2016 [cit. 2020-02-06]. Dostupné z: https://www.howtogeek.com/115483/htg-explains-learn-how-websites-are-tracking-you-online/

[33] SCHAMBERGER, Pavel. *Anonymita v prostředí internetu*. Praha, 2014.. Bakalářská práce. Univerzita Karlova v Praze. Vedoucí práce Mgr. Vít Šisler, Ph.D.

[34] GRELF, bjorn. *Cookies, Fingerprinting & Co.: Tracking Methods Clearly Explained* [online]. Mnichov: Cliqz, 2018 [cit. 2020-02-06]. Dostupné z: https://cliqz.com/en/magazine/cookies-fingerprinting-co-tracking-methods-clearly-explained

[35] KRČMÁŘ, petr. *Nová metoda fingerprintingu pozná uživatele i po výměně prohlížeče* [online]. Praha: RootCZ, 2017 [cit. 2020-12-08]. Dostupné z: https://www.root.cz/clanky/nova-metoda-fingerprintingu-pozna-uzivatele-i-po-vymene-prohlizece/

[36] HOFFMAN, chris. *What Is a Browser's User Agent?* [online]. Potomac Falls: How to geek, 2017 [cit. 2020-02-06]. Dostupné z: https://www.howtogeek.com/114937/htg-explains-whats-a-browser-user-agent/

[37] CIMPANU, Catalin. *Half of all Google Chrome extensions have fewer than 16 installs* [online]. San Francisco: ZDNet, 2019 [cit. 2020-03-15]. Dostupné z: https://www.zdnet.com/article/half-of-all-google-chrome-extensions-have-fewer-than-16-installs/

[38] *Historie projektu Mozilla* [online]. Mountain View: Mozilla, b.r. [cit. 2020-03-19]. Dostupné z: https://www.mozilla.org/cs/about/history/

[39] NADER, Youssef. *Top 10 Open Source Security Testing Tools for Web Applications* [online]. hackr.io, 2019 [cit. 2020-03-19]. Dostupné z: https://hackr.io/blog/top-10-open-source-security-testing-tools-for-web-applications

[40] *OWASP Foundation* [online]. US: OWASP Foundation, 2019 [cit. 2020-03-19]. Dostupné z: https://www.owasp.org/index.php/Main_Page

[41] JAISWAL, Sarang. *Configuring OWASP ZAP Proxy To Trace Browser Traffic.* [online]. Chicago: Sarang Jaiswal, 2018 [cit. 2020-03-19]. Dostupné z: https://www.sarangjaiswal.com/configuring-owasp-zap-proxy-to-trace-browser-traffic.html

[42] BELMER, Charlie. *How to Detect If a Browser Plugin is Spying On You - A Complete Guide* [online]. USA: NullSweep, 2019 [cit. 2020-03-19]. Dostupné z: https://nullsweep.com/how-to-detect-if-a-browser-plugin-is-spying-on-you/

[43] *Firefox Browser Add-ons* [online]. Mountain View, Kalifornie, USA: Firefox, 2020 [cit. 2020-04-04]. Dostupné z: https://addons.mozilla.org/cs/firefox/

[44] *Internetový obchod chrome* [online]. Mountain View, Kalifornie, USA: Google, 2020 [cit. 2020-04-04]. Dostupné z: https://chrome.google.com/webstore/category/extensions

[45] HENRY, Alan. *Ad-Blocker Ghostery Actually Helps Advertisers, If You "Support" It* [online]. New York: LifeHacker, 2013 [cit. 2020-03-19]. Dostupné z: https://lifehacker.com/ad-blocking-extension-ghostery-actually-sells-data-to-a-514417864

[46] BRUNNER, Grant. *Is it safe to use the Ghostery privacy extension?* [online]. New Castle County, Delaware: ExtremeTech, 2015 [cit. 2020-03-19]. Dostupné z: https://www.extremetech.com/internet/212476-is-it-safe-to-use-the-ghostery-privacy-extension

[47] *Human Web* [online]. Mnichov: Cliqz, 2020 [cit. 2020-04-05]. Dostupné z: https://cliqz.com/en/whycliqz/human-web

[48] OSBOURNE, Charlie. *Adblock Plus filters can be abused to execute malicious code in browsing sessions* [online]. Londýn: ZDNet, 2019 [cit. 2020-03-22]. Dostupné z: https://www.zdnet.com/article/adblock-plus-filters-can-be-abused-by-hackers-to-execute-malware/

[49] *Adblock Plus Privacy Policy — Frequently Asked Questions* [online]. Kolín nad Rýnem: Adblockplus, 2018 [cit. 2020-03-22]. Dostupné z: https://adblockplus.org/faq-privacy

[50] *Privacy policy* [online]. GitHub, 2019 [cit. 2020-03-22]. Dostupné z: https://github.com/gorhill/uBlock/wiki/Privacy-policy

[51] PALANT, Wladimir. *Avast Online Security and Avast Secure Browser are spying on you* [online]. Německo: Palant, 2019 [cit. 2020-03-22]. Dostupné z: https://palant.de/2019/10/28/avast-online-security-and-avast-secure-browser-are-spying-on-you/

[52] HACHMAN, Mark. *Update: Avast kills Jumpshot data-collection business after privacy concerns mount* [online]. PCworld, 2020 [cit. 2020-03-22]. Dostupné z: https://www.pcworld.com/article/3516502/report-avast-and-avg-collect-and-sell-your-personal-info-via-their-free-antivirus-programs.html

[53] MCEVOY, MIKE. *7 Reasons Google Search Results Vary Dramatically* [online]. S. Gadzooks Drive: WEB PRESENCE, 2015 [cit. 2020-04-05]. Dostupné z: https://www.webpresencesolutions.net/7-reasons-google-search-results-vary-dramatically/

[54] KUMAR, Mohit. *Avast and AVG Browser Extensions Spying On Chrome and Firefox Users* [online]. The Hacker News, 2019 [cit. 2020-04-04]. Dostupné z: https://thehackernews.com/2019/12/avast-and-avg-browser-plugins.html

[55] *Citáty slavných osobností* [online]. citaty.net, 2007 [cit. 2020-07-02]. Dostupné z: https://citaty.net/citaty/275857-albert-einstein-proc-nam-skvela-technika-ktera-setri-praci-a-usna/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

VPN Virtuální privátní síť

ZAP Zed Attack Proxy

SEZNAM OBRÁZKŮ

SEZNAM TABULEK