Kyberkriminalita

Petr Klučka

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

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

Jméno a příjmení:	**Petr Klučka**
Osobní číslo:	**A14246**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Kyberkriminalita**
Téma anglicky:	**Cybercrime**

Zásady pro vypracování:

1. **Proveďte rešerši na téma kyberkriminality.**
2. **Popište nejčastější techniky kyberkriminality používané v současnosti.**
3. **V praktické části popište možnosti obrany proti kyberútokům.**
4. **Otestujte navržené zabezpečení počítače proti vybraným technikám kybernetických útoků.**
5. **Vyhodnoťte a okomentujte dosažené výsledky.**

Rozsah bakalářské práce: -

Rozsah příloh:

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

Seznam odborné literatury:

1. **SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN: 978-80-7380-501-2**
2. **ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017, ix, 135. Právní monografie. ISBN 978-80-7552-758-5.**
3. **KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.**
4. **GŘIVNA Tomáš, POLČÁK Radim. Kyberkriminalita a právo. Vyd. 1. Editor Tomáš GŘIVNA, editor Radim POLČÁK. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.**
5. **MARTÍNEK, Zdeněk. Agresivita a kriminalita školní mládeže. 2., aktualizované a rozšířené vydání. Praha: Grada, 2015, 190 s. Pedagogika. ISBN 978-80-247-5309-6.**

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

Datum zadání bakalářské práce: **27. července 2018**

Termín odevzdání bakalářské práce: **28. srpna 2018**

Ve Zlíně dne 27. července 2018

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

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

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 27.8.2018 Petr Klučka, v.r.

ABSTRAKT

Cílem této bakalářské práce je zmapování kybernetických útoků v minulosti a také trendů kyberkriminality v současnosti. Jsou v ní popsány klíčové pojmy vztahující se k problematice kyberkriminality. Tato práce rovněž informuje o tom, co mohou uživatelé udělat proto, aby tomuto nebezpečí předcházeli.

Teoretická část této bakalářské práce začíná úvodem do problematiky historií kyberkriminality, a definicí pojmu kyberprostor. Následně se zabývá pachateli kyberkriminálních zločinů, vznikem pojmu hacker, hackerskou etikou, a klasifikací hackerů. Podrobně se také věnuje popisu kyberkriminálních technik jako sociální inženýrství, phishing, pharming, a další, a zabývá se tím, na co by si uživatelé měli dát pozor, aby poznali, zda se jedná o phishing nebo pharming. Je zde také zmíněno co je to hoax, jak fungují programy keylogger a backdoor. V závěru teoretické části této práce jsou uvedeny specifické příklady kyberkriminality, konkrétně kyberšikana, kyberstalking, kybergrooming a krádež identity. Řešena je také prevence proti kyberšikaně, jak se mohou chovat oběti nebo pachatelé kyberšikany, a co dělat, když se s ní uživatelé setkají.

Cílem praktické části této bakalářské práce je definovat způsoby, jakými se lze bránit proti v teoretické části zmíněným kyberkriminálním technikám, otestovat nástroje obrany, důležitost dobře zvolených hesel, a funkčnost mechanizmů, které mohou být použity k dodatečnému zabezpečení proti těmto útokům.

Klíčová slova: útok hrubou silou, odposlech komunikace, keylogger, phishing, pharming, VPN

ABSTRACT

The aim of this bachelor thesis is to map cyber attacks in the past as well as current cybercrime trends. It describes the key concepts related to cybercrime issues. This work also explains what users can do to prevent this danger.

The theoretical part of this bachelor thesis starts with an introduction to the problems of cybercrime history and the definition of cyberspace. Subsequently, it deals with cybercrime offenders, the origin of the term hacker, hacker ethics, and hacker classifications. It also deals extensively with the description of cybercrime techniques, such as social engineering, phishing, pharming, and others, and with what users should be careful about to see if phishing or pharming is to be suspected.

There is also mentioned what a hoax is, and how keylogger and backdoor programs work. At the end of the theoretical part of this paper specific examples of cybercriminality are given, namely cyberbullying, cyberstalking, cybergrooming and identity theft. What is also addressed is cyberbullying prevention, behaviour of cyberbullies and victims, and what to do in these situations.

The aim of the practical part of this bachelor thesis is to define the ways in which it is possible to defend against the cybercrime techniques described in the theoretical part, to test how the attacks work, the importance of well-chosen passwords, and the functionality of the mechanisms that can be used to provide additional security against these attacks.

Keywords: brute force, sniffing, keylogger, phishing, pharming, VPN

Děkuji vedoucímu své bakalářské práce panu doc. Ing. Jiřímu Vojtěškovi, Ph.D. za jeho vstřícnost, cenné rady, připomínky a metodické vedení práce.

Dále bych chtěl poděkovat panu Ing. Davidu Malaníkovi, Ph.D. za doplňující konzultace a odborné nasměrování mé práce.

Chci poděkovat také své rodině za neutuchající podporu během mého studia.

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

OBSAH

ÚVOD

Problematika kybernetické kriminality je v dnešní době více než aktuální, a její význam roste společně s rozvojem informačních technologií – čím více se budou zdokonalovat informační technologie, tím více poroste i důležitost znalosti problematiky kybernetické kriminality.

První kapitola teoretické části této bakalářské práce pojednává o historii kyberkriminality, kdy byl poprvé použit tento pojem, o vývoji tohoto pojmu a jeho definicích – obecných i specifických pro určité organizace. Dále pojednává o právních normách upravujících problematiku kyberkriminality. Na konci první kapitoly je definován pojem kyberprostor. Druhá kapitola se zabývá pachateli kyberkriminálních zločinů, vznikem pojmu hacker, hackerskou etikou, a klasifikací hackerů. Ve třetí kapitole jsou definovány kyberkriminální techniky jako sociální inženýrství, phishing, pharming, a další. V poslední kapitole teoretické části této práce jsou uvedeny specifické případy kyberkriminality, konkrétně kyberšikana, kyberstalking, kybergrooming a krádež identity.

Cílem praktické části této bakalářské práce je definovat způsoby, jakými se bránit v teoretické části zmíněným kyberkriminálním technikám. Tyto způsoby jsou následně otestovány a z hlediska efektivity jsou zhodnoceny jednotlivé postupy obrany proti kybernetickým útokům.

Tato práce si klade za cíl informovat o nebezpečí kyberkriminality, seznámit uživatele s teoretickými poznatky, které by jim umožnily uvědomit si přítomnost hrozby těchto útoků, a ukázat jim, jak je tomuto nebezpečí možné předcházet použitím odpovídajících bezpečnostních prostředků.

V závěru této bakalářské práce jsou shrnuty teoretické poznatky a analyzovány dosažené výsledky z praktických simulací fungování bezpečnostních prostředků.

I. TEORETICKÁ ČÁST

1 KYBERKRIMINALITA

V osmdesátých letech minulého století se zdálo, že největším přínosem pro rozvoj elektroniky a mikroprocesorů bude osobní počítač. Proto se jakémukoliv zneužití tohoto osobního počítače začalo říkat počítačová kriminalita. Ale pojmenování kriminálního činu podle použitého prostředku bylo neobvyklé, a proto byl zaveden termín kriminalita spojená s počítači, který měl zahrnovat všechny trestné činy, ve kterých počítač figuruje jako nástroj nebo předmět použitý při trestném činu. Ke spáchání takových trestných činů však bylo zapotřebí mít znalosti z výpočetní techniky nebo informatiky, a proto bylo navrženo slovní spojení kriminalita v informatice. [1], [2]

Následný rozvoj elektroniky a mikroprocesorů vedl ke vzniku dalších zařízení (např. mobilní telefony, tablety). Společným jmenovatelem takových zařízení se stala data a komunikační síť, kterou tvoří terminálová zařízení jako servery a směrovače. Díky tomu se zavedl pojem kriminalita informačně-komunikačních technologií. Dnes je nejznámější komunikační sítí internet, který poskytuje různé způsoby komunikace a služby. V důsledku toho vzniklo hned několik označení pro trestné činy spáchané na internetu – internetová kriminalita, e-kriminalita, virtuální kriminalita nebo kriminalita na počítačových sítích. [3], [4]

V roce 2001 vznikla tzv. Úmluva o počítačové kriminalitě, která je považována za první mezinárodní právní akt v oblasti kybernetické bezpečnosti. Právě v této úmluvě se poprvé objevuje slovní spojení kyberkriminalita. Tento pojem je ale nedostačující, a proto se společně s ním používá pojem kriminalita high-tech. Pojem kriminalita high-tech dává prostor pro přidání nových technologií. Důsledkem vzniku nových možností ve využívání informačních a komunikačních technologií rostou i možnosti jejich zneužívání. Proto neexistuje univerzální definice, která by zcela vysvětlovala pojem kyberkriminalita, teoreticky ani legislativně. [3], [4]

Jsou však organizace, které se o to snaží – v následující kapitole jsou uvedeny některé definice, se kterými tyto organizace přišly.

Nejvíce obecná definice definuje kyberkriminalitu jako jednání, které je namířeno proti počítači, počítačovým sítím, nebo když je počítač použit jako nástroj pro spáchání trestného činu. Zásadní podmínkou pro použití této definice je, že se spáchání trestného činu odehrává v kyberprostoru. Pro definování kybernetické kriminality je rovněž důležité vymezit pojem kriminalita jako takový, protože v souvislosti s ICT dochází k řadě jednání, která jsou

nežádoucí, ale nepovažují se za trestný čin, i když mohou být pro společnost nebezpečná. Jednání, která nemohou být kvalifikována jako kyberkriminalita nebo jakákoliv jiná kriminalita, se za kriminalitu nepovažují. Pokud definujeme pojem kriminalita, vycházíme z definice, že kriminalita je souhrn všech jednání, která se dají zařadit pod skutkovou podstatu upravenou zákonem. Podle zmíněné definice se jednání, která se nedají zařadit pod žádnou skutkovou podstatu upravenou zákonem, nepovažují za kriminalitu. [4], [5]

Bohužel v oblasti ICT jsou většinou tato jednání využívána ke spáchání trestných činů. Tato jednání jsou zároveň důležitou součástí v procesu odhalování a objasňování trestné činnosti.

Kybernetická kriminalita představuje jakýsi souhrn všech trestných činů, ke kterým dochází v prostředí ICT. Tento souhrn je dále možné rozdělit na podmnožiny, které se mohou označovat pojmy jako „internetová kriminalita“, „e-kriminalita“, či „pirátství“. V odborných publikacích bývá kyberkriminalita označena jako jednání, při kterém jsou ICT prostředky použity jako nástroj ke spáchání trestného činu, nebo jsou tyto prostředky cílem útoku. [4], [5]

V dnešní době ale tato definice není dostatečná, protože by zahrnovala i trestné činy, ve kterých sice byly ICT prostředky použity, ale ne činnosti, ke kterým byly určeny. Například použití části počítače jako zbraně. [4], [5]

Aby tedy bylo možné hovořit výhradně o kybernetické kriminalitě, je třeba k výše uvedené definici přidat podmínku, že ICT prostředky, které byly použity k trestnému činu, byly použity v informačním, systémovém, programovém či komunikačním prostředí, jinými slovy byly použity v kyberprostoru. [4], [5]

Ale i toto vymezení není dostačující, protože by to znamenalo, že podle § 24 zákona č. 40/2009 Sb., trestního zákoníku je možné spáchat každý trestný čin za pomoci ICT (např. útočník přiměje pomocí e-mailových zpráv někoho jiného spáchat trestný čin). Toto jednání se však nedá považovat za kyberkriminalitu. Pokud by se taková jednání za kyberkriminalitu považovala, pak by nastala situace, že každý trestný čin, při kterém byly použity prostředky ICT, se dá označit jako počítačová kriminalita. [4], [5]

Z toho vyplývá, že kyberkriminalitu nelze vymezit pouze pozitivně, to znamená, vymezit jednání, která se považují za kyberkriminalitu, ale musíme ji vymezit i negativně, čili jaká jednání za kyberkriminalitu považovat nelze. [4] [5]

1.1 Klasifikace forem kyberkriminality

Obecně lze kyberkriminalitu klasifikovat jako jednání, které je namířeno proti počítači, počítačovým sítím, nebo v případech, kdy je počítač použit jako nástroj pro spáchání trestného činu. V této kapitole je ukázáno, jak pojem kyberkriminalita vnímají různé právní normy a organizace, které se zabývají bojem s kybernetickou kriminalitou.

1.1.1 Klasifikace podle komise Rady Evropy pro zločin v kyberprostoru

Komise expertů z Rady Evropy pro zločin v kyberprostoru (Commitee of Experts on Crime in Cyberspace) se v roce 2000 rozhodla kyberkriminalitu rozdělit do dvou bodů. V prvním bodě se posuzuje, v jaké pozici se nachází počítač při páchání trestné činnosti, jestli je v pozici cíle, proti kterému je směřována trestná činnost, nebo se použije jako nástroj k páchání trestné činnosti. Ve druhém bodě se posuzují typy trestných činů – tyto se rozdělují na tradiční a nové. Do tradičních trestných činů patří takové trestné činy, které lze spáchat i bez použití počítače, např. padělání bankovek. Za nové trestné činy se považují takové trestné činy, které nelze spáchat bez použití počítače, např. útoky DDoS. [5]

1.1.2 Klasifikace podle iniciativy eEuropa+

Akční plán eEuropa+ rozděluje kyberkriminální zločiny do čtyř kategorií. Do první kategorie patří zločiny tykající se porušování soukromí, konkrétně sem patří nelegální sběr, uchovávání, modifikace a zveřejňování osobních dat. Druhá kategorie se zaměřuje na obsah počítače, hlavně na pornografii, rasismus, vyzývání k násilí aj. Třetí kategorie zahrnuje všechny ekonomické zločiny od počítačových podvodů, počítačové špionáže, až po sabotáže a hackerství. Do poslední kategorie patří zločiny týkající se duševního vlastnictví, např. počítačové pirátství. [5]

1.2 Kyberprostor

Kyberprostor je jedním z klíčových prvků v definici kybernetické kriminality. Než bude řešena definice kyberprostoru, je nutné se také zmínit o pojmu internet, který s kyberprostorem bezprostředně souvisí.

Internet začal vznikat v 50. letech 20. století, kdy se začalo s testováním sítí propojených počítačů, hlavně pro vědeckovýzkumné a vojenské účely. Ačkoliv se internet vyvíjel na základě sítí, které měly vlastníka, dnes neexistuje centrální autorita, která by spravovala celý internet. Hmotnou podstatou internetu je síť, která vede data vzduchem,

kabely a jinými přenosovými médii. Technicky je internet celosvětová síť, která je složena z menších sítí, které spolu vzájemně komunikují, vyměňují si informace a poskytují si služby mezi sebou. [5], [6]

Takto vzniká neustále se měnící a vyvíjející se systém závislý na hardwaru, ale zároveň vytváří špatně definovatelný a prakticky neomezený kyberprostor. Tento prostor je možné popsat jako virtuální realitu, která nemá začátek ani konec, ale je kompletně závislá na materiální podstatě internetu, konkrétně na technologiích, které jsou v reálném světě. Tím vzniká paradox, který umožňuje existenci nehmotného média (kyberprostoru), které je schopné se v případě poškození jednotlivých materiálních prvků (prvky sítě, jednotlivé počítačové systémy aj.) adaptovat a měnit, ale v případě úplného kolapsu všech materiálních prvků, dochází k nevratnému poškození či úplnému zničení kyberprostoru jako takového. [5]

Jako legální definici lze použít znění § 2 písm. a) ZKB, kde se uvádí, že „kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací.“ [5]

2 PACHATELÉ KYBERKRIMINALITY

Pachatelem kyberkriminálních zločinů může být v podstatě kdokoliv. Není podmínkou, že musí mít rozsáhlé počítačové znalosti. Například u zločinů jako kyberšikana, krádež identity a jiné, stačí mít jen velmi základní znalosti. Proto nerozhoduje věk, pohlaví nebo vzhled. Z tohoto důvodu může být pachatelem opravdu každý. U trestných činů, kde jsou tyto znalosti nutností, se pachatel označuje pojmem hacker.

2.1 Hacker

Termín hacker začali používat studenti MIT, kde vznikl první moderní počítač. Od té doby se tento pojem používá k označení pachatele kyberkriminálních zločinů. Tento pojem však z počátku neměl nic společného s trestnou činností. Označoval technicky nadanou osobu, která je schopná řešit problémy novou a nestandardní cestou. V dnešní době hackerská komunita používá pojem hacker pro označení osob s výbornými znalostmi o fungování informačních, komunikačních a počítačových systémů, jejich principů a mechanismů, a zároveň jsou tito i špičkovými programátory. Jejich motivací a filozofií je poznání, jak tyto systémy fungují a předání těchto informací jiným uživatelům. Z toho vychází i schopnost hackera získat si přístup do těchto systémů nestandardním způsobem. To ale neznamená, že takto získaný přístup použije ke způsobení škody danému systému, tato dovednost je pouze jednou z mnoha. [3], [5]

2.1.1 Hackerská etika

Už v roce 1984 byly poprvé definovány základní principy hackerské etiky, ve kterých by měl být přístup k věcem, které nás mohou něco naučit o světě a jeho fungování, neomezený a absolutní. Všechny informace, ke kterým máme přístup, by měly být zdarma. Nevěřit autoritám, které se tyto informace snaží omezovat nebo odstraňovat, společně s tím podporovat decentralizaci. Hackeři by se neměli soudit podle nic neříkajících kritérií, jako jsou rasa či věk, ale měli by se soudit podle svých činů. Počítače by měly být použity ke změně našeho života k lepšímu.

Bohužel, ne vždy jsou tyto principy respektovány, představují však základní vnímání virtuálního světa hackery. [5], [7]

2.1.2 Rozdělení hackerů

O rozdělení hackerů rozhoduje jejich motivace získání nestandardního přístupu do systému a následně, co udělají se získanými daty. Podle těchto kritérií se dělí do tří skupin.

1) White Hats

   Motivací pro tyto hackery je hledat slabiny, kterými je možné získat přístup do systému a následně tyto slabiny opravit. Často pracují, nebo spolupracují se známými firmami v oboru informačních technologií. [5], [8]

2) Black Hats

   Jejich motivace je přesným opakem White Hats. Taktéž hledají slabiny, kterými se lze dostat do systému, ale na rozdíl od White Hats to dělají s úmyslem daný systém poškodit, nebo se na něm obohatit. [5], [8]

3) Grey Hats

   Jsou to hackeři, kteří nespadají pod výše uvedené kategorie. Někdy svou činností poruší zákon, nebo morální principy, ale jejich činnosti nejsou primárně zaměřeny na porušování zákonů. [5], [8]

3 KYBERKRIMINÁLNÍ TECHNIKY

Útočník často používá pro úspěšné dosažení svých cílů různé specifické techniky a postupy, které se označují jako kybernetický útok. Nejznámější metody způsobu hackerské práce jsou popsány v následujících kapitolách.

3.1 Sociální inženýrství

Sociální inženýrství jako takové nelze považovat za kybernetický útok, často je však základem pro uskutečnění jiných útoků.

Tento pojem by se dal definovat jako manipulace, ovlivnění či přesvědčování lidí. Cílem je donutit lidi k určité akci, nebo z nich dostat určité informace, které by za normálních okolností nikomu neprozradili. Dalo by se říci, že jde o „umění klamu“. [5], [9]

Hlavním znakem sociálního inženýrství je, že nejsou použity technické postupy či nástroje. Například pro získání hesla je jednodušší dotyčného přesvědčit, aby nám heslo sám prozradil, protože nejslabším článkem v systému bude vždy člověk. Na světě neexistuje počítačový systém, který by byl kompletně nezávislý na člověku (ať už se jedná o zprovoznění, nastavení, či údržbu počítačového systému), tedy je nejjednodušší získat potřebné informace právě od člověka. Sociální inženýrství se poprvé dostalo do povědomí lidí díky případu Kevina Mitnicka. [5], [9]

3.2 Útok hrubou silou (Brute force)

Útok hrubou silou spočívá v tom, že se útočník snaží zjistit uživatelské jméno a heslo, nebo pouze heslo, pomocí kombinace různých znaků. Dělá to tak, že si zvolí počet znaků, neboli jak dlouhé dané heslo pravděpodobně bude, jejich typ (písmena, číslice, atd.), a pak provádí jejich kombinace. Následně pak zkouší, jestli některý výsledek neodpovídá parametrům hesla. [10], [11]

Do této kategorie spadá i tzv. slovníkový útok. V něm jsou už předem definována nějaká slova a útočník jen zkouší, jestli odpovídají heslu, které chce prolomit.

Tyto metody jsou ale velmi neefektivní. Například pokud jsou vybrány z tabulky ASCII (tabulka znaků používaných v informatice) pouze malá písmena, těch je 26. Pokud bude mít heslo jedno písmeno, lze z něj vytvořit 27 kombinací, jestliže má dvě písmena, heslo může mít 27x27 kombinací, u tří 27x27x27, atd. Pokud je zvolena standardní délka hesla osm

znaků, celkové množství kombinací je asi 282 miliard. Takže je šance 1:282 miliardám, že toto heslo útočník prolomí pomocí útoku hrubou silou. A toto jsou pouze malá písmena. Pokud jsou přidána velká písmena, číslice a speciální znaky, bude šance ještě menší. Pokud si ovšem uživatel zvolí heslo typu 1234, 0000, jméno svého psa, nebo je heslo stejné jako uživatelské jméno apod., je velká pravděpodobnost, že toto heslo útočník prolomí. [10], [11]

Nejlepší možnost, jak se bránit takovým útokům, je vytvořit silné heslo, které by mělo mít alespoň osm znaků a tyto znaky by se měly skládat z kombinace malých a velkých písmen, číslic a speciálních znaků, a písmena by neměla tvořit srozumitelné slovo. [10], [11]

3.3 Odposlech datové komunikace (Sniffing)

V češtině sniffing znamená čenichat nebo čmuchat. V podstatě to znamená, že uživateli někdo odposlouchává komunikaci na síťové kartě a hledá nezašifrovaná data jako uživatelská jména a hesla, aby mohl získat přístup do systému.

3.3.1 Packetový sniffer

Někdy se mu říká síťový analyzátor. Existují softwarové nástroje používané správci sítí k odhalení problémů v dané síti. Bohužel mohou být také použity hackery pro sledování provozu na uživatelově síti a hledání nezašifrovaných hesel. Běžně tento software zachycuje jen data určená pro konkrétní počítač, ale pokud uživatel síťovou kartu přepne do tzv. promiskuitního režimu, může zachycovat všechna data, která projdou přes jeho počítač. Jména a hesla se v dané síti přenášejí pomocí textu, to znamená, že analýzou správných paketů se k nim lze dostat. [12], [13]

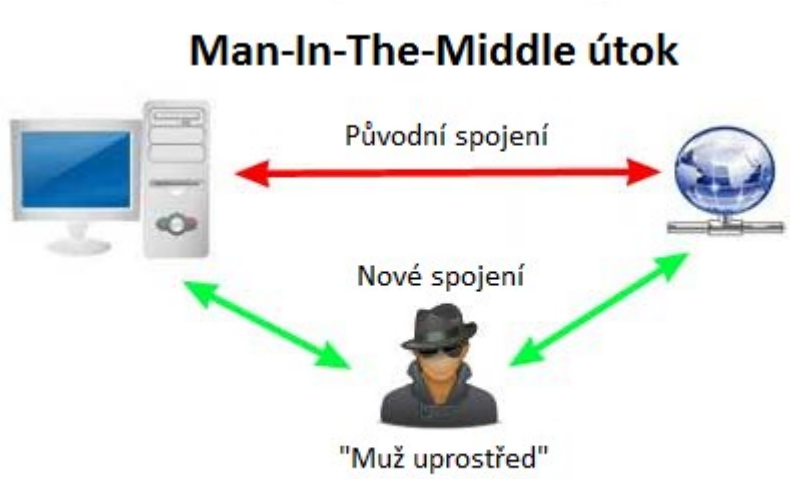
Toto odposlouchávání ale funguje jen v dané podsíti, není možné, aby si uživatel takový software pustil doma a zachytil komunikaci, která probíhá v jeho zaměstnání. Jsou sice možnosti jak to provést, ale v běžných podmínkách je to nemožné. [12], [13]

Zjištění těchto síťových analyzátorů v uživatelově síti je téměř nemožné, protože tyto softwarové systémy jsou pasivní. Tzn., že pouze zachytávají pakety, které protékají sítí uživatele, takže nezanechávají žádné známky své aktivity. Jediné, co může uživatel zjistit v jeho síti je, jestli nějaká síťová karta běží v promiskuitním režimu. Pokud má v síti takové zařízení je možné, že dané zařízení používá již zmíněný software. [12], [13]

Bohužel běžný uživatel nemá možnost se proti tomuto útoku bránit, lze pouze šifrovat danou komunikaci, aby i když jej útočníci odposlouchávají, nemohli nic zjistit. [12], [13]

3.3.2 „Muž uprostřed“ (Man-In-the-Middle)

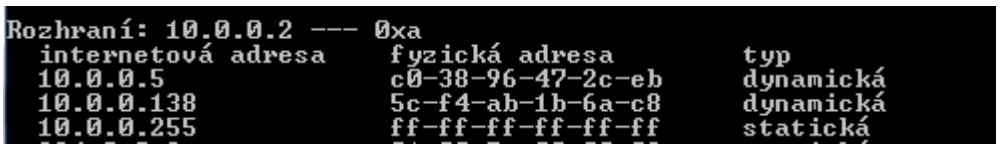
Princip spočívá v tom, že se mezi příjemce a odesílatele dostane někdo třetí, o kterém příjemce ani odesílatel neví, a může odposlouchávat jejich komunikaci, nebo ji i měnit. V případě jednoduché sítě, kde jsou počítače propojené jedním kabelem, v takové situaci může útočník kabely narušit a připojit do sítě vlastní zařízení. Dnes už žádné kabely narušovat nemusí, stačí být na stejné síti a pomocí ARP poisoning může prvky sítě donutit, aby mu data posílaly samy. Zmíněný útok je zobrazen na níže uvedeném obrázku. [14], [15]



Obrázek 1 Man in the middle schéma [17]

3.3.3 ARP poisoning

Aby bylo možné definovat ARP poisoning, nejdříve je nutné uvést definici protokolu ARP a k čemu slouží. ARP protokol slouží k nalezení fyzické adresy (MAC adresy) počítače pomocí jeho IP adresy. Stručně řečeno, odesílatel chce odeslat paket, má IP adresu 10.0.0.1, a chce ji odeslat příjemci na adresu 10.0.0.2, ale nezná fyzickou adresu. Proto pošle dotaz na broadcast [18] a ptá se, kdo zná fyzickou adresu počítače s IP 10.0.0.2. A dostane odpověď, že k IP 10.0.0.2 patří CD:CD:CD:CD:CD:CD a aby se nemusel pokaždé ptát znovu, tak si tuto adresu uloží do tzv. ARP cache. Tato ARP cache má podobu tabulky, kde je IP adrese přiřazena fyzická adresa. [14], [15]



Obrázek 2 ARP tabulka

ARP protokol ale neobsahuje žádný bezpečnostní prvek, pokud by tedy místo příjemce odpověděl útočník, bude dostávat všechna data určená adrese 10.0.0.2. Čili útočník vymění fyzickou adresu příjemce za tu svoji. [14], [15]

3.3.4 Přímé odposlouchávání

Síťový analyzátor nemusí působit jen mezi dvěma počítači, ale i lokálně. Aby takový software fungoval, musí být nainstalován přímo na počítači, kde buď data ukládá, nebo je rovnou odesílá útočníkovi. Tento program buď do počítače nainstaloval útočník, nebo si jej do počítače stáhl a nainstaloval uživatel sám. Uživatel se může bránit tak, že bude aktualizovat systém, a používat antivirus, popřípadě spyware – například SpyBot Search & Destroy, který je zdarma ke stažení. [14], [16]

3.4 Zadní vrátka (Backdoor)

Zadní vrátka je metoda, které se vyhýbá standardním autentizačním systémům v daném zařízení a umožňuje útočníkovi převzít kontrolu nad počítačem, aniž si jeho majitel něčeho všimne. Jakmile se útočníkovi podaří obejít autentizační systémy, může si dělat v podstatě cokoliv. V horším případě se takový počítač stává jednou z mnoha tzv. „zombie“ v síti botnetu. V takovém případě pak slouží k DDoS útokům, rozesílání hoaxů nebo spamů. [19], [20]

Zadní vrátka v systému může vytvořit například virus trojský kůň, ale jsou toho schopny i jiné druhy malwaru. Konkrétně určité druhy tzv. červů. [19], [20]

3.5 Keylogger

Jedná se o program, který zachycuje všechno, co uživatel napíše na klávesnici a ukládá to do textového souboru. Ten pak posílá útočníkovi, který ze souboru zjistí heslo do internetového bankovnictví, na sociální sítě, e-mailovou schránku apod.. Nositelem takového programu je obvykle trojský kůň. [21], [22]

Bohužel běžný uživatel nepozná, jestli na jeho počítači běží takový program, takže nejlepší ochranou pro běžného uživatele jsou antispywarové programy, které umí tento program vyhledat a zneškodnit. [21], [22]

3.6 Hoax

Jako hoax se označuje zpráva, která je mystifikující a nepravdivá. Nejčastěji se šíří formou e-mailu, ve kterém před něčím varuje, nebo řeší nějaký problém. Typickým znakem takové zprávy je, že vyzývá, aby byla zaslána dalším uživatelům. Proto hoax patří pod určitou složku spamu (uživatelem nevyžádanou poštu). [23]

Proč někdo hoaxy vůbec vytváří? Důvody mohou být různé, například vyvolat strach, manipulovat názory lidí, poškodit konkrétní instituci, značku, firmu, výrobek, vylákat peníze, nebo si prostě udělat legraci z důvěřivých uživatelů. [24], [25]

Jak se bránit takovým zprávám? Nevěřit hned všemu, co se na internetu objeví. Každou informaci bychom si měli pečlivě prověřit. Ale některé hoaxy jsou maskované tak, že své tvrzení podpoří nějakými dodatečnými informacemi. Například informací o času, místě, osobě, nebo uměle vytvořeným obrázkem. A proto je někdy velice těžké poznat, jestli je daná zpráva hoax nebo ne. Na internetu lze najít seznam hoaxů, například na stránce www.hoax.cz, kde je možné si ověřit, jestli je daná zpráva hoax, a pokud ano, bez obav ji lze smazat. [24], [25]

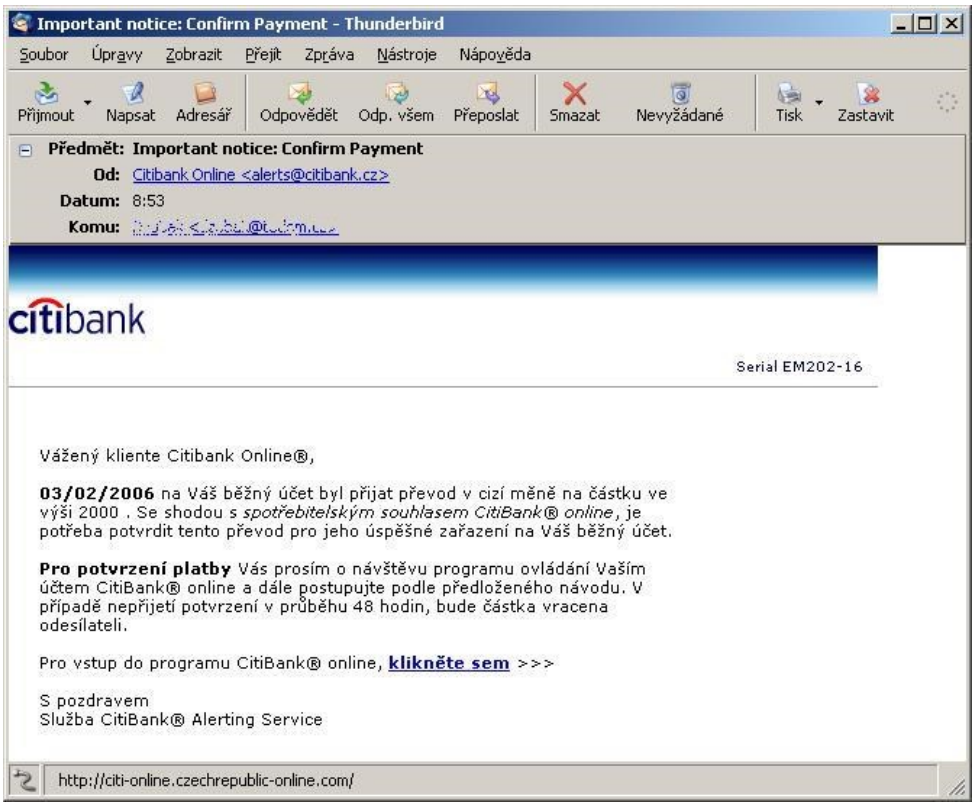
V čem jsou takové zprávy nebezpečné? V nejhorším případě, pokud zprávě uživatel uvěří, se na něm může daná osoba obohatit. Pokud se uživatel v takové situaci ocitne, je nejlepším řešením obrátit se na Policii ČR. V tom lepším případě utrpí jen jeho pověst. [24]

3.7 Rybaření (Phishing)

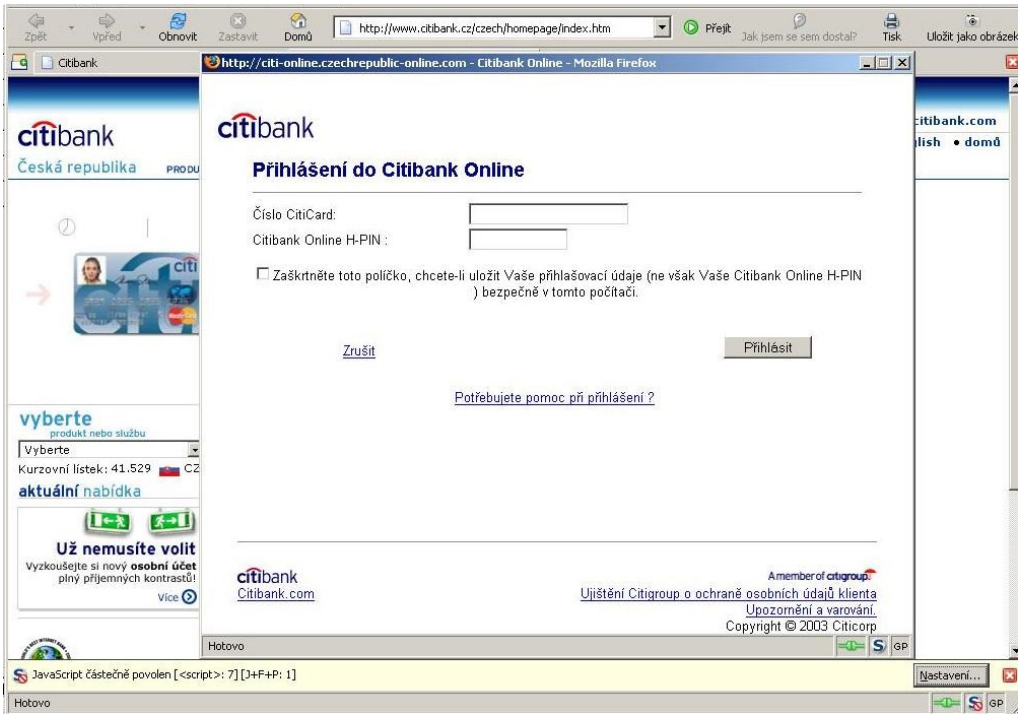
Rybaření spočívá v tom, že útočník odešle podvodný e-mail za účelem vylákání citlivých údajů od nezkušených uživatelů. Poté, co tento e-mail odešle, už jen čeká, až se někdo chytí, jako rybář na rybu. Samotný e-mail budí dojem, že pochází z důvěryhodného zdroje, například z internetového obchodu, banky nebo od policie. V sobě pak má obsažen odkaz, který uživatele přesměruje na stránky útočníka, kde po něm vyžaduje zadání přihlašovacích údajů do internetového bankovnictví nebo PINu a čísla platební karty. [26], [28]

Jak se bránit? Pokud uživatel obdrží podobný e-mail, zcela určitě se jedná o pokus z něj vylákat jeho údaje, protože banky takové e-maily neposílají a nemají takové informace proč požadovat. Pokud se v něm nacházejí nějaké odkazy, nedoporučuje se na ně klikat – mohou obsahovat virus a ten se v případě kliknutí nainstaluje do počítače. [27], [28]

První případ takovéhoto útoku v ČR se stal v roce 2006, konkrétně podniku Citibank.



Obrázek 3 Podvodný e-mail [29]



Obrázek 4 Podvodné přihlašovací okno [29]

Po kliknutí na odkaz v Obrázku 3 se sice uživatel dostane na skutečné stránky společnosti Citibank, ale zároveň se otevře i okno, které vyžaduje zadání důvěrných informací, jak lze vidět na Obrázku 4.

Pokud by uživatel údaje do takového okna zadal, útočníci by získali neomezený přístup do jeho bankovnictví.

3.8 Farmaření (Pharming)

Jedná se o novější podobu phishingu. Už nepoužívá podvodné e-maily, ale rovnou napadne systém DNS, ve kterém přepíše IP adresu dané stránky, takže když se poté chce uživatel přihlásit například do banky, tak jej DNS přesměruje na stránky útočníka. Tato stránka může vypadat stejně jako ta, na které se přihlašuje normálně, pokud ale na této stránce zadá přihlašovací údaje, tak útočník získá plný přístup k jeho informacím. [30], [32]

Takové podvodné stránky lze poznat například tak, že po uživateli chtějí zadat předtím nevyžadované údaje. Jestliže toto uživatel zpozoruje, pak by měl okamžitě operaci ukončit a kontaktovat klientské centrum své banky. [31], [32]

3.9 Distribuované odmítnutí služby (DDoS)

Podstatou DoS a DDoS útoků je znemožnit přístup na server oprávněným uživatelům. To provedou tak, že server zaplní žádostmi o přístup, buď do systému, nebo na stránku. Takové zaplnění informacemi způsobí, že server zkolabuje nebo přestane pracovat, protože nedokáže na tolik žádostí odpovědět. Jsou i jiné typy DoS útoků, ale všem jde o totéž – zabránit oprávněným uživatelům v přístupu do systému nebo na nějakou stránku. [33], [34]

DoS útoky jsou prováděny jen z jednoho zařízení, v dnešní době se už téměř nepoužívají. Nahradily je útoky DDoS, které k útoku používají stovky i tisíce zařízení. Tyto zařízení neútočí za sebe, ale jsou součástí tzv. botnetu (někdy se používá i termín „zombie army“). Zařízení v botnetu většinou nepatří útočníkům, ale byly napadeny a útočníci je jen využívají. [33], [34]

Důvodů, proč někdo uskutečňuje tyto útoky, je hned několik. Například v roce 2011 skupina Anonymous zaútočila na stránky společností PayPal, Visa a MasterCard, aby vyjádřila svou nespokojenost. Zaútočila na ně, protože dané společnosti odmítly zpracovat platby určené pro stránku https://wikileaks.org/. V roce 2013 spameři údajně zaútočili na stránku Spamhouse (stránka, která se zabývá bojem proti spamu) jako odvetu za přidání

společnosti Cyberbunker na spam blacklist (seznam, který společnost Spamhouse poskytuje poskytovatelům e-mailových služeb, aby mohli lépe filtrovat spam). Spamhouse oznámil, že až 75 gbps zahltilo jejich servery. Ani prostředí online her se tomuto fenoménu nevyhnulo. Je spousta lidí, kteří se nechají najmout a vyřadí takto stránky konkurence. Nebo někdo provede útok z politických důvodů. Jiný zase použije tyto útoky jako prostředek k vydírání – pokud nezaplatíte, tak zaútočíme na vaše stránky. Jedním z důvodů je i odvedení pozornosti. Jedna skupina zaútočí DDoS útokem a druhá zaútočí na jiném místě za účelem krádeže citlivých dat. Tyto útoky se ale nevztahují jen na počítače, za oběť jim mohou padnout i telefony nebo telefonní systémy. [33], [34]

3.10 Botnet

Botnet můžeme definovat jako síť botů propojenou pomocí softwaru. Tato síť následně provádí činnosti na základě instrukcí „vlastníka“ této sítě, které můžou být legální (např. distribuované výpočty) nebo nelegální. [5], [35]

Distribuované výpočty bohužel přispěly k vytvoření botnetů tak jak je známe dnes. Princip distribuovaných výpočtů spočívá ve využití velkého množství počítačů s malým výkonem k počítání velmi složitých úloh (např. matematických algoritmů). Tento postup je mnohem efektivnější než použití jednoho „superpočítače“. Tato úloha se rozdělí na velký počet malých částí, které se odešlou všem počítačům, které pracují na dané úloze, a až se dané části zpracují, počítače je odešlou do centra řízení dané úlohy, kde se opět spojí v jeden celek. [5], [35]

Lidé jsou však vynalézaví a někteří si všimli, že se tohoto výkonu, který není geograficky vázán, dá využít i jinak (např. útok DDoS).

Když se jim podaří infikovat cílový počítačový systém, tento systém, kterému se říká „zombie“ nebo „bot“, se připojí k centrálnímu řídícímu serveru, který se označuje jako „Command-and-control server“ (C&C). Útočník (často označován jako botmaster či botherder) následně kontroluje a řídí celý systém pomocí C&C serveru. [5], [35]

Aby mohl být systém označen za botnet musí mít následující prvky:

1. **Command-and-control infrastructure (C&C)**
   Musí mít infrastrukturu skládající se z řídícího prvku (či prvků) a botů (ovladatelných počítačových systémů).

2. **Instalace a ovládání botu**

   Jedná se o program, který je šířen do jiných počítačových systémů s úmyslem připojit je do botnetu.

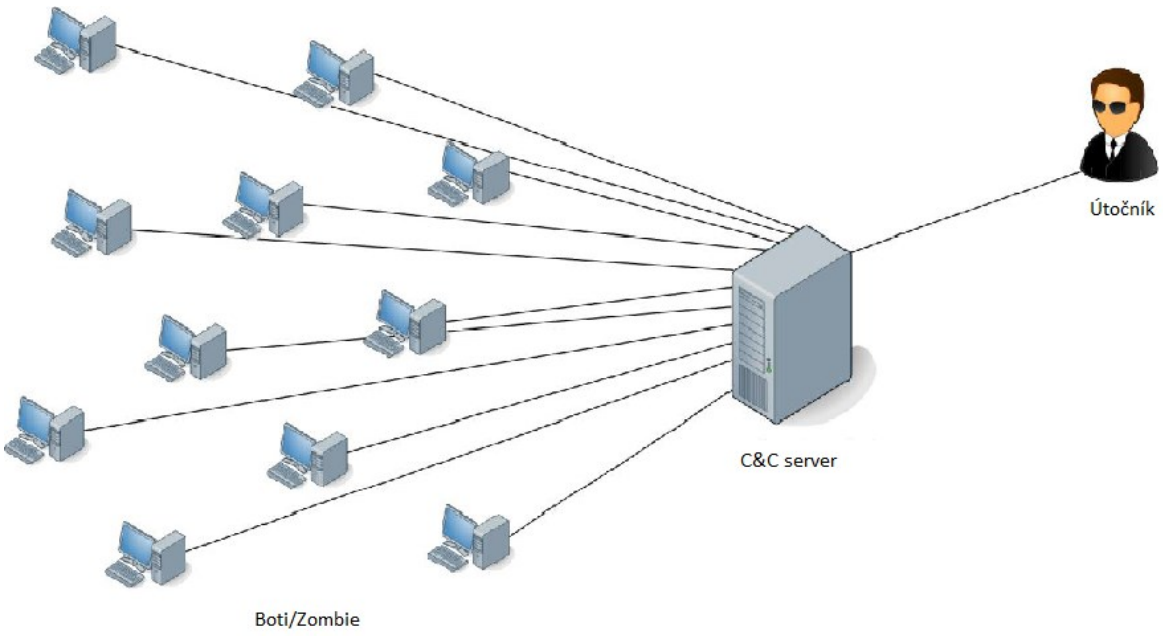
3. **Řízení (ovládání) botů skrze C&C infrastrukturu**

   Software sloužící ke komunikaci s C&C serverem. [5], [35]

Dále botnety můžeme rozdělit podle architektury na:

1. **Centralizovanou architekturu**

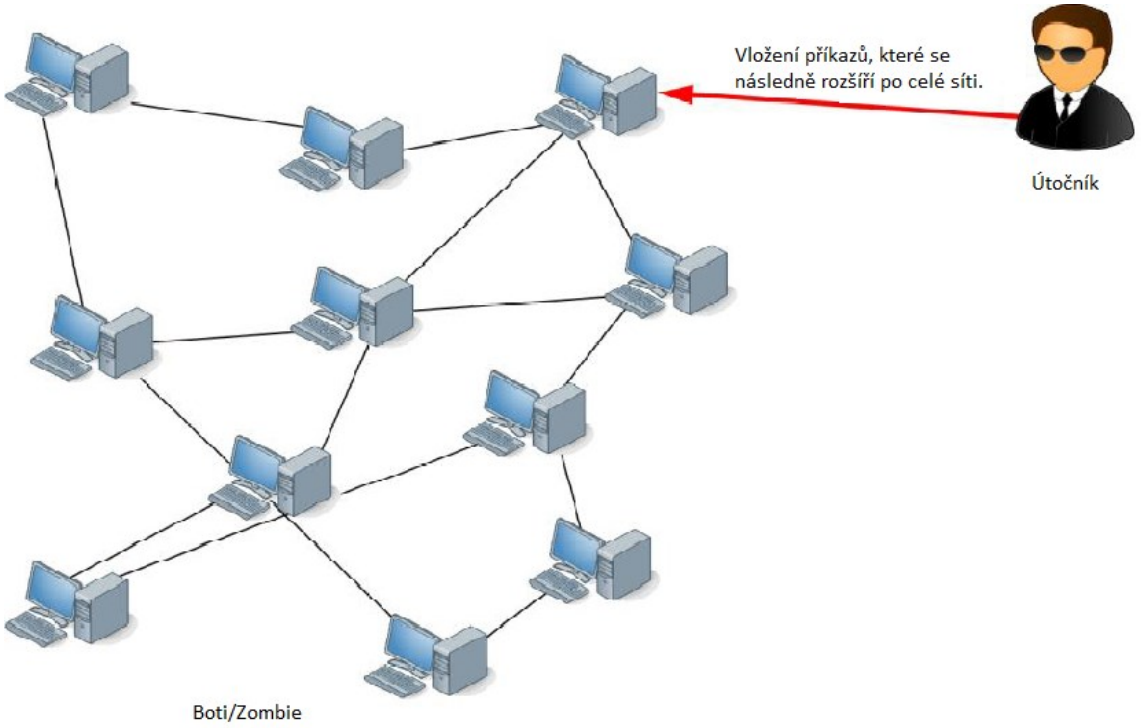
   Tato architektura pracuje na principu klient-server, to znamená, že koncové počítače (zombie/boti) komunikují přímo s C&C (centrální řídící prvek), plní jeho instrukce a využívají jeho zdroje. Zmíněná architektura je zobrazena na níže uvedeném obrázku. [5], [35]



Obrázek 5 Centralizovaná architektura botnetu [35]

2. **Decentralizovanou architekturu**

   Decentralizovaná architektura je přesným opakem centralizované architektury. Nemá žádné C&C (centrální řídící prvek), zdroje a příkazy jsou sdíleny se všemi počítači v dané síti. Příklad dané architektury je zobrazen níže. [5], [35]



Obrázek 6 Decentralizovaná architektura botnetu [35]

4 SPECIFICKÉ PŘÍPADY KYBERKRIMINALITY

V předchozích kapitolách byly popsány některé z technik, které útočníci používají ke kriminální činnosti. Nyní bude uvedeno několik specifických případů.

4.1 Kybergrooming (Cyber grooming)

Považuje se za jeden z nejtěžších a nejnebezpečnějších kyberútoků. Termínem kybergrooming se označuje chování pachatele, kterým se snaží vyvolat v dítěti falešnou důvěru a vylákat jej na schůzku v reálném světě. Cílem této schůzky je pak oběť pohlavně zneužít. Útočník si za cíl nejčastěji vybírá dívky od 9 do 14 let, které mají pocit, že je nikdo nechápe, nerozumí jim, nebo se můžou jednoduše nudit.

Pachatel (většinou někdo dospělý) se pak snaží v nich vyvolat pocit, že je má rád, a že jim rozumí. Když se mu podaří tento pocit vyvolat, docílí tím toho, že se s ním oběť může setkat i v reálném světě. Pachatelé takových činů bývají velice trpěliví, s obětí komunikují pomocí sociálních sítí několik měsíců, někdy i více než rok a až potom se odhodlají ke schůzce ve skutečném světě.

Útočníci jsou až přehnaně přátelští, zajímají se o prohloubení vzájemného vztahu, hlavně se snaží udržet vztah v tajnosti, ujišťují oběť, že ji mají rádi a slibují, že vztah bude pokračovat i ve skutečném světě.

V pozdějším stádiu vztahu pachatel po oběti vyžaduje intimní fotografie nebo videa. Pokud mu oběť fotografie nebo videa poskytne a následně se s ním nechce setkat v reálném světě, jsou tyto materiály použity k vydírání oběti, např. „Pokud nepřijdeš, nahraju tvoje fotky na internet.“ [36], [37]

4.2 Kyberšikana (Cyberbullying)

Obecně je kyberšikana označována jako zneužití komunikačních a informačních technologií, hlavně za použití mobilních telefonů a internetu, za účelem způsobení újmy danému člověku.

Jedním z problémů je, že děti a mladí lidé, kteří ICT takto využívají, to považují za zábavu a vůbec si neuvědomují, jaké následky toto konání může mít.

Kyberšikana a šikana mají stejný cíl, a to někomu ublížit nebo ubližovat. V případě klasické šikany se většinou jedná o fyzické útoky, zato u kyberšikany se jedná o útoky psychické. Díky moderním technologiím je možné se pohybovat ve virtuálním světě, který se ale od reálného podstatně liší. Stejně se liší i běžná šikana od kyberšikany. [36], [38]

4.2.1 Rozdíly mezi šikanou a kyberšikanou

V této kapitole jsou vysvětleny rozdíly mezi klasickou šikanou a kyberšikanou:

1. **Útočníci jsou anonymní**

   Útočníci ve virtuálním prostředí často vystupují pod přezdívkou, neznámou e-mailovou adresou a skrytým telefonním číslem. Útočník nemá žádné překážky ve vytváření více identit. Oběť pak nemá téměř žádnou šanci zjistit, kdo na ni útočí. V důsledku toho se u oběti začínají projevovat pocity nejistoty a nejistota je nejhorší pocit, který může člověk prožívat. Anonymita agresora společně s pocity nejistoty, může mít za následek, že se útočník cítí nedosažitelný a zkouší stále závažnější formy útoků. Ale anonymita je v některých případech jen zdánlivá, protože s využitím patřičné technologie se některé případy dají odhalit. I přesto však bývá velmi obtížné pachatele těchto útoků vypátrat.

2. **Proměna profilu útočníka a profilu oběti**

   Ve virtuálním světě nezáleží na pohlaví, věku, síle, postavení v sociální skupině, nebo jestli je oběť či útočník úspěšný ve společnosti. Pachatelem tedy může být kdokoliv, kdo má přehled o tom, jak fungují informační a komunikační technologie. Může dojít i k paradoxu, kdy se z oběti klasické šikany stane pachatel. Oběť šikany se nedokáže fyzicky bránit a mstí se prostřednictvím sociálních sítí, e-mailu, Skypu apod. Je potřeba zdůraznit fakt, že oběti kyberšikany bývají málo nebo vůbec obeznámeny s riziky používání ICT, nejspíš právě kvůli tomu se na internetu chovají méně zodpovědně, zveřejňují osobní údaje, sdílí fotografie, oznamují, kdy a kam pojedou na dovolenou apod..

3. **Mění se místo a čas útoku**

   Klasická šikana většinou probíhá na několika místech, která se opakují, např. škola, autobusová zastávka, hřiště aj. Můžeme tedy předvídat, kde se šikana bude odehrávat. U kyberšikany nemůžeme předvídat, kdy a kde na oběť někdo zaútočí. Útočník může zaútočit kdykoliv a kdekoliv, stačí, aby oběť byla připojena k internetu, nebo měla zapnutý telefon. Oběť se tedy nemá před kyberšikanou kam

schovat. Útočník na ni může zaútočit i na místě, kde se cítí nejbezpečněji, což je pro většinu lidí domov. Nezáleží také, jestli je den, nebo noc, útočník může zaútočit kdykoliv.

4. **Ve virtuálním světě se lidé chovají jinak než ve světě reálném**
   Mohou vystupovat pod jiným pohlavím, věkem a záměrně manipulovat s obětí. Někteří lidé jsou ve virtuálním světě odvážnější, zkoušejí věci, které by si v reálném světě nedovolili. Myslí si, že jsou anonymní a nikdo je nevystopuje. Útočí na někoho, např. mu vyhrožují, nebo ho vydírají, aby si dodali sebevědomí. Nejsou schopní odhadnout, jak na tyto útoky budou reagovat jejich oběti, a to hlavně v případě, kdy si oběť vybrali náhodně a neznají ji. Ve virtuálním světě je velice jednoduché s někým navázat kontakt, komunikovat s ním o čemkoliv, jakkoliv dlouho, a v případě komplikací kontakt ukončit. Pokud se tento model bere jako standard, může se ten, kdo tento model používá, stát obětí kyberšikany, protože přestává být ostražitý.
5. **Kyberšikana slouží k pobavení každého, útočníkovi pomáhá publikum**
   Díky existenci ICT lze prostředky kyberšikany (zprávy, nahrávky, videa) snadno šířit. Kvůli tomu může kyberšikana získat velmi početné publikum. Pachatel nemusí oběť napadat opakovaně, stačí, když kompromitující materiály zveřejní na internetu, např. na sociálních sítích, kde se o jejich rozšíření postará někdo jiný. Takovéto (někdy i velmi početné) publikum může zvýšit intenzitu útoku, nebo zhoršit jeho následky.
6. **Dopady kyberšikany na oběť není snadné rozpoznat**
   Kyberšikana je převážně spojená s psychickým útokem, který se na rozdíl od útoku fyzického nedá dobře rozpoznat. Oběti kyberšikany většinou se svým okolím nekomunikují a nikomu o svých problémech neřeknou. Takové chování může mít hned několik důvodů – strach, stud, neznalost rodičů. Oběti tedy řeší své problémy samy, což může mít za následek, že danou situaci nezvládnou.
7. **Kyberšikana může být způsobena i neúmyslně**
   Špatný odhad na situaci nebo reakci daného člověka, a místo úsměvu mu můžeme způsobit psychickou újmu. [36]

4.2.2 Typy kyberšikanování

Útoky kyberšikany lze rozdělit na dva základní typy – přímé a nepřímé. Nepřímý útok znamená, že za útočníka udělá práci někdo jiný, který se později, někdy i nevědomě, stává komplicem. Častější jsou ale útoky přímé, např.:

1) Blogování

Útočník založí blog, kde zveřejňuje intimní informace o oběti, nebo ji pomlouvá.

2) Bluejacking

Útočník posílá e-mailem nebo přes chytrý telefon fotografie nebo videa, např. svých spolužáků, na kterých jsou daní spolužáci zesměšňováni.

3) Internetové hlasování

Hlasovací anketa typu „Komu nejvíc smrdí nohy“, „Kdo je největší šprt“, aj.. Podobné typy otázek běží paralelně na více typech sociálních sítí (Facebook, Spolužáci, apod.) a většinou je vytvoří někdo z blízkého okolí oběti.

4) Internetové soutěžení

Oběť je „nominována“ k nějaké činnosti a natočení se při tom na video a sdílení tohoto videa na sociálních sítích. Když to oběť odmítne, tak je pomlouvána, označena za zbabělce, apod. (např. šňupání skořice, aj.).

5) Outing

Útočník šíří o oběti nepravdivé informace. Například, že oběť nosí prádlo opačného pohlaví.

6) Happy-slapping

Video, na kterém je oběť fackována, video je poté zveřejněno na sociálních sítích. Často se s videem pojí i hlasovací anketa typu „Nejlepší facka roku, kdo souhlasí palec nahoru“, „Měl dostat víc“, atd. [36]

4.3 Krádež identity (Identity theft)

Jedná se o útok, při kterém dochází k odcizení virtuální identity. Konkrétně se jedná o získání kontroly (trvalé nebo dočasné) nad danou identitou. Cílů pro takové jednání může být několik, např. finanční zisk, či získání informací o jiných osobách nebo firmách. Odcizená identita může být následně použita k útoku na osobu, která tuto identitu vlastnila, nebo k útoku na jinou osobu. Použití u útoku na jinou osobu je snazší, protože dotyčná osoba o záměně neví.

Většinou jsou odcizené identity používány k:

- phishingovým či malwarovým útokům na osoby v kontaktech odcizené identity,
- zasílání spamu,
- odcizení neveřejných informací,
- získání kontroly nad jinými službami. Většině online služeb stačí ke změně hesla vyplnění e-mailové adresy. Tím, že útočník má přístup do e-mailové schránky napadeného, může změnit přístupové údaje v celé řadě dalších služeb.

Dalším nebezpečím jsou například portály jako Facebook nebo Twitter, kde se útočník může vydávat za kohokoliv, protože systém nepozná, že do něj byly zadány nesprávné údaje. Tohoto problému se využívá při kyberstalkingu nebo kybergroomingu. [5], [39]

4.4 Kyberstalking (Cyber stalking)

Jedná se o posílání zpráv obtěžujícího nebo výhružného charakteru formou SMS, e-mailu, Skype aj.. Například, útočník pošle oběti více jak 30 SMS za hodinu. Kyberstalking je fenomén, kdy pachatel používá komunikační technologie k obtěžování, pronásledování či vydírání. Tento fenomén přišel společně s vývojem komunikačních technologií. Takové pronásledování je opakované, například oběti každý den chodí výhružné e-maily nebo SMS. Je zároveň dlouhodobé, až několik měsíců. A stupňuje se. Nejdříve mohou chodit lichotivé zprávy, pachatel vystupuje příjemně, zjišťuje si informace, a pokud oběť nereaguje podle jeho představ, může začít posílat výhružné zprávy. Toto obtěžování může skončit fyzickým útokem, a v krajním případě i smrtí. [40], [41]

V roce 2010 byl termín stalking zaveden do trestního zákoníku jako zákon s názvem nebezpečné pronásledování. Kyberstalking je tedy charakterizován jako trestný čin, proto se oběť může obrátit na policii o pomoc. První, co by oběť měla udělat, pokud jí chodí obtěžující zprávy, je je ignorovat, ale v žádném případě je nemazat, protože mohou posloužit jako důkazní materiál. Dále na takové zprávy neodpovídat, a pokud ví, kdo je posílá, tak se s ním nestýkat. Rozhodně by na to oběť neměla být sama, tzn. říci to někomu ve svém okolí, rodičům, učiteli, příteli. Hlavně by neměla zaujmout postoj „to se vyřeší“, „za chvíli ho to přestane bavit“. Je tu možnost, že s tím útočník opravdu přestane, ale taky je tu možnost, že

ho toto jednání naštve, a v takovém případě by mohlo jít i o život. Proto by se takovéto situace neměly podceňovat. [40], [41]

II. PRAKTICKÁ ČÁST

5 PREVENCE PROTI KYBERÚTOKŮM

Praktická část této bakalářské práce navrhuje možnosti obrany proti kyberútokům, které byly představeny v teoretické části této práce. Konkrétně se jedná o útok hrubou silou, odposlech datové komunikace, keylogger, phishing a pharming.

5.1 Útok hrubou silou

Útok hrubou silou se zaměřuje na prolomení přihlašovacích údajů, konkrétně hesel. Nejspolehlivější obranou proti útoku hrubou silou je zvolit si silné heslo. Existují i mechanizmy, které mají zabránit útočníkovi přihlásit se k uživatelově účtu, i když získal jeho přihlašovací údaje. Tyto mechanizmy jsou však jen doplňkovým prvkem, nikoliv hlavní možností obrany proti tomuto typu útoku.

Tyto mechanizmy je možno rozčlenit na:

1. **Dvoufázové ověření**
   Jedná se o systém, který k přihlašovacím údajům navíc přidá dodatečný kontrolní prvek v podobě číselného kódu. Tento kód může uživatel obdržet několika způsoby – od e-mailu a SMS zprávy, až po telefonní aplikaci. Tento kód se zadává až po přihlášení, takže i když útočník zná přihlašovací údaje uživatele, bez tohoto kódu se k jeho účtu nepřihlásí.
2. **Omezení počtu pokusů na zadání hesla**
   Nejčastěji se používá v bankovních systémech, kde se po třech chybných zadáních účet zablokuje. Uživatel má tedy jen tři možnosti zadat heslo, což je v případě útoku hrubou silou nedostatečné, a proto se proti bankovním institucím spíše používají útoky typu phishing nebo pharming.

Výše uvedené metody jsou relevantní až v případech, kdy útočník zjistí uživatelovy přihlašovací údaje, a proto je nejlepší zvolit si takové heslo, které nebude možno tímto útokem prolomit. Níže je přehled nejhorších hesel používaných v roce 2017. [42]

Pořadí	Heslo
1	123456
2	password
3	12345678
4	qwerty

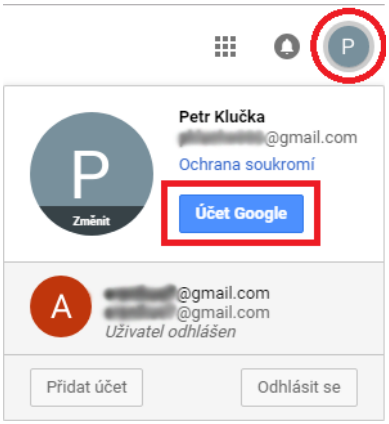
5	12345
6	123456789
7	letmein
8	1234567
9	football
10	iloveyou
11	admin
12	welcome
13	monkey
14	login
15	abc123

Tabulka 1 Nejhorší hesla 2017 [42]

Z toho lze usuzovat, že takto jednoduchá hesla nejspíše nebudou ideální z hlediska bezpečnosti. Bezpečné heslo by mělo být dlouhé alespoň 12 znaků a kombinovat v sobě číslice, malá a velká písmena, a speciální znaky, jako např. „=“. Dále by nemělo být používáno jedno heslo pro více služeb, protože v případě, že toto heslo útočník prolomí, získá přístup k několika službám najednou. Uživatelé by také neměli zapomínat, že se technologie neustále vyvíjejí a heslo, které bylo bezpečné v roce 2000, už nemusí být bezpečné v roce 2018. [43]

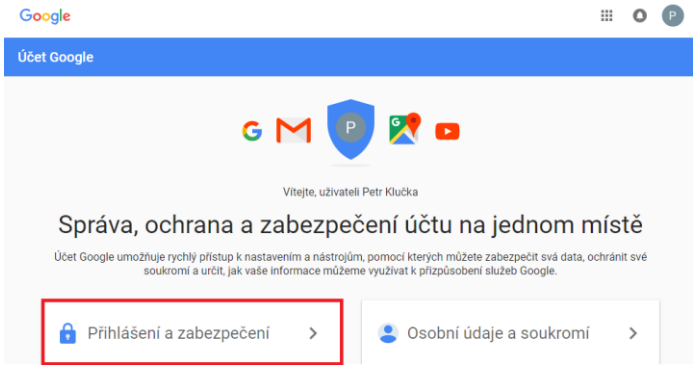
5.1.1 Dvoufázové ověření

Níže jsou popsány kroky, které musí uživatel vykonat pro zapnutí dvoufázového ověření pro účet od společnosti Google. Uživatel se nejdříve přihlásí na svůj Google účet a klikne na ikonu v pravém horním rohu prohlížeče (Obrázek 7), po kliknutí uživatel vybere možnost „Účet Google“, která otevře novou stránku.

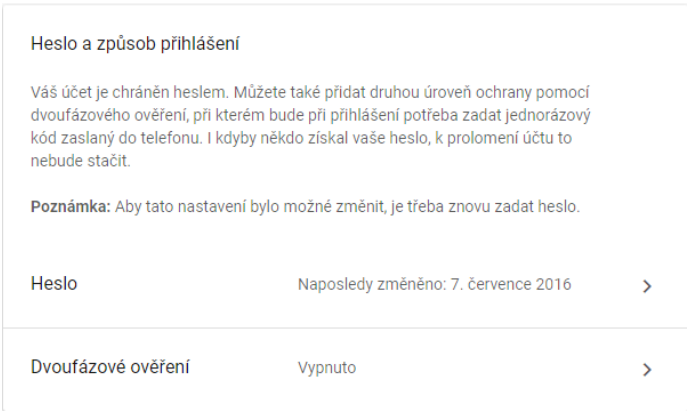


Obrázek 7 Přihlášení do Účtu Google

Na nově otevřené stránce klikne uživatel na možnost „Přihlášení a zabezpečení“, otevře se stránka „Správa, ochrana a zabezpečení účtu“ (Obrázek 8) – na této stránce najde uživatel odstavec „Heslo a způsob přihlášení“ (Obrázek 9) a klikne na možnost „Dvoufázové ověření“.



Obrázek 8 Správa, ochrana a zabezpečení účtu

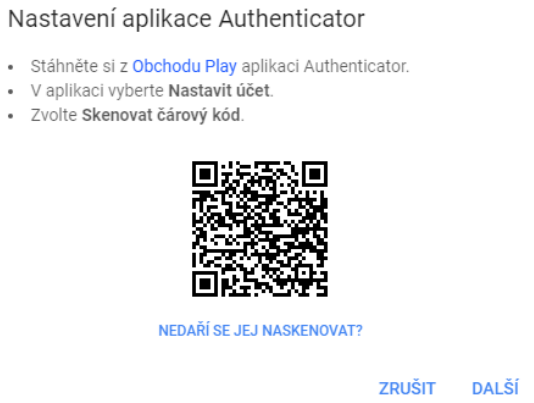


Obrázek 9 Heslo a způsob přihlášení

Na obrazovce, která se zobrazí po kliknutí na možnost „Dvoufázové ověření“ klikne uživatel na tlačítko „Začínáme“. Poté uživatel bude muset znovu zadat své heslo do Google účtu. Následně se bude řídit pokyny na obrazovce a vybere jednu z metod dvoufázového ověření přístupu – hlasová zpráva nebo SMS, výzva od Googlu nebo bezpečnostní klíč. Nejjednodušší možnost je hlasová zpráva nebo SMS – při zvolení této možnosti stačí zadat telefonní číslo, na které uživateli přijde SMS zpráva s kódem, který uživatel zadá pro potvrzení dvoufázového ověření.

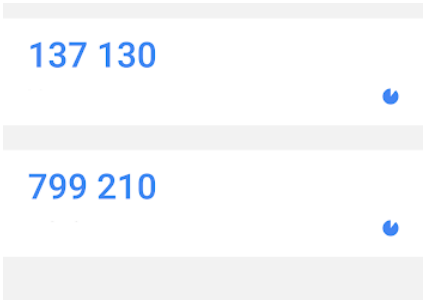
Po zapnutí dvoufázového ověření může uživatel změnit způsob dvoufázového ověření výběrem z nabídky možností poskytnutou společností Google. V níže popsaném případě

bylo změněno na ověření pomocí aplikace „Google Authenticator“ (bezplatná mobilní aplikace od společnosti Google). Stačí jen, aby uživatel vybral tuto možnost z nabídky společnosti Google, zobrazí se následující okno (Obrázek 10), a poté bude postupovat podle instrukcí.



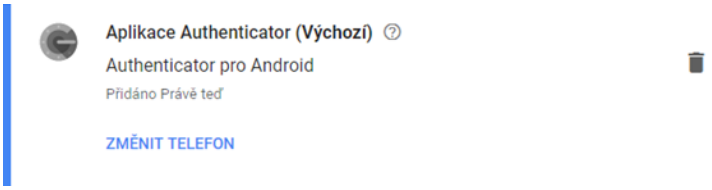
Obrázek 10 Nastavení aplikace Authenticator

Po vykonání těchto instrukcí se v aplikaci „Google Authenticator“ zobrazí kód (Obrázek 11), který uživatel musí zadat do potvrzovacího okna pro aktivaci dvoufázového ověření.



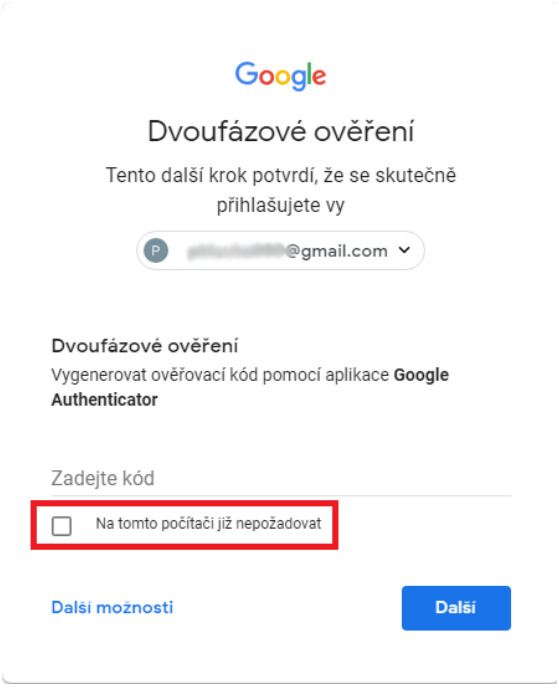
Obrázek 11 Google Authenticator

Po potvrzení bude aplikace přidána jako výchozí kontrolní prvek pro dvoufázové ověření (Obrázek 12).



Obrázek 12 Výchozí kontrolní prvek

Po aktivaci tohoto kontrolního prvku je uživatel vždy povinen zadat unikátní kód vygenerovaný aplikací „Google Authenticator“ po každém přihlášení k účtu od společnosti Google (Obrázek 13). Je možné tento krok přeskočit, pokud uživatel potvrdí možnost „na tomto počítači již nezobrazovat“ (Obrázek 13). Z důvodu bezpečnosti se však tato možnost doporučuje pouze na počítači, ke kterému nemá kromě daného uživatele přístup jiná osoba.



Obrázek 13 Dvoufázové ověření

5.2 Odposlech datové komunikace

V této kapitole je otestována obrana proti síťovým analyzátorům pomocí VPN.

5.2.1 Typy VPN

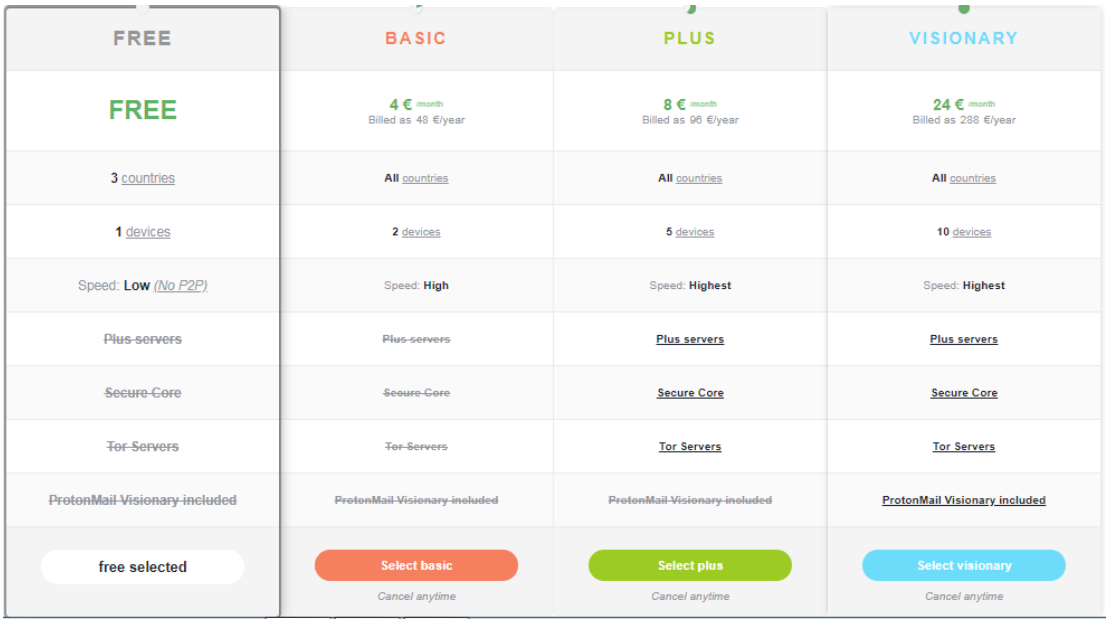
Prvním krokem k vytvoření VPN je vybrání vhodného protokolu. Může být použito několik typů protokolů. Nejčastější typy protokolů, které se používají k vytvoření VPN jsou tyto:

1. **Point-to-Point Tunneling Protocol (PPTP)**
   PPTP je nejstarší a díky své kompatibilitě s většinou operačních systémů a snadné implementaci stále používaný protokol vyvinutý společností Microsoft. V současnosti však již není považován za bezpečný. [44],[45],[48]
2. **Layer 2 Tunneling Protocol/Internet Protocol Security (L2TP/IPSEC)**
   L2TP/IPSEC je kombinace protokolu PPTP a L2F technologie vyvinutou společností CISCO. Na rozdíl od protokolu PPTP protokol L2TP není šifrovaný, proto se používá kombinace protokolů L2TP a IPSEC, kde protokol IPSEC zajišťuje šifrování. Tento protokol se doporučuje jako náhrada za protokol PPTP. [44],[45],[47]
3. **OpenVPN**
   Open-source (otevřený software) VPN protokol vytvořený firmou OpenVPN technologies. Jedná se o nejnovější technologii poskytující kromě šifrování i určitou formu soukromí. Tento protokol využívá šifrovacích protokolů SSL/TSL, a díky skutečnosti, že se jedná o otevřený software, jsou všechny chyby nahlášené veřejností většinou rychle opraveny. [44],[46],[49]

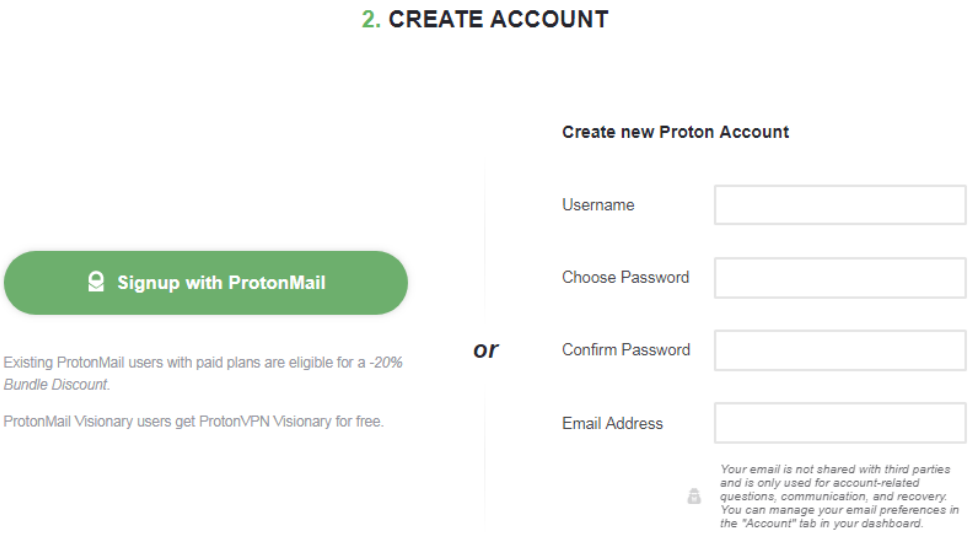
K testování níže je použit produkt od firmy ProtonVPN, který využívá protokol OpenVPN.

K získání VPN klienta od firmy ProtonVPN se uživatel musí zaregistrovat na stránce https://account.protonvpn.com/signup. Nejdříve si uživatel zvolí tarif (Obrázek 14) – v ukázce je použit tarif „FREE“. Největším rozdílem mezi tarify je počet zařízení a rychlost přenosu dat. Podrobně jsou rozdíly mezi tarify znázorněny na Obrázku 14. V dalším kroku musí uživatel vyplnit údaje pro vytvoření účtu (Obrázek 15). Posledním krokem je ověření vytvořeného účtu, a to buď e-mailem, SMS zprávou nebo peněžním příspěvkem. Uživatel

ještě musí odsouhlasit provozní podmínky a pravidla soukromí, a poté klikne na tlačítko „Get ProtonVPN“.



Obrázek 14 Výběr tarifu [50]

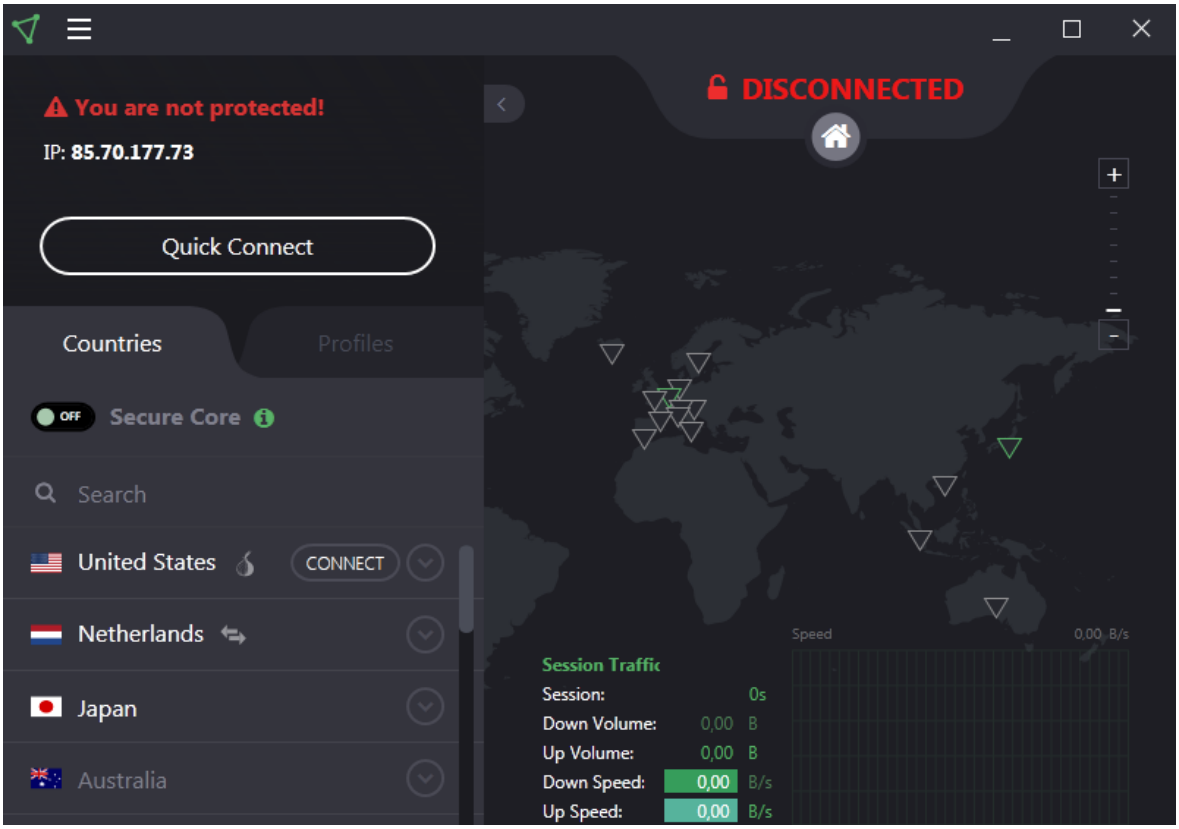


Obrázek 15 Zadání informací pro vytvoření VPN účtu. [50]

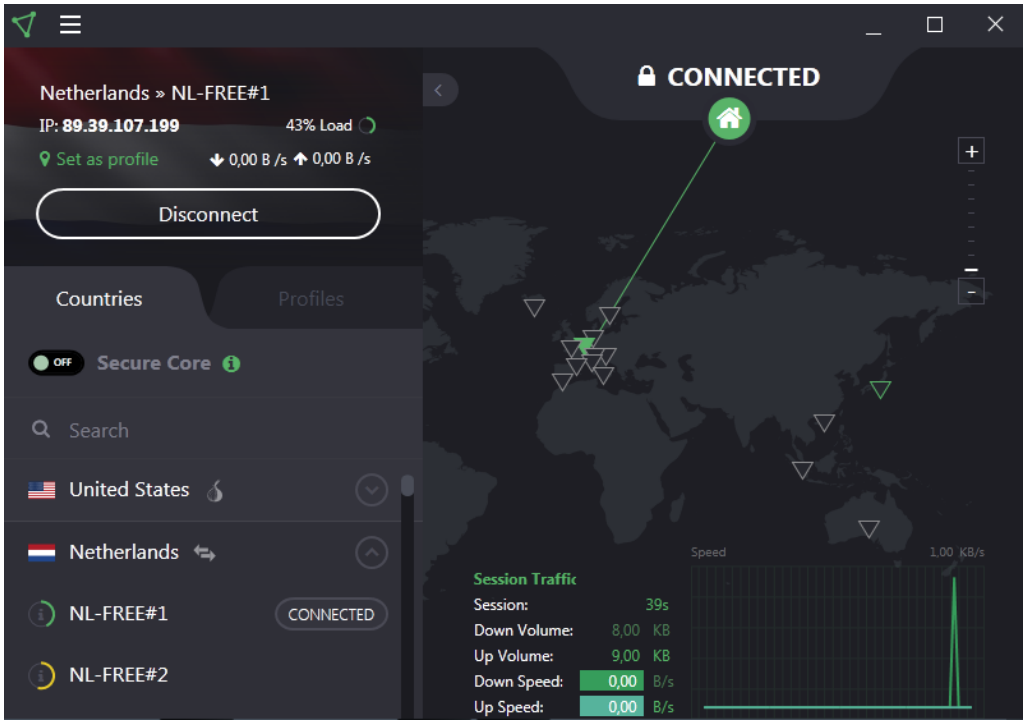
Po úspěšné registraci si uživatel musí stáhnout VPN klienta z adresy https://protonvpn.com/download/. Uživatel si následně vybere operační systém, který používá a klienta stáhne a nainstaluje. V ukázce je VPN klient nainstalován na operační systém Windows.

Do VPN klienta se po nainstalování uživatel přihlásí pomocí údajů, které zadal při vytvoření účtu (Obrázek 15). Přihlašovací údaje budou fungovat až po jejich potvrzení pomocí jedné z uživatelem dříve zvolených metod.

Po přihlášení do VPN klienta se uživateli otevře okno (Obrázek 16), ve kterém si může vybrat VPN server a zemi, ke které se může připojit. Uživatel má také možnost „Quick Connect“, která ho přihlásí k nejbližšímu náhodnému serveru – stačí tedy, aby se uživatel připojil na nějaký VPN server a všechna jeho komunikace bude probíhat přes něj. Připojením na VPN server se uživateli zobrazí jeho statistiky, zátěž a IP adresa (Obrázek 17).



Obrázek 16 VPN klient – nepřipojený k VPN serveru

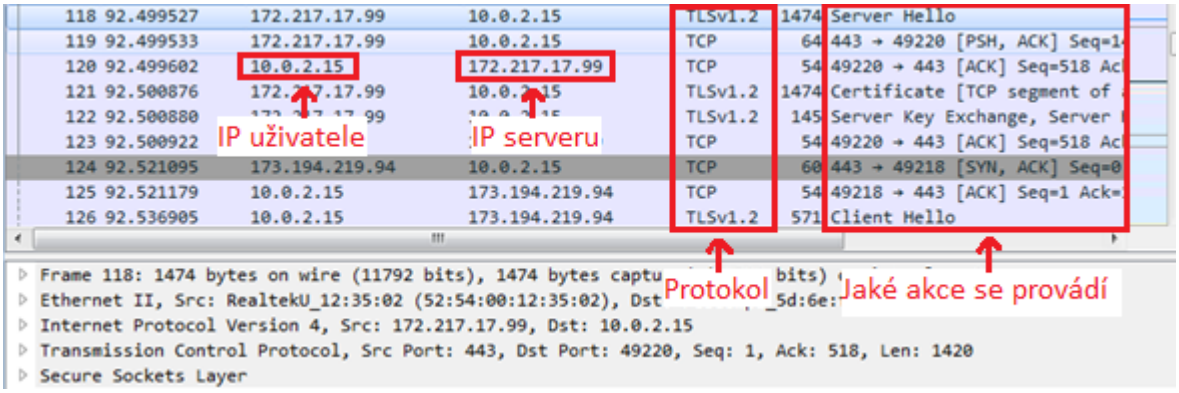


Obrázek 17 VPN klient – připojený k VPN serveru

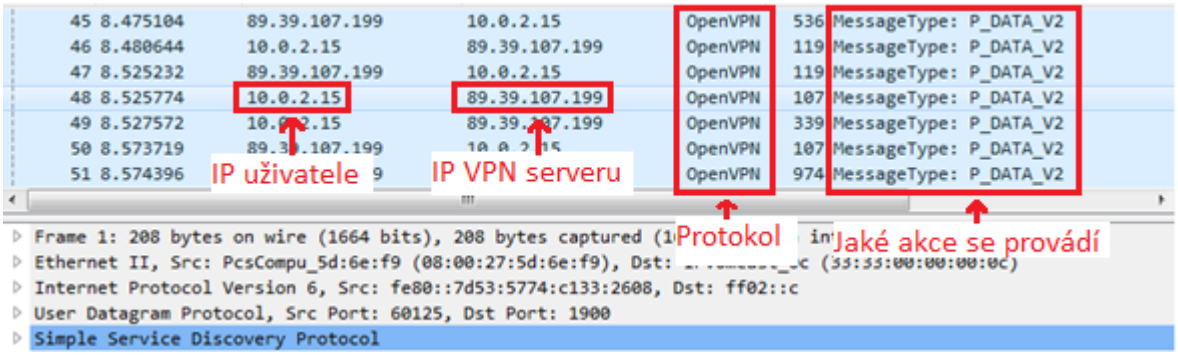
Pomocí programu Wireshark (jedná se o open-source síťový analyzátor volně dostupný na stránce https://www.wireshark.org/) je níže popsáno, jak funguje paketový sniffer a jak se mu uživatel může pomocí VPN bránit.

Obrázek 18 ukazuje program Wireshark při zachycování síťové komunikace. V tomto případě se jedná o připojení k serveru. Z programu lze zjistit IP adresu uživatele, IP adresu serveru, ke kterému se připojuje, protokol který k tomu používá a jakou akci konkrétně vykonává.

Stejná situace je zobrazena i na Obrázku 19 jen s tím rozdílem, že použit je VPN klient. Na rozdíl od Obrázku 18 nelze vidět IP adresu serveru, ke kterému se uživatel připojuje, ale adresu VPN serveru, přes který komunikace prochází. Rovněž nelze vidět ani jaký protokol je použit, nebo jaká akce se vykonává.



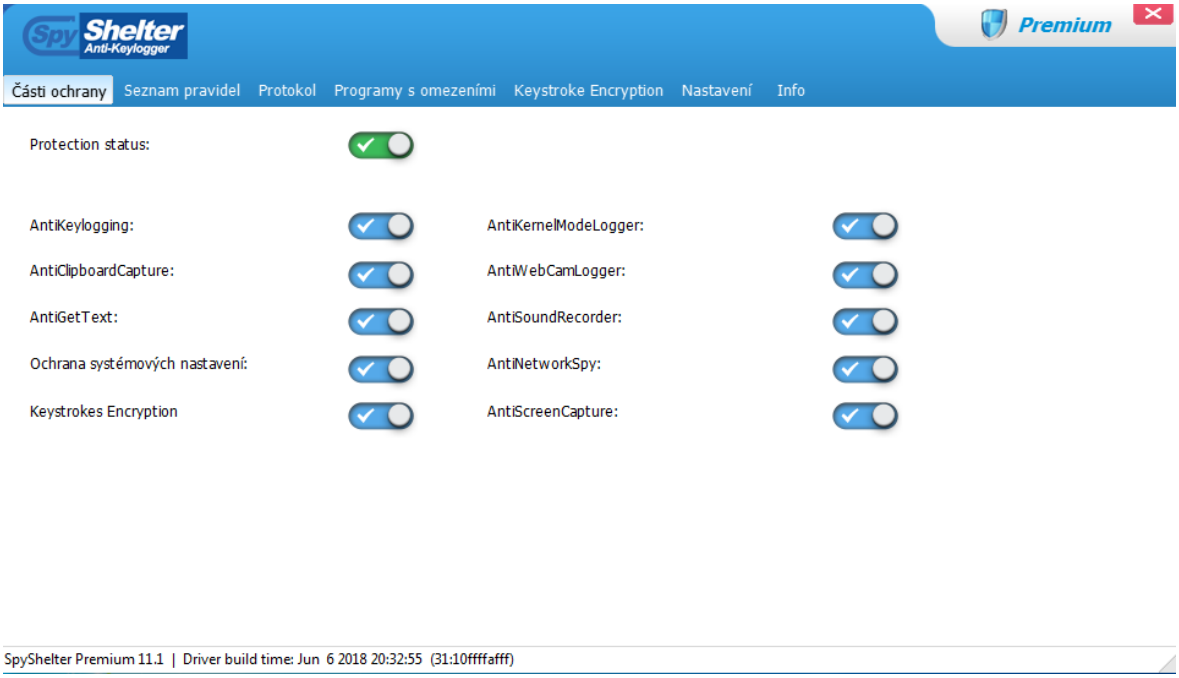
Obrázek 18 Připojení k serveru bez VPN



Obrázek 19 Připojení k serveru s VPN

5.3 Keylogger

Tato kapitola se zabývá programem SpyShelter Anti-Keylogger. Jedná se o program společnosti SpyShelter, zabývající se ochranou počítače proti škodlivým softwarům. Tento program lze stáhnout z adresy „https://www.spyshelter.com/download-spyshelter/“. Po stažení je Program SpyShelter Anti-Keylogger spuštěn ve zkušební verzi, která funguje 14 dní od nainstalování. Po 14ti dnech je nutno zakoupit licenci, aby mohl program dále pracovat. Licence jsou poskytovány na jeden rok – v srpnu 2018 je cena licence €29 pro 1 zařízení. Maximální počet zařízení je 5, cena jedné licence pro 5 zařízení je €69. SpyShelter Anti-Keylogger funguje pouze pro operační systém Windows, 32 bitové i 64 bitové verze. Mezi podporovanými jazyky je i čeština. SpyShelter Anti-Keylogger je pouze program pro blokování nežádoucích programů, nikoliv jejich odstranění. Ochranu proti těmto programům poskytuje až od jeho zapnutí, nedokáže zpětně zablokovat programy, které byly nainstalovány před jeho zapnutím.

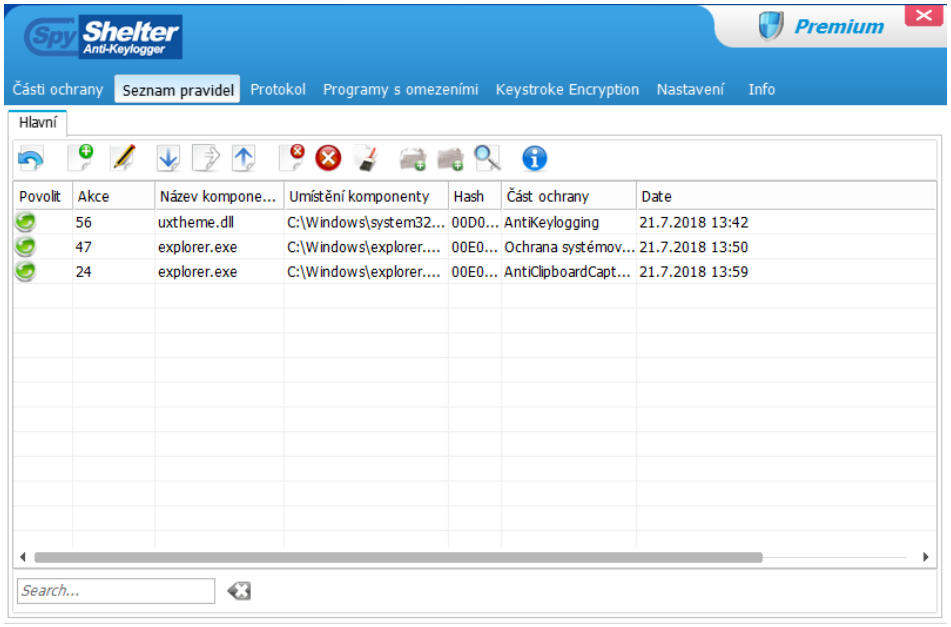


Obrázek 20 Seznam ochran programu SpyShelter Anti Keylogger

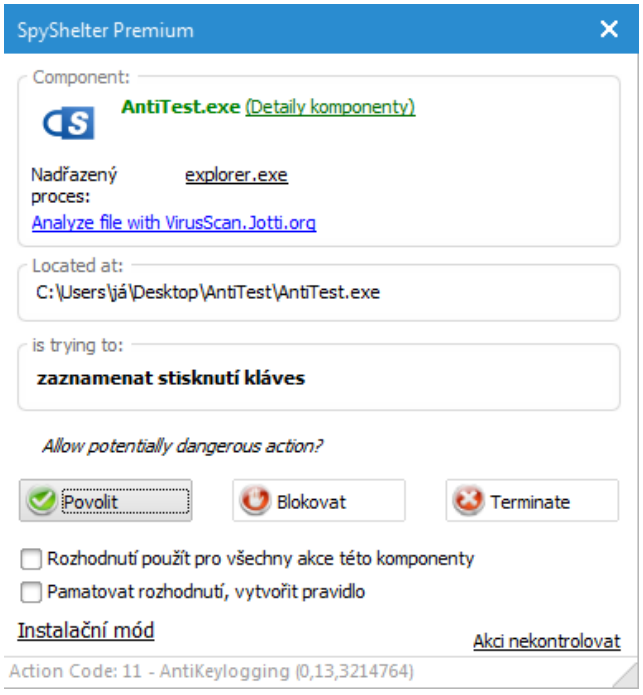
Obrázek 20 ukazuje před jakými útoky je počítač chráněn – položka **AntiKeylogging** chrání před programy, které zaznamenávají stisknutí kláves. **AntiClipboardCapture** poskytuje ochranu proti programům zachytávajícím data ze schránky (prostor, ve kterém jsou uloženy data při kopírování, vložení nebo vyjmutí). **AntiGetText** zabraňuje použití funkce GetText, která může být použita k získání citlivých informací z uživatelova počítače. **Ochrana systémových nastavení** je ochrana počítačových registrů. Položka **Keystrokes Encryption** poskytuje šifrování stisknutých kláves. **AntiKernelModelLogger** představuje ochranu proti keyloggerům, které pracují na úrovni ovladačů nebo služeb. **AntiWebCamLogger** zabraňuje keyloggerům připojit se na kameru a posílat z ní útočníkovi fotografie nebo videa. **AntiSoundRecorder** funguje na stejném principu jako AntiWebCamLogger jen se nejedná o kameru, ale o mikrofon. **AntiNetworkSpy** poskytuje ochranu při důležitých internetových transakcích. Poslední položka **AntiScreenCapture** chrání před keyloggery, které pořizují snímky obrazovky v pravidelných intervalech a posílají je útočníkovi.

Seznam pravidel (Obrázek 21) ukládá aplikace, které chtěly provést akci, která je v rozporu s některou z ochran programu SpyShelter Anti-Keylogger. Je v něm také uloženo, jak má program na tuto aplikaci reagovat (Obrázek 22) – může ji povolit, blokovat, nebo „zničit“. Pokud si je uživatel jistý, že je daná aplikace bezpečná a nechce, aby se program pokaždé ptal, jestli má aplikaci povolit, může zaškrtnout možnost „Pamatovat rozhodnutí,

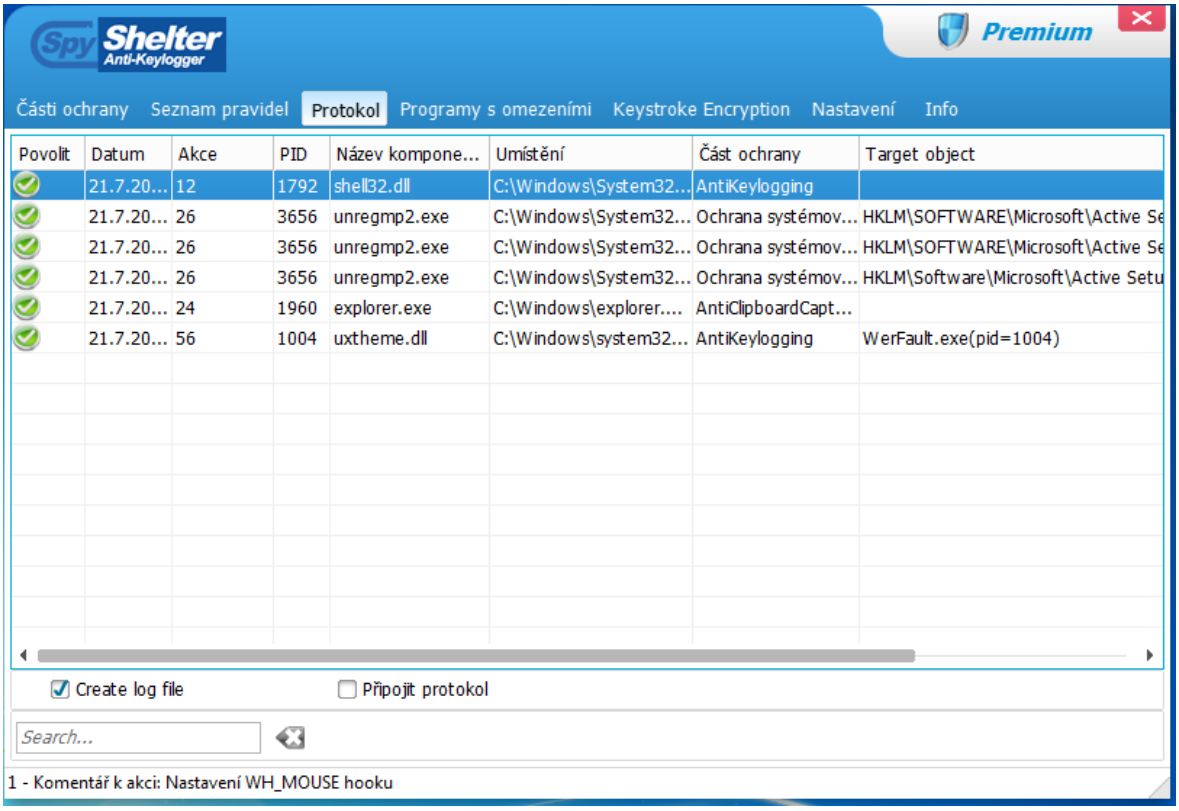
vytvořit pravidlo“, které vytvoří pravidlo v seznamu pravidel, takže příště, až bude aplikace zase chtít provést danou akci, už se nebude ptát, ale rovnou ji povolí. Stejně tak funguje i možnost „Blokovat“, u možnosti „Zničit“ není nutné zaškrtnout možnost „Pamatovat rozhodnutí, vytvořit pravidlo“ – tato možnost se uloží jako pravidlo i bez ní.



Obrázek 21 Položka Seznam pravidel



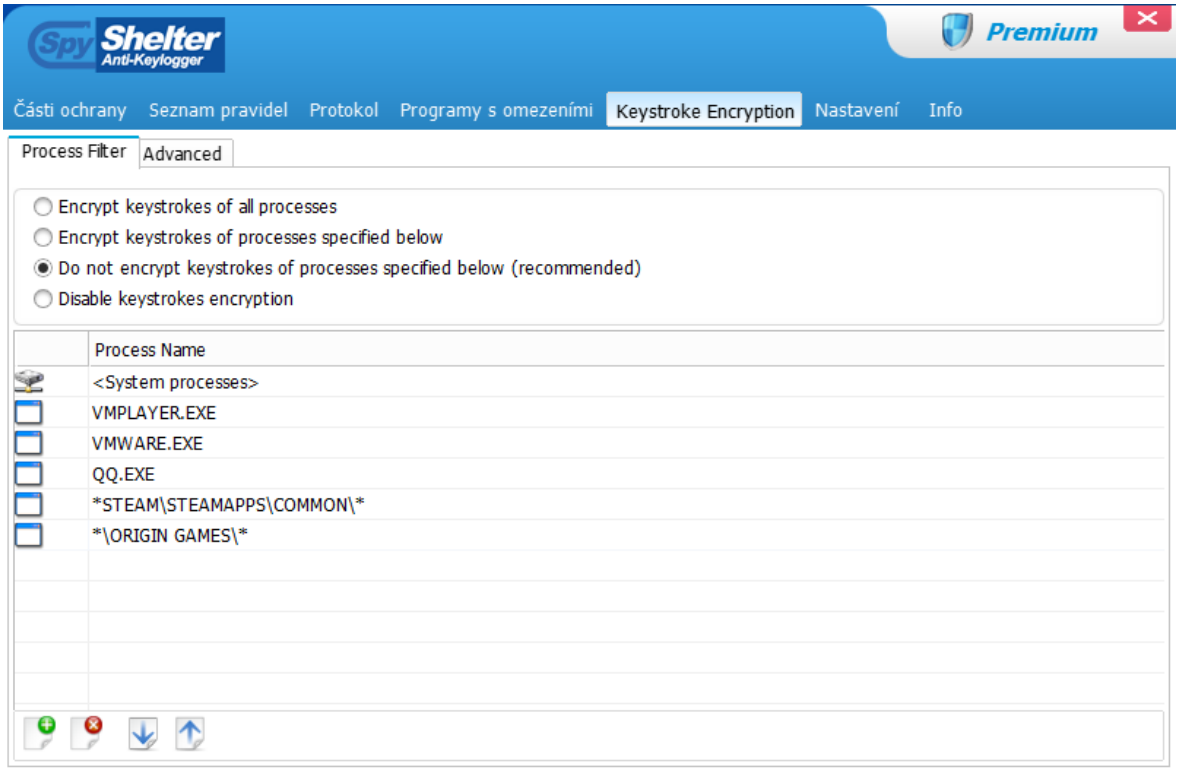
Obrázek 22 Oznámení akce aplikace AntiTest.exe



Obrázek 23 Položka Protokol

Položka Protokol (Obrázek 23) zaznamenává akce programů, na které byla použita nějaká část ochrany, a jestli tato akce byla povolena, zakázána nebo „zničena“. Protokol není automaticky ukládán, tzn., že po vypnutí počítače se smaže i protokol. Pokud chce uživatel protokol uložit do souboru, je nutné zaškrtnout možnost „Připojit protokol“.

Keystroke Encryption (Obrázek 24) nastavuje, které procesy mohou používat šifrování kláves. Uživatel si může sám zvolit procesy, které chce, aby toto šifrování používaly, nebo si může vybrat jednu z možností zobrazenou na Obrázku 24. Není doporučeno používat klávesové šifrování pro systémové procesy – mohlo by dojít k nestabilitě systému.



Obrázek 24 Položka Keystroke Encryption

5.4 Rybaření (Phishing)

V této kapitole je popsán klasický phishingový útok pomocí falešné internetové stránky s formulářem pro zadání hesla, a prostředky, kterými se lze tomuto útoku bránit. Tento útok může probíhat následovně:

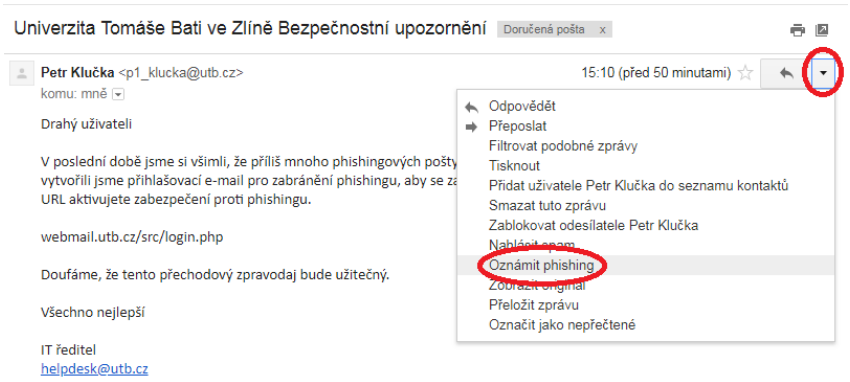
1. Je vytvořena webová stránka, která vypadá stejně, jako originál (např. stránka pro přihlášení do elektronického bankovnictví).
2. Je vytvořen a zaslán e-mail, který přesvědčí příjemce, aby otevřel odkaz, na kterém se nachází útočníkem vytvořená stránka, a zadal potřebné údaje.
3. Do stránky zadané informace se následně dostanou k útočníkovi.

Jak takovému útoku předcházet je následně ukázáno s použitím e-mailového účtu od společnosti Google.

Nejjednodušší možnost pro uživatele je nahlásit e-mail, který považuje za phishing společnosti Google, která jej analyzuje a pokud usoudí, že se jedná o phishing, bude tyto e-maily rovnou mazat, bez toho, aniž by se dostaly k odesílateli.

Nahlášení podvodného e-mailu lze provést následovně – doručený e-mail uživatel otevře, vpravo nahoře vybere možnost „Další“, a poté vybere možnost „Oznámit phishing“

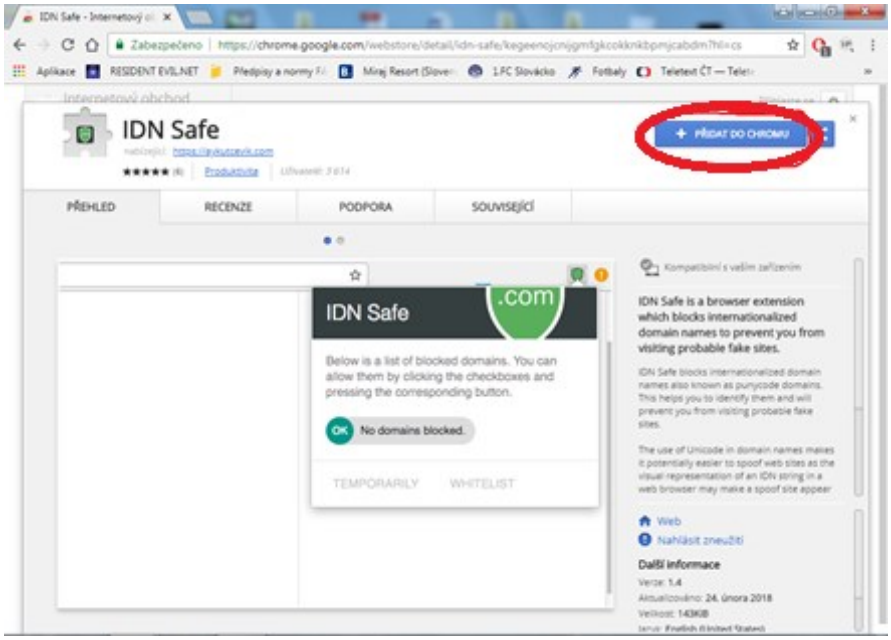
(Obrázek 25). E-mail se odešle k analýze do společnosti Google a přidá se k filtrovanému obsahu e-mailové schránky.



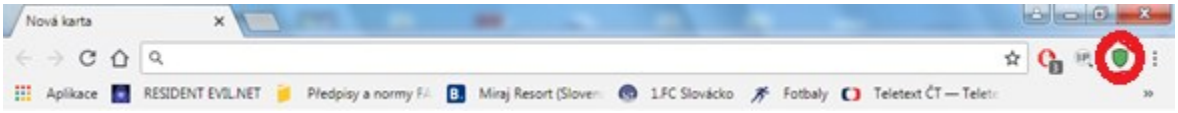
Obrázek 25 Oznámení Phishingu

Nevýhodou tohoto postupu je, že přijatý e-mail je nutné otevřít, a to nemusí být vždy žádoucí.

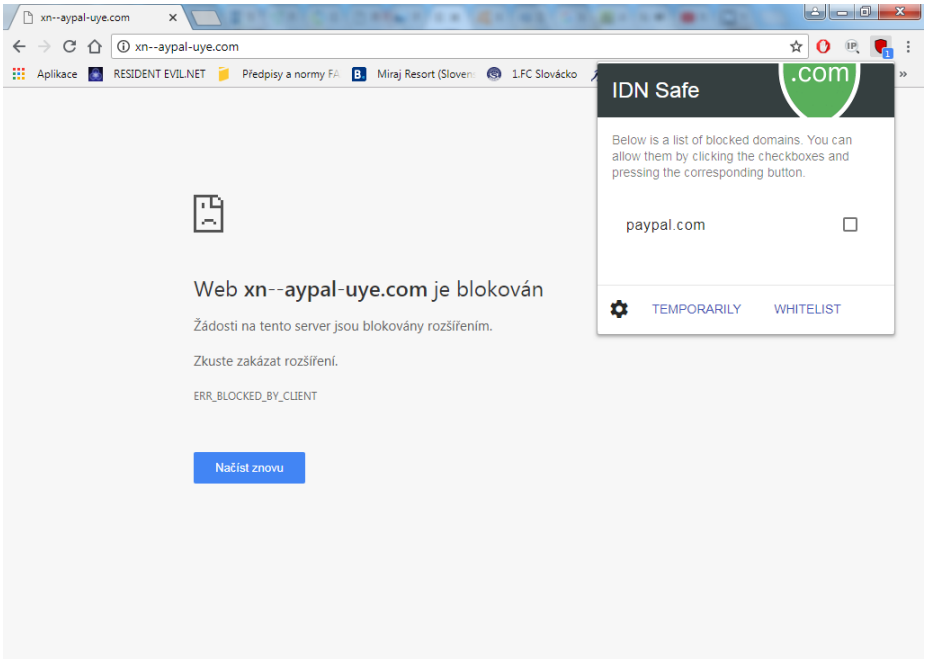
V případě, že uživatel nevyužije předchozí možnost, nebo nepozná, zda se jedná o phishing a klikne na odkaz v e-mailu, může si stáhnout rozšíření pro webový prohlížeč, které dokáže zablokovat tzv. Internationalized Domain Names, čili domény, které jsou psané v Unicode (technická norma pro kódování a zpracování textů) a konvertovány do formátu ASCII (tato konverze se nazývá „punycode“). Např. adresa „apple.com“ vypadá jako normální adresa, ale je psaná ve formátu Unicode a konvertovaná do formátu ASCII. Konvertovaná adresa vypadá takto: „xn--80ak6aa92e.com“. V prohlížeči se však tato adresa zobrazí jako „apple.com“, a proto je obtížné rozpoznat pravou stránku od falešné. Tento problém řeší například rozšíření IDN Safe. Toto rozšíření kontroluje, jestli se v URL adrese nachází „punycode“. Pokud ano, tak je toto rozšíření zablokuje. Toto rozšíření pracuje v prohlížeči Chrome, Firefox a Opera. V ukázce je použit prohlížeč Chrome.



Obrázek 26 Instalace ISN Safe



Obrázek 27 Úspěšně nainstalovaný ISN Safe



Obrázek 28 Zablokovaná možná podvodná stránka

Instalace je jednoduchá – stačí otevřít internetový obchod Google, zadat do vyhledávače IDN Safe, kliknout na tlačítko „Přidat do Chromu“ a potvrdit (Obrázek 26). Po úspěšné instalaci se objeví vpravo nahoře ikonka štítu (Obrázek 27). Obrázek 28 ukazuje, že uživatel klikl na odkaz „paypal.com“, který vypadá na první pohled věrohodně, ale první písmeno v odkazu není znak z tabulky ASCII. Toto rozšíření uživateli zabrání se na takovou stránku dostat.

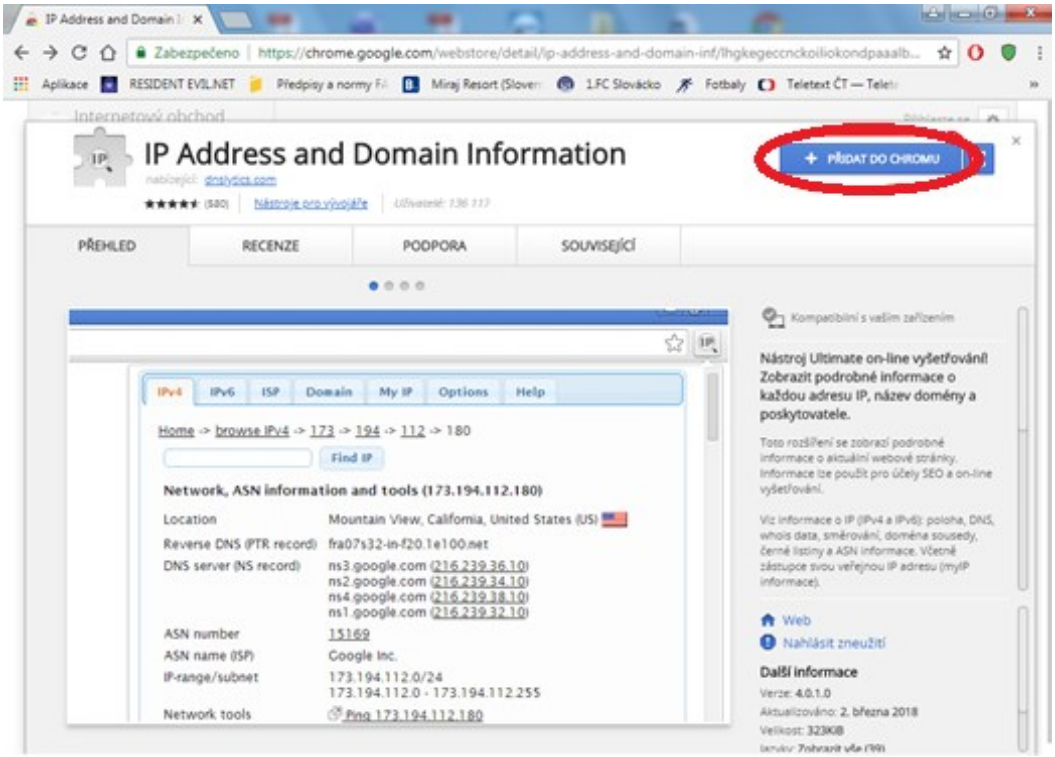
Výše zmíněné metody lze použít k obraně proti phishingu, na prvním místě však zůstává lidský faktor.

5.5 Farmaření (Pharming)

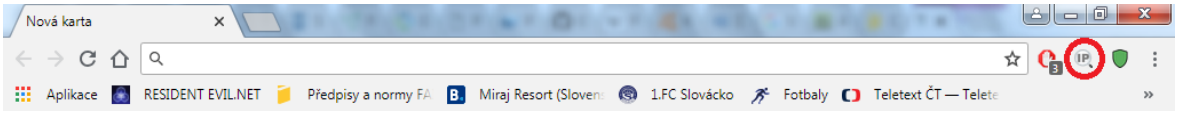
Pharming je možné rozdělit do dvou kategorií – první je útok na samotný DNS server, druhá je útok na uživatelův směrovač, kde útočník vymění DNS server za svůj. V případě, že je útok vedený přímo na DNS server, uživatel sám s tím nic dělat nemůže, ale může si stáhnout rozšíření pro webový prohlížeč IP Address and Domain Information. Pomocí tohoto rozšíření může zjistit podrobné informace o IP adrese, doméně nebo poskytovateli a zjistit, zda se jedná o podvodnou stránku nebo ne.

Níže je ukázáno, jak toto rozšíření nainstalovat a jak funguje.

K získání tohoto rozšíření stačí jít na internetový obchod, ze kterého se získávají rozšíření pro daný webový prohlížeč. Toto rozšíření lze nainstalovat pro prohlížeče Chrome, Firefox, Opera, Safari a Edge. Následující simulace je provedena na prohlížeči Chrome.



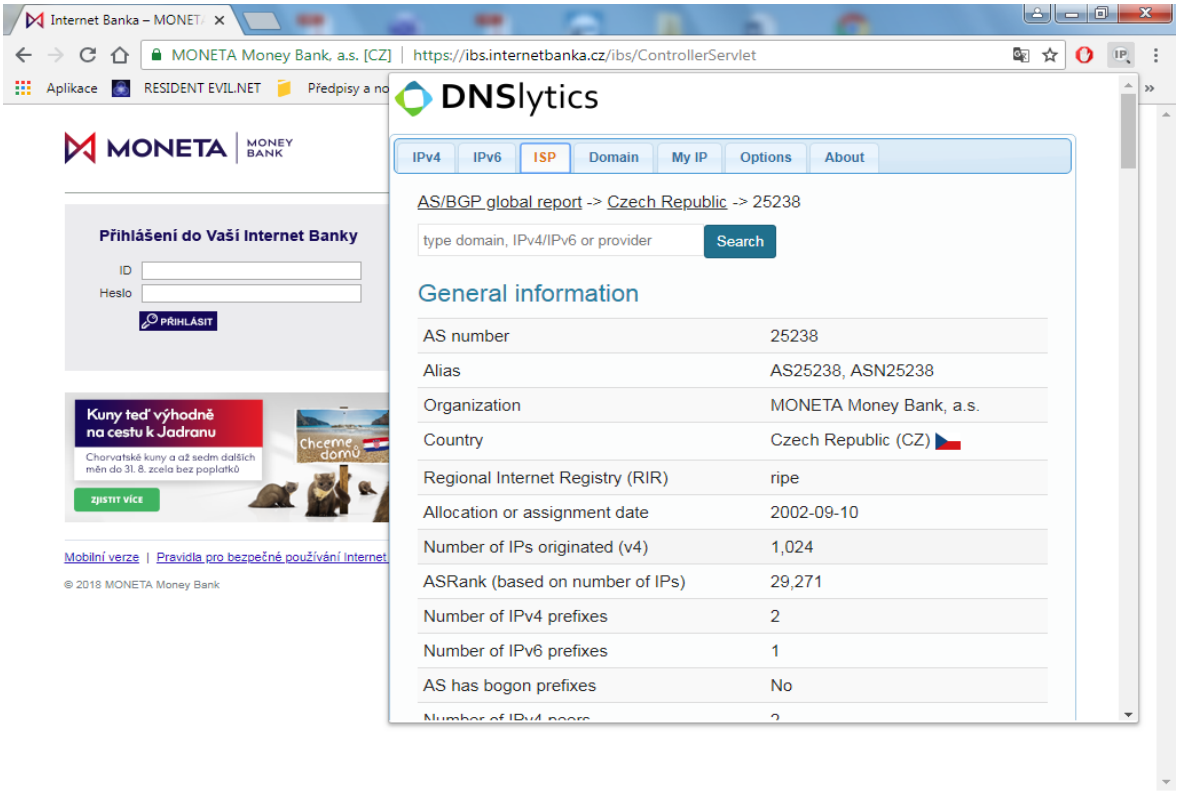
Obrázek 29 Instalace aplikace do internetového prohlížeče



Obrázek 30 Spuštění aplikace v prohlížeči

Instalace je jednoduchá. Jak lze vidět na Obrázku 29, stačí kliknout na tlačítko „Přidat do Chromu“ a potvrdit. Po přidání rozšíření stačí chvíli počkat, než prohlížeč rozšíření nainstaluje. Po úspěšném nainstalování se na liště v daném prohlížeči (zde v Chromu) tato ikona objeví vpravo nahoře (Obrázek 30).

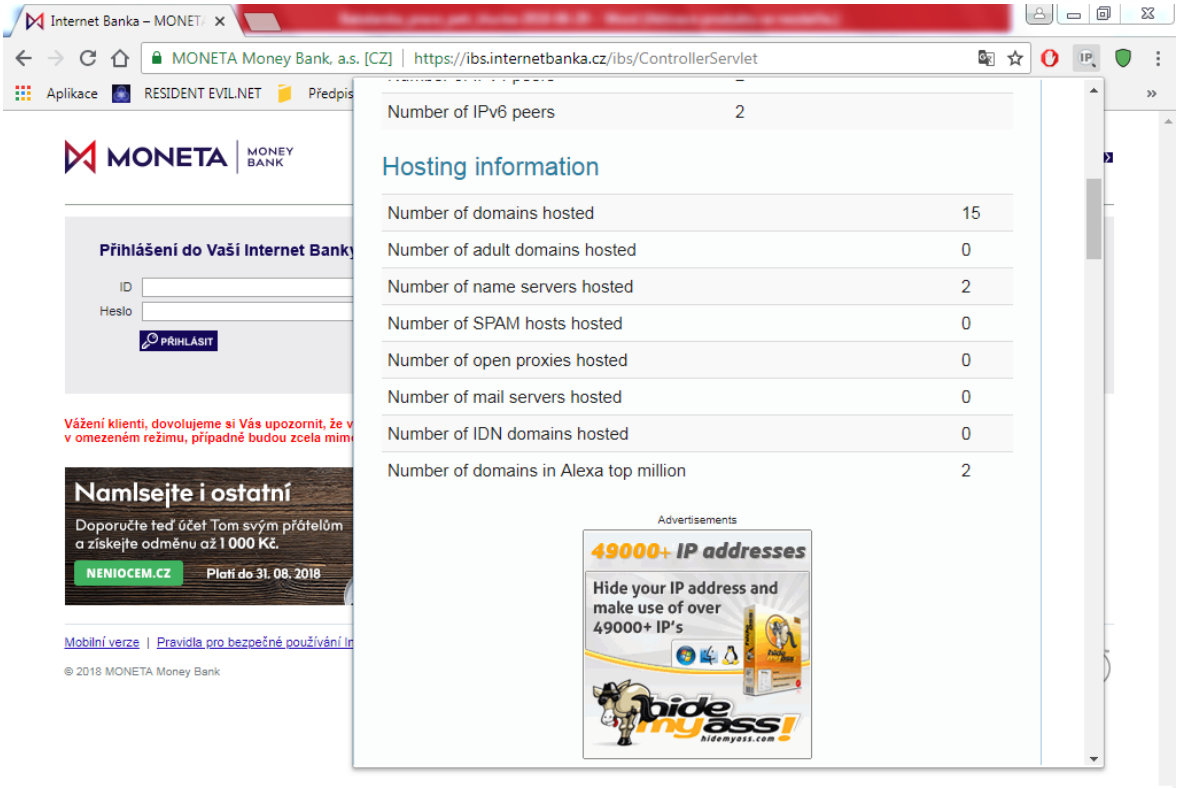
Po kliknutí na tuto ikonu nainstalované rozšíření zobrazí informace o stránce, která je načtená v prohlížeči. Takto vypadá zobrazení na přihlašovací stránce do internetového bankovnictví společnosti Moneta Money Bank:



Obrázek 31 Informace o právě otevřené stránce

Z Obrázku 31 lze pod položkou ISP vidět informace o právě načtené stránce, např. organizaci, které daná stránka patří, kdy byla přidělena, zemi, kde se nachází a všechny další domény, které patří pod tuto organizaci.

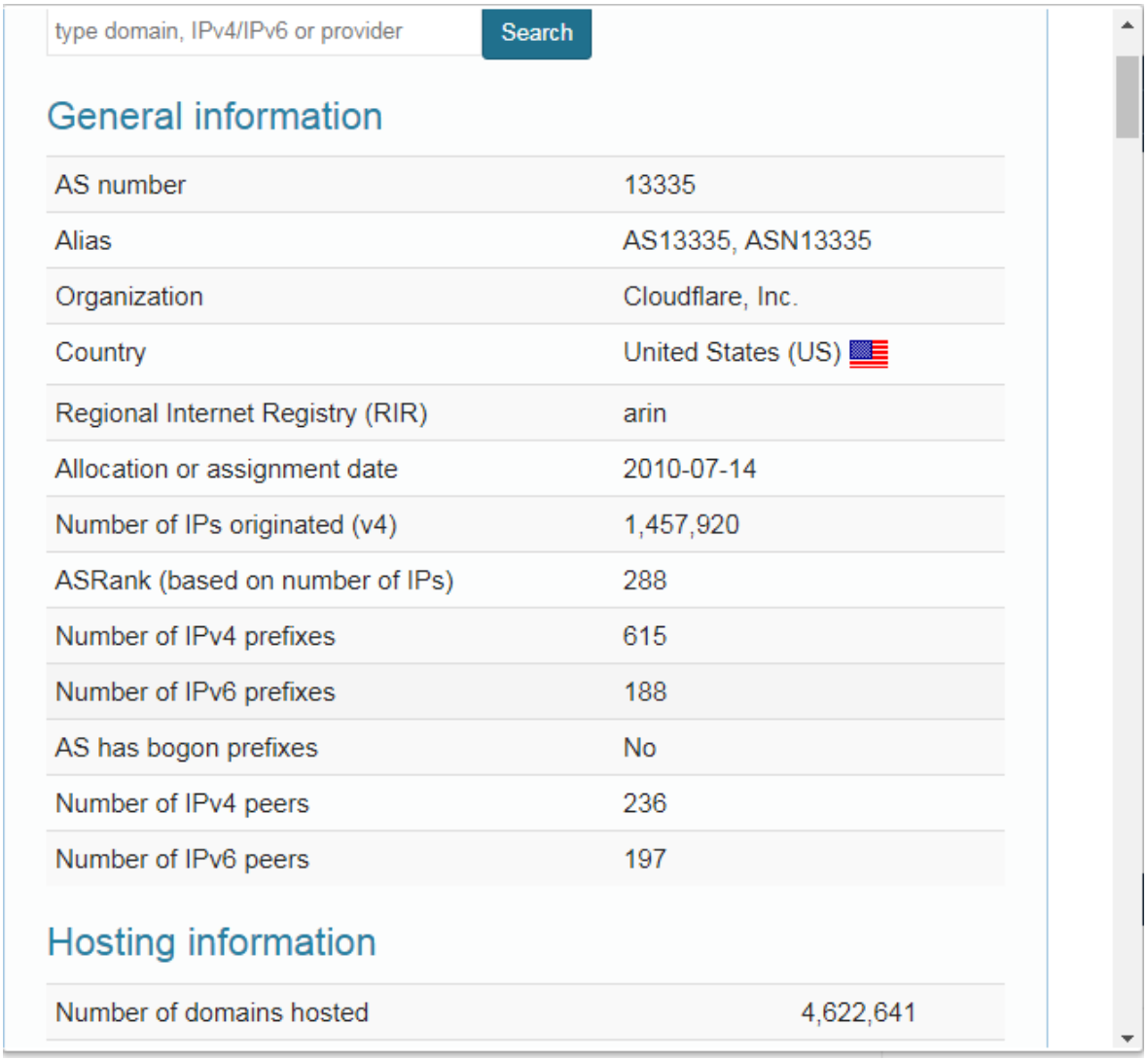
Pokud tedy uživatel vidí, že například stránka pro přihlášení do internetového bankovnictví, která má patřit pod Českou republiku (Obrázek 31) patří pod společnost sídlící v USA (Obrázek 33), pak by to přinejmenším mělo vyvolat pocit, že je něco špatně. Pomocí tohoto rozšíření lze tedy zjistit, jestli se jedná o podvodnou stránku nebo ne.



Obrázek 32 Počet domén, které vlastní daná organizace

Dále lze zjistit (Obrázek 32) kolik domén patří dané organizaci. V tomto případě je vidět, že pod organizaci MONETA Money Bank, a.s. patří 15 domén.

Pokud se uživatel dostane na stránku, která vypadá jako přihlášení do internetového bankovnictví, ale když si zkontroluje informace, které jsou zobrazeny v aplikaci (Obrázek 33) a uvidí, že IP adresa patří organizaci ze Spojených států, která má víc než 4,5 milionu domén, je téměř jisté, že se jedná o podvodnou stránku a rozhodně by se neměl pokoušet přihlásit se na tuto stránku svými přihlašovacími údaji do internetového bankovnictví.

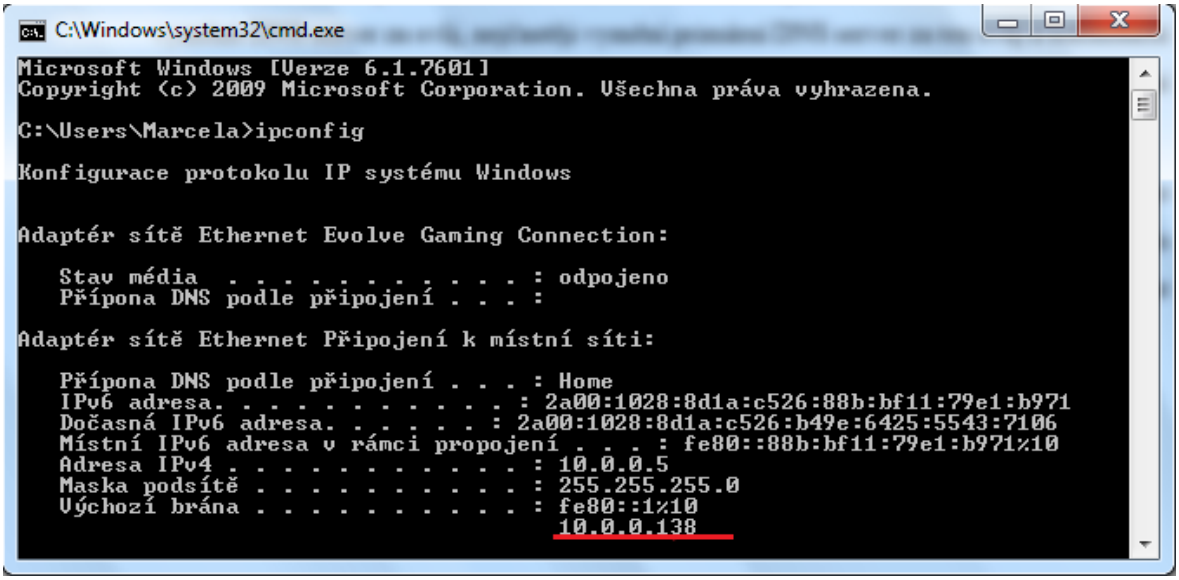


Obrázek 33 Možná podvodná stránka

5.5.1 Lokální Pharming

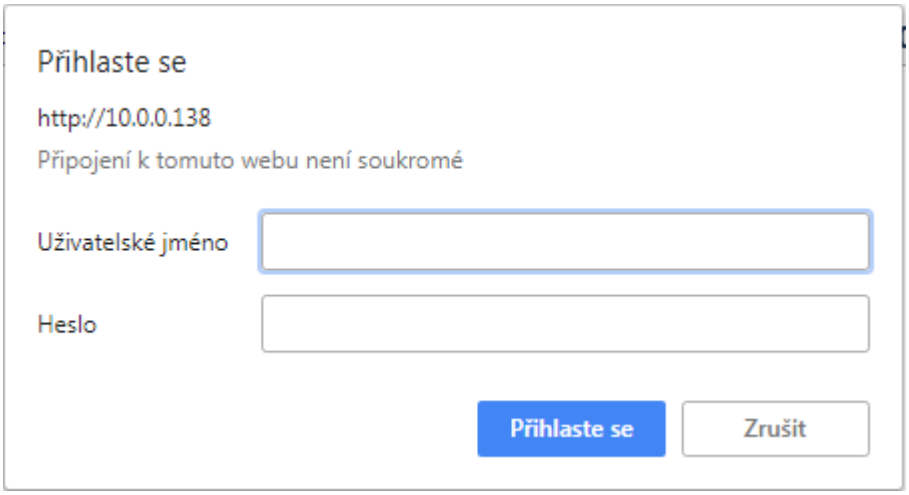
Každý modem má daný primární a sekundární DNS server, tzn., že pokud modem nezná cestu k dané adrese a ptá se DNS serveru, kde daná adresa je, tohoto mohou útočníci využít a vyměnit DNS server za svůj. Nejčastěji vymění primární DNS server za ten svůj a sekundární ponechají stejný, takže když pak primární DNS server odpojí, uživatel nic nepozná, protože sekundární DNS server bude pořád fungovat.

Tomuto lze předejít následujícím způsobem. Nejdříve je nutné změnit přihlašovací údaje k modemu, což lze udělat v jeho nastavení. Do nastavení se lze dostat zadáním výchozí brány do prohlížeče – výchozí bránu lze najít pomocí příkazového řádku, do kterého je následně zadán příkaz „ipconfig“ (Obrázek 34). Ve zkoumaném případě je to adresa 10.0.0.138. Jaká to bude adresa záleží na daném poskytovateli internetového připojení.



Obrázek 34 Zjištění výchozí brány

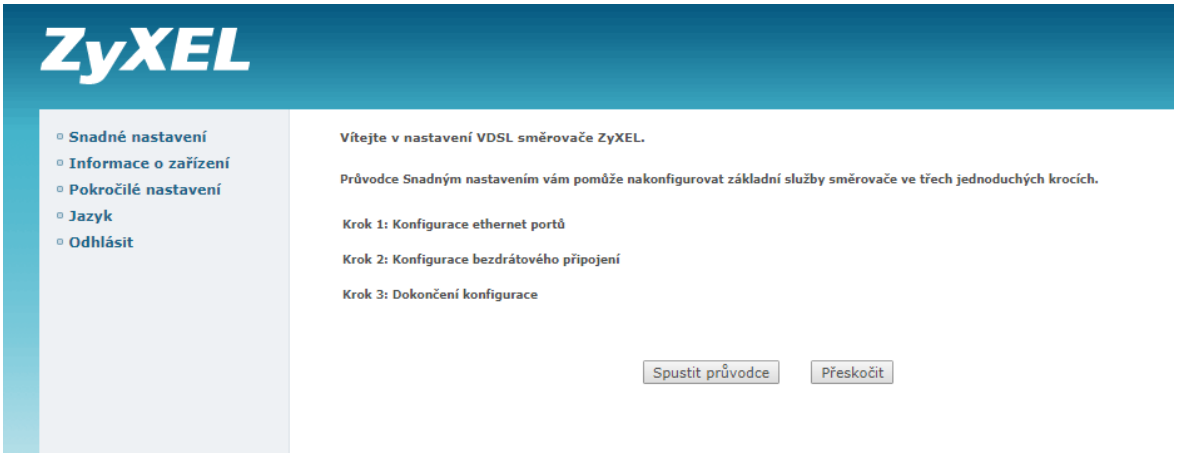
Tuto adresu tedy uživatel zadá do prohlížeče. Objeví se přihlašovací okno (Obrázek 35), do tohoto okna následně zadá přihlašovací údaje, většinou jméno „admin“ a heslo taktéž „admin“.



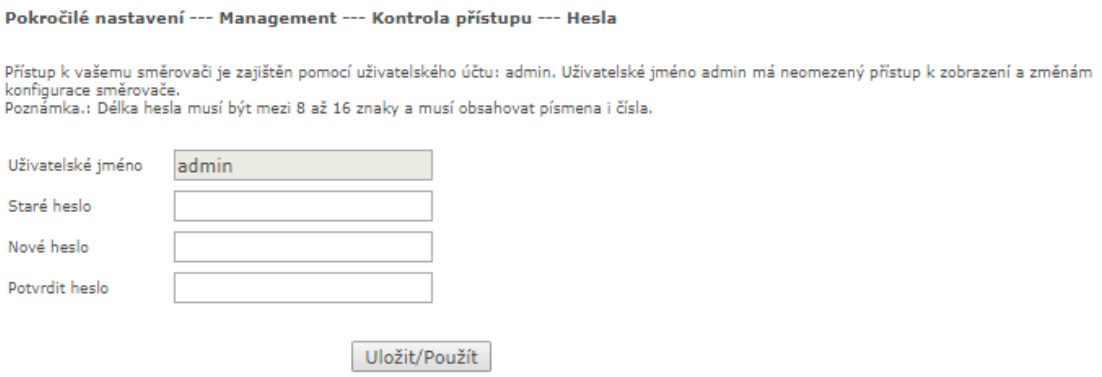
Obrázek 35 Přihlášení k nastavení modemu

Každý modem má jiné uživatelské prostředí a proto postup, který je zde popsán, se nemusí shodovat s postupem pro jiný typ zařízení. V této ukázce je použit produkt ZYXEL VMG1312‑B30B. Jedná se o hybridní zařízení, tzn. kombinaci modemu a směrovače.

Uživatel se tedy přihlásí do nastavení modemu, objeví se tato obrazovka (Obrázek 36). Stávající údaje nejsou ideální z hlediska bezpečnosti, nejdříve tedy změní výše zmíněné přihlašovací údaje. Možnost změnit dosavadní přihlašovací údaje nalezne v oddíle „Pokročilé nastavení“ → „Management“ → „Kontrola přístupu“ → „Hesla“ (Obrázek 37).

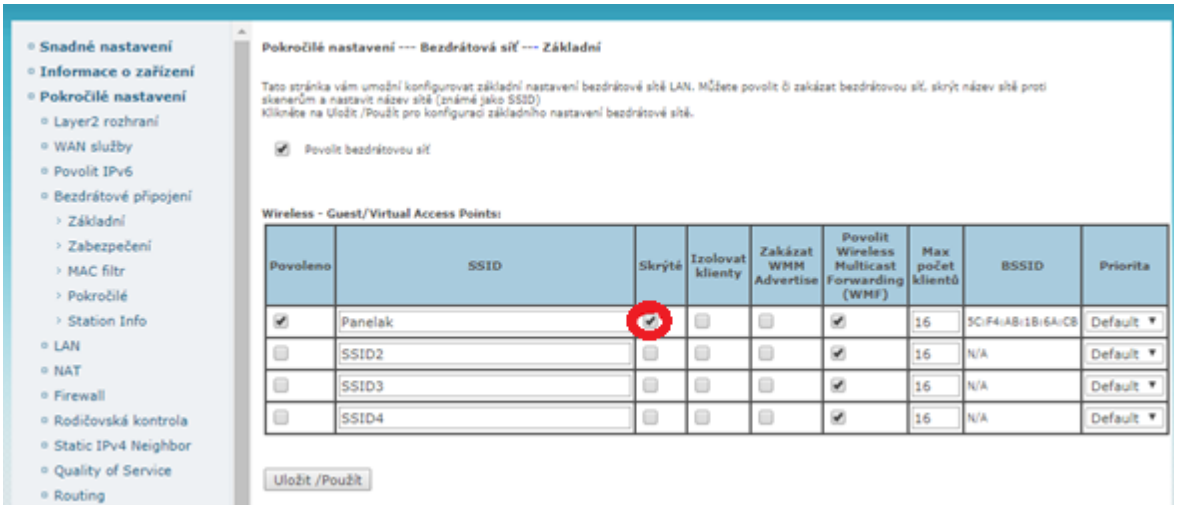


Obrázek 36 Úvodní obrazovka po přihlášení

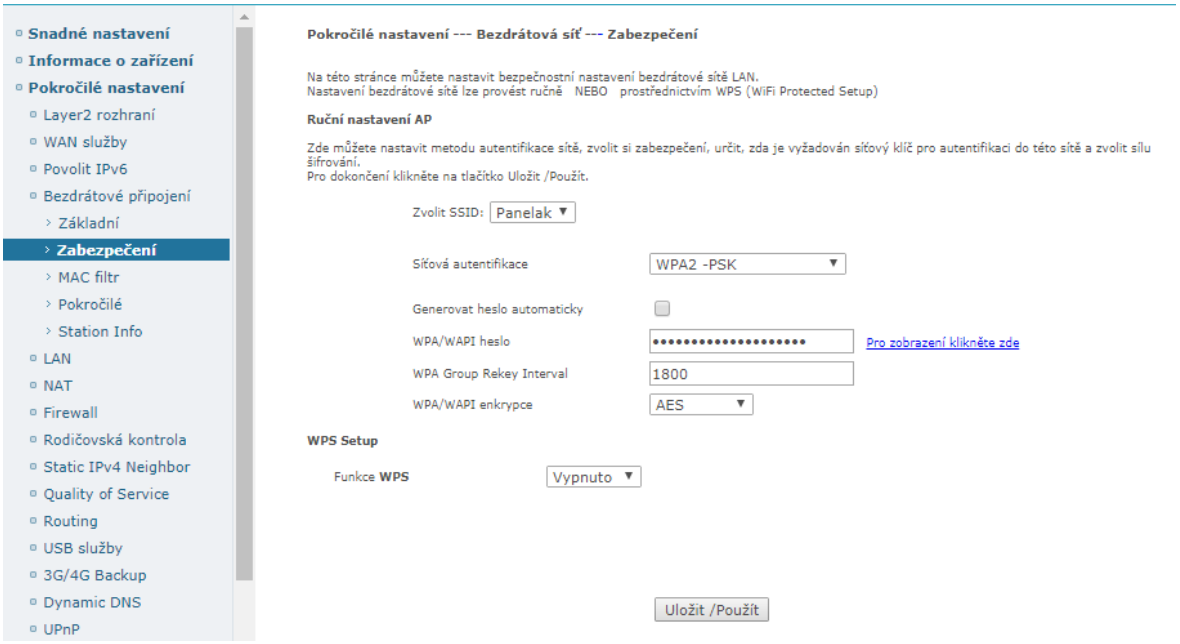


Obrázek 37 Změna hesla

Po změně přihlašovacích údajů může uživatel zabezpečit jeho bezdrátové připojení (wi-fi), které může být použito ke změně jeho DNS serverů. Prvním krokem by mělo být vypnutí vysílání SSID (název sítě uživatele), což znamená, že se jeho síť nebude zobrazovat všem zařízením, která budou v okolí hledat wi-fi připojení. Tuto akci lze provést v oddíle „Pokročilé nastavení“ → „Bezdrátové připojení“ → „Základní“, a zaškrtnutím položky „Skryté“ (Obrázek 38).



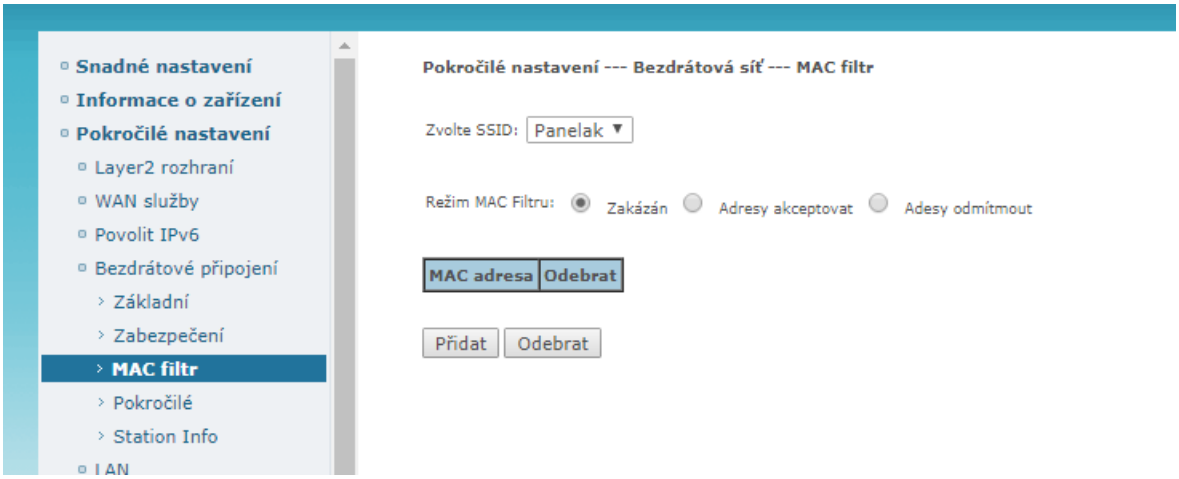
Obrázek 38 Základní nastavení bezdrátové sítě



Obrázek 39 Nastavení zabezpečení bezdrátové sítě

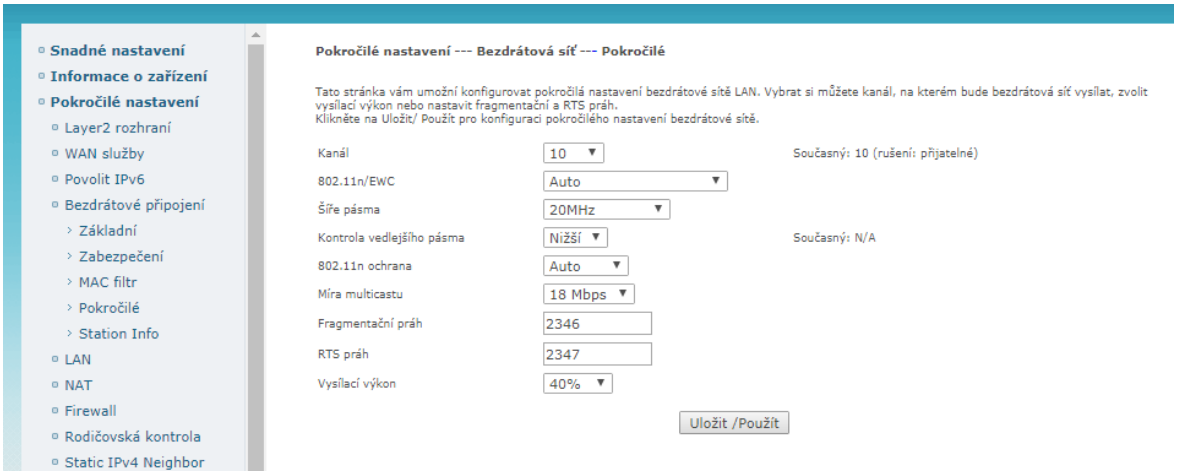
Uživatel provede nastavení zabezpečení wi-fi sítě (Obrázek 39), konkrétně způsob síťové autentizace, heslo, šifrování, funkci WPS (není doporučeno ji používat, protože již není bezpečná).

Následně přejde na položku „MAC filtr“, kde zadá MAC adresy zařízení, které se k wi-fi budou moci připojit (Obrázek 40).



Obrázek 40 Nastavení MAC adres

Jako poslední může přejít na oddíl „Pokročilé nastavení“ (Obrázek 41) a snížit vysílací výkon. To znamená, že omezí dosah wi-fi signálu, aby se dalo k wi-fi připojit jen z určitého prostoru, například jen z konkrétního bytu.



Obrázek 41 Nastavení síly signálu bezdrátové sítě

Tato opatření mohou být použita k zabezpečení modemu, aby se k němu útočník nepřipojil a nemohl změnit adresu DNS serveru. Samozřejmě může být ke kontrole stránek využívána již výše zmíněná aplikace IP Address and Domain Information, která dokáže (bez ohledu na to, jestli uživateli ve směrovači útočník vyměnil adresy DNS serveru) rozpoznat, jestli je daná stránka podvodná nebo ne.

6 ZHODNOCENÍ

Tato kapitola hodnotí účinnost nástrojů kybernetické obrany popsaných v praktické části. Hodnotícími kritérii jsou cena, náročnost implementace a účinnost na stupnici 1 - 5, přičemž 1 znamená velmi dobrá a 5 znamená velmi špatná. Posledním kritériem je úroveň znalostí uživatele, která je důležitá pro efektivní použití daného nástroje. Toto hodnocení vychází z autorových zkušeností s prací s danými nástroji, a je tedy čistě subjektivní.

6.1 Dvoufázové ověření

Cena: 1

Náročnost implementace: 4

Účinnost: 1

Úroveň: Uživatelská

Jedná se o bezplatné a velmi účinné zabezpečení účtu od společnosti Google proti útoku hrubou silou, je však náročnější na implementaci. Toto zabezpečení ovšem vyžaduje účast třetích stran – v testovaném případě mobilního telefonu. Pokud by tedy někdo daný telefon odcizil, stala by se tato obrana irelevantní.

6.2 ProtonVPN

Cena: 1 (záleží na tarifu)

Náročnost implementace: 4

Účinnost: 1

Úroveň: Uživatelská

VPN je účinné řešení proti odposlechu datové komunikace, funguje však jen v komunikaci mezi uživatelem a serverem. Pokud je uživatel odposloucháván pomocí softwaru, který už měl nainstalovaný v počítači, pak je tato ochrana neúčinná.

6.3 SpyShelter Anti-Keylogger

Cena: 4

Náročnost implementace: 1

Účinnost: 3

Úroveň: Pokročilý

Cenově nákladnější program, který chrání počítač před různými typy keyloggerů, pravidla pro ochranu proti nim však tvoří z větší části uživatel – účinnost ochrany tedy záleží i na gramotnosti uživatele. Tento program keyloggery jen vyhledává, neodstraňuje je.

6.4 IDN Safe

Cena: 1

Náročnost implementace: 1

Účinnost: 3

Úroveň: Pokročilý

Jedná se o program implementovaný do prohlížeče Chrome, účinnost záleží stejně jako v případě SpyShelter Anti-Keylogger programu na gramotnosti uživatele. Pokud např. uživatel chybně vyhodnotí míru rizikovosti webových stránek, umožní tím útočníkovi přístup ke svým datům.

6.5 IP Address and Domain Information

Cena: 1

Náročnost implementace: 1

Účinnost: 3

Úroveň: Pokročilý

Jednoduchý program implementovaný přímo do prohlížeče Chrome, ale jeho účinnost jako ve výše zmíněných případech SpyShelter Anti-Keylogger a IDN Safe záleží výhradně na uživatelově schopnosti správně interpretovat získaná data.

Otestováním jednotlivých nástrojů bylo zjištěno, že řešení zabezpečení proti útoku hrubou silou a odposlechu datové komunikace jsou náročné z hlediska procesu implementace (nutnost založení účtu ve službě, instalace aplikací třetích stran), po úspěšné implementaci však nejsou většinou nutné žádné další větší zásahy vyžadující pokročilou znalost dané problematiky ze strany uživatele.

Na rozdíl od dvou výše zmíněných řešení, otestováním nástrojů SpyShelter Anti-Keylogger, IDN Safe a IP Address and Domain Information bylo zjištěno, že tyto nástroje

jsou nenáročné na implementaci (implementačními kroky jsou pouze instalace nástroje a jeho následné spuštění), ale jejich účinnost je přímo odvozena od úrovně uživatelových znalostí – pokud není uživatel schopen na základě analýzy poskytnutých dat správně vyhodnotit míru rizika, stávají se tyto nástroje značně neefektivními.

ZÁVĚR

Teoretická část této bakalářské práce byla zaměřena na historii kyberkriminality, jak souvisí s pojmem kyberprostor, pojmy hackerská etika a hacker. Dále byly zmíněny kyberkriminální techniky jako sociální inženýrství, phishing, pharming, a další. V závěru teoretické části byly uvedeny specifické případy kyberkriminality, konkrétně kyberšikana, kyberstalking, kybergrooming a krádež identity.

Praktická část definovala způsoby, jak se bránit v teoretické části zmíněným kyberkriminálním technikám. Tyto způsoby byly otestovány z hlediska efektivity a zhodnoceny v závěru praktické části. Tato práce si kladla za cíl informovat o nebezpečí kyberkriminality a seznámit uživatele s teoretickými poznatky, které by jim umožnily uvědomit si přítomnost hrozby těchto útoků, a ukázat jim, jak je tomuto nebezpečí možné předcházet.

S neustále se vyvíjejícími technologiemi roste i míra kyberkriminality, a to nejen lokálně, ale i globálně. Vznikají tak nové způsoby páchání trestné činnosti. Je tedy možné, že možnosti obrany proti útokům, které jsou popsány v této práci v roce 2018, již nemusí např. v roce 2022 fungovat.

Pro uživatele je tedy nezbytné sledovat vývoj kyberkriminality, aby byli připraveni ochránit svá zařízení před novými hrozbami. Bohužel díky rychlému vývoji technologií to uživatelé nebudou mít vůbec jednoduché, protože vždy vznikne nejdříve hrozba a teprve po jejím vzniku mohou uživatelé hledat vhodné zabezpečení proti této hrozbě. To znamená, že útočníci budou před uživateli vždy o krok vpřed.

Ne všechny kriminální činnosti v rámci kyberkriminality jsou závislé na technologiích. Někdy útočníci těží jen z lidské nevědomosti nebo nepozornosti. Uživatel tedy musí být obezřetný nejen k novým technologiím, ale hlavně k informacím, které se k němu dostanou. Protože díky informacím může útočník zmanipulovat uživatele, aby udělal věci, které by za normálních okolností neudělal. Uživatelé se tedy nechají zmanipulovat útočníky jen proto, že nemají dostatek informací, ze kterých by poznali, že je jimi manipulováno.

Jedinou obranou jsou vědomosti, je tedy nutné se neustále vzdělávat, aby útočníci nemohli využít naší nevědomosti ke svému obohacení.

SEZNAM POUŽITÉ LITERATURY

[1] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2.

[2] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

[3] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017, ix, 135. Právní monografie. ISBN 978-80-7552-758-5.

[4] *Kyberkriminalita* [online]. [cit. 2018-08-18]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska

[5] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 8088168155.

[6] *Kyberkriminalita* [online]. [cit. 2018-08-18]. Dostupné z: http://www.policie.cz/clanek/kyberkriminalita.aspx

[7] *Hackerská etika* [online]. [cit. 2018-08-18]. Dostupné z: https://www.root.cz/clanky/hacker-kdo-to-je/

[8] *Dělení hackerů* [online]. [cit. 2018-08-18]. Dostupné z: https://www.chip.cz/casopis-chip/earchiv/vydani/r-2012/chip-03-2012/svet-hackeru/

[9] *Sociální inženýrství* [online]. [cit. 2018-08-18]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

[10] *Security-Portal* [online]. [cit. 2016-11-26]. Dostupné z: http://www.security-portal.cz/clanky/hesla-bruteforce

[11] *Útok hrubou silou* [online]. [cit. 2018-08-18]. Dostupné z: https://www.hackingkurzy.cz/blog/brute-force-utok-na-hesla-hrubou-silou/

[12] *ITBIZ* [online]. [cit. 2016-11-26]. Dostupné z: http://www.itbiz.cz/sniffing-odposlech-datove-komunikace

[13] *Paketový sniffing* [online]. [cit. 2018-08-18]. Dostupné z: http://cs.howtodou.com/common-network-attack-strategies-packet-sniffing

[14] *SOOM* [online]. [cit. 2016-11-26]. Dostupné z: http://www.soom.cz/clanky/1128--Man-in-the-middle-utok-v-C-ARP-poisoning-1

[15] *ARP poisoning* [online]. [cit. 2018-08-18]. Dostupné z: https://www.techopedia.com/definition/27471/address-resolution-protocol-poisoning-arp-poisoning

[16] *Síťový analyzátor* [online]. [cit. 2018-08-18]. Dostupné z: https://fluketestery.cz/produkty/sitovy-analyzator-ov3_ina-13.html

[17] *Computer Hope* [online]. [cit. 2016-11-26]. Dostupné z: http://www.computerhope.com/jargon/m/mitma.htm

[18] *Broadcast* [online]. [cit. 2018-03-02]. Dostupné z: https://it-slovnik.cz/pojem/broadcast

[19] *Správa sítě* [online]. [cit. 2016-11-26]. Dostupné z: http://www.sprava-site.eu/backdoor/

[20] *Backdoor* [online]. [cit. 2018-08-18]. Dostupné z: https://it-slovnik.cz/pojem/backdoor

[21] *Správa sítě* [online]. [cit. 2016-11-26]. Dostupné z: http://www.sprava-site.eu/keylogger/

[22] *Keylogger* [online]. [cit. 2018-08-18]. Dostupné z: https://it-slovnik.cz/pojem/keylogger

[23] *Správa sítě* [online]. [cit. 2016-11-26]. Dostupné z: http://www.sprava-site.eu/hoax/

[24] *NEBUĎ OBĚŤ* [online]. [cit. 2016-11-26]. Dostupné z: http://www.nebudobet.cz/?cat=hoax

[25] *Hoax* [online]. [cit. 2018-08-18]. Dostupné z: https://www.techopedia.com/definition/27330/email-hoax

[26] *Správa sítě* [online]. [cit. 2016-11-26]. Dostupné z: http://www.sprava-site.eu/phishing/

[27] *Hoax* [online]. [cit. 2016-11-26]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[28] *Phishing* [online]. [cit. 2018-08-18]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2325-phishing-stale-aktualni-hrozba/

[29] *Hoax* [online]. [cit. 2016-11-26]. Dostupné z: http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=522

[30] *Správa sítě* [online]. [cit. 2016-11-26]. Dostupné z: http://www.sprava-site.eu/pharming/

[31] *Cybre Secure Asia* [online]. [cit. 2016-11-26]. Dostupné z: https://www.cybersecureasia.com/blog/phishing-and-pharming

[32] *Phishing* [online]. [cit. 2018-08-18]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2325-phishing-stale-aktualni-hrozba/

[33] *DDoS* [online]. [cit. 2016-11-26]. Dostupné z: https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/

[34] *DDoS* [online]. [cit. 2018-08-18]. Dostupné z: https://diit.cz/clanek/co-to-je-ddos-utok-a-jak-se-dela

[35] *Botnets: Measurement, Detection, Disinfection and Defence* [online]. [cit. 2018-03-06]. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

[36] MARTÍNEK, Zdeněk. *Agresivita a kriminalita školní mládeže*. 2., aktualizované a rozšířené vydání. Praha: Grada, 2015, 190 s. Pedagogika. ISBN 978-80-247-5309-6.

[37] *Kybergrooming* [online]. [cit. 2018-08-18]. Dostupné z: https://bezpecne-online.saferinternet.cz/pro-rodice-a-ucitele/teenageri-a-komunikace/item/35-co-je-to-kybergrooming

[38] *Kyberšikana* [online]. [cit. 2018-08-18]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

[39] *Krádež identity* [online]. [cit. 2018-08-18]. Dostupné z: http://www.policie.cz/clanek/ztrata-identity.aspx

[40] *Kyberstalking* [online]. [cit. 2016-11-26]. Dostupné z: https://www.jdidoklubu.cz/Kyberstalking-Nebezpecne-pronasledovani-P7027602.html

[41] *Kyberstalking* [online]. [cit. 2018-08-18]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/stalking-a-kyberstalking/66-23

[42] *Nejhorší hesla* [online]. [cit. 2018-04-30]. Dostupné z: https://jablickar.cz/toto-jsou-ta-nejhorsi-hesla-ktera-se-v-roce-2017-pouzivala/

[43] *Testování hesel* [online]. [cit. 2018-04-30]. Dostupné z: https://www.betterbuys.com/estimating-password-cracking-times/

[44] *Protokol PPTP* [online]. [cit. 2018-08-03]. Dostupné z: https://www.ivpn.net/pptp-vs-l2tp-vs-openvpn

[45] *Protokol PPTP,L2TP* [online]. [cit. 2018-08-03]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771298(v=ws.10)

[46] *OpenVPN* [online]. [cit. 2018-08-03]. Dostupné z: https://www.purevpn.com/openvpn

[47] *L2TP* [online]. [cit. 2018-08-03]. Dostupné z: https://www.purevpn.com/l2tp-vpn

[48] *PPTP* [online]. [cit. 2018-08-03]. Dostupné z: https://www.purevpn.com/pptp-vpn

[49] *OpenVPN* [online]. [cit. 2018-08-03]. Dostupné z: https://cs.vpnmentor.com/blog/srovnani-vpn-protokolu-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

[50] *ProtonVPN* [online]. [cit. 2018-08-03]. Dostupné z: https://account.protonvpn.com/signup

[51] *Dvoufázové ověření* [online]. [cit. 2018-08-13]. Dostupné z: https://lh3.googleusercontent.com/SClWEmbk7QxxuKiWshok2T45vAwEQYCduisnnGORqrha7KfpQsvFZa0xac_jyj_tE9Mn=w1024-h631-rw

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČR	Česká Republika
SMS	Short message service
gbps	Gigabites per second
DDoS	Distributed Denial of Service
DoS	Denial of Service
DNS	Domain Name System
IP	Internet Protocol
URL	Uniform Resource Locator
PIN	Personal Identification Number
ARP	Address Resolution Protocol
MAC	Media Access Control
ASCII	American Standard Code for Information Interchange
GNU	GNU is Not UNIX
C&C	Command-and-Control
kps	KeysPerSecond
VPN	Virtual Private Network
JPEG	Joint Photographic Experts Group
SSID	Service set identifier

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ODKAZY KE STAŽENÍ POUŽITÝCH NÁSTROJŮ

Google Authenticator – jedná se o program od společnosti Google, který slouží ke generování číselných kódů pro účely dvoufázového ověření. Je zdarma ke stažení na adrese https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=cs

VPN klient – program od společnosti ProtonVPN, který slouží k šifrovanému spojení mezi uživatelem a VPN serverem. Jeho stažení je zdarma, avšak některé jeho možnosti jsou zpřístupněny až po vybrání a zaplacení jednoho z placených tarifů. Lze jej stáhnout na adrese https://protonvpn.com/download/

SpyShelter Anti-Keylogger – software od společnosti SpyShelter, sloužící k ochraně počítače proti škodlivým programům, konkrétně keyloggerům. Jedná se o placenou verzi, kde licence platí jeden rok. Na adrese https://www.spyshelter.com/download-spyshelter/ si uživatelé mohou stáhnout trial verzi, kterou lze vylepšit na plnou verzi zadáním sériového klíče.

IDN Safe – jedná se o rozšíření internetového prohlížeče. Slouží k blokování webových stránek, které mají ve svých adresách „punycode“. V prohlížeči Chrome jej lze najít v internetovém obchodě Chrome.

IP Address and Domain Information – jako v případě IDN Safe, je IP Address and Domain Information rozšíření internetového prohlížeče. Zobrazuje informace o právě otevřených stránkách. Rovněž je k dispozici v internetovém obchodě Chrome.