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: **1. prosince 2017**

Termín odevzdání bakalářské práce: **25. května 2018**

Ve Zlíně dne 14. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

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

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 22. 05. 2018

Žlučka
.....
podpis diplomanta

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, jak funguje útok hrubou silou, důležitost dobře zvolených hesel, a funkčnost mechanizmů, které mohou být použity k dodatečnému zabezpečení proti tomuto útoku.

Klíčová slova: hacker, útok hrubou silou, odposlech komunikace, zadní vrátka, keylogger, hoax, „rybaření“, „farmaření“, distribuované odmítnutí služby, kybergrooming, kyberšikana, krádež identity, kyberstalking, Wireshark, 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 cyber-crime 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 cybercriminal techniques, such as social engineering, phishing, pharming, and others, and deals with what users should be careful about to see if phishing or pharming is suspected.

There is also mentioned what a hoax is, 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. 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 attack by brute force works, the importance of well-chosen passwords and the functionality of the mechanisms that can be used to provide additional security against this attack.

Keywords: hacker, brute force, sniffing, back door, keylogger, hoax, phishing, farming, DDoS, cyber grooming, cyber bullying, identity theft, cyber stalking, Wireshark, VPN

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

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

OBSAH

ÚVOD

Problematika kybernetické kriminality je v dnešní době více než aktuální, 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, a právní normy upravující 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, otestovat, jak funguje útok hrubou silou, důležitost dobře zvolených hesel, a funkčnost mechanizmů, které mohou být použity k dodatečnému zabezpečení proti tomuto útoku. Kapitola odposlech datové komunikace pojednává o způsobech odchytávání paketů ze síťového provozu, jakým způsobem z těchto paketů získat informace, a jak používání VPN zabraňuje ve sledování síťového provozu. Pátá kapitola se zabývá 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. Jako poslední je zde řešena prevence proti kyberšikaně, jak se mohou chovat oběti nebo pachatelé kyberšikany a co dělat, když se s ní uživatelé setkají.

Tato práce si klade 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 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 to vypadalo, 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, která měla zahrnovat všechny trestné činy, ve kterých počítač figuruje jako nástroj nebo předmět použitý při trestném činu. Ke spáchání takových trestných činů, ale bylo zapotřebí mít znalosti z výpočetní techniky nebo informatiky, proto bylo navrženo slovní spojení kriminalita v informatice. [1], [2]

Následný rozvoj elektroniky a mikroprocesorů ale vedl k jiným zařízením (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-komunikační technologie. Dnes je nejznámější komunikační sítí internet, který poskytuje různé způsoby komunikace a služby. Vzhledem k tomu vzniklo hned několik označení pro trestné činy provedené na internetu – internetová kriminalita, e-kriminalita, virtuální kriminalita nebo kriminalita na počítačových sítích. [3]

V roce 2001 vznikla tzv. budapešťská úmluva, 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 k jejich zneužívání. Proto neexistuje univerzální definice, která by zcela vysvětlovala pojem kyberkriminalita, teoreticky ani legislativně. [3]

Jsou však organizace, které se o to snaží a 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 kdy je počítač použit jako nástroj pro spáchání trestného činu. Zásadní podmínkou pro použití této definice je, že se spáchání trestného činu odehrává v kyberprostoru. Při definici 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 toto chování může být pro společnost nebezpečné. Jednání, která nemohou být kvalifikována jako kyberkriminalita nebo jakákoliv jiná

kriminalita, se za kriminalitu nepovažují. Když 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]

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 se dále může rozdělovat na podmnožiny, které se můžou 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]

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 součásti počítače jako zbraň. [4]

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]

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 emailových 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, ve kterém byly použity prostředky ICT, se dá označit jako počítačová kriminalita. [4]

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]

1.1 Klasifikace forem kyberkriminality

Obecně se může kyberkriminalita klasifikovat jako jednání, které je namířeno proti počítači, počítačovým sítím, nebo 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 směrována trestná činnost, nebo se použije jako nástroj k páchání trestné činnosti. V druhém bodě se posuzují typy trestných činů, rozdělují se 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. [4]

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. [4]

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. [4]

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. [4]

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.“ [4]

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 systému 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], [4]

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. [4]

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. [4]

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. [4]

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. [4]

3 KYBERKRIMINÁLNÍ TECHNIKY

Útočník často používá pro úspěšné dosažení svých cílů různé specifické techniky a postupy, které se označují jako kybernetický útok. Mezi ty nejvíce známé metody způsobu hackerské práce patří:

3.1 Sociální inženýrství

Sociální inženýrství jako takové nelze považovat za kybernetický útok, ale je to základ 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“. [4]

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. [4]

3.2 Útok hrubou silou (Brute force)

Útok hrubou silou spočívá v tom, že se útočník snaží zjistit uživatelské jméno a heslo, nebo jenom heslo, pomocí kombinace daných znaků. Dělá to tak, že si zvolí počet znaků, neboli jak dlouhé dané heslo asi bude, jejich typ (písmena, číslice, atd…) a pak provádí jejich kombinace. Následně pak zkouší, jestli některý výsledek neodpovídá parametrům hesla. [5]

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) 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 běžná velikost osm, celkové množství kombinací je asi 282 miliard. Takže je šance 1 ku 282 miliardám, že toto heslo někdo

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 psa, nebo je heslo stejné jako uživatelské jméno apod., je velká pravděpodobnost, že toto heslo někdo prolomí. [5]

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. [5]

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. [6]

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 běžně je to nemožné. [6]

Zjištění těchto síťových analyzátorů v uživatelově síti je téměř nemožné, protože tyto softwarové systémy jsou pasivní. Jen 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. [6]

Bohužel jako běžný uživatel s tím nic neudělá, jediné co lze dělat je šifrovat danou komunikaci, aby i když jej odposlouchávají, nemohli nic zjistit. [6]

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. [7]

Obrázek 1 Man in the middle schéma [8]

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 [9] 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, tak si tuto adresu uloží do tzv. ARP cache. Tato ARP cache má podobu tabulky, kde je IP adrese přiřazena fyzická adresa. [7]

```
Rozhraní: 10.0.0.2 --- 0xa
  internetová adresa     fyzická adresa         typ
  10.0.0.5               c0-38-96-47-2c-eb      dynamická
  10.0.0.138             5c-f4-ab-1b-6a-c8      dynamická
  10.0.0.255             ff-ff-ff-ff-ff-ff      statická
```

Obrázek 2 ARP tabulka [34]

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. A tomu se říká ARP poisoning. [7]

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. [7]

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 a jeho majitel si ničeho nevšimne. 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. [10]

Zadní vrátka v systému může vytvořit například virus trojský kůň, ale jsou toho schopny i jiné druhy malwaru. Konkrétně určité druhy tzv. červů. [10]

3.5 Keylogger

Jedná se o program, který zachycuje všechno, co napíšeme na klávesnici a ukládá to do textového souboru. Ten pak posílá útočníkovi, který ze souboru zjistí heslo do internetového bankovnictví, na sociální sítě, emailovou schránku apod.. Nositelem takového programu je obvykle trojský kůň. [11]

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. [11]

3.6 Hoax

Jako Hoax se označuje zpráva, která je mystifikující a nepravdivá. Nejčastěji se šíří formou emailu, 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). [12]

Proč někdo hoaxy vůbec vytváří? Každý chce dosáhnout něčeho jiného, například vyvolat strach, manipulovat s názory lidí, poškodit instituci, značku, firmu, výrobek, vylákat peníze, nebo si prostě udělat legraci z důvěřivých uživatelů. [13]

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 informace o času, místě, osobě, nebo uměle vytvořený obrázek. 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, klidně ji lze smazat. [13]

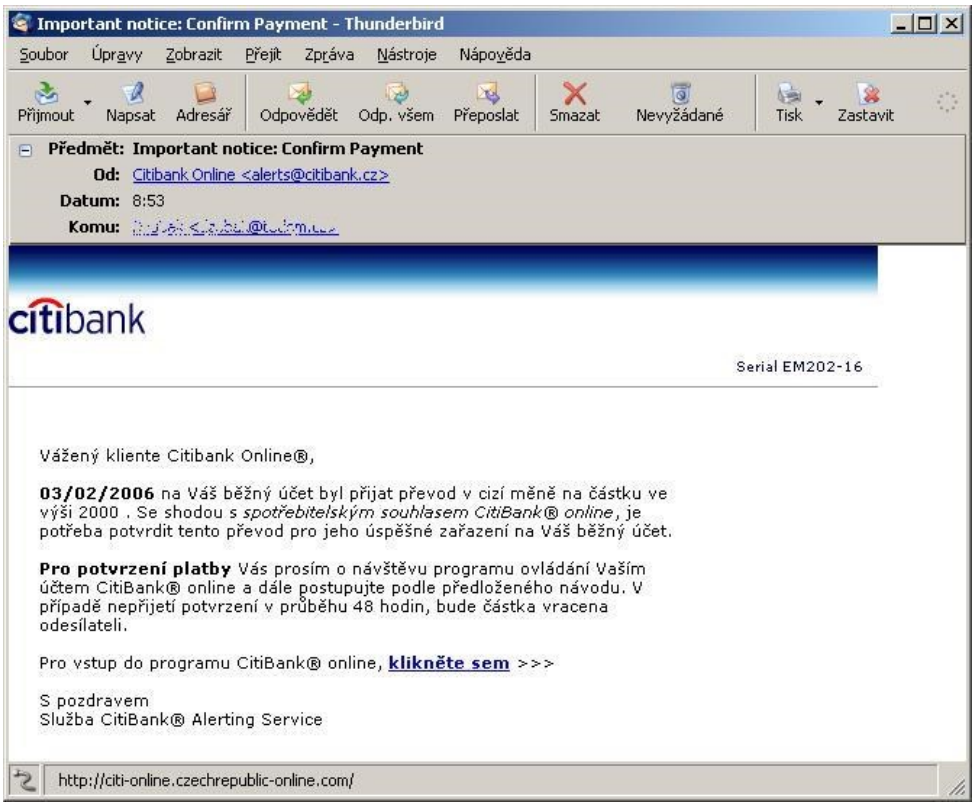
V čem jsou takové zprávy nebezpečné? V nejhorším případě pokud zprávě uživatel uvěří, může se na něm daná osoba obohatit. Pokud se uživatel v takové situaci ocitne, je nejlepším řešením obrátit se na Policii ČR. V tom lepším případě utrpí jen jeho pověst. [13]

3.7 Rybaření (Phishing)

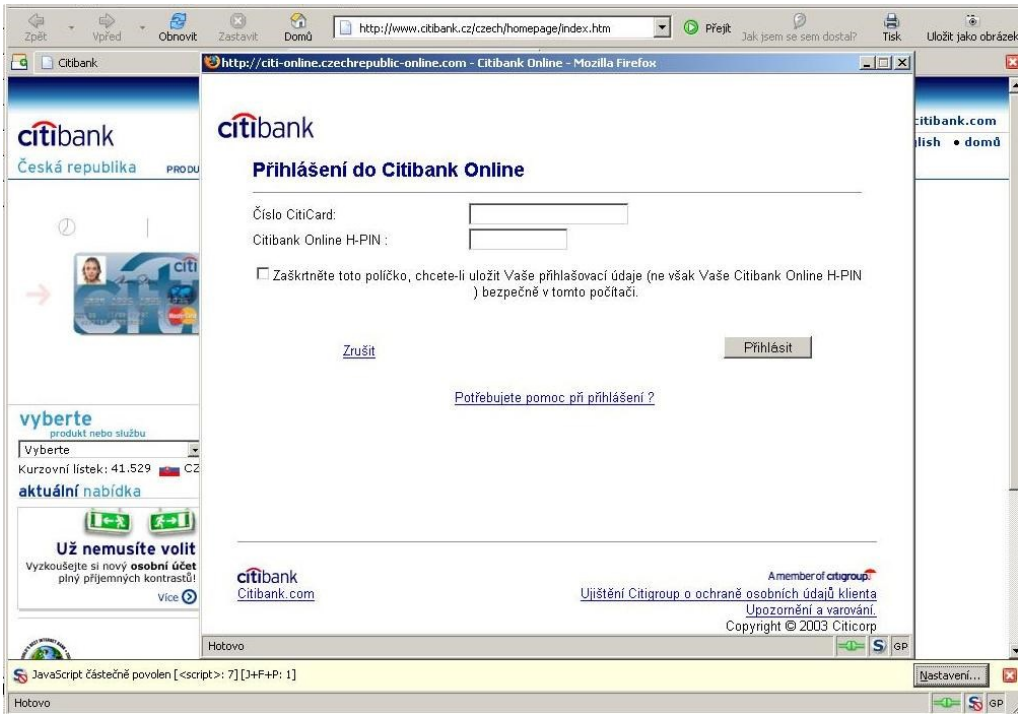
Rybaření spočívá v tom, že útočník odešle podvodný email za účelem vylákání citlivých údajů od nezkušených uživatelů. Až tento email odešle, tak jen čeká, až se někdo chytne, jako rybář na rybu. Samotný email se tváří, že je z důvěryhodného zdroje, například internetový obchod, banka nebo i policie. V sobě pak má odkaz, který uživatele přesměruje na stránky útočníka, kde po něm chce zadat přihlašovací údaje do internetového bankovnictví nebo PIN a číslo platební karty.[14]

Jak se bránit? Pokud uživatel obdrží podobný email, zcela určitě se jedná o pokus z něj vylákat jeho údaje, protože banky takové emaily 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.[15]

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



Obrázek 3 Podvodný email [16]



Obrázek 4 Podvodné přihlašovací okno [16]

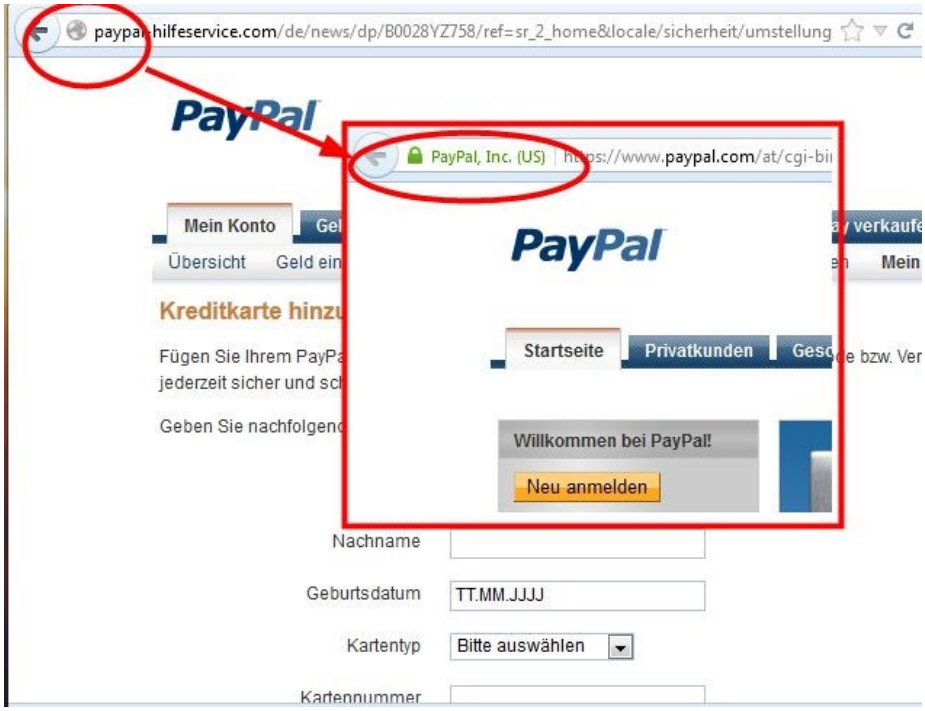
Po kliknutí na odkaz v obrázku 3 se sice uživatel dostane na skutečné stránky společnosti Citibank, ale zároveň se otevře i okno, které vyžaduje zadání důvěrných informací, jak lze vidět na obrázku 4.

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 fishingu. Už nepoužívá podvodné emaily, 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.[17]

Takové podvodné stránky lze poznat například tak, že po uživateli chtějí údaje, které předtím nikdy nechtěly. Jestliže toto uživatel zpozoruje, pak by měl okamžitě operaci ukončit a kontaktovat klientské centrum své banky. Na možné zneužití může upozorňovat i řádek s URL adresou vlevo nahoře v jeho prohlížeči. Například tím, že adresa začíná http:\\ místo https:\\. Příklad takové stránky je na níže uvedeném obrázku. [18]



Obrázek 5 Příklad farming stránky [18]

3.9 Distribuované odmítnutí služby (DDoS)

Podstatou DoS a DDoS útoků je znepřístupnit 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. [19]

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 říká i zombie army). Zařízení v botnetu většinou nepatří útočníkům, ale byly napadeny a útočníci je jen využívají. [19]

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 potom, co přidali společnost Cyberbunker na spam blacklist (seznam, který společnost Spamhouse poskytuje poskytovatelům emailových 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. Jeden 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, ale za oběť jim mohou padnout i telefony nebo telefonní systémy. [19]

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. [4]

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, až se dané části zpracují, počítače je odešlou do centra řízení dané úlohy, kde se opět spojí v jeden celek. [4]

Samozřejmě lidé jsou 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. [4]

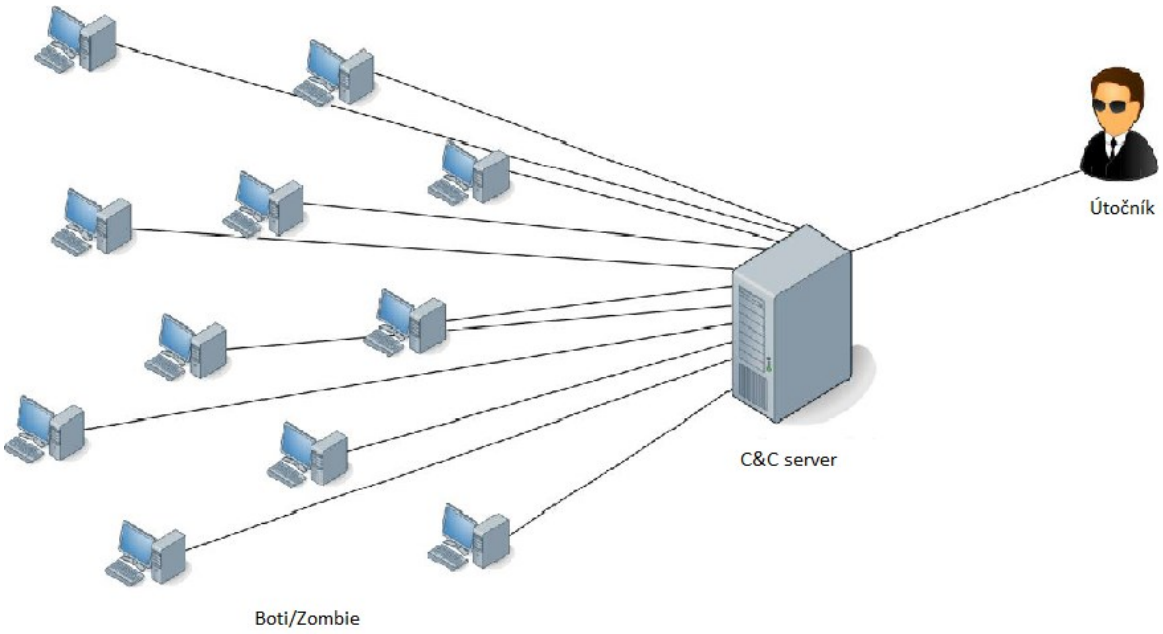
Aby mohl být systém označen za botnet musí mít následující prvky:

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. [4]

Dále botnety můžeme rozdělit podle architektury na:

1. **Centralizovanou architekturu**

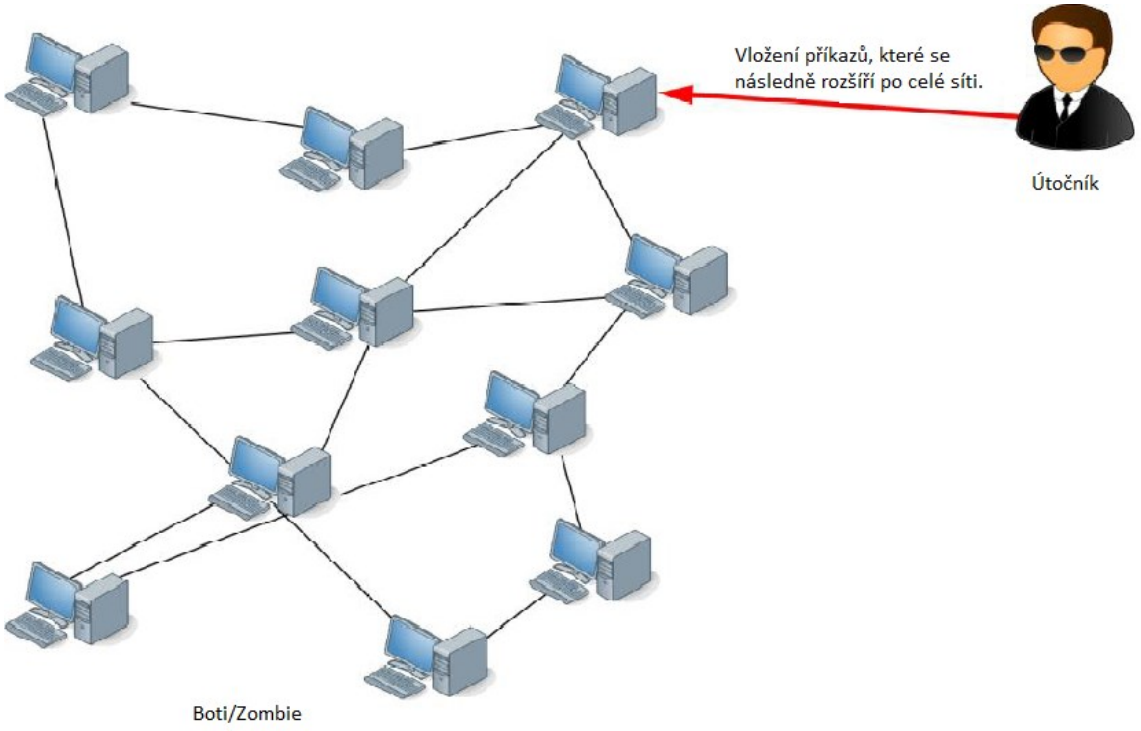
   Tato architektura pracuje na principu klient-server, to znamená, že koncové počítače (zombie/boti) komunikují přímo s C&C (centrální řídící prvek), plní jeho instrukce a využívají jeho zdroje. Zmíněná architektura je zobrazena na níže uvedeném obrázku. [4]



Obrázek 6 Centralizovaná architektura botnetu [20]

2. **Decentralizovaná architektura**

   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. [4]



Obrázek 7 Decentralizovaná architektura botnetu [20]

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.“ [21]

4.2 Kyberšikana (cyberbullying)

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

Jedním z problémů je, že děti a mladí lidé, kteří ICT takto využívají, to považují za zábavu a vůbec si neuvědomují, co tím mohou způsobit.

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. [21]

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 emailovou 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, emailu, 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 dostat 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. Takové 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, to 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. [21]

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, emailem 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) 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 „Nejlepší facka roku, kdo souhlasí palec nahoru“, „Měl dostat víc“, atd. [21]

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 emailové adresy. Tím, že útočník má přístup do emailové 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. [4]

4.4 Kyberstalking (cyber stalking)

Jedná se o posílání zpráv obtěžujícího nebo výhružného charakteru formou SMS, emailu, 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 emaily 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. [22]

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 chvilku ho to přestane bavit. Je tu možnost, že s tím opravdu přestane, ale taky je tu možnost, že ho to

naštve a v takovém případě by mohlo jít i o život. Proto by se takovéto situace neměly podceňovat. [22]

II. PRAKTICKÁ ČÁST

5 PREVENCE PROTI KYBER ÚTOKŮM

V této kapitole jsou rozebrána opatření proti kybernetickým útokům a způsoby, jak těmto útokům předcházet.

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 emailu a SMS zprávy po telefonní aplikaci. Tento kód se zadává až po přihlášení, takže i když útočník zná přihlašovací údaje uživatele, tak bez tohoto kódu se k jeho účtu nepřihlásí. [23]
2. **Omezení počtu pokusů na zadání hesla**
   Nejčastěji se používá v bankovních systémech, kde se po třech špatných zadáních účet zablokuje. Uživatel má tedy jen tři možnosti zadat heslo, což je v případě útoku hrubou silou nedostatečné, proto se proti bankovním institucím spíše používají útoky typu fishing nebo farming.
3. **Autorizace počítače**
   Jedná se o podobný princip jako dvoufázové ověření, v tomto případě se ale neověřují jednotlivé účty, nýbrž jednotlivé počítače. To znamená, že pokud se útočník nepřihlásí z autorizovaného počítače, tak se k danému účtu nepřihlásí. Autorizace počítače se provádí zadáním kódu, který dostaneme buď z emailové adresy nebo z mobilní aplikace. [24]

Výše uvedené metody jsou relevantní, až když útočník zjistí uživatelovy přihlašovací údaje, proto je nejlepší zvolit si takové heslo, které nebude možno tímto útokem prolomit. Níže jsou rozebrána nejhorší hesla v roce 2017. [25]

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 [25]

Z toho lze usuzovat, že takové heslo nejspíše nebude 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 někdo prolomí, dostane se k několika službám najednou. Uživatelé by také neměli zapomínat, že se technologie neustále vyvíjí a heslo, které bylo bezpečné v roce 2000, už nemusí být bezpečné v roce 2017. [26]

5.1.1 Slovníkový útok

Při obraně před slovníkovým útokem se používají stejné mechanizmy jako u útoku hrubou silou. Nejspolehlivější ochranou proti tomuto typu útoku je volit taková hesla, která nic neznamenají, jelikož slovníkový útok pracuje se seznamy hesel, a není tedy možné prolomit heslo, které v tomto seznamu není.

5.1.2 Test hesel

Tato kapitola se zaměří na vyzkoušení odolnosti hesel proti útoku hrubou silou. Ukáže jak různorodost a délka hesla ovlivňuje čas, za jaký se je podaří prolomit pomocí útoku hrubou silou.

Nejdříve bude testováno heslo „123456“. Toto heslo lze prolomit útokem hrubou silou asi za dvě a půl minuty. Pokud použijeme slovníkový útok, nebude prolomení hesla trvat ani jednu vteřinu, ale pokud k heslu přidáme čísla navíc, zvýší se doba potřebná k jeho prolomení.

Heslo	Čas
123456	3 min. 12 s
1234567	1 h 55 min.
12345678	2 dny 21 h
123456789	3 měsíce 1 týden
1234567891	10 let 2 měsíce
12345678910	367 let
123456789101	13 235 let

Tabulka 2 růst časů po přidání jednoho znaku [26]

Jak můžeme vidět v tabulce 2, přidání jediného znaku k heslu výrazně zvyšuje dobu potřebnou k jeho prolomení, což znamená, že záleží jak je heslo dlouhé a čím je delší, tím je bezpečnější. Slovníkový útok není brán v potaz, k výpočtu je použito 99% výkonu procesoru Core i5-6600K. [26]

Nyní bude testováno heslo „Nqdr18y.E3PQ“ podle doporučení z předchozí kapitoly. Prolomení tohoto hesla zabere při použití stejného procesoru 1 026 997 let. Z tohoto výsledku můžeme usuzovat, že hesla vytvořená z kombinací malých písmen, velkých písmen, čísel a speciálních znaků jsou velmi účinná proti útoku hrubou silou.

Výsledky tohoto testu dokazují, že čím jsou hesla delší a různorodější (kombinace malých a velkých písmen, čísel a speciálních znaků), tím jsou bezpečnější a útočníkovi bude trvat velmi dlouho prolomit je tímto způsobem.

Výsledky dosažené v tomto testu se mohou lišit od jiných výsledků nalezených na internetu kvůli odlišným postupům při výpočtu. [26]

5.1.3 Test dvoufázového ověření

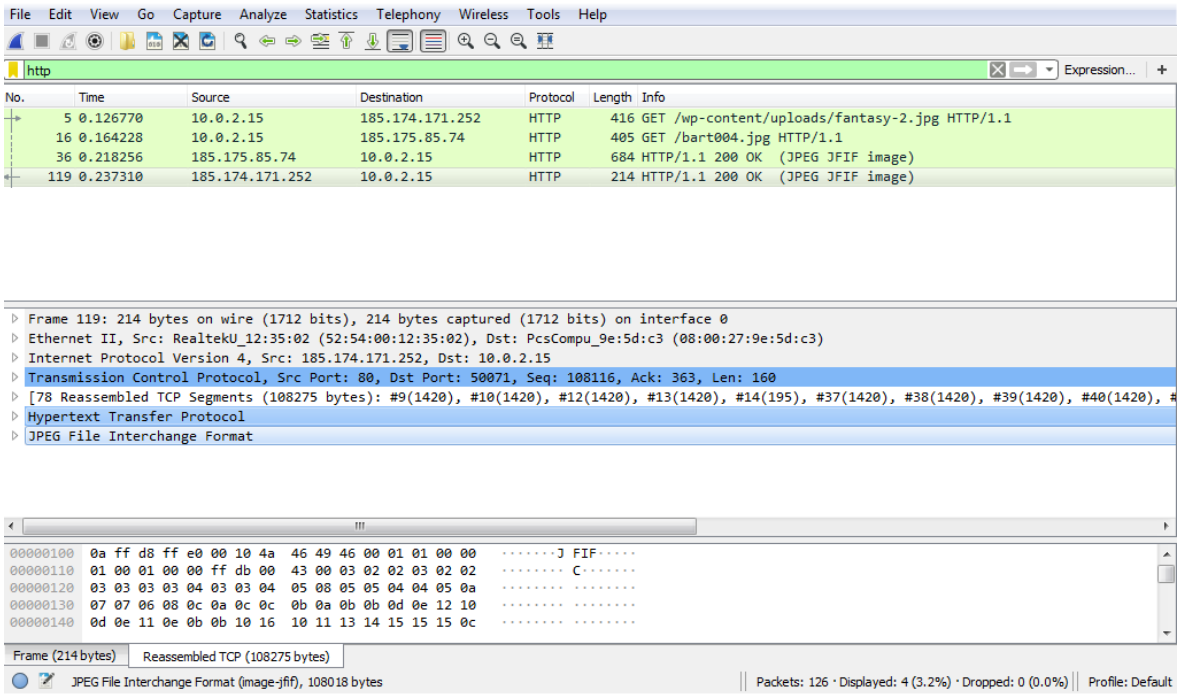
Test dvoufázového ověření provedeme na programu Uplay od firmy Ubisoft. Nainstalujeme program Uplay a povolíme v nastavení možnost dvoufázového ověřování. Program Uplay používá pro dvoufázové ověření aplikaci třetích stran, konkrétně aplikaci Google Authenticator. Následně synchronizujeme program Uplay s aplikací Google Authenticator, pokud jsme je synchronizovali správně, zobrazí se nám v aplikaci Google Authenticator šestimístný číselný kód, který je potřeba zadat do programu Uplay při každém přihlášení. Pokud se útočníkovi podaří prolomit naše přihlašovací údaje pomocí útoku hrubou silou, ale nemá přístup k šestimístnému kódu z aplikace Google Authenticator, nepodaří se mu přihlásit. Když zkusí použít stejný typ útoku k prolomení kontrolního kódu, bude tento kód útočníkovi už k ničemu, protože například prolomení kódu „759599“ bude trvat přibližně tři minuty, při použití 99% výkonu procesoru Core i5-6600K. Tento kód sice útočník zjistí, ale už je pozdě, protože kontrolní kódy se v aplikaci Google Authenticator mění každých 30 vteřin, tzn., že útočník neprolomí tyto kódy dost rychle, aby je mohl použít. Bereme v potaz pouze útok hrubou silou, nikoli útok slovníkový. [26]

Proti útoku hrubou silou je tedy tento mechanizmus účinný, ale tento mechanizmus se stává irelevantním v momentě, kdy má útočník přístup k našemu mobilnímu telefonu, ze kterého si kód opíše a nemusí ho prolomit pomocí útoku hrubou silou. Nesmíme zapomínat, že tento mechanizmus je pouhým doplňkem při obraně proti útoku hrubou silou – hlavním prvkem obrany je pořád dobře zvolené heslo.

5.2 Odposlech datové komunikace

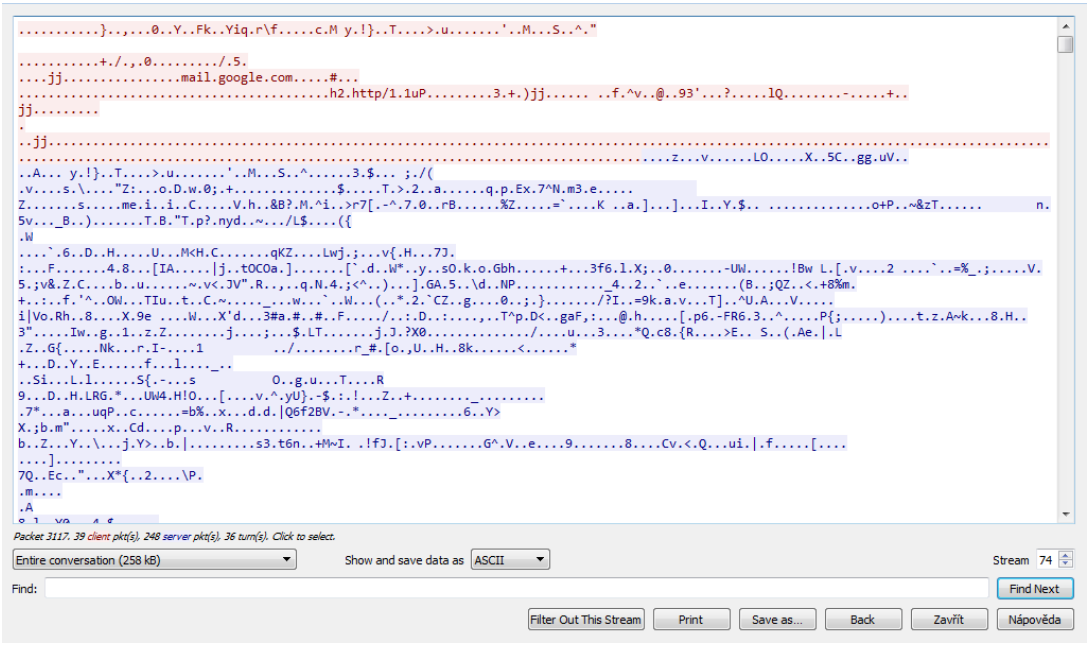
V této kapitole si ukážeme, jak můžeme použít program Wireshark k odposlechu datové komunikace. Wireshark je světově nejpoužívanější analyzátor síťových protokolů, dokáže podrobně rozebrat uživatelův provoz na síti a považuje se za standard v mnoha komerčních a neziskových organizacích, vládních agenturách a výukových ústavech. [27]

Na obrázku 8 je zobrazeno zachycení komunikace mezi klientem a serverem, konkrétně se jedná o přihlášení k emailovému účtu. Komunikace probíhá v šifrovaném protokolu https, proto, jak lze vidět na obrázku 9, se zobrazují jen nic neříkající kombinace znaků, ale v případě, že známe šifrovací klíč, je možné tyto data dešifrovat a získat z nich požadované údaje.



Obrázek 8 Wireshark zachycené pakety protokolu http

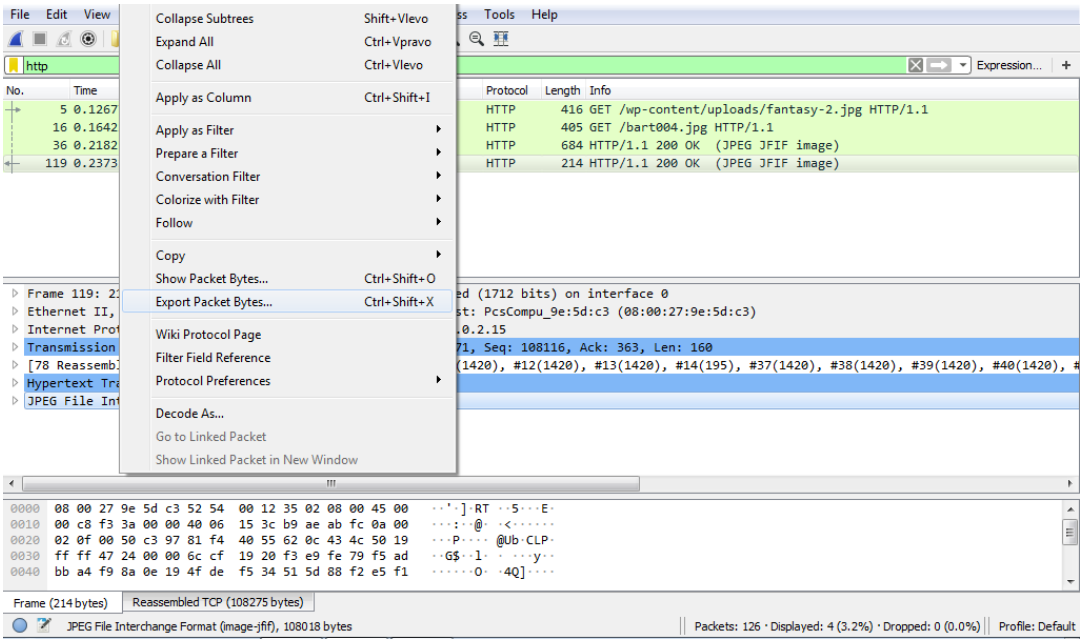
Pokud by komunikace probíhala v nešifrovaném protokolu jako Telnet nebo FTP, dalo by se z dané komunikace vyčíst uživatelské jméno a heslo, pod kterým se chceme přihlásit k danému serveru. Je tedy důležité používat šifrované protokoly, jako https, SSH a FTPS, aby tato situace nemohla nastat. To není to jediné, co se dá z odposlouchaných dat získat, například obrázky 10-13 ukazují, jak lze z odposlechnutých dat vytáhnout obrázek.



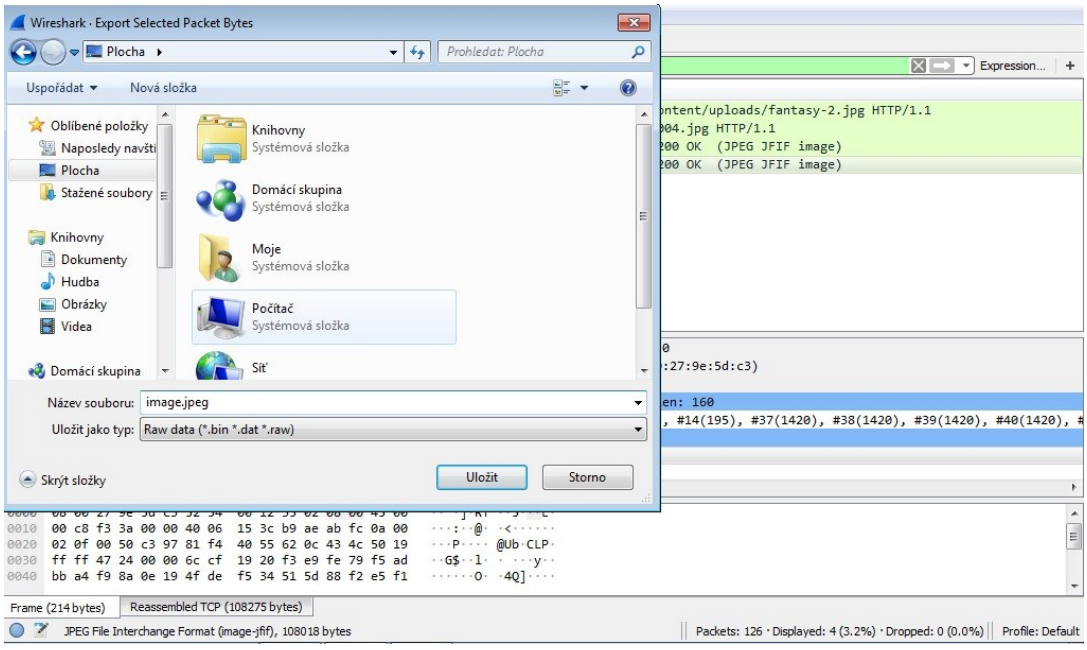
Obrázek 9 Šifrovaná data posílána přes protokol HTTP

Z obrázku 8 je patrné, že odposlechnutá data obsahují obrázek ve formátu JPEG, ale samotná zachycená data nejsou ve formátu JPEG, pro získání obrázku je tedy nutné exportovat získaná data, jak je ukázáno na obrázku 10.

K exportování obrázku, klikneme pravým tlačítkem na položku „JPEG File Interchange Format“, objeví se menu, jak je ukázáno na obrázku 10, a vybereme možnost „Export Packet Bytes“.



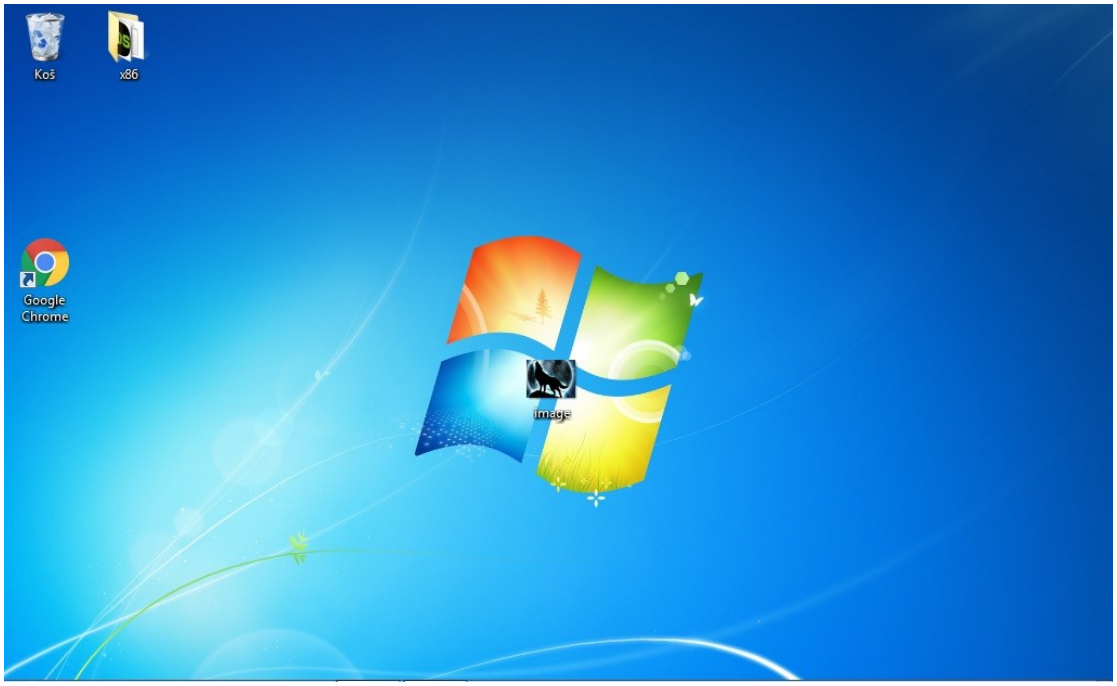
Obrázek 10 Export odposlechnutých dat



Obrázek 11 Uložení odposlechnutých dat

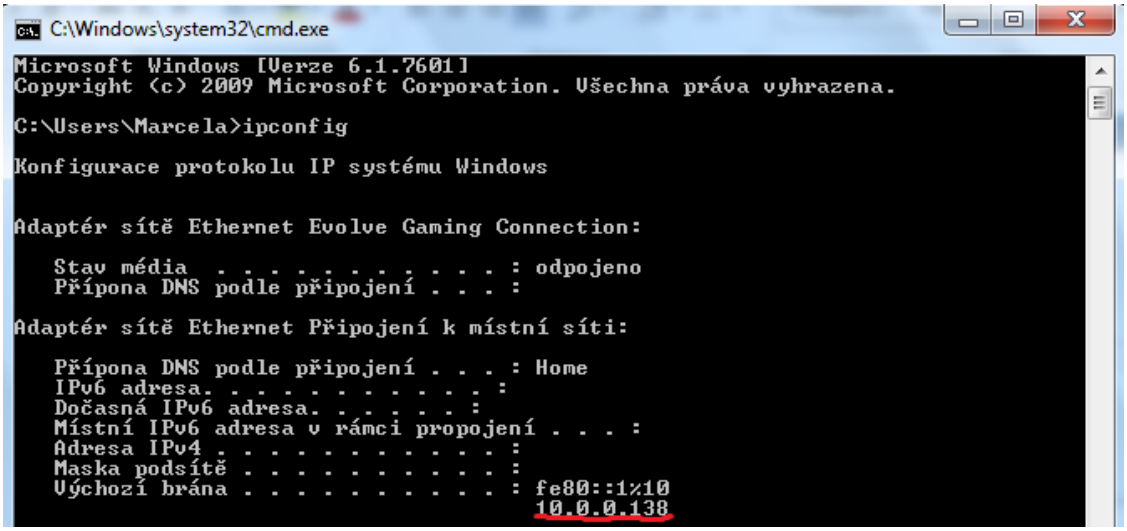
Jak vidíme na obrázku 11, exportovaná data se uloží jako „Raw data“ neboli jako pouhé bajty, proto k názvu obrázku doplníme koncovku „.jpeg“, která zajišťuje, že se budou uložené bajty číst jako obrázek.

Obrázek 12 ukazuje, že uložená data se otevírají jako obrázek ve formátu „.jpeg“.



Obrázek 11 Vyexportovaný obrázek

První, co bychom mohli udělat jako ochranu proti tomuto útoku, je změnit heslo k routeru, protože pokud je útočník schopný nás odposlouchávat to znamená, že se připojil k naší síti a mohl by se dostat k nastavení našeho routeru a pokud se tam dostane, tak jakákoliv jiná opatření jsou naprosto zbytečná. K nastavení routeru se dostaneme přes webový prohlížeč zadáním výchozí brány, která se nám zobrazuje po zadání příkazu „ipconfig“, obrázek 13.



Obrázek 12 Konfigurace protokolu IP

Na obrázku 14 je adresa 10.0.0.138, nemusí být u všech stejná, záleží na poskytovateli internetového připojení. Zadáním této adresy do webového prohlížeče budeme vyzváni k zadání uživatelského jména a hesla, standardně bývá nastaveno jméno i heslo „admin“, a takové heslo nelze považovat za bezpečné. Přihlásíme se tedy a změníme v nastavení routeru heslo na takové, které splňuje požadavky z kapitoly 5.1. Samozřejmě nesmíme zapomenout mít zapnutý firewall a aktualizovaný antivirus.

To byla první věc, kterou bychom mohli udělat pro zabezpečení naší sítě proti útoku. Další věc, kterou lze použít k zabezpečení naší sítě je VPN. Princip VPN sítí spočívá v zašifrování dat již u nás na počítači pomocí VPN klienta, která jsou následně poslána na vybraný VPN server, který data rozšifruje a přepošle je cílovému serveru. Díky tomu náš poskytovatel internetu nevidí, jaké stránky navštěvujeme nebo s kým komunikujeme. To platí i pro cílový server, který vidí jen adresu VPN serveru a ne naši skutečnou IP adresu, čili nepozná, odkud jsme se připojili. To, že se data šifrují již u nás, neznamená, že jsou v naprostém bezpečí, protože poskytovatel VPN serveru k nim má plný přístup, je tedy zásadní důvěra mezi zákazníkem a poskytovatelem VPN. [28]

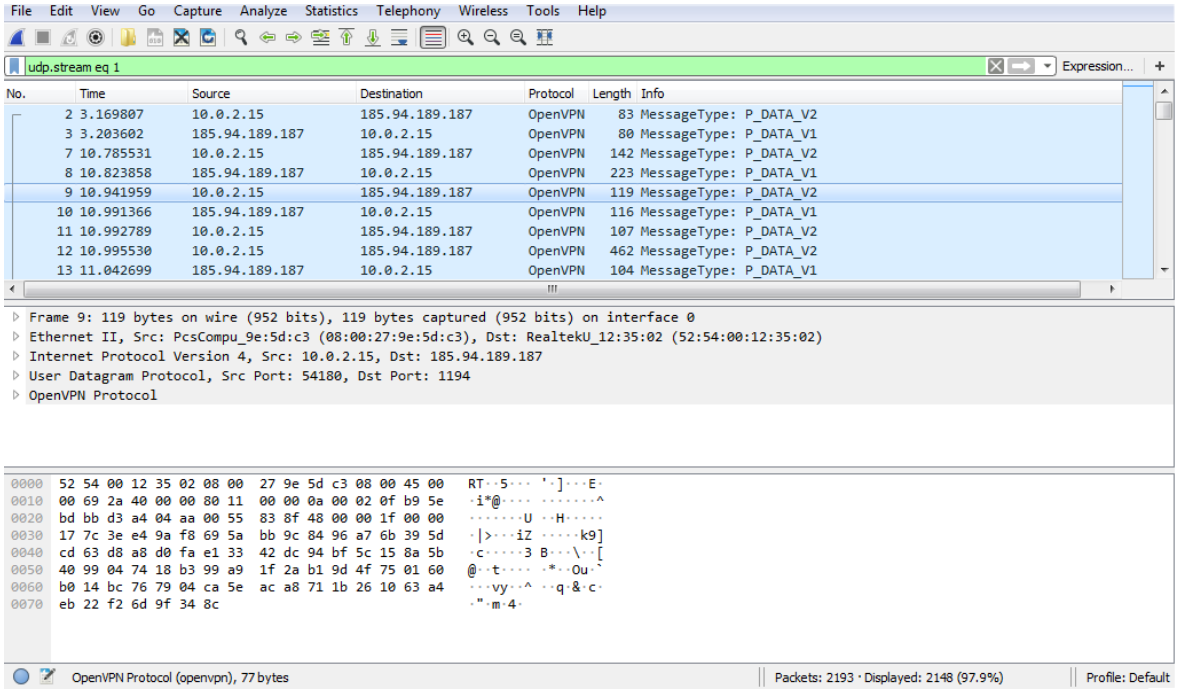
5.2.1 Test VPN

Pro test VPN sítě nejdříve stáhneme VPN klienta, nainstalujeme ho a nakonfigurujeme pro připojení na VPN server. V předchozí části jsme si ukázali jak použít Wireshark ke sledování síťového provozu, teď si ukážeme, jak to vypadá, když používáme VPN.

Jako první nainstalujeme VPN klienta, následně si založíme účet, pod kterým se do klienta přihlásíme. Po přihlášení si vybereme VPN server, ke kterému se chceme připojit. Připojením k VPN serveru se vytvoří zabezpečené připojení mezi námi a VPN serverem. Po vytvoření zabezpečeného spojení, můžeme bezpečně komunikovat mezi námi a VPN serverem.

V předchozí kapitole jsme si popsali, jak ze síťové komunikace můžeme vybrat požadovaná data pomocí programu Wireshark, v tomto případě to byl obrázek. Teď když komunikujeme přes VPN server a chceme získat data stejným způsobem, zjistíme, že to nejde, jak můžeme vidět na obrázku 14, protože veškerá komunikace mezi námi a VPN serverem je zašifrovaná.

Zašifrovaný je nejen obsah zprávy, ale i protokoly, takže když někdo odposlouchává síťovou komunikaci mezi námi a VPN serverem, tak nepozná, jestli se přihlašujeme do emailu nebo stahujeme soubor, vidí jen, že mezi sebou komunikujeme, ale nemá šanci zjistit, o co v té komunikaci jde.



Obrázek 13 Komunikace zašifrovaná pomocí VPN

Z použití VPN vyplývá hned několik věcí – zaprvé je to soukromí. Ten, co odposlouchává naši komunikaci, nemá šanci zjistit, co na internetu děláme. Jelikož jsou servery VPN v různých zemích, můžeme VPN využít, abychom se dostali k obsahu, který není v naší zemi dostupný. Ne všechny věci jsou pozitivní, protože nejdříve se odesílají data na VPN server a až potom na server cílový, proto dochází ke zpomalení internetového připojení. To sice při běžném prohlížení internetu moc nevadí, avšak například při hraní her je to docela závažný problém. Dalším problémem může být cena, protože údržba VPN serverů něco stojí, za provoz VPN jsou účtovány poplatky, cena se pohybuje mezi 3-10 € za měsíc. [28] Další problém může být v dostupnosti některých služeb, protože pod IP adresou VPN serveru vystupuje více lidí, může se stát, že tuto adresu zablokují z důvodu nelegálního chování jiných uživatelů.

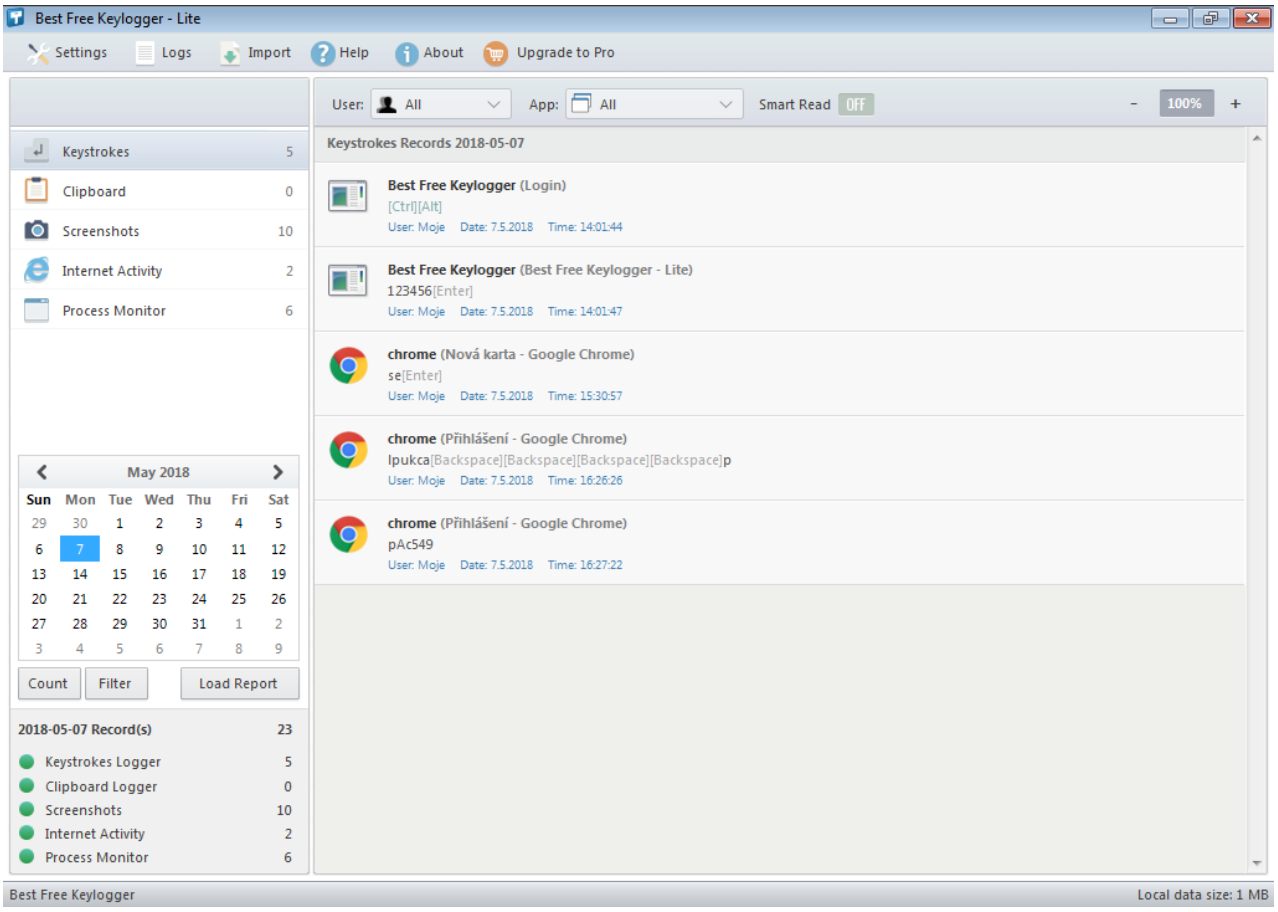
Z výsledků testu vyplývá, že VPN je účinná obrana proti odposlechu datové komunikace, ale musíme si dávat pozor, od koho VPN pořídíme, protože na VPN serveru se musí všechna data dešifrovat, aby mohla být poslána dál, proto má vlastník VPN serveru přístup k naším údajům a my mu můžeme jen věřit, že tyto údaje nijak nezneužije.

5.3 Zadní vrátka (Backdoor)

Tato metoda buď využívá chyby, které se už nacházejí v daném systému nebo je v systému vytvořena pomocí viru jako trojský kůň. V prvním případě, můžeme jedině pravidelně aktualizovat daný systém, aby útočníci nemohli takové chyby použít. V druhém případě si musíme dávat pozor, co stahujeme a mít aktuální antivirus.

5.4 Keylogger

Existuje mnoho programů, které lze zařadit pod název keylogger, z těchto programů jsem vybral program Best Free Keylogger - Lite na kterém si ukážeme, jak takovéto programy fungují.



Obrázek 14 Grafické rozhraní programu Best Free Keyloger

Na obrázku vidíme grafické rozhraní výše zmíněného programu. V levé části rozhraní vidíme, co konkrétního program na počítači sleduje. Položka keystrokes sleduje aktivitu klávesnice, co a v jakém programu se psalo, clipboard zaznamenává všechno, co se uložilo do schránky pro kopírování, patří sem složky i text, screenshot vytváří screenshoty plochy, in-

ternet activity ukládá všechno, co jsme dělali na internetu daný den, process monitor zaznamenává, jaké složky a soubory jsme daný den prohlíželi. Tyto data se pak z daného programu můžou získat z cílového počítače čtyřmi způsoby:

1. **Email**
   Ve vybraných intervalech odesílá data na vybraný email.
2. **FTP**
   Odesílá data na vybraný FTP server.
3. **Síťové sdílení**
   V lokální síti využívá sdílení složek a data ukládá do sdílené složky.
4. **USB**
   Dokáže nakopírovat po připojení k počítači kopii dat na dříve nakonfigurované USB zařízení.

Programy, které mají podobnou funkci jako výše zmíněný Best Free Keylogger, se většinou nezobrazují jako proces ve správci úloh, je tedy obtížné pro běžného uživatele zjistit, jestli má takový program v počítači. Pro běžné uživatele existují programy, které slouží k vyhledávání a odstranění keyloggerů. Jediné, co tedy můžeme udělat jako prevenci proti keyloggeru, je nestahovat a neinstalovat soubory u kterých si nejsme jistí, co dělají, mít aktualizovaný antivirus, popřípadě nainstalovaný nějaký z programů na odstranění škodlivého softwaru.

5.5 Hoax

Většina lidí věří, že přeposíláním hoaxů se nemůže stát nic vážného. Při bližším zkoumání, zjistíme, že to není tak docela pravda. I když nepočítáme obsah samotné zprávy, jen její rozeslání může mít velmi nepříjemné následky. Protože většina hoaxů se rozesílá typem přeposlat všem, tzn. poslat zprávu všem lidem, kteří jsou v našich kontaktech. Tyto adresy zůstávají ve správě uloženy a kdokoliv kdo zprávu obdrží, je může získat. A někteří lidé mají k emailu připojenou i adresu a telefonní číslo. [29]

Abychom se něčemu takovému vyhnuli, můžeme udělat několik věcí. Nevěřit všemu co nám přijde do emailu, nerozesílat takové zprávy dál popřípadě upozornit odesílatele, že se jedná o hoax. Pokud si nejste jisti, že se jedná o hoax, můžete se podívat na stránku http://www.hoax.cz/ na které je databáze známých hoaxů, a pokud tam najdete i ten svůj nebo jemu podobný, můžete si být jisti, že se jedná o hoax. [29]

5.6 Rybaření (Phishing)

Při Phishingovém útoku útočníci využívají sociálního inženýrství, aby z nás dostali osobní údaje, nejčastěji údaje pro přihlášení do internetového bankovnictví nebo PIN kódu k platební kartě. Ale protože roste povědomost o těchto útocích, jsou útočníci nuceni tyto útoky neustále zdokonalovat.

V červenci v roce 2017 se zvýšil počet phishingových útoků přes Facebook. Útočník se podívá na náš seznam přátel, zkopíruje si jeho profil a vytvoří věrohodnou kopii, následně nám pošle žádost o přátelství s tím, že má nový profil. Pokud mu žádost potvrdíme, požádá nás o telefonní číslo, na které nám přijde SMS s kódem, tento kód je potvrzení platby v hodnotě mezi 1300 – 1400 Kč. Pak nás požádá o zaslání daného kódu. V případě, že mu kód zašleme, přijdeme o peníze a profil, který útočník vytvořil, se sám smaže. [31]

Jako prevenci proti tomuto typu útoku si můžeme nastavit seznam přátel jako soukromý nebo jen pro přátele, když nám dojde žádost o přátelství od někoho, koho už bychom v přátelích měli mít, pokud ho známe, měli bychom ho kontaktovat, jestli je to on, pokud to není on, nebudeme jeho žádost přijímat. V případě, že ho neznáme a požádá nás o něco podobného, rozhodně bychom mu nic posílat neměli, jestli už je pozdě, můžeme jedině kontaktovat policii popřípadě i svého operátora.

Abychom se nenechali nachytat, měli bychom dodržovat několik zásadních věcí:

1. Neklikat na žádné odkazy, které nám přijdou emailem.
2. Nestahovat žádné soubory.
3. Kontrolovat pravopis příchozího emailu.
4. Banky ani jiné instituce po nás nikdy nebudou chtít heslo po emailu. [32]

5.7 Farmaření (Pharming)

Jedná se o nebezpečnější formu phishingu. Nebezpečnější v tom, že nedochází k útoku přímo na uživatele, ale dochází k útoku na DNS server. Protože tedy útok neprobíhá na náš počítač, nelze se proti němu nijak bránit. Jedinou možností je DNS server obejít a zadat přímo IP adresu požadované stránky, to ale ve většině případů není možné. Zbývá tedy jen jedna možnost a to vizuálně dané stránky zkontrolovat, jestli nechybí certifikát, stránka nevypadá jinak nebo není špatný název domény. [4]

5.8 Distribuované odmítnutí služby (DDoS)

Tento útok se ve většině případů zaměřuje na společnosti a jen ve velmi ojedinělých případech na jednotlivce, tedy šance, že se stanete obětí tohoto útoku je velmi mizivá. [33]

5.9 Prevence proti kyberšikaně

Jako prevenci proti kyberšikaně je vhodné děti seznámit s pravidly bezpečného chování se ve virtuálním světě již od útlého věku. Rozhodně by měly být poučeny ve škole o Listině dětských práv na internetu. [21]

Mají právo prohledávat internet, učit se z něj a užívat si všechny dobré věci, které na internetu objeví. Neměly by vyplňovat žádné podezřelé formuláře, odpovídat na nevhodné otázky nebo emailové či jiné zprávy. Měly by veškeré citlivé informace o sobě uchovávat v tajnosti. Pokud potřebují s něčím pomoci, neměly by váhat požádat o pomoc rodiče, případně učitele a zároveň jim oznámit pokud se k nim někdo chová divně nebo agresivně. [21]

5.9.1 Nejčastější projevy chování oběti kyberšikany

Nejčastější změna chování, kterého si můžeme u oběti kyberšikany všimnout je, že náhle přestane používat počítač nebo mobilní telefon, i když ho ještě donedávna používala bez problémů. S tím se pojí i změna chování, např. po přečtení SMS, nebo emailu je oběť rozčílená, frustrovaná nebo jinak zneklidněná. Když se zeptáme na důvod tohoto chování, odpovídá vyhýbavě a ustrašeně. Ve škole se může vyhýbat hodinám, kde učí předměty spojené s počítači. Další známkou kyberšikany může být špatné spaní nebo i noční můry. [21]

5.9.2 Nejčastější projevy chování kyberagresora

Stejně jako můžeme pozorovat chování oběti, můžeme pozorovat chování kyberagresora. Například v blízkosti dospělé osoby vypíná monitor, nebo programy, aby dospělá osoba neviděla, co na počítači dělá. Používá počítač dlouho do večera, přehnaně se u něj směje a je rozčílený, když ho nemůže používat. Na otázky typu, „Co na tom počítači pořád děláš?“ odpovídá vyhýbavě a neurčitě. [21]

5.10 Základní pravidla při setkání s kyberšikanou

První co musíme v takové situaci udělat, je ukončit komunikaci, to znamená neodpovídat na žádné zprávy ať už v podobě SMS, emailů, aj. Příchozí zprávy ale v žádném případě nemazat, můžou posloužit jako důkazní materiál. Změna kyberidentity, tzn. změna facebookového účtu, změna emailové adresy, změna telefonního čísla, tyto změněné kontakty poskytnout jen osobám, které znám a kterým věřím. Vše oznámit, např. ve škole třídnímu učiteli, popřípadě na policii, rozhodně se nesnažit s danou situací vypořádat sami. [21]

ZÁVĚR

Cílem této práce bylo zmapování kybernetických útoků v minulosti a také trendů kyberkriminality v současnosti. Zároveň v ní byly popsány pojmy jako DDoS, krádež identity, kyberstalking apod. Cílem práce rovněž bylo informovat o nebezpečí kybernetické kriminality a o tom, co mohou uživatelé udělat proto, aby tomuto nebezpečí předcházeli.

První kapitola teoretické části této bakalářské práce pojednávala o historii kyberkriminality, kdy byl poprvé použit tento pojem, jak se vyvíjel a jeho definicích – obecných i specifických pro určité organizace a právní normy upravující problematiku kyberkriminality. Na konci první kapitoly byl definován pojem kyberprostor. Druhá kapitola se zabývala pachateli kyberkriminálních zločinů, vznikem pojmu hacker, hackerskou etikou, a klasifikací hackerů. Ve třetí kapitole byly definovány kyberkriminální techniky, jako sociální inženýrství, phishing, pharming, a další. V poslední kapitole teoretické části této práce byly uvedeny specifické příklady kyberkriminality, konkrétně kyberšikana, kyberstalking, kybergrooming a krádež identity.

Cílem praktické části této bakalářské práce bylo definovat způsoby, jakými se bránit v teoretické části zmíněným kyberkriminálním technikám, otestovat, jak funguje útok hrubou silou, důležitost dobře zvolených hesel, a funkčnost mechanizmů, které mohou být použity k dodatečnému zabezpečení proti tomuto útoku. Kapitola odposlech datové komunikace pojednávala o způsobech odchytávání paketů ze síťového provozu, jakým způsobem z těchto paketů získat informace, a jak používání VPN zabraňuje ve sledování síťového provozu. Pátá kapitola se zabývala 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. Jako poslední byla řešena prevence proti kyberšikaně, jak se mohou chovat oběti nebo pachatelé kyberšikany a co dělat, když se s ní uživatelé setkají.

Z testu, ve kterém byla sledována odolnost hesel proti útoku hrubou silou bylo zjištěno, že čím je heslo delší a různorodější, tím je obtížnější toto heslo prolomit útokem hrubou silou. Toto tvrzení se sice jeví jako pravdivé, ale lze předpokládat, že většina uživatelů toto doporučení dodržovat nebude, protože pokud si zvolí heslo jako „Nqdr18y.E3PQ“, bude mít problém si ho zapamatovat, a proto používají jako heslo třeba své jméno. Tento problém tedy není na straně počítače, nýbrž uživatele.

Z testu o dvoufázovém ověřování bylo zjištěno, že se jedná o vcelku spolehlivou ochranu proti útoku hrubou silou, která se ale stává irelevantní v momentě, kdy má útočník přístup k telefonu uživatele.

V testu o odposlechu datové komunikace bylo zjištěno, že VPN je účinná ochrana proti tomuto útoku, ale uživatel musí mít důvěru k poskytovateli VPN, protože on má neomezený přístup k jeho údajům a nezbývá mu, než poskytovateli důvěřovat, že tyto informace nezneužije.

V souhrnu výsledků z těchto testů lze říct, že tyto obranné mechanizmy jsou účinné, proti útokům proti kterým byly testovány, ale nejsou dokonalé, protože existují možnosti jak tyto mechanizmy obejít.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[20] *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

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

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

[23] *Dvoufázové ověření* [online]. [cit. 2018-04-30]. Dostupné z: https://support.ubi.com/cs-CZ/Faqs/000025170/Secure-your-account-with-2-Step-Verification

[24] *Autorizace počítače* [online]. [cit. 2018-04-30]. Dostupné z: https://support.steam-powered.com/kb_article.php?ref=4020-ALZM-5519&l=czech#what

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

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

[27] *Wireshark* [online]. [cit. 2018-04-30]. Dostupné z: https://www.wireshark.org/

[28] *VPN* [online]. [cit. 2018-05-08]. Dostupné z: https://www.root.cz/clanky/vpn-pro-zacatecniky-princip-fungovani-vyhody-a-nevyhody/

[29] *HOAX* [online]. [cit. 2018-04-04]. Dostupné z: http://www.hoax.cz/hoax/cim-hoax-skodi

[30] *Dvoufázové ověření* [online]. [cit. 2018-04-30]. Dostupné z: https://support.ubi.com/cs-CZ/Faqs/000025170/Secure-your-account-with-2-Step-Verification

[31] *Phishing* [online]. [cit. 2018-04-04]. Dostupné z: https://csirt.cz/page/3595/narust-phishingovych-utoku-na-socilani-siti-facebook/

[32] *Phishing* [online]. [cit. 2018-04-04]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/phishing.aspx

[33] *DDoS* [online]. [cit. 2018-04-04]. Dostupné z: https://www.root.cz/clanky/ddos-utoky-jak-se-ucinne-branit/

[34] Vlastní zdroje

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

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: NÁZEV PŘÍLOHY