Malware a sociální inženýrství

Malware and social engineering

Libor Jasný

Bakalářská práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Libor JASNÝ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Malware a sociální inženýrství**

Zásady pro vypracování:

1. **Popište druhy jednotlivých počítačových infiltrací a jejich vlastnosti.**
2. **Uveďte metody šíření a možné následky jejich činností.**
3. **Navrhněte preventivní ochranu proti napadeni PC systému.**
4. **Analyzujte možnosti obrany v již napadeném systému.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SZOR, Peter. Počítačové viry : analýza útoku a obrana. Brno : Zoner Press, 2006. 608s.**
2. **JIROVSKÝ, Václav. Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha : Grada, 2007. 284s.**
3. **KOUŘIL, Lukáš. Počítačové viry a umělá inteligence . [s.l.], 2008. 57s. Vedoucí diplomové práce Zelinka Ivan, doc. Ing. Ph.D.**
4. **HÁK, Igor. Ochrana dat : škodlivý software. Hradec Králové : Gaudeamus, 2005. 211s.**
5. **GALDOVÁ, Lucie. Operační systémy – Security. [s.l.], 2005. 58s. Vedoucí bakalářské práce Sysel Martin, doc. Ing. Ph.D.**
6. **SKÁCELOVÁ BÁRTOVÁ, Alena. Způsoby zabezpečení informačních systémů . [s.l.], 2008. 83s. Vedoucí bakalářské práce Zelinka Ivan, doc. Ing. Ph.D.**
7. **MLČEK, Viktor. Metody prevence počítačové kriminality . [s.l.], 2008. 76s. Vedoucí diplomové práce Jašek Roman, doc. Mgr. Ph.D.**

Vedoucí bakalářské práce: **Ing. David Malaník**
Ústav aplikované informatiky

Datum zadání bakalářské práce: **20. února 2009**

Termín odevzdání bakalářské práce: **20. května 2009**

Ve Zlíně dne 20. února 2009

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

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce představuje přehled nejčastějších a nejnebezpečnějších programů nesoucí souhrnný název malware. Popisuje jednotlivé druhy infiltrací, jejich funkci, šíření a nebezpečí, které sebou nesou, včetně obrany proti těmto útokům. Druhá část této práce je věnována sociálnímu inženýrství na Internetu, jeho technikám a způsobům zneužití osobních informací. Práce je doplněna reálnými příklady a názornými ukázkami.

Klíčová slova: Malware, Adware, Spyware, Vir, Červ, Keylogger, Trojský kůň, Sociální inženýrství, Phishing, Pharming, Cybersquatting

ABSTRACT

This work presents an overview of the most common and most dangerous programs carrying summary name malware. Describes the various types of infiltration, their function, distribution and risk, which entail, including defense against these attacks. The second part of this work is devoted to social engineering on the Internet, its techniques and methods of misuse of personal information. The work is complemented by real examples and illustrative previews.

Keywords: Malware, Adware, Spyware, Virus, Worm, Keylogger, Trojan, Social engineering, Phishing, Pharming, Cybersquatting

Děkuji Ing. Davidu Malaníkovi za odborné vedení, pomoc a poskytnutí informací při realizaci této bakalářské práce.

Motto:

Jen dvě věci jsou nekonečné - vesmír a lidská hloupost. Tím prvním si ovšem nejsem tak jist.

Albert Einstein

- Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/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 – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- 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.

Ve Zlíně …….
podpis diplomanta

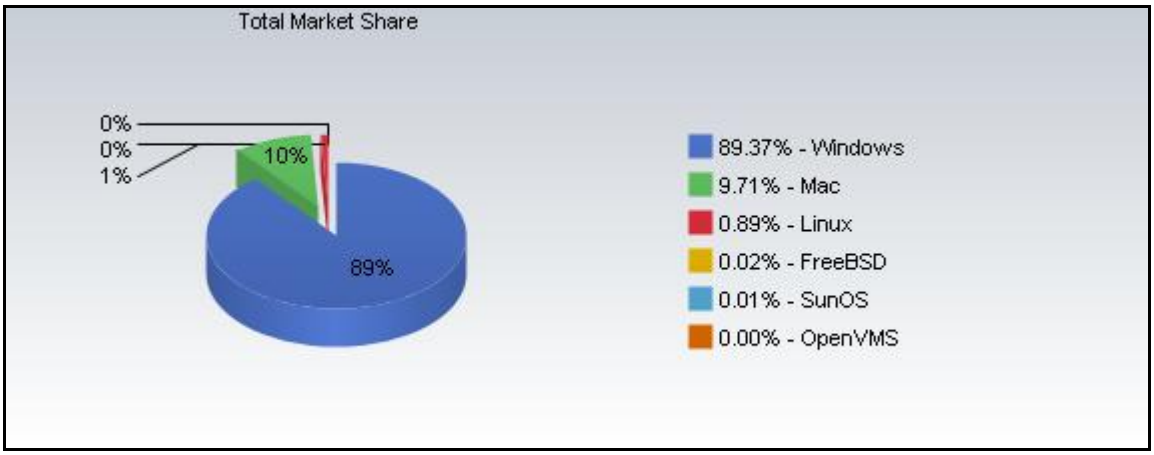
OBSAH

ÚVOD

Informační technologie ovlivňují náš každodenní život. S počítači a Internetem se setkáváme ve stále větší míře. Usnadňují nám práci, pomáhají v našem osobním životě, slouží jako druh zábavy. Avšak s rostoucími možnostmi informačních technologií, rostou i možnosti kyberkriminality. Proto je nutné znát potenciální rizika, která nám hrozí a před kterými bychom se měli chránit. O tom, že není dobré tato rizika podceňovat, svědčí i to, že Americký Federální vyšetřovací úřad (FBI) řadí důležitost kyberzločinu na třetí místo hned za terorismem a průmyslovou špionáží [9], a uvádí, že zisky z počítačové kriminality přesahují zisky z prodeje drog. [10]

Proto cílem této bakalářské práce je seznámit čtenáře s bezpečnostním rizikem škodlivých programů označovaných jako malware. Nebere si za úkol složitě popisovat a rozebírat jednotlivé počítačové infiltrace a principy na nichž fungují, ale snaží se srozumitelnou formou podat zvídavému uživateli informace, které mu pomohou udělat si představu o současném softwarovém nebezpečí, které mu hrozí. Dále se zabývá sociotechnikami využívanými na Internetu za účelem zneužití osobních informací, kde rozebírá jednotlivé techniky a popisuje řešení, jak se proti nim bránit a uchovat tak naše citlivá data v bezpečí.

Podle nezávislé analytické společnosti Gartner [1] byla v roce 2008 na světě zhruba jedna miliarda počítačů, přičemž podle serveru Market Share [2] k březnu roku 2009 zabíral operační systém od společnosti Microsoft téměř 90% trhu s osobními počítači. Proto se tato bakalářská práce zaměřuje výhradně na šíření malwaru pod tímto operačním systémem.



Obr. 1. Graf podílu operačních systémů v březnu 2009 [2]

I. TEORETICKÁ ČÁST

1 MALWARE

Výraz Malware vznikl složením dvou anglických slov - **Mal**icious (zlomyslný/ záludný/zákeřný) a Soft**ware** (počítačový program). Jedná se o souhrnné označení pro všechny typy infiltrací škodlivým kódem. Malware je počítačový program, který je obvykle určen ke vniknutí, poškození nebo zneužití počítačového systému. Je často označován také jako Crimeware, Riskware nebo Grayware. Jeho rozdělení je komplikované, protože se jednotlivé typy mohou prolínat mezi sebou. Možné rozdělení malwaru:

- Adware
- Spyware
- Virus
- Worm
- Trojan
- Keylogger
- Rootkit
- Dialer
- Hoax
- Backdoor
- Hijack
- Downloader
- Exploit
- Botnet

1.1.1 Šíření malwaru

Podle odborníků na počítačovou bezpečnost bylo v roce 2007 v oběhu téměř jeden a čtvrt miliónu škodlivého softwaru. Studie společnosti Symantec [3] ukazuje, že 64% veškerého softwaru, který v roce 2007 vznikl, tvořily právě tyto nebezpečné kódy. Je to vůbec poprvé,

kdy počet škodlivého softwaru přerostl počet užitečného. Podle analýz tvoří až 70% z veškerého škodlivého softwaru trojské koně (viz kapitola Trojan / Trojský kůň).

Malware se může šířit mnoha způsoby. Nejčastějším je přenášení pomocí sítě Internet v podobě stahování torrent souborů, warezu nebo sdílení souborů přes P2P sítě, ale také navštěvováním webových stránek s porno tématikou, cracky, sériovými čísly, keygeny apod. Malware se může šířit také přenášením paměťových disků a optických médií, emailovou (Spam) a IM komunikací (ICQ, MSN, Jabber), instalací multimediálních kodeků a především pak také skrze bezpečnostní díry v operačním systému, či díry v programech výrobců třetích stran.

Podle renomované dánské společnosti Secunia [4], zabývající se monitorováním a analýzou bezpečnostních rizik v IT, vydala po otestování cca 20.000 počítačů šokující informaci.

Plných 98,08% z testovaných počítačů s operačním systémem Windows je zranitelných z důvodů neošetřených chyb v operačním systému, anebo v mnohem častějším případě díky neošetřeným chybám v softwaru třetích stran. Skoro 50% počítačů obsahuje 10 a více bezpečnostních chyb.

Skenování počítačů bylo prováděno na základě dobrovolné účasti v tomto programu za použití softwaru Secunia PSI (Personal Software Inspector).

Je nutno dodat, že se testoval pouze stav aktuálního PC, nikoliv s použitím bezpečnostních prvků jakou jsou např. firewally apod., které dokáží značnou část bezpečnostních hrozeb účinně eliminovat.

1.1.2 Cíle malwaru

Útoky malwarových programů mohou být různé. Záleží především na záměru jeho autora, za jakým cílem škodlivý kód vytváří. Tyto aplikace mohou mít za úkol poškodit operační systém, mazat soubory, zneužívat počítač k jiným účelům jako např. rozesílání spamu (nevyžádané pošty) – Spam server, provádět DoS útoky apod., v horším případě pak slouží k vykrádání osobních informací a dat, a jejich následnému zneužívání. Těmito citlivými údaji mohou být čísla platebních karet včetně CVV kódů, čísla pojištění, přihlašovací a autentizační údaje k webovým účtům a službám, emaily, sledování zvyklostí uživatele,

které mohou být následně využity pro cílenou reklamu, ale také ke sledování a zaznamenávání stisků kláves a dokonce i k odposlechům (viz kapitola Keylogger).

1.1.3 Ochrana před malwarem

Ve velkém procentu malwarových útoků je infiltrace škodlivým kódem způsobena dobrovolně, neboť je vyžadována přímá interakce s uživatelem, který svou neopatrností nebo nepozorností vpustí škodlivý kód do systému. Pro příklad, uveďme videa na porno stránkách. Ty mohou vyžadovat instalaci příslušného multimediálního kodeku, potřebného k přehrání daného videa. Často se jedná o dobrovolnou instalaci na základě požadavku webové stránky. Dalším častým zdrojem dobrovolné instalace malwaru bývají spořiče obrazovky popř. jiné neškodně vypadající programy, které rovněž nesou nákazu ve své instalaci.

Ochrana před malwarem by měla být založena na tzv. defense-in-depth strategy, neboli na obranné hloubkové strategii, která je tvořena několika vrstvami. Takovýto obranný systém je pak méně prostupný a lépe eliminuje útoky na jednotlivých vrstvách. Těmito vrstvami se rozumí hardwarový firewall tvořený routerem, switchem případně jiným síťovým prvkem, následovaný softwarovým firewallem popř. aplikační bránou řídící síťový provoz. Využívání těchto bezpečnostních prvků je téměř nutností pro uživatele přistupujícího do celosvětové sítě pod veřejnou IP adresou (Public IP), protože je přímo viditelný vzdáleným útočníkem.

Dalším krokem je použití antivirových programů a softwaru na odstranění adwaru, spywaru, rootkitů aj. Dnešní moderní antivirové programy však řadu těchto prvků integrují do sebe. Dalším důležitým prvkem je mít neustále aktualizovaný operační systém a také programy výrobců třetích stran, především pak ty, které přistupují k Internetu (webový prohlížeč, IM klient, poštovní klient, programy využívající P2P sítě atd., ale i doplňky, které tyto programy využívají – java, flash apod.). Zde se však objevuje problém, protože některé softwarové společnosti mohou chtít za aktualizaci svého programu zaplatit určitou sumu peněz z celkové částky produktu, což vede k odrazení uživatele, protože tak musí platit za něco, co už jednou zaplatil a používá tak dál původní verzi produktu, u kterého již byly objeveny bezpečnostní díry. Neméně důležitým prvkem v obraně proti malwaru je také aktualizovat a záplatovat webový prohlížeč, protože je to právě on, pomocí něhož přistupujeme k Internetu. A nejspíše nejdůležitějším prvkem v této strategii je poučený

uživatel, který je seznámen s nebezpečím, které mu v celosvětové síti hrozí. Základem je neklikat na všechno, co mu příjde pod ruku, neotevírat emaily a přílohy od neznámých adresátů, vyvarovat se podezřelým webovým stránkám, neinstalovat neznámé programy a pokud možno pracovat v účtu s omezenými právy.

Jelikož malwarový průmysl roste daleko rychleji než ten bezpečnostní a jeho útoky jsou čím dál více sofistikovanější, je prakticky nemožné, aby byli uživatelé před hrozbami kyberprostoru v bezpečí. Bude-li záviset bezpečnost počítače na defense-in-depth strategy, bude se muset v budoucnu tento obranný systém stále více rozšiřovat, což povede k jeho větší komplikovanosti a nákladnosti jak na hardwarové, tak na finanční prostředky. Proto se dnes přední světové bezpečnostní společnosti zabývají jiným řešením, jak tento problém co nejvíce eliminovat. Řešením může být opačná změna přístupu [7].

Současné antivirové programy a jiný podobný software určený k zabezpečení počítače pracují na principu blacklistu (černé listině). To znamená, že obsahují databáze toho, co se v systému spustit nesmí, popř. co do něho (z něho) nesmí proniknout (viz databáze virových definic). Novým způsobem ochrany by v budoucnu mohl být tzv. whitelist (bílá listina), tedy povolení spuštění a přístupu jen vítaným aplikacím. Byl by tak identifikován pouze program, který by měl být spuštěný a všechen ostatní by měl být automaticky zakázán. Odpadla by tak závislost na aktualizacích potřebných ke správné funkci dnešního řešení. Při neustálém aktualizování antivirových definic a signatur, nekonečném záplatování operačního systému a jiných aplikací, vynakládání finančních prostředků za bezpečnostní řešení se cesta blacklistingu nejeví jako konečná a systém whitelistingu by tedy mohl přinést revoluci v zabezpečení a ochraně soukromí uživatele.

1.1.4 Obrana v již napadeném systému

Obrana v již napadeném systému bývá často dosti omezena na možnostmi, které nám daný druh malwaru dovolí. Zde záleží pouze na autorovi, za jakým účelem daný škodlivý kód vytváří a jakou funkci bude v napadeném systému plnit. Tímto se nám vymezují možnosti, jak s daným malwarem bojovat popř. ho odstranit úplně. Bude-li např. daný druh škodlivého kódu vytvořen pro rozesílání nevyžádané pošty, je nutné postupovat jiným způsobem než v případě viru sestrojeného za účelem maximálního vytěžování hardwarových prostředků počítače.

Ve všech případech ovšem platí, že v případě podezření nákazy, by antivirový program měl prověřit systém jako první a to především tzv. hloubkovou analýzou, popř. ručně nastaveným skenem s rozšířenými možnostmi, kde lze nastavit kritická místa jako systémové disky nebo důležité složky a zvolit také konkrétní typy souborů. V dalším bodu by měl následovat antispywarový software, který mnohdy odhalí infiltrace, které můžou antivirovým programům uniknout. Je-li chování počítače doprovázeno charakteristickými rysy, je možné podle těchto prvků identifikovat konkrétní druh škodlivého kódu a naleznout odpovídající postup, popř. přímo software na jeho odstranění.

Nákaza počítače je často doprovázena dalšími jevy, jako jsou nemožnost instalace dalších bezpečnostních prvků, provádění změn v nastavení systému, omezený pohyb po síti, zpomalený chod počítače aj. Dojde-li k takovémuto chování a operační systém je omezen, je možno uvést systém do tzv. stavu nouze, kde malware často není schopen své funkce a lze tak provést výše popsané kroky. Bude-li se počítač i po provedení těchto kroků chovat nekorektně, můžeme ještě využít bodů obnovy, které si OS Windows pravidelně dělá (není-li nastaven jinak) a navrátit tak vše do původní podoby. V případě, že na počítači není antivirový a jiný bezpečnostní software nainstalován a není nám ani následná možnost jeho instalace povolena, můžeme využít online řešení a provést tak kontrolu počítače vzdáleně. Když ani tento způsob není k dispozici, zůstává nám už jenom možnost pevný disk manuálně vyndat za PC, připojit k jinému počítači a kontrolu provést skrze něj.

Bude-li operační systém poškozen natolik, že již žádné softwarové opravy nepomohou, je nutno pevný disk zformátovat a nainstalovat operační systém znovu. Přestože se jedná o krajní řešení, téměř vždy se tím vyřeší všechny problémy. Jen v případě, kdyby došlo k napadení boot virem (viz. kapitola Boot viry), je potřeba smazat veškeré logické oddíly na pevném disku a podle potřeby vytvořit nové.

1.1.5 Scareware

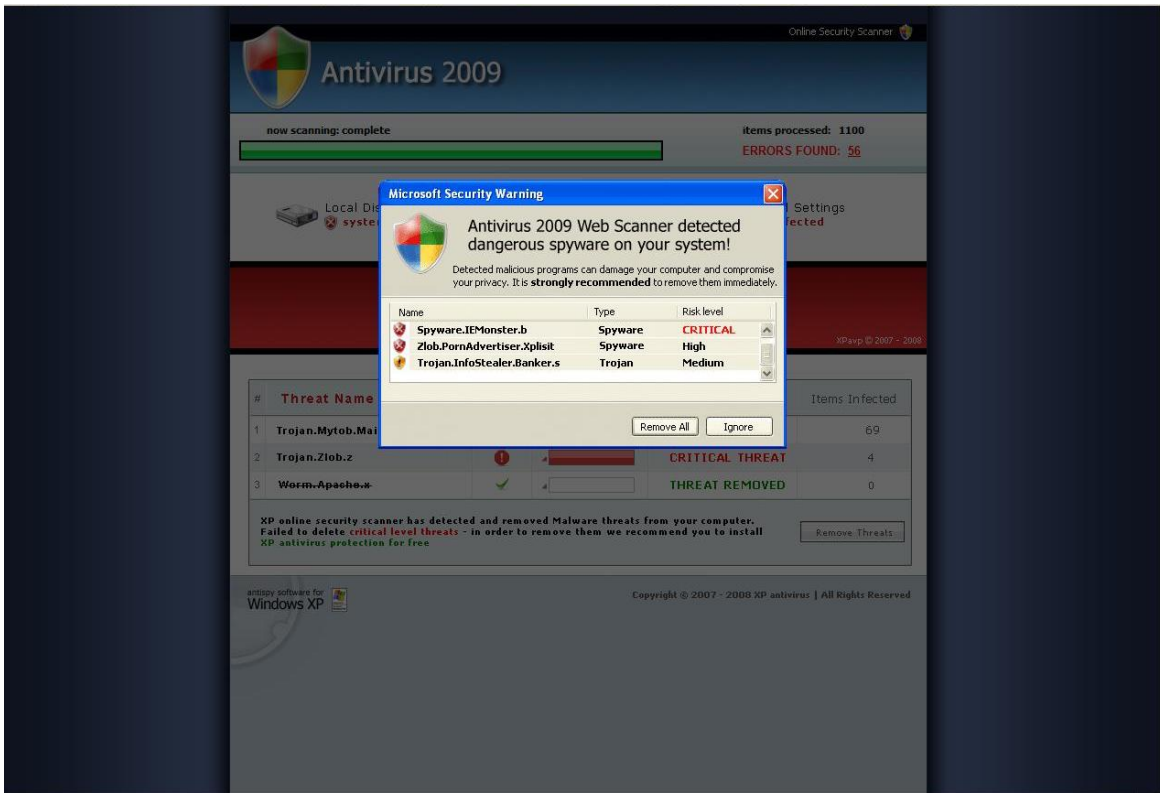
V říjnu 2008 vydala společnost PandaLabs [5] zprávu, že až 30 miliónů počítačů na celém světě je infikováno falešným antimalwarovým programem tzv. scarewarem. Údajně se po Internetu šíří až 7000 variant těchto podvodných programů.

Tyto podvodné programy se objevují na Internetu nejčastěji v podobě adwaru (reklamy) popř. se šíří cestami popsanými výše v kapitole Šíření malwaru. Po infikování počítače obtěžují uživatele vyskakujícími pop-up okny a jinými nežádoucími prvky, zobrazují

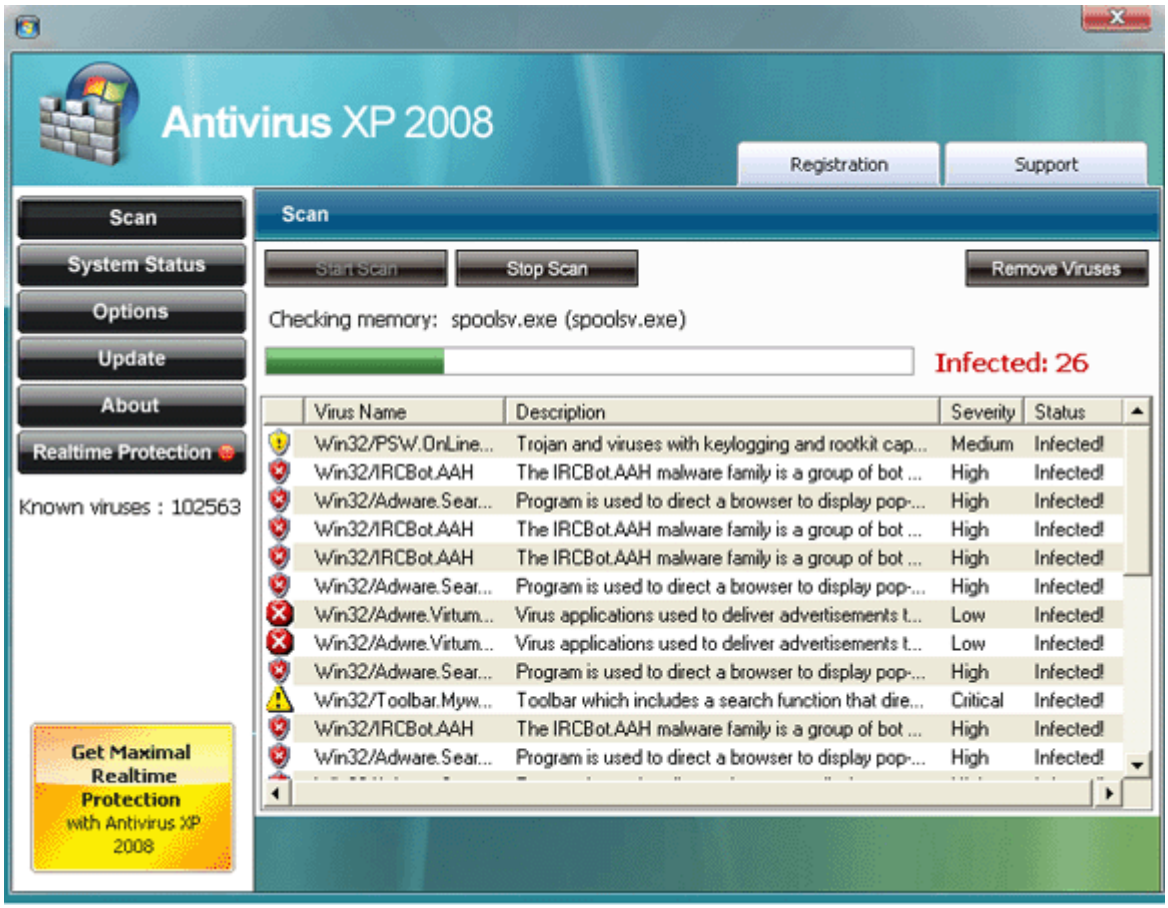
krátký scan počítače a následně varování o tom, že PC je infikováno několika škodlivými kódy. Jako řešení pro jejich odstranění, pak uživatele vybízí k zakoupení licence, která činí v průměru 50€. Za měsíc si tak kybernetičtí podvodníci mohou přijít až na 10 000 000€. Mimo finanční částky však uživatelé přijdou i o své cenné osobní informace, které mohou být pak dále zneužívány a prodávány na černém trhu.

Tyto falešné antimalwarové programy jsou často doprovázeny velmi působivou a přesvědčivou reklamou, která má uživatele přimět k jejich koupi. Často se srovnávají s jinými antimalwarovými produkty výrobců renomovaných značek, popř. udávají, kde se tento software používá. Je zde tak využíváno moderního sociální inženýrství založeného na neznalosti uživatele, který si tak kupuje falešný pocit bezpečí.

1.1.6 Příklady falešných antimalwarových programů



Obr. 2. Antivirus 2009



Obr. 3. Antivirus XP 2008 [6]

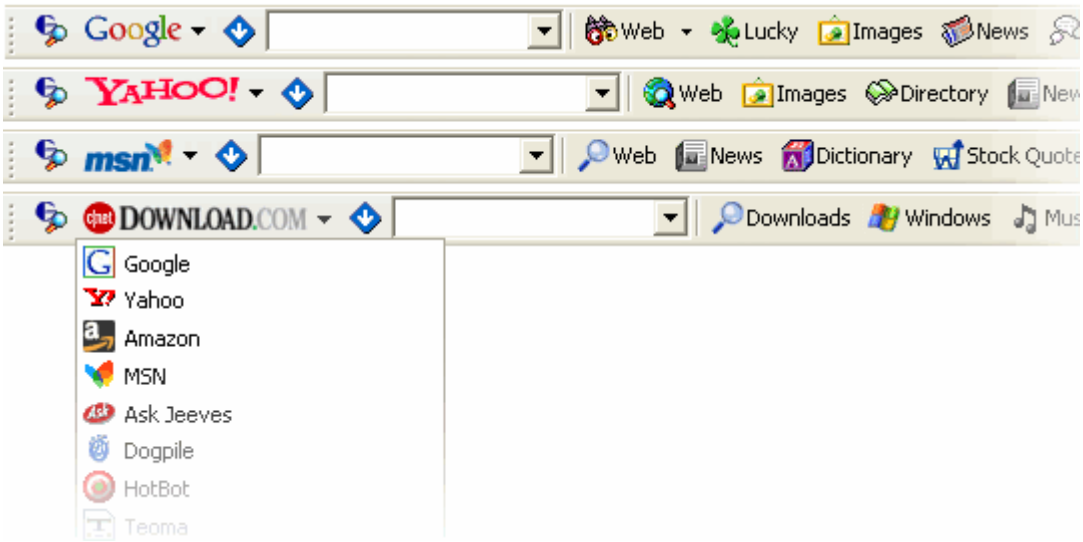
Obr. 4. Webová stránka nabízející Antivirus XP 2008 [6]

1.2 Adware

Adware – **Ad**vertising (reklamní) soft**ware** (počítačový program). Pod pojmem adware se rozumí jakýkoliv produkt, který se do počítače uživatele nainstaluje spolu s jiným softwarem a to buď skrytě nebo na základě licenčního ujednání tzv. EULA – End User License Agreement (licenční smlouva s koncovým uživatelem, která definuje podmínky užívání daného softwaru. Může také obsahovat podmínky instalace adwaru!), tím se myslí programy, které vstupují do počítače se souhlasem uživatele, protože podmínkou jejich bezplatného používání je právě přítomnost reklamních materiálů. Software bývá vybaven adwarem především proto, že slouží jako zdroj reklamních příjmů pro výrobce daného programu a jedná se tak o zvláštní druh licencování, protože zde platíme tím, že jsme nuceni sledovat reklamu.

1.2.1 Možnosti Adwaru

- Zobrazování nebo přehrávání reklamních a propagačních materiálů
- Vyskakování pop-up oken
- Neznámé ikony v oznamovací oblasti (System Tray)
- Vnucování stránek
- Nastavení cizí domovské stránky (homepage) bez vědomí uživatele
- Zobrazování reklamních bannerů
- Instalace toolbarů do webových prohlížečů
- Pomalé načítání webových stránek
- Zpomalený chod počítače



Obr. 5. Příklady webových toolbarů [8]

1.3 Spyware

Spyware – označení pro software, který shromažďuje osobní informace nebo mění konfiguraci systému, obvykle bez získání předchozího souhlasu uživatele a posílá je útočníkovi prostřednictvím sítě Internet. Podobně jako u adwaru, může být souhlas k jeho nainstalování spojený s licenční smlouvou a může být součástí volně šiřitelného programu.

1.3.1 Možnosti Spywaru

- Shromažďování a odesílání historie navštívených webových stránek a seznamu nainstalovaných programů, za účelem zjištění potřeb nebo zájmů uživatele a tyto informace následně využít pro cílenou reklamu
- Vykrádání citlivých informací o uživateli, jako jsou přihlašovací údaje k bankovním a jiným webovým účtům, PINy, emailové adresy atd.
- Nastavení jiné domovské stránky (homepage) a výchozího poskytovatele vyhledávání
- Zneužívání PC pro rozesílání nevyžádané pošty – Spamu (Spamserver)
- Změna chování PC – zpomalený chod, nové ikony na ploše, nestabilita OS

1.4 Virus

Virus (z latinského slova jed) je program, který se dokáže šířit formou replikace za přítomnosti hostitele, bez vědomí uživatele všemi dostupnými prostředky. Má tendenci vkládat se do spustitelných souborů (.exe, .com .bat), přičemž má schopnost modifikovat se tak, aby lépe zapadl do svého hostitelského souboru. Chová se tedy jako biologický originál. Dojde-li ke spuštění hostitele, provede se kód viru, ve kterém se mimo svoji primární činnost, snaží infikovat také další hostitelský soubor. Virus se mezi dvěma počítači může přenést jedině tím, že někdo přenese jeho hostitele, např. zkopírováním souboru na vyměnitelné médium, nebo ho pošle prostřednictvím Internetu nebo sítě LAN. U některých virů se škodlivý kód spouští až se zpožděním (např. v určité datum či po infikování určitého počtu jiných souborů), což se někdy označuje jako logická bomba (Logic Bomb).

Dříve, v dobách kdy Internet nebyl tak masově rozšířený jako dnes, se počítačové viry zaměřovaly spíše na záškodnickou činnost, ve které se snažily mazat nebo poškozovat soubory na pevném disku, popř. celý disk zformátovat, anebo zatěžovat výkon počítače tak, aby práce na něm nebyla možná.

Takovýmto příkladem může být legendární virus One_Half.3544.A, který během své přítomnosti na hostitelském počítači postupně šifroval uživatelská data na pevném disku. Pokud operační systém potřeboval zapsat nějaká data na disk, virus převzal kontrolu a tato data nejdříve svým algoritmem zašifroval a až poté je nechal zapsat na disk. Při požadavku na čtení je naopak dešifroval a předal dál operačnímu systému. Při neodborném odstranění takového viru z počítače mohlo dojít i ke ztrátě klíče, podle něhož byla data šifrována. Uživatel tak přišel o data a ve většině případů i o možnost úspěšného startu PC. Operační systém a tedy i PC se tak stalo závislým na samotném viru. [11]

Dalším zajímavým případem se stal virus Win95/CIH novináři pojmenován jako Černobyl. Tento virus proslul tím, že se každého 26. dne v měsíci (záleželo na variantě) pokusil přemazat paměť Flash BIOS na základní desce a kromě toho, i část dat na disku. Pokud se přemazání paměti Flash BIOS podařilo, pak nebyl počítač schopný provozu a jinak než zásahem do hardwaru nebylo možné tento problém vyřešit. Virus Win95/CIH tak narušil do té doby spolehlivé tvrzení, že hardware nelze virem poškodit. [11]

S postupným rozvojem celosvětové sítě a využíváním sociotechnicky se však jejich úloha začala měnit. Tvůrci těchto škodlivých kódů si začali uvědomovat, že by svoje výtvory mohli využít za účelem zisku. A tak se začaly objevovat viry, jejichž primárním účelem, bylo vykrádat citlivá data, a ty pak následně dál zneužívat.

1.4.1 Obecné rozdělení virů

1.4.1.1 Souborové viry

Jejich hostiteli jsou zpravidla spustitelné soubory (.exe, .com), dávkové soubory (.bat) i ovladače. Po spuštění takového hostitele, se kromě původního programu provede také kód viru, který mimo svou primární činnost vyhledá také další možné spustitelné soubory, které by mohl infikovat.

1.4.1.2 Rezidentní viry

Jedná se o viry, které se načítají do operační paměti RAM při spuštění nakaženého souboru (paměťově nerezidentní) a jsou zde přítomny po celou dobu činnosti systému. Mohou tak ovlivňovat všechny soubory, se kterými uživatel pracuje a nemusí tak hledat další hostitele na disku.

1.4.1.3 Boot viry

Infikují zaváděcí oblasti disket (Boot sektor) a pevných disků (MBR – Master Boot Record). Největší nebezpečí těchto virů je, že se dostanou do operační paměti hned se zaváděním operačního systému (bootovaním) jako první program (jedná se tak o paměťově rezidentní virus). Při práci s počítačem hlídají diskové služby a v případě zjištění nové diskety se ihned zapíší do jejího Boot sektoru. K odstranění virů však nevede zformátování disku, jak si většina uživatelů myslí, protože Boot sektor, kde je vir umístěn, leží mimo oblast, která je vyhrazena operačnímu systému a běžné formátování se jí nijak nedotkne. Uživatel tak přijde o všechna svá data, virus však zůstane na pevném disku dále.

1.4.1.4 Makroviry

Napadají makra dokumentů především kancelářského balíku Microsoft Office, nejčastěji Word (.doc), Excel (.xls), Powerpoint (.pps). Jsou psány programovacím jazykem VBA a

dokáží pomocí maker (např. posloupnost příkazů) dokumentu zneužívat program a ovládat tak počítač (spouštět jiné aplikace atd.).

Výhodou pro uživatele české sady MS Office je to, že je u těchto programů lokalizován také makro jazyk a tudíž jsou makroviry psané jiným jazykem nefunkční.

1.4.2 Antivirové programy

Antivirové programy jsou jedním ze základních stavebních kamenů zabezpečení počítače. To vyplývá i z podstaty dříve zmiňované obrané hloubkové strategie (defense-in-depth strategy). Tyto programy se mohou lišit v závislosti na jejich použití (ochrana pracovních stanic/serverů). Antivirový software však není konečným řešením bezpečnosti PC, ačkoliv si to většina uživatelů myslí. Je to pouze jeden z prvků tvořící celkové zabezpečení.

Na trhu je dnes velký výběr antivirových řešení mnoha výrobců. Většina těchto výrobců nabízí ve svých produktech mimo klasických virových skenerů a technologií i metody proaktivní detekce, tedy schopnost reagovat na dosud neznámou hrozbu. Jsou to pak především ony, které jsou v boji proti stále sofistikovanějším škodlivým kódům rozhodující. Vezměme si příklad, kdy se uživatel nakazí dosud neznámým druhem viru. Každé antivirové společnosti nějakou dobu trvá, než se o nové virové infekci, popř. mutaci již známého viru dozví a stihne na něj zareagovat formou aktualizace virové databáze na straně počítače uživatele. V tuto chvíli jsou tu pro nás formy proaktivní detekce, které jsou v množství případů schopny ochránit a zamezit tak způsobení škod, které může nový virus napáchat.

Často jsou AV řešení opomínány v důsledku vynaložení nadbytečných finančních prostředků za ně a jsou považovány za zbytečné. Řeknou si totiž: „Proč bych měl platit za něco, co nepotřebuji, když přece nic tak nebezpečného nedělám?“. Problém je však v tom, že uživatel často nic dělat nemusí, stačí jenom, když je připojen k Internetu a on už si ho nějaký ten počítačový robot prohledávající IP adresy najde a zaútočí. Uživatel by si měl především uvědomit, že prevence proti softwarovému nebezpečí, je ve srovnání s likvidací škod a odstraňováním následků mnohonásobně menší. Smutné je, že většina lidí tuto pravdu zjistí, až když je pozdě.

AV systémy však mají také nevýhody. Největší z nich je ta, že rezidentní ochrana/štít (On-Acces skener), která běží na pozadí operačního systému, zabírá systémové prostředky a

ubírá tak na výkonu počítače. I když jsou dnes počítače tak výkonné, že chod AV programu na pozadí systému skoro nepoznáme, na pomalejších sestavách se to může citelně projevit a omezovat tak práci uživatele. Je to také zároveň jeden z mnoha faktorů, kterými se jednotlivé AV programy odlišují od sebe a rozdělují tak konkurenci, neboť každý uživatel má svá kritéria, podle kterých si antivirové řešení vybírá. A tak cena a příjemné uživatelské rozhraní mohou být na straně jedné a rychlost skenování a zátěž systému na straně druhé. Záleží tak především na uživateli, co je pro něho nejdůležitější.

Na trhu jsou v dnešní době mimo placené AV programy dostupné i jejich freeware kolegové (programy zadarmo). Nabízejí je stejné společnosti, které se zabývají vývojem placených variant. Ve výsledcích antivirových testů podávají velmi dobré výkony a jako AV řešení pro běžného nenáročného uživatele plně dostačují.

Mnoho antivirových společností však mimo jednotlivých antivirových produktů vydává také celé bezpečností balíky. Tyto produkty v sobě zahrnují několik bezpečnostních prvků (antivir + firewall + antispyware + antispam + antirootkit + ochrana proti phishingu aj.) a poskytují tak lepší ochranu, než jen samostatný antivirus. Toto řešení je však také finančně nákladnější a proto je jen na uživateli, kolik se rozhodne investovat do zabezpečení svého počítače.

1.4.2.1 Funkce antivirových programů

On-Acces Scanner

Nepřetržitá kontrola na pozadí operačního systému, kontrolující všechny operace, které uživatel provádí (procházení webových stránek, instalace softwaru, rozbalování archivů, otevírání emailových příloh atd.). Nazýván též jako rezidentní štít.

On-Demand Scanner

Kontrola na vyžádání, kde si uživatel může zvolit, jakou kontrolu má antivirový program provést (standardní, volitelná, hloubková, předem nadefinovaná apod.), jaká místa má skenovat (lokální disky, vyměnitelná média, operační paměť, boot sektory), či jaké typy souborů má vynechávat (archivy, poštovní soubory aj.)

Heuristická analýza

Jedna z metod proaktivní detekce. Slouží k odhalování dosud neznámých virů, které zatím antivirový systém nemá ve své databázi. Funguje na principu virtuálního prostředí, kde se pomocí emulátoru kódů simuluje chování potenciálně nebezpečného programu. Je-li toto chování označeno jako shodující se s nebezpečným kódem, je považováno za vir (může se jednat o otevírání nebo zapisování do spustitelných souborů, ovládání systémových služeb apod.). Nevýhoda této metody v analyzování potenciálně nebezpečných souborů je v tom, že může označit za virus i zcela neškodný soubor, který se tak chová a vyhlásit tak falešný poplach. [25]

Generická detekce

Další proaktivní metoda detekce. Dokáže odhalit neznámé viry na základě stejné programové struktury, protože jisté sekvence v kódu viru se nemění ani při jeho modifikaci. Vzniknou-li tak jiné mutace mateřského viru, je možné pomocí signatur generické detekce odhalit. [25]

Kontrola integrity

Jedná se o proces, při kterém dochází k porovnání informací (např. atributy souboru, kontrolní součet CRC) o souborech s předchozí kontrolou. Jedná se tak o nejrychlejší detekci, přičemž v případě, kdy integrita souboru nesouhlasí s jeho původní verzí, se tak může jednat o napadení virem a nastupují na řadu další metody detekce.

Kontrola příchozí a odchozí emailové komunikace

Kontrola emailových zpráv v poštovním klientu na straně uživatele a na straně serveru poskytovatele (providera) emailové schránky.

Virová databáze

Antivirové programy stahují nejnovější databáze virových definic a signatur, které definují nové škodlivé kódy (nejčastěji v inkrementální podobě – snižuje se přenášení množství dat). Tato procedura je závislá na tom, jak rychle dokáží antivirové společnosti na nový druh nebezpečného kódu zareagovat. (Důležitá je také ovšem aktualizace samotného antivirového programu, protože i on samotný může obsahovat bezpečnostní díry, skrze které může nebezpečný kód vniknout do systému)

Karanténa

Speciální složka, do které si antivir ukládá infikované soubory, které nelze vyléčit, ale jsou pro uživatele natolik důležité, že je nechce odstranit. Může tak např. počkat až vyjde nová verze AV programu a poté se je pokusit ze souboru odstranit.

Plánovač (Scheduler)

Pomocí této funkce může uživatel nastavit požadovanou skenovací metodu v libovolný den a hodinu. Kontrola se pak bude provádět zcela automaticky.

1.4.2.2 Falešné antivirové programy

Stejně jako falešné antimalwarové programy se však nabízejí i podvodné antivirové programy. Jejich podoba od kvalitních AV produktů je téměř nerozeznatelná a není-li uživatel informovaný o renomovaných značkách, může se stát obětí podvodu např. díky cybersquattingu (viz. kapitola Cybersquatting). Pro příklad slouží ukázky podvodných internetových stránek známé české společnosti Alwil Software a.s., vyvíjející antivirový softwarem avast!.

Obr. 6. Podvodná webová stránka AV programu avast! 4.7

Obr. 7. Podvodná stránka AV programu avast! 4.8

1.4.3 Online antivirové systémy

Tomu, kdo antivirový program na svém počítači mít nainstalovaný nechce a spokojí se pouze s občasnou kontrolou, jsou určeny online antivirové skenery. Jsou to bezplatné internetové služby, které téměř všechny přední AV společnosti nabízejí na svých webových stránkách. Většina z nich pak nabízí kromě detekce i následné odstranění malwarového programu.

Nevýhodou těchto řešení je, že téměř všechny spolupracují pouze s Internet Explorerem, protože pro svou funkci vyžadují ActiveX prvky, které alternativní webové prohlížeče nenabízejí. Za další nevýhodu tohoto řešení můžeme považovat to, že v případě nákazy nebezpečnějším virem, jsou tyto služby nedostupné, neboť takovýto virus zpravidla blokuje přístup na domény serverů antivirových společností (typickým příkladem je dnes nejrozšířenější a v historii počítačových hrozeb jeden z nejnebezpečnějších, červ Win32/Conflicker.X (Eset), známý také jako Net-Worm.Win32.Kido.iq (Kaspersky) nebo W32.Downadup.C (Symantec), který ke dni 31. 3. 2009 infikoval více než 10 miliónů počítačů skrze kritickou bezpečnostní chybu v operačním systému Windows [12]).

Obr. 8. Online skener společnosti Eset s.r.o.

Další zajímavou službu na poli online AV ochrany poskytuje server Virus Total (www.virustotal.com). Pomocí tohoto serveru si uživatel může nechat zkontrolovat jakýkoli vámi zvolený soubor na přítomnost škodlivého kódu. Pracuje na bázi On-Demand skeneru a kombinuje v sobě řešení všech předních výrobců AV produktů (ke dni 3.4.2009 obsahoval 38 skenovacích motorů).

1.5 Worm / Červ

Worm, česky červ, je typ škodlivého programu, který se kopírováním šíří počítačovými sítěmi a emailem bez použití hostitelského souboru. Je tedy opakem viru. Využívá bezpečnostní díry v systému nebo spuštěném programu, kde se následně z infikovaného počítače šíří náhodně nebo podle daného algoritmu formou síťových paketů na další počítače. Šíření červů je tak rychlejší než šíření virů a takovýto dominový efekt může vést až k zahlcení sítě. Červi se na rozdíl od virů mohou šířit sami a v současnosti již představují větší hrozbu než viry. Mezi nejznámější červy, kteří se zapsali do historie, můžeme jmenovat např. Blaster, Sasser, MyDoom nebo Conflicker.

1.6 Trojan / Trojský kůň

Trojan neboli Trojský kůň, je software, který se již dále nešíří, ale vydává se za užitečný program, přičemž se jedná o nebezpečnou aplikaci. Může se šířit jako emailová příloha nebo jako užitečná, volně stažitelná aplikace (často shareware, freeware). Pokud je takový program spuštěn, uživatel vidí pouze onen žádaný software a trojský kůň běží na pozadí. Takovýto program sebou může nést spyware, keylogger, spam server, backdoor aj., popř. sloužit k jinému účelu.

1.7 Hijack

Aplikace, která nejdříve přebírá kontrolu nad Internet Explorerem (mění domovskou stránku, způsobuje vyskakování pop-up oken) a následně nad operačním systémem. Projevuje se zejména vypínáním firewallu a antivirového programu přičemž následně otevírá systém jinému škodlivému softwaru. Nebezpečí spočívá ve složitém odstranění, protože nástroje používané pro jeho likvidaci, nepovoluje spustit.

1.8 Dialer

Dialer (z angl. dial - vytočit) je škodlivý program, který přesměruje telefonické připojení (Dial-Up), prostřednictvím kterého se uživatel připojuje k Internetu, na určité placené číslo s mnohonásobně vyšším tarifem. Tyto programy lze využívat legálně při placení za internetové služby, často se však zneužívají k podvodům při přesměrování bez vědomí uživatele.

1.9 Downloader

Tento typ škodlivého programu stahuje do systému další malware z Internetu z předem definovaných URL adres. Pomocí skriptů na straně serveru, může stejný downloader stahovat různé druhy infiltrací. Ve výsledku se pak počítač infikovaný jediným downloaderem může stát téměř nepoužitelný. [11]

1.10 Keylogger

Keylogger - program nebo zařízení určené k monitorování PC. Primárně byly určeny k zaznamenávání stisknutých kláves, většinou za účelem krádeže důvěrných údajů jako

jsou čísla kreditních karet, PINy, hesla k bankovním účtům, e-mailům a podobným citlivým informacím. Dnes jsou však keyloggery vybaveny celou řadou jiných, více nebezpečných, funkcí.

Samotný keylogger je legální nástroj, o jeho používání se již totéž říct nedá.

1.10.1 Vlastnosti keyloggerů

- Těžko zjistitelné antivirovými a antispywarovými programy
- Program skryt v systému a zpravidla neodhalitelný v běžících procesech (softwarový keylogger), minimální zátěž systému.
- Zanedbatelná velikost programu (řádově stovky KB)
- Záznamy ukládány v šifrované podobě

1.10.2 Hardwarové

Zařízení vypadající jako redukce mezi počítačem a konektorem klávesnice (PS/2, USB). Můžou být také zabudovány přímo v klávesnici a být tedy úplně skryté. Jsou neodhalitelné jiným softwarem a nezávislé na volbě OS. Mají vlastní paměť (od desítek KB do několika desítek MB), do které si ukládají data. Po zapojení nenásleduje žádná konfigurace a není potřeba ani instalace žádných ovladačů. Zachytávají klávesy ihned po zapnutí počítače (heslo do BIOSu). Odhalení HW keyloggerů bylo spjato s myšlenkou zpoždění v odezvě, ale tato skutečnost se nepotvrdila, protože prodleva která vzniká, je tak malá, že ji nelze ani detekovat. Odhalení je možné jen měřením spotřeby energie pomocí ampérmetru (zvýšená spotřeba). Zamezit zachycení hesla do systému a webových formulářů lze napsáním přístupových údajů skrze virtuální klávesnici na obrazovce.

Obr. 9. Ukázky HW keyloggerů. Vlevo pro PS/2 konektor, vpravo pro USB [13]

1.10.3 Bluetooth/Wireless

Zařízení funguje stejně jako HW keyloggery, navíc však umožňuje pomocí bezdrátové technologie online odposlech na libovolném mobilním telefonu, PDA, PC nebo notebooku (okamžitě se zobrazuje, co se na klávesnici píše). Ovládat a vybírat data je rovněž možno na dálku. Bezdrátový keylogger dokáže komunikovat pouze se zařízením útočníka a je viditelné pomocí MAC adresy. Zařízení je také možno kamuflovat do klávesnice.

1.10.4 Softwarové

Počítačové programy nainstalované, nebo jinak implementované do OS. Můžou být přibaleny a maskovány v jiném souboru, a jejich možnosti jsou daleko rozsáhlejší, než mají jejich HW kolegové. Mezi jejich přednosti patří:

- keystrokes (stisky kláves – i vymazané znaky)
- monitorování obsahu schránky (Clipboard)
- monitorování spuštěných aplikací
- monitorování práce s OS (mazání složek, manipulace se soubory)
- screenshoty – nastavení kvality, snímané oblasti (fullscreen, aktivní okno)
- pohyb na Internetu
- záznam chatů Instant messengerů (ICQ, QIP, Miranda, Google Talk, MSN aj.)
- zvukový odposlech
- nastavitelný interval odesílání logů na E-mail, FTP, LAN
- možnost nastavení formátu odesílaných logů s podporou šifrování
- nastavení minimální velikosti logů (neposílání prázdných log souborů)
- sebe destrukce (Ardamax Keylogger)

1.11 Rootkit

Rootkit je jedna z nejnebezpečnějších typů infiltrací, která může napadnout počítač. Má schopnost skrýt svoji přítomnost nebo přítomnost jiného nežádoucího softwaru (vir, červ, trojan) v systému a uniknout tak detekci. Obvykle se jedná o program, který útočníkovi umožňuje skrytí souborů, procesů a systémových údajů, ale také změn v registrech OS, informacích o souborech na discích, případně jejich používání a získat tak plnou kontrolu

nad napadeným počítačem. Jsou schopny maskovat svou činnost za procesy jiných programů, takže pomáhají útočníkovi zůstat skrytý (upravují operační systém tak, aby nebyly běžnými systémovými prostředky zjistitelné). Odstranění těchto škodlivých kódů je velmi složité, i když většina současných antivirových řešení již detekci rootkitů podporuje. Závisí na tom, zdali se rootkit (např. jako trojský kůň) dostal do systému již před instalací samotného antivirového programu. Pokud ne, bývá zpravidla odhalen před infikováním systému. V opačném případě jej ani antivir s nejnovější virovou databází nemusí odhalit a je potřeba použít specializovaných programů třetích stran pro jeho odstranění.

1.12 Backdoor

Backdoor (zadní vrátka) je aplikace, která umožní útočníkovi vzdálený přístup do počítače. Na zvoleném portu (TCP/IP) otevírá komunikační kanál, pomocí něhož s ním útočník vzdáleně komunikuje. Napadené počítače poté mohou sloužit útočníkům k další činnosti jako např. instalaci botů. Častým nositelem backdoorů bývají trojské koně. Jedním z nejznámějších případů je Back Orifice, který bylo možno připojit k jakémukoli spustitelnému .exe souboru a pak např. odeslat emailem.

1.13 Hoax

Hoax - poplašná zpráva šířící se emailem (i IM komunikací), která se nezakládá na pravdě. Obvykle má podobu zábavné zprávy, falešného poplachu nebo prosby. Často je psána s množstvím vykřičníků, velkými písmeny nebo barevně, s textem odkazující se na důvěryhodné zdroje (Microsoft, IBM, Nokia atd.). Zpráva vyzývá k přeposlání (forwardování) dalšímu, zpravidla co největšímu počtu uživatelů. Proto se také označuje jako řetězový e-mail. Riziko u Hoaxů spočívá především v tom, že s následným přeposíláním roste počet e-mailových adres v něm obsažených. Takový mail se může stát následným přeposíláním nositelem několika desítek až stovek e-mailových adres a nabízí tak skvělou možnost ke zneužití spamery. Pomineme-li riziko zneužití e-mailových adres, musíme brát na vědomí také to, že přeposílání zprávy více kontaktům zatěžuje výkon serverů a sítí. Domácí uživatel tento problém řešit nemusí, avšak v podnikové síti je tato otázka opodstatněná.

1.13.1 Příklad hoaxu

Důležité upozornění pro majitele mobilních telefonů!! Pokud se někomu z vás objeví na mobilním telefonu hovor a na displeji uvidíte "ACE-?", NEZVEDAT, ale okamžitě ODMÍTNOUT! Jde o virus, který všechna IMEI a IMSI data na telefonu a SIM kartě vymaže. Tak nemůže přístroj žádná data přijmout ze sítě a je nepoužitelný. Tuto informaci potvrdili výrobci Motorola a Nokia, je také k nalezení na stránkách CNN. 3 miliony mobilních telefonů byly už tímto virem zničeny. Pošlete tuto zprávu na další uživatele mobilních telefonů!! [14]

1.14 Exploit

Exploit je program, využívající bezpečnostní díru v operačním systému, webovém prohlížeči nebo jiných programech, která dovoluje útočníkovi ovládat systém a provádět v něm změny. Ochrana proti těmto chybám v softwaru je ve formě aktualizací, hotfixů a updatů popř. service packů, které poskytuje výrobce daného programu.

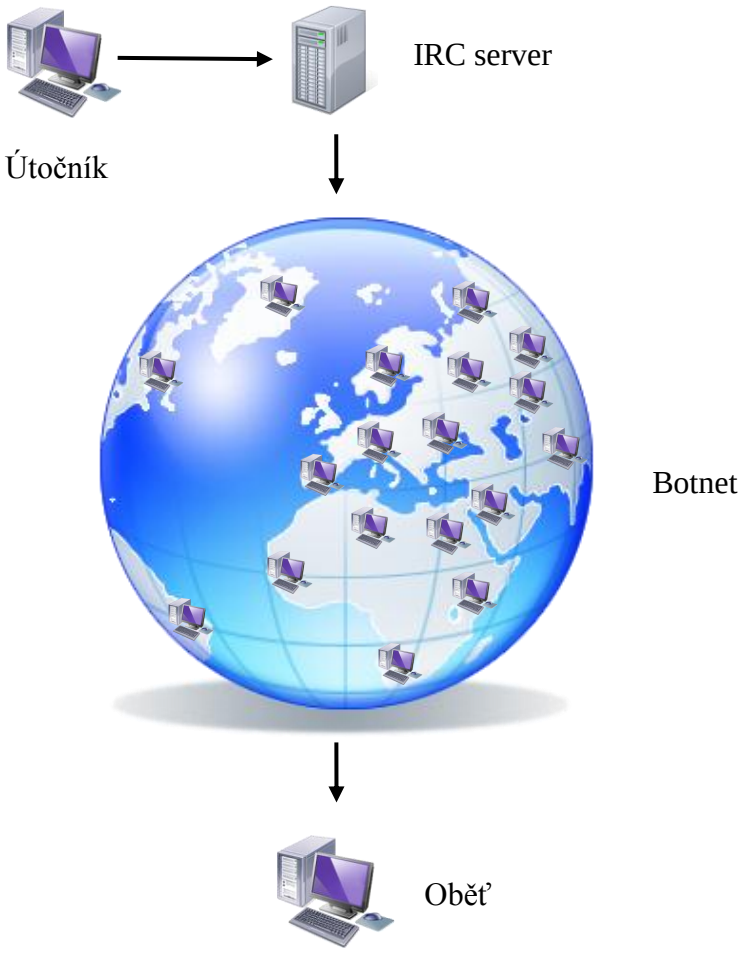
1.15 Botnet

Botnetem se rozumí síť infikovaných počítačů, stejným typem škodlivého kódu. Bot (od českého slova robot) je program, který do systému dokáže proniknout skrze slabé místo v zabezpečení, díky jedné z výše popsaných infiltrací (zpravidla se jedná o backdoor nebo exploit) a dokáže vzdáleně plnit příkazy jeho autora. Nejčastěji se tak děje přes P2P sítě nebo IRC kanály. Takto na dálku útočníkem ovladatelné počítače, označované jako zombie, mohou být následně zneužity k hromadnému rozesílání nevyžádané pošty (Spamu), protože jednotlivé počítače nejsou předem tak podezřelé a je jich tolik, že odfiltrování je téměř nemožné. Dále pak k masivnímu DDoS útoku nebo k rozesílání dalšího malwaru. Nejčastějšími oběťmi botů jsou většinou počítače domácích uživatelů, protože je u nich velká pravděpodobnost slabého zabezpečení a snadného zneužití. Na druhé straně jsou pak firemní PC, u kterých se sice předpokládá vysoká úroveň zabezpečení, ale také poskytnutí většího výkonu a rychlejšího připojení do sítě Internet. Botnety mohou být složeny až ze statisíců nakažených počítačů a jsou tak útočníkovi schopny poskytovat obrovský výkon a konektivitu zdarma, na úkor samotných uživatelů (především zvýšená zátěž procesoru a síťových aktivit).

Toto uskupení se dále stává velmi výnosným byznysem, neboť si lze botnety (i konkrétní počet počítačů) pronajímat za peníze a využívat tak jejich služeb. Společnosti závislé na Internetu a zisku plynoucího z něho, mohou být vydírány DDoS útoky a v případě nezaplacení požadované částky hrozí, že se útok uskuteční. Otázkou je pouze kolik počítačů daný útočník potřebuje a jakou cenu je za ně ochoten zaplatit. [15]

1.15.1 DoS

Denial of Service (Odmítnutí Služby) neboli DoS útok je technika sloužící k zahlcení serveru, služby, sítě nebo konkrétního počítače formou nekonečných požadavků. Útok může pocházet z jediného, na dálku řízeného (i lokálního) počítače, ale i z desítek, stovek nebo tisíců počítačů zapojených v síti. V tomto případě se jedná o DDoS útok (Distributed Denial of Service). Takovýmto útokem může být docíleno, že daná služba, server nebo síť nebude dostupná, nebude odpovídat, zhroutí se a bude nucena k restartu. [16]



Obr. 10. Schématicky znázorněný příklad DDoS útoku pomocí sítě Botnet

2 SOCIÁLNÍ INŽENÝRSTVÍ

Sociálním inženýrstvím (sociotechnikou) se rozumí přesvědčování a ovlivňování lidí, s cílem oklamat uživatele tak, aby uvěřil, že útočník je ten, za koho se vydává. Dokázal ho zmanipulovat k vyzrazení důležitých informací nebo přimět k provedení určitých činů v jeho prospěch. Velkou měrou vyplývá z psychologie a je založeno zpravidla na důvěřivosti, strachu, soucitu nebo nátlaku. Úspěch sociotechnika, jak se útočník nazývá, závisí především na jeho znalostech a vědomostech o konkrétním subjektu, na který chce útočit. Na základě těchto informací, které si předem zjistí, se pak odvíjí jeho útok (např. chce-li se nabourat do podnikového serveru, zjistí si informace o dané společnosti, zaměstnancích, vedoucích pracovnících, firemní infrastruktuře, používané technice, bezpečnostní politice a zvyklostech, které jsou uvnitř typické apod.). Všechny tyto informace pak cíleně využije pro uskutečnění svého plánu. Zpravidla se vydává za důležitou osobu, člověka, který potřebuje pomoc nebo naopak za člověka, který pomoc nabízí. Ve všech případech však využívá uživatele, jako nejslabšího článku, protože právě přes něj vede nejjednodušší cesta, jak se k tíženému cíli dopracovat, aniž by musel překonávat složité, jak hardwarové, tak softwarové bezpečnostní prvky. [26]

Tato práce se zabývá sociálním inženýrstvím páchaným prostřednictvím Internetu pomocí současných technik.

2.1 Phishing

Phishing (česky známý také jako rhybaření) je druh internetového podvodu, jehož cílem je vylákat z uživatele citlivé informace jako např. čísla bankovních účtů, hesla, CVV a CVC kódy, čísla platebních karet nebo jiné identifikační či autentizační údaje. Phishing je tak obrazové znázornění rybolovu, kde je návnadou podvodný email, který čeká, až se na něho nějaký, problematiky neznalý uživatel chytí a zareaguje na něj.

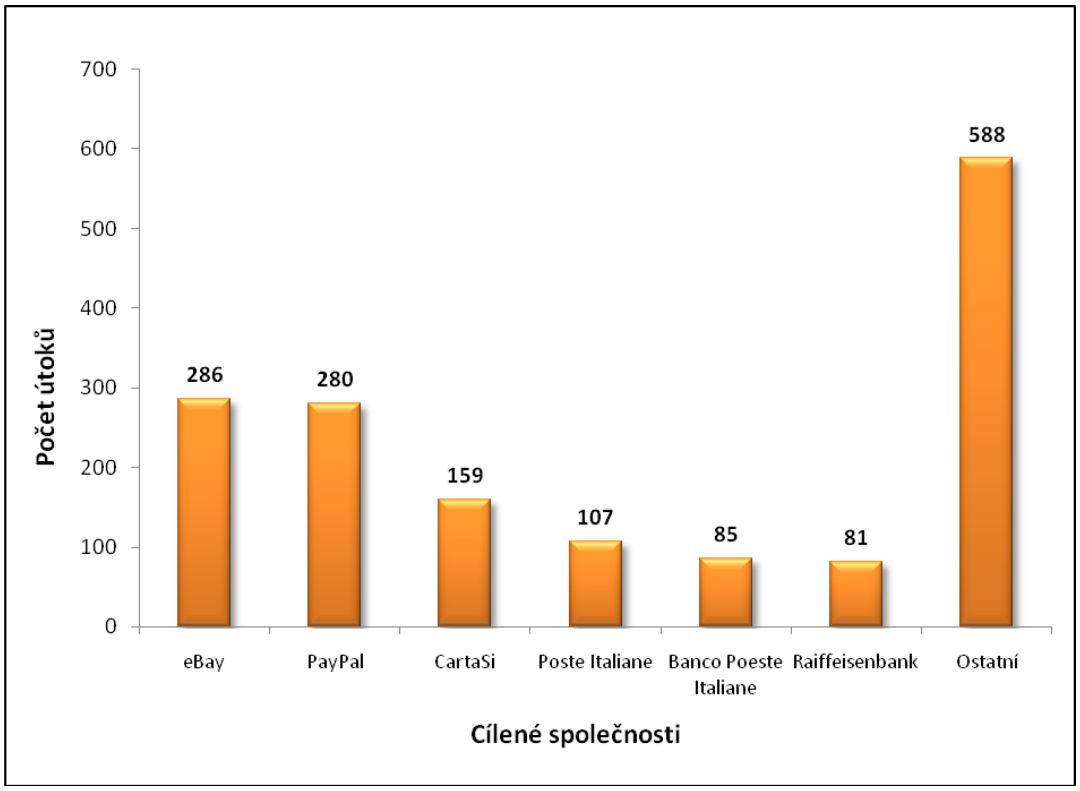
Phishing probíhá nejčastěji pomocí elektronické pošty (možné také přes IM komunikaci nebo webové stránky), kdy útočník (Phisher – autor phishingu) rozesílá podvodné phishingové emaily, které jsou často nerozeznatelné o těch pravých a vydává se v nich za bankovní nebo jiné, nejčastěji finanční instituce (může se jednat také o webové služby – PayPal, eBay, Amazon). Jejich prostřednictvím pak vyzývá k reakci na zprávu v emailu. Jedná se zpravidla o žádost ověřit účet, nebo potvrdit informace z důvodu například úpravy

databáze nebo zavedením nového bezpečnostního prvku. Uživatel je pak dále přesměrován na podvodné webové stránky, vypadající totožně jako korektní stránky dané společnosti, lišící se jen nepatrnou změnou ve své URL adrese (např. ve změně znaku: WWW.CS0B.CZ místo WWW.CSOB.CZ). Takto zmanipulovaná oběť se pak ve snaze podřídit se dobré věci, stane dobrovolným dárcem svých důležitých údajů.

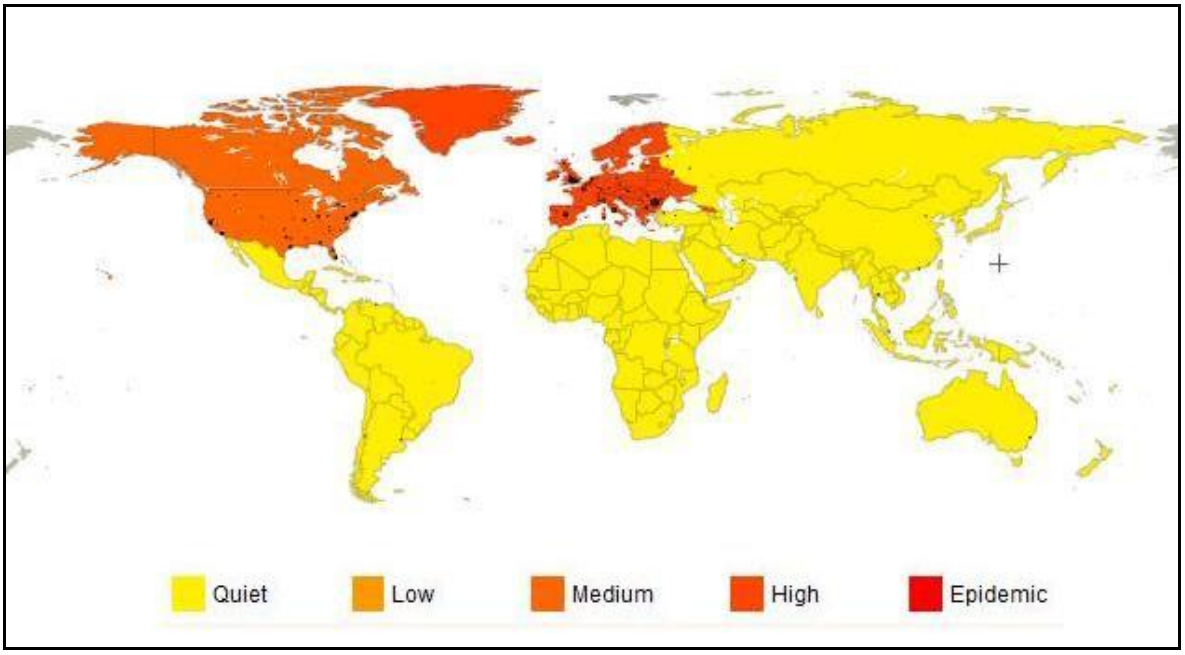
Mezi nejznámější a nejrozšířenější phishingové cíle patří banky a zneužívání internetového bankovnictví (e-banking). Jedná se především o velké a známé banky (Bank of America, Western Union, Citibank) u kterých je předpoklad, že velká část oslovených je právě jejich klientem. Tyto emailové zprávy jsou překládány do mnoha světových jazyků, aby se zvýšila cílená skupina uživatelů. Často se tak děje za pomoci automatických překladačů, jejichž výsledky jsou tak mnohdy nesrozumitelné a někdy dokonce i vtipné (např. oslovení *Drahoušek zákazník*). Najdou se však i takové, které jsou výborně zpracované v konkrétním jazyce. Může se tak stát, že phishingový email přijde i člověku, který bankovním kontem u zmiňované banky vůbec nedisponuje a nemá s ní nic společného.

Důležité pravidlo, které by mělo platit všeobecně, říká, že banka se svými klienty prostřednictvím elektronické pošty nikdy nekomunikuje. V případě že ano, mají její zprávy výhradně informativní charakter, neobsahují žádné aktivní linky a v žádném případě nevybízejí uživatele k přihlášení k účtu.

Statistiky ukazují, že z obrovského množství podvodných emailů, které jsou dnes v oběhu, na ně zareaguje přibližně 1% lidí, zisk phisherů se však stále pohybuje v miliónech dolarů měsíčně. [17]



Obr. 11. Graf znázorňující počet phishingových útoků na vybrané cíle. [18] Údaj poskytuje informace za poslední 3 měsíce a je platný k datu 13. 4. 2009. Zdroj http://www.avira.com



Obr. 12. Mapa světa zobrazující země, které jsou největšími zdroji phishingu. [19] Údaj poskytuje informace za poslední 3 měsíce a je platný k datu 13. 4. 2009. Zdroj: http://www.avira.com

2.1.1 Ochrana před phishingem

Ochrana před podvodnými emaily existuje, avšak zdaleka není dokonalá. Dnešní moderní webové prohlížeče sice obsahují filtry proti podvodným stránkám. Emailoví klienti se snaží odhalovat phishingové emaily a zakazovat spouštění obsahu z přiložených adres. Také tvůrci bezpečnostních prvků nabízejí ve svých řešeních doplňky na detekci toho druhu internetové kriminality. A tak největším problémem zůstává stále slabá informovanost široké veřejnosti o tomto problému. Proto všechny tyto bezpečnostní prvky bohužel často selhávají na nejslabším článku řetězce - člověku.

Všechny kvalitní webové služby, ať už se jedná o elektronické bankovnictví, emailové schránky nebo sociální sítě, dnes používají zabezpečené spojení https:// komunikující na šifrovaného protokolu SSL/TLS, podepsané digitálním certifikátem, který spravuje vybraná certifikační autorita (znázorněné někdy malou ikonou zámku v adresním nebo stavovém řádku). Problémem je však opět v samotném uživateli, který často ignoruje varování, které ho upozorňuje, že daný certifikát je neplatný nebo se ho nepodařilo ověřit. V případě, že se žádná výzva nezobrazí, se už neobtěžuje zjišťovat, komu daný certifikát patří a vstoupí na webovou stránku.

Ochrana před phishingem proto může znít takto. Nikdy nezadávat důležité údaje na odkazované stránky z emailů. K e-bankingu přistupovat pokud možno se zabezpečených počítačů a vyhýbat se veřejným místům. Webovou adresu e-bankingu zadávat ručně a ověřit si certifikát, kterým se banka prokazuje. Informovat se o bezpečnostních hrozbách.

2.1.2 Příklad phishingového emailu

Typický příklad phishingu vydávající se za Českou spořitelnu. Email upozorňuje na podvodné emaily a sám přitom vybízí k verifikaci.

Od: Ceská sporitelna [csas@csas.cz] Odesláno: út 11.3.2008 9:02
Komu: Holcik Tomas
Kopie:
Předmět: Varování pred novou verzí podvodných e-mailu
Přílohy:

VERIFIED by VISA

ČESKÁ SPOŘITELNA

Varování pred novou verzí podvodných e-mailu

Vázení klienti,

rádi bychom Vás upozornili na novou verzi podvodného e-mailu (tzv. phishingu). Nová verze e-mailu má jako ty predeslé vzbudit dojem, ze byla odeslána z e-mailové adresy Ceské sporitelny, tentokrát vsak z oficiální e-mailové adresy banky csas@csas.cz. Obsahuje odkaz v tele na údajné webové stránky internetového bankovnictví banky a uzivatel je vyzván k prihlásení, tedy zadání osobních bankovních údaju.

Prosím, verifikujte tuto emailovou adresu kliknutím na spojení níze:

https://www.servis24.cz/ebanking-s24/app/register.pl?code=2E1E-EBB6-EA1N-D1EC&step=vrf_email_actions

Verifikovací spojení je platné do 24 hodin.

Obr. 13 Příklad phishingového emailu České spořitelny [20]

2.2 Vishing

Vishing je další metoda sociálního inženýrství vycházející z phishingu. Může být prováděna přes telefon, avšak daleko lepším řešení je VoIP technologie. Stejně jako v předchozím případě popsaná sociotechnika, využívá i tato, oklamání lidí za účelem zisku a je zaměřená především na organizace manipulujícími s penězi.

Útok probíhá tak, že uživatel obdrží telefonát či hlasovou zprávu, ve které je telefonním automatem informován o nějakém smyšleném bankovním problému (např., že finanční transakci nebylo možné provést, nastal problém s kreditní kartou apod.) a zároveň vyzván, aby se obrátil, na zpravidla bezplatnou telefonickou linku kde potvrdil své osobní údaje.

Technika vishingu se stává čím dál více populární, neboť hlasová komunikace (přestože je jen vygenerovaná přes počítačový program) se jeví důvěryhodnější než emailová zpráva. [21]

Obdobou této techniky je i SMiShing, rozdíl je v upozorňování pomocí SMS zpráv.

Protože je vishing méně v podvědomí uživatelů než phishing, je i ochrana komplikovanější než před minulou technikou. Uživatel proto musí spoléhat více na vlastní rozum a méně důvěřovat všem a všemu, co se jeho osobních informací týče. Jedinou možnou obranou se tak jeví přímá interakce s druhou stranou, která by neměla znát odpovědi na vámi kladené otázky.

2.3 Pharming

Modernější a nebezpečnější technika získávání citlivých informací nese název pharming a je označována za novou generaci phishingu. Stejně jako phishing (se kterým má mnoho společného) a jiné sociotechnicky, slouží k oklamání uživatele. Používá při tom však mnohem sofistikovanější metodu, jak toho dosáhnout.

Princip spočívá v napadení DNS systému. DNS neboli Domain Name System (/Server/Service) je databáze obsahující seznam URL a jim odpovídajících IP adres. Zajišťuje překlad mezi IP adresou a URL konkrétní webové stránky. Místo těžko zapamatovatelného čtyřčíslí odděleného tečkami, nám dovolí do adresového řádku napsat snáze zapamatovatelný název námi požadovaného serveru. Tedy např. místo 77.75.76.3 – www.seznam.cz, nebo místo 207.46.192.254 – www.microsoft.com.

Pharmingový útok, tak spočívá v přesměrování požadované webové stránky, na stránku falešnou, ničím se nelišící od originálu. Toho může být docíleno dvěma způsoby.

První možností jak toho dosáhnout, je změnou položky v seznamu překladů na nějakém z DNS serverů, což by vedlo k tomu, že u všech uživatelů, kteří zadají ve svém webovém prohlížeči konkrétní adresu a připojí se na tento DNS server, nedojde k překladu na odpovídající IP adresu, nýbrž na útočníkem podvrženou. Tato metoda není závislá na klientských počítačích, avšak je potřeba zdolat ochranu DNS serveru. Jelikož však DNS servery tvoří páteř celého Internetu, jsou velice dobře zabezpečeny a objevit v nich bezpečnostní chybu, která by se dala zneužít tak, aniž by si toho správci všimli, je extrémně obtížná záležitost.

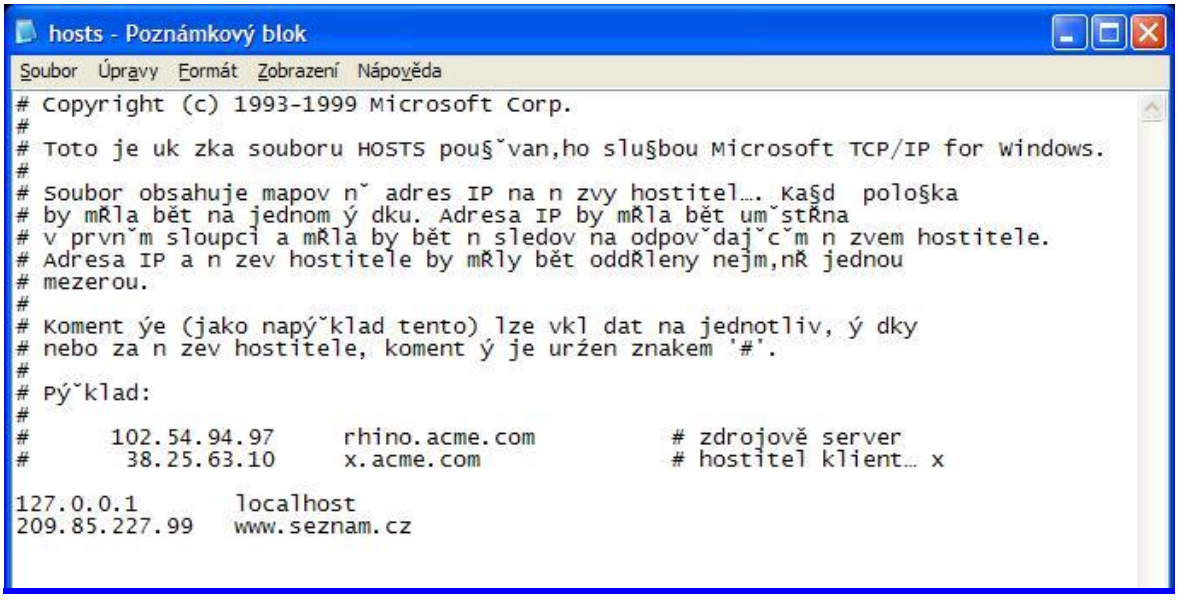
Druhá varianta, jak přesměrovat požadované webové stránky na jinou adresu je daleko méně složitější, a to díky změnám provedeným v hosts souboru umístěném ve složce Windows (zpravidla v C:\WINDOWS\System32\drivers\etc), který je lokální alternativou DNS serverů. V něm se nacházejí IP adresy a jim korespondující URL. Změnu v tomto souboru může útočník provést skrze nějaký druh malwarového programu (červem, trojanem). Obrana proti tomuto útoku je tak zřejmá a vyplývá z dříve zde popsané obrané hloubkové strategie (defense-in-depth strategy).

Jedním z řešení jak zabezpečit hosts soubor je, uzamknout ho a chránit před změnou. To je však diskutabilní, protože jej využívají i jiné aplikace a mohlo by tak docházet ke kolizím.

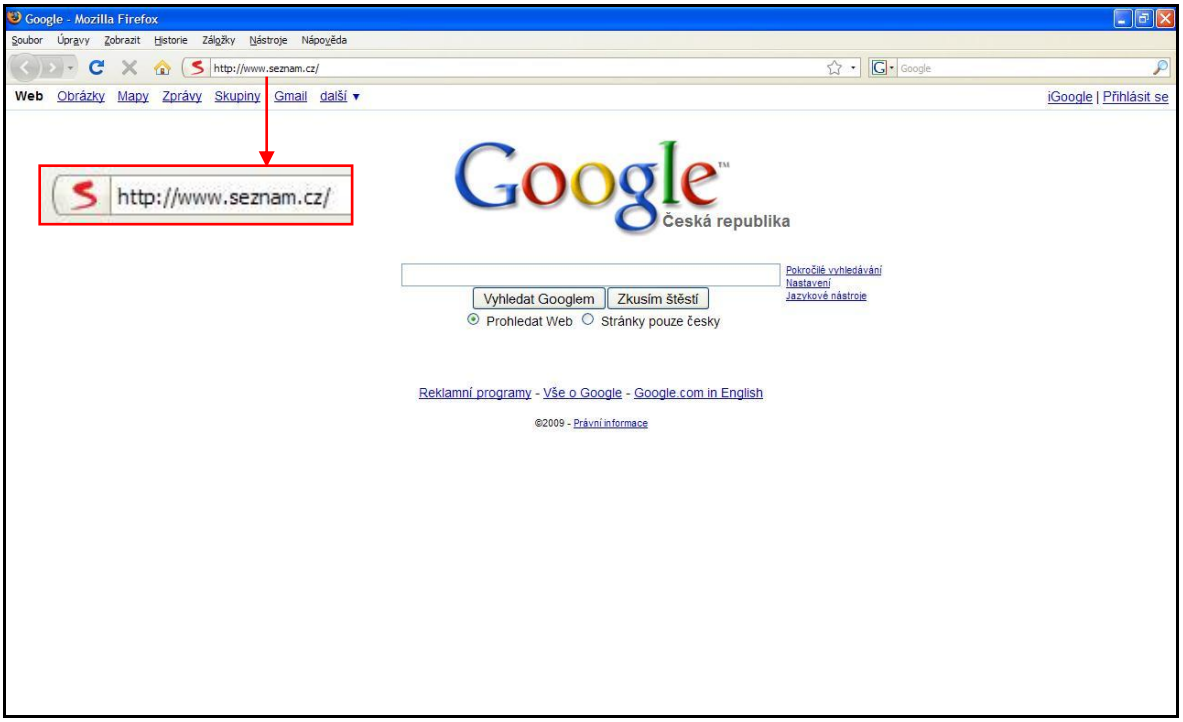
2.3.1 Příklad pharmingu pomocí hosts souboru

Na obrázku číslo 13. je zobrazen hosts soubor z operačního systému MS Windows XP SP2. Pod řádky začínajícími znaky # (značící komentář), se nacházejí dva sloupečky. První obsahuje seznam IP adres, druhý pak URL adresy k nim přiřazené.

Přidáním dalšího řádku můžeme nastavit, jaká URL se má zobrazit pod danou IP adresou. V tomto případě je serveru www.seznam.cz přiřazeno číslo 209.85.227.99, což je IP adresa serveru www.google.com. Po uložení změn v tomto souboru, bude vždy adresa www.seznam.cz přesměrována na stránky www.google.com



Obr. 14. hosts soubor upravený v Poznámkovém bloku



Obr. 15. Webové stránky www.google.com po zadání adresy www.seznam.cz

Z výše popsaného tak vyplývá, že i když uživatel napíše adresu webové stránky správně, na správnou stránku se už dostat nemusí. A jestli se v případě phishingu jednalo o hloupost, důvěřivost nebo nevědomost lidí, u této metody sociálního inženýrství se může stát obětí i zkušený a informovaný IT uživatel. [22]

Jako nevýhoda této techniky oproti předchozím, je její složitost, neboť ne každý útočník má patřičné znalosti, potřebné k jejímu provedení, což se u podvodných emailů říci nedá.

2.4 Cybersquatting

Cybersquatting neboli doménové spekulantství je druh internetové kriminality, jehož podstatou je registrace doménového jména, u něhož je předpoklad, že jej bude v budoucnu potřebovat některá z velkých společností, známých obchodních značek nebo slavných osobností. Tuto doménu se pak snaží squatter prodat za několikanásobně větší cenu, než za jakou by ji pořídil daný subjekt. [23]

Jedním typem této počítačové kriminality je tzv. Typosquatting, kde spekulant předpokládá překlep v psaní. (např: www.gogle.cz nebo www.seynam.cz). [23] Uživatelé, kteří hledají oficiální webové stránky konkrétního produktu či společnosti, se pak takto snadno dostanou na domény, které jsou často zneužívány pro phishingové podvody, šíření malwaru

nebo zobrazování reklam. Z minulosti je znám případ státu Kamerun, kterému patří mezinárodní doména ".cm". V Kamerunu poté odstartovali automatizovaný cybersquatting na všech svých neregistrovaných doménách a doufali, že je budou navštěvovat lidé, kteří při zadávání adresy končící na ".com" vypustí písmeno "o". V praxi to pak znamenalo, že se jejich sponzorované odkazy objevovaly například na microsoft.cm. [24]

Dalším druhem cybersquattingu je Domain grabbing, který má za cíl hromadnou registraci podobných doménových jmen s úmyslem blokování takto alternativně využitelných domén. [23]

Nejčastějšími oběťmi cybersquattingu jsou farmaceutické společnosti, bankovní a jiné finanční instituce, IT společnosti (např.: Google, eBay, Facebook, MySpace, BBC, Blackberry), ale postihovány jsou i sportovní kluby či celebrity (např.: FC Arsenal, Scarlet Johansson, Dennis Rodman, J.R.R. Tolkinen).

Z případů v České republice jmenujme např. spor o doménu ceskapojistovna.cz, kdy Česká pojišťovna vlastnila několik ochranných známek obsahující slova Česká pojišťovna a jejich vlastníkem byla i před registrací domény ceskapojistovna.cz. Pojišťovna proto žalovala původního majitele domény a také sdružení nic.cz (www.nic.cz), které je registrátorem českých domén. Vrchní soud v Praze v srpnu 2004 rozhodl o tom, že tato doména má patřit České pojišťovně. [24]

První případy týkající se internetových domén se objevily již v roce 1999, v roce 2000 šlo už o 1857 případů a dnes se počet případů tohoto druhu kyberkriminality stále zvyšuje. Problematiku cybersquattingu řeší WIPO (World Intellectual Property Organization / Světová organizace duševního vlastnictví) - agentrua při OSN. V České republice se od roku 2004 zabývá řešením těchto sporů Rozhodčí soud při Hospodářské komoře ČR. [24]

ZÁVĚR

Tato práce byla vytvořena za účelem, seznámit a varovat běžného uživatele před nástrahami dnešní doby v oblasti počítačů a celosvětové sítě Internet. Měla za úkol nastínit minulé, současné a v určitém směru i budoucí hrozby a možnosti kyberzločinu, softwarových infiltrací a útoků. Tento text byl vytvořen především z internetových zdrojů, přičemž články ze kterých čerpá, pocházejí výhradně z renomovaných serverů poskytujících ověřené informace a nabízí data od předních světových společností zabývajících se počítačovou bezpečností. Dále je doplněna statistikami a výzkumy několika nezávislých analytických společností, které poskytují konkrétní údaje a čísla, jenž uživatele uvádí do reality spojené s touto prací.

Jelikož téma zde popsané je natolik rozsáhlé, že spadá hluboko za hranice možností této práce, bylo zde nastíněno aspoň základní rozdělení, metody šíření a také potenciální rizika jednotlivých malwarových programů. Dále jsem se snažil čtenáře seznámit s možnostmi jak se proti těmto infiltracím bránit a uvést postup, jak se chovat je-li už systém napaden. V kapitole sociální inženýrství byly představeny současné techniky používané k odcizení osobních informací a citlivých dat, a jejich následné zneužití. I u těchto způsobů kyberkriminality jsem se pokusil uvést řešení, jak se chránit a čeho se vyvarovat, neboť sociotechniky je v dnešní době využíváno ve stále větší míře a díky dostupnosti Internetu a provázanosti jednotlivých služeb je nebezpečnější než kdykoli předtím. Jedinou možností, jak tomu podle mého názoru předcházet je, dostat tyto informace do podvědomí co nejširší veřejnosti, neboť zde nezáleží na technice, tak jako na lidech samotných.

Můj osobní pohled na bezpečnost počítačů (v prostředí OS MS Windows) je velmi kritický, protože dnešní množství malwaru, které je v oběhu, je obrovské a stále velmi rychle stoupá. Jelikož je Microsoft téměř monopolem na trhu s OS, je jasné, že lze tento trend předpokládat i do budoucna. Jako alternativa se mi jeví změna strategie v oblasti identifikace škodlivých kódů ze současného blacklistingu na whitelisting, neboť stávající obrana se přesto jeví jako neúčinná a útočníci vynalézají stále sofistikovanější řešení, jak do systému proniknout. Počítačoví roboti chrlící do Internetu kvanta malwaru se jen tak nezastaví a nezmění-li se přístup tvůrců operačních systémů a bezpečnostních prvků jak této hrozbě předejít, bude lidstvo s kyberkriminalitou i nadále prohrávat.

ZÁVĚR V ANGLIČTINĚ

This work was created for the purpose, to acquaint and alert the casual user before dangers of our time in the field of computers and worldwide net Internet. It was the task to outline the past, present and determine the direction future threats and the possibilities of cyber crime, software infiltrations and attacks. This text was created mainly from internet sources, the articles from which to draw, derived exclusively from reputable servers providing verified informations and offers data from leading world companies conversant computer security. Further is supplemented by statistics and analytical studies of several independent companies that provide concrete data and numbers, which presents users to the reality connected with this work.

Since the theme here described is so extensive that it falls far beyond the possibilities of this work, at least was here outlined the basic fission, dissemination methods and potential risks of each malware programs. Next I tried to acquaint the reader with the possibilities of how to defend against these infiltrations and give instructions how to behave if it is system already infected. In chapter social engineering were presented current techniques used for stealing personal information and sensitive data, and their subsequent abuse. And in these ways of cybercrime I tried to give solutions how protect and what to avoid, because social engineering nowadays is used increasingly, and with the availability of the Internet and cohesion individual services, it is more dangerous than ever. The only way to be preventing in my opinion is, get this informations into the subconscious as the general public, because it doesn‘t matter on technology, as in humans themselves.

My personal view on computer security (in MS Windows OS) is very critical because the current amount of malware that is in circulation, is huge and still rapidly rising. Since Microsoft is almost a monopoly in the market with the OS, it is clear that this trend can be expected in the future. As an alternative to seems me change the strategy in the identification of malicious codes from the current blacklisting to whitelisting because the current defense still appears to be ineffective and attackers inventing increasingly sophisticated solutions to penetrate into the system. Computer robots spouting quantum of malware to the Internet is just not stop and if will the makers of operating systems access and security elements not change to prevent this threat, mankind will continue lose with cybercrime.

SEZNAM POUŽITÉ LITERATURY

[1] NOSKA, Martin. Gartner: Počet počítačů se do roku 2014 zdvojnásobí. *Computerworld.cz* [online]. 2008 [cit. 2009-03-02]. Dostupný z WWW: <http://computerworld.cz/udalosti/gartner-pocet-pocitacu-se-do-roku-2014-zdvojnasobi-1001>.

[2] *Marketshare* [online]. 2009 [cit. 2009-03-02]. Dostupný z WWW: <http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8&qpmr=100&qpdt=1&qpct=3&qptimeframe=M>.

[3] KLIMÁNEK, Oldřich. Viry jsou jiné. Jsou antiviry jen vyhozenými penězi? . *Www.scinet.cz* [online]. 2008 [cit. 2009-03-03]. Dostupný z WWW: <http://www.scinet.cz/viry-jsou-jine-jsou-antiviry-jen-vyhozenymi-penezi.html>. ISSN 1803-1277.

[4] TůMA, Martin. Pouze necelá 2% počítačů s MS Windows nemají bezpečnostní díru. *Www.emag.cz [online]*. 2008 Dostupný z WWW: <http://www.emag.cz/pouze-necela-2-pocitacu-s-ms-windows-nemaji-bezpecnostni-diru/ >.

[5] S ekonomickou krízou vznikajú aj dômyselnejšie techniky online podvodov. *Www.lupa.cz* [online]. 2009 [cit. 2009-03-02]. Dostupný z WWW: <http://www.lupa.cz/tiskove-zpravy/domyselnejsie-techniky-online-podvodov/>. ISSN 1213-0702.

[6] *Antivirus XP 2008 Removal Guide* [online]. 2008 [cit. 2009-03-02]. Dostupný z WWW: <http://www.spyware-techie.com/antivirusxp-2008-how-to-remove-antivirus-xp-2008/>.

[7] KLIMÁNEK, Oldřich. Viry jsou jiné. Jsou antiviry jen vyhozenými penězi?. *Www.scinet.cz* [online]. 2008 [cit. 2009-03-06]. Dostupný z WWW: <http://www.scinet.cz/viry-jsou-jine-jsou-antiviry-jen-vyhozenymi-penezi.html>. ISSN 1803-1277.

[8] *Www.toptenseo.org* [online]. 2009 [cit. 2009-03-10]. Dostupný z WWW: <http://www.toptenseo.org/index.php/top-ten-seo/top-10-sem-browser-tools/>.

[9] KOCOUREK, Jiří. Průzkum: v Británii je každých 10 sekund spáchán kyberzločin. *Www.itbiz.cz* [online]. 2007 [cit. 2009-04-22]. Dostupný z WWW: <http://www.itbiz.cz/pruzkum-kyber-zlocin>. ISSN 1802-1581.

[10] MOLČAN, Filip. Vladimír Brož: Kyberzločinci vydělávají více než prodejci drog. *Www.itbiz.cz* [online]. 2007 [cit. 2009-04-22]. Dostupný z WWW: <http://www.itbiz.cz/mcafee-rozhovor>. ISSN 1802-1581 .

[11] HÁK, Igor. *Moderní počítačové viry*. [s.l.], 2005. 110 s. Univerzita Hradec Králové. Vedoucí bakalářské práce Doc. RNDr. Josef Zelenka, CSc.

[12] LOHNISKÝ , Jakub . *Www.eset.cz : Napadl váš počítač Win32/Conficker?* [online]. 2009 [cit. 2009-04-22]. Dostupný z WWW: <http://www.eset.cz/buxus/generate_page.php?page_id=22668>.

[13] *Hardware Key Loggers* [online]. c2009 [cit. 2009-04-22]. Dostupný z WWW: <http://www.netpcdirect.co.uk/hardware-key-loggers.html>.

[14] *Www.hoax.cz* [online]. 2009 [cit. 2009-03-10]. Dostupný z WWW: <http://www.hoax.cz/hoax/vir-v-mobilnim-telefonu---mobile-phone/>.

[15] NYKODÝMOVÁ, Helena. Botnety: nová internetová hrozba. *Www.lupa.cz* [online]. 2006 [cit. 2009-04-22]. Dostupný z WWW: <http://www.lupa.cz/clanky/botnety-internetova-hrozba/>. ISSN 1213-0702.

[16] HALLER, Martin. Denial of Service (DoS) útoky: úvod. *Www.lupa.cz* [online]. 2006 [cit. 2009-04-22]. Dostupný z WWW: <http://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/>. ISSN 1213-0702.

[17] DOČEKAL, Daniel. Jak se dělá phishing. *Www.lupa.cz* [online]. 2008 [cit. 2009-04-22]. Dostupný z WWW: <http://www.lupa.cz/clanky/jak-se-dela-phishing/>. ISSN 1213-0702.

[18] *Phishing Statistics - Top Targets* [online]. 2009 [cit. 2009-04-22]. Dostupný z WWW: <http://www.avira.com/en/threats/section/phishing/top/7/index.html>.

[19] *Phishing Statistics - World Phishing* [online]. 2009 [cit. 2009-04-22]. Dostupný z WWW: <http://www.avira.com/en/threats/section/worldphishing/top/7/index.html>.

[20] HOLČÍK, Tomáš. Česká spořitelna: phishing na druhou. *Www.zive.cz* [online]. 2008 [cit. 2009-04-22]. Dostupný z WWW: <http://www.zive.cz/Bleskovky/Ceska-sporitelna-phishing-na-druhou/sc-4-a-140704/default.aspx>. ISSN 1212-8554.

[21] HOBZA, Otakar. Vishing - phishing přes telefon. *Www.emag.cz* [online]. 2008 [cit. 2009-04-22]. Dostupný z WWW: <http://www.emag.cz/vishing-phishing-pres-telefon/>. ISSN 1802-4238.

[22] CHVOJKA, Jan. Ochrana proti podvodným e-mailům stojí banky miliony. *Www.itbiz.cz* [online]. 2007 [cit. 2009-04-22]. Dostupný z WWW: <http://www.itbiz.cz/phishing-rhybareni-pharming>. ISSN 1802-1581 .

[23] JANSA, Lukáš. Cybersquatting a jeho podoby. *Www.pravoit.cz* [online]. 2008 [cit. 2009-04-22]. Dostupný z WWW: <http://www.pravoit.cz/view.php?nazevclanku=cybersquatting-a-jeho-podoby&cisloclanku=2008090003>.

[24] KOCOUREK, Jiří. Cybersquatting: když jsou internetové domény v ohrožení. *Www.itbiz.cz* [online]. 2008 [cit. 2009-04-22]. Dostupný z WWW: <http://www.itbiz.cz/spory-domeny-cesko>. ISSN 1802-1581 .

[25] HÁK, Igor. Proaktivní detekce virů. *Securityworld.cz* [online]. 2007 [cit. 2009-04-24]. Dostupný z WWW: <http://securityworld.cz/securityworld/proaktivni-detekce-viru-945>.

[26] ŠIMEK, Richart. *Historie a vývojové trendy ve výpočetní technice* . [s.l.], 2003. 100 s. Masarykova univerzita Brno . Kolokviální práce. Dostupný z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AV	Antivirové/ý
BIOS	Basic Input Output System
CRC	Cyclic Redundancy Check
CVV	Card Verification Value
DoS	Denial of Service
DDoS	Distributed Denial of Service
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
HW	Hardware
IM	Instant Messaging
IP	Internet Protocol
IRC	Internet Relay Chat
IT	Informační Technologie
LAN	Local Area Network
OS	Operační Systém
OSN	Organizace Spojených Národů
P2P	Peer To Peer
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PSI	Personal Software Inspector
SSL	Secure Sockets Layer
SW	Software

TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
VBA	Visual Basic for Applications
VoIP	Voice over Internet Protokol
WIPO	World Intellectual Property Organization

SEZNAM OBRÁZKŮ