Provozně ekonomická fakulta
-
Katedra informačních technologií

Bakalářská práce

Název tématu:

Nebezpečí na Internetu

Vypracoval: Jiří Kočí

Vedoucí bakalářské práce: RNDr. Eva Jablonská, CSc.

2007/2008

Prohlášení

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze kterých jsem při vypracování čerpal.

V Praze dne 15.4.2008

……

podpis

Poděkování

Děkuji vedoucí mé bakalářské práce paní RNDr. Evě Jablonské, CSc. za její laskavý přístup, cenné rady a připomínky, které mi při vypracování této bakalářské práce poskytovala.

Nebezpečí na Internetu

Internet Dangers

Souhrn

Tato práce se zaměřuje na popsání nejčastěji se vyskytujících nebezpečích na Internetu v podobě škodlivého softwaru, se kterým se může běžný uživatel v každodenním životě setkat.

Práce je rozdělena do dvou větších částí. První z nich blíže popisuje vybrané nebezpečné programy a techniky, druhá část se podrobněji zabývá prevencí a tím, jak se může uživatel před daným nebezpečím chránit. Obsahem druhé části je také několik obecných rad, které se doporučují při práci na počítači dodržovat.

Klíčová slova:
Internet, počítačový virus, červ, trojský kůň, spyware, spam, hoax, phishing, antivirový, antispamový, antispywarový program, malware

Summary

This project is focused on a describing of the most frequently occurred dangers on Internet in a shape of a mischievous software that a common user can meet in every day life with.

The project is divided to two more comprehensive parts. The first one describes the term of Internet, choice dangerous programs and techniques. The second one deals much detailed with a prevention and explains what ways can computer users guard against given dangers. There are also several universal advice connected with a protection that is recommended to keep it by every computer work.

Key words:
Internet, computer virus, worm, trojan horse, spyware, spam, hoax, phishing, antivirus, antispam, antispyware program, malware

Obsah

1. Úvod 8
2. Cíl a metodika práce 9
   2.1. Cíl práce 9
   2.2. Metodika práce 9
3. Vymezení základních pojmů 10
   3.1. Internet 10
      3.1.1 Historie Internetu 10
      3.1.2 Internet dnes 11
   3.2. Počítačové viry 12
      3.2.1 Co to vlastně počítačový virus je? 12
      3.2.2 A co počítačový virus není? 13
      3.2.3 Historie počítačových virů: 14
      3.2.4 Možná nebezpečí způsobená virem 14
      3.2.5 Druhy virů 15
         3.2.5.1 Bootviry 15
         3.2.5.2 Souborové viry 16
         3.2.5.3 Multipartitní viry 16
         3.2.5.4 Rezidentní viry 17
         3.2.5.5 Nerezidentní viry (viry přímé akce) 17
         3.2.5.6 Stealth viry – dnes Rootkity 17
         3.2.5.7 Polymorfní viry 18
   3.3. Počítačoví červi neboli worms 18
      3.3.1 Metody infiltrace pomocí červů 19
   3.4. Trojské koně (Trojan) – špión v počítači 19
      3.4.1 Zástupci škodlivých trojských koní 20
   3.5. Spyware 22
      3.5.1 Příznaky spyware v počítači 22
      3.5.2 Druhy spyware 23
         3.5.2.1 Adware neboli reklama 23
         3.5.2.2 Dialer 23
         3.5.2.3 Další trojské koně 23
   3.6. Spam 24
      3.6.1 Spamové nebezpečí 25
      3.6.2 Spam – nyní i v podobě MP3 souboru 26
   3.7. Hoax 27
      3.7.1 Nejčastější případy, kdy se jedná o hoax 27
      3.7.2 Hoaxy a jejich škodlivost: 28
      3.7.3 Názory odborníku na hoax 28
      3.7.4 Typické formy hoaxů: 29
      3.7.5 Klasické podvodné hoaxy 30
         3.7.5.1 Podvodné loterie 30
         3.7.5.2 Nigerijské podvodné emaily 30

3.8. Phishing – podskupina spamu 30
3.8.1 Phishing a jeho způsoby útoku 31
3.8.2 Proč phishing funguje? 33
4. Ochrana před nebezpečím na Internetu 34
4.1. Prevence 34
4.2. Zásady související s prevencí 35
4.3. Ochrana a prohlížeč Internet Explorer 37
4.3.1 Internet Explorer 7 38
4.4. Ochrana před viry 40
4.5. Ochrana před počítačovými červy 42
4.6. Ochrana před trojskými koni 43
4.7. Ochrana před spywary 44
4.8. Ochrana přes spamy 45
4.9. Ochrana před hoaxy 47
4.10. Ochrana před phishingem 47
5. Závěr 49
6. Seznam použité literatury 51
7. Seznam obrázků 53
8. Přílohy 54

1. Úvod

Dnešní Internet je prostředím, od kterého lidé očekávají čím dál tím více. Využívají ho pro svoje nejrůznější každodenní činnosti. Od pracovní činnosti, čtení aktualit ze zpravodajství, korespondenci s dalšími lidmi, získávání nových informací z nejrůznějších oblastí, přes zábavu až například k on-line nakupování. Není problém využívat Internet pro styk s úřady, nejrůznější obchodní transakce, investování a mnoho dalších. Internet se stal, podobně jako dříve mobilní telefon, středem lidského zájmu. Neexistuje už snad žádná oblast informací, které by nebylo možné získat na Internetu.

Přitom lidé samozřejmě očekávají, že se vůči nim bude Internet chovat slušně a důvěryhodně. To znamená, že když na Internetu naleznou požadovanou stránku s hledanými informacemi, automaticky předpokládají, že je zde vše spolehlivé a pravdivé. Dále očekávají, že budou moci bezpečně zjistit, kdo s nimi prostřednictvím Internetu komunikuje. Na druhé straně spoléhají na to, že když oni sami něco Internetu svěří, nedostane se to do nepovolaných rukou. To se týká informací v podobě přístupových hesel, přihlašovacích jmen, e-mailové adresy či jiných osobních informací.

Nic není ovšem tak ideální, jak by se na první pohled mohlo zdát. Existují samozřejmě lidé, kteří dokáží, díky svým odborným znalostem a vytrvalému snažení, vytvářet nebezpečné programy, s jejichž pomocí se pokouší zneužívat informace získané nekalým způsobem od jiných uživatelů ve svůj prospěch.

Žijeme v době, kdy informace mají „cenu zlata“. Proto jsou dnes na počítačovou bezpečnost kladeny stále náročnější požadavky. Specialisté dnes a denně pracují na vylepšení stávajících ochranných programů ve snaze co nejúčinněji chránit uživatele, neboť úsilí a vynalézavost autorů škodlivých produktů nezná mezí.

2. Cíl a metodika práce

2.1. Cíl práce

Úkolem této práce je seznámit běžného uživatele s nejčastějšími hrozbami, se kterými se může setkat kdekoli na Internetu. Práce se zabývá vysvětlením pojmů týkajících se této oblasti a způsoby, jak těmto hrozbám předejít a chránit se proti nim.

První část práce poskytuje stručné a obecné informace o Internetu a jeho využití a popisuje podrobněji vybrané škodlivé programy. Seznamuje čtenáře se způsoby, jak si lze použitím internetových služeb infikovat počítač a představuje možné podoby nebezpečí škodlivých programů. Pozornost je věnována především počítačovým virům, wormům, trojským koním, spamům, spywarům, hoaxům a phishingu.

Druhá část práce je zaměřena na prevenci a ochranu proti těmto zmíněným počítačovým škůdcům.

2.2. Metodika práce

Tato práce byla zpracována na základě analýzy literárních pramenů. K jejímu zhotovení byly použity zdroje v elektronické podobě, především informace o prevenci a ochraně, které byly v práci podrobněji rozebrány a zpracovány. Dále jsem využil vlastních zkušeností se škodlivými programy.

3. Vymezení základních pojmů

3.1. Internet

Internet je celosvětová síť, která spojuje jednotlivé menší lokální sítě pomocí sady protokolů IP. Lze říci, že Internet je síť, která je podobná běžné počítačové síti, ve které jsou počítače vzájemně propojeny pomocí kabelů nebo bezdrátově a díky tomu mezi sebou mohou komunikovat, předávat nebo sdílet data.

Internet je tedy síť počítačů. Ale to by nestačilo – důležitou složkou, která ho vytváří, je jeho vlastní síťový operační systém (protokol). Ten zajišťuje, že na náš pokyn (zadání adresy) se přes v tomto okamžiku volné datové spoje připojíme ke zvolenému počítači kdekoliv na světě. [1]

3.1.1 Historie Internetu

S počátky Internetu je spojena americká armáda, která hledala ve druhé polovině 60. letech 20.století způsob, jak propojit důležitá vojenská centra. To se podařila v roce 1969, kdy byla vybudována síť, která dostala jméno ARPANET. Měla čtyři rovnocenné uzly a každý z nich měl možnost přijímat i vysílat zprávy, což bylo hlavním úkolem této sítě. Jednalo se o decentralizovanou síť, která měla fungovat i při výpadku některého z uzlů.

Arpanet se postupně v dalších letech rozšiřoval a zdokonaloval. V roce 1987 se poprvé setkáváme s pojmem „Internet“ a v síti je propojeno okolo 27 000 počítačů. Devadesátá léta jsou spojená s ukončením sítě Arpanet a také se vznikem World Wide Web (WWW nebo také zkráceně web), který je používán dodnes. [9]

3.1.2 Internet dnes

Internet je fenoménem dnešní doby a člověk, který na něm neumí pracovat nebo ho dokonce nezná je v určité nevýhodě.. S touto obrovskou, celosvětovou počítačovou sítí přicházejí uživatelé do styku i při řešení denních rutinních záležitostí.

Kamenné obchody se postupně transformují do virtuálních obchodních domů. Takřka všechny banky dnes umí provádět rozličné finanční transakce pouhým „kliknutím“ myši. Denně po Internetu proudí miliardy e-mailů, obrázků, filmů, hudby, programů – všechno hmotné, co je jen možné převést na digitální formát, denně koluje sem a tam, z jednoho místa na světě na druhé. [2]

Jeho největší nevýhodou je, že skrývá nespočetné množství nebezpečí nejrůznějších druhů. A to jak ve formě malware, který může zapříčinit svou přítomností v počítači uživatele chaos, ztrátu či zneužití jeho důležitých soukromých dat, tak ve formě útoků na uživatelovu psychiku, city nebo dokonce zdraví.

Malware je nový pojem, který v sobě zahrnuje všechny softwarové hrozby pro počítač nebo server. Jedná se zejména o tyto hrozby:

- Viry
- Trojské koně
- Spyware
- Adware
- Phishing
- Spam

Malware je tedy jakýkoliv program, kód nebo funkce, který narušuje bezpečnost nebo soukromí, případně i pohodlí při práci s počítači. [24]

Uživatel je schopen na Internetu trávit několik hodin denně, neboť právě díky němu je možno utéci od běžné reality do světa plného virtuálních kamarádů, u kterých často člověk nachází větší porozumění a soucit než ve skutečném životě. Díky velké

anonymitě ze sebe uživatel může vytvářet vymyšlený ideál, se kterým se ve virtuálním světě ztotožňuje a vydává se za něj. Toto je často příčinou, kdy se uživatel stává na Internetu dokonce závislým. Dlouhé vysedávání a několikahodinové hledění do obrazovky může mít samozřejmě negativní dopad na zdraví uživatele. Poměrně vážné nebezpečí také představují erotické a pornografické stránky, které si mohou díky anonymitě prohlížet často i nezletilé děti.

Boj proti nebezpečí na Internetu je neustálý, proti sobě na jedné straně stojí běžní uživatelé a na druhé straně autoři nebezpečných serverů.

3.2. Počítačové viry

S největší pravděpodobností každý, kdo se v dnešní době pohybuje ve světě počítačů, se s počítačovým virem minimálně jednou setkal nebo o něm alespoň slyšel či četl. V každém případě se jedná vždy o nějaký problém.

3.2.1 Co to vlastně počítačový virus je?

Na tuto otázku není jednoznačná odpověď, neboť existuje mnoho definic, které nám říkají, co je počítačový virus. Např. podle knihy „Computerviruses.Theory and Experiments“ autora F.Cohena je virus: Program, který může infikovat jiné programy tím, že k nim přidá vlastní kopii. Touto infekcí se může virus šířit v počítači nebo v síti tak, že si uživatelé infikují vlastní programy. Každý infikovaný program se může chovat jako virus a tím se virus šíří. [12]

Obecně lze virus definovat jako programový (spustitelný nebo interpretovatelný) kód, který se bez vědomí uživatele replikuje (tedy množí a šíří). Reprodukce je pro viry charakteristická, není nutné, aby měly škodlivé projevy.

Některé viry jsou relativně neškodné popřípadě pouze obtěžující, ale mnoho z nich vzniká za určitým účelem, kterým může být cílené ničení např. zformátování pevného disku, poškození FAT tabulky, dat aj.

3.2.2 A co počítačový virus není?

Objevily se informace o virech, které spalují monitory přepnutím na vysoké pracovní frekvence, které dokážou "uvařit" procesor zadáním náročného matematického výpočtu, které mohou zrušit pevný disk nebo ničí hlavičky pevných disků jejich rychlým pohybem a prudkým zastavováním a mnoho dalších. I když byly tyto příhody před několika lety zaznamenávány, stojí na vině především nižší kvalita hardwaru, nikoli vir (program). Je tedy třeba říci, že žádný počítačový program, tedy ani virus, nemůže zničit hardware počítače, neboť je proti tomu ochráněn a prakticky neexistuje způsob, jak tuto ochranu obejít.

Při studování různých druhů virů je možné zjistit jistou výjimku, do níž se zahrnují viry, které umí přepisovat flash paměť počítače. Tato paměť je umístěna na základní desce. Je v ní uložen základní program BIOS (Basic Input/Output System), který se spustí hned po zapnutí počítače. Bez tohoto programu se počítač nespustí. Slouží jako správce a kontrolor hardwaru a dále poskytuje určité služby dalšímu softwaru. A právě tuto paměť typu flash s BIOSem přepisují viry nesmyslnými daty, tím tak znemožní start počítače a bez opravy už počítač není nadále schopný provozu. Ale příčinou je softwarová chyba, nikoliv zničení hardwaru. [2]

Počítačový virus tedy napadá určité programy a je schopen se při šíření sám modifikovat, čímž ztěžuje uživateli svou detekci.

Napadený program:

- pracuje jinak než jak bylo původně zamýšleno
- šíří další kopie viru
- je infikován pouze jednou
- může se určitou dobu chovat nevinně
- může být vůči určitému viru imunní

3.2.3 Historie počítačových virů:

Co se historie virů týče, objevují se už v padesátých a šedesátých létech první zákeřné programy s vlastní životaschopností v povídkách vědecko-fantastických autorů. Teprve od konce osmdesátých let představují pro uživatele počítačů vážnou hrozbu. V roce 1981 byl naprogramován první funkční vir na platformu Apple Macintosh, ale kvůli malému rozšíření počítačů se v té době velké reprodukce nedočkal. Teprve 19.ledna 1986 se objevil virus Brain (mozek) pro IBM PC, který útočil na určitou část disku. Na starších počítačích dokázal způsobit větší škody. Oproti tomu dnešní viry jsou daleko vyspělejší a dokážou zhroutit i celou síť počítačů. [9]

3.2.4 Možná nebezpečí způsobená virem

V zásadě lze uvést, že možné nebezpečí závisí na konkrétním viru. U destruktivního viru se může přihodit prakticky cokoliv. Ať už to jsou uživatelova důvěrná data, která mohou být rozeslána na náhodné adresy, tak kompletní smazání či zformátování disku.

U nedestruktivního viru jde především o tyto projevy:

- Snížení výkonu programů, které je způsobeno virovou aktivitou. K aktivaci viru může dojít před spuštěním programu, uprostřed jeho vykonávání nebo při ukončení programu.
- Úbytek místa na disku, kdy je hostitelský program virem zvětšen a tím dochází ke snížení volného místa na disku.
- Vynášení důvěrných dat, kdy je vir schopen najít uživatelovy důvěrné informace jako jsou například přístupová hesla nebo čísla kreditních karet a ty odeslat autorovi daného viru.
- Snížení výkonu počítače v důsledku přítomnosti viru, který dokáže na pozadí vyhledávat a infikovat další programy.
- Poruchy operačního systému a programů, které jsou zapříčiněny chybou v daném kódu viru.

- Další nepříjemnosti mezi které patří automatické stahování a instalace nechtěných programů z Internetu, chyby na disku, zpomalení sítě Internet, apod. [2]

3.2.5 Druhy virů

Viry lze dělit podle různých hledisek:

- podle cíle infekce
- podle umístění v paměti
- podle projevu chování

A) Podle cíle infekce:

3.2.5.1 Bootviry

Jejich mechanismus šíření je velmi jednoduchý, neboť stačí získat médium, jehož zaváděcí oblast je napadena virem. Pak už se stačí jen pokusit nastartovat operační systém z tohoto média (ať už úmyslně nebo neúmyslně – např. proto, že jste zapomněli vytáhnout disketu při startu nebo restartu počítače. Při startu systému se startovací rutina pokouší zavést operační systém z prvního dostupného zařízení podle pořadí určeného nastavením v BIOSu. V praxi tedy předá řízení kódu uloženému ve spouštěcí oblasti tohoto média. Zde uložený virus je aktivován a zahájí svou činnost. Infekce disku spočívá nejčastěji v tom, že se virus zapíše do zaváděcí oblasti pevného disku a její původní obsah si většinou uschová na bezpečné místo např. do klusteru, který potom označí jako vadný. Od této chvíle má kontrolu nad operačním systémem při každém jeho startu z pevného disku. Jakmile takový bootovací virus zachytí požadavek na práci s disketou prohlédne si její spouštěcí oblast, aby ověřil zda již byla infikována. Pokud nebyla, zapíše do její zaváděcí oblasti kód viru. Od tohoto okamžiku je taková disketa napadena virem, stává se tedy nosičem, s jehož pomocí se virus přenáší na jiné počítače. Protože ani sám operační systém nezapisuje běžně do zaváděcí oblasti, je tato akce vždy spojená s podezřením na bootovací vir.

Hlavní výhodou bootvirů je to, že se dostanou do paměti jako první program zaváděný z disku nebo z diskety. Díky tomu mají k dispozici informace o stavu počítače bezprostředně po jeho startu a mohou také ovlivňovat činnost všech následně spuštěných programů. [13]

3.2.5.2 Souborové viry

Napadají soubory. Cílem viru je, aby provedením hostitelského kódu došlo k rozmnožení virového kódu, nejčastěji se jedná o soubory EXE a COM. K aktivaci a zavedení do paměti tohoto typu virů dochází spouštěním infikovaného souboru s programem.

Souborové viry lze dělit na:

- **Přepisující viry** - které jsou s největší pravděpodobností nejjednodušší formou počítačových virů, většinou bývají okamžitě odhaleny. Způsob infekce spočívá pouze ve vyhledávání spustitelných souborů, kterým vir přepisuje jejich obsah sám sebou a tím dochází vlastně k jejich ničení.
- **Link viry** – připojují se k infikovanému souboru a zachovávají jeho původní funkce. Tyto viry mění spustitelný kód své oběti tak, aby při spuštění napadeného souboru došlo nejprve k aktivaci programového kódu viru, který provede vše, co považuje za nutné (např. napadení dalších souborů), a poté obnoví a spustí původní program.
- **Doprovodné viry** – nezapisují svůj kód přímo do napadeného EXE souboru, ale vytváří kopii souboru stejného jména, ale s příponou COM. Využívají tak vlastnosti MS DOSu, který při spouštění dává COM souborům přednost. [13]

3.2.5.3 Multipartitní viry

Tyto viry napadají soubory i systémové oblasti (jsou kombinací bootvirů a souborových virů). Při útoku na soubor mohou multipartitní viry využívat libovolný postup souborové infekce a napadení systémové oblasti je shodné s technikami používanými běžnými bootviry.

B) Podle umístění v paměti:

3.2.5.4 Rezidentní viry

Mohou neustále ovlivňovat činnost počítače. Jsou uloženy v operační paměti počítače, ve které zůstanou až do doby vypnutí počítače. Jejich velkou výhodou je, že si nemusí samy hledat programy vhodné k napadení. Viru stačí pozorovat, se kterými soubory uživatel pracuje a útočit na ně.

3.2.5.5 Nerezidentní viry (viry přímé akce)

Aktivují se pouze během spuštění infikovaného souboru, kdy musí stihnout vykonat veškeré své povinnosti (např. rozšíření do nalezených nenakažených souborů) a poté předat kontrolu původnímu programu.Virus musí svoji činnost provést co nejrychleji, aby uživatel nic nepoznal.

C) Podle projevů chování:

3.2.5.6 Stealth viry – dnes Rootkity

Název této skupiny je odvozen z anglického slova “stealth“- tj.tajnost. Hlavním rysem těchto virů je schopnost maskovat svoji přítomnost na počítači. Pokud je virus tohoto typu přítomen v paměti, dokáže převzít kontrolu některých funkcí operačního systému a při pokusu o čtení infikovaných objektů a místo skutečného obsahu vracet stav před infekcí. Tyto viry byly charakteristické pro operační systém MS DOS.

V souvislosti s vývojem operačních systémů (Windows XP, Windows Vista) se objevil pro Stealth viry v nedávné době nový pojem „rootkit“. Je to program, který se zdokonalil oproti původním stealth virům technikami maskování své přítomnosti v počítači. Rootkity umožňují útočníkovi převzít plnou kontrolu nad uživatelovým osobním počítačem. Podobně jako trojské koně, tak i rootkity instalují sebe sama. Využívají k tomu několik způsobů. Prvním je instalace prostřednictvím zranitelností počítačů připojených k síti. Další pomocí utajených doplňků zpráv elektronické pošty nebo spustitelných programů.

Princip funkčnosti rootkitů je následující. Pro názornost je uveden zjednodušený příklad. Máme operační systém, antivirový program a virus. Pokud je vše v pořádku, antivirový program virus při kontrole systému nalezne. Ovšem vstoupí-li do hry rootkit, mohou být soubor nebo oblast s virem skryté tak, že o nich operační systém nepředá žádné informace antivirovému programu (operační systém je jednoduše nevidí). Proto je daný antivir v napadeném počítači nemůže prohledat a detekovat. Rootkit se fakticky postaví nad operační systém, kterému modifikuje určité volání a funkce, čímž začne řídit jeho činnost.

Jinak řečeno rootkit změní princip fungování operačního systému tak, že tento i všechny aplikace nad ním postavené vidí jen to, co jim ukrytý rootkit dovolí vidět. Naopak co jim vidět nedovolí, to neuvidí. Z tohoto je možné konstatovat, že samotný rootkit nebezpečný není. To jen v případě, že skrývá pouze sám sebe. Ovšem rootkit neumí skrývat jen sebe, ale i jiné nebezpečné aplikace. [7]

3.2.5.7 Polymorfní viry

Mění svou podobu. Hlavní vlastností těchto virů je skutečnost, že žádné ze dvou kopií virového těla nejsou totožné. Virus je zakódovaný a dělí se na dvě části (dekódovač, tělo zakódovaného viru). Tento virus ve snaze uniknout skenování a následnému objevení se vrací jako nový virus, s kterým se antivir ještě nesetkal, čehož dosáhne kódováním části těla při výrobě své kopie, přičemž použije jiný kódovací klíč, který si náhodně vygeneruje.

3.3. Počítačoví červi neboli worms

Počítačoví červi se vyskytují na Internetu již okolo třiceti let a využívají především nevědomosti, nepozornosti nebo hlouposti uživatele, nízkého zabezpečení nebo chyb v systému. Mohou nechávat otevřená zadní vrátka v počítači, posílat hesla nebo rozesílat spam. Šíří se především pomocí elektronické pošty, jako soubory v přílohách pošty a napadají adresy nalezené v adresáři infikovaného počítače.

Původním záměrem vyvinutí počítačových červů nebylo škodit, ale naopak pomáhat při práci na počítači.

Červ je program, který pracuje podobně jako počítačový virus. Rozdíl spočívá v tom, že červ nenapadá soubory a nepotřebuje ke svému šíření hostitele. Stačí mu pouze počítačová síť, přes kterou rozesílá své kopie a rozmisťuje je na připojené počítače. Následkem tohoto šíření může dojít až k zahlcení sítě. [2]

3.3.1 Metody infiltrace pomocí červů

- Spustí se pouze tehdy, pokud je spustí nepozorný uživatel. Mohou se tedy šířit neustále, protože teoreticky se vždy najde uživatel, který červa svou nevědomostí nebo nepozorností spustí.
- Šíří se nekontrolovaně. Využívají chyby v programech a nezabezpečené systémy.

Existují i červi, kteří dokážou jak využívat obě metody infiltrace, tak na napadeném počítači nainstalovat různé trojské koně. Tím se dostáváme k dalšímu vážnému nebezpečí na Internetu, které se nazývá trojský kůň.

3.4. Trojské koně (Trojan) – špión v počítači

Označení trojské koně získaly tyto programy podle starověkých řeckých bájí, kdy se Řekové rozhodli dobýt město Trója úskočnou lstí – darovali tamějším obyvatelům dřevěného koně, v jehož útrobách byli skryti vojáci. Paralela s novodobými elektronickými verzemi trojských koňů je jasná. [19]

Jako viry a červi, tak i trojský kůň je počítačový program, který se jeví na první pohled jako neškodný, nebo dokonce nadmíru užitečný, případně zábavný software, ale místo toho provádí destruktivní nebo špionážní činnost, o které uživatel neví a dokonce ji nemůže nijak ovlivnit.

Drtivá většina trojských koní se od klasických počítačových virů liší tím, že se nesnaží o samovolné kopírování a šíření sebe samotného. Nejčastějším způsobem jak se

nakazit trojským koněm, je otevření nějaké neznámé přílohy v e-mailu, která vypadá jako běžný soubor.

Základním pravidlem je, aby člověk také trochu přemýšlel, pokud se pohybuje na Internetu a neklikl na vše, co se snaží získat jeho pozornost – například: „JSTE 999 999 999 NÁVŠTĚVNÍK VYZVEDNĚTE SI SVOU VÝHRU ZDE!“ [17]

3.4.1 Zástupci škodlivých trojských koní

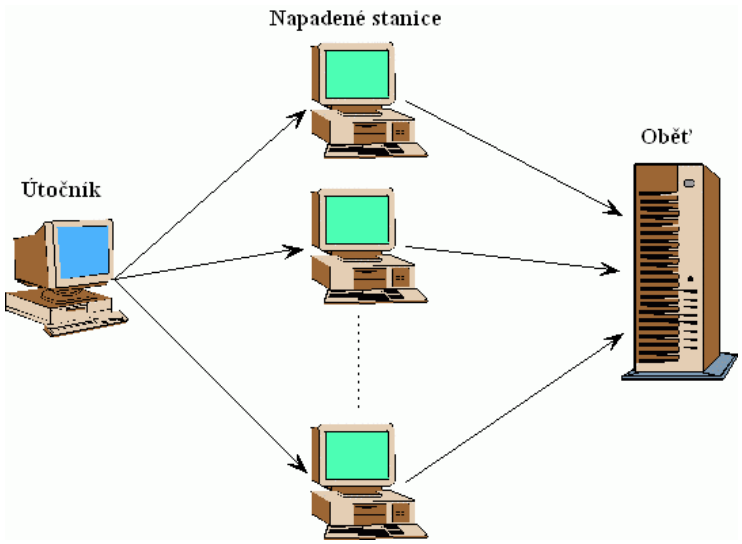
Škodlivá činnost trojských koní je rozsáhlá, ale přesto lze rozlišit některé typy:

- **Trojské koně pro síťové ovládání vzdáleného systému** (RAT) – umožňují útočníkům kontrolovat uživatelův počítač prostřednictvím internetového připojení. Trojský kůň zobrazuje a mění soubory, sleduje a zaznamenává aktivity oběti a využívá počítač k útokům na další počítače jiných uživatelů. Většinou pracuje na pozadí při každém startu napadaného počítače. Příkladem jsou tzv. backdoory („zadní vrátka“), které útočníkovi umožňují vzdáleně ovládat počítač, aniž by o tom napadený uživatel věděl. Zadní vrátka umožňují útočníkovi obejít běžné ověření identity uživatele při vstupu do programu nebo do systému, zároveň skrývají tento přístup před běžnou kontrolou. Backdoor je kód, který může mít formu samostatně instalovaného programu nebo je modifikací stávajícího systému. Pokud se program do systému nainstaluje ukryje se tak, aby maximálně ztížil nebo znemožnil svou detekci. Poté se nastaví tak, aby byl spouštěn při každém startu počítače. Zatímco uživatel pracuje na počítači, backdoor si stále hlídá, jestli se někdo nesnaží přes síť připojit na počítač. Pokud ano, tak mu to umožní. V tomto okamžiku útočník může zadávat své příkazy například „přenes soubor po síti, spusť program, smaž disk“. Zadní vrátka může úmyslně zanechat v programu programátor nebo se může jednat o pomůcku pro ladění programu, která byla omylem ponechána i v ostré verzi. [9] Backdoory jsou velmi nebezpečné programy, umožňující manipulaci se soukromými daty cizí osobou.

- **Trojské koně zasílající získaná hesla** – spustí-li se na systému nic netušícího uživatele, hledá všechna možná hesla a následně se je snaží odeslat na předem určený cíl (příkladem může být útočníkův e-mail). Tyto koně většinou plní funkci pouze jednou, pouze když je spuštěn odpovídající soubor.
- **Trojské koně v podobě klasických keyloggerů** – aplikace, které jsou schopny zaznamenávat klávesy, které uživatel stisknul. Nejčastěji se spouštějí po každém startu systému a všechny stisknuté klávesy ukládají do určeného souboru nebo posílají útočníkovi.
- **Trojské koně, které mají destruktivní charakter** – snaží se na disku oběti smazat vše nalezené nebo zaútočí na vybrané soubory. Nejzajímavějším příkladem této kategorie je trojský kůň sloužící k provedení DDoS (Distributed Denial of Service – česky „distribuované odmítnutí služby“). [19]

  Cílem takové toho útoku je:

  - vnucení opakovatelného restartu počítače
  - znemožnit nebo alespoň velmi zpomalit komunikace mezi serverem a obětí



Obrázek 1 - DDos útok [19]

Schéma, kde desítky, ale třeba i tisíce napadených stanic zaútočí na cílový server (například na povel útočníka), který se pod návalem požadavků zhroutí a přestane poskytovat své služby.

3.5. Spyware

Obecně se uvádí, že devět z deseti počítačů je nakaženo spywarem. Spyware neboli „špión“ je program, který se uloží v počítači, sleduje a krade hesla, uživatelská jména, IP adresu uživatele, historii navštívených stránek, čísla kreditních karet, mění úvodní stránky na Internetu apod. Poté využije Internet k odesílání získaných dat bez vědomí jeho uživatele jinému uživateli, který tyto údaje dál zpracovává.

Někteří autoři spywaru se hájí tím, že jejich program odesílá pouze seznamy webových stránek nebo nainstalovaných programů, neboť tím zjistí zájmy a potřeby uživatele. Tyto informace tudíž mohou být využity pro cílenou reklamu. Ale nelze zaručit nezneužitelnost těchto informací a proto s existencí a legálností spywaru řada uživatelů nesouhlasí.

Spyware se často šíří společně se sharewarovými programy nebo také surfováním po Internetu (hlavně návštěvou rizikových webových stránek například pornografických).

Spyware patří mezi malware, který běží na počítači bez vědomí uživatele a nějakým způsobem ho poškozují, nebo zhoršují jeho funkci

Na otázku „A proč vlastně spyware existuje?“ lze odpovědět, že za vším stojí peníze. Ať už jsou to firmy, které si nechávají za nemalé částky spyware vyrábět pro zobrazování vlastní reklamy pomocí pop-up oken, hackeři, kteří se snaží získat soukromé informace uživatelů pro nelegální činnost (peněžní převody) a nebo programátoři, kteří na zakázku vytváří programy, kam spyware umisťují.

3.5.1 Příznaky spyware v počítači

- pomalý start počítače a dlouhé nabíhání Internetu
- nežádoucí domovská stránka (přesměrování na jinou webovou stránku)
- vyskakování reklamy tzv. pop-up okna
- přesměrování telefonní linky u vytáčeného připojení
- padající Windows (např.častý restart, chyby)
- záhadně se objevující nové ikony na pracovní ploše [9]

3.5.2 Druhy spyware

3.5.2.1 Adware neboli reklama

Obtěžuje při práci na počítači. Typickými příznaky jsou pop-up okna a vnucování výchozích stránek Internetu bez zájmu uživatele. Uživatel v řadě případů souhlasí s instalací adware, protože při instalaci různých volně dostupných programů (freeware) si nepřečte a označí souhlas s licenčním ujednáním tzv. EULA (End User License Agreement). Bez souhlasu s EULA není možno v instalaci programů pokračovat. Dále může být adware součástí produktů jako je např. DivX. [2]

3.5.2.2 Dialer

Program či skript ActiveX, který dokáže změnit způsob přístupu na Internet prostřednictvím modemu. Přesměruje vytáčení čísla pro internetové připojení na linky s vysokými tarify. Většinou toto uživatel pozná až podle výpisu za telefon, který bývá mnohonásobně vyšší. S nárůstem trvalého připojení k Internetu jako je Wi-Fi nebo ADSL se v dnešní době toto riziko postupně vytrácí.

3.5.2.3 Další trojské koně

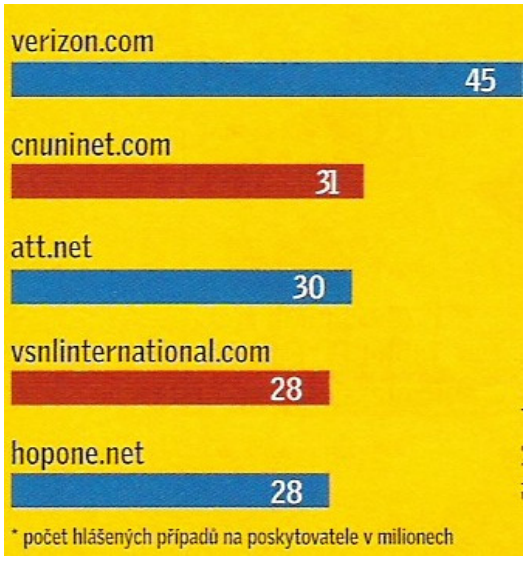
- **Hijacker** – mění domovskou stránku.
- **Browser helper object** - jedná se o DLL knihovnu, která umožňuje programátorům změnit a sledovat Internet Explorer.
- **Keystroke Logger** - sleduje každý pohyb na uživatelově klávesnici. Některé typy tohoto spyware odesílají hesla na e-mail autora spywaru.
- **Remote Administration** – umožňuje vzdálenému uživateli ovládat cizí počítač.
- **Miscellaneous** - je směsí skupin spyware.

3.6. Spam

Tento výraz původně představoval název amerických konzerv lančmítu, které byly po druhé světové válce velmi rozšířené, ale velmi málo chutné. Proto tedy „spam“ jako označení něčeho nechtěného. Opakem spamu je pošta, která by se dala nazvat chtěná či vyžádaná a pro tu se občas používá (ale spíše jen z recese) výraz „ham“, čili anglicky šunka. [9]

Spam je nevyžádaná zpráva, která obsahuje reklamu a je rozesílána profesionálními spammery. Na Internetu dnes existuje několik prostředků, které lze použít pro rozesílání spamu. Nejčastěji využívaným prostředkem je elektronická pošta. Dalšími možnostmi jsou Instant Messenging (typu ICQ, MSN,…) diskuzní fóra, chat i komentáře pod článkem. Předními bojovníky proti spamům jsou firmy (které samy nevyužívají spamy jako prostředek ke své firemní reklamě), protože jejich zaměstnanci musí denně ze svých pracovních e-mailových schránek třídit a odstraňovat desítky nevyžádané pošty. Po tuto dobu, kterou by mohli využít efektivněji, se nevěnují své práci, za kterou jsou placeni. Na webové stránce www.spamy.cz si lze pomocí spamové kalkulačky přibližně vypočítat, o kolik cenného času a peněz daná firma přichází.

Pro názornost je zde uveden příklad:
Firma, která má sto zaměstnanců s e-mailovými schránkami, jejichž čistá hodinová mzda činí 150 Kč. Denně do jedné schránky průměrně dorazí deset spamů.
Výsledky jsou následující:
Každý zaměstnanec tříděním a odstraňováním spamů stráví 2,5 minuty denně.
Za měsíc je to 0,9 hod. pro každého zaměstnance.
Průměrné měsíční náklady jsou 13 750 Kč a roční 165 000 Kč.
V případě firem, které mají více zaměstnanců jsou ztráty mnohonásobně větší.



Obrázek 2 - Hlavní šiřitelé spamu [8]

Verizon, největší americký poskytovatel, má ve své klientele mnoho spammerů, ale nic proti nim nepodniká. [8]

3.6.1 Spamové nebezpečí

Spamy představují jeden z největších problémů, které se řeší v souvislosti s Internetem.

- zaplnění emailové schránky

Pokud pravidelně nedochází k promazávání doručených zpráv, obzvláště spamových, schránka se zaplní. Uživatelova schránka již nebude schopna přijímat nové zprávy, které budou nenávratně ztraceny.

- zpomalení přenosu pošty

Nedojde-li přímo k zahlcení schránky, stoprocentně se zpomalí přenos pošty. Spamy zabírají více místa než obyčejné textové zprávy, protože obsahují obrázky nebo i zvuky.

- zneužití osobních údajů uživatele

Rozesílání nevyžádaných emailů ze svého principu představuje zneužití uživatelovy adresy – jestliže se jedná o e-mail, který si uživatel sám nevyžádá, znamená to, že někdo jiný využil danou adresu k jinému účelu, než vlastník adresy předpokládal. Platí to i v případě, kdy sám uživatel zveřejnil svou adresu na některých webových stránkách nebo v různých webových adresářích.

Další formou zneužití je samotné shromažďovaných adres, které jsou považované za osobní údaje. Tím vznikají databáze e-mailových adres, na které pak mohou spammeři posílat své spamy.

- obtěžování uživatele

V případě přijatého spamu chvilku trvá než uživatel zjistí, že jde o zbytečnost a spam smaže. Většině uživatelům vadí, že je někdo obtěžuje a ubírá jim odstraňováním nevyžádaných zpráv drahocenný čas. A co teprve v případě, že by uživatel takovýchto e-mailů dostával desítky denně.

- zcizování dalších zdrojů

Spam spotřebovává kromě času, znalostí a schopností také přenosovou a výpočetní kapacitu nebo paměť.

Spamming je zneužitím elektronické pošty a síťových news na Internetu. Může vážným způsobem narušit provoz veřejných služeb, nemluvě již o efektu, jaký může spamming mít na systém elektronické pošty kteréhokoli jednotlivce. …. Provozovatelé spammingu ve skutečnosti odnímají významné zdroje uživatelům a provozovatelům služeb, aniž by k tomu měli jejich souhlas a bez jakékoli kompenzace. [11]

3.6.2 Spam – nyní i v podobě MP3 souboru

Spamové e-maily nyní neobsahují pouze texty. Pro překonání spamových filtrů používají spammeři stále zákeřnější metody.

- Spam jako obraz

  Spamové fitry hledají v kontrolované zprávě určité kombinace slov, aby poznaly, zda se jedná o reklamu. Nyní autoři spamu reklamní text nakreslí jako obrázek. Tím se vyhýbají spamovým filtrům, protože ty pouze zjistí, že se jedná o JPEG soubor, nikoli jeho obsah.

- Spam jako MP3

  U této metody spammeři používají spam v audiosouboru. Rozesílají e-mail, většinou bez textu a vyplnění předmětu, s přiloženým souborem ve formátu MP3. Časté obměňování názvů přiložených souborů (např. „madona.mp3“ nebo „elvis.mp3“)

zabraňuje identifikaci a také má za úkol přimět adresáta k poslechu přiloženého zvukového souboru. Ve většině případů se po spuštění takového souboru o velikosti 50 až 150 KB ozve abstraktní ženský hlas, který anglicky propaguje akcie. Cílem takto vytvořeného spamu je snaha spammerů vyhnat kurs akcií výše, aby je mohli prodat se ziskem. [8]

3.7. Hoax

Hoax, který je odnoží (nebo též odrůdou) spamu, se volně překládá jako žert, mystifikace, šprým či kachna. V počítačovém světě se hoaxem nejčastěji označuje falešná, poplašná nebo důvěryhodně podaná zpráva, která uživatele varuje před nebezpečným virem, poskytuje informace o různých nebezpečích, žádá o pomoc, ale i se snaží ho pobavit.

Vyskytuje se hlavně v podobě e-mailové zprávy, ale existují i Jabber a ICQ zprávy, které vyzývají k opětovnému rozesílání.

Cílem tvůrců hoaxů je především zmást uživatele a přinutit je k co největšímu rozšíření poplašné zprávy dalším uživatelům.

Hoax převážně zneužívá neinformovanosti a naivity uživatele.

3.7.1 Nejčastější případy, kdy se jedná o hoax

- Popis nebezpečí

V tomto případě bývá smyšlené nebezpečí stručně charakterizované. Jedná-li se o vir, je uváděn i způsob jeho šíření.

- Varování před ničivými účinky viru

Ničivé účinky mohou být například formátování disku nebo méně důvěryhodné např. roztočení harddisku opačným směrem, vyhození počítače do povětří dokonce i útěk myši do ledničky. Záleží zde pouze na fantazii autora.

- Varování z důvěryhodných zdrojů

Zde se autor hoaxu snaží přesvědčit, že varování pochází z důvěryhodných zdrojů například Microsoft varuje, Intel upozorňuje,…

- Vyzvání k dalšímu rozesílání

Tuto výzvu poplašná zpráva obsahuje vždy. Nezkušení uživatelé se nechají zprávou nachytat a bez přemýšlení hoax rozesílají dál. Důsledkem uposlechnutí této výzvy k dalšímu rozesílání je masové šíření.

- Zpráva obsahuje mnoho interpunkčních znamének

Vidí-li uživatel za každou druhou větou tři vykřičníky, vypovídá to o neserióznosti zprávy. I takto lze hoax rozpoznat.

V praxi lze uplatňovat následující pravidlo:
Pokud zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, tak je to s největší pravděpodobností hoax. [22]

3.7.2 Hoaxy a jejich škodlivost:

Hoax nepředstavuje pro uživatele nebezpečí v podobě zformátování disku, ztráty či modifikace soukromých dat, jako je tomu například u virů, červů, trojských koňů atd. Přestože se mnohým uživatelům šíření hoaxů jeví jako neškodné, odborníci a správci sítí jsou opačného názoru. Tvrdí, že hoaxy představují nebezpečný jev, před kterým je nutné se chránit.

3.7.3 Názory odborníku na hoax

Odborníci argumentují tím, že hoax:

- obtěžuje příjemce – opakovaný příjem nesmyslných zpráv je pro většinu uživatelů obtěžující obzvláště v případech, kdy se v jejich e-mailových stránkách stejná zpráva objevuje i několikrát denně
- obsahuje nebezpečné rady - pokud se uživatel těmito radami řídí, může svému počítači spíše ublížit (např. co udělat pro zrychlení počítače, odstranění domnělého viru)
- nesmyslně zatěžuje linky a servery

- ohrožuje ztrátu uživatelovy důvěryhodnosti – odesílatel lživých zpráv nebo informací ohrožuje důvěryhodnost svou ale i firemní, pokud tyto zprávy odesílá z pracovního emailu
- umožňuje prozradit důvěryhodné informace – pokud se hoax přeposílá na další adresy, přeposílají se s ním i adresy všech příjemců. Tudíž odesílatel zprávy nemůže ani vědět, komu byl e-mail i s jeho adresou dále doručen. Tím vznikají obrovské seznamy e-mailových adres, které se šíří mezi neurčeným počtem cizích lidí. Do tohoto počtu spadají i spammeři, pro které je tento seznam emailových adres vítaným zdrojem.

3.7.4 Typické formy hoaxů:

- falešný poplach – zpráva manipulující s uživatelem za účelem přimět ho k dalšímu šíření nebo k destruktivnímu zásahu.Patří sem různá varování před smyšlenými viry a různými útoky na počítač, smyšlenky o mobilních telefonech, popis jiného nereálného nebezpečí (vymyšlené nebezpečí z běžného života, mimo oblast výpočetní techniky)
- prosby o pomoc – špatný pokus o vtip, který působí na lidské city. Typickým příkladem jsou prosby o různou pomoc pro nemocné lidi (např. darování krve). Tyto prosby můžou být i skutečné, ale obvykle se masově rozšíří až když nejsou aktuální.
- petice a výzvy – petice šířená e-mailem, ke které se vedle jména připojí i další osobní údaje se dostává k dispozici všem, kteří tento e-mail dostanou. Zde hrozí nebezpečí, že text petice (výzvy) by mohl být změněn a naše osobní údaje, popřípadě podpis, mohou být zneužity a vyskytnout se pod prohlášením, se kterým podepsaný nesouhlasí
- zábavné hoaxy – využívají uživatelovy snahy být vtipný (např.žertovné zprávy). Ne všichni mají stejný smysl pro humor a proto by neměli být masově šířeny na všechny adresy. Dále sem řadíme řetězové dopisy štěstí, které využívají lidské pověrčivosti a dokonce i „vyhrožují“

(„pokud neodešlete tuto zprávu dalším deseti lidem, přerušíte tento řetězec, a budete mít deset let smůlu“). Naopak člověku, který „výhružku“ poslechne a řetězový dopis pošle dalším lidem, je ve zprávě slibován úspěch, štěstí, peníze či láska.

3.7.5 Klasické podvodné hoaxy

3.7.5.1 Podvodné loterie

Uživatelům je rozeslán e-mail, že vyhráli vysokou částku v mezinárodní loterii, do jejíhož slosování se dostali náhodným výběrem jejich e-mailové adresy z celého světa. Trik spočívá v tom, že šťastlivec musí zaplatit před výběrem výhry manipulační poplatek, který může být několik desítek až tisíců EUR a nelze ho strhnout z údajné výhry. Pokud naivní výherce tento poplatek uhradí, výhru samozřejmě neobdrží.

3.7.5.2 Nigerijské podvodné emaily

Tyto e-maily se velkého rozmachu dočkaly právě s rozšířením Internetu. Jedná se o podvodné emaily, které se snaží nalákat důvěřivce na snadné získání velké sumy peněz. Odesílatelé se vydávají za velmi bohaté lidi, kteří prosí o pomoc při převádění peněz ze země na jiný účet, aby ušetřili například na daních. Příjemce je požádán, aby poskytl svůj účet a jako odměna mu je přislíbená slušná peněžní částka. Hlavní princip podvodu spočívá v tom, že podvodník si vyžádá zálohu na poplatky spojené s převodem peněz a po obdržení této částky se již neozve.

3.8. Phishing – podskupina spamu

Phishing je známý také jako brand spoofing nebo carding. V češtině se tato technika podvodu někdy nazývá rhybaření. Jedná se o podvodné rozesílání emailových zpráv, které na první pohled vypadají jako informace z různých legálních institucí (například bank nebo spořitelen) a jsou samozřejmě rozesílány na obrovské množství adres. [4]

Jejich cílem je získávání důvěrných a citlivých údajů jako jsou přihlašovací jména a hesla k bankovním účtům, čísla a PIN kódy platebních karet od obětí apod.

3.8.1 Phishing a jeho způsoby útoku

K phishingu jsou nejčastěji používány tři cesty:

- Využití tzv. sociálního inženýrství

V tomto případě je oběť nějakým způsobem přesvědčena, aby vydala své přihlašovací jméno a heslo. Nejčastěji k tomu dochází po kliknutí na odkaz podvodné webové stránky přímo v přijatém e-mailu.

- Využití keyloggerů

To jsou programy, které si dokážou ukládat uživatelovy stisky na klávesnici a tato data poté odesílat podvodníkovi. Samozřejmě bez vědomí oběti. Keyloggery se do počítače dostanou pomocí trojského koně, kterého si uživatel může stáhnout s nějakým nelegálním softwarem nebo z pochybné Internetové stránky.

- Využití útoku Man-in-the-Middle.

Při využití této cesty je hacker prostředníkem mezi bankou a oprávněným uživatelem, kteří o něm ale nic netuší. Když uživatel ukončí svou práci s připojením k bance, nastává chvíle pro podvodníka vydávajícího se za oprávněného klienta, který pokračuje ve spojení s bankou. Tohoto okamžiku samozřejmě využije ve svůj prospěch.

Autoři phishingové pošty se stále zdokonalují a používají čím dál tím více rafinovanějších podvodných e-mailů a informačních oken. Zpráva často obsahuje oficiálně vypadající loga a obrázky pravých institucí, převzaté ze skutečných webových stránek. Tyto napodobeniny se označují jako podvržené weby a pokud se oběť na takovýto server dostane, může podvodníkovi odeslat nevědomky osobní údaje.

Obrázek 3 - Podvodný e-mail [26]

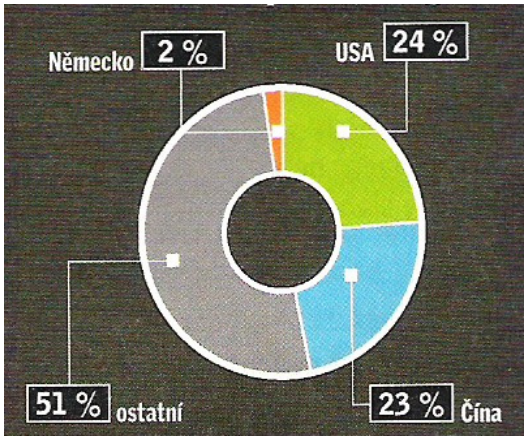
Příklad podvodné e-mailové zprávy, včetně podvodné adresy URL s odkazem na server nevyžádané pošty.

(1) Odkaz, který zdánlivě vede na opravdový web a používá se kvůli důvěryhodnosti podvodného e-mailu.
(2) Pravý odkaz falešného webu, na který je uživatel ve skutečnosti přesměrován. Oběť může být případně nasměrována i k informačnímu oknu, které vypadá totožně jako oficiální webová stránka.

3.8.2 Proč phishing funguje?

Fungování je spojeno s jednoduchostí vytvoření kampaně na Internetu. Zatímco postavit „kamennou“ napodobeninu banky není jednoduché, vybudování falešné internetové identity banky v současnosti již tak náročné pro útočníka zdaleka není. Realitou je také jednoduchost vytvoření phishingové zprávy a oslovení obrovského množství uživatelů. Navíc zde nedochází k osobnímu kontaktu s obětí, a proto je mnohem obtížnější identifikace útočníka. [25]

Dalšími fakty, kterých phishing využívá jsou bezpochyby nepozornost, neznalost, neinformovanost a důvěřivost samotných obětí, které nesledují, kam jsou z podvodných zpráv směrováni nebo neznají danou problematiku. Tyto fakta částečně napravují média i samotné poškozené instituce pomocí informativních zpráv. Takovým příkladem jsou banky, které samy své uživatele informují o možných nebezpečích a snaží se jim poradit, jak se bránit.



Obrázek 4 - Původci phishingu [8]

4. Ochrana před nebezpečím na Internetu

Internet je obrovským zdrojem svobodných informací, ale tato svoboda zároveň dává mnoha podvodným živlům velký prostor pro vyvíjení různých škodlivých aktivit. [22]

Žijeme ve světě rychlého Internetu, kdy je počítač součástí naší práce a zábavy. Proto je naše soukromí, bezpečnost i pohodlí důležitější než kdykoliv předtím. Na Internetu se šíří velké spektrum počítačových virů, červů, trojských koní a jiných nebezpečných programů, které jsou svými autory neustále zdokonalovány. Na bezpečnost práce na počítači se dnes kladou stále větší a větší požadavky, protože vznikají novější a propracovanější techniky počítačových škůdců. Odborníci proto musí každý den pracovat na stále lepších antivirových produktech a opravných balíčcích pro děravé programy. Dále vyvíjí nové a bezpečnější produkty, vytvářejí nové techniky detekce a léčení napadených programů, z kterých se stejně postupem času stanou neefektivní a nedostačující „ochránci“. Co se ochrany týče, měl by uživatel začít od prevence.

4.1. Prevence

V současnosti je prevence bohužel velice podceňována a mnoho uživatelů počítače se jí nevěnuje vůbec, popřípadě jen částečně. Uživatel by si měl uvědomovat, že používání antivirového programu, softwaru pro odstraňování škodlivého malwaru, popřípadě osobního firewallu je samo o sobě nedostatečnou prevencí. Jedná se totiž pouze o programy, kterým dává „smysl života“ teprve uživatel. Ten často spoléhá právě na tyto programy a nechává na nich osud svého počítače. Právě tento přístup většinou vede k napadení počítače nebezpečnými škůdci. Je tedy důležité, aby uživatel nebyl pouze pasivním, ale poučeným uživatelem.

4.2. Zásady související s prevencí

Ohledně prevence je užitečné znát několik obecných zásad:

- Antivirovému systému, který by měl být nainstalován v každém počítači, by uživatel měl zajišťovat jeho pravidelnou, nejlépe automatickou aktualizaci. Čím častěji se provede aktualizace, tím lépe. V současné době je možné konstatovat, že aktualizování dvakrát do hodiny neznamená zbytečnost. Uživatel by se ale určitě neměl držet hesla „mám antivirus, nic se mi nemůže stát“. Měl by ho spíše považovat za doplněk zabezpečení svého počítače. Antivirové programy v sobě mají dnes také integrovány antispywary. Ovšem není to pravidlem.

- Dále je dobré zajistit alespoň chod modulu, který se stará o nepřetržitou kontrolu souborů, se kterými uživatel či aplikace pracuje (otevírání, spouštění, ukládání apod.). Tyto moduly, obstarávající nepřetržité skenování souborů, se odborně nazývají „on-access skener“ nebo také rezidentní štít a jsou součástí každého moderního antiviru. Samozřejmě je často nabízen i modul, který dokáže kontrolovat přijaté, odeslané i stažené zprávy. Ale i kdyby tento modul neběžel, nic nebezpečného by se nestalo, protože on-access skener by případný virus zachytil v momentě, kdy by se uživatel pokusil otevřít infikovanou přílohu e-mailu.

- Je potřeba myslet na to, že přítomnost infikovaného souboru, infikované přílohy v e-mailu nemusí jednoznačně znamenat, že je počítač infikován. Malware se totiž může vyskytovat na pevném disku v neaktivním stavu. Příkladem může být malware, který uživatel najde v adresáři, kam si prohlížeč Internet Explorer odkládá soubory, nutné pro zobrazení webových stránek, které si uživatel vyžádal. Tento adresář se nazývá

Internet Temporary Files. A právě zde mohou speciální programy, zvané „exploit“ , nacházející se na některých webových serverech, neaktivní škůdce najít a spustit je. To vše bez uživatelova vědomí. Proto je důležité aktualizovat i webové prohlížeče, čímž dochází k opravení dosavadních chyb a tím k znemožnění provedení takového útoku.

- Uživatel by měl být schopen zajišťovat pravidelnou aktualizaci. Přinejmenším těch produktů, které jsou ve společném kontaktu se sítí nebo Internetem. Tyto programy totiž mohou být zastaralé a mohou obsahovat bezpečnostní díry – chyby. V případě, že se chyby vyskytují zrovna v části zajišťující přístup do Internetu, může se najít hacker, který díky této chybě dokáže získat i kontrolu nad uživatelovým počítačem. V praxi to znamená povolit pravidelnou aktualizaci operačního systému Windows, ale také běžně používaných produktů (typu ICQ), které by mohly být zneužity z Internetu. Také by měl uživatel navštěvovat stránky Windows Update a Office Update, kde je možné pomocí průvodce zjistit aktuální stav počítače uživatele a nabídnout mu ke stažení opravy bezpečnostních chyb.

- Výbavou počítače, jehož uživatel přistupuje na Internet, by měl být firewall. Nejčastěji v podobě osobního neboli tzv. personálního firewallu. Jedná se o programový nástroj, který odděluje nedůvěryhodné sítě od důvěryhodných a zabraňuje nevyžádaným útokům. Jinak řečeno je to software, který stojí mezi uživatelovým počítačem a Internetem a chrání ho před útoky zvenčí. Podobně jako je tomu u antivirů, tak i u firewallu musí uživatel umět tento prostředek správně ovládat. Jinak jeho přítomnost v počítači ztrácí smysl.

- Místa, na kterých na uživatele číhá největší množství nebezpečí, jsou zejména erotické stránky, pornografické servery a ne zcela legální stránky typu „warez“, které jsou zaměřeny na nelegální podezřelé nebo jiné pirátské činnosti a umožňují uživateli stáhnout si na nich komerční program zcela zdarma. Další nebezpečné programy mohou být ukryty v legálních programech typu shareware a freeware. Ani tak samozřejmá věc jako je elektronická pošta by se neměla podceňovat. I tímto způsobem se šíří velké množství škodlivého softwaru.

- V neposlední řadě je nutné, aby uživatel používal zdravý rozum. To je ta nejúčinnější rada pro prevenci, která je velice jednoduchá. Je třeba při práci na počítači přemýšlet a „neklikat“ myší na vše, co uživatele zaujme. Nejčastěji je právě neopatrné „klikání“ myší zdrojem většiny problémů.

4.3. Ochrana a prohlížeč Internet Explorer

Do nedávna byla změna internetového prohlížeče velice cennou radou proti boji se škodlivým malwarem, který se šíří Internetem. Internet Explorer byl a stále je nejpoužívanějším prohlížečem. Je tomu tak mimo jiné i díky tomu, že je poskytován uživatelům s operačním systémem Microsoft Windows.

Ovšem většina odborníků zabývající se ochranou před nebezpečím na Internetu dává přednost prohlížečům jako jsou Mozilla FireFox nebo Opera. Internet Explorer do verze 6 byl často kritizován kvůli svým chybám v bezpečnostní architektuře, které často podporovaly šíření veškerého malwaru, který umožňoval jeho autorům kontrolu nad systémem či nad citlivými údaji oběti. Také zůstával v pozadí oproti Mozille a Opeře kvůli své rychlosti, chybnému vykreslování určitých prvků stránek a přílišné jednoduchosti. Ovšem o Operu, jako alternativní řešení, mnoho uživatelů nejevilo příliš velký zájem pro velké množství jejích funkcí, které komplikují ovládání. Řešením pro mnohé z nich byl internetový prohlížeč Mozilla FireFox.

V době, kdy jsou dostupné plné verze internetových prohlížečů, jako je Internet Explorer verze 7, Mozilla Firefox 2 a Opera 9, záleží jen na uživatelově uvážení, který prohlížeč si nainstaluje. Protože Internet Explorer je stále nejpoužívanější po celém světě, měl by jeho uživatel být seznámen s některými novými funkcemi, které tento prohlížeč oproti dosavadním verzím v nové verzi přináší.

4.3.1 Internet Explorer 7

Prohlížeč vydaný spolu s operačním systémem Windows Vista nabízí několik nových funkcí týkajících se především bezpečnosti a usnadnění práce na Internetu. Proto by již neměl být snadným cílem útoku hackerů či škodlivého software. Je velkým přínosem, ovšem ne pro držitele nelegálního Windows, je potřeba vlastnit originální operační systém. Při instalaci této verze je uživatel nejprve povinen souhlasit s autorskými podmínkami a poté s ověřením své kopie Windows. Bez těchto dvou nejdůležitějších kroků je instalace nemožná.

Nejvýznamnějšími funkcemi pro usnadnění práce jsou:

- Panely, které zpříjemňují surfování a poskytují uživateli přehled o otevřených webových stránkách.
- Quick Tabs - náhledy otevřených panelů, které slouží pro snazší orientaci uživatele v otevřených webových stránkách. Jedná se o funkci, kdy se všechny otevřené stránky zobrazí v podobě miniatur vedle sebe.
- Vyhledávání – nyní lze vyhledávat nejen pomocí pole pro vyhledávání, ale také zadáním hledané fráze přímo do adresního řádku.
- Informační kanály RSS – tato technologie umožňuje uživatelům Internetu přihlásit se k odběru novinek z webových stránek, které nabízí RSS kanál.
- Vylepšený tisk. Aplikace Internet Explorer 7 automaticky přizpůsobí webovou stránku pro tisk, takže se celá webová stránka vejde na požadovaný formát papíru. Možnosti tisku zahrnují také upravitelné okraje, upravitelné rozložení stránky, odstranitelná záhlaví a zápatí a možnosti tisku pouze vybraného textu. [26]

Mezi nové ochranné prvky proti škodlivému software patří:

- Filtr útoků phishing. Tento filtr chrání před možnými a známými falešnými webovými stránkami a v případě potřeby dokáže daný web zablokovat.
- Ochrana adresního řádku.
- Zabezpečení zpracování adres URL. Nový nástroj pro zpracování adres URL pomáhá centralizovat analýzy důležitých dat a zvyšuje konzistentnost dat v celé aplikaci.
- Mezinárodní ochrana názvů domén před vkládáním falešného obsahu. Aplikace může uživatele upozornit v případě, že vizuálně podobné znaky v adrese URL nejsou vyjádřeny ve stejném jazyce. To zajišťuje ochranu před webovými stránkami, které se mohou jevit jako známé a důvěryhodné.
- Odstranění historie procházení webových stránek. Umožňuje z jediného okna odstranit dočasné soubory, data formulářů, cookies, hesla a historii. A to buď všechny údaje najednou nebo každý typ zvlášť.
- Panel stavu zabezpečení. Zobrazí se barevně kódované upozornění vedle adresního řádku. Podle barev upozorňuje na zabezpečení webu a nastavení zabezpečení .
- Funkce ActiveX Opt-in. Zakazuje téměř všechny ovládací prvky ActiveX, aby došlo k zabránění rizika útoků na potenciálně ohrožené ovládací prvky. [26]

O Internetu Exploreru 7 lze konstatovat, že je poměrně kvalitní program, ale v podstatě přináší pro uživatele pouze to, co po celou dobu nabízí Firefox nebo Opera.

I přes řadu svých bezpečnostních vylepšení, kterých verze 7 dosáhla je tento prohlížeč stále kritizován svojí zranitelností. Pokud se uživatel pokusí pomocí toho internetového prohlížeče přeci jen navštěvovat nebezpečnější internetové stránky, měl by nejprve provést několik základních opatření. V Internet Exploreru kliknout

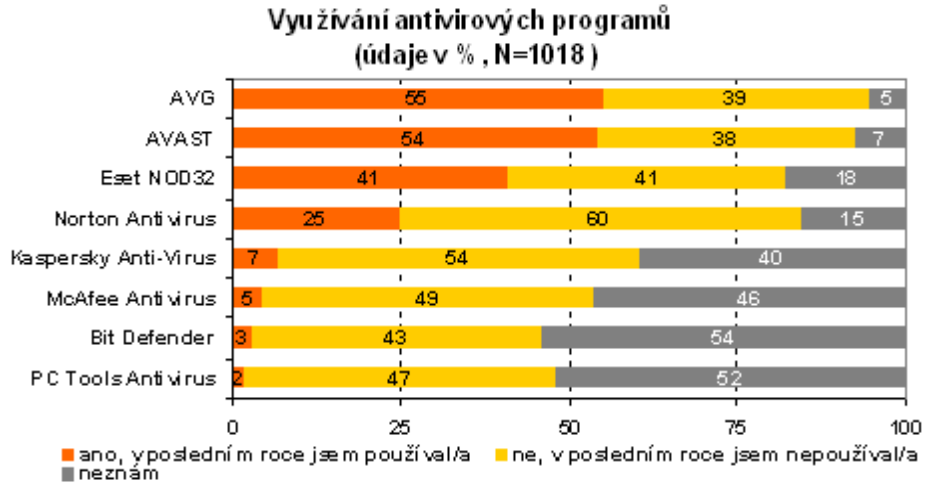
na nabídku *Nástroje* / *Nastavení Internetu* a v otevřeném okně na kartu *Zabezpečení*. Poté zvolit *Internet*, kde je možné v dolní části okna kliknout na tlačítko *Vlastní úroveň*. Nyní je třeba deaktivovat vše v sekci ActiveX, zakázat aktivní skriptování a skriptování appletů v jazyce Java. V sekci *IFRAME* zakázat spouštění programů a souborů. Poslední neméně důležitou sekcí jsou doplňky. Kliknout na nabídku *Nástroje* / *Spravovat doplňky* a vybrat příkaz *Povolit nebo zakázat doplňky*. Zde uživatel nalezne seznam všech nainstalovaných a aktuálně zavedených doplňků pro Internet Explorer. Pokud začne prohlížeč vykazovat nestandardní chování, je třeba první kontrolu směřovat právě sem.

4.4. Ochrana před viry

Žádný antivirový program nezaručí stoprocentní zabezpečení počítače. Jestliže se chce uživatel dostatečně bránit a snížit možnost před napadením, měl by dodržovat některé důležité zásady:

- Pravidelně používat a aktualizovat antivirový program.
- Používat bránu firewall pro připojení k Internetu.
- Pravidelně zálohovat důležitá data, dříve než uživatel zjistí napadení virem nebo jiné potíže.
- Nespouštět programy z cizích médií. Je dobré dané médium před použitím nejdříve otestovat antivirem.
- Nikdy neotvírat přílohu e-mailu s dvojitou příponou (např. dopis.txt.vbs) a od odesílatele, kterého uživatel nezná.
- Neotvírat ani e-mailové přílohy od známých osob, pokud přesně uživatel neví, co příloha obsahuje, protože odesílatel e-mailu třeba ani netušil, že příloha, kterou poslal, obsahuje virus.
- Mazat e-maily, ve kterých je text zprávy napsán v cizím jazyce.
- Každý nový program či dokument otestovat antivirovým programem.

- V případě zjištění napadeného souboru je lepší a bezpečnější obnovit ho ze zálohy.
- Pravidelně aktualizovat software, protože novější verze mají již opravené bezpečnostní chyby.



Obrázek 5 - Využívání antivirových programů [28]

Antivirové programy jsou v současnosti dosti vyrovnané a uživatel si je volí na základě rychlosti detekce, dostupnosti a ceny.

V souvislosti s ochranou počítače před viry se nyní častěji mluví právě o rootkitech a antirootkitových technologiích. V napadeném počítači je složité rootkity detekovat. Rootkit je pro každého hackera, kyberzločince či průmyslového špióna velmi žádaný, protože jimi vytvořené programy se mohou v uživatelově počítači beze stopy skrýt a přesto zůstat plně funkční. Zásadní ochrana před rootkity spočívá v prevenci a přítomnosti kvalitního antirootkitového programu. Za prevenci se považuje standardní komplexní bezpečnostní systém. Ten ovšem na odhalovaní rootkitů nestačí. Pokud selže prevence, je třeba použít specializovaný program. Takovým programem je například AVG Anti-Rootkit Free, který je možné zdarma stáhnout na internetové stránce www.grisoft.cz a je velice jednoduchý na ovládání. Boj s rootkity je jednou z oblastí,

kde platí pravidlo – více znamená lépe. Čím více se použije nástrojů, tím je větší pravděpodobnost, že se rootkit nalezne. Mezi další pomocníky proti rootkitům patří Panda Anti-Rootkit, McAfee Anti-Rootkit, Sophos Anti-rootkit, Gmer nebo BitDefender Rootkit Uncover.

Důvod, proč ještě není svět zcela zahlcený rootkity, je následující. Není vůbec jednoduché naprogramovat takovou aplikaci, která je schopná zásadním způsobem měnit činnost jádra operačního systému. Nestačí k tomu jen určité základy, ale naopak naprogramovat rootkit vyžaduje hluboké znalosti programování, systémů, analytického myšlení apod. Jinak řečeno: rootkit nedokáže naprogramovat každý, ale je to technologie vyhrazená pouze opravdovým špičkám v oboru. [7]

4.5. Ochrana před počítačovými červy

Infikace červem je stejně nebezpečná jako infikace virem. V důsledku jeho replikace je zvýšená pravděpodobnost zpomalení nebo dokonce zkolabování sítě.

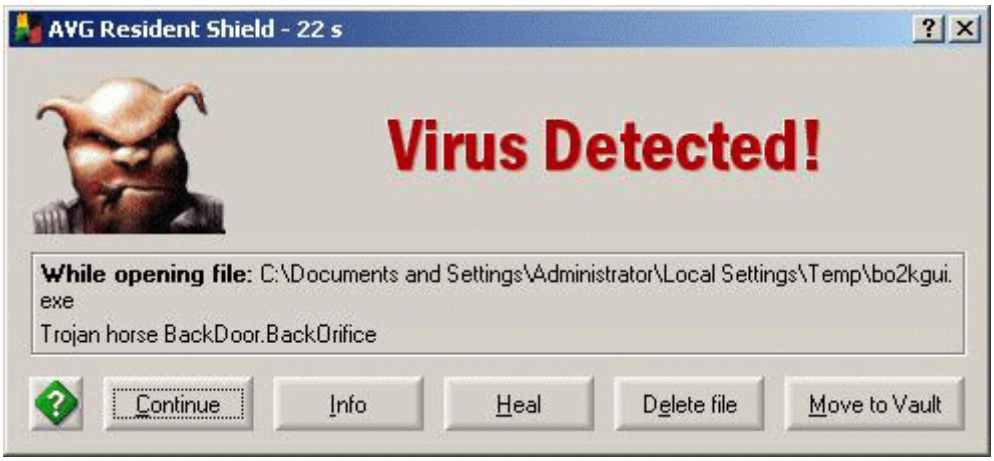
Jako preventivní opatření se doporučuje dodržovat zásady, které jsou stejné jako u virů. Nejlepší ochranou je mít bezpečný operační systém, nemít žádné programy s chybami a pracovat dostatečně opatrně s e-mailem, aby nedošlo ke spuštění červa. Této ochrany je prakticky nemožné dosáhnout. Proto je důležité instalovat antiviry nebo jiný bezpečnostní software, který bude uživatel neustále aktualizovat.

Nejobvyklejším útokem červů jsou nejčastěji používané programy. Většina červů funguje jen na Microsoft Windows a proto je možné považovat za určitou ochranu i používání alternativního operačního systému, například Linuxu. Avšak ani používání jiného operačního systému neznamená stoprocentní bezpečnost pro uživatele. Vyskytnou-li se v infikovaném systému dva „znepřátelení“ červi, tak jeden zaútočí na druhého a odstraní ho, aby měl celý systém sám pro sebe. Pokud dojde k napadení počítače červem, je možné odhalit ho a odstranit jednoúčelovým programem, který výrobci antivirových programů poskytují na svých stránkách zdarma ke stažení.

4.6. Ochrana před trojskými koni

Obecně platí stejná pravidla jako u virů a červů. Velký důraz je kladen hlavně na pozornost při otvírání cizích programů. Preventivním způsobem obrany je nespouštět každý zajímavý soubor, který mohl přijít e-mailem, nebo který uživatel nalezl na nějakém serveru. Nejčastěji nás může postihnout nebezpečí ve formě modifikace či ztráty dat, zpomalení systému včetně počítačové sítě.

Na stránce www.glocksoft.com nebo www.anti-trojan.com je možné prohlédnout si seznam známých trojských koní a dozvědět se základní informace o nejčastěji používaných trojanech. Bude-li uživatel dodržovat základní pravidla při práci s neznámými e-mailovými přílohami, bude mít správně nakonfigurovaný firewall a vždy funkční antivirový systém je možné se před útokem trojského koně do velké míry ubránit. Pokud se nějaký trojský kůň dostane do počítače, lze ho detekovat a někdy odstranit antivirovým programem nebo využít specializovaných aplikací. Příkladem specializovaného softwaru je antivirový program Anti Trojan Elite, Anti Trojan Shield, Trojan Remover, TrojanHunter atd.



Obrázek 6 - Ukázka detekce trojského koně [19]

Na webovém serveru http://test.bezpecnosti.cz je dokonce možné si nechat bezplatně zkontrolovat bezpečnost počítače nebo firewallu pomocí rozšířeného testu na trojské koně.

Velkým nebezpečím z kategorie trojských koňů jsou pro uživatele programy se vzdáleným přístupem (RAT).
Jak se před nimi chránit :

- E-mailovou adresu sdělovat jen osobám, které uživatel zná. Neuvádět ji v rozsáhlých internetových adresářích a na webech s nabídkami práce.
- Neotvírat přílohy neznámých e-mailů nebo rychlých zpráv.
- Používat software od firem s dobrou pověstí.
- Používat bránu firewall.
- Zajišťovat aktuálnost programového vybavení počítače.

4.7. Ochrana před spywary

Nejlepší radou pro uživatele je neinstalovat spyware. Pokud se stane, že si uživatel nechtěně spyware nainstaluje, k jeho zneškodnění by měl použít anti-spywarový program, který může být samostatný nebo součástí antiviru. S tím souvisí pravidelné aktualizování programů, které přicházejí do styku s Internetem a instalace bezpečnostních „záplat“.

Velkým problémem u spywaru je to, že ho nelze snadno odinstalovat, protože to není samostatná aplikace. Často je složena z několika spolupracujících částí, které se navíc různě maskují. V případě spywaru, který je napsán jako tzv. BHO (Browser Hepler Object, pomocník prohlížeče) vydává se za neškodnou součást prohlížeče a tudíž není možné na firewallu zakázat odesílání informací. [2] Toto je důvodem pro používání speciálního softwaru. Nejčastěji používanými jsou Spyware Terminator, Spybot Search & Destroy, Ad Aware SE Personal Edition, AVG Anti-Spyware Free.

Proti spywarům je možné chránit se také:

- Omezením práv uživatele. Velmi účinné je pracovat pod právy skupiny USERS a nikoliv s plnými právy administrátora, protože operační systém brání uživateli provést větší zásahy do operačního systému a instalovat další aplikace, kterou může být i případný malware.
- Na internetových stránkách by uživatel neměl klikat myší na každý odkaz nebo ikonu, kterou vidí.
- Nevěřit všem aplikacím, protože se na Internetu vyskytuje mnoho podvodných produktů, které vypadají jako anti-spyware. Tyto produkty právě naopak v počítači vyhledají nějakou neexistující infekci a poté se snaží od uživatele vylákat peníze na nakoupení plné verze, která už bude schopna fiktivní infekci odstranit. Na internetové stránce www.spywarewarrior.com si může uživatel prohlédnout falešné antispywarové programy.

4.8. Ochrana přes spamy

Jak již bylo uvedeno, spam je nevyžádaná obtěžující zpráva, která se v obrovském měřítku šíří Internetem. Naprostá většina je rozesílána z počítačů, které jsou infikovány viry a červy.

Uživatelova e-mailová adresa se ke spammerům dostává pomocí tzv. robotů, které jsou umístěny na webových stránkách. Tyto roboti sbírají e-mailové adresy, zadávané uživatelem bez jeho vědomí a shromažďují vše, co se podobá e-mailové adrese. Tedy posloupnost číslic, písmen či diakritiky, která obsahuje hlavně zavináč. Toto je důvodem, proč by uživatel neměl psát svoji e-mailovou adresu přímo na webové stránky, ale raději ji napsat nějakým jiným srozumitelným způsobem - například „jmeno (zavinac) domena.cz“.

Spamovací robot ovšem může také získávat e-mailové adresy sledováním odpovědí vzdálených SMTP (Simple Mail Transfer Protocol) serverů. Tato metoda je prováděna prostřednictvím tzv. slovníkového útoku, kdy se pokouší doručit e-mail

na adresy, které jsou složeny z obvyklých jmen a příjmení, oblíbených názvů či přezdívek. Radou pro ochranu je doplnění adresy o další znaky (například adresu „petrnovak@seznam.cz“ rozšířit na xpetrnovak@seznam.cz). Dále by měl být SMTP server nakonfigurován tak, aby nepřebíral k doručení e-maily, které přicházejí z vnějšku domény a nemají adresáta uvnitř domény, kterou server pokládá za „vlastní“. Příklad: SMTP server pro doménu firma.cz propustí pouze e-maily, které v doméně firma.cz začínají nebo končí. [18]

V poslední době také narůstá množství „ukradených“ e-mailových adres pomocí virové nákazy. Proti tomuto způsobu odcizování adres je možné se chránit tím, že bude uživatel znát základní pravidla pro chování na Internetu a dále bude mít dostatečně zabezpečený a programově aktualizovaný počítač proti virům.

Dalším způsobem obrany proti spamu v e-mailových schránkách je dobré zvážit, zda je opravdu nutné svou e-mailovou adresu ostatním uživatelům svěřit, protože si daný uživatel nikdy nemůže být jistý, jestli právě jeho e-mail nezneužije třetí strana. Je třeba být opatrný při registracích na různých webových stránkách, ať už to jsou e-shopy, seznamky, chaty nebo diskusní fóra. Pro tyto i další činnosti je doporučeno založit si novou e-mailovou adresu.

Pokud se přeci jen nějaký nevyžádaný e-mail ve schránce objeví, rozhodně by uživatel neměl „klikat“ na odkaz, který může být uvedený v příloze nebo jakkoli na tento e-mail reagovat. V rámci uživatelovi ochrany před spamy je dobré tyto e-maily ihned odstranit. Neboť pouhé kliknutí na příslušný odkaz je jen potvrzení o funkčnosti elektronické adresy spammerovi, kterému se vyplatí na tuto adresu posílat další a další spam.

Antispamové programy mohou být k dispozici jako samostatná řešení nebo mohou být vlastností některých poštovních programů. Pokud se jedná o antispamy, často používanými jsou Spamihilator, SpamPal, SpamBayes, Spam Monitor a jiné. Pokud jde o poštovní programy, které mají integrovaný antispam, jsou často využívány Microsoft Outlook, Mozilla Thunderbird, The Bat.

Proti spamům v podobě obrazového souboru nestačí pouze filtry blokující tyto soubory, které nabízejí freewarové nástroje. Ty dokáží pouze určit, že se jedná o JPEG

soubor, ale už neanalyzují jeho obsah. Velké bezpečnostní firmy věří technice OCR (Optical Character Recognition – Optické rozpoznávání znaků). Tak se převede grafický soubor na text, a poté už je možné rozpoznat a odfiltrovat spamové zprávy.

4.9. Ochrana před hoaxy

V případě hoaxu nehrozí nebezpečí ve formě ztráty či modifikace dat. Proti hoaxu se lze bránit tím, že pokud si uživatel není jistý, zda je obdržená zpráva je hoax, může si prohlédnout některý ze seznamu hoaxů. Tyto databáze jsou k dispozici například na stránkách www.hoax.cz a uživatel v nich může najít většinu již existujících hoaxů.

Také je možné zadat klíčová slova do různých webových vyhledávačů, která jsou typická pro příslušnou zprávu, protože s největší pravděpodobností nám vyhledávač stejný nebo podobný text nalezne. Pokud se tak doopravdy stane, může uživatel danou zprávu bez obav odstranit.

Další možností je také odpovědět pouze odesílateli daného mailu, samozřejmě slušně, a upozornit ho, že zpráva, kterou zaslal, je hoax.

Co se týče ochrany před hoaxy, které rozesílá podvodník, který se v nich snaží z uživatelů vylákat finanční prostředky na jakoukoli pomoc, lze se bránit pouze „instinktivně“ či rozumným uvažováním. Sama oběť si musí zjistit informace, zda se jedná o podvod nebo pravdu. V neposlední řadě je odborníky doporučováno, aby uživatelé tyto podvodné zprávy vědomě dále nerozesílali.

4.10. Ochrana před phishingem

Boj s phishingem je do značné míry podobný jako ten se spamem: ochrana je nutná v pasivní i v aktivní formě. Výsledky jsou však často komplikované faktem, že uživatel zde stojí proti organizovaným skupinám, vybavených silným technickým zázemím. [16]

Jako v případě jiných bezpečnostních hrozeb, je prvním krokem velmi důležitá osvěta široké veřejnosti a seznámení se s praktikami útočníků. To je nejúčinnější obrannou, jakou je možné se postavit proti phishingovým útokům. Neboť ke snížení úspěšnosti rhybaření povede jedině opětovné nabádání uživatelů k větší pozornosti při práci s citlivými údaji a neustálé připomínání základních bezpečnostních pravidel.

Dalším krokem jak zvýšit bezpečnost je používat poslední verze internetových prohlížečů a e-mailových klientů, které jsou dnes schopny do určité míry odhalit, upozornit či zablokovat phishingový útok.

Vznikly i organizace, které se přímo zabývají bojem s phishingem, například APWG (Anti-Phishing Working Group), což je mezinárodní organizace sídlící v USA. Ta umožňuje každému uživateli Internetu mít přehled o nových phishingových útocích. V dnešní době je možné chránit se i softwarově, protože jsou na trhu k dostání nejpoužívanější internetové prohlížeče Internet Explorer verze 7, Mozilla FireFox 2, Opera 9 s integrovanou anti-phishingovou ochranou.

5. Závěr

Práce se zaměřuje na běžné uživatele osobních počítačů připojených k Internetu, kteří nejsou dostatečně seznámeni a poučeni o problematice týkající se škodlivého softwaru (malware).

Pojmy jsou vysvětleny tak, aby byly snadno pochopitelné i pro laiky. Cílem práce bylo přiblížit jednotlivé kategorie počítačových škůdců, kterých je v dnešní době velké množství, které se neustále vyvíjejí a ohrožují počítač a uživatele Internetu. Pro názornost problémů jsou uvedeny i některé vybrané příklady.

Problematika internetového nebezpečí je natolik rozsáhlá, že je obtížné všechen aktuální škodlivý software, jeho metody a důsledky průniku a ochranné produkty podrobně zaznamenat do jedné práce. Vývoj nových a nebezpečnějších škodlivých programů je v době Internetu tak rychlý, že kniha, která by všechna nebezpečí obsahovala, by po vydání už nebyla aktuální.

Práce proto může posloužit jako ucelený souhrn nejčastěji se vyskytujících nebezpečných programů v současné době. Uvádí různé způsoby infikace uživatelova počítače. Řeší, jak předcházet napadení škodlivým softwarem a následně uvádí možné ochranné nástroje, pomocí kterých je možné malware odstranit. Práce informuje o zdarma dostupných ochranných produktech a o webových stránkách, na kterých je možné nechat si zkontrolovat počítač online.

Práce se podrobněji zabývá ochranou proti malwaru, neboť podle odborníků včasná prevence znamená pro uživatele o 90% bezpečnější pohyb na Internetu.

Lze konstatovat, že jednotlivé typy malwaru spolu v některých případech úzce souvisejí, či se dokonce vzájemně ovlivňují. Neustálý vývoj a zdokonalování je dáno především rozsahem znalostí v oboru vytváření škodlivého softwaru.

I přes velké úsilí expertů vytvářet stále účinnější ochranné produkty se škodlivé produkty také neustále zdokonalují a vždy se objeví někdo, kdo bude schopen najít i tu nejmenší chybu v nejaktuálnějším programu. Proto se uživatelé nemohou spoléhat pouze na antivirové a další programy. Musí se při práci na Internetu chovat obezřetně, používat svůj zdravý rozum a neustále doplňovat svoje znalosti o této problematice.

6. Seznam použité literatury

[1] ROUBAL, Pavel. Počítače pro úplné začátečníky. Praha: Computer Press, 1997. 230 s. ISBN 80-85896-96-6

[2] STŘIHAVKA, Marek. Vaše bezpečnost a anonymita na Internetu. Praha: Computer Press, 2001. 87 s. ISBN 80-7226-586-5

[3] ČERNÝ, Jaroslav. Domácí Internet : 150 programů pro maximální využití a zabezpečení. Brno : CP Books, 2005. 200 s. ISBN 80-251-0452-4

[4] LANCE, James. Phishing bez záhad. Přel. Lubomír Moudrý. Praha: Grada Publishing, 2007 . 281 s. ISBN 978-80-247-1766-1

[5] HEINIGE, Karel. Viry a počítače. Praha: Mobil Media, 2001. 80 s. ISBN 80-86593-02-9

[6] JALŮVKA, Josef. Moderní počítačové viry: podstata, prevence, ochrana: viry na různých systémech (Windows, Unix): viry šířené Internetem, makroviry a nové hrozby: zdrojové tvary virů: princip a funkce antivirů. Praha: Computer Press, 2000. 224 s. ISBN 80-7226-402-8

[7] Publikace PC World, IDG Czech, a.s., PŘIBYL, Tomáš. Seznamte se s rootkity, 2007, s. 108-110. ISSN 1210-1079
Dostupné z www.pcworld.cz

[8] Magazín informačních technologií CHIP, Vogel Burda Communications, s.r.o. 2008, ISSN 1210-0684
Dostupné z www.chip.cz

[9] http://cs.wikipedia.org/

[10] http://www.pcworld.cz/

[11] http://antispam.ooo.cz/info.htm

[12] http://www.kpsoft.eu/_techinfo/00070/Pocitacove_viry.pdf

[13] http://www.publish.cz/pczone/

[14] http://www.spyware.cz/

[15] http://www.rootkit.cz/

[16] http://www.lupa.cz/
[17] http://www.viry.cz/
[18] http://www.spammer.cz/
[19] http://www.zive.cz/
[20] http://www.actinet.cz/
[21] http://spampal.sidak.net/
[22] www.hoax.cz/
[23] http://test.bezpecnosti.cz/
[24] www.MalWare.cz/
[25] http://interval.cz/
[26] http://www.microsoft.com/
[27] http://www.chip.cz/
[28] http://www.factum.cz/
[29] http://www.earchiv.cz/

7. Seznam obrázků

Obrázek 1 - DDos útok [19] 21
Obrázek 2 - Hlavní šiřitelé spamu [8] 25
Obrázek 3 - Podvodný e-mail [26] 32
Obrázek 4 - Původci phishingu [8] 33
Obrázek 5 - Využívání antivirových programů [28] 41
Obrázek 6 - Ukázka detekce trojského koně [19] 43
Obrázek 7 - Test bezpečnosti internetových prohlížečů 55

8. Přílohy

Příloha č. 1 - Top 10 Malware roku 2007

1. Win32/Virut
2. I-Worm/Stration
3. I-Worm/Nuwar
4. Downloader.Tibs
5. Downloader.Zlob
6. BackDoor.Hupigon
7. PSW.OnlineGames
8. I-Worm/Netsky
9. I-Worm/Mytob
10. Worm/Feebs

[Zdroj: Magazín CHIP]

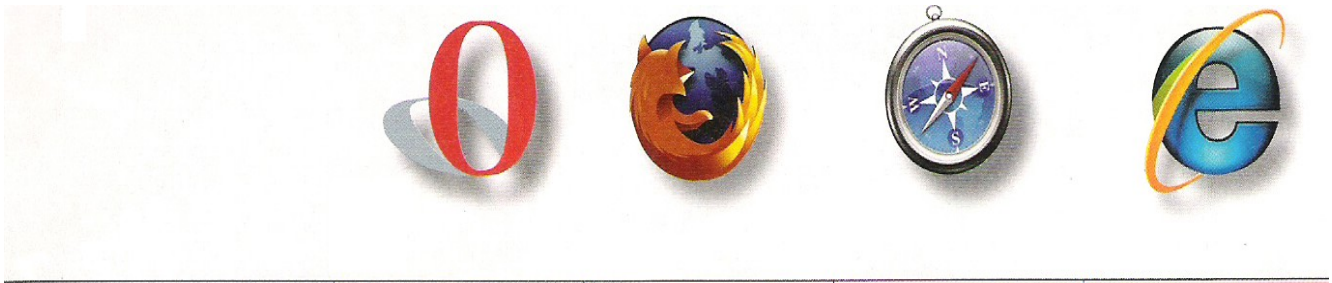
Příloha č. 2 - Nejaktivnější malware 1.pol. roku 2008

Trojan Downloader.MDW	Exploit.Win32.WMF-PFV
Worm Bagle.RC	Win32.Netsky.P@mm
Worm Lineage.GXD	Spyware.Pws.A
Worm Bagle.RP	Win32.Worm.Sohanat.AJ
Worm Lineage.HJT	Trojan.Dropper.RNY
Worm Perlovga.A	Win32.NetSky.D@mm
Worm Bagle.HX	Win32.Netsky.AA@mm
Worm Lineage.HIC	Trojan.Kobcka.CG
Worm Puce.E	Win32.Nyxem.E@mm
Worm Lineage.HJB	Trojan.Pandex.AC

[Zdroj: http://www.infomaticsonline.co.uk/, http://www.pcworld.cz/]

Příloha č. 3 - Stručné výsledky testu bezpečnosti internetových prohlížečů

Tento test byl proveden autory magazínu informačních technologií CHIP. Podle jeho výsledků je zřejmé, i když je Internet Explorer nejpoužívanějším browserem, že není nejbezpečnějším. Obsadil poslední 4.pozici z níže vybraných. I tyto výsledky jsou důvodem vzestupu ve využívání alternativních prohlížečů jako je například Opera či Firefox.



Přehled	1. MÍSTO	2. MÍSTO	3. MÍSTO	4. MÍSTO
Produkt	Opera 9.5 Beta (Kestrel)	Firefox 3.0 Alpha 8 (Gran Paradiso)	Safari 3.0 Beta	Internet Explorer 7
Výrobce	Opera Software	Mozilla Foundation	Apple	Microsoft
Web	www.opera.com	www.mozilla.org	www.apple.com/safari	www.microsoft.com
Celkové výsledky	94	78	63	55
	■■■■■	■■■■□	■■■□□	■■□□□
Bezpečnost (45 %)	99	96	70	59
Funkce (35 %)	100	66	45	53
Výkon (20 %)	72	60	77	51
Bezpečnost				
Phishingový filtr	●	●	▬	●
Deaktivace ActiveX	●	●	●	částečně
Známé záplatované/nezáplatované mezery v testované verzi	0/0	0/0	0/0	20/8
Známé záplatované/nezáplatované mezery v předchozí verzi	10/0	16/4	6/3	121/21
Blokování reklam/blokování pop-up oken	●/●	●/●	▬/●	▬/●
Cookie management	Velmi dobrý, konfigurovatelný pro každý web zvlášť.	Whitelist pro cookies vybraných webů.	Pouze základní nastavení: přijmout či zakázat.	Pouze základní nastavení: přijmout či zakázat.
Ukládání hesel/hlavní heslo	●/●	●/●	●/▬	●/▬
Mazání soukromých dat	Dvanáct různých možností.	Několik individuálních možností.	Volba „Private browsing", kdy není ukládáno nic...	Všechna data mohou být smazána jedním kliknutím...

Obrázek 7 - Test bezpečnosti internetových prohlížečů

[Zdroj: Magazín CHIP]