TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky a mezioborových inženýrských studií

Studijní program: B2612 – Elektrotechnika a informatika
Studijní obor: 2612R011 – Elektronické informační a řídicí systémy

MalWare a jeho nebezpečnost

Malware and his dangerousness

Bakalářská práce

Autor: **Michal Gottwald**
Vedoucí práce: Mgr. Jiří Vraný

V Liberci 18. 5. 2006

//Originální zadání práce

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 o právu autorském, zejména § 60 (školní dílo).

Beru na vědomí, že TUL má právo na uzavření licenční smlouvy o užití mé bakalářské práce a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem TUL, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených univerzitou na vytvoření díla (až do jejich skutečné výše).

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Datum 18. 5. 2006

Podpis

Poděkování

Děkuji Mgr. Jiřímu Vranému za odborné konzultace a vedení bakalářské práce.

Děkuji též celé rodině, která mi byla při studiu oporou.

Abstrakt

Bakalářská práce se zabývá nebezpečným softwarem. Děli ho do skupin a pro každou skupinu hledá vhodnou antivirovou ochranu. Jsou zde zmíněny jak starší způsoby počítačové infiltrace, tak i nové a velice nebezpečné metody. Malware sleduje na všech platformách a zařízeních (pracovní počítače, počítačové sítě, mobilní zařízení). Práce obsahuje i seznam nejpoužívanějších antivirových programu v České republice.

Summary

The baccalaureate work is concerned with dangerous software. Devides it on group and for each group look for suitable antivirus program. In this work are written ways of old and new computing infiltration. Monitor it on each platform and machinery (work computer, computer network, mobile equipment). Work contain catalog the most used antivirus program in Czech Republic.

Obsah:

0 Úvod……11

1 Dělení infiltrace……..12

1.1 Viry.……...12

1.2 Trojské koně (Trojan, Trojan Horse)……13

1.3 Červi (worm)……13

1.4 Backdoor (zadní vrátka)……..…….....14

1.5 Ostatní škodliviny…….....15

1.5.1Spyware……15

1.5.2 Dieler…….....16

1.5.3 Hoax……16

1.5.4 Phishing…….....17

1.5.5 Adware…...……..…..18

1.5.6 Downloader…….18

1.5.7Dropper……...……19

2 Dělení počítačových virů…….……..…19

2.1 Umístění v paměti…….…….……..19

2.1.1 Nerezidentní viry…….…….……. 19

2.1.2 Rezidentní viry…….…….…….20

2.2 Cíl infekce…….…....….....20

2.2.1 Bootovací viry…….…...….....20

2.2.2 Souborové viry…….…….....21

2.2.2.1 Prodlužující viry…… ……..21

2.2.2.2 Přepisující viry……..22

2.2.2.3 Duplicitní viry…….....22

2.2.2.4 Adresářové viry ……22

2.2.3 Multipartitni viry…….…….....…23

2.3 Projev Chování…….……..…23

2.3.1 Stealth viry……...…….23

2.3.2 Polymorfní viry……..……24

2.3.2.1 Mutation engine…….24

2.3.2.2 MtE-Mutation Engine……24

2.3.2.3 TPE-Trident Polymorphic Engine…….25

2.3.3 Tunelující viry…….…..…….25

3 Makroviry……...26

3.1 Makroviry v Microsoft Office…….……..26

4 Kryptové viry……..……...27

5 Antivirová ochrana…….……...28

5.1 Prevence……..28

5.2 Zvýšení bezpečnosti……29

5.3 Dělení antivirových programů……..…..……29

5.3.1 Jednoúčelové……..…….30

5.3.2 Jednoduché skenery……..…..……..30

5.3.3 Antivirové systémy…….……30

5.4 Metody antivirových systémů……..…….…….30

5.4.1 Skenování……30

5.4.2 Heuristická analýza……..31

5.4.3 Kontrola integrity (Integrity Checker)……31

5.4.4 Monitorovací systém (Behavior Blocker)……...……32

5.5 Metody léčení…….……32

5.5.1 Léčení počítače……33

6 Ochrana počítačových sítí…….33

6.1 Ochrana poštovního serveru ……..……....34

6.2 Ochrana protokolů HTTP, FTP a SMTP……..…..……34

6.3 Firewall……..……36

6.4 Clustering……..…….37

7 Antivirové programy…….……37

7. Avast!.....37

7.2 AVG…….....38

7.3 NOD32…….....38

7.4 Panda……..39

7.5 Norton…….....39

7.6 Kasperský antiviru…….39

7.7 McAfee VirusScan ……40

8 Nebezpečný software pod Linuxem……..40

8.1 Viry pod Linuxem…….……40

8.2 Červy pod Linuxem……..…….....41

9 Hacker versus virus……..……41

10 Sociální inženýrství…….……..……...42

11 Infiltrace v mobilních zařízeních…….……..……42

11.1 Viry v mobilních telefonech……..…….……42

11.2 Viry v PDA ……43

12Závěr…… …….……..45

13 Seznam použité literatury……... ……...46

Seznam obrázků

Obr. 6.1: Způsob ochrany poštovního serveru……..35

Obr. 6.2: Způsob ochrany pomocí CVP, kdy se používá více speciálních serverů pro jednotlivé protokoly…….36

Obr. 6.3: Způsob ochrany pomocí proxy serveru…….37

Obr. 7.1: Ukazuje počet zachycených virů za poslední měsíc u nejvíce aktuálního červa Win32/Netsky.Q worm…….39

Obr. 7.2: Ukazuje procento e-mailů infikovaných červem Win32/Netsky.Q worm za poslední měsíc……40

Seznam použitých zkratek

CVP	Content Vectoring Protokol	Přesměrující protokol
DNS	Domain Name Server	Server doménových jmen
FTP	File Transfer Protocol	Protokol pro přenos souborů
HTTP	HyperText Transfer Protocol	Hypertextový přenosový protokol
ICQ	I Seek You	Slouží pro komunikaci mezi uživateli
IRC	Internet Relay Chat	Přenos psaného rozhovoru
ISP	Internet Service Provider	Poskytovatel služeb Internetu
MBR	Master Boot Record	Hlavní zaváděcí sektor disku
pop3	Post Office Protocol 3	Protokol pro komunikaci poštovního klienta se SMTP serverem
SMTP	Simple Mail Transfer Protocol	Jednoduchý protokol elektronické pošty
TCP/IP	Transmission Control Protocol / Internet Protocol	Řídící přenosový protokol / protokol Internetu

0 Úvod

Skoro každá domácnost, která má doma počítač, je připojená k internetu. Pomocí internetu se šíří většina škodlivých kódů. Proto znalost ochrany před nebezpečným softwarem je v dnešní době nezbytně důležitá jak pro odborníka v oblasti IT technologie, tak i pro běžného laika. Metody, které využívají útočníci jsou důmyslné a mnohdy velice účinné. Škody napáchané neznalostí mohou být i katastrofální.

Tato bakalářská práce by měla analyzovat počítačovou bezpečnost před nebezpečnými kódy. Text je rozdělen do několika částí. První část je věnována dělením základních virů. Potom následují metody antivirové ochrany a ochrany počítačových sítí. Konečná část se zabývá bezpečností v Linuxu a mobilních zařízeních.

MALWARE (MALicious SoftWARE) je v překladu škodlivý software. Nebezpečný Software se může též označit jako počítačovou infiltrací. Tento termín označuje jakýkoliv neoprávněný vstup do počítačového systému.

1 Dělení infiltrace

Mnoho lidí za počítačovou infiltraci považuje počítačový virus a do tohoto pojmu shromažduje veškeré druhy infiltrace např. červy nebo trojské koně. Skutečnost však není zase tak jednoduchá. Každý ten druh se vyznačuje různými vlastnostmi a dovednostmi. Proto je nutné udělat řádné dělení.

1.1 Viry

Počítačový virus lze chápat z několika hledisek. První je hledisko uživatelské, které ho chápe jako určitý druh hrozby počítačového systému. Druhé hledisko je programátorské.
Zde je nutné napsat definici:

Počítačový virus je počítačový program, který může infikovat jiný počítačový program takovým způsobem, že do něj zkopíruje své tělo, čímž se infikovaný program stává prostředkem pro další aktivaci viru.

Autorem této definice je Fred B. Cohen.
Schopnost replikovat své tělo je vlastnost, která odděluje virus, tedy počítačový program, od jiných programů. Tímto se počítačový virus hodně podobá viru biologickému.
Velikost počítačového viru se pohybuje kolem desítky bajtů až desítky kilobajtů. Důvod tak malé velikosti je kvůli svému utajení. Čím menší virus je, tím je míně nápadný. Je nezbytná nutnost hostitele. Hostitelem může být spustitelný soubor nebo systémové oblasti disku. Virus se svým hostitelem žije v symbióze.

Virus se může šířit ve spustitelných aplikacích nebo pomocí maker v dokumentu Microsoft Word, Excel nebo PowerPoint. Díky Microsoft Outlook se šíří i pomocí internetu. Nesmíme zapomenout, že i formát PDF má vlastnosti, které mohou sloužit k šíření virů.

1.2 Trojské koně (Trojan, Trojan Horse)

Trojský kůň je program provádějící většinou destruktivní činnost o které uživatel neví. Tváří se jako užitečný, ale jeho účinky jsou škodlivé. Na rozdíl od virů nepotřebuje ke svému životu hostitele a nemá schopnost replikace. Nejčastěji se schovává pod spustitelným souborem EXE. Přenáší se pomocí virů, které ho nosí ve svých útrobách, nebo nevědomky sám uživatel. Jedinou možností, jak se trojského koně zbavit, je jeho smazáním. Trojské koně mají většinou destruktivní charakter. Likvidují soubory na disku nebo ho hnedka celý zformátují. Dále jsou používáni jako backdoory (v překladu "zadní vrátka"), spyware, dropper nebo keylogger. Zařazení trojského koně do nějaké skupiny virů je obtížné.

Šíření trojského koně je hlavně pomocí červa, který se do počítače může dostat pomocí e-mailu nebo bezpečnostních děr. Na počátku roku 2006 zneužili trojané bezpečnostní díru ve Windows a šířili se pomocí obrázků. Jde o chybu ve zpracování obrázku ve formátu WMF (Windows Metafile). Do počítače se může dostat pomocí e-mailového červa, který má v příloze obrázek s příponou WMF, nebo pomocí webové stránky, kde jsou infikované WMF obrázky. Ovšem ne každý WMF obrázek obsahuje škodlivý kód. Než takový obrázek otevřeme, tak je nutné ho zkontrolovat antivirovým programem. Již existuje záplata na tuto bezpečnostní díru.

1.3 Červi (worm)

Červ je program, který na rozdíl od virů neinfikuje spustitelné soubory, ale škodí systému tím, že pomocí počítačové sítě kopíruje sebe na připojené jiné počítače. Největší problém je potom s velikým zatížením sítě a se zahlcením disků počítačových stanic.

. Červ stejně tak jako trojský kůň nepotřebuje ke svému životu hostitele. Je výsadou sítí WAN a internetového protokolu TCP/IP.

Červy bychom mohli rozdělit na dva základní druhy. E-mailový, který se do počítače dostane pomocí elektronické pošty, a síťový, který pro vniknutí do systému využívá bezpečnostních děr.

Po spuštění škodlivého mailu se červ zkopíruje na disk počítače do adresáře Windows a zajistí si spuštění při každém nabíhání Windows pomocí záznamu v registru systému. Potom skenuje disky a hledá e-mailové adresy, aby se mohl dále šířit. Po vyhledání e-mailů přijde na řadu filtrace. Červ se snaží, aby nebyl zlikvidován, proto ze seznamu mailů eliminuje adresy antivirových společností a univerzit. Červ pro svoji utajenost otupuje zbraně antivirového softwaru. Snaží se udržet v infikovaném počítači co nejdéle.

Moderní červi už se nešíří volně ve spustitelných souborech, ale v ZIP archivu. ZIP soubory komplikují práci antivirových programů.

Snad nejznámějším zástupcem je e-mailový červ LoveLetter nebo-li I Love You. Jeho první výskyt byl v květnu roku 2000. Fungoval na všech operačních systémech. Tvůrce červa spoléhal na naivitu účastníků internetu. Přiložený soubor měl dvě přípony, čehož si leckdo nemusel vůbec všimnout (LOVE-LETTER-FOR-YOU.TXT.vbs). Na všech počítačích, které infikoval, smazal obrázky ve formátu JPG nebo JPEG. Tento červ je celosvětově známý.

Začátek viru obsahoval text:

rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispyder@mail.com / @GRAMMERSoft Group / Manila,Philippines

[7]

1.4 Backdoor (zadní vrátka)

Je to program typu klient-server, který je hodně podobný komerčním programům, jako je např. VNC, Ale narozdíl od nich uživatel o něm neví. Backdoor je používán pro vzdálenou správu počítače a jeho nebezpečnost závisí na člověku, který tuto správu vykonává. Klient je zde brán jako počítač útočníka a server jako počítač uživatele.Komunikace většinou probíhá na protokolu TCP/IP.

Backdoory se většinou nacházejí v e-mailové příloze síťových červů. Pokud ho svojí

neopatrností spustíme, tak se obvykle zkopíruje do adresáře Windows nebo Windows System, vytvoří si záznam v registru systému, což mu zaručí spuštění při každém nabíhání Windows. Jakmile se backdoor pevně umístí v našem počítači, snaží se kontaktovat svého tvůrce.

K tomu použije běžně dostupné prostředky, jako je e-mail nebo ICQ. Informuje ho o IP adrese, konfigurace počítače nebo o instalovaných programech. Dále jen čeká na příchozí instrukce. Útočník může získat úplnou kontrolu nad infikovaným počítačem. Může spustit jakýkoliv soubor, prohlídnout si obsah jednotlivých disku, pořizovat snímky z obrazovky, vysouvat dvířka mechaniky, přehrávat video nebo zvuk, hýbat s kurzorem myši, měnit datum, využívat periferních zařízeních a mnoho jiných nekalostí.

Samostatnou skupinou backdooru tvoří IRC backdoory. Principiálně fungují stejně. Odlišují se jen v řízení. Jsou ovládány přes speciální kalály IRC. Je to protokol, ve kterém spolu účastníci navzájem komunikují v reálném čase. Fuguje na principu chatu. Přístup k tomuto protokolu mají jen oprávnění uživatelé, tedy tvůrci backdooru. IRC backdoory mají omezené funkce.

Zástupci backdooru mohou být například NetBus, Master´s Paradise nebo SubSeven.

1.5 Ostatní škodliviny

1.5.1 Spyware

Program, který využívá internetu k rozesílaní dat z počítače bez vědomí uživatele.Od backdooru se liší tím, že nepřejímá kontrolu nad PC. Jde jen o statická data. Je to snaha zjistit zájmy uživatele.Vědět, jaké programy používá atd. Proto ho používá řada firem. Spyware je doposud legální. Mnoho antivirových programů vůbec nemají databáze proti spywaru. Pokud by je do svých programů zařadily, tak by jim mohlo být vyhrožováno žalobou.

Jak se tedy proti spywaru chránit. Běžné programy proti virům spywary nelikvidují. Ovšem existují specializované programy. Zástupce freewaru je například Spybot Search & Destroy, který je pro domácí použití zdarma.

Zástupce placeného programu je například Spy Sweeper. V řadě programů na internetu je zdarma skenování počítače, ale destrukce nebo izolace nalezené škodliviny je až se zakoupení licence. Na rozdíl od antivirového programu, který může být v počítači jen jeden, je počet antispywaru neomezený. Jako doplňkovou ochranu se může použit nejnovější záplaty operačního systému nebo využití nových verzí prohlížeče.

Spyware je velice pestrý, proto ho nelze 100% detekovat. Lze ho plně odstranit jen prevencí. Tento škodlivý kód se může do počítače dostat při instalaci nějakého softwaru nebo při surfování internetem (lákavá pop-up okna).

1.5.2 Dieler

Je to program, který změní parametry spojení. Přesměruje vytáčení na čísla

s vysokým tarifem (linka s předvolbou 976) , který potom musí uživatel zaplatit. Dieler využívá děr v prohlížeči a do počítače se dostane pomocí např. pornografických stránek. Existuje i jako legální forma. Ta slouží pro zpřístupnění na placené stránky. Je však obtížné potom dokázat, jestli je dieler nainstalován bez nebo s vědomím uživatele.

1.5.3 Hoax

Hoaxy jsou poplašné zprávy, které nás před něčím varují, žádají nás

o pomoc, něco nám nabízejí apod.

Tyto zprávy mají své specifické znaky:

1. Varují před nějakým nebezpečím.
2. Kladou na něho důraz, abychom dbali zvýšené opatrnosti.
3. Přesvědčování o důvěryhodnosti zprávy.
4. Vyzývání k dalšímu rozeslání.

Hlavně díky naivním lidem, kteří zprávě uvěří se hoaxy hodně šíří.

Typicky příklap hoaxu.:

Firma Nokia nabizi mobilni telefony WAP zdarma uzivatelum
Microsoft Windows. Pokud poslete tuto informaci 10krat,
obdrzite Nokia 3210.
Zaslete-li tuto zpravu 25krat nebo vice, ziskate Nokia 7110.
Nezapomente poslat kopii na adresu James.Dorfeld@nokia.com.
Pokud takto uciníte, bude Vás do ctrnácti dnu kontaktovat firma Nokia.

[6]

1.5.4 Phishing

Phishing je zkomolenina anglického slovíčka fishing. Do češtiny přeloženo jako rybaření. Termín označující podvodné e-maily rozesílané na více adres. Tyto dopisy jsou většinou z významné instituce např. banky. Uživatel je nucen vyplnit přidaný formulář nebo je uveden odkaz na stránku s formulářem. V něm se po příjemci žádá, aby vyplnil údaje o svém účtu apod. Ovšem žádný seriózní podnik by si nedovolil žádat takové údaje elektronickou poštou. Jedná se zde jen o trik získat z důvěřivých lidí informace. Využívá metod sociálního inženýrství.

Mladším zástupcem phishingu je pharming. Opět jde o zkomoleninu anglického výrazu. V tomto případě jde o „farming“. Do čestiny by to mohlo být přeloženo jako zemědělství nebo obdělávání. Pharming je mnohem zákeřnější. Zatímco phishing spoléhal na naivitu lidí a využíval metod sociálního inženýrství. Pharming takový není. Pro svou nekalou činnost používá překladu jména serveru na příslušnou IP adresu. Jinak řečeno zneužívá DNS. V tomto případě se tomu říká DNS cache poisoning. Pokud uživatel zadá požadovanou adresu, nedojde k přeložení na danou IP adresu, nýbrž na IP adresu podvodníka. Útočník si vytvoří podobné internetové stránky. Proto uživatel nebude vůbec nic tušit.

Útoky phishingu jsou čím dál častější a propracovanější. Už se nenaleznou chyby v pravopisu nebo v nekorektním oslovení. Obrana proti němu není jednoduchá. Detekovat phishing pomocí klasických antivirových programů je skoro nemožné. Neobsahuje žádný škodlivý kód a nemá důvod se dál šířit. Vyvíjejí se programy, které mají kombinovanou

ochranu. Spojení antivirového programu s firewallem, který monitoruje jakýkoliv odchod informací z počítače a informuje na to uživatele. Útokem Phisherů už nejsou banky nebo veliké instituce. Cílem jsou menší podniky.

Phishing se objevil i v Český republice. Podvodník, který se vydával za zástupce banky Citibank, chtěl po uživatelích elektronického bankovnictví čísla citiCard a PINu. Jeho úmysl byl následující. Nejprve rozeslal mnohým uživatelům internetu e-mail, ve kterém lidi přesvědčoval, že tato zpráva je skutečně od zmiňované banky. Dokonce byl přidán i odkaz na stránky Citibank. Ovšem pokud člověk kliknul na daný odkaz, tak se otevřela nejen potřebná stránka, ale i pop-up okno, které požadovalo právě daný PIN. Toto okno už nepatřilo bance, ale podvodníkovi. Phishing není v České republice ještě moc rozšířený. Důvody jsou ekonomického charakteru. Jsou vyspělejší státy, kde phishing jen kvete.

Jeden vzorový příklad phishingu:

> Vážený Citibank kliente
> V naší bance, kde si ceníme našich klientů a peněz, jsme nuceni aktualizovat naši databázi. Aktualizace vyžaduje vaši spolupráci a poskytnutí informací o vašich platebních kartách. Tím se vyhnete problémům se službami v našich bankomatech. Smyslem celé aktualizace je to, že chceme být dobře připraveni na aktualizaci ze smartcard na VISA. Nové karty čtou různé typy kódů v našich databází jsou bezpečnější než starý typ.
> Prosím aktualizace vaše informace kartově co nejdříve.
>
> **[6]**

1.5.5 Adware

Je to program, který znepříjemňuje práci a surfování po internetu pomocí neustálého zobrazování reklamních oken. Často nás nutí zobrazit nějaké stránky, o které nemusíme mít zájem.

1.5.6. Downloader

Škodlivý program, který se snaží stáhnout z internetu další nějakou škodlivinu.

1.5.7. Dropper

Nebezpečný program, který nestahuje škodlivinu z internetu, ale má ji ve svém kódu.

Potom existují ještě jiné formy programů, které sice přímo neškodí, ale škůdcům napomáhají. Jsou to programy typu **Rootkit**. Ty pracují pod systémem Windows. Jejich úkolem je skrýt vira, červa, trojského koně nebo třeba i spyware před antivirovým a antispamovým programem..

2 Dělení počítačových virů

Počítačové viry můžeme dělit do tří skupin. Jak jsou umístěni v paměti, co je cílem jejich napadení a jak se chovají vůči svému okolí. Je hodně časté, že jednotlivé skupiny se navzájem prolínají. Existuje ještě jeden typ virů, kterým se říká „In the Wild“. Jde o seznam nejrozšířenějších virů, který se používá k testování antivirových programů.

2.1 Umístění v paměti

2.1.1 Nerezidentní viry

Jsou to viry „přímé akce“. Nerezidentní virus v průběhu spuštění zavirovaného programu přebere řízení jako první před hostitelským programem. Provede svoji činnost, nejčastěji replikaci a pak předá řízení zpět svému hostitelskému programu. Nerezidentní viry jsou po stránce programátorské mnohem snazší na vytvoření. V dnešní době se už vyskytují jen zřídka.

2.1.2 Rezidentní viry

Je to daleko rozšířenější skupinou virů. Mají schopnost setrvat v paměti. Rezidentní programy mají vlastnost umožňující běh programu na pozadí operačního systému. Typickým příkladem těchto programů je ovladač myši. Ale na rozdíl od těchto programů rezidentní viry provádějí svoji činnost bez uživatelova vědomí. Jejich činnost je nelegální. Můžeme se setkat se souborovým virem nebo bootovacím virem. (U nerezidentních virů jsou jen souborové viry. Boot virus v reálné praxi neexistuje.)

Většina virů pro operační systém MS-DOS se umísťuje těsně pod hranici 640kB paměti RAM. Zaberou část této paměti pro vlastní potřebu. Operační systém o odebrané paměti nic neví, tak má virus zajištěno, že nedojde k jeho přemazání jinými daty.

Jak ale rezidentní viry nebo programy v počítači fungují? Možnost dostat se k prostředkům BIOSu nebo DOSu je díky přerušení běhu programu. *Přerušení (interrupt)* je hardwarový signál, který vede k přerušení běhu programu vykonávaného procesorem a přesměrování procesoru na program obsluhující přerušení. Po ukončení tohoto programu dojde k obnovení původního stavu a k pokračování přerušeného programu.

2.2 Cíl infekce

2.2.1 Bootovací viry

Tyto viry infikují části, které se nacházejí v určitých systémových oblastech na disku. Těmito oblastmi mohou být boot sektory disket, tabulka rozdělení pevného disku (partition table) nebo boot sektor pevného disku (MBR). Protože jsou v těchto oblastech instrukce, které po každém spuštění zavedou operační systém do pamětí počítače, mají viry, které se nacházejí v těchto oblastech, zajištěno jejich spuštění při každém zapnutí počítače.

Uvedené viry se chovají tak, že přepíší svým vlastním kódem boot sektor a původní přepsanou část boot sektoru uschovají na jiné místo disku. Virová infekce potom probíhá pomocí boot sektorů disket, kam se bootový virus replikoval. Operační systém DOS

je pro tyto viry ideální.Hlavně díky tomu, že často využívá příkazů, jako jsou zápis a čtení z disku, kopírování disket, prohledávání obsahu adresáře atd. Typickým symptomem bootových virů je skutečnost, že volná systémová

paměť je menší, než paměť instalovaná ve skutečnosti. Je nutné si uvědomit, že se zavirovanou disketou lze libovolně manipulovat, aniž by došlo k zavirování počítače. Jediná možnost zavirování je při pokusu o zavedení operačního systému z této diskety.

Tento druh virů je v dnešní době vzhledem ke snižujícímu významu disket na ústupu.

2.2.2 Souborové viry

Nejvíce rozšířená skupina virů, která napadá spustitelné soubory operačního systému. Nejčastěji jsou to soubory s příponami COM a EXE (přímo spustitelné), BAT (příkazový řádek), BIN (binární soubory), OVL (překryvné soubory) a SYS (ovladače). Tuto skupinu virů lze rozdělit do tří oblastí podle způsobu, jakým daná skupina infikuje daný program. Jsou to prodlužující, přepisující a duplicitní viry. Zajímavý způsob infikace mají adresářový viry. Všechny viry v těchto třech oblastí mohou být rezidentní nebo nerezidentní.

Pro své utajení nenapadají souborové viry malé programy. U kB programů se několika B vir lehce ztratí. Inteligentní souborové viry jsou schopni zajistit, že nedojde k vícenásobné infikaci. To znamená, že při opětovném spuštění nebude program znovu napaden stejným virem. Dokud nespustíme zavirovaný soubor, nemůže dojít k aktivaci souborového viru. Jiné aktivity se souborem jsou bezpečné.

2.2.2.1 Prodlužující viry

Tato skupina virů zkopírují svoje tělo na konec infikovaného programu. Změní údaje v hlavičce souboru a tím dojde k přesměrování ukazatele na tělo viru. Nejprve se provede tělo viru a po jeho ukončení předá řízení infikovanému souboru. Za normálních podmínek není virus pozorovatelný, ale pokud je rezidentní a obsahuje techniku stealth, tak během činnosti viru není prodloužení programu vidět.

Odstranění viru není složité. Stačí opravit začátek programu a smazat vir z jeho konce nebo začátku.

Vir můžeme umístit na začátek nebo konec souboru. Existují i viry, které své tělo vkládají dovnitř souboru. Tato skupina nepatří mezi prodlužující viry. Říká se jim mezerové viry. Jsou to hlavně soubory COMMAND.COM.

2.2.2.2 Přepisující viry

Málo zastoupená skupina virů. Jsou starší a ne moc inteligentní. Jejich činnost spočívá v přepisování infikovaného programu. Tím úplně znehodnotí program a způsobí jeho nefunkčnost. Tak dojde k jeho odhalení. Jsou to většinou nerezidentní viry přímé akce. Zavirované programy jsou definitivně ztraceny. Příkladem těchto virů jsou původní viry skupiny Hydra.

2.2.2.3 Duplicitní viry

Tyto viry napadají pouze programy s příponou .EXE tak, že vytvoří nový soubor se stejným jménem a s příponou .COM. Do něj umístí jen svoje tělo. V MS-DOS platí pro spuštění programu pravidlo priority. Nejprve operační systém hledá přípony .COM, .EXE a nakonec .BAT. Díky tomu, že infikovaný program je nedotčen, jde tyto viry obtížně detekovat. Příkladem je virus AIDS 2.

2.2.2.4 Adresářové viry

Tento vir je v počítači jen jeden. Napadá spustitelné soubory tak, že přepisuje v adresáři směrník takovým způsobem, aby ukazoval na začátek viru. Původní směrník si ukládá. Pokud je vir rezidentní, dokáže po provedení vlastního kódu i spuštění původních souborů. Příkladem těchto virů je DIR II.

2.2.3 Multipartitni viry

Tyto viry se chovají jako bootovací i jako souborové. Jsou schopny infikovat zaváděcí sektor disku, tabulku rozdělení disku, tak i spustitelné soubory. Jakmile se vir nabootuje, uchová si paměťovou rezidentnost a dále se chová jako vir souborový. Typickým reprezentantem multipartitních viru je vir OneHalf. Jiným příkladem je kombinace souborového viru a makroviru (vir Anarchy), makroviru a skriptového viru (vir ColdApe).

2.3 Projev Chování

2.3.1 Stealth viry

Tyto viry mají schopnost maskovat svoji činnost na počítači. Jsou rezidentní. Název je odvozen od anglického slova ‚stealth', což znamená lstivou činnost, vykonávanou potajmu. Mezi základní vlastností stealth virů patří:

-Skrývají jakoukoliv změnu spustitelných komponent v systému (např. změna délky souboru, změna boot-sektoru, tabulky rozdělení disku).

-Jsou schopny dezinfikovat programy ‚za letu'. Jakmile je zadán požadavek na otevření zavirovaného programu, virus jej nejdříve odviruje a pak předá operačnímu systému. Nakonec, když dojde požadavek k uzavření programu, tak jej virus opět zaviruje. Tato technika slouží jako ochrana před antivirovými programy.

-Většinou infikují programy už v okamžiku, kdy je program otevírán. Je to změna oproti klasické technice zavirování při spouštění programu. Díky tomu se tyto viry rychle šíří po celém systému.

Existuje ještě jedna podskupina těchto virů. Nazývají se sub-stealth. Od klasických stealth virů se liší tím, že mají jen jednu vlastnost z výše uvedených. Ale i přesto jsou velice nebezpečné.

2.3.2 Polymorfní viry

Polymorfní viry jde stejně jako stealth viry obtížně detekovat antivirovými programy. Používají však jiné prostředky. Jejich maskovací technika spočívá v tom, že žádná kopie při replikaci není totožná. Tato proměnlivost (polymorfismus) jej činí špatně identifikovatelným a odstranitelným skenovacími metodami.

Zakódovaný virus se skládá z dekódovací částí, která je většinou malá a virus rozkóduje, a se zakódovanou částí, která tvoří tělo viru. Klasické antivirové programy, pracujících na principu charakteristických řetězců, jej nedokáží odhalit. Jedinou nevýhodou tohoto mechanismu je ve skutečnosti, že právě dekódovací část využívá řada antivirových programů pro nalezení virů. Jde o semi-polymorfní viry, které používají statický dekódovač. Ten se nikdy nemění a tím je snadno detekovatelným. Tuto nevýhodu odstraňují plně polymorfní viry, neboť je u nich i dekódovač generován různě. Na nejvyšší úrovni je matamorfismus, který mění veškeré instrukce viru, tedy nejenom dekódovač.

2.3.2.1 Mutation engine

Mutační motory jsou kódy, které se přidají k jakémukoliv viru a tím se z něj stane vir polymorfní. To přináší velikou hrozbu, protože i starý a jednoduchý vir muže být velice nebezpečný. Mezi nejznámější mutační motory patří MtE nebo TPE.

2.3.2.2 MtE-Mutation Engine

Je od bulharského tvůrce virů Dark Avengera (1991). Jeho velikost je asi 2,4 kB. Jinak se tomuto motoru taky říká „Self Mutation Engine “ a „DAME“ (Dark Avenger Mutation Engine).

Princip tohoto algoritmu je následující. Nejprve se požádá generátor náhodných čísel o pseudonáhodné číslo. To bude bráno jako klíč k zakódování programu. Na základě klíče a vstupních parametrů se vybere registr pro indexování a následně se zvolí metoda kódovacího postupu. Potom se pomocí generátoru náhodných čísel vygeneruje mapa pro použití jednotlivých registrů procesoru. Nakonec se pomocí registrové mapy vygeneruje cílový algoritmus.

2.3.2.3 TPE-Trident Polymorphic Engine

Je menší než MtE. Jeho hodnota je asi 1,5 kB. Pochází z Nizozemí (1992). Metody TPE jsou podobné jako u MtE, avšak TPE má obecnější povahu. Všestrannost činí TPE obtížně detekovatelným antivirovými programy.

2.3.3 Tunelující viry

Jsou to viry, které neprovádějí zápis na disk klasickou cestou, ale způsobem, kdy tyto viry „protunelují“ řetězy ovladačů zařízení v paměti. Připojí se na konec řetězu a přímo ovládají řadič harddisku. Díky této technice jsou antivirové programy, fungující na principu kontroly stavu vektorů přerušení, bezradné. Je ovšem nutno říci, že tuto techniku využívá i některý antivirový software, aby obešel neznámé nebo nedetekovatelné viry.

Zde bych ukončil základní členění virů. Klasifikace virů není jednoduchá a mnohdy se setkáme i s členěním jiným. Makroviry a kryptové viry budou probrány ve zvláštních kapitolách.

3 Makroviry

Jak už napovídá název, jsou tvořeny makry. Makrojazyk je jazyk, který byl vyvinut, aby ulehčil práci s danou aplikací. Ve většině případů jde o zapamatování a uložení klávesových zkratek. Například program Microsoft Word lze pomocí makrojazyka naprogramovat tak, aby po stisku určitých kláves provedl nějakou činnost.

Makrovirem je nazýváno makro, které je schopno samo sebe zkopírovat z jednoho dokumentu do druhého. Může být zkopírováno i několikrát. S makroviry se můžete nejčastěji setkat v programech Microsoft Word nebo Microsoft Excel, které jsou součástí kancelářského balíku Microsoft Office. Tyto programy jsou pro tvůrce virů nejatraktivnější, protože jsou nejpoužívanější. První makrovir se objevil v roce 1995 a jmenoval se Concept.

Makroviry jsou nezávislé na platformě. To je jejich velikou výhodou. Mohou fungovat na počítačích IBM PC i Macintosh a i na operačních systémech Windows 3.1, Windows NT, MacOS.

Dále se budu zabývat makroviry v aplikaci MS Word.

3.1 Makroviry v Microsoft Office

Systém bude infikován, jakmile editor načte nakažený soubor. Potom při jakémkoliv otevření textového dokumentu spustí Word pomocí šablony infikované makro.

Je nutno říci, že Word rozlišuje mezi šablonou a dokumentem. Šablony nesou kromě klasických dat i klávesové zkratky, definice tlačítek lišty nebo právě zmiňovaná makra. A jaký je mezi nimi rozdíl? Odlišují se v příponě (pro dokumenty .DOC a pro šablony .DOT) a v jednom bitu uvnitř stavového slova v dokumentu. Dokumenty, které byly napadeny makroviry, byly změněny na šablony, aby vir mohl být při jejich načtení aktivován.

Nejvíce používaná jsou automatická makra. Příkladem může být makro AutoExec šablony NORMAL.DOT (automatické spuštění při startu), AutoOpen (při otevření

dokumentu), AutoClose (při uzavření dokumentu), AutoNew (při vytváření nového dokumentu) a AutoExit (při ukončení práce s Wordem).

Další způsob, jak proniknout do systému může být pomocí systémových maker. Jsou to jednoslovné operátory jazyka WordBasicu, které poskytují různé funkce. Tyto funkce jsou běžně volány pomocí klávesových zkratek nebo panelu nástrojů. Nejpoužívanější makra jsou FileSave, FileSaveAs nebo FileClose. Pokud je zavirovaný dokument a použije se makro FileSave, tak dojde k aktivaci viru.

4 Kryptové viry

Podle definice je kryptografie psaní tajným nebo šifrovaným písmem. Psaní šifer je tradičně považováno za ochranou záležitost. Z hlediska virů je to slovo velice útočné. Kryptografie tedy může vést k tvorbě nebezpečného softwaru.

Útoky spojují kryptografické metody s technikou počítačového viru. Dá se říct, že viry se díky kryptografii stanou ještě nebezpečnějšími. Tyto viry mohou být použity jako nástroj vydírání nebo jiné počítačové kriminality.

Pisatel viru se snaží, aby jeho výtvor byl špatně detekovatelný antivirovými programy, co nejdéle přežil a napáchal co nejvíce škody. Je zřejmé, že čím více je hostitelský program závislý na viru, tím vir déle a snáze přežije. Učinit hostitele být maximálně závislým na viru, je smyslem použití šifer. I když bude takový virus detekován, nemůže být zničen nebo smazán, protože by mohlo dojít k poškození dat hostitele. Virus může být zničen s pomocí autora viru. Tento případ je ideální pro vydírání.

Jak vlastně takový útok kryptoviru vypadá? Jakmile virus infikuje a zašifruje data, upozorní vlastníka infikovaných dat a vyzve ho, aby kontaktoval autora viru. Ten bude požadovat výkupné za soukromý klíč. Většinou to nejsou malé částky. Pohybují se kolem stovek tisíc v závislosti na důležitosti dat. Jakmile získá soukromý klíč, tak je schopen dešifrovat soubory a získat zpět svoje data.

Situace pro vlastníka důležitých dat není tak bezvýchodná. Již existují opatření proti infekci kryptoviru. Ve velikých firmách nebo v bankovním sektoru se používají mimo antivirové i kryptografické ochrany, jako je například šifrování firemních CD nebo zamezení přístupu neautorizovaného softwaru.

5 Antivirová ochrana

Funguje jako obrana před různými druhy infiltrace. V dnešní době je to už samozřejmostí, že každá rodina nebo firma má nainstalovaný nějaký antivirový software. Problematika ochrany dat je pořád aktuální. Není totiž vůbec jednoduché efektivně chránit svoje data. A to hlavně platí pro veliké firmy. Některé útoky můžou být i cílené a ztráty na datech mohou být katastrofální. Tato problematika nesmí být podceněna. Domácí uživatelé jsou na tom lépe. Jim stačí si nainstalovat z nějakých nabízených antivirových programů. A těch je na trhu nepřeberné množství. Mnoho programů je na internetu jako shareware, kde si můžete nainstalovat volně šířitelnou verzi. Zadarmo si můžete nejprve produkt vyzkoušet a pak si to zaregistrovat. Registrace umožňuje řadu výhod jako je přístup k aktuálním virovým identifikačním řetězcům a mnoho dalších. Je ovšem důležité si uvědomit, že každý antivirový program je nutno aktualizovat.

5.1 Prevence

Prevence je velice důležitá. Hodně lidí přenechává ochranu svých dat antivirovým programům a firewallu. V klidu brouzdají nebezpečnými servery s pocitem bezpečí. Ovšem ne každý antivirový program je tak kvalitní, že pozná každou škodlivinu. Ve světě počítačů roste počet nebezpečného softwaru neuvěřitelně rychle. Ani častá aktualizace antiviru nedokáže zaručit 100% zabezpečení. Tvůrci škodlivin hlavně spoléhají na naivitu a nevědomosti uživatelů počítače. Pokud by chtěl uživatel zajistit vysoké procento zabezpečení

svého počítače, musel by svým ochranným programům porozumět a umět je správně používat. A ne je jenom mít nainstalovaný na disku.

5.2 Zvýšení bezpečnosti

V první řadě je důležité mít v počítači nainstalovaný antivirový program a zajištěnou jeho pravidelnou aktualizaci. Čím častěji se bude aktualizovat virová databáze, tím se bude více zvyšovat bezpečnost. Nejlepší je zajistit si automatickou aktualizaci. Stahovat z internetu se může třeba i každou hodinu.

Zajistit minimální chod modulu, který se stará o neustálé hlídání souborů, ke kterým uživatel přistupuje. Které uživatel otevírá, uzavírá, kopíruje atd. V antivirových systémech se jim jinak říká rezidentní štít nebo on-access skener.

Snížit riziko vniknutí nebezpečného softwaru se dá i pomocí aktualizací programů, které pracují s internetem nebo celkově s nějakou sítí. Tyto programy mohou obsahovat bezpečnostní díry, které může někdo zneužít pro ovládnutí cizího počítače.

Vlastnit Firewall je dnes už téměř samozřejmosti hlavně pro lidi, kteří vlastní veřejnou IP adresu, která je dostupná pro všechny uživatele internetu. Mít vypnutý firewall znamená zpřístupnit data jiným uživatelům sítě. Může to mít výhodu, že člověk může pracovat na svém počítači prostřednictvím jiného počítače. Stačí znát IP adresu. Freeware programu, který zvládne vzdálený přenos dat se nazývá VNC (virtual network computing).

Aby měl zapnutý firewall smysl, musí se určit, kterou komunikaci povolit a kterou zakázat. Firewallu je věnována samostatná kapitola.

5.3 Dělení antivirových programů

Antivirový software lze rozdělit podle mnoha kritérií. Já jsem vybral dělení

podle složitosti programů (od nejjednodušších po nejsložitější).

5.3.1 Jednoúčelové

Nejde o plnohodnotnou ochranu dat. Jsou to jednoúčelové programy, které slouží pro detekci nebo dezinfekci jednoho konkrétního viru. Tento software je zdarma a je ho možné stáhnout z internetu.

5.3.2 Jednoduché skenery

Opět nejsou plnohodnotnou ochranou dat. Jsou to spíše jako kontrolní složky, nedokážou léčit. Určeny pro kontrolu systému. Jsou taky zdarma.

5.3.3 Antivirové systémy

Nejrozšířenější forma antivirových programů. Hlídá všechny místa, kterými by mohla infiltrace do systému proniknout. Antivirové systémy jsou aktualizovány prostřednictvím internetu. Současně může být použit i firewall. Produkty této skupiny jsou například AVG, žvast!, McAfee Viruscan aj.

5.4 Metody antivirových systémů

5.4.1 Skenování

Tyto programy využívají identifikační řetězec pro zjišťování přítomnosti viru. Řetězce jsou uloženy ve virové databázi. Ta dokáže odhalit viry, které byly vytvořeny před datem vzniku dané databáze. Častou aktualizací bude docíleno, že i novější viry budou detekovány.

Po skeneru požadujeme vysokou detekční schopnost, nízký počet falešných poplachů a velikou rychlost. Aby docílily nízkého počtu falešných poplachů, používají více různých řetězců spolu s přesným umístěním pro zachycení jednoho viru. Vybrat správný řetězec nebylo zase tak náročné do té doby, dokud se nezačaly psát zakódované viry. Pak se řetězce vybíraly z tzv. dekryptovací smyčky.

Dobré skenery obsahují anti-stealth techniky, které naleznou stealth viry.

Existují dva typy skenerů:

On-access scanner – V dnešní době je velice používaný antivirovými programy. Existoval už v době DOSu. Ale nevýhodou bylo, že MSDOS byl nenáročný na výkon a velikost operační paměti. To způsobilo, že takový rezidentní skener chod počítače hodně zpomalil. Změna nastala až příchodem Microsoft Windows 95. Ten používá velikou operační paměť a je náročný na výkon, tak mu přítomnost on-access scanneru nečinil žádný problém.

Hlavní výhodou je, že monitoruje veškerou činnost uživatele se soubory a pokud narazí na nějaký vir, tak ho na to upozorní. Upozorní dřív, než stihne soubor otevřít a tím vir aktivovat.

On-demand scanner – Funguje na požádání. Uživatel si vybere, jakou část chce zkontrolovat (disketa, pevný disk). Byly nejvíce využívány v MSDOS.

5.4.2 Heuristická analýza

Detekce virů podle identifikačních řetězců nelze u polymorfních virů. Zde se využívá tzv. heuristické analýzy. Její principem je expertní systém, který zkoumá úvodní instrukce programu. U heuristické analýzy na rozdíl od identifikačních řetězců, které hledají konkrétní vir, hledají přítomnost jakéhokoliv viru.

5.4.3 Kontrola integrity (Integrity Checker)

Je založena na principu porovnání aktuálního stavu souborů se vzory uložených v kontrolních programech. Kontrolované objekty by měly být důležité programy. Kontrola

integrity dokáže detekovat i novější viry, které ani heuristická analýza nedokáže nalézt. Tato metoda dokáže viry nejen nalézt, ale i odstranit. Jelikož si musí pamatovat kontrolní součty původního souboru, není pro něj problém si zkontrolovat, jestli daný program správně vyléčil. Proto je léčení pomocí kontroly integrity bezpečný. Metoda kontroly integrity se nejčastěji vyskytuje ve spojení s on-demand skenerem obohacenémo heuristickou analýzu.

5.4.4 Monitorovací systém (Behavior Blocker)

V reálném čase sleduje změny v chování systému. Hledá viry na základě jejich podezřelých akcí. Například jedná-li se o zápis do chráněných souborů. Monitorovací systém není dokonalou metodou při vyhledávání virů. I obyčejný program může provést akci, kterou monitorovací program vyhodnotí jako útok viru. Může tedy docházet k planým poplachům. Na druhou stranu mohou nové viry používat takové akce, které naprogramované moduly vůbec nemusí znát. A aby toho nebylo málo, tak existují viry, které dokážou monitorovací systém obejít nebo úplně vypnout. Jedná se o tunelující viry.

U monitorovacího systému je důležité jeho nastavení. Pokud se to podcení, tak může hlásit přítomnost viru téměř neustále nebo naopak nenahlásí vůbec nic, i když je počítač plně zavirovaný. Pokud tento systém nahlásí podezřelou akci, tak je jen na uživateli, aby posoudil, jestli se jedná o planý poplach nebo o útok viru.

Tato metoda má i svoje klady. Nevyžaduje častou aktualizaci a pokud ji správně nastavíme, tak může být i dobrým prostředkem pro detekci virů.

5.5 Metody léčení

Antivirové programy nabízejí řadu činností, co s infikovaným programem udělat. Asi nejjistější likvidací virů je jejich smazaní. 100% se vir odstraní. Ale jsou případy, kdy je tato metoda nevhodná a ne pokaždé chceme odstranit daný program. Může obsahovat důležitá data. Další metodou je přesunutí infikovaného souboru do karantény, pokud ovšem to nainstalovaný antiviru nabízí. Velice podobné je přejmenování souboru. Tím se zabrání jeho

spuštění a aktivací viru. Tato metoda je jen dočasná. Nejlepší metodou, jak odstranit virus a získat zpět svoje data, je daný soubor vyléčit.

5.5.1 Léčení počítače

Pokud se podcení antivirová ochrana nebo selže antivirový software, je nutné zachovat chladnou hlavu a hnedka neformátovat pevný disk. Nejprve se musí vir, který napadl počítač identifikovat. K tomu poslouží různé databáze na internetu bud on-line nebo off-line verzi. Potom se musí zapnout antivirový program z CD. Antivir z pevného disku může být už zavirovaný a jeho spuštěním by se mohl vir aktivovat. Po spuštění se musí aktivovat položka léčení.

Je ovšem nutné si uvědomit, že ne všechny programy lze vyléčit. Daný antivirový program v sobě nemusí mít příslušný algoritmus nebo je léčení nemožné. Léčit program napadený přepisujícím virem je velice náročné a může způsobit, že už soubor nikdy nebude funkční. V tomto případě je jen jediná možnost v přeinstalovaní neúplných souborů z instalačního CD.

Antivirový software dokáže při léčení makrovirů přesně určit, kde se nacházejí jednotlivá makra a i makra virem napadená. Přepíše virová makra a zachová původní. Pokud by je nedokázal navzájem odlišit, tak je přepíše všechny. Samotný text však zůstane nepoškozen.

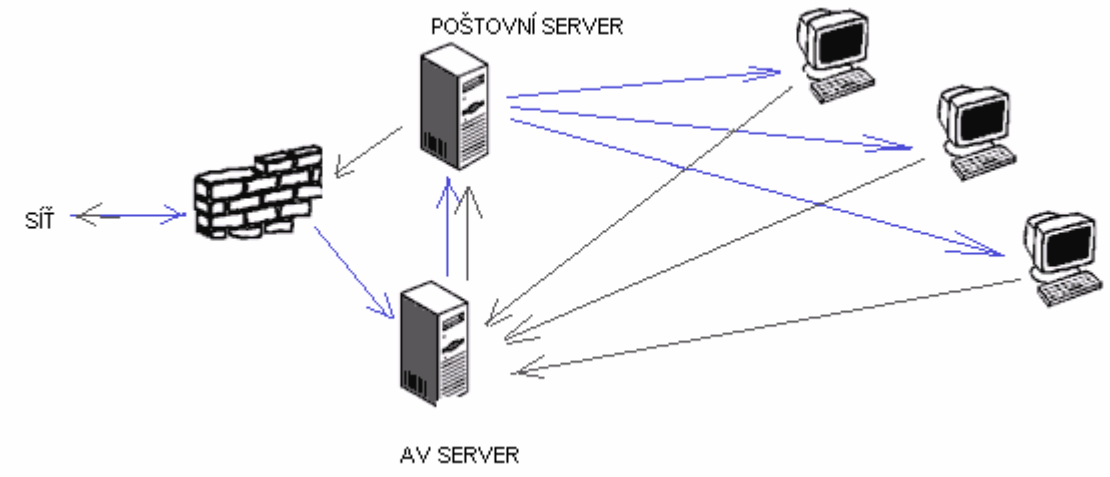
Nesmí se instalovat více antivirových programů na jeden počítač. Neplatí pravidlo, že více ochrany způsobí větší bezpečnost. Právě naopak. Antiviry se mohou ve své činnosti navzájem ovlivňovat a způsobit více škody než užitku.

6 Ochrana počítačových sítí

Je důležité mít minimálně 3 druhy ochrany. Základem je antivirový program na pracovní stanici, který je doplněn ochranou vstupních bran nebo poštovního a souborového serveru. Nezbytá je taky účinná centrální správa, která dohlíží na celý systém.

6.1 Ochrana poštovního serveru

Hlavní ochrana je soustředěna na e-mailový protokol SMTP. Princip je takový, že mail nejprve směřuje na antivirový skener, kde jsou pakety složeny do ucelené formy. Potom dochází k antivirové kontrole. Nakonec jsou opět rozloženy na pakety a směřují na pravý poštovní server. Stejný princip funguje i na lokální síti. Rychlost je výhodou tohoto principu. Používají ho Internet Service Provider.



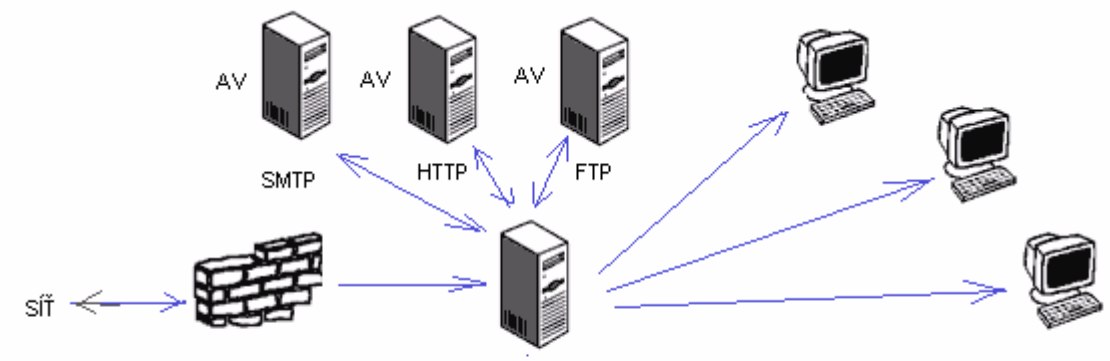
Obr. 6.1: Způsob ochrany poštovního serveru. **[5]**

6.2 Ochrana protokolů HTTP, FTP a SMTP

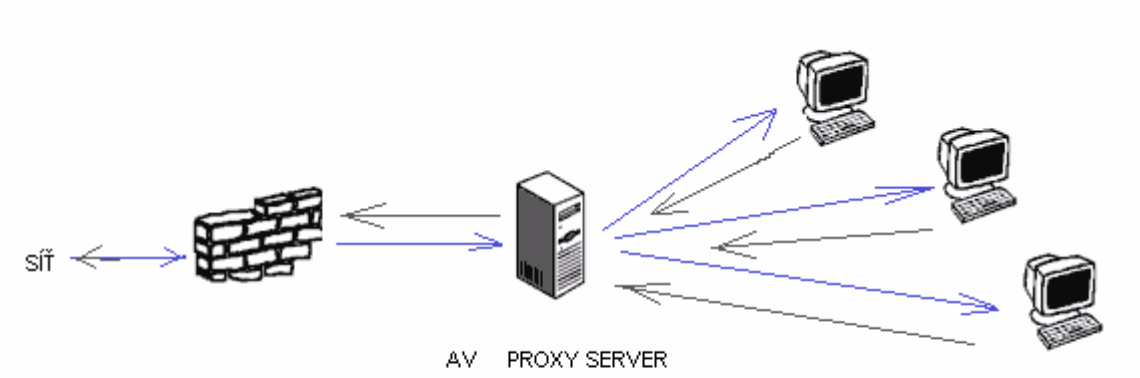
Pomocí SMTP protokolu se šíří většina škodlivých kódů. Ale není to jediná možnost pro šíření. I HTTP nebo FTP protokol může být zneužit. Nejpoužívanější řešení pro ochranu HTTP a FTP nebo i SMTP protokolů jsou antivirové programy pro proxy servery a firewally, které fungují na principu CVP.

Protokol CVP přesměruje dané protokoly na speciální server, kde dojde k jejich antivirové kontrole. Potom jsou poslány zpět na firewall. Pokud neobsahují škodlivý kód, jsou poslány na pracovní stanice. Pro zavedení tohoto principu je nutné vlastnit firewall s podporou CVP. Je hardwarově náročný. Je možnost využít více speciálních serverů. Každý by měl na starosti jeden z protokolů (SMTP, HTTP, FTP).

Jinou zmiňovanou metodou je využití proxy serveru. Princip této metody je následující. Mezi firewallem a pracovními stanicemi se vloží speciální proxy server. Data jsou posílány na tento proxy server, kde dochází k jejich antivirové kontrole. Nezávadná data jsou směřují z proxy serveru na pracovní stanice. Tento princip funguje i pro data posílaná z pracovní stanice do sítě. Výhoda této metody je v rychlosti. Nemusí se vracet zpátky, jak je tomu u metody CVP. Firewall nemusí podporovat CVP. Nízké hardwarové nároky a možnost kontrolovat i jiné protokoly (POP3). Nevýhodou je vysoká cena nebo nemožnost zálohování dat.



Obr. 6.2: Způsob ochrany pomocí CVP, kdy se používá více speciálních serverů pro jednotlivé protokoly. **[5]**



Obr. 6.3: Způsob ochrany pomocí proxy serveru. **[5]**

6.3 Firewall

Do češtiny přeloženo jako protipožární zeď, která chrání jednotlivé počítače nebo sítě před nebezpečnými kódy z internetu. Může být provedeno ve formě hardwaru nebo softwaru. Monitoruje všechny data, která jsou přenášena z internetu do místní sítě nebo z místní sítě ven. Vytvoří jejich analýzu a rozhodne, jestli jsou data nebezpečná. Pokud jde o škodlivé kódy, může zamezit jejich přístup nebo odchod. Rozpoznání nebezpečí závisí na nastavení firewallu. Dokáže skrýt některé vlastnosti počítače, jako je například otevřené komunikační porty. Nastavení by mělo být optimální.Pokud by byl nastaven na maximální ochranu, mohlo by se stát, že budou zamítnuty některé služby.

Softwarový firewall je program, který je nainstalován v operačním systému počítače.

Pro svou práci používá síťové rozhraní tohoto počítače. Hardwarový firewall je samostatné zařízení umístěné většinou v rozvaděči (rack). Má vlastní síťové rozhraní pro připojení k internetu.

Osobní firewall monitoruje síťový provoz, vyhledává nedovolené pokusy o komunikaci, povoluje komunikaci schváleným aplikacím nebo blokuje vyskakující okna a reklamu. Funkcí je opravdu hodně. Zaleží na nastavení, které potlačit nebo naopak posílit.

Firewall je možno stáhnout z internetu. Například česká firma Kerio nabízí Kerio Personal firewall. Betaverze je zdarma.

6.4 Clustering

Metoda clustering nabízí možnost vložit do sítě neomezený počet serverů. Jejich výkon je sčítán pomocí softwaru třetí strany (Stone Beat Securyty Server). Tato metoda je dobrá pro ISP.

7 Antivirové programy

Zde je seznam nejznámějších a nejpoužívanějších antivirových programu v České republice.

7.1 Avast!

Tento antivirový program pochází od české společnosti Alwil. Zajišťuje zabezpečení PDA , PC, servery, groupware nebo firewall.

Firma nabízí i domácí verzi zdarma (avast!4 Home Edition), verzi pro Linux (avast!4 Linux/UNIX) nebo odlehčenou verzi pro spolupráci s produkty firmy Kerio Technologies, která nabízí duální antivirovou ochranu (Kerio MailServer s antivirovými moduly). A jaký je princip? Dvojitá antivirová ochrana prověří každý e-mail jak integrovaným antivirovým programem, tak antivirem třetí strany. Dvojitá antivirová ochrana snižuje riziko vniknutí viru ještě dříve, než výrobce vydá novou aktualizaci databáze virů.

7.2 AVG

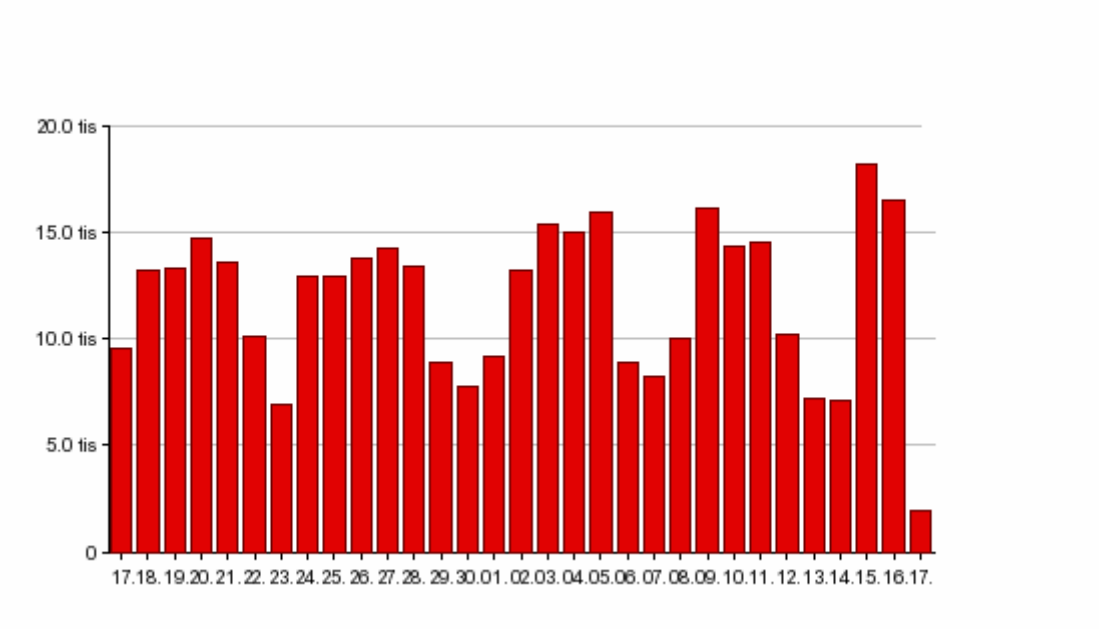
V České republice je to nejrozšířenější antivirový program. Je od firmy Grisoft. I přes to, že nedosahuje takových kvalit, má veliký podíl na truhu.

7.3 NOD32

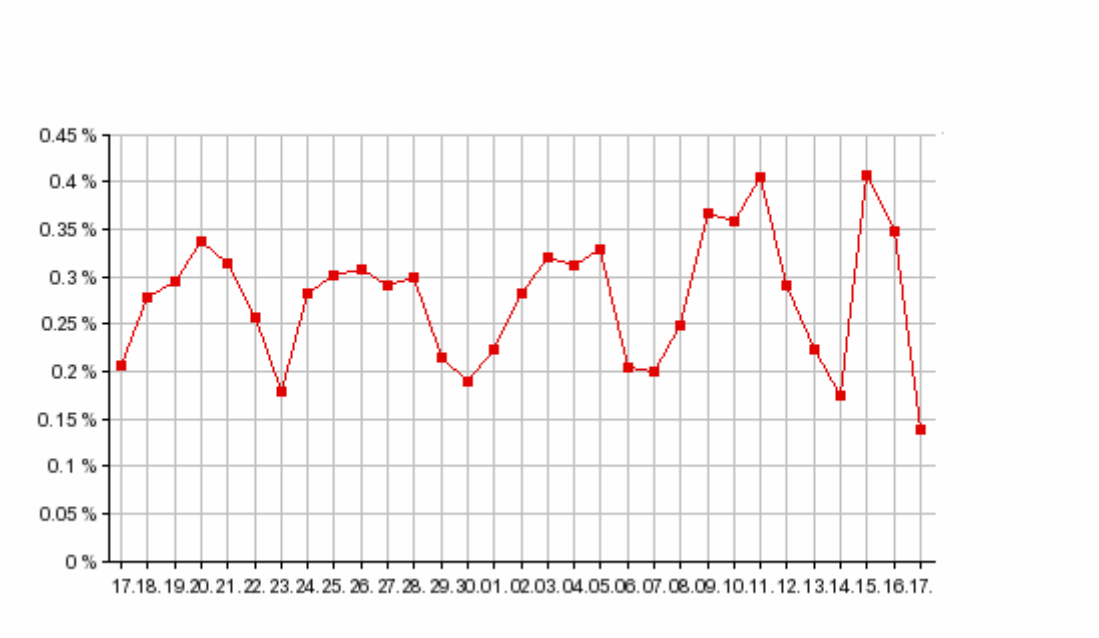
Jeden z nejrychlejších antivirových programů. Pochází ze Slovenska od společnosti ESET. Je držitelem mnoha ocenění britského časopisu Virus Bulletin, který provádí testy antivirových programů " In the Wild ". Jeho nevýhoda je v hardwarové náročnosti.

Používá technologii ThreatSence, která spočívá v kombinaci různých metod testování založených na heuristické analýze včetně emulace 32-bitového kódu. Využívá paralelní kontrolu.

Tato slovenská firma vytvořila na internetu on-line **virový radar**, který slouží pro monitorování a statickou analýzu virových infiltrací šířících se pomocí e-mailu. Statistiky ukazují počet zachycených virů za posledních 24 hodin, 168 hodin, 31 dní nebo až 12 měsíců. Určují i stupeň ohrožení.



Obr. 7.1: Ukazuje počet zachycených virů za poslední měsíc u nejvíce aktuálního červa Win32/Netsky.Q worm. **[7]**



Obr. 7.2: Ukazuje procento e-mailů infikovaných červem Win32/Netsky.Q worm za poslední měsíc. **[7]**

7.4 Panda

Oproti NOD 32 je Panda použitelná i na slabší počítače. To je snad jeho jedinou výhodou. Mezi jeho nevýhody patří například pomalá aktualizace.

7.5 Norton

Tento program je od veliké softwarové firmy Symantec. Má ochranné řešení pro společnosti i pro jednotlivce. Funguje na všech platformách. Jeho hlavní nevýhoda je v hardwarové náročnosti nebo v absence technické podpory v českém jazyce.

7.6 Kasperský antivirus

Velice známý ochranný program pocházející z Ruska od společnosti Kasparsky Lab.

Zakladatelem je Evžen Kasperský. Program je hardwarově a síťově náročný. Má vynikající skenovaní vlastnosti. Aktualizace je vydávána každou hodinu.

7.7 McAfee VirusScan

Je od klasické americké společnosti McAfee. Tato firma je druhým největším výrobcem antivirových programů na světě. Její produkty obsahují mnoho nadstandardních funkcí, mezi niž patří ochrana přístupu a detekci adwaru.

8 Nebezpečný software pod Linuxem

Linux vznikl přenesením operačního systému UNIX na platformu IBM PC. Od UNIXU si Linux převzal bezpečnostní principy.

8.1 Viry pod Linuxem

. Viry napsané pro Linux skoro neexistují. Je to způsobeno tím, že Linux má řadu opatření, které starší verze systému Windows vůbec nevlastní. Jde především o zakázání měnit programy nebo instalovat nové aplikace pro ostatní uživatele. Jen správce má taková oprávnění. Novější verze (od Windows 2000 a Windows XP) už mají podobný systém oprávnění. Ale není tak bezpečný jako pod Linuxem. Uživatele Windows převážně používají jen jeden přístup do systému a to ten správcův. Správcem tedy bývá vlastník počítače (otec rodiny nebo starší bratr) a uživatelé bývají mladší děti.

8.2 Červy pod Linuxem

Pro Linux vznikly tři významní červy. První z nich byl červ Blues, který byl objeven antivirovou firmou McAfee.

Druhý byl červ nesoucí název Slapper, který napadal některé verze serveru Apache. Slapper napadá systém pokud je přítomen kompilátor GCC. Tento kompilátor musí být spuštěný, pokud běží Apache.

A nakonec Linux/Ramen, který napadal starší systémy Red Hat.

9 Hacker versus virus

Je pojem se kterým je seznámena i laická společnost. Hacker je člověk znalý IT technologie, programování, operačních systémů, počítačových protokolů. Všechny tyto vědomosti využívá ve prospěch firmy. Nalézá a upozorňuje na chyby v softwaru. Tato skupina hackerů patří mezi ty hodné. Ovšem existuje i taková skupina, která svých vědomostí využívá ve svůj prospěch. Snaží se proniknout do jiných systémů a chtějí z nich získat data pro svoji vlastní potřebu. Neváhají svých vědomostí zneužít.

Vir je program, který dělá to, co mu programátor zadal. Hacker má vědomosti a určitou inteligenci, což ho činní nebezpečnějším. Ovšem hacker nemá schopnost replikace Proto jsou jeho útoky méně častější. Vybírá si spíše veliké a bohaté instituce, kde by mohl napáchat veliké škody. Obyčejný účastník internetu se nemusí bát, že by jeho počítač hacker navštívil. Pro svůj útok často používají sociální inženýrství.

Obrana je stejná jako u virů. Záplatovat bezpečnostní díry a používat osobní firewall. Je totiž pravidlem, že pokud hacker narazí u nevýznamného počítače na odpor, nebude se snažit do systému proniknout. Firma Kaspersky nabízí program, který zaručuje ochranu před útokem zvenčí a před nežádoucím odesílání dat z počítače (Kaspersky Anti-Hacker). Trial verze programu je volně ke stažení na internetu.

Známý je i ScriptKiddie. Jde o člověka, který dané problematice vůbec nerozumí. Nalezne program, který má škodit. Použije ho, i když neví, jak funguje. Jelikož nemají svou činnost pod kontrolou, jsou mnohdy nebezpečnější než hackeři.

10 Sociální inženýrství

Tento pojem je v počítačovém světě velice známý. Nejde o žádnou vědu, ale o soubor metod, kterými se snaží útočník (hacker) přesvědčit uživatele, aby otevřel mail, řekl mu svoje heslo, PIN, konfiguraci počítače atd. Tyto techniky jsou velice účinné. Je to nejsnadnější cesta k potřebným informacím.

Většinou se útočník vydává za zástupce banky, za správce sítě nebo za opraváře. Aby mohl udělat svoji práci, potřebuje potřebná data. Majitel, který se domnívá, že opravdu komunikuje s údržbářem, data předá. Tyto útoky jsou však přesně cílené. Během několika minut může být počítač zavirovaný a důležitá data odcizena.

Další odvětví, kde se sociální inženýrství používá je v pestré a lákavé nabídce e-mailů. Typickým příkladem použití sociálního inženýrství je e-mailový červ I Love You. Kdo by odolal láskyplnému mailu. Navíc byly použity dvě přípony, přičemž druhá nemusela být díky systému Windows vůbec vidět.

Tato metodika je v dnešní době velice používána.

11 Infiltrace v mobilních zařízeních

11.1 Viry v mobilních telefonech

V moderních mobilních telefonech, které obsahují operační systém, je určitě reálný, že mohou být napadeny škodlivými kódy. Starší telefony měly speciální software pro každý typ telefonu. Software se lišil nejen značkou a výrobcem, ale i různými modely určitého dodavatele. Tento software se nazýval firmware. V těchto telefonech nemá virus šanci existovat. Nemá možnost proniknout do systému, protože pro zápis do vnitřní paměti se používá speciální software a hardware. Tyto telefony neumí spustit jiný software než ten, který mají napevno nahraný ve firmwaru. Nemá funkci AutoRun, čímž nemá možnost se šířit.

Novější telefony používají operační systém vytvořený pro mobilní telefony. Na dnešním trhu je nejrozšířenější operační systém OS Symbian. Používá ho mnoho známých značek jako je Siemens, Nokia, Samsung, Panasonic, Sony Ericsson, Motorola a řada jiných.

I samotná firma Microsoft vyvinula svůj vlastní operační systém s názvem MS Windows Mobile 2002/3. Jeho výhodou je v plně kompatibilním operačním systémem se systémy na osobních počítačích. V těchto typech mobilních telefonů je jistá možnost proniknutí škodlivého programu. Obsahují nepřepisovatelnou pamět pro programy, které jsou potřebné pro spuštění zařízení, a přepisovatelnou pamět pro ostatní programy, které se mohou měnit nebo mazat. Mají funkci AutoRun i spustitelné programy s příponou SIS. A pro šíření programů používají infraport, Bluetooth nebo GPRS. Tyto operační systémy mají stejné vlastnosti jako u osobních počítačů. Viry mohou infikovat mobilní telefony a mohou se v nich šířit.

První virus pro mobilní telefony byl typu červ a pracoval pod operačním systémem Symbian. Šířil se pomocí Bluetooth. Tento červ neměl likvidovat software mobilních telefonů. Jeho smyslem bylo šíření na ostatní telefony. Chtěl jen dokázat, že je toho schopný.

Jak se proti takovým virům bránit? Obrana je jednoduchá. Neinstalovat si nelegální software. Je velice pravděpodobné, že na internetu volně dostupné aplikace budou obsahovat škodlivé kódy. V budoucnu se jistě objeví další viry a mnohem chytřejší a zákeřnější. Nebude dlouho trvat a i mobilní telefony budou vlastnit antivirové programy.

11.2 Viry v PDA

PDA neboli Personál Digital Asistent, v překladu tedy osobní digitální asistent. Tato anglická zkratka označuje souhrnně všechny kapesní počítače bez rozdílu platforem.

I tyto kapesní počítače mohou být napadeny virem. Používají několik druhů operačních systémů. První je platforma Pocket PC s operačním systémem Microsoft Pocket PC. Další jsou například operační systém Palm OS nebo Windows CE.

PDA nejsou jen obyčejným elektronickým diářem pro plánování schůzek. Ale používají i kancelářské aplikace MS Word nebo Excel. Je možné převádět soubory, které se v těchto aplikacích vytvoří z PDA do PC nebo obráceně. Je možno hrát hry nebo pouštět multimediální soubory. PDA mají všechny předpoklady pro vznik a šíření virů.

V létě roku 2004 se objevil první vir pro tyto kapesní počítače. Dostal jméno WinCE.Dust.1520. Vytvořila ho skupina lidí, která si říká A29. Tento virus napadá spustitelné soubory a šíří se pomocí klasické výměně napadených souborů. Při spuštění škodlivého kódu, se program zeptá, jestli může infikovat další soubory. WinCE4.Dust by Ratter/29A Dear User, am I allowed to spread? Pokud dostane kladnou odpověď, pokusí se nakazit všechny EXE soubory nacházející se ve stejné složce. Tento vir chce spíš jen dokázat, že je možné PDA infikovat.

Dalším virem byl Backdoor.Brador.A. Jde o trojského koně. Po spuštění škodlivého kódu se vir zkopíruje do adresáře Windows/StartUp/Suchost.exe a tém si zajistí opětovné spuštění po nabíhání systému i po restartu. Jeho úkolem je poslat svému pánovi e-mailem IP adresu napadeného PDA. Opakuje to do té doby, dokud není úspěšný. Otevírá příslušný port a čeká na instrukce útočníka. Tento trojský kůň už je opravdu škodlivý. Pokud bude vir úspěšný, tak má útočník toto PDA zcela ve svých rukou.

Řada firem zabývající se antivirovou ochranou, se snaží nabídnout program pro zabezpečení kapesních počítačů. Patří mezi ně firma Alwil (avast!4 PDA Edition), Symantec (Symantec Antiviru for Handheld) nebo AirScanner Mobile Antiviru Pro, který je pro domácí použití zdarma.

12 Závěr

Počítačová infiltrace je v dnešní době tak rozšířená, že znalost prevence a ochrany je nutností pro všechny. Viry se neustále vyvíjí a stupňují svoji agresivitu. Dříve to byly viry vytvořené pro OS DOS, dnes jsou to WIN32 viry a v blízké budoucnosti se masivně budou zaměřovat i na mobilní kapesní počítače nebo telefony. Každé zařízení, které vlastní operační paměť, umí komunikovat s okolím, má přepisovatelnou paměť, je potenciálním terčem útoku. Znalost malwaru není jednorázovou záležitostí. Je potřeba neustále sledovat jejich vývoj.

Nejrozšířenější jsou infiltrace, které využívají metod sociálního inženýrství. Patří k nim lákavé e-maily nebo žádosti o vyplnění dotazníku. Účelem je zaujmout jedince, aby daný mail otevřeli nebo dotazník vyplnili.

Jak se vyvíjejí viry, tak i jejich likvidátoři procházejí jistou počítačovou evolucí. Antivirové společnosti se snaží co možná nejvíce zpřístupnit jejich ochranu. Ať už trial verzemi nebo kompletními programy zdarma, které jsou ovšem použitelné jen pro domácí použití.

Tato práce by měla pomoct všem, kteří chtějí rozšířit svoje znalosti v oblasti počítačových virů.

13 Seznam použité literatury

[1] JALŮVKA, Josef. *Moderní počítačové viry: Podstata, prevence, ochrana*. 2. aktualizované vyd. Praha: Computer Press, 2000. 224 s. ISBN 80-7226-402-8.

[2] MRNUŠTÍK, Jiří. *Viry 98: Včetně makrovirů a antivirové ochraně sítí*. Praha: Grada Publishing, 1998. 96 s. ISBN 80-7169-683-8.

[3] BUREŠ, Pavel. Svět PDA. [online]. 2001 [cit. 2006-05-12]. Dostupné z <http://www.svetpda.cz/svetpda/svetpda.nsf/s?searchview&start=1&count=40>.

[4] HÁK, Igor. Kniha o virech. [online]. 2005 [cit. 2006-03-11]. Dostupné z <http://www.viry.cz/go.php?p=viry&t=clanek&id=23>.

[5] KLAŠKA, Luboš. Moderní antivirová ochrana v kostce. *Tutoriál* [online]. 2002. [cit. 2006-05-12]. Dostupné z <http://www.svetsiti.cz/view_list.asp?rubrika=Tutorialy&temaID=188>.

[6] DŽUBÁK, Josef. Databáze hoaxů. *Database* [online]. 2006. [cit. 2006-05-15]. Dostupné z <http://www.hoax.cz/cze/index.php?action=hoax_database>.

[7] Eset spol. s r.o.. Virový radar on-line. [cit. 2006-05-15]. Dostupné z <http://www.virovyradar.cz/index_csy.html>.

[8] BRBLA. Viry a hackeři. *Above* [online]. 2006. [cit. 2006-05-15]. Dostupné z <http://www.abowe.brbla.net/1-kapitola-uzivatelske-minimum/bezpecnost-zaklady/viry-a-hackeri.php>.

[9] PC WORLD Security. září 2004. Praha: IDG Czech. Vychází čtvrtletně. ISSN 1214-794X.

[10] PC WORLD Security. prosinec 2004. Praha: IDG Czech. Vychází čtvrtletně. ISSN 1214-794X.

[11] PC WORLD Security. červen 2005. Praha: IDG Czech. Vychází čtvrtletně. ISSN 1214-794X.