

Obsah

1. ÚVOD	13
2. ŠKODLIVÝ SOFTWARE.....	14
2.1 KLASIFIKACE ŠKODLIVÉHO SOFTWARE.....	14
2.1.1 Klasifikace podle způsobu šíření.....	14
2.1.2 Klasifikace podle typu škodlivé činnosti.....	15
3. ČERVY.....	16
4. TROJSKÉ KONĚ	18
4.1 TYPY TROJSKÝCH KOŇŮ	18
4.1.1 Password-stealing trojani (PWS).....	19
4.1.2 Destruktivní trojské koně.....	19
4.1.3 Trojský kuň typu dropper	19
4.1.4 Zadní vrátka	19
5. DALŠÍ TYPY MALWARE A ŠKODLIVÝCH AKTIVIT	22
5.1 HOAX	22
5.2 DIALER.....	23
5.3 SPAM.....	24
5.4 ADWARE.....	25
5.5 SPYWARE	25
5.6 ZNEUŽITÍ INTERNETOVÉHO PROHLÍZEČE.....	25
5.7 HLADOVÉ PROGRAMY	26
6. POČÍTAČOVÉ VIRY.....	27
6.1 DEFINICE A ZÁKLADNÍ VLASTNOSTI VIRŮ	27
6.2 HISTORIE POČÍTAČOVÝCH VIRŮ A ČERVŮ	29
6.3 ŠKODY ZPŮSOBOVANÉ VIRY	32
6.4 KLASIFIKACE POČÍTAČOVÝCH VIRŮ.....	34
6.4.1 Klasifikace podle rychlosti šíření.....	34
6.4.2 Klasifikace podle umístění v paměti.....	34
6.5 VIRY PRO MS DOS	34
6.5.1 Předpoklady operačního systému MS - DOS pro šíření a destruktivní činnost virů.....	35
6.5.2 Boot viry.....	36
6.5.3 Souborové viry	38
6.5.3.1 Metody infekce COM a EXE souborů.....	41
6.5.3.1.1 Parazitické metody infekce.....	42

6.5.3.2	Typické aktivity souborových virů	44
6.5.3.2.1	Viry přímé akce – prepisující	44
6.5.3.2.2	Paměťová rezidentnost a nerezidentnost	45
6.6	VIRY PRO OPERAČNÍ SYSTÉMY WIN32.....	49
6.6.1	<i>Struktura systému a souborů – vybrané aspekty</i>	50
6.6.1.1	Portable Executable.....	50
6.6.1.2	PE hlavička.....	50
6.6.1.3	Section Table.....	51
6.6.1.4	Import Table.....	52
6.6.1.5	Export Table.....	53
6.6.1.6	Zjišťování vstupních adres funkcí API.....	53
6.6.2	<i>Metody infekce</i>	55
6.6.2.1	Metoda prepisování.....	55
6.6.2.2	Parazitická metoda	55
6.6.2.2.1	Přidání nové sekce	55
6.6.2.2.2	Připojení ke stávající sekci	55
6.6.2.2.3	Infekce hlavičky	56
6.6.2.2.4	Cavity „mezerová“ infekce.....	56
6.6.2.3	Infekce DLL, speciálně KERNEL32.DLL	57
6.6.2.4	VMM & VxD	57
6.6.2.5	Speciální případy.....	58
6.6.3	<i>Techniky Win32 virů</i>	59
6.6.3.1	EPO	59
6.6.3.2	Multithreading.....	59
6.6.3.3	Multiprocesing a IPC	60
6.6.3.4	Stream companion.....	60
6.6.3.5	SFP disabling	61
6.7	MAKROVIRY.....	61
6.7.1	<i>Historie</i>	62
6.7.2	<i>Šíření a fungování makrovirů</i>	63
6.7.3	<i>Makroviry pro MS Word</i>	65
6.7.3.1	Dokumenty a šablony.....	66
6.7.3.2	Možnosti aktivace makrovirů.....	66
6.7.3.2.1	Automakra	66
6.7.3.2.2	Změny v menu a předefinování kláves.....	67
6.7.4	<i>Další techniky makrovirů</i>	67
6.7.4.1	Šifrovaná makra	67
6.7.4.2	Skrývání	67
6.7.4.3	Kombinace makroviru s klasickým virem	68
6.7.4.4	Multipartitní makroviry.....	69

6.7.4.5	Manipulační činnost.....	69
6.7.5	<i>Vlivy na šíření makrovirů.....</i>	70
6.7.5.1	Setkání více makrovirů	70
6.7.5.2	Vlastní degenerace	70
6.7.5.3	Chyby v produktu.....	70
6.7.5.4	Rozpad makroviru	71
6.7.5.5	Rozdílné verze aplikací.....	71
6.7.5.6	Konverze	72
6.7.5.7	Opatření proti makrovirům v MS Word	72
6.8	SKRIPTOVÉ VIRY.....	74
6.9	VIRY ŠÍŘÍCÍ SE ELEKTRONICKOU POŠTOU.....	76
6.9.1	<i>Poštovní viry v binárních souborech</i>	76
6.9.1.1	Získávání e-mailových adres pro napadení.....	77
6.9.1.2	Proces rozesílání / replikace.....	77
6.9.2	<i>Poštovní skriptové viry a makroviry</i>	79
6.9.3	<i>Techniky virů šířících se elektronickou poštou.....</i>	80
6.9.3.1	Maskovací techniky	80
6.9.3.1.1	Dvojitá přípona.....	80
6.9.3.1.2	„Bílé“ znaky	80
6.9.3.2	Využívání bezpečnostních chyb.....	80
6.9.3.3	Aktualizace viru prostřednictvím Internetu	81
6.9.3.4	Vypouštění dalších programů	83
6.9.3.5	Likvidace antivirových programů.....	83
6.9.3.6	Falšování skutečného odesílatele	84
6.9.4	<i>Alternativní cesty šíření.....</i>	85
6.9.4.1	Šíření po síťově sdílených discích	85
6.9.4.2	Šíření po IRC kanálech, p2p klientech	85
6.9.5	<i>Ukončení vlastní činnosti.....</i>	86
6.10	SPECIÁLNÍ SKUPINY VIRŮ	86
6.10.1	<i>Multiplatformní.....</i>	86
6.10.2	<i>Multipartitní.....</i>	87
6.10.3	<i>HLL viry</i>	87
6.10.4	<i>Kryptovirologie</i>	88
6.11	OBECNÉ ČÁSTI VIRŮ	89
6.11.1	<i>Reprodukční část.....</i>	89
6.11.2	<i>Analytická část</i>	90
6.11.3	<i>Maskovací část.....</i>	90
6.11.4	<i>Vlastní identifikace a příznak napadení.....</i>	90
6.11.5	<i>Vyhledání obětí.....</i>	91
6.11.6	<i>Manipulační část.....</i>	91

6.11.7	<i>Aktivační podmínky</i>	92
6.11.8	<i>Ošetření chyb</i>	92
6.12	VYBRANÉ TECHNIKY VIRŮ	92
6.12.1	<i>Stealth</i>	92
6.12.2	<i>Kódování a polymorfismus</i>	94
6.12.2.1	Souborové viry	94
6.12.2.2	Makroviry	96
6.12.2.3	Metamorfismus	97
6.12.3	<i>Vybrané techniky obrany virů proti AV programům</i>	101
6.12.3.1	Obrana proti krokování kódu	101
6.12.3.2	Tunelování	101
6.12.3.3	Retroviry	102
6.12.3.4	Viry vyhýbající se antivirovým programům a společností	102
6.12.3.5	Viry šířící se elektronickou poštou a vyhýbající se AV společností	103
6.12.4	<i>Závislost operačního systému na infiltraci</i>	103
6.12.5	<i>Generátory virů</i>	103
6.12.6	<i>Viry specifických aplikací</i>	105
6.13	VIROVÁ SCÉNA	106
6.13.1	<i>Osobnosti a skupiny</i>	106
6.13.2	<i>Aktivity tvůrců virů</i>	107
7.	ANTIVIROVÁ OCHRANA	108
7.1	OMYLY A MÝTY	108
7.2	ANTIVIROVÉ PROGRAMY	111
7.2.1	<i>Funkcionalita antivirového programu</i>	111
7.2.2	<i>Dělení antivirových programů</i>	113
7.2.2.1	Jednoúčelové antivirové programy	113
7.2.2.2	On-demand skenery	113
7.2.2.3	Antivirové systémy	114
7.3	ANTIVIROVÁ OCHRANA POČÍTAČOVÝCH SÍTÍ	114
7.3.1	<i>Antivirová ochrana stanic</i>	115
7.3.1.1	Aktualizace (update) antivirového systému	118
7.3.1.2	Virová databáze	122
7.3.1.3	Antivirové skenery	123
7.3.1.4	Principy vyhledávání virů a jejich omezení	125
7.3.1.4.1	Heuristická analýza	126
7.3.1.4.2	Falešné poplachy	128
7.3.1.4.3	Kontrola integrity	130

7.3.1.4.4	Monitorovací programy	132
7.3.1.4.5	Další části antivirových programů	133
7.3.1.5	Osobní firewally	134
7.3.2	<i>Antivirový hardware</i>	136
7.3.3	<i>Síťové schopnosti antivirových systémů</i>	136
7.3.3.1	Centrální správa	136
7.3.3.2	Zrcadlení aktualizací	137
7.3.3.3	Notifikace	137
7.3.3.4	Hromadné a centrální instalace	137
7.3.4	<i>Antivirová ochrana bran, groupware a serverů</i>	138
7.3.4.1	Zabezpečení vstupní brány.....	138
7.3.4.1.1	AV ochrana integrovaná s firewally.....	139
7.3.4.2	Ochrana poštovních bran	142
7.3.5	<i>Ochrana Groupware serverů</i>	143
7.3.5.1	Microsoft Exchange	144
7.3.5.2	Lotus Notes & Domino	145
7.3.6	<i>Pošta pod Linuxem</i>	146
7.3.7	<i>Ochrana souborových serverů</i>	147
7.3.7.1	Microsoft Windows Server	147
7.3.7.2	Novell NetWare	148
7.3.7.3	Samba server	148
7.4	IDENTIFIKACE INFILTRACE A NÁSLEDNÉ ČINNOSTI.....	149
7.4.1	<i>Pojmenování</i>	149
7.4.2	<i>Projekt VGrep</i>	151
7.4.3	<i>Činnosti po identifikaci</i>	152
7.4.3.1	Algoritmické léčení.....	153
7.4.3.2	Heuristické léčení.....	154
7.4.3.3	Další metody léčení.....	154
7.4.3.3.1	Očkování souborů.....	154
7.4.3.3.2	Kontrola Integrity	155
7.4.3.3.3	Sebeléčení.....	155
7.5	PŘÍSTUPY K ANTIVIROVÉ OCHRANĚ	155
7.5.1	<i>Vybrané zásady a možnosti prevence</i>	155
7.5.2	<i>Vybrané formy a techniky prevence</i>	156
7.5.2.1	Doporučený způsob instalace nového software.....	156
7.5.2.2	Inteligence	158
7.5.2.3	Informovanost a znalosti.....	158
7.5.2.4	Aktuální verze softwaru	161
7.5.2.5	Nastavení softwaru.....	162
7.5.2.5.1	Nastavení funkcí operačního systému.....	162

7.5.2.5.2	MS Internet Explorer	162
7.5.2.5.3	MS Outlook a MS Outlook Express	162
7.5.2.5.4	MS Office	162
7.5.2.5.5	Poštovní servery	163
7.5.2.5.6	Firewally	163
7.6	SLUŽBY	163
7.6.1	<i>PC Viruses In-the-Wild</i>	163
7.6.2	<i>MessageLabs</i>	165
7.6.3	<i>EICAR</i>	168
7.6.4	<i>CERT</i>	168
7.7	SROVNÁVACÍ TESTY ANTIVIROVÝCH SKENERŮ	169
7.7.1	<i>Virus Bulletin</i>	171
7.7.2	<i>GEGA IT-Solutions</i>	172
7.7.3	<i>Universita Hamburg</i>	172
7.8	ANTIVIROVÉ FIRMY	172
7.8.1	<i>Činnost antivirové firmy</i>	172
7.8.2	<i>Vybrané antivirové firmy</i>	173
7.8.2.1	Alwil Software	173
7.8.2.2	Grisoft	173
7.8.2.3	ESET	174
7.8.2.4	McAfee	174
7.8.2.5	Symantec	174
7.8.2.6	Kaspersky Lab	175
7.8.2.7	RAV Anti-Virus	175
7.9	PRAKTICKÉ RADY	175
7.9.1	<i>NTFS</i>	176
7.9.2	<i>Obnova systému</i>	177
7.9.3	<i>Internet</i>	178
7.9.3.1	Služby Internetu a maligní software	179
7.9.3.2	Bezpečnost moderních jazyků pro WWW	179
7.9.3.2.1	Java aplety	179
7.9.3.2.2	ActiveX objekty	180
7.9.3.2.3	Java Beans	181
7.9.3.2.4	Skripty	181
7.9.3.2.5	ActiveX objekty a skript	182
7.9.3.2.6	Cookies	182
7.9.3.2.7	CGI, ASP, PHP, servlety a jiný skript na straně serveru	183
7.9.3.3	Prevence na Internetu	183
7.10	SOUČASNÉ A BUDOUCÍ PROBLÉMY AV OCHRANY	183

8.	ŠKODLIVÝ SOFTWARE – ZÁVĚRY	186
8.1	TRENDY.....	186
8.2	OBRANA PROTI ŠKODLIVÉMU SOFTWARE.....	187
8.3	ZÁVĚRY.....	187
9.	OTÁZKY A ÚKOLY	188
10.	REJSTŘÍK	190
11.	LITERATURA A DALŠÍ ZDROJE INFORMACÍ	193
12.	PŘÍLOHY	196

Seznam obrázků

Obr. 1	Graf ukazující extrémní vytížení LAN 100 Mbit/s sítě UDP pakety....	17
Obr. 2	Ukázka komunikace prostřednictvím aplikace mIRC32	21
Obr. 3	Hoax – zdánlivá nabídka mobilních telefonů zdarma. Zdroj: www.hoax.cz	23
Obr. 4	Varianty umístění viru vůči souboru	28
Obr. 5	Schéma převzetí kontroly COM infektorem. Instrukce skoku JMP na samotném začátku předá řízení viru.....	42
Obr. 6	Schéma převzetí kontroly EXE infektorem. Hodnota entry pointu (CS:IP) v hlavičce ukazuje na kód viru	43
Obr. 7	Metoda infekce, kdy se virus se nachází před původním programem.....	43
Obr. 8	Připojení viru na konec souboru	44
Obr. 9	Vložení viru dovnitř souboru	44
Obr. 10	Přehled atributů hlavičky PE souboru.	51
Obr. 11	Příklad seznamu jednotlivých sekcí a informací.	52
Obr. 12	Příklad import table - vlevo příslušný DLL, vpravo konkrétní funkce.....	53
Obr. 13	Princip fungování cross-infektorů, kdy je exportován zdrojový kód makroviru do speciálního souboru (v uvedeném případě SOURCE.TXT) a následně pak importován do dalších aplikací balíku Microsoft Office. Převzato ze [17].....	65
Obr. 14	Ilustrační schéma přehození podprogramů [27]	99
Obr. 15	Tři různé generace viru Win95/Zperm [27].....	100
Obr. 16	Generátor W97MVCK pro tvorbu makrovirů.	104
Obr. 17	V generátoru VBSWG vznikl i veleúspěšný virus VBS/SST.A - Anna Kurnikova.....	105

Obr. 18	Portál VX Heavens pro podporu vytváření počítačových virů....	107
Obr. 19	Databáze údajů o virech v AV programu Avast!.....	117
Obr. 20	Dynamika šíření viru Win32/Fizzer. Převzato z [39]......	120
Obr. 21	Dynamika šíření viru Win32/BugBear.B, nejrychlejší nástup viru v celé dosavadní historii. Převzato z [39]......	120
Obr. 22	Dynamika šíření viru Win32/Sobig.B. Převzato z [39]......	121
Obr. 23	Nastavení akcí firewallu Kerio ve vztahu k obsahu WWW stránek	134
Obr. 24	Nastavení akcí firewallu Kerio ve vztahu k útokům s různou prioritou	135
Obr. 25	Nastavení akcí firewallu Kerio pro instalované aplikace	135
Obr. 26	Záznamy firewallu Kerio o různých aspektech bezpečnosti systému.....	136
Obr. 27	CVP protokol, možná varianta.....	139
Obr. 28	Příklad řešení, kdy je každému monitorovanému protokolu přiřazen server	140
Obr. 29	Proxy řešení antivirové ochrany.	142
Obr. 30	Schéma zapojení antiviru pro SMTP Gateway.....	143
Obr. 31	Rozhraní VSAPI 1.0 [19].....	144
Obr. 32	Rozhraní VSAPI 2.0 [19].....	145
Obr. 33	Rozhraní ESEAPI [19].....	145
Obr. 34	Schéma činnosti Lotus Notes & Domino [19].....	146
Obr. 35	Schéma činnosti poštovního serveru pod Linuxem. MDA (Mail Delivery Agent) uloží e-mail do konkrétní schránky.....	147
Obr. 36	Ukázka podezřelého předmětu i textu zprávy – v příloze byl zaslán virus, zachycený AV programem.....	159
Obr. 37	První zasláná zpráva se zavirovanou přílohou.....	159
Obr. 38	Druhá zasláná zpráva se zavirovanou přílohou	160
Obr. 39	Část úvodní strany www.viry.cz.....	160
Obr. 40	Úvodní strana informací o hoaxech: www.hoax.cz.....	161
Obr. 41	Ukázka deseti nejvíce se šířících virů elektronickou poštou za posledních 24 hodin (snímek z 26.4.2004 11:01). Převzato z [39].	165
Obr. 42	Informace o viru Win32/NetSky-D.-mm, (snímek z 26.4.2004 11:01). Převzato z [39].	166
Obr. 41	Poměr infikovaných a čistých e-mailů v globálním měřítku v roce 2003 (nahore) a 2003/2004 (dole). Prudký pokles v roce 2003 způsobil virus Win32/Sobig.F, kdy byl zaznamenán i poměr 1:15 (každý patnáctý e-mail infikován virem Win32/Sobig.F). Převzato z [39].	167

Obr. 42 Avast! BART CD, hlavní menu.....	177
Obr. 43 Nastavení úrovně zabezpečení v prohlížeči MS Internet Explorer ve vztahu k objektům ActiveX	181

Seznam tabulek

Tab. 1 Přehled používaných zkratk a zkrácených označení.....	13
Tab. 2 Historie počítačových virů (a červů) v datech	30
Tab. 3 Změny, vyvolané v systémových službách aktivitami virů.....	49
Tab. 4 Automakra v MS Word.....	66
Tab. 5 Vybraná označení pro typ infiltrace.....	150
Tab. 6 Další atributy pro označení virů.....	151
Tab. 7 Vybrané názvy červa Opaserv.A	152
Tab. 8 Přehled funkcí VBA, které umožňují přístup na disk.....	210

Seznam příkladů

Příklad 1 Červ SQLSlammer.....	17
Příklad 2 Zadní vrátka s využitím IRC - virus Win32/Anarxy	20
Příklad 3 Nejčastější hoax – modelová struktura varování před počítačovým virem.....	22
Příklad 4 Clusterový virus DIR-II.....	40
Příklad 5 Ukázka propojení makroviru a klasického viru [14].....	68
Příklad 6 Ukázka části makroviru Nuclear	69
Příklad 7 Skript, který ve spojení s MSIE způsobí vyjetí dvířek všech CD/DVD	75
Příklad 8 Bezpečnostní díra Typelib.scriptlet/Eyedog.....	81
Příklad 9 Bezpečnostní díra s nekorektní hlavičkou MIME, což může způsobit vykonání přílohy e-mailu	81
Příklad 10 Vybrané odvetné viry pro MS DOS	84
Příklad 11 Ukázky kryptovirů.....	88
Příklad 12 Rutina pro zamaskování MS DOS viru v MBR pevného disku nebo boot sektoru diskety	93
Příklad 13 Jednoduchá smyčka pro dosažení polymorfie.....	95
Příklad 14 Zápis stejné instrukce různým způsobem.....	96
Příklad 15 Ukázka realizace polymorfismu makrovirů s využitím prohazování řádků kódu	96
Příklad 16 Ukázka realizace polymorfismu makrovirů s využitím prokládání kódu poznámkami (rem)	97
Příklad 17 Ukázka realizace polymorfismu makrovirů s využitím proměnlivosti názvů proměnných, procedur a funkcí.....	97

Příklad 18 Modifikace kódu výměnou používaných registrů	98
Příklad 19 Metamorfie – virus Win32/Evol.....	99
Příklad 20 MS DOS viry, vyhýbající se antivirovým programům	102
Příklad 21 W32/BugBear-B	121
Příklad 22 Nežádoucí ovlivnění ActiveX objektu skriptem	182

Seznam příloh

Příloha 1 Vybrané termíny	196
Příloha 2 Vybrané důležité odkazy	209
Příloha 3 Vybrané příkazy jazyka Visual Basic pro přístup k disku	210