

Obsah

O autorovi	18
Předmluva	19
Poděkování	21

Část I – Strategie útočníka

Kapitola 1 Úvod do her přírody 25

1.1 Rané modely seberekopujících struktur	26
1.1.1 John von Neumann: Teorie automatů schopných vlastní reprodukce	27
1.1.2 Fredkin: Reprodukční struktury	28
1.1.3 Conway: Hra života	29
1.1.4 Války o jádro: bojující programy	33
1.2 Geneze počítačových virů	37
1.3 Automaticky se replikující kód: teorie a definice počítačových virů	38
Odkazy	40

Kapitola 2 Fascinující analýza škodlivého kódu 41

2.1 Obvyklé vzorce výzkumu v oblasti virů	43
2.2 Vývoj antivirové obrany	44
2.3 Terminologie škodlivých programů	45
2.3.1 Viry	45
2.3.2 Počítačovní červi	45
2.3.3 Logické bomby	46
2.3.4 Trojští koně	47
2.3.5 Zárodky	48
2.3.6 Exploity	48
2.3.7 Stahovače	49
2.3.8 Dialery	49
2.3.9 Droppers	49
2.3.10 Injektor	49
2.3.11 Auto-Rootery	50
2.3.12 Kity (generátory virů)	50
2.3.13 Programy pro spam	50
2.3.14 Floodery	51

2.3.15 Snímače stisku kláves	51
2.3.16 Rootkity	51
2.4 Další kategorie	51
2.4.1 Zábavné programy	51
2.4.2 Poplašné zprávy: řetězové dopisy	52
2.4.3 Další hmyz: adware a spyware	52
2.5 Schéma pojmenování počítačových škodlivých programů	53
2.5.1 <jméno_rodiny>	54
2.5.2 <typ_škodlivého_programu>://	54
2.5.3 <platforma>/	54
2.5.4 <jméno_skupiny>	55
2.5.5 <infekční_délka>	55
2.5.6 <varianta>	55
2.5.7 [<<převod >]	55
2.5.8 <modifikátory>	55
2.5.9 <specifikátor_lokace>	55
2.5.10 #<způsob_komprimace>	56
2.5.11 @m nebo @mm	56
2.5.12 !<výrobce_speciální_komentář >	56
2.6 Komentovaný seznam oficiálně rozpoznávaných platforem	56
Odkazy	60

Kapitola 3 Prostředí škodlivého kódu **61**

3.1 Závislost na počítačové architektuře	63
3.2 Závislost na procesoru	64
3.3 Závislost na operačním systému	65
3.4 Závislost na verzi operačního systému	66
3.5 Závislost na souborovém systému	66
3.5.1 Cluster viry	66
3.5.2 Viry pro NTFS Stream	68
3.5.3 Viry využívající kompresi NTFS	68
3.5.4 Infekce ISO obrazů	69
3.6 Závislost na formátu souboru	69
3.6.1 COM viry v prostředí DOSu	69
3.6.2 EXE viry v prostředí DOSu	69
3.6.3 NE (New Executable) viry pro 16bitová Windows a OS/2	69
3.6.4 LX viry na OS/2	70
3.6.5 Viry napadající soubory PE prostředí 32bitových Windows	70

11.11.5 Nezbytné změny v objektech	422
11.11.6 Možná řešení	422
11.12 Monitorování podezřelého chování	422
11.13 Sand-Boxing	424
11.14 Závěr	425
Odkazy	425

Kapitola 12 Skenování paměti a dezinfekce **429**

12.1 Úvod	431
12.2 Systém virtuální paměti ve Windows NT	432
12.3 Virtuální adresovací prostor	434
12.4 Skenování paměti v uživatelském režimu	438
12.4.1 Tajemství funkce NtQuerySystemInformation()	438
12.4.2 Obecné procesy a speciální systémová práva	439
12.4.3 Viry v subsystému Win32	440
12.4.4 Viry Win32 alokující privátní stránky	441
12.4.5 Viry nativních služeb Windows NT	443
12.4.6 Viry Win32, které používají proceduru skrytého okna	443
12.4.7 Viry Win32, které jsou součástí spustitelného obrazu	443
12.5 Skenování paměti a stránkování	446
12.5.1 Vyhodnocení procesů a skenování obrazů v souborech	448
12.6 Dezinfekce paměti	448
12.6.1 Ukončení procesu, který obsahuje kód viru	448
12.6.2 Detekce a ukončování threadů virů	448
12.6.3 Záplatování virového kódu v aktivních stránkách	451
12.6.4 Postup dezinfekce zavedených DLL a běžících aplikací	452
12.7 Skenování paměti v režimu jádra	453
12.7.1 Skenování uživatelského adresovacího prostoru procesů	453
12.7.2 Rozlišení vstupních bodů API služeb NT	453
12.7.3 Důležité funkce NT pro skenování paměti v režimu jádra	454
12.7.4 Kontext procesu	455
12.7.5 Skenování horních 2 GB adresovacího prostoru	455
12.7.6 Jak lze deaktivovat virus ve filtračním ovladači?	456
12.7.7 Paměť jádra, která je pouze pro čtení	458
12.7.8 Skenování paměti v režimu jádra na 64bitových platformách	458
12.8 Možné útoky proti skenování paměti	461
12.9 Shrnutí a budoucnost	462
Odkazy	463

Kapitola 13**Techniky blokování červů a ochrany před pronikáním na bázi hostitele 465**

13.1 Úvod	466
13.1.1 Blokování skriptů a SMTP červů	467
13.1.2 Blokování nových útoků – CodeRed a Slammer	470
13.2 Techniky blokování útoků využívající přetečení bufferu	470
13.2.1 Přezkoumání kódu	471
13.2.2 Řešení na úrovni kompilátoru	472
13.2.3 Řešení na úrovni operačního systému a rozšíření run-time	479
13.2.4 Rozšíření subsystému – Libsafe	480
13.2.5 Rozšíření režimu jádra	480
13.2.6 Doprovázení programů	482
13.3 Techniky blokování červů	482
13.3.1 Detekce injektovaného kódu	483
13.3.2 Blokování posílání: blokování kódu, který se sám rozesílá	487
13.3.3. Validace ovladačů výjimek	489
13.3.4 Techniky zmírňování útoků "return-to-LIBC"	493
13.3.5 Atributy stránky "GOT" a "IAT"	496
13.3.6 Velký počet spojení a chyby spojení	497
13.4 Možné budoucí útoky červů	498
13.4.1 Možné zvýšení počtu retro-červů	498
13.4.2 "Pomalí" červi pod radarem	498
13.4.3 Polymorfní a metamorfní červi	498
13.4.4 Škody velkého rozsahu	499
13.4.5 Automatizovaná detekce exploitů – učení se z prostředí	499
13.5 Závěr	500
Odkazy	501

Kapitola 14 Strategie obrany na síťové úrovni**503**

14.1 Úvod	504
14.2 Použití přístupových seznamů routerů	505
14.3 Ochrana firewallly	507
14.4 Systémy pro detekci průniku do sítě	509
14.5 Systémy honeypotů	511

14.6	Protiútoky	513
14.7	Systémy včasného varování	514
14.8	Vzory chování červů v síti	515
14.8.1	Zachycení červa Blaster	515
14.8.2	Zachycení červa Linux/Slapper	516
14.8.3	Zachycení červa W32/Sasser.D	518
14.8.4	Zachycení požadavku ping červa W32/Welchia	520
14.8.5	Detekce červa W32/Slammer a souvisejících možností exploitace	521
14.9	Závěr	523
	Odkazy	523

Kapitola 15 Techniky analýzy škodlivého kódu **525**

15.1	Vaše osobní laboratoř pro analýzu virů	526
15.1.1	Jak získat potřebný software?	528
15.2	Informace, informace, informace	528
15.2.1	Průvodci architekturami	528
15.2.2	Báze znalostí	528
15.3	Dedikovaná analýza virů pomocí VMWARE	529
15.4	Proces analýzy počítačového viru	531
15.4.1	Příprava	531
15.4.2	Dekomprese	536
15.4.3	Disasemblování a dešifrování	537
15.4.4	Techniky dynamické analýzy	543
15.5	Udržování sbírky škodlivého kódu	564
15.6	Automatizovaná analýza: Digital Immune System	565
	Odkazy	567

Kapitola 16 Shrnutí **569**

	Doporučené čtení	570
	Informace o bezpečnosti a včasných varováních	570
	Bezpečnostní aktualizace	571
	Statistiky vypuknutí počítačových červů	571
	Dokumenty o výzkumu počítačových virů	571
	Kontaktní informace na prodejce antivirů	572
	Testeři antivirů a příbuzné stránky	573

Rejstřík



3.6.6	Viry infikující soubory ELF v prostředí systému UNIX	73
3.6.7	Viry napadající ovladače zařízení	73
3.6.8	Viry infikující objekty a LIB	74
3.7	Závislost na překladači	75
3.7.1	Makro viry v produktech firmy Microsoft	75
3.7.2	REXX viry na systémech IBM	84
3.7.3	DCL viry na DEC/VMS	85
3.7.4	Shell skripty na UNIXu (csh, ksh a bash)	86
3.7.5	VBScript viry na systémech Windows	87
3.7.6	Dávkové viry	87
3.7.7	Viry ve skriptech programů mIRC, PIRCH	88
3.7.8	SuperLogo Viry	88
3.7.9	JScriptové viry	90
3.7.10	Perlovské viry	91
3.7.11	Červi WebTV napsaní v JellyScriptu a vložení do HTML e-mailů	91
3.7.12	Viry pro Python	91
3.7.13	VIM viry	92
3.7.14	EMACS viry	92
3.7.15	TCL viry	92
3.7.16	PHP viry	92
3.7.17	MapInfo viry	93
3.7.18	ABAP viry na SAPu	93
3.7.19	Viry pro soubory nápovědy Windows – když zmáčknete F1...	93
3.7.20	JScriptové hrozby v souborech Adobe PDF	94
3.7.21	Závislost na AppleScript	94
3.7.22	Závislost na ANSI	94
3.7.23	Hrozby v ActionScriptu	95
3.7.24	Hrozby skriptů HyperTalk	95
3.7.25	Skriptovací viry pro AutoLisp	96
3.7.26	Závislost na registru	97
3.7.27	Závislost na PIF a LNK	97
3.7.28	Makro viry programu Lotus Word Pro	98
3.7.29	Viry dokumentů AmiPro	98
3.7.30	Viry pro Corel Script	98
3.7.31	Závislost na makrech produktů Lotus 1-2-3	99
3.7.32	Závislost na instalačních skriptech systému Windows	99
3.7.33	Závislost na AUTORUN.INF a souborech INI systému Windows	99
3.7.34	Závislost na HTML (Hypertext Markup Language)	100

3.8 Závislost na zranitelnosti	100
3.9 Závislost na času a datu	101
3.10 JIT závislost – viry Microsoft .NET	101
3.11 Závislost na archivovaných formátech	102
3.12 Závislost na příponě souboru	103
3.13 Závislost na síťovém protokolu	104
3.14 Závislost na zdrojových kódech	104
3.14.1 Zdrojové kódy trojských koní	105
3.15 Závislosti na zdrojích v platformách Mac a Palm	106
3.16 Závislost na velikosti hostitele	107
3.17 Závislost na debuggerech	107
3.17.1 Zamýšlené hrozby spoléhající na debugger	108
3.18 Závislost na kompilátoru a linkeru	109
3.19 Závislost na vrstvě překladači zařízeních	109
3.20 Závislost na vkládaných objektech	111
3.21 Závislost na vlastním prostředí	112
3.22 Multipartitní viry	114
3.23 Závěr	115
Odkazy	115

Kapitola 4 Klasifikace metod infekce **119**

4.1 Boot viry	120
4.1.1 Techniky infekce Master Boot Recordu (MBR)	121
4.1.2 Techniky infekce DOS BOOT Recordu (DBR)	123
4.1.3 Boot viry, které dovedou pracovat s Windows 95	125
4.1.4 Možné útoky boot virů v síťovém prostředí	125
4.2 Techniky infekce souborů	126
4.2.1 Přepisující viry	126
4.2.2 Náhodně přepisující viry	128
4.2.3 Připojující viry	128
4.2.4 Viry připojující se na začátek souboru	129
4.2.5 Klasické parazitické viry	131
4.2.6 Dutinové viry	132
4.2.7 Dělené dutinové viry	133
4.2.8 Komprimující viry	134
4.2.9 Infekce typu Amoeba	134
4.2.10 Technika přidání decryptoru	135
4.2.11 Technika vložení decryptoru a virového těla	136

4.2.12	Technika matoucího odskoku	137
4.2.13	Technika utajení vstupního bodu (EPO)	139
4.2.14	Možné budoucí techniky infekce: stavitelé kódu	148
4.3	Důkladný pohled na Win32 viry	149
4.3.1	Win32 API a platformy, které je podporují	150
4.3.2	Techniky infekce na 32bitových Windows	152
4.3.3	Win32 a Win64 viry: navržené pro Microsoft Windows?	168
4.4	Závěr	170
	Odkazy	170

Kapitola 5 Klasifikace metod infekce paměti **173**

5.1	Viry přímé akce	174
5.2	Paměťově rezidentní viry	174
5.2.1	Obsluha a zavěšování na přerušení	175
5.2.2	Závěsné rutiny na INT 13h (boot viry)	179
5.2.3	Závěsné rutiny na INT 21h (souborové viry)	180
5.2.4	Obvyklé techniky instalace do paměti pod DOSem	183
5.2.5	Stealth viry	185
5.2.6	Infekce diskové cache a systémového bufferu	194
5.3	Dočasné paměťové rezidentní viry	195
5.4	Swapovací viry	196
5.5	Viry v procesech (v uživatelském režimu)	196
5.6	Viry v režimu jádra (Windows 9x/Me)	197
5.7	Viry v režimu jádra (Windows NT/2000/XP)	197
5.8	Viry vkládající se do paměti přes síť	199
	Odkazy	200

Kapitola 6 Základní obranné strategie virů **201**

6.1	Tunelující viry	202
6.1.1	Skenování v paměti původní obsluhy	202
6.1.2	Trasování s pomocí ladících rozhraní	202
6.1.3	Tunelování na bázi emulace kódu	203
6.1.4	Přístup k disku přes I/O porty	203
6.1.5	Použití nedokumentovaných funkcí	203
6.2	Obrněné viry	203
6.2.1	Obrana proti disassemblování	204
6.2.2	Zakódovaná data	204

6.2.3 Matení kódu pro znesnadnění analýzy	205
6.2.4 Matení kódu založené na míchání operačních kódů	206
6.2.5 Používání kontrolních součtů	207
6.2.6 Komprimovaný matoucí kód	207
6.2.7 Obrana proti ladění	208
6.2.8 Obrana proti heuristické analýze	215
6.2.9 Obrana proti emulaci	222
6.2.10 Viry vyhýbající se návnadám	225
6.3 Agresivní retroviry	226
Odkazy	228

Kapitola 7

Pokročilé techniky vývoje kódu a generátory počítačových virů **229**

7.1 Úvod	230
7.2 Vývoj virového kódu	230
7.3 Zakódované viry	231
7.4 Oligomorfní viry	235
7.5 Polymorfní viry	237
7.5.1 Virus 1260	237
7.5.2 Dark Avengerův mutovací engine (MtE)	238
7.5.3 32bitové polymorfní viry	240
7.6 Metamorfní viry	244
7.6.1 Co je metamorfní virus?	245
7.6.2 Jednoduché metamorfní viry	246
7.6.3 Složitější metamorfní viry a permutační techniky	247
7.6.4 Mutování dalších aplikací: definitivní generátor virů?	250
7.6.5 Pokročilé metamorfní viry: Zmist	251
7.6.6 {W32, Linux}/Simile: metamorfní engine napříč systémy	254
7.6.7 Temná budoucnost – metamorfní MSIL viry	258
7.7 Generátory počítačových virů	260
7.7.1 VCS (Virus Construction Set)	260
7.7.2 GenVir	260
7.7.3 VCL (Virus Creation Laboratory)	261
7.7.4 PS-MPC (Phalcon-Skism Mass-Produced Code Generator)	261
7.7.5 NGVCK (Next Generation Virus Creation Kit)	262
7.7.6 Další nástroje a mutační enginey	262
7.7.7 Jak testovat generátory počítačových virů?	263
Odkazy	264

Kapitola 8	Klasifikace podle payloadu	265
8.1	Bez payloadu	266
8.2	Náhodně destruktivní payload	267
8.3	Nedestruktivní payload	267
8.4	Příležitostně destruktivní payload	269
8.5	Velmi destruktivní payload	270
8.5.1	Víry přepisující data	270
8.5.2	Data Diddlers	271
8.5.3	Víry šifrující data: dobří, zlí a oškliví	272
8.5.4	Ničení hardware	273
8.6	Útoky DoS – odmítnutí služby	274
8.7	Získávání peněz pomocí virů	276
8.7.1	Phishing	276
8.7.2	Vlastnosti zadních vrátek	276
8.8	Závěr	278
	Odkazy	279
Kapitola 9	Strategie počítačových červů	281
9.1	Úvod	282
9.2	Generická struktura počítačových červů	283
9.2.1	Vyhledávač obětí	283
9.2.2	Modul pro šíření infekce	283
9.2.3	Vzdálené ovládání a rozhraní pro aktualizaci	283
9.2.4	Plánovač životního cyklu	284
9.2.5	Payload	285
9.2.6	Sledování počtu infikovaných systémů	286
9.3	Vyhledávač obětí	286
9.3.1	Skřízení e-mailových adres	286
9.3.2	Útoky založené na prohledávání sdílených prostředků	290
9.3.3	Skenování sítě a označení cíle	291
9.4	Šíření infekce	295
9.4.1	Útok na systémy kompromitované pomocí zadních vrátek	296
9.4.2	Útoky na peer-to-peer sítě	297
9.4.3	Útoky pomocí systémů pro okamžitý přenos zpráv	297
9.4.4	Útoky pomocí e-mailů a klamavých technik	298
9.4.5	Útoky pomocí přímého vkládání e-mailů do schránky	298
9.4.6	Útoky založené na SMTP Proxy	299

9.4.7 Útoky přes SMTP	299
9.4.8 Použití MX dotazů pro zrychlené šíření pomocí SMTP	301
9.4.9 Útoky pomocí NNTP (Network News Transfer Protocol)	302
9.5 Běžný kód červa a spouštěcí techniky	302
9.5.1 Útoky založené na spustitelném kódu	302
9.5.2 Odkazy na webové stránky nebo webové proxy	302
9.5.3 E-mail založený na HTML kódu	303
9.5.4 Útoky založené na vzdáleném přihlašování	304
9.5.5 Útoky injektáží kódu	304
9.5.6 Útoky založené na interpretech příkazů	305
9.6 Aktualizační strategie počítačových červů	307
9.6.1 Autentizované aktualizace z webu	308
9.6.2 Aktualizace založené na zadních vrátkách	312
9.7 Vzdálené ovládání pomocí signalizace	313
9.7.1 Kontrola nad Peer-to-Peer sítěmi	314
9.8 Úmyslné a náhodné interakce	315
9.8.1 Spolupráce	315
9.8.2 Soutěžení	317
9.8.3 Budoucnost – jednoduchý komunikační protokol pro červy?	318
9.9 Červi pro bezdrátová mobilní zařízení	319
Odkazy	320

Kapitola 10

Exploity, zranitelná místa, útoky založené na přetečení bufferu	323
10.1 Úvod	324
10.1.1 Definice smíšeného útoku	324
10.1.2 Hrozba	324
10.2 Pozadí	325
10.3 Typy zranitelností	326
10.3.1 Přetečení bufferu	326
10.3.2 První generace útoků	326
10.3.3 Útoky druhé generace	328
10.3.4 Útoky třetí generace	335
10.4 Současné a dřívější hrozby	348
10.4.1 Internetový červ Morris, 1988(přetečení bufferu ke spuštění kódu shellu)	348
10.4.2 Linux/ADM, 1998 (napodobenina červa Morris)	350
10.4.3 Vypuknutí epidemie červa CodeRed, 2001 (injektování kódu)	351
10.4.4 Červ Linux/Slapper, 2002 (příklad přetečení heapu)	353

10.4.5 Červ W32/Slammer, leden 2003 (miničerv)	358
10.4.6 Červ Blaster, srpen 2003 (útok pomocí shellkódu na Win32)	361
10.4.7 Obecné použití přetečení bufferu v počítačových virech	363
10.4.8 Popis W32/Badtrans.B@mm	363
10.4.9 Exploity v W32/Nimda.A@mm	364
10.4.10 Popis W32/Bolzano	364
10.4.11 Popis VBS/Bubbleboy	366
10.4.12 Popis W32/Blebla	366
10.5 Shrnutí	367
Odkazy	368

Část II – Strategie obránce

Kapitola 11 Techniky antivirové obrany

373

11.1 Skenery první generace	375
11.1.1 Skenování řetězců	376
11.1.2 Zástupné znaky	377
11.1.3 Neshody	378
11.1.4 Generická detekce	379
11.1.5 Hašování	379
11.1.6 Záložky	379
11.1.7 Skenování začátku a konce	380
11.1.8 Skenování vstupních a fixních bodů	381
11.1.9 Hyper-rychlý přístup k disku	381
11.2 Skenery druhé generace	382
11.2.1 Chytré skenování	382
11.2.2 Detekce struktury	382
11.2.3 Téměř přesná identifikace	382
11.2.4 Přesná identifikace	383
11.3 Algoritmické skenovací metody	385
11.3.1 Filtrování	386
11.3.2 Statická detekce decryptoru	388
11.3.3 Rentgenová metoda (X-raying)	389
11.4 Emulace kódu	393
11.4.1 Detekce zakódovaných a polymorfních virů s použitím emulace	397
11.4.2 Dynamická detekce decryptoru	400
11.5 Příklady detekce metamorfních virů	401

11.5.1 Geometrická detekce	402
11.5.2 Disassemblovací techniky	402
11.5.3 Použití emulátorů pro trasování	403
11.6 Heuristická analýza 32bitových virů pro Windows	406
11.6.1 Vykonávání kódu začíná v poslední sekci	407
11.6.2 Podezřelé příznaky sekce	407
11.6.3 Nesprávná virtuální velikost v PE hlavičce	407
11.6.4 Možné "díry" mezi sekcemi	407
11.6.5 Podezřelé přeměrování kódu	408
11.6.6 Podezřelé jméno kódové sekce	408
11.6.7 Možná infekce hlavičky	408
11.6.8 Podezřelé importhy z KERNEL32.DLL přes pořadová čísla	408
11.6.9 Tabulka importovaných adres je přešpaná	408
11.6.10 Vícenásobné PE hlavičky	408
11.6.11 Vícenásobné hlavičky Windows a podezřelé importhy z KERNEL32.DLL	408
11.6.12 Podezřelé relokace	409
11.6.13 Pevné ukazatele na systémové oblasti	409
11.6.14 Nekonzistence knihovny KERNEL32.DLL	409
11.6.15 Načítání sekce do adresního prostoru VMM	409
11.6.16 Nesprávná velikost kódu v hlavičce	410
11.6.17 Příklady kombinací podezřelých příznaků	410
11.7 Heuristická analýza používající neuronové sítě	411
11.8 Obyčejné a generické metody dezinfekce	412
11.8.1 Standardní dezinfekce	413
11.8.2 Generické decryptory	414
11.8.3 Jak generický dezinfektor funguje?	414
11.8.4 Jak si může být dezinfektor jistý, že je soubor infikován?	415
11.8.5 Kde je původní konec hostitelského souboru?	415
11.8.6 Kolik druhů virů můžeme takto odstranit?	415
11.8.7 Příklady heuristiky pro generické léčení	416
11.8.8 Příklady generické dezinfekce	417
11.9 Očkování	418
11.10 Systémy řízení přístupu	419
11.11 Kontrola integrity	420
11.11.1 Falešné poplachy	420
11.11.2 Prvotní čistý stav	421
11.11.3 Rychlost	421
11.11.4 Speciální objekty	421