

# Počítačové viry

## analýza útoku a obrana

**Peter Szor**



## **Art of Computer Virus Research and Defense by Peter Szor.**

Authorized translation from the English language edition, entitled ART OF COMPUTER VIRUS RESEARCH AND DEFENSE, THE, 1st Edition, 0321304543, by SZOR, PETER, published by Pearson Education, Inc, publishing as Addison Wesley Professional, Copyright © 2005 by Symatec Corporation.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc. CZECH language edition published by ZONER SOFTWARE, s.r.o., Copyright © 2006.

Autorizovaný překlad anglického vydání nazvaného ART OF COMPUTER VIRUS RESEARCH AND DEFENSE, první vydání, 0321304543, autor SZOR, PETER, vydal Pearson Education, Inc. ve vydavatelství Addison Wesley Professional, Copyright © 2005 Symatec Corporation.

Všechna práva vyhrazena. Žádná část této publikace nesmí být reprodukována nebo předávána žádnou formou nebo způsobem, elektronicky ani mechanicky, včetně fotokopíí, natáčení ani žádnými jinými systémy pro ukládání bez výslovného svolení Pearson Education, Inc. České vydání vydal ZONER SOFTWARE, s.r.o., Copyright © 2006.

## **Počítačové viry – analýza útoku a obrana**

Autor: Peter Szor

Copyright © ZONER software s.r.o. Vydání první v roce 2006. Všechna práva vyhrazena.

Zoner Press

KATALOGOVÉ ČÍSLO: **ZR505**

**ZONER software s.r.o.**

Nové sady 18, 602 00 Brno

Překlad: Ing. Lukáš Pelikán, Ing. Roman Skřivánek

Odpovědný redaktor: Miroslav Kučera

Šéfredaktor: Ing. Pavel Kristián

DTP: Miroslav Kučera

© Cover foto: Jiří Heller, HELLER.CZ s.r.o, [www.heller.cz](http://www.heller.cz)

© Cover: PYRAMIDE, s.r.o.

Informace, které jsou v této knize zveřejněny, mohou být chráněny jako patent. Jména produktů byla uvedena bez záruky jejich volného použití. Při tvorbě textů a vyobrazení bylo sice postupováno s maximální péčí, ale přesto nelze zcela vyloučit možnost výskytu chyb. Vydavatelé a autoři nepřebírají právní odpovědnost ani žádnou jinou záruku za použití chybných údajů a z toho vyplývajících důsledků. Všechna práva vyhrazena. Žádná část této publikace nesmí být reprodukována ani distribuována žádným způsobem ani prostředkem, ani reprodukována v databázi či na jiném záznamovém prostředku či v jiném systému bez výslovného svolení vydavatele, s výjimkou zveřejnění krátkých částí textu pro potřeby recenzí.

Veškeré dotazy týkající se distribuce směřujte na:

Zoner Press

**ZONER software s.r.o.**

Nové sady 18, 602 00 Brno

tel.: **532 190 883**, fax: **543 257 245**

e-mail: **[knihy@zoner.cz](mailto:knihy@zoner.cz)**

**<http://www.zonerpress.cz>**

ISBN 80-86815-04-8

Věnováno Natálii



# Obsah

O autorovi	18
Předmluva	19
Poděkování	21

## Část I – Strategie útočníka

<b>Kapitola 1</b>	<b>Úvod do her přírody</b>	<b>25</b>
1.1	Rané modely sebereplikujících 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
<b>Kapitola 2</b>	<b>Fascinující analýza škodlivého kódu</b>	<b>41</b>
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	Počítačové 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	Injektory	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

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 zařízení	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: Zmíst	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 enginy	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 Viry přepisující data	270
8.5.2 Data Diddlers	271
8.5.3 Viry 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 Sklizení 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 síť	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

<b>Kapitola 11    Techniky antivirové obrany</b>	<b>373</b>
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 přesměrování kódu	408
11.6.6 Podezřelé jméno kódové sekce	408
11.6.7 Možná infekce hlavičky	408
11.6.8 Podezřelé importy z KERNEL32.DLL přes pořadová čísla	408
11.6.9 Tabulka importovaných adres je přepsaná	408
11.6.10 Vícenásobné PE hlavičky	408
11.6.11 Vícenásobné hlavičky Windows a podezřelé importy z KERNEL32.DLL	408
11.6.12 Podezřelé reloky	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

11.11.5 Nezbytné změny v objektech	422
11.11.6 Možná řešení	422
11.12 Monitory 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 filtrovacím 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 Disassemblování 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** **576**

## 0 autorovi

Peter Szor je světově proslulý odborník na počítačové viry a bezpečnost. Aktivní výzkum počítačových virů vede více než 15 let – na viry a ochranu proti nim se zaměřil už ve své diplomové práci v roce 1991. Během své kariéry Peter pracoval s neznámějšími antivirovými produkty, jako jsou AVP, F-PROT a Symantec Norton AntiVirus. V letech 1990 až 1995 v Maďarsku vytvořil svůj vlastní antivirový program Pasteur. Kromě vývoje počítačových antivirů se Peter už roky zabývá vývojem systémů odolných proti chybám a systémům pro bezpečné finanční transakce.

V roce 1997 byl pozván do organizace CARO (Computer Antivirus Researchers Organization). Peter je také v dozorčí radě magazínu Virus Bulletin a je zakládajícím členem sítě AVED (AntiVirus Emergency Discussion). Více než pět let byl vedoucím výzkumníkem ve firmě Symantec v Santa Monice v Kalifornii.

Peter je autorem více než 70 článků na téma počítačových virů a bezpečnosti pro magazíny Virus Bulletin, Chip, Source, Windows NT Magazine, Information Security Bulletin a další. Je častým přednášejícím na konferencích, jako jsou Virus Bulletin, EICAR, ICSA nebo RSA a byl přizván i na takové bezpečnostní konference, jako je USENIX Security Symposium. Snaží se sdílet výsledky svého výzkumu a předávat své znalosti o počítačových virech a bezpečnosti ostatním.

# Předmluva

## Komu je tato kniha určena

V posledních dvou desetiletích se objevilo větší množství publikací na téma počítačových virů, ale pouze několik z nich bylo napsáno profesionály ("znalci") v oboru. Existuje mnoho knih, které se zabývají problematikou počítačových virů, a které se obvykle zaměřují na nováčky – z tohoto důvodu pak nejsou příliš zajímavé pro technické odborníky. Existuje pouze několik knih, které se zabývají technickými detaily, jejichž pochopení je nezbytné pro efektivní obranu proti počítačovým virům.

Součástí problému je i to, že existující knihy obsahují jen málo komplexních informací o aktuálních počítačových virech. Postrádají například důležité technické informace o rychle se šířících počítačových červech, které k napadení cílových systémů exploitují jejich zranitelnosti, nebo se nezabývají posledními technikami v oblasti evoluce kódu, jako je třeba metamorfismus. Pokud byste chtěli získat všechny informace, které jsou obsaženy v této knize, museli byste strávit mnoho času čtením článků, které lze jen obtížně vyhledávat v konferencích, zabývajících se počítačovými viry a bezpečností. K získání důležitých detailů byste se museli také roky zabývat zkoumáním škodlivého kódu.

Věřím, že tato kniha bude velice užitečná IT odborníkům a bezpečnostním profesionálům, kteří každodenně bojují proti počítačovým virům. V současné době musí systémoví administrátoři, stejně jako domácí uživatelé, bojovat s počítačovými červi a dalšími škodlivými programy ve svých sítích. Různé bezpečnostní kurzy se velmi málo věnují tématu ochrany proti počítačovým virům, přičemž široká veřejnost toho ví ještě méně o analýze a ochraně sítí proti takovým útokům. Faktem ovšem je, že techniky analýzy počítačových virů zatím ještě nebyly v žádné práci popsány v dostatečné míře.

Myslím si, že pro každého, kdo se zabývá počítačovou bezpečností, je důležité vědět, čeho všeho již autoři počítačových virů dosáhli.

Po mnoho let se výzkumníci počítačových virů soustředili na "soubory" nebo "infikované objekty". Na druhé straně jsou bezpečnostní profesionálové více než znepokojeni podezřelými událostmi probíhajícími na úrovni počítačové sítě. Hrozby typu červa CodeRed pracují tak, že prostřednictvím počítačové sítě injektují svůj kód do paměti zranitelných procesů, ale "neinfikují" soubory na disku. Z toho vyplývá, že dnes je důležité rozumět všem těmto perspektivám (jak samotným souborům a ukládání informací do nich, tak i obsahu paměti a počítačové sítě) a pomocí technik analýzy škodlivého kódu hledat souvislosti mezi vzniklými událostmi.

Během let jsem trénoval mnoho bezpečnostních analytiků, aby dokázali efektivně pracovat s nebezpečími plynoucími ze škodlivého kódu, a reagovat na ně. V této knize jsou obsaženy informace o všem, s čím jsem kdy pracoval. Uvádím například důležité informace o starých hrozbách, jako jsou 8-bitové viry pro počítač Commodore 64. Uvidíte, že techniky, jako je například technika stealth, se objevovaly už v dřívějších počítačových virech a na mnoha platformách. Tím si uvědomíte, že současné rootkity rozhodně nepředstavují nic nového! V knize naleznete dostatečně pokrytá témata, která se věnují nejenom hrozbám 32-bitových a 64-bitových červů pro Windows, ale i nebezpečím cíhajícím na mobilních zařízeních, společně s obsáhlým popisem souvisejících exploitů. Mým cílem je nejenom ilustrovat, jak

se mnoho starých technik "reinkarnováno" do nových hrozeb, ale také předvést moderní útoky s uvedením technických detailů.

Jsem si jist, že mnoho z vás se připojí k boji proti škodlivému kódu a stejně jako já vyvinou nové techniky obrany. Přitom je však potřeba si uvědomovat i nebezpečí a výzvy v tomto oboru!

## O čem je tato kniha

Účelem této knihy je demonstrovat současný stav oboru počítačových virů a vývoje antivirů a naučit vás metodám analýzy počítačových virů a ochraně proti nim. Popisují zde techniky infekce počítačovými viry ze všech možných perspektiv – souborů (ve smyslu uložení obsahu), paměti a počítačové sítě. Dozvíte se všechno o špinavých tricích počítačových virů, které byly v posledních dvou desetiletích vytvořeny těmi na druhé straně, a také o tom, jak pracovat se složitostmi polymorfního kódu a exploitů.

Nejjednodušší cestou, jak číst tuto knihu, je postupovat od jedné kapitole ke druhé. Některé kapitoly popisující útok ovšem mohou získat na své důležitosti poté, co si přečtete kapitoly, pojednávající o příslušných způsobech obrany. Pokud cítíte, že vám některá kapitola není po chuti nebo je příliš dlouhá nebo obtížná, můžete ji přeskóčit. Jsem si jistý, že každý čtenář podle svých zkušeností shledá některé části jako jednoduché a jiné jako obtížnější.

Předpokládám, že čtenář této knihy je na jisté úrovni obeznámen s technologiemi a programováním. Je zde popsáno tolik věcí, že je naprosto nemožné, aby se kniha zabývala všemi tématy do nejmenších detailů. Vše, co budete potřebovat k úspěšnému boji proti počítačovým virům, se však určitě dozvíte jinde. A abych vám v tomto ohledu pomohl, přidal jsem ke každé kapitole obsáhlý seznam odkazů, který vás navede k podrobnějším informacím.

Tato kniha určitě mohla mít více než 1000 stran. Jak jsem však řekl – nejsem Shakespeare. Mám znalosti počítačových virů, nikoliv angličtiny. Pokud by kniha byla psána jinak, neměli byste z ní velký užitek.

## O čem tato kniha není

V knize nepíšu nic o programech trojských koňů, a v celém rozsahu se nevěnuji "zadním vrátkám" v programech. Tato kniha je v první řadě o škodlivém kódu, který se sám replikuje. O škodlivých programech jako takových existuje spousta dobrých knih (narozdíl od tématu počítačových virů).

V této knize neuvádím žádný zdrojový kód, který by mohl být přímo použit k vytvoření jiného viru. Tato kniha není o tom, jak vytvářet viry. Rozumím však tomu, že autoři virů zpravidla znají většinu technik, které uvádím v této knize. Aby vyvinuli svoje vlastní techniky obrany, musí se "ti dobří" dozvědět více a začít přemýšlet (nikoliv však jednat) jako skuteční útočníci! Je zajímavé, že se mnoho univerzit snaží vyučovat výzkum počítačových virů tak, že nabízí kurzy jejich psaní. Může opravdu pomoci to, že je student schopen napsat virus, který infikuje miliony systémů po celém světě? Budou mít takoví studenti lepší znalosti vývoje lepších technik obrany? Odpověď na tuto otázku je pochopitelně záporná. Výuka by raději měla zaměřit na analýzu existujícího škodlivého kódu. Existuje mnoho hrozeb, které čekají na svůj rozbor a na to, až bude proti nim něco podniknuto.

Znalost počítačových virů je něco jako "Síla" ve Hvězdných válkách. Podle způsobu použití "Síly" může tato znalost působit dobro nebo zlo. Nemůžu vás ovšem přimět zůstat mimo Temnou stranu...

# Poděkování

Nejdříve bych chtěl poděkovat své ženě Natalii za to, že mě v mé práci více než 15 let povzbuzovala! Také bych jí chtěl poděkovat za to, že tolerovala všechnen čas, který jsem věnoval psaní knihy o víkendech, místo toho, abych se věnoval jí samotné.

Chtěl bych poděkovat všem, kteří umožnili vznik této knihy. Ta vzešla ze série článků o počítačových virech, z nichž jsem některé během let sepsal já, společně s dalšími výzkumníky. Nemohu proto dostatečně poděkovat Ericu Chienovi, Peterovi Ferriemu, Bruce McCorkendaleovi a Fredericu Perriotovi za jejich velký přínos ke kapitolám 7 a 10.

Tato kniha by nemohla být napsána bez pomoci mnoha přátel, antivirových odborníků a kolegů. Na prvním místě bych chtěl poděkovat Dr. Vesselinu Bontchevovi za to, že mě během mnoha let spolupráce naučil spoustu věcí o terminologii škodlivých programů. Vesselin je známý svou pečlivostí a můj výzkum velmi ovlivnil a podpořil.

Velký dík patří těmto lidem, kteří mě povzbudili při psaní této knihy, předali mi hodně svých znalostí a během let ovlivňovali můj výzkum: Oliver Beke, Zoltan Hornak, Frans Veldman, Eugene Kaspersky, Istvan Farmosi, Jim Bates, Dr. Frederick Cohen, Fridrik Skulason, David Ferbrache, Dr. Klaus Brunnstein, Mikko Hypponen, Dr. Steve White, a Dr. Alan Solomon.

Velký dík dlužím svým technickým recenzentům, kterými jsou Dr. Vesselin Bontchev, Peter Ferrie, Nick Fitzgerald, Halvar Flake, Mikko Hypponen, Dr. Jose Nazario a Jason V. Miller. Vaše podpora, kritika, porozumění a recenzování první verze rukopisu byly opravdu neocenitelné.

Chtěl bych poděkovat Janosi Kisovi a Zsoltu Szoboszlajmu, kteří mi poskytli přístup k virovým kódům v době, kdy centrem počítačového světa byla BBS. Také chci poděkovat Gunter May za největší dárek, který může dítě z východní Evropy dostat – C64.

Velký dík patří všem lidem v Symantecu, zejména však Lindě A. McCarthyové a Vincentu Weaferovi, kteří mě při psaní této knihy velice povzbudili. Chtěl bych poděkovat také Nancy Connerové a Chrisu Andrymu za jejich vynikající práci při editaci knihy. Bez jejich pomoci by tento projekt nebyl nikdy dokončen. Velký dík dlužím i Jessice Goldsteinové, Kristy Hartové a Christy Hackerdové, kteří mi pomáhali s procesem publikování.

Velký dík rovněž patří všem bývalým a současným členům CARO (Computer Antivirus Researchers Organization), VFORUM a AVED (AntiVirus Emergency Discussion) za zajímavé diskuse nejenom o počítačových virech a jiných škodlivých programech, ale také o systémech obrany.

Chtěl bych poděkovat všem lidem ve Virus Bulletinu za to, že po více než 10 let mezinárodně publikovali mé články, a že mi umožnili použít tento materiál pro tuto knihu.

Chtěl bych poděkovat svým rodičům a prarodičům za velké "domácí vzdělání" v matematice, fyzice, hudbě a historii.

## Kontakt na autora

Naleznete-li v této knize chyby, nebo pokud máte náměty na to, co by nemělo chybět v případném v budoucím vydání, velmi rád se o tom dozvím. Na své webové stránce plánuji uvádět podrobnější vysvětlení, případné korekce knihy, a také nové informace, které se vztahují k obsahu této knihy. Ačkoliv jsem vynaložil veškeré úsilí, abych vám poskytl "důvěryhodné" informace podle mých nejlepších znalostí, myslím si, že práce takového rozsahu a složitosti nemůže existovat bez jakýchkoliv nedostatků. Věřím, že na tyto eventuální nedostatky budete pohlížet s porozuměním.

Peter Szor

Santa Monica, CA

[pszor@acm.org](mailto:pszor@acm.org)

<http://www.peterszor.com>