Počítačové viry

analýza útoku a obrana

Peter Szor

symantec press
Addison Wesley
Zoner PRESS

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.

Počítačové viry – analýza útoku a obrana

Autor: Peter Szor

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
© Cover: PYRAMIDE, s.r.o.

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**
http://www.zonerpress.cz

ISBN 80-86815-04-8

Věnováno Natálii

Obsah

Část I – Strategie útočníka

Část II – Strategie obránce

O autorovi

Peter Szor je světově proslulý odborník na počítačové viry a bezpečnost. Aktivní výzkum počítačových virů vede více než 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 nejznámějšími 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 síti) 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 číhajícím 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. Popisuji 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 přeskočit. 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 nevěnují "zadním vrátkám" v programech. Tato kniha je v prvé 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 všechen 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 pomocí 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 věci 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 Szoboszlaymu, 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 poskytnul "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
http://www.peterszor.com