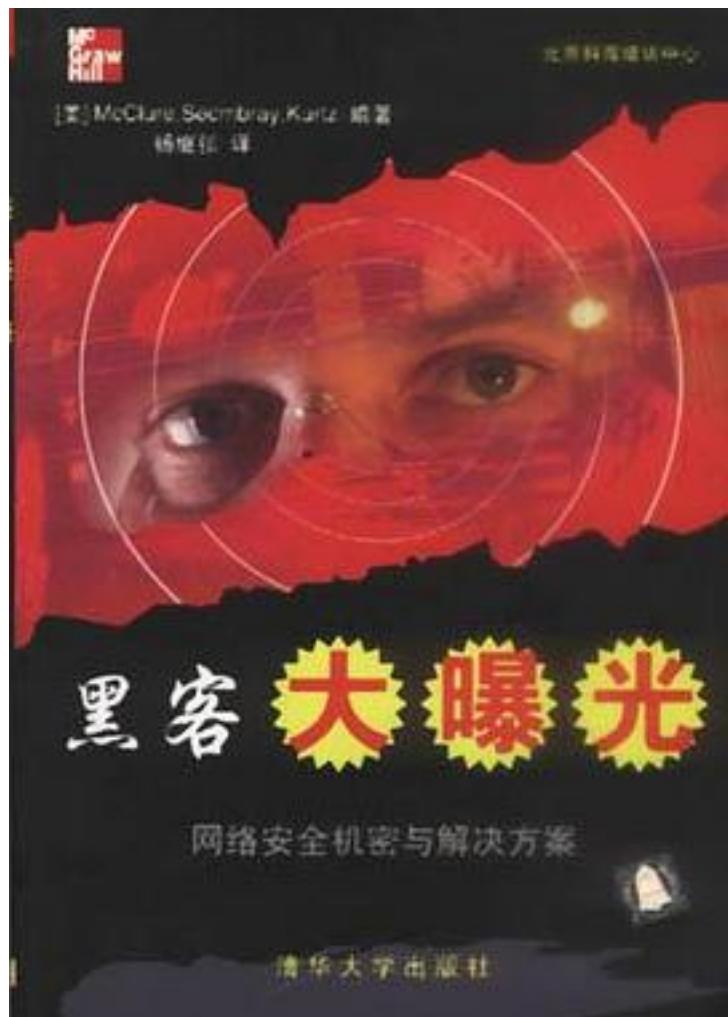


黑客大曝光



[黑客大曝光 下载链接1](#)

著者:Michael A.Davis

出版者:机械工业出版社华章公司

出版时间:2011-6-10

装帧:

isbn:9787111340348

抵御恶意软件和Rootkit不断掀起的攻击浪潮！《黑客大曝光：恶意软件和Rootkit安全

》用现实世界的案例研究和实例揭示了当前的黑客们是如何使用很容易得到的工具渗透和劫持系统的，逐步深入的对策提供了经过证明的预防技术。本书介绍了检测和消除恶意嵌入代码、拦截弹出式窗口和网站、预防击键记录以及终止Rootkit的方法，详细地介绍了最新的入侵检测、防火墙、蜜罐、防病毒、防Rootkit以及防间谍软件技术。

《黑客大曝光：恶意软件和Rootkit安全》包括以下内容：

- 理解恶意软件感染、生存以及在整个企业中传染的方法。
- 了解黑客使用存档文件、加密程序以及打包程序混淆代码的方法。
- 实施有效的入侵检测和预防程序。
- 防御击键记录、重定向、点击欺诈以及身份盗窃威胁。
- 检测，杀死和删除虚拟模式、用户模式和内核模式Rootkit。
- 预防恶意网站、仿冒、客户端和嵌入式代码攻击。
- 使用最新的防病毒、弹出窗口拦截程序和防火墙软件保护主机。
- 使用HIPS和NIPS识别和终止恶意进程。

作者介绍：

Michael A. Davis是Savid Technologies公司的CEO，该公司是一家全国性的技术和安全咨询公司。由于Michael将snort、ngrep、dsniff和honeyd这样的安全工具移植到Windows平台，因此他在开源软件安全界声名卓著。作为Honeynet项目成员，他为基于Windows的honeynet（蜜罐）开发了数据和网络控制机制。Michael还是sebek for Windows的开发者，这是一种基于内核的honeynet数据收集和监控工具。Michael曾经在领先的防病毒保护和漏洞管理企业—McAfee公司担任全球威胁高级经理，领导一个研究机密审查和尖端安全的团队。在McAfee工作之前，Michael曾在Foundstone工作过。

Sean M. Bodmer是Savid Corporation公司的政府项目主管。Sean是一位活跃的honeynet研究人员，精于分析恶意软件和攻击者的特征、模式和行为。最为引人注目的是，他花费了多年的时间来领导高级入侵检测系统（honeynet）的运作和分析，这一系统能够捕捉和分析入侵者及其工具的动机和目的，从而生成对进一步保护用户网络有价值的信息。在过去的10年中，Sean已经为华盛顿特区的多个联邦政府机构和私人公司负责过各种系统安全工程。Sean在全国的业界会议，如DEFCON、PhreakNIC、DC3、NW3C、Carnegie Mellon CERT和Pentagon安全论坛上发表过演讲，主题包括对攻击特征和攻击者的剖析，这些剖析能够帮助识别网络攻击的真正动机和意图。

Aaron LeMasters（乔治·华盛顿大学理科硕士）是一位精通计算机取证、恶意软件分析和漏洞研究的安全研究人员。他在职业生涯的头5年用在保护不设防的国防部网络上，现在他是Raytheon SI的高级软件工程师。Aaron乐于在大的安全会议（如Black Hat）和较小的区域黑客会议（如Outerzone）上分享研究成果。他更愿意关注与Windows内部构件、系统完整性、逆向工程和恶意软件分析相关的高级研究和开发问题。他是一位热心的原型构造者，很喜欢开发增强其研究趣味性的工具。在业余时间，Aaron喜欢打篮球、画素描、摆弄他的Epiphone Les Paul电吉他，以及和妻子一起去纽约旅行。

目录: 目录

对本书的赞誉

译者序

序言

前言

作者简介

技术编辑简介

第一部分 恶意软件

第1章 传染方法 5

1.1 这种安全设施可能确实有用 5

1.1.1 操作系统漏洞的减少 6

1.1.2 边界安全 7

1.2 为什么他们想要你的工作站 8

1.3 难以发现的意图 8

1.4 这是桩生意 9

1.5 重要的恶意软件传播技术 10

1.5.1 社会工程 10

1.5.2 文件执行 12

1.6 现代恶意软件的传播技术 14

1.6.1 StormWorm (恶意软件实例: trojan.peacomm) 15

1.6.2 变形 (恶意软件实例: W32.Evol、W32.Simile) 16

1.6.3 混淆 18

1.6.4 动态域名服务 (恶意软件实例: W32.Reatle.E@mm) 21

1.6.5 Fast Flux (恶意软件实例:

trojan.peacomm) 21

1.7 恶意软件传播注入方向 23

1.7.1 电子邮件 23

1.7.2 恶意网站 25

1.7.3 网络仿冒 27

1.7.4 对等网络 (P2P) 32

1.7.5 蠕虫 34

1.8 本书配套网站上的实例 36

1.9 小结 36

第2章 恶意软件功能 37

2.1 恶意软件安装后会做什么 37

2.1.1 弹出窗口 37

2.1.2 搜索引擎重定向 41

2.1.3 数据盗窃 47

2.1.4 单击欺诈 48

2.1.5 身份盗窃 49

2.1.6 击键记录 52

2.1.7 恶意软件的表现 55

2.2 识别安装的恶意软件 57

2.2.1 典型安装位置 58

2.2.2 在本地磁盘上安装 58

2.2.3 修改时间戳 59

2.2.4 感染进程 59

2.2.5 禁用服务 59

2.2.6 修改Windows注册表 60

2.3 小结 60

第二部分 Rootkit

第3章 用户模式Rootkit 64

3.1 维持访问权	64
3.2 隐身：掩盖存在	65
3.3 Rootkit的类型	66
3.4 时间轴	66
3.5 用户模式Rootkit	67
3.5.1 什么是用户模式Rootkit	68
3.5.2 后台技术	68
3.5.3 注入技术	71
3.5.4 钩子技术	80
3.5.5 用户模式Rootkit实例	81
3.6 小结	88
第4章 内核模式Rootkit	89
4.1 底层：x86体系结构基础	89
4.1.1 指令集体体系结构和操作系统	90
4.1.2 保护层次	90
4.1.3 跨越层次	91
4.1.4 内核模式：数字化的西部蛮荒	92
4.2 目标：Windows内核组件	92
4.2.1 Win32子系统	93
4.2.2 这些API究竟是什么	94
4.2.3 守门人：NTDLL.DLL	94
4.2.4 委员会功能：Windows Executive (NTOSKRNL.EXE)	94
4.2.5 Windows内核 (NTOSKRNL.EXE)	95
4.2.6 设备驱动程序	95
4.2.7 Windows硬件抽象层(HAL)	96
4.3 内核驱动程序概念	96
4.3.1 内核模式驱动程序体系结构	96
4.3.2 整体解剖：框架驱动程序	97
4.3.3 WDF、KMDF和UMDF	99
4.4 内核模式Rootkit	99
4.4.1 内核模式Rootkit简介	99
4.4.2 内核模式Rootkit所面对的挑战	100
4.4.3 装入	100
4.4.4 得以执行	101
4.4.5 与用户模式通信	101
4.4.6 保持隐蔽性和持续性	101
4.4.7 方法和技术	102
4.5 内核模式Rootkit实例	118
4.5.1 Clandestiny创建的Klog	118
4.5.2 Aphex创建的AFX	121
4.5.3 Jamie Butler、Peter Silberman 和C.H.A.O.S创建的FU和FUTo	123
4.5.4 Sherri Sparks和Jamie Butler创建的Shadow Walker	124
4.5.5 He4 Team创建的He4Hook	126
4.5.6 Honeynet项目创建的Sebek	129
4.6 小结	129
第5章 虚拟Rootkit	131
5.1 虚拟机技术概述	131
5.1.1 虚拟机类型	132
5.1.2 系统管理程序	132
5.1.3 虚拟化策略	134
5.1.4 虚拟内存管理	134
5.1.5 虚拟机隔离	135
5.2 虚拟机Rootkit技术	135

5.2.1 矩阵里的Rootkit：我们是怎么到这里的 135

5.2.2 什么是虚拟Rootkit 136

5.2.3 虚拟Rootkit的类型 136

5.2.4 检测虚拟环境 137

5.2.5 脱离虚拟环境 143

5.2.6 劫持系统管理程序 144

5.3 虚拟Rootkit实例 145

5.4 小结 150

第6章 Rootkit的未来：如果你现在认为情况严重 151

6.1 复杂性和隐蔽性的改进 151

6.2 定制的Rootkit 157

6.3 小结 157

第三部分 预防技术

第7章 防病毒 163

7.1 现在和以后：防病毒技术的革新 163

7.2 病毒全景 164

7.2.1 病毒的定义 164

7.2.2 分类 165

7.2.3 简单病毒 166

7.2.4 复杂病毒 168

7.3 防病毒—核心特性和技术 169

7.3.1 手工或者“按需”扫描 169

7.3.2 实时或者“访问时”扫描 170

7.3.3 基于特征码的检测 170

7.3.4 基于异常/启发式检测 171

7.4 对防病毒技术的作用的评论 172

7.4.1 防病毒技术擅长的方面 172

7.4.2 防病毒业界的领先者 173

7.4.3 防病毒的难题 175

7.5 防病毒曝光：你的防病毒产品是个Rootkit吗 180

7.5.1 在运行时修补系统服务 181

7.5.2 对用户模式隐藏线程 182

7.5.3 是一个缺陷吗 183

7.6 防病毒业界的未来 184

7.6.1 为生存而战斗 184

7.6.2 是行业的毁灭吗 185

7.6.3 可能替换防病毒的技术 186

7.7 小结和对策 187

第8章 主机保护系统 189

8.1 个人防火墙功能 189

8.1.1 McAfee 190

8.1.2 Symantec 191

8.1.3 Checkpoint 192

8.1.4 个人防火墙的局限性 193

8.2 弹出窗口拦截程序 195

8.2.1 Internet Explorer 195

8.2.2 Firefox 195

8.2.3 Opera 196

8.2.4 Safari 196

8.2.5 Chrome 196

8.2.6 一般的弹出式窗口拦截程序代码实例 198

8.3 小结 201

第9章 基于主机的入侵预防 202

9.1 HIPS体系结构 202

9.2 超过入侵检测的增长	204
9.3 行为与特征码	205
9.3.1 基于行为的系统	206
9.3.2 基于特征码的系统	206
9.4 反检测躲避技术	207
9.5 如何检测意图	210
9.6 HIPS和安全的未来	211
9.7 小结	212
第10章 Rootkit检测	213
10.1 Rootkit作者的悖论	213
10.2 Rootkit检测简史	214
10.3 检测方法详解	216
10.3.1 系统服务描述符表钩子	216
10.3.2 IRP钩子	217
10.3.3 嵌入钩子	217
10.3.4 中断描述符表钩子	218
10.3.5 直接内核对象操纵	218
10.3.6 IAT钩子	218
10.4 Windows防Rootkit特性	218
10.5 基于软件的Rootkit检测	219
10.5.1 实时检测与脱机检测	220
10.5.2 System Virginity Verifier	220
10.5.3 IceSword和DarkSpy	221
10.5.4 RootkitRevealer	223
10.5.5 F-Secure的Blacklight	223
10.5.6 Rootkit Unhooker	225
10.5.7 GMER	226
10.5.8 Helios和Helios Lite	227
10.5.9 McAfee Rootkit Detective	230
10.5.10 商业Rootkit检测工具	230
10.5.11 使用内存分析的脱机检测：内存取证的革新	231
10.6 虚拟Rootkit检测	237
10.7 基于硬件的Rootkit检测	238
10.8 小结	239
第11章 常规安全实践	240
11.1 最终用户教育	240
11.2 纵深防御	242
11.3 系统加固	243
11.4 自动更新	243
11.5 虚拟化	244
11.6 固有的安全（从一开始）	245
11.7 小结	245
附录A 系统安全分析：建立你自己的Rootkit检测程序	246
· · · · · (收起)	

[黑客大曝光](#) [下载链接1](#)

标签

网络安全

黑客

安全

hacker

计算机科学

计算机

计算机技术

已入手

评论

有些启发意义 但是实际价值不大

不太适合初学者，攻击原理 技术 和对抗方案交错在一起，稍有点乱。
初学者更适合另一本书：恶意软件、rootkit和僵尸网络

[黑客大曝光 下载链接1](#)

书评

[黑客大曝光 下载链接1](#)