第一图书网, tushu007.com

<<恶意软件分析诀窍与工具箱>>

图书基本信息

书名：<<恶意软件分析诀窍与工具箱>>

13位ISBN编号：9787302274407

10位ISBN编号：7302274401

出版时间：2012-1

出版时间：清华大学出版社

作者：Michael Hale Ligh,Steven Adair,Blake Hartstein,Matthew Richard

页数：584

译者：胡乔林,钟读航

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

<<恶意软件分析诀窍与工具箱>>

内容概要

针对多种常见威胁的强大而循序渐进的解决方案

我们将《恶意软件分析诀窍与工具箱——对抗“流氓”软件的技术与利器》称为工具箱，是因为每个诀窍都给出了解决某个特定问题或研究某个给定威胁的原理和详细的步骤。

在配书光盘中提供了补充资源，您可以找到相关的支持文件和原始程序。

您将学习如何使用这些工具分析恶意软件，有些工具是作者自己开发的，另外数百个工具则是可以公开下载的。

如果您的工作涉及紧急事件响应、计算机取证、系统安全或者反病毒研究，那么本书将会为您提供极大的帮助。

●学习如何在不暴露身份的前提下进行在线调查
●使用蜜罐收集由僵尸和蠕虫分布的恶意软件
●分析javascript、pdf文件以及office文档中的可疑内容
●使用虚拟或基础硬件建立一个低预算的恶意软件实验室
●通用编码和加密算法的逆向工程
●建立恶意软件分析的高级内存取证平台
●研究主流的威胁，如zeus、silent banker、coreflood、conficker、virut、clampi、bankpatch、blackenergy等

第一图书网, tushu007.com

作者简介

作者：莱(Michael Hale Ligh) (美国)Steven Adair (美国)Blake Hartstein 等 译者：胡乔林 钟读航Michael Hale Ligh，是Verisign iDefense公司的恶意代码分析专家，同时也是MNIN Security公司特别项目的主管。
Steven Adair，是Shadowserver Foundation的成员之一，经常分析恶意软件和跟踪僵尸网络。他与重点调查网络间谍组织发起的各种网络攻击。
Blake Hartstein，是多个安全工具的开发人员，同时也是Verisign iDefense公司的快速响应工程师，主要负责恶意软件突发事件的响应。
Matthew Richard开发过多种安全工具，同时为多家银行和信用机械提供安全管理服务。

第一图书网, tushu007.com

书籍目录

《恶意软件分析诀窍与工具箱——对抗“流氓”软件的技术与利器》
第1章 行为隐匿
1.1 洋葱路由器(tor)
1.2 使用tor研究恶意软件
1.3 tor缺陷
1.3.1 速度
1.3.2 不可信赖的tor操作员
1.3.3 tor阻止列表
1.4 代理服务器和协议
1.4.1 超文本传输协议(http)
1.4.2 socks4
1.4.3 socks5
1.5 基于web的匿名代理
1.6 保持匿名的替代方法
1.6.1 蜂窝internet连接
1.6.2 虚拟专用网
1.7 唯一且匿名
第2章 蜜罐
2.1 nepenthes蜜罐
2.1.1 利用nepenthes收集恶意软件样本
2.1.2 使用irc日志进行实时攻击监视
2.1.3 使用基于python的 http接收nepenthes提交的文件
2.2 使用dionaea蜜罐
2.2.1 使用dionaea收集恶意软件样本
2.2.2 使用基于python的http接收dionaea提交的文件
2.2.3 实时事件通告以及使用xmpp共享二进制文件
2.2.4 分析重放dionea记录的攻击
2.2.5 使用p0f工具被动识别远程主机操作系统
2.2.6 使用sqlite 和gnuplot绘制dionaea记录的攻击模式图
第3章 恶意软件分类
3.1 使用clamav分类
3.1.1 检查现有clamav特征码
3.1.2 创建自定义clamav特征码数据库
3.2 使用yara分类
3.2.1 将clamav特征码转换到yara格式特征码
3.2.2 使用yara和peid识别加壳文件
3.2.3 使用yara检测恶意软件的能力
3.3 工具集成
3.3.1 使用python识别文件类型及哈希算法
3.3.2 编写python多杀毒扫描软件
3.3.3 python中检测恶意pe文件
3.3.4 使用ssdeep查找相似恶意软件
3.3.5 使用ssdeep检测自修改代码
3.3.6 使用ida和bindiff检测自修改代码
第4章 沙箱和多杀毒扫描软件

第一图书网, tushu007.com

4.1 公用杀毒扫描软件
4.1.1 使用virus total扫描文件
4.1.2 使用jotti扫描文件
4.1.3 使用novirusthanks扫描文件
4.1.4 启用数据库的python多杀毒上传程序
4.2 多杀毒扫描软件的比较
4.3 公用沙箱分析
4.3.1 使用threatexpert分析恶意软件
4.3.2 使用cwsandbox分析恶意软件
4.3.3 使用anubis分析恶意软件
4.3.4 编写joebox autoit脚本
4.3.5 使用joebox应对路径依赖型恶意软件
4.3.6 使用joebox应对进程依赖型动态链接库
4.3.7 使用joebox设置主动型http代理
4.3.8 使用沙箱结果扫描项目
第5章 域名与ip地址
5.1 研究可疑域名
5.1.1 利用whois研究域
5.1.2 解析dns主机名
5.2 研究ip地址
5.3 使用被动dns和其他工具进行研究
5.3.1 使用bfk查询被动dns
5.3.2 使用robtex检查dns记录
5.3.3 使用domaintools执行反向ip搜索
5.3.4 使用dig启动区域传送
5.3.5 使用dnsmap暴力攻击子域
5.3.6 通过shadowserver将ip地址映射到asn
5.3.7 使用rbl检查ip信誉
5.4 fast flux域名
5.4.1 使用被动dns和ttl检测fast flux网络
5.4.2 跟踪fast flux域名
5.5 ip地址地理映射
第6章 文档、shellcode和url
6.1 分析javascript
6.1.1 使用spidermonkey分析javascript
6.1.2 使用jsunpack自动解码javascript
6.1.3 优化jsunpack-n的解码速度和完整性
6.1.4 通过模拟浏览器dom元素触发漏洞利用
6.2 分析pdf文档
6.2.1 使用pdf.py从pdf文件中提取javascript
6.2.2 伪造pdf软件版本触发漏洞利用
6.2.3 利用didier stevens的pdf工具集
6.2.4 确定利用pdf文件中的哪些漏洞
6.2.5 使用distorm反汇编shellcode
6.2.6 使用iibemu模拟shellcode
6.3 分析恶意office文档
6.3.1 使用officemalscanner分析microsoft office文件

第一图书网, tushu007.com

6.3.2 使用disview和malhost-setup调试office shellcode
6.4 分析网络流量
6.4.1 使用jsunpack从报文捕获文件中提取http文件
6.4.2 使用jsunpack绘制url关系图
第7章 恶意软件实验室
7.1 网络互联
7.1.1 实验室中tcp/ip路由连接
7.1.2 捕获、分析网络流量
7.1.3 使用inetsim模拟internet
7.1.4 使用burp套件操作http/https
7.2 物理目标机
7.2.1 使用joe stewart开发的truman
7.2.2 使用deep freeze保护物理系统
7.2.3 使用fog克隆和映像磁盘
7.2.4 使用mysql数据库自动调度fog任务
第8章 自动化操作
8.1 恶意软件分析周期
8.2 使用python实现自动化操作
8.2.1 使用virtualbox执行自动化恶意软件分析
8.2.2 分析virtualbox磁盘以及内存映像
8.2.3 使用vmware执行自动化恶意软件分析
8.3 添加分析模块
8.3.1 在python中使用tshark捕获报文
8.3.2 在python中使用inetsim收集网络日志
8.3.3 使用volatility分析内存转储
8.3.4 组合所有的沙箱块
8.4 杂项系统
8.4.1 使用zerowine和qemu执行自动化分析
8.4.2 使用sandboxie和buster执行自动化分析
第9章 动态分析
9.1 变化检测
9.1.1 使用process monitor记录api调用
9.1.2 使用regshot进行变化检测
9.1.3 接收文件系统变化通知
9.1.4 接收注册表变化通知
9.1.5 句柄表的差异比较
9.1.6 使用handlediff研究代码注入
9.1.7 观察bankpatch.c禁用windows文件保护的活动
9.2 api监视/钩子
9.2.1 使用microsoft detours构建api监视器
9.2.2 使用api监视器追踪子进程
9.2.3 捕获进程、线程和映像加载事件
9.3 数据保护
9.3.1 阻止进程终止
9.3.2 阻止恶意软件删除文件
9.3.3 阻止加载驱动程序
9.3.4 使用数据保护模块

第一图书网, tushu007.com

9.3.5 使用reactos创建定制命令shell
第10章 恶意软件取证
10.1 the sleuth kit(tsk)
10.1.1 使用tsk发现备用数据流
10.1.2 使用tsk检测隐藏文件和目录
10.1.3 使用microsoft脱机api查找隐藏注册表数据
10.2 取证/事件响应混合
10.2.1 绕开poison ivy锁定的文件
10.2.2 绕开conficker文件系统的acl限制
10.2.3 使用gmer扫描rootkit
10.2.4 通过检查ie的dom检测html注入
10.3 注册表分析
10.3.1 使用regripper插件对注册表取证
10.3.2 检测恶意安装的pki证书
10.3.3 检查泄露数据到注册表的恶意软件
第11章 调试恶意软件
11.1 使用调试器
11.1.1 打开和附加到进程
11.1.2 为shellcode分析配置jit调试器
11.1.3 熟悉调试器的图形用户界面
11.1.4 检查进程内存和资源
11.1.5 控制程序执行
11.1.6 设置和捕获断点
11.1.7 使用有条件的日志记录断点
11.2 immunity debugger的python api接口
11.2.1 使用python脚本和pycommand调试
11.2.2 在二进制文件中检测shellcode
11.2.3 调查silentbanker木马的api钩子
11.3 winappdbg python调试器
11.3.1 使用winappdbg工具操作进程内存
11.3.2 使用winappdbg工具设计一个python api监视器
第12章 反混淆
12.1 解码常见算法
12.1.1 python中的逆向xor算法
12.1.2 使用yaratize检测xor编码的数据
12.1.3 使用特殊字母解码base64
12.2 解密
12.2.1 从捕获的数据包中隔离加密数据
12.2.2 使用snd反向工具、findcrypt和kanal搜索加密机制
12.2.3 使用zynamics bindiff移植open ssl的符号
12.2.4 在python中使用pycrypto解密数据
12.3 恶意软件脱壳
12.3.1 查找加壳恶意软件的oep
12.3.2 使用lordpe转储进程内存
12.3.3 使用imprec重建导入表
12.4 与脱壳有关的资源
12.5 调试器脚本

第一图书网, tushu007.com

12.5.1 破解域名生成算法
12.5.2 使用x86emu和python解码字符串
第13章 处理dll
13.1 枚举dll的导出函数
13.1.1 cff explorer
13.1.2 pefile
13.1.3 ida pro
13.1.4 常见和不常见的导出名
13.2 使用rundll32.exe执行dll
13.3 绕过宿主进程的限制
13.4 使用rundll32ex远程调用dll导出函数
13.4.1 创建新工具的原因
13.4.2 使用rundll32ex
13.5 使用loaddll.exe调试dll
13.5.1 将dll加载到调试器中
13.5.2 找到dll的入口点
13.6 捕获dll入口点处的断点
13.7 执行作为windows服务的dll
13.7.1 服务dll的入口点
13.7.2 服务初始化
13.7.3 安装服务dll
13.7.4 传递参数给服务
13.8 将dll转换成独立的可执行文件
第14章 内核调试
14.1 远程内核调试
14.2 本地内核调试
14.3 软件需求
14.3.1 使用livekd进行本地调试
14.3.2 启用内核调试启动开关
14.3.3 调试vmware工作站客户机(在windows系统中)
14.3.4 调试parallels客户机(在mac os x上)
14.3.5 windbg命令和控制简介
14.3.6 探索进程和进程上下文
14.3.7 探索内核内存
14.3.8 在驱动程序加载时捕捉断点
14.3.9 脱壳驱动程序
14.3.10 转储和重建驱动程序
14.3.11 使用windbg脚本检测rootkit
14.3.12 使用ida pro进行内核调试
第15章 使用volatility进行内存取证
15.1 内存获取
15.1.1 使用moonsols windows内存工具箱转储内存
15.1.2 使用f-response获取远程、只读内存
15.1.3 访问虚拟机的内存文件
15.2 准备安装volatility
15.2.1 volatility概览
15.2.2 在内存转储中研究进程

第一图书网, tushu007.com

15.2.3 使用psscan检测dkom攻击
15.2.4 研究csrss.exe的备用进程列表
15.2.5 识别进程上下文的技巧
第16章 内存取证：代码注入与提取
16.1 深入研究dll
16.1.1 搜寻已加载的可疑dll
16.1.2 使用ldr_modules检测未链接的dll
16.2 代码注入和vad
16.2.1 研究vad
16.2.2 转换页面保护
16.2.3 在进程内存中搜索证据
16.2.4 使用malfind和yara识别注入代码
16.3 重建二进制文件
16.3.1 从内存中重建可执行文件的映像
16.3.2 使用impscan扫描导入函数
16.3.3 转储可疑的内核模块
第17章 内存取证：rootkit
17.1 检测iat钩子
17.2 检测eat钩子
17.3 检测内联api钩子
17.4 检测idt钩子
17.5 检测驱动程序的irp钩子
17.6 检测ssdt钩子
17.6.1 ssdt的角色
17.6.2 钩子和钩子检测
17.7 使用ssdt_ex自动研究
17.8 根据附加的内核线程搜索rootkit
17.8.1 使用线程在内核中隐藏
17.8.2 在内存转储中检测分离线程
17.9 识别系统范围的通知例程
17.9.1 找出检查的位置
17.9.2 使用notifyroutines插件
17.10 使用svscan定位恶意的服务进程
17.10.1 恶意软件如何滥用服务
17.10.2 scm的服务记录结构
17.10.3 枚举进程内存中的服务
17.10.4 blazgel木马的例子
17.10.5 使用volatility的svcscan插件
17.11 使用mutantscan扫描互斥体对象
第18章 内存取证：网络和注册表
18.1 探索套接字和连接对象
18.1.1 套接字和连接证据
18.1.2 套接字和连接对象
18.2 分析zeus留下的网络证据
18.3 检测企图隐藏tcp/ip的活动
18.3.1 扫描套接字和连接对象
18.3.2 其他项目

第一图书网, tushu007.com

18.4 检测原始套接字和混杂模式的网络接口
18.4.1 混杂模式的套接字
18.4.2 检测混杂模式
18.5 注册表分析
18.5.1 使用内存注册表工具分析注册表证据
18.5.2 通过最后写入时间戳排序注册表项
18.5.3 使用volatility和reg-ripper

第一图书网, tushu007.com

章节摘录

版权页：插图：日常生活中，我们喜欢拥有某种程度的隐私。
窗户上有窗帘，办公室有门，甚至计算机都有特制的屏保以防止窥视。
对隐私的需求也延伸到Internet的使用上。
我们不希望其他人知道我们在Google中输入的内容、即时通信对话的内容，以及访问的网站。
但是，如果有人监视，那么他们往往可以看到您的私密信息。
访问Intemet时有许多选择匿名方式的理由。
而匿名并不意味着是您在做违法或错误的事情。
调查恶意软件和追踪别有用心者时，进行匿名的理由非常直接。
您不希望信息显示在日志或其他记录中，因为这可能暴露自己或自己所在公司的信息。
例如，假设您在金融公司工作，最近检测到银行特洛伊木马感染了系统中的部分计算机。
您收集恶意域名、IP地址和恶意软件相关的其他数据。
在调查中，随后采取的步骤是找到罪犯拥有的网站。
结果，如果未提前采取措施进行匿名访问，那么您的IP地址会被记录到各种日志中，还会被罪犯看到
。

第一图书网, tushu007.com

媒体关注与评论

“本书是我今年所阅读过的最有用的安全技术书籍，对于所有希望保护其系统免受恶意软件威胁的人员来说，这是一本必备书籍。
”　　——Lenny Zeltser,Savvis公司的安全业务主管和SANS机构的高级教师“每个恶意软件分析受好者的终极行动指南。
”　　——Ryan，Olson VeriSign iDefense公司快速响应部门的主管　“每一页都充满了实用的恶意软件知识、创新的理念、有用的工具，非常值得购买！
”　　——AAron Walters Terremark公司的Volatility和VP安全研究项目的领导者

第一图书网, tushu007.com

编辑推荐

《恶意软件分析诀窍与工具箱:对抗"流氓"软件的技术与利器》编辑推荐：“一本极好的恶意软件书籍”August14，2011By Ashraf Aziz“Ash Aziz”“我乐意向在计算机取证领域工作的任何人甚至是桌面支持人员推荐《恶意软件分析诀窍与工具箱:对抗"流氓"软件的技术与利器》，不要忘记使用配书光盘中的命令和示例，它们也很有帮助。
”“恶意软件分析人员（包括反应人员和CERT）必备书籍”January1，2011By Aaed Salah Nemer“我已经阅读过很多有关恶意软件从概念到实验分析的安全书籍，但从来没有一本书籍像《恶意软件分析诀窍与工具箱:对抗"流氓"软件的技术与利器》这样给出了大量的技术细节。
我进行的大量的安全活动，需要我具有最新的恶意软件的坚实背景，并提升我的事件响应技能和分析技术。
”“一本优秀的书籍”December14，2010By ShaWn“这是我读过的有关恶意软件分析的最好、最容易的书籍。
《恶意软件分析诀窍与工具箱:对抗"流氓"软件的技术与利器》包含了有用的代码、巧妙的方法以及其他实用的信息。
这并不是一本随便拼凑编写几个工具的典型的大杂烩书籍。
显而易见，作者在内容和组织上花费了大量心思。
如果您也认真对待恶意软件分析，那么《恶意软件分析诀窍与工具箱:对抗"流氓"软件的技术与利器》值得您拥有。
”

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com