Equation_Ops

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。

概述

后渗透的主要操作就是横向移动和数据收集与外带，DSz中的有大量的模块来实现这个功能，Ops模块主要是Python扩展，利用脚本进行数据收集，提高操作效率，规范数据格式，对目标系统进行深入渗透。

操作

Ops默认操作过程是可以定制的，保存在survey.xml中。
先看看其执行过程，然后进行进一步的分析。

```
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.
```

Ops启动后，设置环境变量，添加库文件到Python。

然后开始对目标机进行信息收集。

创建数据库

```
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: aa1523fb-98cc-4bc5-9150-3336bd08336c
hostname: hacker-PC
macs: [u'00-15-5d-03-1f-51']
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: 0.8) fb / hacker-PC / PC ID 0x0000000000000000 / aa1523fb-
98cc-4bc5-9150-3336bd08336c / MACS: ['00-15-5d-03-1f-51']

Enter selection:
1
- [2022-08-04 08:42:06 z0.0.0.36] Target ID completed, ID 4dfbf1ae-3d24-4d9f-
b3ff-028e4da07c58 (in project fb)
- [2022-08-04 08:42:06 z0.0.0.36] You have been on this target previously
with the following CP addresses
z0.0.0.47
=====================================================================
- [2022-08-04 08:42:06 z0.0.0.36] Showing ifconfig data so you can make sure
you are on the correct target
FQDN: hacker-PC
DNS Servers: 172.19.144.1
- [2022-08-04 08:42:07 z0.0.0.36] Showing all non-local and non-tunnel
encapsulation adapter information, see command 188 for full interface list
|     Description      |        MAC        |       IP       |    Netmask    |
Gateway    | DHCP Server  |                    Name                        |
+----------------------+-------------------+----------------+---------------
+-------------+-------------+-----------------------------------------------
-+
| Microsoft 虚拟机总线网络适配器 | 00-15-5D-03-1F-51 | 172.19.144.205 |
255.255.240.0 | 172.19.144.1 | 172.19.144.1 | 本地连接 ({59456774-DC8D-4DED-
8548-5A660F2E5A79}) |
Running command 'survey -run
D:\work\malware\bvp47\FB\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
- [2022-08-04 08:42:10 z0.0.0.36] Loaded safety handlers from previous op(s)


    Command completed successfully
```

执行Connected.py，先创建目标机的数据库，DSz采用sqlite3来保存目标信息，为后门的survey提供基础信息。
然后开始执行servey.

进程列表

```
Running command 'survey -run'

- [2022-08-04 08:42:11 z0.0.0.36] ================================= Process
list ===================================================================
- [2022-08-04 08:42:13 z0.0.0.36] Data age: 00 seconds - data is fresh
- | PID  | PPID |                        Full Path                        |
User              | Comment |
- +------+------+---------------------------------------------------------+----
-------------------------+---------+
- |    0 |    0 |                                                         |
|         |
- |    4 |    0 | System                                                  |
|         |
- |  280 |    4 | ---\SystemRoot\System32\smss.exe                        | NT
AUTHORITY\SYSTEM          |         |
- |  360 |  352 | csrss.exe                                               |
|         |
- |  408 |  352 | C:\Windows\system32\wininit.exe                         | NT
AUTHORITY\SYSTEM          |         |
- |  504 |  408 | ---C:\Windows\system32\services.exe                     | NT
AUTHORITY\SYSTEM          |         |
- |  624 |  504 | ------svchost.exe                                       | NT
AUTHORITY\SYSTEM          |         |
- |  688 |  504 | ------svchost.exe                                       | NT
AUTHORITY\NETWORK SERVICE |         |
- |  740 |  504 | ------svchost.exe                                       | NT
AUTHORITY\LOCAL SERVICE   |         |
- |  864 |  504 | ------svchost.exe                                       | NT
AUTHORITY\SYSTEM          |         |
- | 1496 |  864 | ---------C:\Windows\system32\Dwm.exe                    |
hacker-PC\hacker             |         |
- |  892 |  504 | ------svchost.exe                                       | NT
AUTHORITY\SYSTEM          |         |
```

```
- | 1016 |  504 | ------svchost.exe                                    | NT
AUTHORITY\LOCAL SERVICE   |         |
- | 1088 |  504 | ------svchost.exe                                    | NT
AUTHORITY\NETWORK SERVICE |         |
- | 1220 |  504 | ------spoolsv.exe                                    | NT
AUTHORITY\SYSTEM          |         |
- | 1272 |  504 | ------svchost.exe                                    | NT
AUTHORITY\LOCAL SERVICE   |         |
- | 1388 |  504 | ------C:\Windows\system32\taskhost.exe               |
hacker-PC\hacker            |         |
- | 1428 |  504 | ------vmicsvc.exe                                    | NT
AUTHORITY\NETWORK SERVICE |         |
- | 1460 |  504 | ------vmicsvc.exe                                    | NT
AUTHORITY\LOCAL SERVICE   |         |
- | 1536 |  504 | ------vmicsvc.exe                                    | NT
AUTHORITY\SYSTEM          |         |
- | 1576 |  504 | ------vmicsvc.exe                                    | NT
AUTHORITY\LOCAL SERVICE   |         |
- | 1640 |  504 | ------vmicsvc.exe                                    | NT
AUTHORITY\SYSTEM          |         |
- | 1704 |  504 | ------svchost.exe                                    | NT
AUTHORITY\LOCAL SERVICE   |         |
- | 1660 |  504 | ------svchost.exe                                    | NT
AUTHORITY\NETWORK SERVICE |         |
- | 2148 |  504 | ------SearchIndexer.exe                              | NT
AUTHORITY\SYSTEM          |         |
- | 3832 |  504 | ------sppsvc.exe                                     | NT
AUTHORITY\NETWORK SERVICE |         |
- | 3868 |  504 | ------svchost.exe                                    | NT
AUTHORITY\SYSTEM          |         |
- |  512 |  408 | ---C:\Windows\system32\lsass.exe                     | NT
AUTHORITY\SYSTEM          |         |
- |  520 |  408 | ---C:\Windows\system32\lsm.exe                       | NT
AUTHORITY\SYSTEM          |         |
- |  420 |  400 | csrss.exe                                            |
|         |
- | 2864 |  420 | ---C:\Windows\system32\conhost.exe                   |
hacker-PC\hacker            |         |
- |  468 |  400 | C:\Windows\system32\winlogon.exe                     | NT
AUTHORITY\SYSTEM          |         |
- | 1524 | 1468 | C:\Windows\Explorer.EXE                              |
hacker-PC\hacker            |         |
- | 2344 | 1524 | ---C:\Program Files\Internet Explorer\iexplore.exe   |
hacker-PC\hacker            |         |
- | 2440 | 2344 | ------C:\Program Files\Internet Explorer\iexplore.exe |
hacker-PC\hacker            |         |
- | 2448 | 2344 | ------C:\Program Files\Internet Explorer\iexplore.exe |
hacker-PC\hacker            |         |
- | 2856 | 1524 | ---C:\Windows\system32\cmd.exe                       |
```

```
hacker-PC\hacker             |         |
- | 3996 | 1524 | ---C:\Windows\system32\taskmgr.exe                    |
hacker-PC\hacker             |         |
- | 2756 | 1524 | ---C:\test\PC_Level3a.exe                             |
hacker-PC\hacker             |         |
```

进程监控

```
background python monitorwrap.py -args "-g -t OPS_PROCESS_MONITOR_TAG -i 5 -s
\"processes -monitor  \" "

- [2022-08-04 08:42:13 z0.0.0.36] ====================================
Uptime ============================================================================
Uptime: 1 days, 21:05:24

- [2022-08-04 08:42:14 z0.0.0.36] ================== Auditing status check,
dorking will be later ================================================
- [2022-08-04 08:42:14 z0.0.0.36] 1 safety handler registered for audit
- [2022-08-04 08:42:15 z0.0.0.36] Data age: 00 seconds - data is fresh
- [2022-08-04 08:42:16 z0.0.0.36] Auditing is enabled on this machine
|             Category               | Success | Failure |
+------------------------------------+---------+---------+
| System_SecurityStateChange         | True    | False   |
| System_Integrity                   | True    | True    |
| System_Others                      | True    | True    |
| Logon_Logon                        | True    | False   |
| Logon_Logoff                       | True    | False   |
| Logon_AccountLockout               | True    | False   |
| Logon_SpecialLogon                 | True    | False   |
| Logon_NPS                          | True    | True    |
| PolicyChange_AuditPolicy           | True    | False   |
| PolicyChange_AuthenticationPolicy  | True    | False   |
| AccountManagement_UserAccount      | True    | False   |
| AccountManagement_SecurityGroup    | True    | False   |
- [2022-08-04 08:42:16 z0.0.0.36] The above is only being shown for
informational purposes, you will be prompted about dorking later
```

驱动列表

```
- [2022-08-04 08:42:16 z0.0.0.36] ================================== Driver
list ================================================================
Running command 'python
D:\work\malware\bvp47\FB\Resources\Ops\PyScripts\driverlist.py -project Ops -
args "-nofreshscan"'
- [2022-08-04 08:42:17 z0.0.0.36] 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 | 2022-08-04 |            |
- | dump_dumpata.sys | C:\Windows\system32\drivers | NEW,RANDOM,NO_HASH | !!!
POSSIBLE driver mem dump !!! | WARNING | 2022-08-04 |            |
- | dump_dumpfve.sys | C:\Windows\system32\drivers | NEW,RANDOM,NO_HASH | !!!
POSSIBLE driver mem dump !!! | WARNING | 2022-08-04 | hacker-pc9 |

    Command completed successfully
```

这里可以看到，不仅仅是查看了目标机的信息，也显示了相关机器的驱动安装情况。

安装软件列表

```
- [2022-08-04 08:42:25 z0.0.0.36] ============================== Installed
software ========================================================================

- ------------------------------------------------------------------ Installer
Packages ------------------------------------------------------------------
- [2022-08-04 08:42:26 z0.0.0.36] Data age: 00 seconds - data is fresh
| Arcitecture |                Name                |      Description      |
Installed version | Date installed |
+-------------+------------------------------------+-----------------------+--
-----------------+----------------+
| 32-bit      | Debugging Tools for Windows (x86) | Microsoft Corporation |
6.12.2.633        | 2022-08-02     |

- ------------------------------------------------------------------ Software
key(s) ------------------------------------------------------------------
- [2022-08-04 08:42:28 z0.0.0.36] Data age: 01 seconds - data is fresh
| Architecture |          Name          | Last update |
+--------------+------------------------+-------------+
| 32-bit       | ATI Technologies       | 2009-07-14  |
| 32-bit       | Classes                | 2022-08-02  |
| 32-bit       | Clients                | 2009-07-14  |
| 32-bit       | Intel                  | 2009-07-14  |
| 32-bit       | Microsoft              | 2022-08-04  |
| 32-bit       | ODBC                   | 2009-07-14  |
| 32-bit       | Policies               | 2009-07-14  |
| 32-bit       | RegisteredApplications | 2009-07-14  |
| 32-bit       | Sonic                  | 2009-07-14  |

- ------------------------------------------------------------------ Program
```

```
files dir(s) ------------------------------------------------------------
- [2022-08-04 08:42:30 z0.0.0.36] Data age: 00 seconds - data is fresh
| Architecture |            Folder Name            |           Modified
|
+--------------+-----------------------------------+-------------------------
------+
| 32-bit       | Common Files                      | 2009-07-
14T02:37:05.485289900 |
| 32-bit       | Debugging Tools for Windows (x86) | 2022-08-
02T03:45:44.835500000 |
| 32-bit       | DVD Maker                         | 2009-07-
14T08:41:23.676766100 |
| 32-bit       | Internet Explorer                 | 2009-07-
14T08:27:27.702965100 |
| 32-bit       | MSBuild                           | 2009-07-
14T04:52:30.938524700 |
| 32-bit       | Reference Assemblies              | 2009-07-
14T04:52:30.938524700 |
| 32-bit       | Uninstall Information             | 2009-07-
14T04:53:23.912062200 |
| 32-bit       | Windows Defender                  | 2009-07-
14T08:27:27.640462700 |
| 32-bit       | Windows Journal                   | 2009-07-
14T08:41:23.145546700 |
| 32-bit       | Windows Mail                      | 2009-07-
14T08:27:27.749841900 |
| 32-bit       | Windows Media Player              | 2009-07-
14T08:27:27.702965100 |
| 32-bit       | Windows NT                        | 2021-03-
12T06:04:11.325125000 |
| 32-bit       | Windows Photo Viewer              | 2009-07-
14T08:27:27.687339500 |
| 32-bit       | Windows Portable Devices          | 2009-07-
14T04:52:32.763727900 |
| 32-bit       | Windows Sidebar                   | 2009-07-
14T08:27:27.702965100 |
```

目标机上只安装了windbg，然后显示注册表的软件信息，program files目录下的文件列表

运行的服务

```
- [2022-08-04 08:42:30 z0.0.0.36] ================================ Running
services ============================================================
- [2022-08-04 08:42:32 z0.0.0.36] Data age: 01 seconds - data is fresh
|              Display name               |     Service name     |
+-----------------------------------------+----------------------+
```

Application Information	Appinfo
Windows Audio Endpoint Builder	AudioEndpointBuilder
Windows Audio	Audiosrv
Base Filtering Engine	BFE
Background Intelligent Transfer Service	BITS
Computer Browser	Browser
Cryptographic Services	CryptSvc
Offline Files	CscService
DCOM Server Process Launcher	DcomLaunch
DHCP Client	Dhcp
DNS Client	Dnscache
Diagnostic Policy Service	DPS
Windows Event Log	eventlog
COM+ Event System	EventSystem
Function Discovery Resource Publication	FDResPub
Group Policy Client	gpsvc
IKE and AuthIP IPsec Keying Modules	IKEEXT
IP Helper	iphlpsvc
Server	LanmanServer
Workstation	LanmanWorkstation
TCP/IP NetBIOS Helper	lmhosts
Windows Firewall	MpsSvc
Network Connections	Netman
Network List Service	netprofm
Network Location Awareness	NlaSvc
Network Store Interface Service	nsi
Program Compatibility Assistant Service	PcaSvc
Plug and Play	PlugPlay
IPsec Policy Agent	PolicyAgent
Power	Power
User Profile Service	ProfSvc
RPC Endpoint Mapper	RpcEptMapper
Remote Procedure Call (RPC)	RpcSs
Security Accounts Manager	SamSs
Task Scheduler	Schedule
System Event Notification Service	SENS
Shell Hardware Detection	ShellHWDetection
Print Spooler	Spooler
Software Protection	sppsvc
SPP Notification Service	sppuinotify
SSDP Discovery	SSDPSRV
Superfetch	SysMain
Themes	Themes
Distributed Link Tracking Client	TrkWks
Desktop Window Manager Session Manager	UxSms
Hyper-V Heartbeat Service	vmicheartbeat
Hyper-V Data Exchange Service	vmickvpexchange
Hyper-V Guest Shutdown Service	vmicshutdown
Hyper-V Time Synchronization Service	vmictimesync

```
| Hyper-V Volume Shadow Copy Requestor     | vmicvss               |
| Diagnostic Service Host                  | WdiServiceHost        |
| Diagnostic System Host                   | WdiSystemHost         |
| Windows Defender                         | WinDefend             |
| Windows Management Instrumentation       | Winmgmt               |
| Security Center                          | wscsvc                |
| Windows Search                           | WSearch               |
| Windows Update                           | wuauserv              |
```

防病毒软件

```
- [2022-08-04 08:42:32 z0.0.0.36] ================================== AV
Check!!! ========================================================================
Running command 'python windows\checkpsp.py -project Ops '
- Checking for any running known PSP's...
-   microsoft
-

- Checking for target PSP history...

- No target history found.

- Saw PSP's we can act on. Running scripts.
- ==========================================
- =                microsoft                 =
- ==========================================
- Checking for a change in configuration

- The following PSPs were NEWLY ADDED to target:
-   Microsoft Windows Defender Windows 7 Professional
- +--------------------+------------------------+
- |                    |     Setting Value      |
- +--------------------+------------------------+
- | Vendor             |              Microsoft |
- | Product            |       Windows Defender |
- | Version            | Windows 7 Professional |
- | Definition Updates |                   None |
- | Information        |                   None |
- | Install Date       |                   None |
- | Log File           |                   None |
- | Quarantine         |                   None |
- | ServiceStart       |                      2 |
- | Software           |                    PSP |
- | SpyNet             |                      0 |
- | Status             |                Enabled |
- +--------------------+------------------------+
```

```
    Command completed successfully
```

审计日志

```
- [2022-08-04 08:42:39 z0.0.0.36] ================================ Auditing
dorking ======================================================================
- [2022-08-04 08:42:39 z0.0.0.36] Data age: 24 seconds (from local cache, re-
run manually if you need to)
- [2022-08-04 08:42:39 z0.0.0.36] Auditing is enabled on this machine
|             Category               | Success | Failure |
+------------------------------------+---------+---------+
| System_SecurityStateChange         | True    | False   |
| System_Integrity                   | True    | True    |
| System_Others                      | True    | True    |
| Logon_Logon                        | True    | False   |
| Logon_Logoff                       | True    | False   |
| Logon_AccountLockout               | True    | False   |
| Logon_SpecialLogon                 | True    | False   |
| Logon_NPS                          | True    | True    |
| PolicyChange_AuditPolicy           | True    | False   |
| PolicyChange_AuthenticationPolicy  | True    | False   |
| AccountManagement_UserAccount      | True    | False   |
| AccountManagement_SecurityGroup    | True    | False   |
Do you want to dork security auditing?
z0.0.0.36: [2022-08-04 08:42:41] Hashhunter completed on hacker-PC!
YES
- [2022-08-04 08:42:56 z0.0.0.36] Security auditing dorked, do not stop
command 254 or you will lose your blessing
```

关闭审计日志。

安装网络驱动

```
- [2022-08-04 08:42:56 z0.0.0.36] ===================================
Monitors ===============================================================
     Monitors
     ----------------------------
 1)  Full - arp, netstat, activity
 2)  Netstat and activity
 3)  Activity only

 4)  Done

Select your monitors (full recommended for most situations): [1] 1
```

```
Staring a monitor with activity -monitor
- [2022-08-04 08:43:06 z0.0.0.36] Activity monitor started (or already
running)
Staring a monitor with netconnections -monitor
- [2022-08-04 08:43:07 z0.0.0.36] Netconnections monitor started (or already
running)
Staring a monitor with arp -delay 10s -monitor
- [2022-08-04 08:43:08 z0.0.0.36] Arp monitor started (or already running)
- [2022-08-04 08:43:08 z0.0.0.36] Process deep started in the background as
command ID 262.
- [2022-08-04 08:43:09 z0.0.0.36] Informational SIG check started in the
background as command ID 263.
```

定时任务

```
- [2022-08-04 08:43:09 z0.0.0.36] ================================ Scheduler
survey ================================================================
- [2022-08-04 08:43:14 z0.0.0.36] Data age: 03 seconds - data is fresh
| source  |                                                    command
|                     nextrun                     |                  triggers
|         runas          |
jobname                                                  |
+---------+-------------------------------------------------------------------
-----------------------------------------------------+---------------------
------------------------+-----------------------------------------------------+---
--------------------+-----------------------------------------------------------
-----------------------------------------------+
| SERVICE | COM job ClassID and data: {BF5CB148-7C77-4D8A-A53E-D81C70CF743C}
-                                                        | LOGON
| LOGON                                             |  LEAST                 |
Active Directory Rights Management Services Client\AD RMS Rights Policy
Template Management (Manual) |
| SERVICE | aitagent  (runs in "")
| DAILY 2007-10-08T02:30:00                         | DAILY 2007-10-08T02:30:00
| SYSTEM LEAST          | Application Experience\AitAgent
|
| SERVICE | %%%%windir%%%%\system32\rundll32.exe aepdu.dll,AePduRunUpdate
(runs in "")                                              | DAILY 2007-10-
08T00:30:00                       | DAILY 2007-10-08T00:30:00
| SYSTEM LEAST          | Application Experience\ProgramDataUpdater
|
| SERVICE | %%%%windir%%%%\system32\rundll32.exe /d
acproxy.dll,PerformAutochkOperations (runs in "")
| BOOT                                              | BOOT
| LOCAL SERVICE LEAST   | Autochk\Proxy
|
```

```
| SERVICE | BthUdTask.exe $(Arg0) (runs in "")
|                                                 |
| SYSTEM LEAST          | Bluetooth\UninstallDeviceTask
|
| SERVICE | COM job ClassID and data: {58FB76B9-AC85-4E55-AC04-427593B1D060}
- SYSTEM                                                | EVENT  , REGISTRATION
, BOOT                 | EVENT  , REGISTRATION  , BOOT                 |
SYSTEM LEAST          | CertificateServicesClient\SystemTask
|
| SERVICE | COM job ClassID and data: {58FB76B9-AC85-4E55-AC04-427593B1D060}
- USER                                                  | EVENT  , REGISTRATION
, LOGON                | EVENT  , REGISTRATION  , LOGON                |
LEAST                | CertificateServicesClient\UserTask
|
| SERVICE | %%%%SystemRoot%%%%\System32\wsqmcons.exe  (runs in "")
| TIME 2004-01-02T00:00:00                          | TIME 2004-01-02T00:00:00
| SYSTEM LEAST          | Customer Experience Improvement
Program\Consolidator                                                    |
| SERVICE | COM job ClassID and data: {E7ED314F-2816-4C26-AEB5-54A34D02404C}
-                                                       | WEEKLY 2008-09-
01T03:30:00                    | WEEKLY 2008-09-01T03:30:00
| LOCAL SERVICE LEAST   | Customer Experience Improvement
Program\KernelCeipTask                                                  |
| SERVICE | COM job ClassID and data: {C27F6B1D-FE0B-45E4-9257-38799FA69BC8}
- SYSTEM                                                | DAILY 2008-04-
25T01:30:00                     | DAILY 2008-04-25T01:30:00
| LOCAL SERVICE LEAST   | Customer Experience Improvement Program\UsbCeip
|
| SERVICE | %%%%windir%%%%\system32\defrag.exe -c (runs in "")
| WEEKLY 2005-01-01T01:00:00                        | WEEKLY 2005-01-01T01:00:00
| SYSTEM HIGHEST        | Defrag\ScheduledDefrag
|
| SERVICE | COM job ClassID and data: {C1F85EF8-BCC2-4606-BB39-70C523715EB3}
-                                                       | WEEKLY 2004-01-
01T01:00:00                    | WEEKLY 2004-01-01T01:00:00
|  HIGHEST              | Diagnosis\Scheduled
|
| SERVICE | %%%%windir%%%%\system32\rundll32.exe
dfdts.dll,DfdGetDefaultPolicyAndSMART (runs in "")
| WEEKLY 2004-01-01T01:00:00                        | WEEKLY 2004-01-01T01:00:00
| SYSTEM LEAST          | DiskDiagnostic\Microsoft-Windows-
DiskDiagnosticDataCollector                                             |
| SERVICE | %%%%windir%%%%\System32\LocationNotifications.exe  (runs in "")
| EVENT                                             | EVENT
|  LEAST                | Location\Notifications
|
| SERVICE | COM job ClassID and data: {A9A33436-678B-4C9C-A211-7CC38785E79D}
-                                                       | IDLE
| IDLE                                              |  HIGHEST              |
```

```
Maintenance\WinSAT
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /DoActivateWindowsSearch
(runs in "")                                                    |
|                                                 | SYSTEM LEAST          |
Media Center\ActivateWindowsSearch
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe
/DoConfigureInternetTimeService (runs in "")
|                                                 |
| SYSTEM LEAST          | Media Center\ConfigureInternetTimeService
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /DoRecoveryTasks $(Arg0)
(runs in "")                                                    |
|                                                 | SYSTEM LEAST          |
Media Center\DispatchRecoveryTasks
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /DRMInit (runs in "")
|                                                 |
| LOCAL SERVICE LEAST   | Media Center\ehDRMInit
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /InstallPlayReady $(Arg0)
(runs in "")                                                    |
|                                                 | SYSTEM LEAST          |
Media Center\InstallPlayReady
|
| SERVICE | %%%%SystemRoot%%%%\ehome\mcupdate $(Arg0) (runs in "")
|                                                 |
| NETWORK SERVICE LEAST | Media Center\mcupdate
|
| SERVICE | %%%%SystemRoot%%%%\ehome\mcupdate.exe -MediaCenterRecoveryTask
(runs in "")                                                      |
|                                                 | SYSTEM LEAST          |
Media Center\MediaCenterRecoveryTask
|
| SERVICE | COM job ClassID and data: {23E5D772-327A-42F5-BDEE-C65C6796BB2A}
- $(Arg1)                                                       |
|                                                 | SYSTEM LEAST          |
Media Center\MediaCenterRecoveryTask
|
| SERVICE | %%%%SystemRoot%%%%\ehome\mcupdate.exe -ObjectStoreRecoveryTask
(runs in "")                                                      |
|                                                 | NETWORK SERVICE LEAST |
Media Center\ObjectStoreRecoveryTask
|
| SERVICE | COM job ClassID and data: {177AFECE-9599-46CF-90D7-68EC9EEB27B4}
- $(Arg1)                                                       |
|                                                 | NETWORK SERVICE LEAST |
Media Center\ObjectStoreRecoveryTask
```

```
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /OCURActivate (runs in "")
|                                                    |
| SYSTEM LEAST          | Media Center\OCURActivate
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /OCURDiscovery $(Arg0)
(runs in "")                                                    |
|                                                    | SYSTEM LEAST          |
Media Center\OCURDiscovery
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /PBDADiscovery (runs in
"")                                                             |
|                                                    | SYSTEM LEAST          |
Media Center\PBDADiscovery
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /wait:7 /PBDADiscovery
(runs in "")                                                    |
|                                                    | SYSTEM LEAST          |
Media Center\PBDADiscoveryW1
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /wait:90 /PBDADiscovery
(runs in "")                                                    |
|                                                    | SYSTEM LEAST          |
Media Center\PBDADiscoveryW2
|
| SERVICE | %%%%SystemRoot%%%%\ehome\mcupdate.exe -PvrRecoveryTask (runs in
"")                                                             |
|                                                    | NETWORK SERVICE LEAST |
Media Center\PvrRecoveryTask
|
| SERVICE | COM job ClassID and data: {7FA3A1C3-3C87-40DE-AC16-B6E2815A4CC8}
- $(Arg1)                                                       |
|                                                    | NETWORK SERVICE LEAST |
Media Center\PvrRecoveryTask
|
| SERVICE | %%%%SystemRoot%%%%\ehome\mcupdate.exe -PvrSchedule (runs in "")
|                                                    |
| NETWORK SERVICE LEAST | Media Center\PvrScheduleTask
|
| SERVICE | COM job ClassID and data: {CEF51277-5358-477B-858C-4E14F0C80BF7}
- $(Arg1)                                                       |
|                                                    | NETWORK SERVICE LEAST |
Media Center\PvrScheduleTask
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /DoRegisterSearch $(Arg0)
(runs in "")                                                    |
|                                                    | SYSTEM LEAST          |
Media Center\RegisterSearch
|
```

```
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /DoReindexSearchRoot (runs
in "")                                                    |
|                                                  | SYSTEM LEAST          |
Media Center\ReindexSearchRoot
|
| SERVICE | %%%%SystemRoot%%%%\ehome\mcupdate.exe -SqlLiteRecoveryTask (runs
in "")                                                    |
|                                                  | NETWORK SERVICE LEAST |
Media Center\SqlLiteRecoveryTask
|
| SERVICE | COM job ClassID and data: {59116E30-02BD-4B84-BA1E-5D77E809B1A2}
- $(Arg1)                                                 |
|                                                  | NETWORK SERVICE LEAST |
Media Center\SqlLiteRecoveryTask
|
| SERVICE | %%%%SystemRoot%%%%\ehome\ehPrivJob.exe /DoUpdateRecordPath
$(Arg0) (runs in "")                                      |
|                                                  | SYSTEM LEAST          |
Media Center\UpdateRecordPath
|
| SERVICE | COM job ClassID and data: {190BA3F6-0205-4F46-B589-95C6822899D2}
- PageNotZero                                             | EVENT
| EVENT                                            |  LEAST                |
MemoryDiagnostic\CorruptionDetector
|
| SERVICE | COM job ClassID and data: {190BA3F6-0205-4F46-B589-95C6822899D2}
- Decompression                                           | EVENT
| EVENT                                            |  LEAST                |
MemoryDiagnostic\DecompressionFailureDetector
|
| SERVICE | COM job ClassID and data: {06DA0625-9701-43DA-BFD7-FBEEA2180A1E}
-                                                        | LOGON
| LOGON                                            |  LEAST                |
MobilePC\HotStart
|
| SERVICE | %%%%windir%%%%\system32\lpremove.exe  (runs in "")
| BOOT                                             | BOOT
| SYSTEM HIGHEST        | MUI\LPRemove
|
| SERVICE | COM job ClassID and data: {2DEA658F-54C1-4227-AF9B-260AB5FC3543}
-                                                        | LOGON
| LOGON                                            |  LEAST                |
Multimedia\SystemSoundsService
|
| SERVICE | %%%%windir%%%%\system32\gatherNetworkInfo.vbs  (runs in
"$(Arg1)")                                                          |
|                                                  |  HIGHEST              |
NetTrace\GatherNetworkInfo
|
```

```
| SERVICE | %%%%SystemRoot%%%%\System32\powercfg.exe -energy -auto (runs in
"")                                                    | DAILY 2008-01-
01T06:00:00                    | DAILY 2008-01-01T06:00:00
| SYSTEM LEAST          | Power Efficiency Diagnostics\AnalyzeSystem
|
| SERVICE | COM job ClassID and data: {42060D27-CA53-41F5-96E4-B1E8169308A6}
- $(Arg0)                                                | EVENT   , TIME 2008-
03-31T00:00:00Z            | EVENT   , TIME 2008-03-31T00:00:00Z            |
LOCAL SERVICE LEAST    | RAC\RacTask
|
| SERVICE | COM job ClassID and data: {C463A0FC-794F-4FDF-9201-01938CEACAFA}
-                                                       | EVENT
| EVENT                                          | LOCAL SERVICE LEAST    |
Ras\MobilityManager
|
| SERVICE | COM job ClassID and data: {CA767AA8-9157-4604-B64B-40747123D5F2}
-                                                       | DAILY 2008-01-
01T00:00:00                    | DAILY 2008-01-01T00:00:00
| SYSTEM LEAST          | Registry\RegIdleBackup
|
| SERVICE | %%%%windir%%%%\system32\RAServer.exe /offerraupdate (runs in
"%%%%windir%%%%")                                        | EVENT   ,
REGISTRATION                          | EVENT   , REGISTRATION
| SYSTEM HIGHEST        | RemoteAssistance\RemoteAssistanceTask
|
| SERVICE | COM job ClassID and data: {FF87090D-4A9A-4F47-879B-29A80C355D61}
- $(Arg0)                                                | LOGON
| LOGON                                          |  LEAST                |
SideShow\GadgetManager
|
| SERVICE | %%%%windir%%%%\system32\rundll32.exe /d
srrstr.dll,ExecuteScheduledSPPCreation (runs in "")
| DAILY 2005-06-14T00:00:00 , BOOT              | DAILY 2005-06-14T00:00:00 ,
BOOT              | SYSTEM LEAST          | SystemRestore\SR
|
| SERVICE | COM job ClassID and data: {855FEC53-D2E4-4999-9E87-3414E9CF0FF4}
- $(Arg0)                                                |
|                                                 |  LEAST                |
Task Manager\Interactive
|
| SERVICE | %%%%windir%%%%\system32\rundll32.exe
ndfapi.dll,NdfRunDllDuplicateIPOffendingSystem (runs in "")
| EVENT                                          | EVENT
|  HIGHEST              | Tcpip\IpAddressConflict1
|
| SERVICE | %%%%windir%%%%\system32\rundll32.exe
ndfapi.dll,NdfRunDllDuplicateIPDefendingSystem (runs in "")
| EVENT 2006-02-23T16:27:43                      | EVENT 2006-02-23T16:27:43
|  HIGHEST              | Tcpip\IpAddressConflict2
```

```
|
| SERVICE | COM job ClassID and data: {01575CFE-9A55-4003-A5E1-F38D1EBDCBE1}
-                                                    | LOGON
| LOGON                                          |  LEAST                |
TextServicesFramework\MsCtfMonitor
|
| SERVICE | %%%%windir%%%%\system32\sc.exe start w32time task_started (runs
in "")                                               | WEEKLY 2005-01-
01T01:00:00                    | WEEKLY 2005-01-01T01:00:00
| LOCAL SERVICE HIGHEST | Time Synchronization\SynchronizeTime
|
| SERVICE | sc.exe config upnphost start= auto (runs in "")
|                                                |
| SYSTEM LEAST          | UPnP\UPnPHostConfig
|
| SERVICE | COM job ClassID and data: {900BE39D-6BE8-461A-BC4D-B0FA71F5ECB1}
-                                                    |
|                                                |  HIGHEST              |
WDI\ResolutionHost
|
| SERVICE | %%%%windir%%%%\system32\wermgr.exe -queuereporting (runs in "")
| LOGON                                          | LOGON
|  LEAST                | Windows Error Reporting\QueueReporting
|
| SERVICE | %%%%windir%%%%\system32\rundll32.exe
bfe.dll,BfeOnServiceStartTypeChange (runs in "")
| EVENT                                          | EVENT
| SYSTEM LEAST          | Windows Filtering
Platform\BfeOnServiceStartTypeChange
|
| SERVICE | "%%%%ProgramFiles%%%%\Windows Media Player\wmpnscfg.exe"  (runs
in "")                                               | EVENT
| EVENT                                          |  LEAST                |
Windows Media Sharing\UpdateLibrary
|
| SERVICE | %%%%systemroot%%%%\System32\sdclt.exe /CONFIGNOTIFICATION (runs
in "")                                               | DAILY 2021-03-
19T10:00:00                    | DAILY 2021-03-19T10:00:00
| LOCAL SERVICE LEAST   | WindowsBackup\ConfigNotification
|
| SERVICE | c:\program files\windows defender\MpCmdRun.exe Scan -ScheduleJob
-WinTask -RestrictPrivilegesScan (runs in "")         | DAILY 2000-01-
01T02:23:33 2100-01-01T00:00:00 | DAILY 2000-01-01T02:23:33 2100-01-
01T00:00:00 | SYSTEM HIGHEST        | Windows Defender\MP Scheduled Scan
|
```

持久化

```
- [2022-08-04 08:43:15 z0.0.0.36] ============================== Persistence
checks ==========================================================
- |                           Path/Key                            |  File/Value
|                 Data                      |
- +---------------------------------------------------------------+-------------
--+-----------------------------------------+
- | system\currentcontrolset\Services\tcpip\Parameters\Winsock |
HelperDllName | %%%%SystemRoot%%%%\System32\wshtcpip.dll |
- | Software\Microsoft\Windows NT\CurrentVersion\Windows       | AppInit_Dlls
|                                         |
- | Software\Microsoft\Windows NT\CurrentVersion\winlogon      | Shell
| explorer.exe                            |
- | Software\Microsoft\Windows NT\CurrentVersion\winlogon      | Userinit
| C:\Windows\system32\userinit.exe,        |
- [2022-08-04 08:43:23 z0.0.0.36] Saved safety handlers for future op(s)
```

hashdump

```
- [2022-08-04 08:43:24 z0.0.0.36] ================================= Password
dump ============================================================
- [2022-08-04 08:43:24 z0.0.0.36] 1 safety handler registered for
passworddump
I think it's safe to run passworddump.  Do you want to run it?
YES
```

操作系统信息

```
- [2022-08-04 08:46:00 z0.0.0.36] ================================= OS
information ====================================================================
- [2022-08-04 08:46:02 z0.0.0.36] Data age: 02 seconds - data is fresh

- OS installed on Fri Mar 12 14:04:12 2021
- System language settings
  Locale:    Chinese (PR China)
  Installed: Chinese (PR China)
  UI:        Chinese (PR China)
  OS:        English (USA)
- System version information
  Version:   6.1.0.0 Build 7600 winnt i386
```

网络信息

```
- [2022-08-04 08:46:03 z0.0.0.36] ============================== Networking
Information ================================================================

FQDN: hacker-PC
DNS Servers: 172.19.144.1
- [2022-08-04 08:46:03 z0.0.0.36] Showing all non-local and non-tunnel
encapsulation adapter information, see command 188 for full interface list
|     Description      |        MAC        |       IP       |    Netmask    |
Gateway    | DHCP Server  |                     Name                         |
+----------------------+-------------------+----------------+---------------
+-------------+-------------+-----------------------------------------------
-+
| Microsoft 虚拟机总线网络适配器 | 00-15-5D-03-1F-51 | 172.19.144.205 |
255.255.240.0 | 172.19.144.1 | 172.19.144.1 | 本地连接 ({59456774-DC8D-4DED-
8548-5A660F2E5A79}) |

- ------------------------------------------------------------------------ Route
table ------------------------------------------------------------------------
- [2022-08-04 08:46:05 z0.0.0.36] Data age: 01 seconds - data is fresh
|       Dest. network       |      Mask       |   Gateway    |   Interface
| Metric |  Origin   |
+---------------------------+-----------------+--------------+---------------
-+--------+-----------+
| 0.0.0.0                   | 0.0.0.0         | 172.19.144.1 | 172.19.144.205
|      5 | MANUAL    |
| 127.0.0.0                 | 255.0.0.0       | 0.0.0.0      | 127.0.0.1
|    306 | MANUAL    |
| 127.0.0.1                 | 255.255.255.255 | 0.0.0.0      | 127.0.0.1
|    306 | MANUAL    |
| 127.255.255.255           | 255.255.255.255 | 0.0.0.0      | 127.0.0.1
|    306 | MANUAL    |
| 172.19.144.0              | 255.255.240.0   | 0.0.0.0      | 172.19.144.205
|    261 | MANUAL    |
| 172.19.144.205            | 255.255.255.255 | 0.0.0.0      | 172.19.144.205
|    261 | MANUAL    |
| 172.19.159.255            | 255.255.255.255 | 0.0.0.0      | 172.19.144.205
|    261 | MANUAL    |
| 224.0.0.0                 | 240.0.0.0       | 0.0.0.0      | 127.0.0.1
|    306 | WELLKNOWN |
| 224.0.0.0                 | 240.0.0.0       | 0.0.0.0      | 172.19.144.205
|    261 | WELLKNOWN |
| 255.255.255.255           | 255.255.255.255 | 0.0.0.0      | 127.0.0.1
|    306 | MANUAL    |
| 255.255.255.255           | 255.255.255.255 | 0.0.0.0      | 172.19.144.205
|    261 | MANUAL    |
```

```
| ::1                       | 128             | ::            | 127.0.0.1
|    306 | MANUAL    |
| fe80::                    | 64              | ::            | 172.19.144.205
|    261 | MANUAL    |
| fe80::5efe:ac13:90cd      | 128             | ::            |
|    256 | MANUAL    |
| fe80::3840:3e5f:3718:f012 | 128             | ::            | 172.19.144.205
|    261 | MANUAL    |
| ff00::                    | 8               | ::            | 127.0.0.1
|    306 | WELLKNOWN |
| ff00::                    | 8               | ::            | 172.19.144.205
|    261 | WELLKNOWN |
```

ARP 表

```
- ------------------------------------------------------------------------ ARP
table ------------------------------------------------------------------------
- [2022-08-04 08:46:05 z0.0.0.36] Data age: 00 seconds - data is fresh
|        IP          | Type |   Interface    |        MAC        |
+--------------------+------+----------------+-------------------+
| 224.0.0.22         |      | 127.0.0.1      |                   |
| 224.0.0.251        |      | 127.0.0.1      |                   |
| 239.255.255.250    |      | 127.0.0.1      |                   |
| 172.19.144.1       |      | 172.19.144.205 | 00-15-5D-62-99-19 |
| 172.19.159.255     |      | 172.19.144.205 | FF-FF-FF-FF-FF-FF |
| 224.0.0.22         |      | 172.19.144.205 | 01-00-5E-00-00-16 |
| 224.0.0.251        |      | 172.19.144.205 | 01-00-5E-00-00-FB |
| 224.0.0.252        |      | 172.19.144.205 | 01-00-5E-00-00-FC |
| 239.255.255.250    |      | 172.19.144.205 | 01-00-5E-7F-FF-FA |
| 255.255.255.255    |      | 172.19.144.205 | FF-FF-FF-FF-FF-FF |
| ff02::2            |      | 127.0.0.1      |                   |
| ff02::c            |      | 127.0.0.1      |                   |
| ff02::16           |      | 127.0.0.1      |                   |
| ff02::fb           |      | 127.0.0.1      |                   |
| ff02::1:2          |      | 127.0.0.1      |                   |
| ff02::1:ff6d:bd7e  |      | 127.0.0.1      |                   |
| ff02::1:ffb0:18bb  |      | 127.0.0.1      |                   |
| ff02::1:ffd0:6610  |      | 127.0.0.1      |                   |
| ff02::1:ffe0:62a7  |      | 127.0.0.1      |                   |
| ff02::2            |      | 172.19.144.205 | 33-33-00-00-00-02 |
| ff02::16           |      | 172.19.144.205 | 33-33-00-00-00-16 |
| ff02::fb           |      | 172.19.144.205 | 33-33-00-00-00-FB |
| ff02::1:2          |      | 172.19.144.205 | 33-33-00-01-00-02 |
| ff02::1:3          |      | 172.19.144.205 | 33-33-00-01-00-03 |
| ff02::1:ff18:f012  |      | 172.19.144.205 | 33-33-FF-18-F0-12 |
```

NETBIOS

```
- ------------------------------------------------------------------------
NETBIOS -------------------------------------------------------------------
Running command 'netbios '
------------------------------------------------------------------------
HACKER-PC           UNIQUE REGISTERED       File Server Service
HACKER-PC           UNIQUE REGISTERED       Workstation Service
WORKGROUP           GROUP REGISTERED        Domain Name
WORKGROUP           GROUP REGISTERED        Browser Service Elections
WORKGROUP           UNIQUE REGISTERED       Master Browser
??__MSBROWSE__?     GROUP REGISTERED        Master Browser

Adapter Address: 00.15.5d.03.1f.51
Adapter Type    : Ethernet Adapter


    Command completed successfully
```

netmap

```
Do you want to run background netmap -minimal?
YES
- Netmap will require user credentials (and probably won't work on 2K8)
- If you want to run netmap, you have to go run "duplicatetoken -duplicate"
or logonasuser for me
Do you want to do this?
YES
Please enter the user handle you were given by duplicatetoken or logonasuser
I should use (i.e. proc1234)
hacker
- [2022-08-04 08:47:11 z0.0.0.36] 1 safety handler registered for netmap
```

内存信息

```
- [2022-08-04 08:47:12 z0.0.0.36] ============================ Memory usage
information ============================================================
- [2022-08-04 08:47:12 z0.0.0.36] 1 safety handler registered for memory
- [2022-08-04 08:47:13 z0.0.0.36] Data age: 01 seconds - data is fresh
- Memory Load       : 29%%
- Physical Available: 722 M
- Physical Total    : 1023 M
```

磁盘信息

```
- [2022-08-04 08:47:14 z0.0.0.36] ============================ Disk list and
space info ============================================================
- [2022-08-04 08:47:17 z0.0.0.36] Data age: 01 seconds - data is fresh
| Drive |  Serial   |   Type    |   In use (MB)     | Change (MB) |
+-------+-----------+-----------+-------------------+-------------+
| A     |           | Removable |                   |             |
| C     | 4415-b715 | Fixed     | 7244/129945 (5%%) |           0 |
| D     |           | Cdrom     |                   |             |
```

USB

```
- [2022-08-04 08:47:18 z0.0.0.36] ================================= USB
survey info ================================================================
- [2022-08-04 08:47:19 z0.0.0.36]
System\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-
00a0c91efb8b} data is only 0:00:00.840000 old, was not re-run
- [2022-08-04 08:47:19 z0.0.0.36] SYSTEM\CurrentControlSet\Enum\USB not found
- [2022-08-04 08:47:20 z0.0.0.36] SYSTEM\CurrentControlSet\Enum\USBSTOR not
found
- [2022-08-04 08:47:20 z0.0.0.36] Showing recent USB devices
[2022-08-02 03:36:47] ##?
#IDE#DiskVirtual_HD_____________________________1.1.0___#5&35dc7040&0&0.0.0#
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
- [2022-08-04 08:47:22 z0.0.0.36] User info started in the background as
command ID 315.
```

最近修改文件

```
- [2022-08-04 08:47:23 z0.0.0.36] Extra info to get started in the background
as command ID 318.
Running command 'python diffhour.py -args "-safe -sysdrive -recursive"'
- [2022-08-04 08:47:25 z0.0.0.36] Recording initial data, running "dir -mask
"*" -path C: -age 1h -recursive"
- [2022-08-04 08:47:25 z0.0.0.36] Running dir -path C: -after "2022-08-03
23:47:25" -mask "*" -recursive -before "2022-08-04 00:47:25"
|       Modtime       |   Size   |                    Path
|                                        Name
|
+---------------------+----------+-----------------------------------------
-+-------------------------------------------------------------------------
-----+
```

```
| 2022-08-04 00:29:25 | <DIR>     | C:\ProgramData\Microsoft\RAC
| Temp
|
| 2022-08-04 00:31:25 |   413696 | C:\ProgramData\Microsoft\RAC\PublishedData
| RacWmiDatabase.sdf
|
| 2022-08-04 00:31:25 |   544768 | C:\ProgramData\Microsoft\RAC\StateData
| RacDatabase.sdf
|
| 2022-08-04 00:31:25 |        8 | C:\ProgramData\Microsoft\RAC\StateData
| RacMetaData.dat
|
| 2022-08-04 00:31:25 |    16412 | C:\ProgramData\Microsoft\RAC\StateData
| RacWmiDataBookmarks.dat
|
| 2022-08-04 00:31:25 |    32796 | C:\ProgramData\Microsoft\RAC\StateData
| RacWmiEventData.dat
|
| 2022-08-04 00:41:45 |   524288 | C:\Users\hacker
| NTUSER.DAT
|
| 2022-08-04 00:41:45 |   262144 | C:\Users\hacker
| ntuser.dat.LOG1
|
| 2022-08-04 00:29:24 |    12022 | C:\Windows\Prefetch
| CONHOST.EXE-1F3E9D7E.pf
|
| 2022-08-04 00:39:11 |    11622 | C:\Windows\Prefetch
| IPCONFIG.EXE-912F3D5B.pf
|
| 2022-08-04 00:29:52 |    22320 | C:\Windows\Prefetch
| MOBSYNC.EXE-C5E2284F.pf
|
| 2022-08-04 00:39:50 |     9440 | C:\Windows\Prefetch
| PC_LEVEL3A.EXE-65432FB1.pf
|
| 2022-08-04 00:39:24 |    11040 | C:\Windows\Prefetch
| PING.EXE-7E94E73E.pf
|
| 2022-08-04 00:29:24 |    34376 | C:\Windows\Prefetch
| TASKHOST.EXE-7238F31D.pf
|
| 2022-08-04 00:29:23 |     3992 | C:\Windows\rescache\rc0001
| ResCache.hit
|
| 2022-08-04 00:34:15 |    13792 | C:\Windows\System32
| 7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-
601632D005A0 |
| 2022-08-04 00:34:15 |    13792 | C:\Windows\System32
```

```
| 7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-
601632D005A0 |
| 2022-08-04 00:46:16 | 23330816 | C:\Windows\System32\config
| SOFTWARE
|
| 2022-08-04 00:46:16 |   262144 | C:\Windows\System32\config
| SOFTWARE.LOG1
|
| 2022-08-04 00:30:04 |  8912896 | C:\Windows\System32\config
| SYSTEM
|
| 2022-08-04 00:30:03 |   262144 | C:\Windows\System32\config
| SYSTEM.LOG1
|
| 2022-08-04 00:29:24 |       12 | C:\Windows\System32\LogFiles\Scm
| 9b75c702-ea13-406a-badb-6c588ee4375b
|
| 2022-08-04 00:29:24 |       12 | C:\Windows\System32\LogFiles\Scm
| 9efacbe6-a797-4905-a0c6-014cd3000dbb
|
| 2022-08-04 00:29:24 |       12 | C:\Windows\System32\LogFiles\Scm
| a1cfa52f-06f2-418d-addb-cd6456d66f43
|
| 2022-08-04 00:29:25 |       12 | C:\Windows\System32\LogFiles\Scm
| a316e645-1c56-45a6-bd6a-7dca79778090
|
| 2022-08-04 00:29:24 |       12 | C:\Windows\System32\LogFiles\Scm
| a6394592-54ce-4e93-8d64-1a068f462632
|
| 2022-08-04 00:29:22 |       12 | C:\Windows\System32\LogFiles\Scm
| de8bae53-2809-4f75-85ef-427d364b9b2c
|

    Command completed successfully
```

后台命令列表

```
- [2022-08-04 08:47:29 z0.0.0.36] Commands currently running in the
background:
| ID  |  Target   |
Full Command                                                          |
Sent | Received |
+-----+-----------+-----------------------------------------------------
-----------------------------------------------------------------------
---+------+----------+
| 109 | z0.0.0.36 | keepalive -delay 1m
|  109 |        0 |
```

```
| 170 | z0.0.0.36 | getadmin
|  140 |       17 |
| 180 | z0.0.0.36 | script Connected/Connected.dss
|    0 |        0 |
| 181 | z0.0.0.36 | python Connected/Connected.py -project Ops
|    0 |        0 |
| 196 | z0.0.0.36 | python survey.py -args " -run "
|    0 |        0 |
| 200 | z0.0.0.36 | background python monitorwrap.py -args "-g -t
OPS_PROCESS_MONITOR_TAG -i 5 -s "processes -monitor  " "
|    0 |        0 |
| 201 | z0.0.0.36 | background log=monitor guiflag=monitor processes -monitor
|  236 |     1037 |
| 254 | z0.0.0.36 | stopaliasing dst=z0.0.0.36 audit -disable security
|  152 |       14 |
| 256 | z0.0.0.36 | activity -monitor
|  154 |       37 |
| 258 | z0.0.0.36 | netconnections -monitor
|  175 |      646 |
| 260 | z0.0.0.36 | arp -delay 10s -monitor
|  169 |      297 |
| 315 | z0.0.0.36 | background python survey/launcher.py -project Ops -args
"--module ops.survey.userinfo --name "User info" --marker "ops::userinfo""
|    0 |        0 |
| 318 | z0.0.0.36 | background python survey/launcher.py -project Ops -args
"--module ops.survey.extra --name "Extra info to get" --marker
"ops::extrainfo"" |    0 |        0 |
```

就是上面操作的命令列表，可以看到，信息搜集非常全面，仔细。

分析

下面分析几个典型的脚本，方便理解Ops。

reboothistory

操作方法是执行python 脚本

命令输出

```
02:36:24>> aliases -add -alias "reboothistory" -replace "python
windows\reboothistory.py -project Ops" -location remote
[02:36:24] ID: 431 'aliases' started [target: z0.0.0.36]
Alias 'reboothistory' to 'python windows\reboothistory.py -project Ops'
added.
```

```
    Command completed successfully
02:36:26>> reboothistory
[02:36:26] ID: 432 'python' started [target: z0.0.0.36]
- Reboot Eventlogs
- |    Date    |   Time   |  ID  | Eventlog | RecNum |
Info                      |                      Process
|    Hostname     |     Title     |    Code    | Type | Description |
User         |
- +------------+----------+------+----------+--------+----------------------
------------------------+-------------------------------------------------------
+----------------+--------------+-----------+------+------------+--------
------------+
- | 2021-03-12 | 05:56:45 | 6009 | system   |     19 | System boot
|                                                  |                   |
|            |      |             |                     |
- | 2021-03-12 | 05:56:45 | 6005 | system   |     20 | Start of event log
service                     |
|                |              |           |      |             |
|
- | 2009-07-14 | 04:56:46 |  109 | system   |     21 | Kernel-Power: Shutdown
transition              |                                                       |
|               |            |      |             |                        |
- | 2009-07-14 | 04:56:50 |   13 | system   |     22 | Kernel: Stop
|                                                  |                   |
|            |      |             |                     |
- | 2021-03-12 | 05:56:23 |   12 | system   |     23 | Kernel: Start
|                                                  |                   |
|            |      |             |                     |
- | 2021-03-12 | 05:58:20 | 1074 | system   |    265 | Shutdown info
| C:\Windows\system32\winlogon.exe (37L4247D28-05) | WIN-A5SG7CFC47V | 操作系
统: 升级(计划内) | 0x80020003 | 重新启动 |              | NT AUTHORITY\SYSTEM |
- | 2021-03-12 | 05:58:21 | 6006 | system   |    267 | Event service stopped
(clean shutdown)         |                                                       |
|               |            |      |             |                        |
- | 2021-03-12 | 06:01:48 | 6009 | system   |    291 | System boot
|                                                  |                   |
|            |      |             |                     |
- | 2021-03-12 | 06:01:48 | 6005 | system   |    292 | Start of event log
service                     |
|                |              |           |      |             |
|
- | 2021-03-12 | 05:58:21 |  109 | system   |    296 | Kernel-Power: Shutdown
transition              |                                                       |
|               |            |      |             |                        |
- | 2021-03-12 | 05:58:22 |   13 | system   |    297 | Kernel: Stop
|                                                  |                   |
|            |      |             |                     |
- | 2021-03-12 | 05:58:29 |   12 | system   |    298 | Kernel: Start
```

```
|                                                    |                 |
|            |      |             |                     |
- | 2021-03-12 | 06:10:49 |   12 | system   |    416 | Kernel: Start
|                                                    |                 |
|            |      |             |                     |
- | 2021-03-12 | 06:10:52 | 6008 | system   |    418 | System shut down
unexpectedly (dirty shutdown) |
|                 |              |           |      |            |
|
- | 2021-03-12 | 06:10:52 | 6009 | system   |    419 | System boot
|                                                    |                 |
|            |      |             |                     |
- | 2021-03-12 | 06:10:52 | 6005 | system   |    420 | Start of event log
service                     |
|                 |              |           |      |            |
|
- | 2021-03-12 | 06:10:51 |   41 | system   |    424 | Kernel-Power: Critical
|                                                    |                 |
|            |      |             |                     |
- | 2021-03-12 | 06:14:00 | 6008 | system   |    513 | System shut down
unexpectedly (dirty shutdown) |
|                 |              |           |      |            |
|
- | 2021-03-12 | 06:14:00 | 6009 | system   |    514 | System boot
|                                                    |                 |
|            |      |             |                     |
- | 2021-03-12 | 06:14:00 | 6005 | system   |    515 | Start of event log
service                     |
|                 |              |           |      |            |
|
- | 2021-03-12 | 06:13:56 |   12 | system   |    517 | Kernel: Start
|                                                    |                 |
|            |      |             |                     |
- | 2021-03-12 | 06:13:58 |   41 | system   |    520 | Kernel-Power: Critical
|                                                    |                 |
|            |      |             |                     |
- | 2021-11-29 | 07:52:08 |   12 | system   |    603 | Kernel: Start
|                                                    |                 |
|            |      |             |                     |
- | 2021-11-29 | 07:52:12 | 6008 | system   |    604 | System shut down
unexpectedly (dirty shutdown) |
|                 |              |           |      |            |
|
- | 2021-11-29 | 07:52:12 | 6009 | system   |    605 | System boot
|                                                    |                 |
|            |      |             |                     |
- | 2021-11-29 | 07:52:12 | 6005 | system   |    606 | Start of event log
service                     |
|                 |              |           |      |            |
```

|
- | 2021-11-29 | 07:52:10 | 41 | system | 610 | Kernel-Power: Critical
| | |
| | | | |
- | 2022-08-02 | 03:36:46 | 12 | system | 662 | Kernel: Start
| | |
| | | | |
- | 2022-08-02 | 03:36:50 | 6008 | system | 663 | System shut down
unexpectedly (dirty shutdown) |
| | | | | |
|
- | 2022-08-02 | 03:36:50 | 6009 | system | 664 | System boot
| | |
| | | | |
- | 2022-08-02 | 03:36:50 | 6005 | system | 665 | Start of event log
service |
| | | | | |
|
- | 2022-08-02 | 03:36:49 | 41 | system | 669 | Kernel-Power: Critical
| | |
| | | | |

- | Boot | Shutdown | Uptime | Reason |
Crash |
- +---------------------+---------------------+--------+---------------+-----
--+
- | 2021-03-12 05:56:45 | 2021-03-12 05:58:21 | 1m36s | 操作系统: 升级(计划内)
| False |
- | 2021-03-12 06:01:48 | | | | True
|
- | 2021-03-12 06:10:52 | | | | True
|
- | 2021-03-12 06:14:00 | | | | True
|
- | 2021-11-29 07:52:12 | | | | True
|
- | 2022-08-02 03:36:50 | | | |
False |

- CrashControl and Dump information
- Dumps:
No dump found, or there was a problem with the dirs.

- Minidumps:

```
No dump found, or there was a problem with the dirs.



| CrashControl Key |                          Value
|
+------------------+-------------------------------------------------------
-+
| AutoReboot       | 1
|
| CrashDumpEnabled | 2
|
| Overwrite        | 1
|
| LogEvent         | 1
|
| MinidumpsCount   | 50
|
| DumpFile         | %%%%SystemRoot%%%%\MEMORY.DMP
|
| MinidumpDir      | %%%%SystemRoot%%%%\Minidump
|
| DumpFilters      | 640075006d007000660076006500 2e0073007900730000000000
|


- Windows Error Reporting registry keys
|                                                        Windows Error Reporting
key                                                       |
Value                  |
+-------------------------------------------------------------------------------
-----------------------------------------------------+-------------------
-------------------+
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\ConfigureArchive                                                    | 1
|
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\DisableArchive                                                      | 0
|
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\DisableQueue                                                        | 0
|
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\Disabled                                                            | 0
|
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\DontSendAdditionalData                                              | 0
|
```

```
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\DontShowUI                                                    | 0
|
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\ForceQueue                                                    | 0
|
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\LastQueuePesterTime                                           |
132600028369559843                    |
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\LastResponsePesterTime                                        |
132600040223333750                    |
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\LoggingDisabled                                               | 0
|
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\MaxArchiveCount                                               |
500                                   |
| HKEY_CURRENT_USER\software\microsoft\windows\windows error
reporting\MaxQueueCount                                                 | 50
|
| HKEY_LOCAL_MACHINE\software\microsoft\windows\windows error
reporting\ErrorPort                                                    |
\WindowsErrorReportingServicePort    |
| HKEY_LOCAL_MACHINE\software\microsoft\windows\windows error
reporting\MachineID                                                    |
80DB5994-5E35-49C6-8F68-7906E57426C3 |
| HKEY_LOCAL_MACHINE\software\microsoft\windows\windows error
reporting\MaxQueueSizePercentage                                       | 1
|
| HKEY_LOCAL_MACHINE\software\microsoft\windows\windows error
reporting\PurgeThreshholdValueInKB                                     | 10
|
| HKEY_LOCAL_MACHINE\software\microsoft\windows\windows error
reporting\ServiceTimeout                                               |
60000                                 |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error reporting\ConfigureArchive
| 1                                     |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error reporting\DisableArchive
| 0                                     |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error reporting\DisableQueue
| 0                                     |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error reporting\Disabled
| 0                                     |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
```

```
1000\software\microsoft\windows\windows error
reporting\DontSendAdditionalData | 0                                    |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error reporting\DontShowUI
| 0                                    |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error reporting\ForceQueue
| 0                                    |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error reporting\LastQueuePesterTime
| 132600028369559843                   |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error
reporting\LastResponsePesterTime | 132600040223333750                  |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error reporting\LoggingDisabled
| 0                                    |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error reporting\MaxArchiveCount
| 500                                  |
| HKEY_USERS\S-1-5-21-3475432181-1155754943-1615030112-
1000\software\microsoft\windows\windows error reporting\MaxQueueCount
| 50                                   |


- Windows Error Reporting ReportQueue in
C:\ProgramData\Microsoft\Windows\WER\ReportQueue
|                                        Dump
|           Modified            |           Accessed            |
Created            |
+-------------------------------------------------------------------------
------+-------------------------------+-------------------------------+------
-------------------------+
| NonCritical_x86_b5815bb88579b252665dcda9a35be218fa7f01_cab_07b14afe
| 2021-03-12T05:57:47.828125000 | 2021-03-12T05:57:47.828125000 | 2021-03-
12T05:57:47.828125000 |
| NonCritical_x86_8273482bb99351974d117bbb85b92ab698c5_cab_03c965c9
| 2021-03-12T05:57:54.687500000 | 2021-03-12T05:57:54.687500000 | 2021-03-
12T05:57:54.687500000 |
| NonCritical_x86_5112bff5bf5f6d7bcbd0f57be308aa36ac4a0_cab_058168c7
| 2021-03-12T05:57:55.453125000 | 2021-03-12T05:57:55.453125000 | 2021-03-
12T05:57:55.453125000 |
| NonCritical_x86_a9afd9cebb1d3c1a7ffc10b6456346227e55a79a_cab_0565779c
| 2021-03-12T05:57:59.250000000 | 2021-03-12T05:57:59.250000000 | 2021-03-
12T05:57:59.250000000 |
| NonCritical_x86_daa01e22fa232888398265a32e5089f18f8fc61d_cab_07e979fd
| 2021-03-12T05:57:59.859375000 | 2021-03-12T05:57:59.859375000 | 2021-03-
12T05:57:59.859375000 |
| NonCritical_x86_a8ecfd076265c2ce9f8a43642966cf41161a29_cab_06997f3d
```

```
| 2021-03-12T05:58:01.203125000 | 2021-03-12T05:58:01.203125000 | 2021-03-
12T05:58:01.203125000 |
| NonCritical_80072efe_eed54846deb8b3ece27f3b18d37b7066c8c31be_cab_09b3d0e3
| 2021-03-12T06:31:16.239625000 | 2021-03-12T06:31:16.239625000 | 2021-03-
12T06:31:16.239625000 |
|
NonCritical_7.3.7600.16385_83d89db3bee8694b325a46ad46dd6fefb24c93ab_cab_02dbd
b82 | 2021-03-12T06:31:18.958375000 | 2021-03-12T06:31:18.958375000 | 2021-
03-12T06:31:18.958375000 |
| NonCritical_80072efe_eed54846deb8b3ece27f3b18d37b7066c8c31be_05b0e751
| 2021-03-12T06:36:49.661500000 | 2021-03-12T06:36:49.661500000 | 2021-03-
12T06:36:49.661500000 |
|
NonCritical_7.3.7600.16385_83d89db3bee8694b325a46ad46dd6fefb24c93ab_0e44f1ff
| 2021-03-12T06:36:52.395875000 | 2021-03-12T06:36:52.395875000 | 2021-03-
12T06:36:52.395875000 |
| NonCritical_80072efe_eed54846deb8b3ece27f3b18d37b7066c8c31be_0233cdb7
| 2022-08-02T03:54:04.523000000 | 2022-08-02T03:54:04.523000000 | 2022-08-
02T03:54:04.523000000 |
|
NonCritical_7.3.7600.16385_83d89db3bee8694b325a46ad46dd6fefb24c93ab_08b3d865
| 2022-08-02T03:54:07.257375000 | 2022-08-02T03:54:07.257375000 | 2022-08-
02T03:54:07.257375000 |
| NonCritical_80072efe_eed54846deb8b3ece27f3b18d37b7066c8c31be_0488d986
| 2022-08-02T03:59:35.226125000 | 2022-08-02T03:59:35.226125000 | 2022-08-
02T03:59:35.226125000 |
|
NonCritical_7.3.7600.16385_83d89db3bee8694b325a46ad46dd6fefb24c93ab_0ff4e405
| 2022-08-02T03:59:37.913625000 | 2022-08-02T03:59:37.913625000 | 2022-08-
02T03:59:37.913625000 |
| NonCritical_80072efe_eed54846deb8b3ece27f3b18d37b7066c8c31be_0ed0b6b4
| 2022-08-02T04:30:01.319875000 | 2022-08-02T04:30:01.319875000 | 2022-08-
02T04:30:01.319875000 |
|
NonCritical_7.3.7600.16385_83d89db3bee8694b325a46ad46dd6fefb24c93ab_0f8cc114
| 2022-08-02T04:30:03.976125000 | 2022-08-02T04:30:03.976125000 | 2022-08-
02T04:30:03.976125000 |
| NonCritical_80072efe_eed54846deb8b3ece27f3b18d37b7066c8c31be_053a7ae4
| 2022-08-02T07:00:29.976125000 | 2022-08-02T07:00:29.976125000 | 2022-08-
02T07:00:29.976125000 |
|
NonCritical_7.3.7600.16385_83d89db3bee8694b325a46ad46dd6fefb24c93ab_0f3e8563
| 2022-08-02T07:00:32.663625000 | 2022-08-02T07:00:32.663625000 | 2022-08-
02T07:00:32.663625000 |
| NonCritical_80072efe_eed54846deb8b3ece27f3b18d37b7066c8c31be_0a05b6c6
| 2022-08-03T12:39:04.619750000 | 2022-08-03T12:39:04.619750000 | 2022-08-
03T12:39:04.604125000 |
|
NonCritical_7.3.7600.16385_83d89db3bee8694b325a46ad46dd6fefb24c93ab_0975c0aa
```

```
| 2022-08-03T12:39:07.135375000 | 2022-08-03T12:39:07.135375000 | 2022-08-
03T12:39:07.135375000 |


- DrWatson logs
- No Dr. Watson logs found, or there was a problem with the dirs.


- Checking shutdown logs
- No logfile xmls found, or there was a problem with the dirs.



    Command completed successfully
```

这个脚本先查看了eventlog中的启动日志，然后查看了crashdump信息，注册表的错误报告，windows系统的错误信息上报目录，DrWatson的日志，关机日志。
非常全面的信息收集。用在故障分析，取证溯源都很有价值。

代码分析

尽管Dsz有大量的DLL载荷，但是脚本在便利性上更有优势，简单看看上面的eventlog日志查看的代码执行过程，了解一下脚本的使用。

这个脚本在Ops\PyScripts\windows目录下，我们拷贝内容到一个测试脚本里面，删除无关代码。然后进行跟踪。

代码执行过程如下。

```
    Command completed successfully
01:39:08>> python test\hello.py
[01:39:08] ID: 734 'python' started [target: z0.0.0.48]
- Reboot Eventlogs
>d:\work\malware\bvp47\fb\resources\ops\pyscripts\test\hello.py(36)doeventlog
s()
-> eventfilter(6005, info='Start of event log service', color=dsz.DEFAULT)
(Pdb) c
- |    Date    |   Time   |  ID  | Eventlog | RecNum |
Info                        |                      Process
|    Hostname     |     Title     |    Code    | Type | Description |
User         |
- +------------+----------+------+----------+--------+----------------------
-------------------------+-------------------------------------------------
+-----------------+---------------+------------+------+-------------+--------
-------------+
- | 2021-03-12 | 05:56:45 | 6009 | system   |     19 | System boot
```

```
|                                                  |                 |
|            |      |             |                      |
- | 2021-03-12 | 05:56:45 | 6005 | system   |     20 | Start of event log
service                      |
|                 |              |           |      |             |
|
- | 2009-07-14 | 04:56:46 |  109 | system   |     21 | Kernel-Power: Shutdown
transition              |                                                  |
|               |            |      |             |                      |
- | 2009-07-14 | 04:56:50 |   13 | system   |     22 | Kernel: Stop
|                                                  |                 |
|            |      |             |                      |
- | 2021-03-12 | 05:56:23 |   12 | system   |     23 | Kernel: Start
|                                                  |                 |
|            |      |             |                      |
- | 2021-03-12 | 05:58:20 | 1074 | system   |    265 | Shutdown info
| C:\Windows\system32\winlogon.exe (37L4247D28-05) | WIN-A5SG7CFC47V | 操作系
统: 升级(计划内) | 0x80020003 | 重新启动 |              | NT AUTHORITY\SYSTEM |
- | 2021-03-12 | 05:58:21 | 6006 | system   |    267 | Event service stopped
(clean shutdown)         |                                                  |
|               |            |      |             |                      |
- | 2021-03-12 | 06:01:48 | 6009 | system   |    291 | System boot
|                                                  |                 |
|            |      |             |                      |
- | 2021-03-12 | 06:01:48 | 6005 | system   |    292 | Start of event log
service                      |
|                 |              |           |      |             |
|
- | 2021-03-12 | 05:58:21 |  109 | system   |    296 | Kernel-Power: Shutdown
transition              |                                                  |
|               |            |      |             |                      |
- | 2021-03-12 | 05:58:22 |   13 | system   |    297 | Kernel: Stop
|                                                  |                 |
|            |      |             |                      |
- | 2021-03-12 | 05:58:29 |   12 | system   |    298 | Kernel: Start
|                                                  |                 |
|            |      |             |                      |
- | 2021-03-12 | 06:10:49 |   12 | system   |    416 | Kernel: Start
|                                                  |                 |
|            |      |             |                      |
- | 2021-03-12 | 06:10:52 | 6008 | system   |    418 | System shut down
unexpectedly (dirty shutdown) |
|                 |              |           |      |             |
|
- | 2021-03-12 | 06:10:52 | 6009 | system   |    419 | System boot
|                                                  |                 |
|            |      |             |                      |
- | 2021-03-12 | 06:10:52 | 6005 | system   |    420 | Start of event log
service                      |
```

```
|                 |               |           |      |             |
|
- | 2021-03-12 | 06:10:51 |   41 | system   |    424 | Kernel-Power: Critical
|                                                    |                 |
|            |      |             |                      |
- | 2021-03-12 | 06:14:00 | 6008 | system   |    513 | System shut down
unexpectedly (dirty shutdown) |
|                 |               |           |      |             |
|
- | 2021-03-12 | 06:14:00 | 6009 | system   |    514 | System boot
|                                                    |                 |
|            |      |             |                      |
- | 2021-03-12 | 06:14:00 | 6005 | system   |    515 | Start of event log
service                     |
|                 |               |           |      |             |
|
- | 2021-03-12 | 06:13:56 |   12 | system   |    517 | Kernel: Start
|                                                    |                 |
|            |      |             |                      |
- | 2021-03-12 | 06:13:58 |   41 | system   |    520 | Kernel-Power: Critical
|                                                    |                 |
|            |      |             |                      |
- | 2021-11-29 | 07:52:08 |   12 | system   |    603 | Kernel: Start
|                                                    |                 |
|            |      |             |                      |
- | 2021-11-29 | 07:52:12 | 6008 | system   |    604 | System shut down
unexpectedly (dirty shutdown) |
|                 |               |           |      |             |
|
- | 2021-11-29 | 07:52:12 | 6009 | system   |    605 | System boot
|                                                    |                 |
|            |      |             |                      |
- | 2021-11-29 | 07:52:12 | 6005 | system   |    606 | Start of event log
service                     |
|                 |               |           |      |             |
|
- | 2021-11-29 | 07:52:10 |   41 | system   |    610 | Kernel-Power: Critical
|                                                    |                 |
|            |      |             |                      |
- | 2022-08-02 | 03:36:46 |   12 | system   |    662 | Kernel: Start
|                                                    |                 |
|            |      |             |                      |
- | 2022-08-02 | 03:36:50 | 6008 | system   |    663 | System shut down
unexpectedly (dirty shutdown) |
|                 |               |           |      |             |
|
- | 2022-08-02 | 03:36:50 | 6009 | system   |    664 | System boot
|                                                    |                 |
|            |      |             |                      |
```

```
- | 2022-08-02 | 03:36:50 | 6005 | system    |    665 | Start of event log
service                      |
|                 |              |           |      |             |
|
- | 2022-08-02 | 03:36:49 |   41 | system    |    669 | Kernel-Power: Critical
|                                                 |                 |
|            |      |             |                     |


- |        Boot          |      Shutdown       | Uptime |    Reason     |
Crash |
- +----------------------+---------------------+--------+---------------+-----
--+
- | 2021-03-12 05:56:45 | 2021-03-12 05:58:21 | 1m36s  | 操作系统: 升级(计划内)
| False |
- | 2021-03-12 06:01:48 |                     |        |               | True
|
- | 2021-03-12 06:10:52 |                     |        |               | True
|
- | 2021-03-12 06:14:00 |                     |        |               | True
|
- | 2021-11-29 07:52:12 |                     |        |               | True
|
- | 2022-08-02 03:36:50 |                     |        |               |
False |



    Command completed successfully
```

可以看到，这个脚本按照我们的目的，执行了eventlog的读取。
再看看代码。

```
import dsz, dsz.control, dsz.cmd, os.path, dsz.version
import sys
import ops.data, ops.cmd
from ops.pprint import pprint
import datetime
import time
import ops.timehelper

def eventfilter(id, info='', num=10000, eventlog='system', color=dsz.DEFAULT,
max=100, source=None):
    eventcmd = ops.cmd.getDszCommand('eventlogfilter', log=eventlog, id=id,
num=num, max=max)
    eventobject = eventcmd.execute()
```

```
    shutdowninfo_list = []
    for record in eventobject.record:
        if ((source is not None) and (record.source != source)):
            continue
        recdict = {'date': record.datewritten, 'time': record.timewritten,
'id': record.id, 'num': record.number, 'eventlog': eventlog, 'info': info,
'process': None, 'host': None, 'title': None, 'code': None, 'type': None,
'description': None, 'user': None}
        if (id == 1074):
            if dsz.version.checks.windows.IsVistaOrGreater():
                recdict['user'] = record.string[6].value
            recdict['process'] = record.string[0].value
            recdict['host'] = record.string[1].value
            recdict['title'] = record.string[2].value
            recdict['code'] = record.string[3].value
            recdict['type'] = record.string[4].value
            recdict['description'] = record.string[5].value
        recdict['color'] = color
        record_list.append(recdict)

def doeventlogs():
    global record_list
    record_list = []
    color_list = []
    import pdb;
    pdb.set_trace()
    eventfilter(6005, info='Start of event log service', color=dsz.DEFAULT)
    eventfilter(6006, info='Event service stopped (clean shutdown)',
color=dsz.DEFAULT)
    eventfilter(6008, info='System shut down unexpectedly (dirty shutdown)',
color=dsz.ERROR)
    eventfilter(6009, info='System boot', color=dsz.GOOD)
    eventfilter(1001, info='BugCheck', color=dsz.ERROR)
    eventfilter(1074, info='Shutdown info', color=dsz.WARNING)
    eventfilter(109, info='Kernel-Power: Shutdown transition',
color=dsz.DEFAULT)
    eventfilter(42, info='Kernel-Power: Informational', source='Microsoft-
Windows-Kernel-Power')
    eventfilter(41, info='Kernel-Power: Critical', color=dsz.ERROR,
source='Microsoft-Windows-Kernel-Power')
    eventfilter(13, info='Kernel: Stop', color=dsz.DEFAULT,
source='Microsoft-Windows-Kernel-General')
    eventfilter(12, info='Kernel: Start', color=dsz.DEFAULT,
source='Microsoft-Windows-Kernel-General')
    record_list.sort(key=(lambda x: x['eventlog']))
    record_list.sort(key=(lambda x: x['num']))
    for record in record_list:
        color_list.append(record['color'])
    pprint(record_list, header=['Date', 'Time', 'ID', 'Eventlog', 'RecNum',
```

```
'Info', 'Process', 'Hostname', 'Title', 'Code', 'Type', 'Description',
'User'], dictorder=['date', 'time', 'id', 'eventlog', 'num', 'info',
'process', 'host', 'title', 'code', 'type', 'description', 'user'],
echocodes=color_list)
    print '\n'
    makebootlog(record_list)
    print '\n'

def makebootlog(record_list):
    boot_hist = []
    this_event = []
    for record in record_list:
        if (record['id'] == 6009):
            boot_hist.append(this_event)
            this_event = []
        this_event.append(record)
    boot_hist.append(this_event)
    boot_summary = []
    color_list = []
    for this_event in boot_hist:
        if (len(this_event) == 0):
            continue
        boot = None
        shutdown = None
        reason = []
        crash = False
        uptime = None
        for record in this_event:
            if (record['id'] == 6009):
                boot = ('%s %s' % (record['date'], record['time']))
            elif (record['id'] == 6006):
                shutdown = ('%s %s' % (record['date'], record['time']))
            elif (record['id'] == 6008):
                crash = True
            elif (record['id'] == 1001):
                crash = True
            elif (record['id'] == 1074):
                reason.append(record['title'])
        reason = ','.join(reason)
        boot_summary.append({'boot': boot, 'shutdown': shutdown, 'reason':
reason, 'crash': crash, 'uptime': uptime})
        if crash:
            color_list.append(dsz.ERROR)
        else:
            color_list.append(dsz.DEFAULT)
    for boot in boot_summary:
        if ((boot['boot'] is not None) and (boot['shutdown'] is not None)):
            boottime = datetime.datetime(*time.strptime(boot['boot'], '%Y-%m-
%d %H:%M:%S')[0:6])
```

```
            shutdowntime = datetime.datetime(*time.strptime(boot['shutdown'],
'%Y-%m-%d %H:%M:%S')[0:6])
            uptime = (shutdowntime - boottime)
            boot['uptime'] =
ops.timehelper.get_age_from_seconds((((uptime.days * 3600) * 24) +
uptime.seconds))
    pprint(boot_summary, header=['Boot', 'Shutdown', 'Uptime', 'Reason',
'Crash'], dictorder=['boot', 'shutdown', 'uptime', 'reason', 'crash'],
echocodes=color_list)

def main(arguments):
    dsz.ui.Echo('Reboot Eventlogs', dsz.GOOD)
    doeventlogs()

if (__name__ == '__main__'):
    try:
        main(sys.argv[1:])
    except RuntimeError as e:
        dsz.ui.Echo(('\nCaught RuntimeError: %s' % e), dsz.ERROR)
```

脚本在导入dsz和ops后，开始进行操作，dsz提供了基础的UI和命令操作，ops则自己增加了部分辅助函数，用来简化开发。

通过多次调用eventlogfilter，根据eventlog id来筛选日志。可以看出。

```
6005 Event log startup
6006 Event log service was stoppped
6008 Last shutdown was unexpected
6009 User restarted or shut down system
1001 Application crashed or hung
1074 System shut down or restarted by other task
109 Shutdown by kernel power manager
42 System went into sleep mode
41 Shutdown during sleep mode(?)
13 Proper shutdown(?)
12 System started
```

这几个日志，代码说的比较清楚，比如可以只看系统启动。

```
01:56:14>> python test\hello.py
[01:56:14] ID: 746 'python' started [target: z0.0.0.48]
- Reboot Eventlogs
- |     Date     |    Time    | ID | Eventlog | RecNum |      Info       | Process
| Hostname | Title | Code | Type | Description | User |
- +------------+----------+----+----------+--------+---------------+---------
```

```
+----------+-------+------+------+-------------+------+
- | 2021-03-12 | 05:56:23 | 12 | system   |     23 | Kernel: Start |
|          |       |      |      |             |      |
- | 2021-03-12 | 05:58:29 | 12 | system   |    298 | Kernel: Start |
|          |       |      |      |             |      |
- | 2021-03-12 | 06:10:49 | 12 | system   |    416 | Kernel: Start |
|          |       |      |      |             |      |
- | 2021-03-12 | 06:13:56 | 12 | system   |    517 | Kernel: Start |
|          |       |      |      |             |      |
- | 2021-11-29 | 07:52:08 | 12 | system   |    603 | Kernel: Start |
|          |       |      |      |             |      |
- | 2022-08-02 | 03:36:46 | 12 | system   |    662 | Kernel: Start |
|          |       |      |      |             |      |


- | Boot | Shutdown | Uptime | Reason | Crash |
- +------+----------+--------+--------+-------+
- |      |          |        |        | False |



    Command completed successfully
```

这样就只看系统的启动日志，当然，也可以在前面的输出日志中过滤即可。

主要的逻辑

```
    eventcmd = ops.cmd.getDszCommand('eventlogfilter', log=eventlog, id=id,
num=num, max=max)
   eventobject = eventcmd.execute()
```

执行代码后，就得到了eventlog，然后就是添加到列表中，整理输出即可。

总结

通过Python脚本，提供了极大的便利。这里的Python脚本，还可以设置断点，通过pdb进行调试。确实非常方便，比CS的强，与MSF持平。

这里的Python文件，不支持utf-8编码，只支持默认的ascii或者latain编码。

参考

1. Inside of Danderspritz post-exploitation modules | HackerNoon
2.