网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

基于DMI的内存获取卡的威胁捕获与分析

安天 | 安全研究与应急处理中心

CONTENTS

目 录

01
当前APT攻击技术现状
无文件攻击已成为高级威胁常态

02
对APT攻击取证的难点
反取证技术被普遍使用

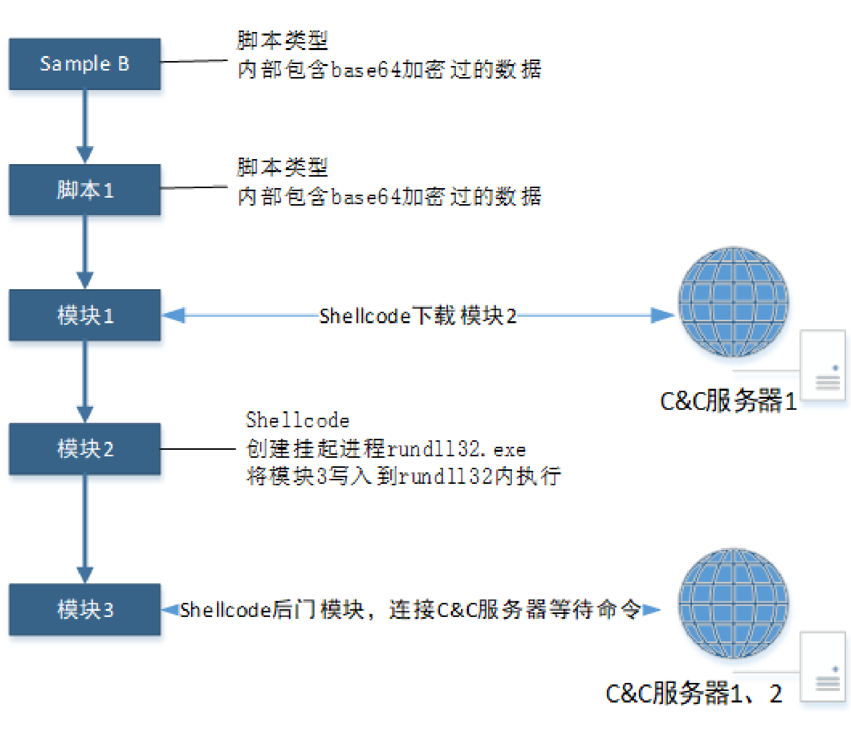
03
对易失介质取证的探索
已有技术情况

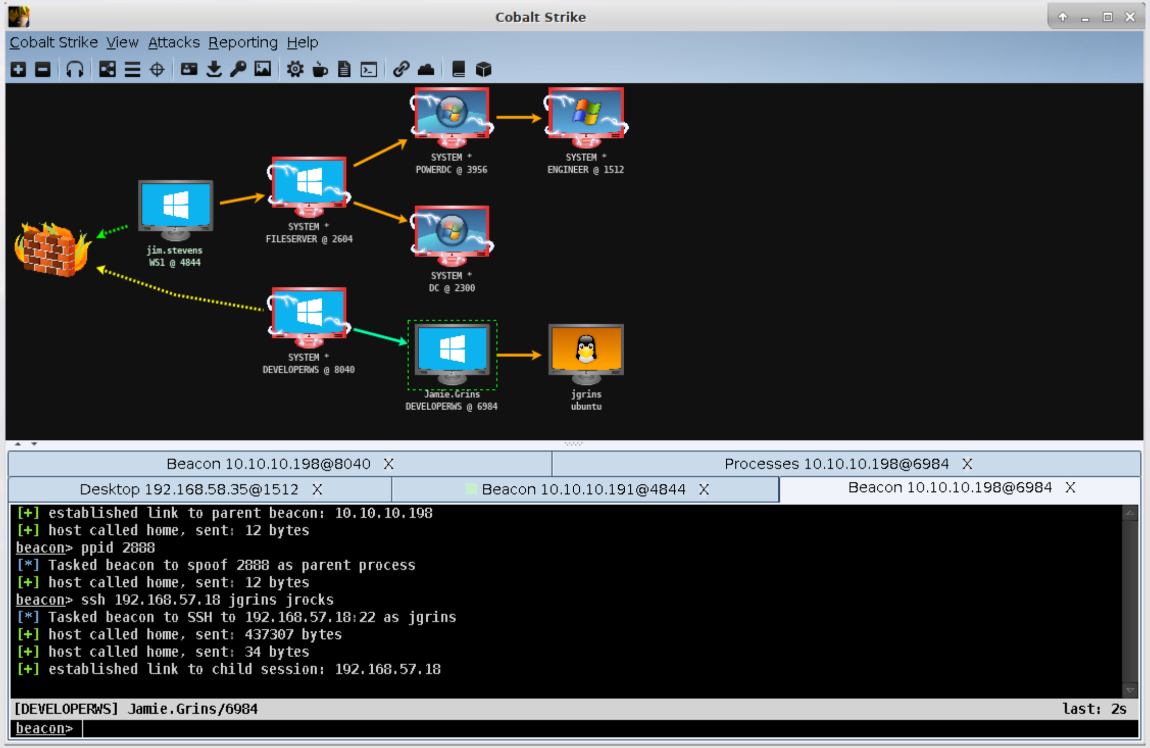
04
基于DMI的内存获取卡的内存取证
系统无感取证

01 当前APT攻击技术现状

无文件攻击已成为高级威胁常态

当前APT攻击技术现状——无文件攻击已成为高级威胁常态

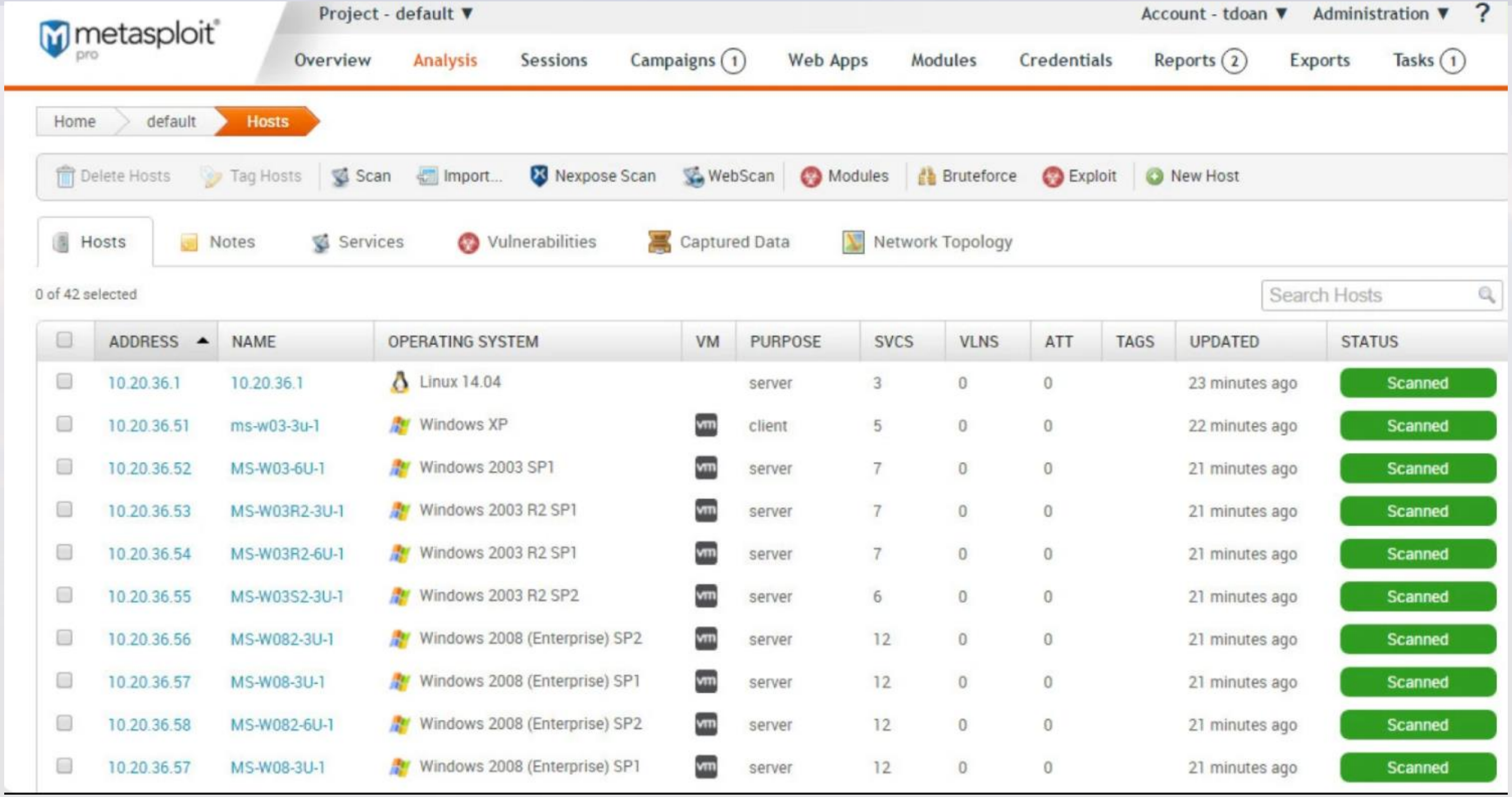

Sample B
脚本类型
内部包含base64加密过的数据
脚本1
脚本类型
内部包含base64加密过的数据
模块1
Shellcode下载模块2
C&C服务器1
模块2
Shellcode
创建挂起进程rundll32.exe
将模块3写入到rundll32内执行
模块3
Shellcode后门模块，连接C&C服务器等待命令
C&C服务器1、2



```
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2888
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18

[DEVELOPERWS] Jamie.Grins/6984                                   last: 2s
beacon>
```

APT-TOCS（又名海莲花）组织基于Cobalt Strike平台的攻击内存植入ShellCode

当前APT攻击技术现状——无文件攻击已成为高级威胁常态

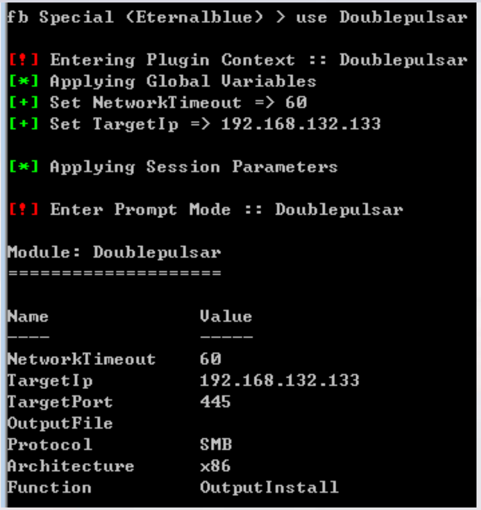


0 of 42 selected

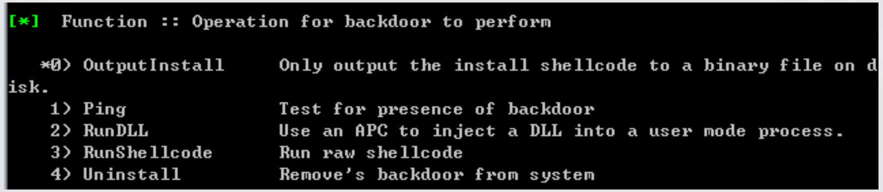
□	ADDRESS ▲	NAME	OPERATING SYSTEM	VM	PURPOSE	SVCS	VLNS	ATT	TAGS	UPDATED	STATUS
□	10.20.36.1	10.20.36.1	Linux 14.04		server	3	0	0		23 minutes ago	Scanned
□	10.20.36.51	ms-w03-3u-1	Windows XP	vm	client	5	0	0		22 minutes ago	Scanned
□	10.20.36.52	MS-W03-6U-1	Windows 2003 SP1	vm	server	7	0	0		21 minutes ago	Scanned
□	10.20.36.53	MS-W03R2-3U-1	Windows 2003 R2 SP1	vm	server	7	0	0		21 minutes ago	Scanned
□	10.20.36.54	MS-W03R2-6U-1	Windows 2003 R2 SP1	vm	server	7	0	0		21 minutes ago	Scanned
□	10.20.36.55	MS-W03S2-3U-1	Windows 2003 R2 SP2	vm	server	6	0	0		21 minutes ago	Scanned
□	10.20.36.56	MS-W082-3U-1	Windows 2008 (Enterprise) SP2	vm	server	12	0	0		21 minutes ago	Scanned
□	10.20.36.57	MS-W08-3U-1	Windows 2008 (Enterprise) SP1	vm	server	12	0	0		21 minutes ago	Scanned
□	10.20.36.58	MS-W082-6U-1	Windows 2008 (Enterprise) SP2	vm	server	12	0	0		21 minutes ago	Scanned
□	10.20.36.57	MS-W08-3U-1	Windows 2008 (Enterprise) SP1	vm	server	12	0	0		21 minutes ago	Scanned

Metasploit pro 同样支持无文件攻击

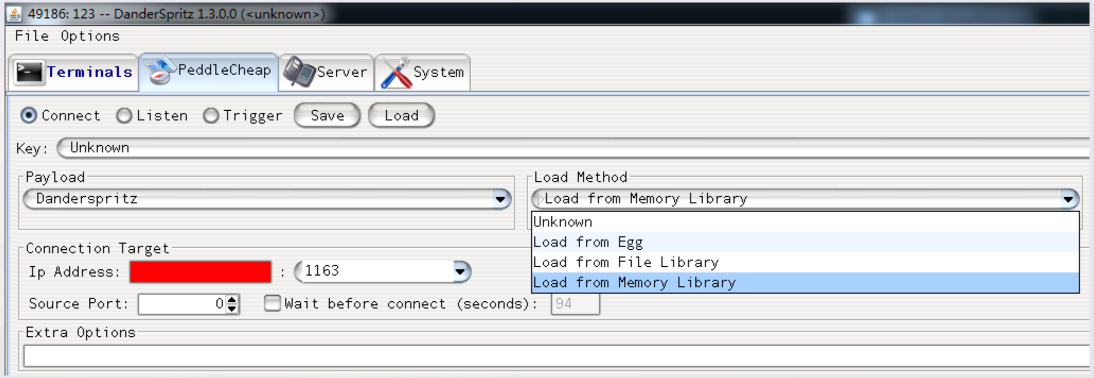
当前APT攻击技术现状——无文件攻击已成为高级威胁常态



```
fb Special (Eternalblue) > use Doublepulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.132.133

[*] Applying Session Parameters

[!] Enter Prompt Mode :: Doublepulsar

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

Name                Value
----                -----
NetworkTimeout      60
TargetIp            192.168.132.133
TargetPort          445
OutputFile
Protocol            SMB
Architecture        x86
Function            OutputInstall
```



```
[*]  Function :: Operation for backdoor to perform

   *0) OutputInstall     Only output the install shellcode to a binary file on d
isk.
    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
```



● Connect ○ Listen ○ Trigger Save Load

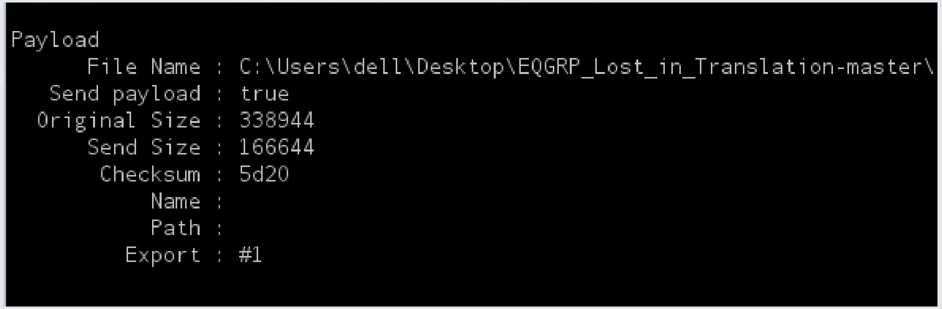
Key: Unknown

Payload: Danderspritz

Load Method: Load from Memory Library
- Unknown
- Load from Egg
- Load from File Library
- Load from Memory Library

Connection Target
Ip Address: [redacted] : 1163
Source Port: 0 □ Wait before connect (seconds): 94

Extra Options



```
Payload
      File Name : C:\Users\dell\Desktop\EQGRP_Lost_in_Translation-master\
   Send payload : true
  Original Size : 338944
      Send Size : 166644
       Checksum : 5d20
           Name :
           Path :
         Export : #1
```

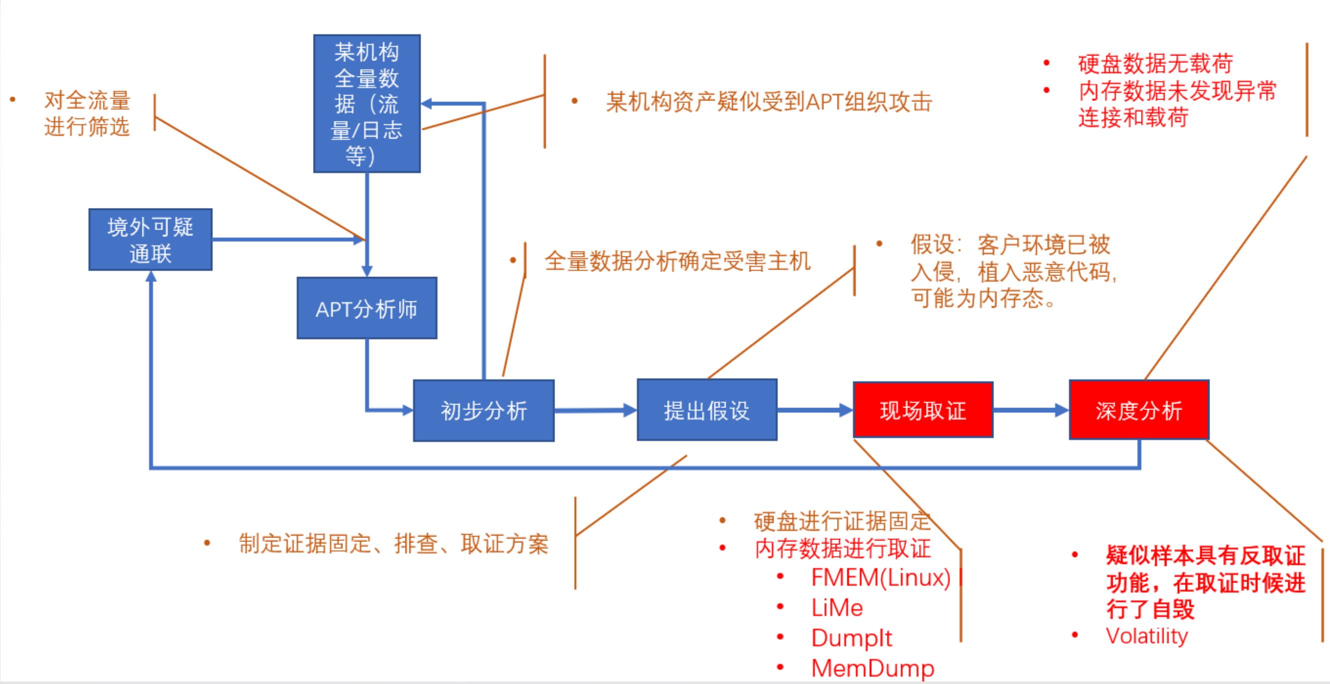
方程式组织基于Fuzzbunch平台的攻击内存APC方式植入DLL

DanderSpritz平台PeddleCheap插件可以在连接时验证载荷加载方式

02 对APT攻击取证的难点

反取证技术被普遍使用

对APT攻击取证的难点——反取证技术被普遍使用



- 对全流量进行筛选
- 某机构资产疑似受到APT组织攻击
- 硬盘数据无载荷
- 内存数据未发现异常连接和载荷

某机构全量数据（流量/日志等）

境外可疑通联

APT分析师

- 全量数据分析确定受害主机
- 假设：客户环境已被入侵，植入恶意代码，可能为内存态。

初步分析

提出假设

现场取证

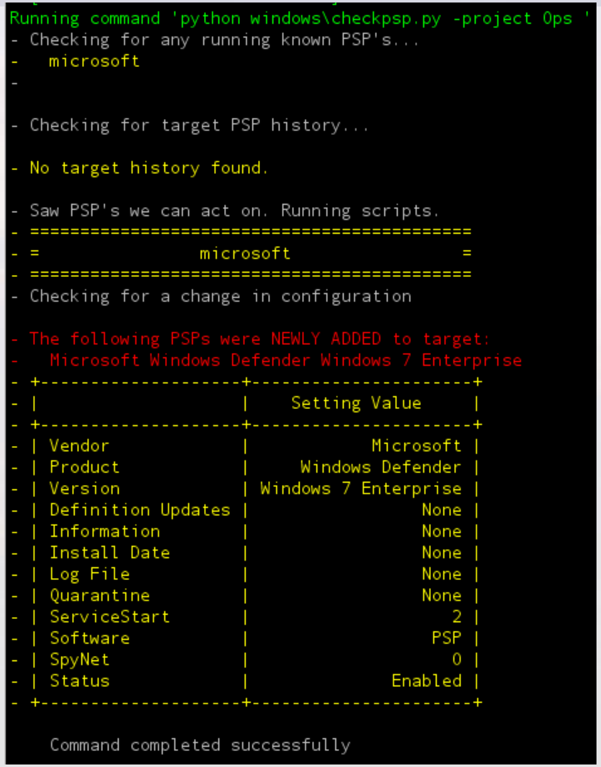
深度分析

- 制定证据固定、排查、取证方案
- 硬盘进行证据固定
- 内存数据进行取证
  - FMEM(Linux)
  - LiMe
  - DumpIt
  - MemDump
- **疑似样本具有反取证功能，在取证时候进行了自毁**
- Volatility

某攻击事件发现及取证分析流程

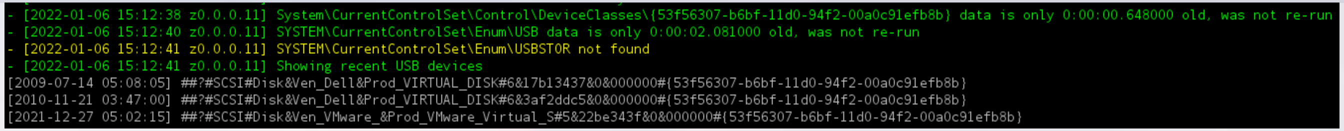
- 通过流量数据发现异常网络连接，排查定位主机取证；
- 对异常主机分别使用多款取证工具进行内存取证；
- 对取证后的内存分均未发先恶意代码和网络连接数据；
- 通过后续分析发现攻击代码存在反取证自毁功能。

对APT攻击取证的难点——反取证技术被普遍使用



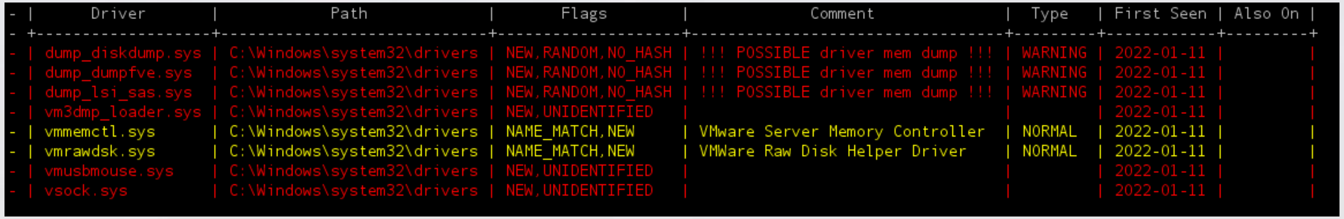
```
Running command 'python windows\checkpsp.py -project Ops '
- Checking for any running known PSP's...
-   microsoft
-

- 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 Enterprise
- +--------------------+---------------------+
- |                    |    Setting Value    |
- +--------------------+---------------------+
- | Vendor             |           Microsoft |
- | Product            |    Windows Defender |
- | Version            | Windows 7 Enterprise |
- | Definition Updates |                None |
- | Information        |                None |
- | Install Date       |                None |
- | Log File           |                None |
- | Quarantine         |                None |
- | ServiceStart       |                   2 |
- | Software           |                 PSP |
- | SpyNet             |                   0 |
- | Status             |             Enabled |
- +--------------------+---------------------+

    Command completed successfully
```

DanderSpirtz载荷检查反病毒软件



```
- [2022-01-06 15:12:38 z0.0.0.11] System\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b} data is only 0:00:00.648000 old, was not re-run
- [2022-01-06 15:12:40 z0.0.0.11] SYSTEM\CurrentControlSet\Enum\USB data is only 0:00:02.081000 old, was not re-run
- [2022-01-06 15:12:41 z0.0.0.11] SYSTEM\CurrentControlSet\Enum\USBSTOR not found
- [2022-01-06 15:12:41 z0.0.0.11] Showing recent USB devices
[2009-07-14 05:08:05] ##?#SCSI#Disk&Ven_Dell&Prod_VIRTUAL_DISK#6&17b13437&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
[2010-11-21 03:47:00] ##?#SCSI#Disk&Ven_Dell&Prod_VIRTUAL_DISK#6&3af2ddc5&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
[2021-12-27 05:02:15] ##?#SCSI#Disk&Ven_VMware_&Prod_VMware_Virtual_S#5&22be343f&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
```

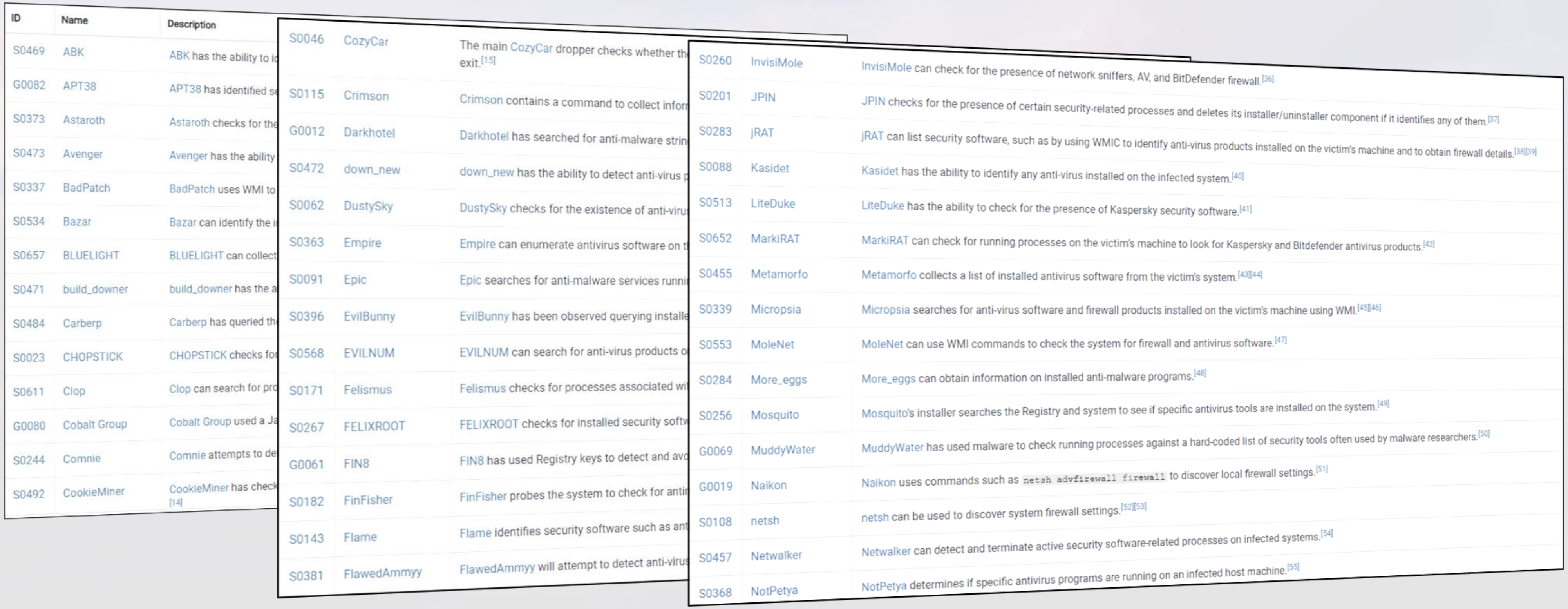
DanderSpirtz载荷可移动设备检测



```
- |       Driver       |             Path              |       Flags        |            Comment             |   Type   | First Seen | Also On |
- +--------------------+-------------------------------+--------------------+--------------------------------+----------+------------+---------+
- | dump_diskdump.sys  | C:\Windows\system32\drivers | NEW,RANDOM,NO_HASH | !!! POSSIBLE driver mem dump !!! | WARNING | 2022-01-11 |         |
- | dump_dumpfve.sys   | C:\Windows\system32\drivers | NEW,RANDOM,NO_HASH | !!! POSSIBLE driver mem dump !!! | WARNING | 2022-01-11 |         |
- | dump_lsi_sas.sys   | C:\Windows\system32\drivers | NEW,RANDOM,NO_HASH | !!! POSSIBLE driver mem dump !!! | WARNING | 2022-01-11 |         |
- | vm3dmp_loader.sys  | C:\Windows\system32\drivers | NEW,UNIDENTIFIED   |                                  |         | 2022-01-11 |         |
- | vmmemctl.sys       | C:\Windows\system32\drivers | NAME_MATCH,NEW     | VMware Server Memory Controller  | NORMAL  | 2022-01-11 |         |
- | vmrawdsk.sys       | C:\Windows\system32\drivers | NAME_MATCH,NEW     | VMWare Raw Disk Helper Driver    | NORMAL  | 2022-01-11 |         |
- | vmusbmouse.sys     | C:\Windows\system32\drivers | NEW,UNIDENTIFIED   |                                  |         | 2022-01-11 |         |
- | vsock.sys          | C:\Windows\system32\drivers | NEW,UNIDENTIFIED   |                                  |         | 2022-01-11 |         |
```

DanderSpirtz载荷内存转储驱动检测

对APT攻击取证的难点——反取证技术被普遍使用



ID	Name	Description
S0469	ABK	ABK has the ability to id
G0082	APT38	APT38 has identified se
S0373	Astaroth	Astaroth checks for the
S0473	Avenger	Avenger has the ability
S0337	BadPatch	BadPatch uses WMI to
S0534	Bazar	Bazar can identify the i
S0657	BLUELIGHT	BLUELIGHT can collect
S0471	build_downer	build_downer has the a
S0484	Carberp	Carberp has queried the
S0023	CHOPSTICK	CHOPSTICK checks for
S0611	Clop	Clop can search for pro
G0080	Cobalt Group	Cobalt Group used a Ja
S0244	Comnie	Comnie attempts to de
S0492	CookieMiner	CookieMiner has check [14]

S0046	CozyCar	The main CozyCar dropper checks whether th exit.[15]
S0115	Crimson	Crimson contains a command to collect infor
G0012	Darkhotel	Darkhotel has searched for anti-malware strin
S0472	down_new	down_new has the ability to detect anti-virus p
S0062	DustySky	DustySky checks for the existence of anti-virus
S0363	Empire	Empire can enumerate antivirus software on t
S0091	Epic	Epic searches for anti-malware services runni
S0396	EvilBunny	EvilBunny has been observed querying installe
S0568	EVILNUM	EVILNUM can search for anti-virus products o
S0171	Felismus	Felismus checks for processes associated wi
S0267	FELIXROOT	FELIXROOT checks for installed security softw
G0061	FIN8	FIN8 has used Registry keys to detect and avo
S0182	FinFisher	FinFisher probes the system to check for antin
S0143	Flame	Flame identifies security software such as ant
S0381	FlawedAmmyy	FlawedAmmyy will attempt to detect anti-virus

S0260	InvisiMole	InvisiMole can check for the presence of network sniffers, AV, and BitDefender firewall.[36]
S0201	JPIN	JPIN checks for the presence of certain security-related processes and deletes its installer/uninstaller component if it identifies any of them.[37]
S0283	jRAT	jRAT can list security software, such as by using WMIC to identify anti-virus products installed on the victim's machine and to obtain firewall details.[38][39]
S0088	Kasidet	Kasidet has the ability to identify any anti-virus installed on the infected system.[40]
S0513	LiteDuke	LiteDuke has the ability to check for the presence of Kaspersky security software.[41]
S0652	MarkiRAT	MarkiRAT can check for running processes on the victim's machine to look for Kaspersky and Bitdefender antivirus products.[42]
S0455	Metamorfo	Metamorfo collects a list of installed antivirus software from the victim's system.[43][44]
S0339	Micropsia	Micropsia searches for anti-virus software and firewall products installed on the victim's machine using WMI.[45][46]
S0553	MoleNet	MoleNet can use WMI commands to check the system for firewall and antivirus software.[47]
S0284	More_eggs	More_eggs can obtain information on installed anti-malware programs.[48]
S0256	Mosquito	Mosquito's installer searches the Registry and system to see if specific antivirus tools are installed on the system.[49]
G0069	MuddyWater	MuddyWater has used malware to check running processes against a hard-coded list of security tools often used by malware researchers.[50]
G0019	Naikon	Naikon uses commands such as `netsh advfirewall firewall` to discover local firewall settings.[51]
S0108	netsh	netsh can be used to discover system firewall settings.[52][53]
S0457	Netwalker	Netwalker can detect and terminate active security software-related processes on infected systems.[54]
S0368	NotPetya	NotPetya determines if specific antivirus programs are running on an infected host machine.[55]

ATT&CK收录的使用技术点T1518/001（安全软件发现）的恶意样本

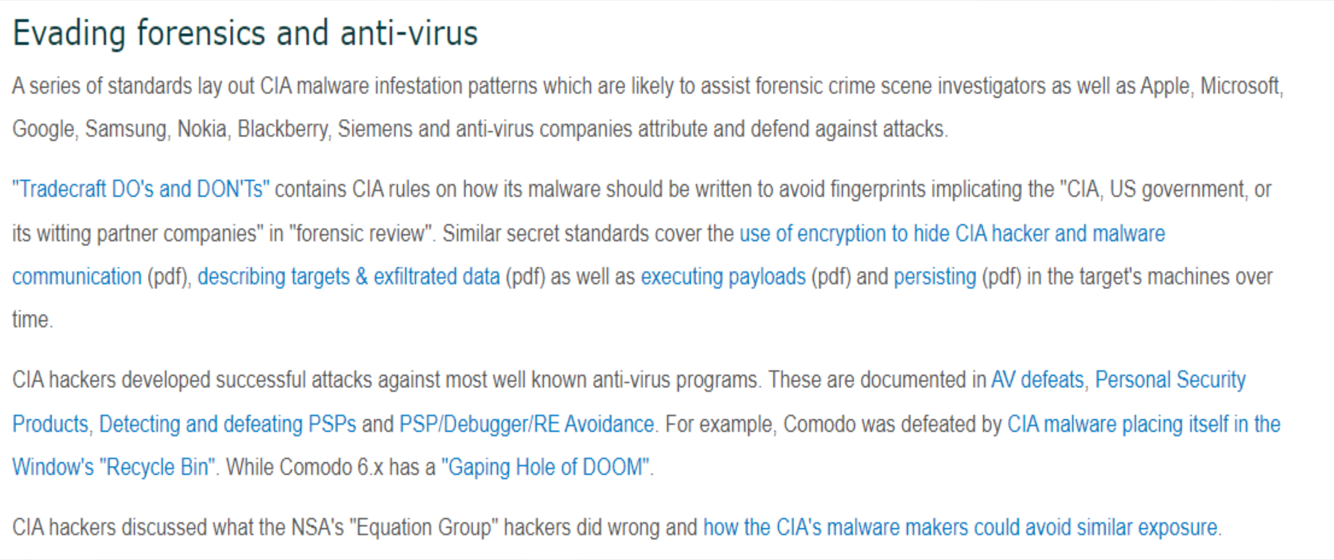
对APT攻击取证的难点——反取证技术被普遍使用

1.数据隐藏

2.资料抹除

3.痕迹混淆

4.工具对抗



Evading forensics and anti-virus

A series of standards lay out CIA malware infestation patterns which are likely to assist forensic crime scene investigators as well as Apple, Microsoft, Google, Samsung, Nokia, Blackberry, Siemens and anti-virus companies attribute and defend against attacks.

"Tradecraft DO's and DON'Ts" contains CIA rules on how its malware should be written to avoid fingerprints implicating the "CIA, US government, or its witting partner companies" in "forensic review". Similar secret standards cover the use of encryption to hide CIA hacker and malware communication (pdf), describing targets & exfiltrated data (pdf) as well as executing payloads (pdf) and persisting (pdf) in the target's machines over time.

CIA hackers developed successful attacks against most well known anti-virus programs. These are documented in AV defeats, Personal Security Products, Detecting and defeating PSPs and PSP/Debugger/RE Avoidance. For example, Comodo was defeated by CIA malware placing itself in the Window's "Recycle Bin". While Comodo 6.x has a "Gaping Hole of DOOM".

CIA hackers discussed what the NSA's "Equation Group" hackers did wrong and how the CIA's malware makers could avoid similar exposure.

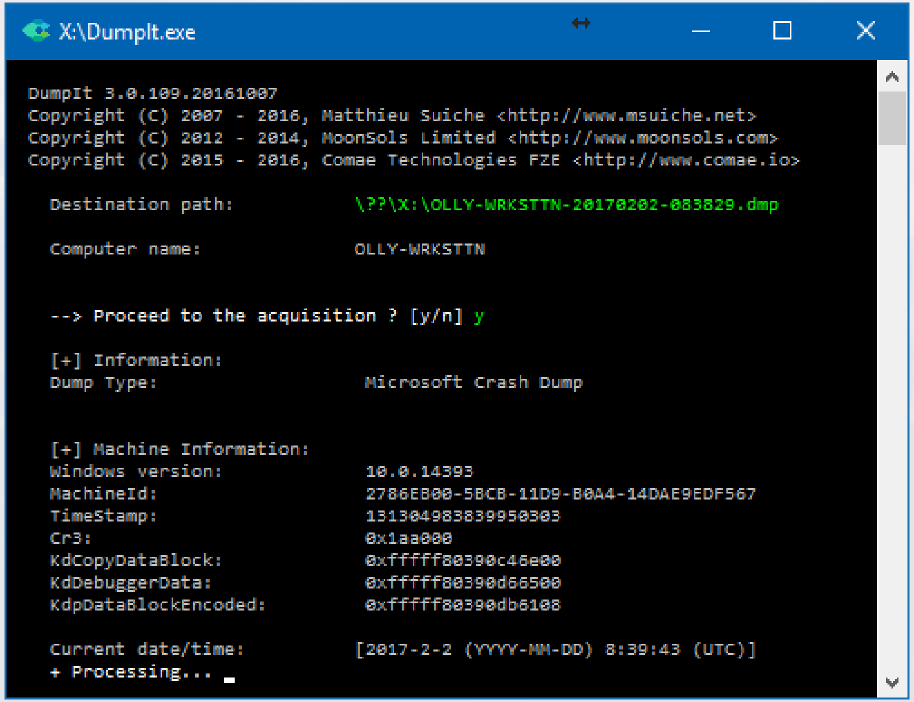
维基解密泄露CIA七号军火库资料显示美方反取证研究资料

03 对易失介质取证的探索

已有技术情况

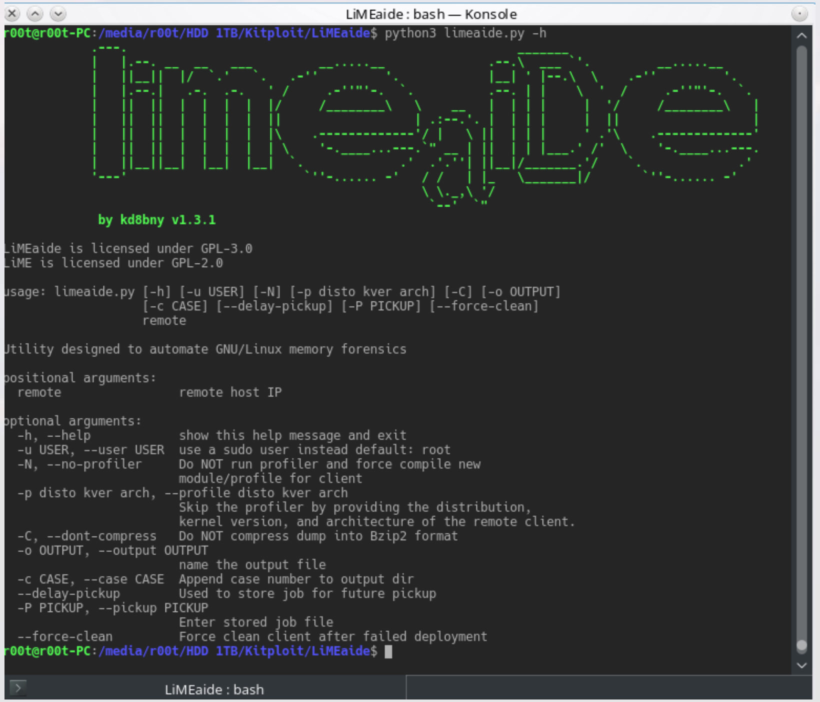
对易失介质取证的探索——已有技术情况

1、内存转储软件



```
DumpIt 3.0.109.20161007
Copyright (C) 2007 - 2016, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2016, Comae Technologies FZE <http://www.comae.io>

  Destination path:           \??\X:\OLLY-WRKSTTN-20170202-083829.dmp

  Computer name:              OLLY-WRKSTTN


  --> Proceed to the acquisition ? [y/n] y

  [+] Information:
  Dump Type:                   Microsoft Crash Dump


  [+] Machine Information:
  Windows version:             10.0.14393
  MachineId:                   2786EB00-5BCB-11D9-B0A4-14DAE9EDF567
  TimeStamp:                   131304983839950303
  Cr3:                         0x1aa000
  KdCopyDataBlock:             0xfffff80390c46e00
  KdDebuggerData:              0xfffff80390d66500
  KdpDataBlockEncoded:         0xfffff80390db6108

  Current date/time:          [2017-2-2 (YYYY-MM-DD) 8:39:43 (UTC)]
  + Processing... _
```

Windows主机使用DumpIt内存取证



```
r00t@r00t-PC:/media/r00t/HDD 1TB/Kitploit/LiMEaide$ python3 limeaide.py -h

            by kd8bny v1.3.1

LiMEaide is licensed under GPL-3.0
LiME is licensed under GPL-2.0

usage: limeaide.py [-h] [-u USER] [-N] [-p disto kver arch] [-C] [-o OUTPUT]
                   [-c CASE] [--delay-pickup] [-P PICKUP] [--force-clean]
                   remote

Utility designed to automate GNU/Linux memory forensics

positional arguments:
  remote                remote host IP

optional arguments:
  -h, --help            show this help message and exit
  -u USER, --user USER  use a sudo user instead default: root
  -N, --no-profiler     Do NOT run profiler and force compile new
                        module/profile for client
  -p disto kver arch, --profile disto kver arch
                        Skip the profiler by providing the distribution,
                        kernel version, and architecture of the remote client.
  -C, --dont-compress   Do NOT compress dump into Bzip2 format
  -o OUTPUT, --output OUTPUT
                        name the output file
  -c CASE, --case CASE  Append case number to output dir
  --delay-pickup        Used to store job for future pickup
  -P PICKUP, --pickup PICKUP
                        Enter stored job file
  --force-clean         Force clean client after failed deployment
r00t@r00t-PC:/media/r00t/HDD 1TB/Kitploit/LiMEaide$ 
```

Linux主机使用LiMe内存取证

对易失介质取证的探索——已有技术情况

Windows：

MAGNET RAM Capture

MDD

Process Hacker

Winen

Forensic Toolkit

WinPmem

MANDIANT Memoryze

WindowsSCOPE

……

Mac Os：

Goldfish

Mac Memory Reader

OSXPMem

……

Linux：

LiME

Linux Memory Grabber

Fmem

……

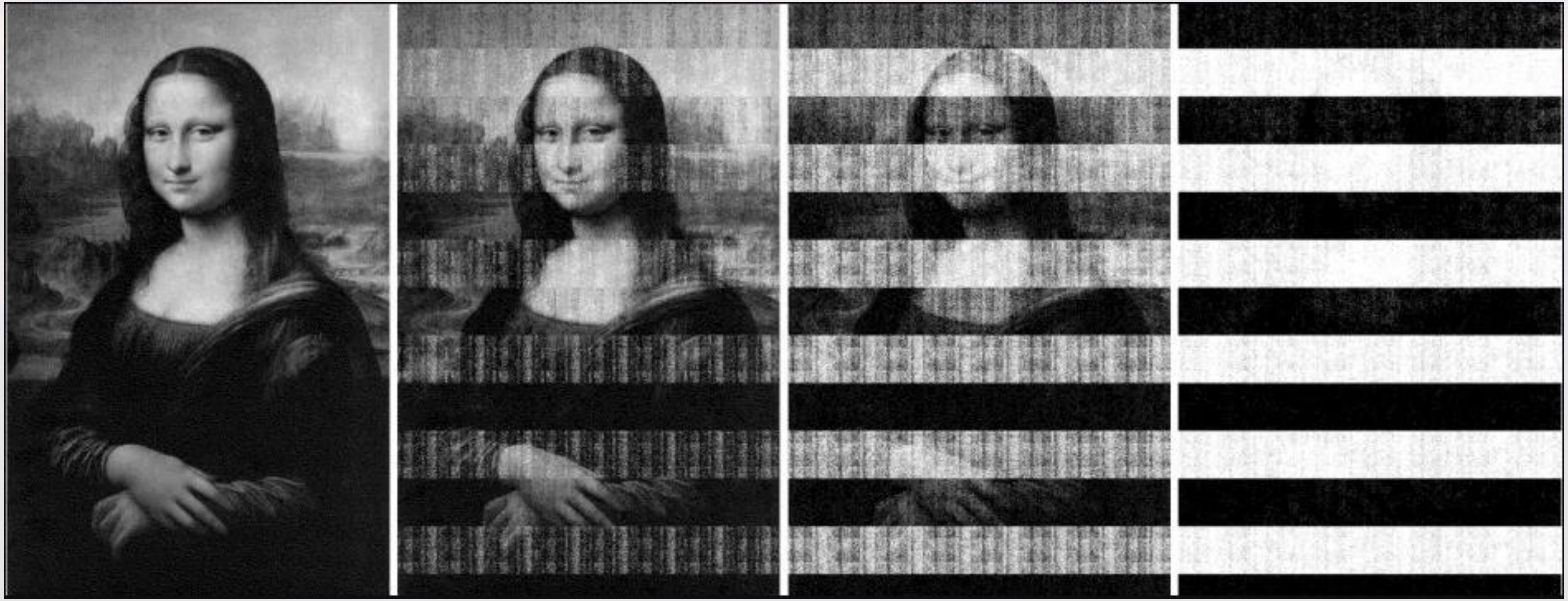
对易失介质取证的探索——已有技术情况

- 高级攻击都针对软件取证进行了对抗，因此存在取证软件无法获取攻击代码的情况。因此需要不依赖操作系统，进行取证的方案。

低温断电内存取证

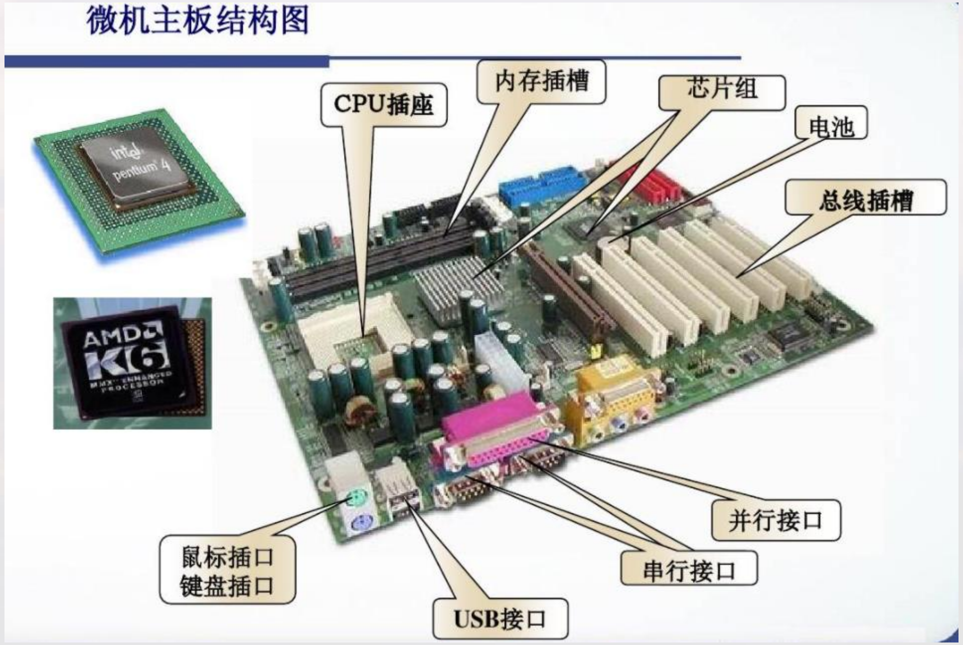
对易失介质取证的探索——已有技术情况

1、内存断电取证



低温情况下断电5秒/断电30秒/断电60秒/断电5分钟内存取证数据恢复情况

对易失介质取证的探索——已有技术情况



各类外设接口设备取证

04

基于DMI的内存获取卡的内存取证

系统无感取证

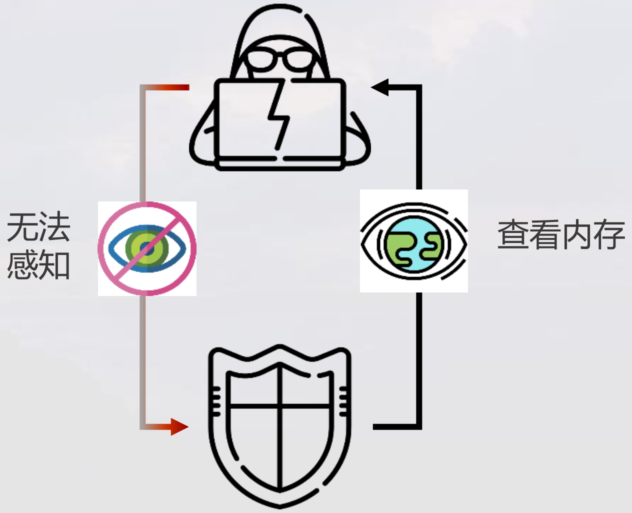
基于DMI的内存获取卡的内存取证——系统无感取证

网络攻防核心是控制权的争夺，以获取数据或控制系统为目标

基于DMI的内存获取卡的内存取证——系统无感取证

系统权限争夺

在当前高烈度的安全对抗场景下，攻守双方以争夺关键节点操作系统的控制权限为主要目标，由于攻击方手段多样，如何获得比攻击方更高的权限成为防御方研究的一个重要领域

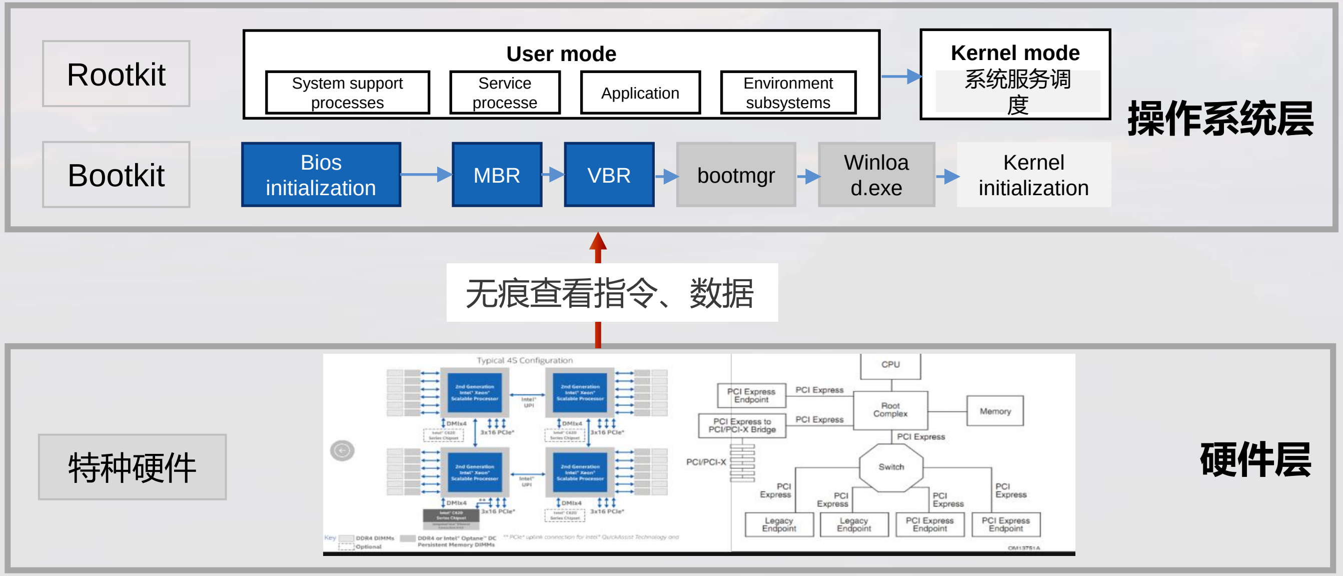


防御方

基于DMI的内存获取卡的内存取证——系统无感取证

攻防状态下的视角

在没有载荷的情况下**无痕读取内存、不受攻击代码干扰**，使攻击方无感知，从而吸引捕获载荷，应用于和的高烈度对抗场景



Rootkit

User mode

System support processes

Service processe

Application

Environment subsystems

Kernel mode

系统服务调度

Bootkit

Bios initialization

MBR

VBR

bootmgr

Winload.exe

Kernel initialization

操作系统层

无痕查看指令、数据

特种硬件

硬件层

Typical 4S Configuration
2nd Generation Intel® Xeon® Scalable Processor
Intel® UPI
DMIx4
3x16 PCIe*
Intel® C620 Series Chipset
Key
DDR4 DIMMs
Optional
DDR4 or Intel® Optane™ DC Persistent Memory DIMMs
** PCIe* uplink connection for Intel® QuickAssist Technology and
CPU
PCI Express Endpoint
PCI Express
Root Complex
Memory
PCI Express to PCI/PCI-X Bridge
PCI/PCI-X
Switch
Legacy Endpoint
PCI Express Endpoint
OM13751A

基于DMI的内存获取卡的内存取证——系统无感取证

内置安全引擎模块，TDU芯片+内存获取卡组合本地检查和处置

提供网卡接口，通过网口进行远程控制，集中完成物理内存全空间的检查和处置

技术发展方向

定义内存访问的硬件和软件接口协议，向第三方安全解决方案提供数据和操作机制，建立基于物理内存访问的安全产品生态

其他 ?

谢谢大家

安天冬训营 wtc.antiy.cn