2024.07.31

初探威脅情資的奧秘

(下)

Tako

TEAMT5
杜浦數位安全
Persistent Cyber Threat Hunters

$Whoami

- Tako
- Threat Intelligence Researcher @ TeamT5
- AIS3 2016~2018
    - 臺灣好厲駭第一屆
- Speaker: Code Blue, JSAC

AGENDA

TEAMT5
杜浦數位安全

01 Lab

02 Malware Analysis - Again

03 Threat Intelligence

04 Q & A

在開始之前...

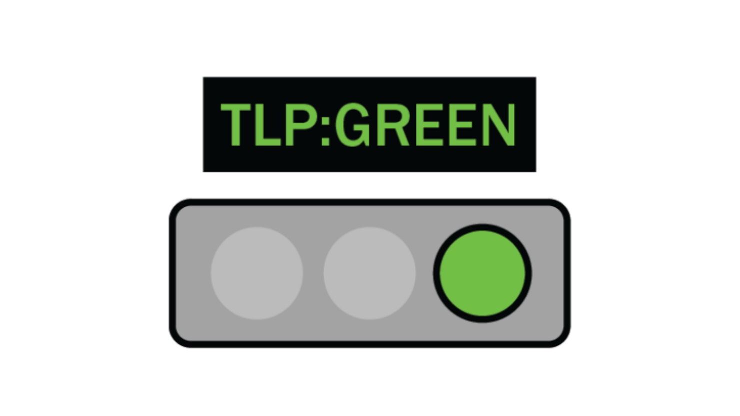
- 麻煩確認以下工具是不是有裝好在分析的VM裡
  - Hex Editor:
    - HxD, WinHex, 010Editor, ...
  - Detect It Easy
    - https://github.com/horsicq/Detect-It-Easy
  - decompiler:
    - Ida pro/Ghidra
  - x64dbg
    - https://x64dbg.com/
  - Sysinternals Suite:
    - Process Monitor, AutoRuns, Process Explorer (只會用到這3個)

在開始之前...

- 簡報檔案跟惡意程式樣本
  - URL: https://shorturl.at/G7uJh
- 簡報檔案解壓縮密碼: AIS3@2024_1
- 惡意程式樣本解壓縮密碼: AIS3@2024_2

TLP Lab

- 今日課程內容是屬於哪個TLP level？
  - Tips: AIS3



Disclaimer

- All the samples are real malwares, please …
  - do not share these samples to other people
  - do not upload samples to online sandbox
  - just execute the samples in VM env.

Lab

- Sample
  - USOPrivate.exe (MD5: adc1463af9514ac48cd963385f08c40f)
- What malware are we dealing with?
- What are some of the known Indicator of Compromise (IoCs)?
  - Hash
  - Domain name
  - IP address
- What threat group is this particular malware associated with?

Lab

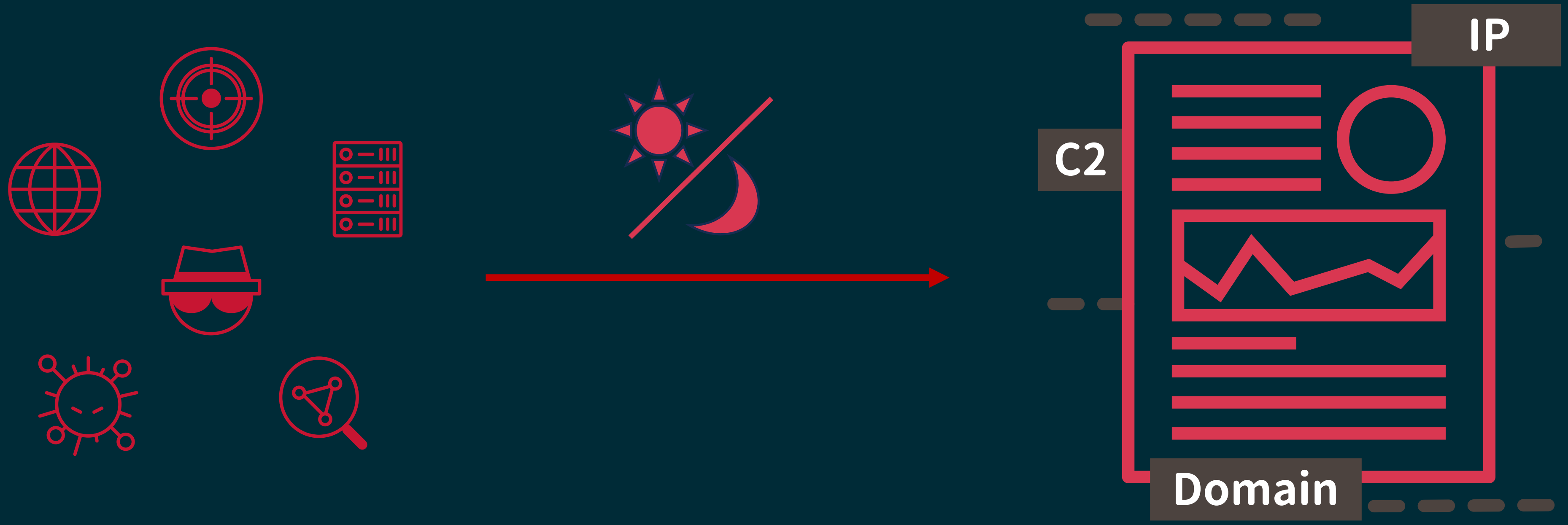
- Sample
  - USOPrivate.exe (MD5: adc1463af9514ac48cd963385f08c40f)
- What malware are we dealing with?
  - PlugX
- What are some of the known Indicator of Compromise (IoCs)?
  - Hash:
    - 1cf26c4edf92541cee6dcb327a15ab97, 1a62834b9f2423effb90e133141b1f05
  - Domain name
    - fuckeryoumm.nmb.bet, helloword.daj8.me, …
  - IP address
    - 18.138.107.235, 52.76.217.82, …
- What threat group is this particular malware associated with?
  - Earth Berberoka / DirtyFuxi

What if there's no related report ?

Lab

- Sample
  - USOPrivate.exe (MD5: adc1463af9514ac48cd963385f08c40f)
- What malware are we dealing with?
  - PlugX
- What are some of the known Indicator of Compromise (IoCs)?
  - Hash:
    - 1cf26c4edf92541cee6dcb327a15ab97, 1a62834b9f2423effb90e133141b1f05
  - Domain name
    - fuckeryoumm.nmb.bet, helloword.daj8.me, …
  - IP address
    - 18.138.107.235, 52.76.217.82, …

- What threat group is this particular malware associated with?
  - Earth Berberoka / DirtyFuxi


IP
C2
Domain

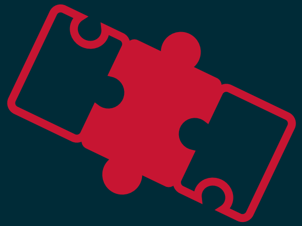
Unknown...

- What if there's so much unknown information ?
  - Unknown malware
    - no detection
    - no analyzed sample
  - Unknown C2
    - no sandbox
    - no connection

Malware Analysis - Again

Malware Analysis - Again

- Target
  - Figure out the information that you don't know yet
  - Verify the information that you have
  - Efficiently (?
- Keep in mind
  - 逆向只是過程 -- DuckLL



Malware Analysis - Again

Observation

Dynamic Analysis

Static Analysis

Malware Analysis

- Tools , lots of tools

Malware Analysis

Observation

Dynamic Analysis

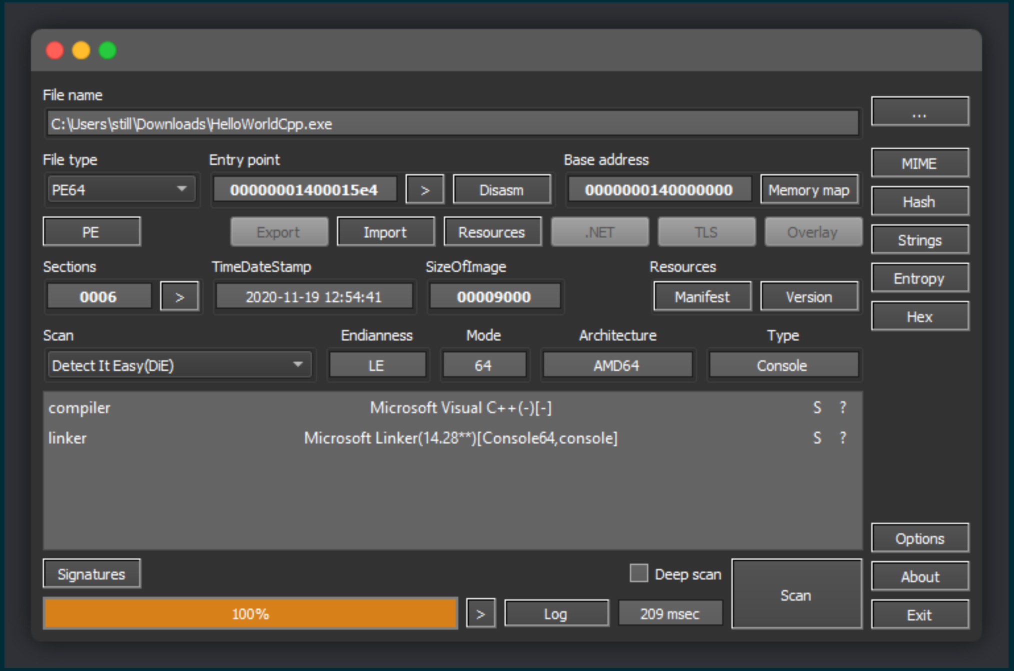
Static Analysis

Malware Analysis - Observation

- 惡意程式就像一盒巧克力，你永遠不知道下一個打開的是哪一種file types
- Tools
  - hex editor: 010 Editor, HxD, WinHex, ...
    - file magic/signature
    - script based malware, e.g. vbs, js, py, ...
    - human disassembler: shellcode (?
  - For PE: Detect it Easy, pestudio, PEbear, DnSpy(.NET)
  - For windows offices: oletools

Detect it Easy

- Swiss army knife for everything PE-related
  - File type
  - Base address
  - Compile info/Packer info
  - Quick hash calculation
  - Strings
  - Imports/Exports
  - Hexdump view
  - Resource view
  - And more!



File name: C:\Users\still\Downloads\HelloWorldCpp.exe

File type: PE64

Entry point: 00000001400015e4

Base address: 0000000140000000

Sections: 0006

TimeDateStamp: 2020-11-19 12:54:41

SizeOfImage: 00009000

Scan: Detect It Easy(DiE)

Endianness: LE

Mode: 64

Architecture: AMD64

Type: Console

```
compiler    Microsoft Visual C++(-)[-]                       S  ?
linker      Microsoft Linker(14.28**)[Console64,console]     S  ?
```

□ Deep scan

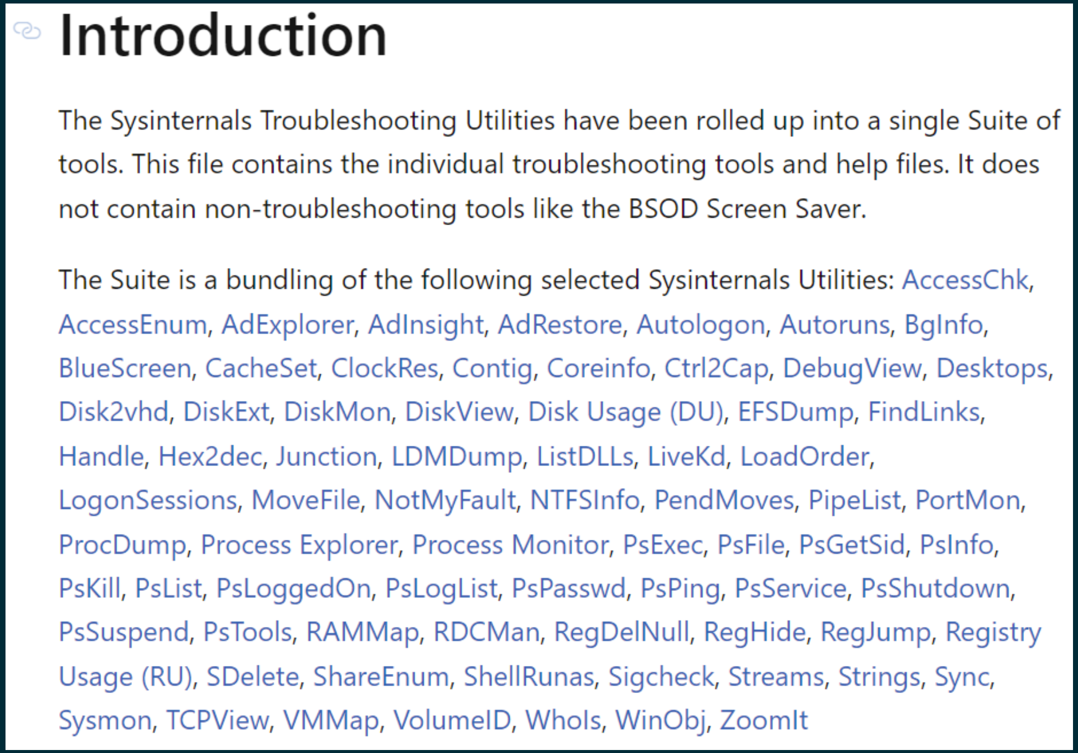
100%

209 msec

Now What ?

Sysinternals Suite

- Originally third-party, now acquired by Microsoft
- Contains a series of tools for system management and Windows debugging



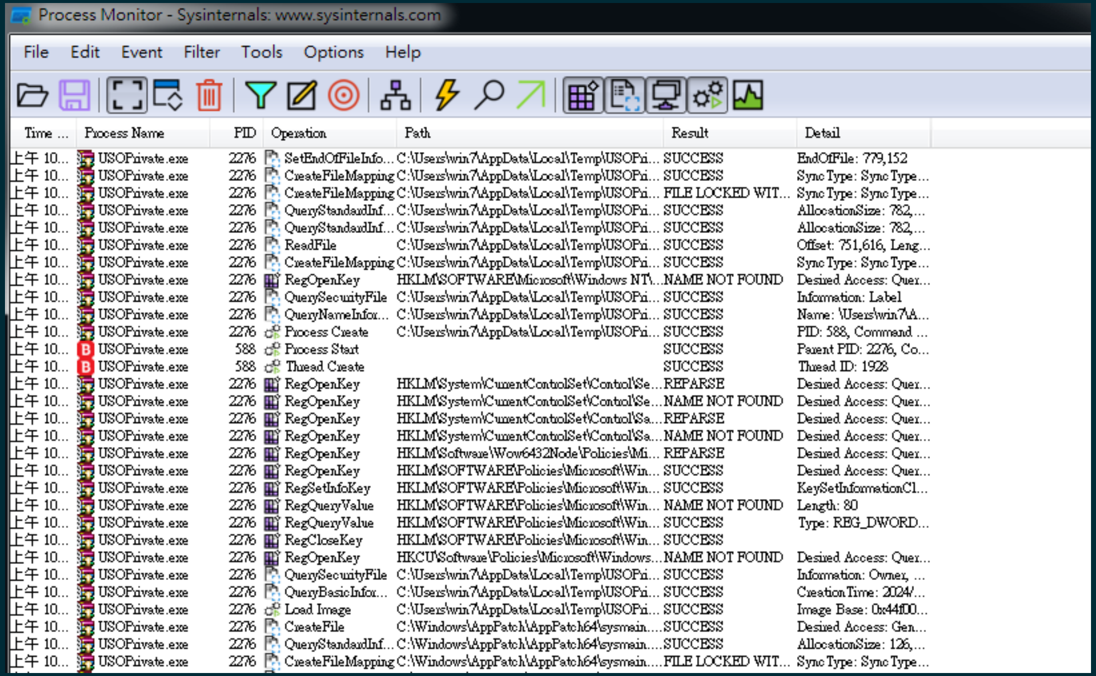
Introduction

The Sysinternals Troubleshooting Utilities have been rolled up into a single Suite of tools. This file contains the individual troubleshooting tools and help files. It does not contain non-troubleshooting tools like the BSOD Screen Saver.

The Suite is a bundling of the following selected Sysinternals Utilities: AccessChk, AccessEnum, AdExplorer, AdInsight, AdRestore, Autologon, Autoruns, BgInfo, BlueScreen, CacheSet, ClockRes, Contig, Coreinfo, Ctrl2Cap, DebugView, Desktops, Disk2vhd, DiskExt, DiskMon, DiskView, Disk Usage (DU), EFSDump, FindLinks, Handle, Hex2dec, Junction, LDMDump, ListDLLs, LiveKd, LoadOrder, LogonSessions, MoveFile, NotMyFault, NTFSInfo, PendMoves, PipeList, PortMon, ProcDump, Process Explorer, Process Monitor, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsList, PsLoggedOn, PsLogList, PsPasswd, PsPing, PsService, PsShutdown, PsSuspend, PsTools, RAMMap, RDCMan, RegDelNull, RegHide, RegJump, Registry Usage (RU), SDelete, ShareEnum, ShellRunas, Sigcheck, Streams, Strings, Sync, Sysmon, TCPView, VMMap, VolumeID, WhoIs, WinObj, ZoomIt

Process Monitor

- Advanced monitoring tool
  - File system
  - Registry
  - Network
  - process/thread
- Helps give a quick idea of what the malware will do upon startup



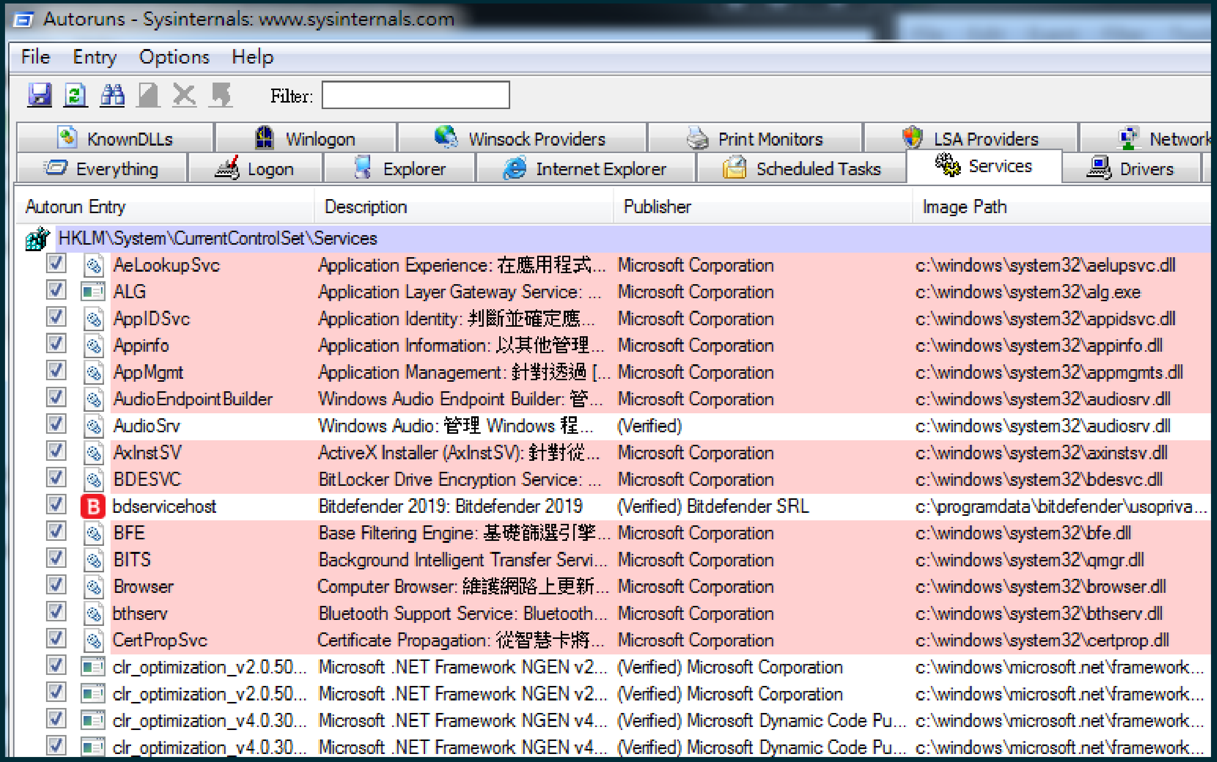
Time ...	Process Name	PID	Operation	Path	Result	Detail
上午 10...	USOPrivate.exe	2276	SetEndOfFileInfo...	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	EndOfFile: 779,152
上午 10...	USOPrivate.exe	2276	CreateFileMapping	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	SyncType: SyncType...
上午 10...	USOPrivate.exe	2276	CreateFileMapping	C:\Users\win7\AppData\Local\Temp\USOPri...	FILE LOCKED WIT...	SyncType: SyncType...
上午 10...	USOPrivate.exe	2276	QueryStandardInf...	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	AllocationSize: 782,...
上午 10...	USOPrivate.exe	2276	QueryStandardInf...	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	AllocationSize: 782,...
上午 10...	USOPrivate.exe	2276	ReadFile	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	Offset: 751,616, Leng...
上午 10...	USOPrivate.exe	2276	CreateFileMapping	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	SyncType: SyncType...
上午 10...	USOPrivate.exe	2276	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\...	NAME NOT FOUND	Desired Access: Quer...
上午 10...	USOPrivate.exe	2276	QuerySecurityFile	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	Information: Label
上午 10...	USOPrivate.exe	2276	QueryNameInfor...	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	Name: \Users\win7\A...
上午 10...	USOPrivate.exe	2276	Process Create	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	PID: 588, Command ...
上午 10...	USOPrivate.exe	588	Process Start		SUCCESS	Parent PID: 2276, Co...
上午 10...	USOPrivate.exe	588	Thread Create		SUCCESS	Thread ID: 1928
上午 10...	USOPrivate.exe	2276	RegOpenKey	HKLM\System\CurrentControlSet\Control\Se...	REPARSE	Desired Access: Quer...
上午 10...	USOPrivate.exe	2276	RegOpenKey	HKLM\System\CurrentControlSet\Control\Se...	NAME NOT FOUND	Desired Access: Quer...
上午 10...	USOPrivate.exe	2276	RegOpenKey	HKLM\System\CurrentControlSet\Control\Sa...	REPARSE	Desired Access: Quer...
上午 10...	USOPrivate.exe	2276	RegOpenKey	HKLM\System\CurrentControlSet\Control\Sa...	NAME NOT FOUND	Desired Access: Quer...
上午 10...	USOPrivate.exe	2276	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Mi...	REPARSE	Desired Access: Quer...
上午 10...	USOPrivate.exe	2276	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Win...	SUCCESS	Desired Access: Quer...
上午 10...	USOPrivate.exe	2276	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Win...	SUCCESS	KeySetInformationCl...
上午 10...	USOPrivate.exe	2276	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Win...	NAME NOT FOUND	Length: 80
上午 10...	USOPrivate.exe	2276	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Win...	SUCCESS	Type: REG_DWORD...
上午 10...	USOPrivate.exe	2276	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Win...	SUCCESS	
上午 10...	USOPrivate.exe	2276	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows...	NAME NOT FOUND	Desired Access: Quer...
上午 10...	USOPrivate.exe	2276	QuerySecurityFile	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	Information: Owner, ...
上午 10...	USOPrivate.exe	2276	QueryBasicInfor...	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	CreationTime: 2024/...
上午 10...	USOPrivate.exe	2276	Load Image	C:\Users\win7\AppData\Local\Temp\USOPri...	SUCCESS	Image Base: 0x44f00...
上午 10...	USOPrivate.exe	2276	CreateFile	C:\Windows\AppPatch\AppPatch64\sysmain....	SUCCESS	Desired Access: Gen...
上午 10...	USOPrivate.exe	2276	QueryStandardInf...	C:\Windows\AppPatch\AppPatch64\sysmain....	SUCCESS	AllocationSize: 126,...
上午 10...	USOPrivate.exe	2276	CreateFileMapping	C:\Windows\AppPatch\AppPatch64\sysmain....	FILE LOCKED WIT...	SyncType: SyncType...

Process Monitor

Demo

AutoRuns

- Quick overview of the existing persistence entries on the machine.



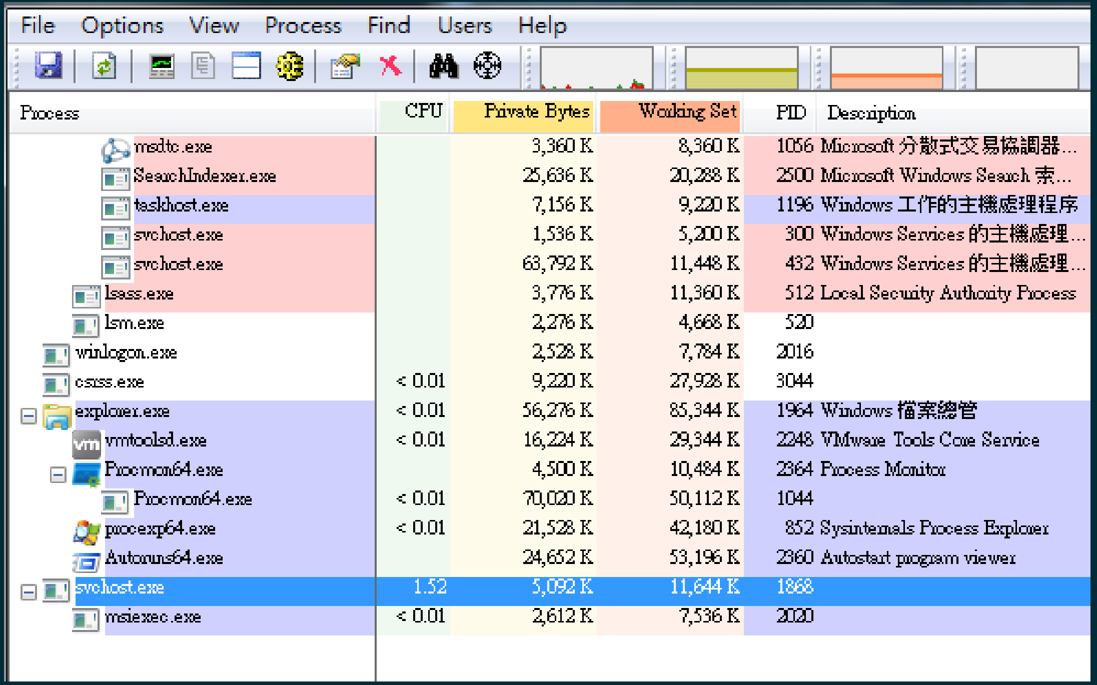
Autorun Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Services			
☑ AeLookupSvc	Application Experience: 在應用程式...	Microsoft Corporation	c:\windows\system32\aelupsvc.dll
☑ ALG	Application Layer Gateway Service: ...	Microsoft Corporation	c:\windows\system32\alg.exe
☑ AppIDSvc	Application Identity: 判斷並確定應...	Microsoft Corporation	c:\windows\system32\appidsvc.dll
☑ Appinfo	Application Information: 以其他管理...	Microsoft Corporation	c:\windows\system32\appinfo.dll
☑ AppMgmt	Application Management: 針對透過 [...	Microsoft Corporation	c:\windows\system32\appmgmts.dll
☑ AudioEndpointBuilder	Windows Audio Endpoint Builder: 管...	Microsoft Corporation	c:\windows\system32\audiosrv.dll
☑ AudioSrv	Windows Audio: 管理 Windows 程...	(Verified)	c:\windows\system32\audiosrv.dll
☑ AxInstSV	ActiveX Installer (AxInstSV): 針對從...	Microsoft Corporation	c:\windows\system32\axinstsv.dll
☑ BDESVC	BitLocker Drive Encryption Service: ...	Microsoft Corporation	c:\windows\system32\bdesvc.dll
☑ bdservicehost	Bitdefender 2019: Bitdefender 2019	(Verified) Bitdefender SRL	c:\programdata\bitdefender\usopriva...
☑ BFE	Base Filtering Engine: 基礎篩選引擎...	Microsoft Corporation	c:\windows\system32\bfe.dll
☑ BITS	Background Intelligent Transfer Servi...	Microsoft Corporation	c:\windows\system32\qmgr.dll
☑ Browser	Computer Browser: 維護網路上更新...	Microsoft Corporation	c:\windows\system32\browser.dll
☑ bthserv	Bluetooth Support Service: Bluetooth...	Microsoft Corporation	c:\windows\system32\bthserv.dll
☑ CertPropSvc	Certificate Propagation: 從智慧卡將...	Microsoft Corporation	c:\windows\system32\certprop.dll
☑ clr_optimization_v2.0.50...	Microsoft .NET Framework NGEN v2...	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework...
☑ clr_optimization_v2.0.50...	Microsoft .NET Framework NGEN v2...	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework...
☑ clr_optimization_v4.0.30...	Microsoft .NET Framework NGEN v4...	(Verified) Microsoft Dynamic Code Pu...	c:\windows\microsoft.net\framework...
☑ clr_optimization_v4.0.30...	Microsoft .NET Framework NGEN v4...	(Verified) Microsoft Dynamic Code Pu...	c:\windows\microsoft.net\framework...

AutoRuns

Demo

Process Explorer

- shows you information about
  - handles
  - DLLs
- Buffed up Task Manager, useful for dynamic analysis (e.g., memory dump, handle listing, etc.)



Process	CPU	Private Bytes	Working Set	PID	Description
msdtc.exe		3,360 K	8,360 K	1056	Microsoft 分散式交易協調器…
SearchIndexer.exe		25,636 K	20,288 K	2500	Microsoft Windows Search 索…
taskhost.exe		7,156 K	9,220 K	1196	Windows 工作的主機處理程序
svchost.exe		1,536 K	5,200 K	300	Windows Services 的主機處理…
svchost.exe		63,792 K	11,448 K	432	Windows Services 的主機處理…
lsass.exe		3,776 K	11,360 K	512	Local Security Authority Process
lsm.exe		2,276 K	4,668 K	520	
winlogon.exe		2,528 K	7,784 K	2016	
csrss.exe	< 0.01	9,220 K	27,928 K	3044	
explorer.exe	< 0.01	56,276 K	85,344 K	1964	Windows 檔案總管
vmtoolsd.exe	< 0.01	16,224 K	29,344 K	2248	VMware Tools Core Service
Procmon64.exe		4,500 K	10,484 K	2364	Process Monitor
Procmon64.exe	< 0.01	70,020 K	50,112 K	1044	
procexp64.exe	< 0.01	21,528 K	42,180 K	852	Sysinternals Process Explorer
Autoruns64.exe		24,652 K	53,196 K	2360	Autostart program viewer
svchost.exe	1.52	5,092 K	11,644 K	1868	
msiexec.exe	< 0.01	2,612 K	7,536 K	2020	

Process Explorer

Demo

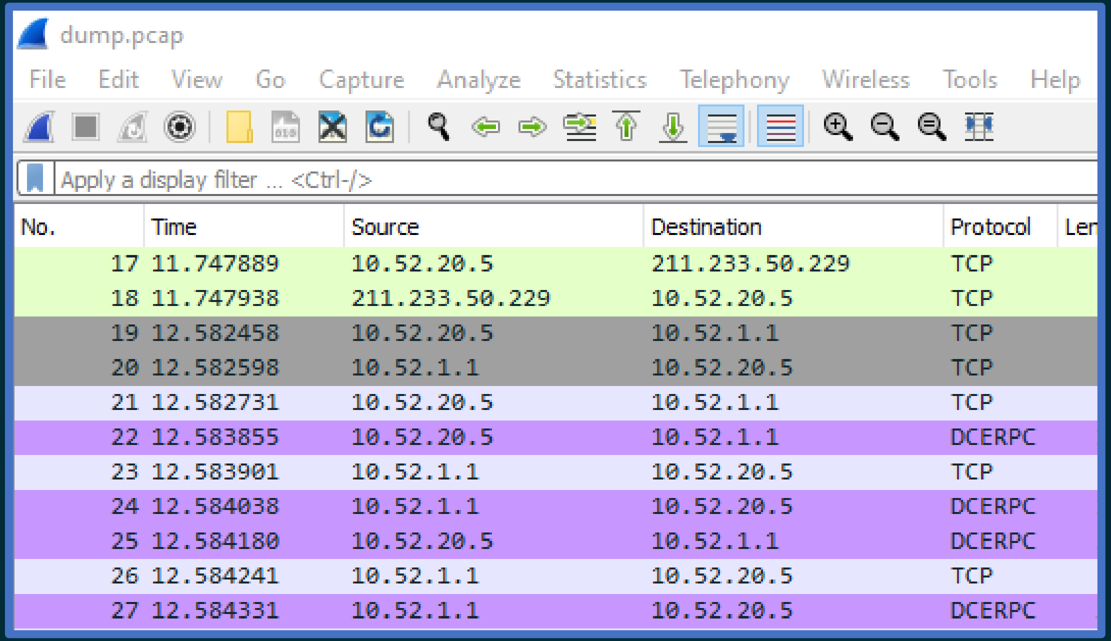
Try It !

USOPrivate.exe (MD5: adc1463af9514ac48cd963385f08c40f)

What about network activities ?

WireShark

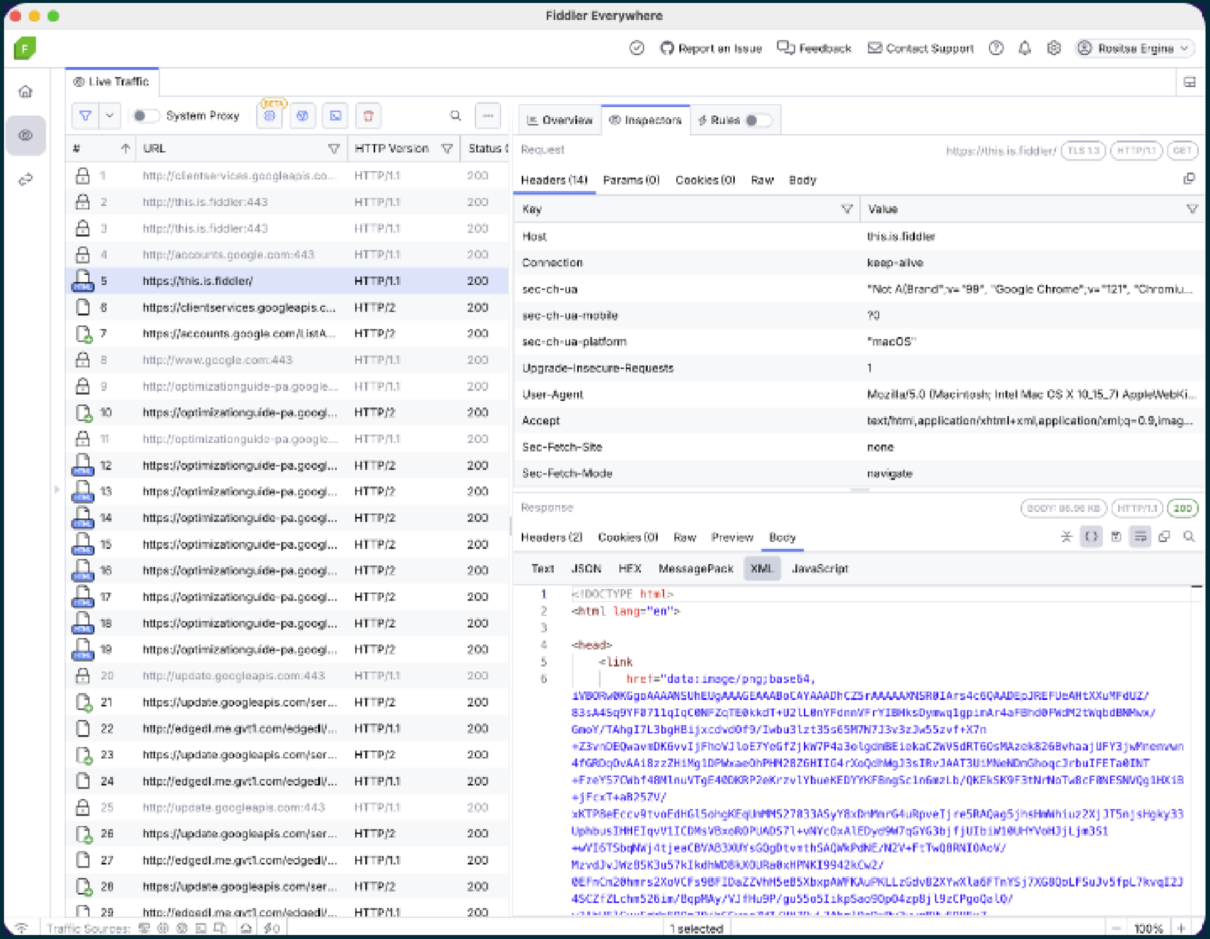
- **Wireshark** is the world's foremost and widely-used network protocol analyzer.
- Provides an overview of the incoming and outgoing packets; useful for traffic analysis.



No.	Time	Source	Destination	Protocol	Len
17	11.747889	10.52.20.5	211.233.50.229	TCP	
18	11.747938	211.233.50.229	10.52.20.5	TCP	
19	12.582458	10.52.20.5	10.52.1.1	TCP	
20	12.582598	10.52.1.1	10.52.20.5	TCP	
21	12.582731	10.52.20.5	10.52.1.1	TCP	
22	12.583855	10.52.20.5	10.52.1.1	DCERPC	
23	12.583901	10.52.1.1	10.52.20.5	TCP	
24	12.584038	10.52.1.1	10.52.20.5	DCERPC	
25	12.584180	10.52.20.5	10.52.1.1	DCERPC	
26	12.584241	10.52.1.1	10.52.20.5	TCP	
27	12.584331	10.52.1.1	10.52.20.5	DCERPC	

Fiddler

- Web debugging proxy for Windows
  - System proxy option for traffic capturing
  - Decoding and inspection of HTTP(S) requests and WebSocket communication



#	URL	HTTP Version	Status
1	http://clientservices.googleapis.co...	HTTP/1.1	200
2	http://this.is.fiddler:443	HTTP/1.1	200
3	http://this.is.fiddler:443	HTTP/1.1	200
4	http://accounts.google.com:443	HTTP/1.1	200
5	https://this.is.fiddler/	HTTP/1.1	200
6	https://clientservices.googleapis.c...	HTTP/2	200
7	https://accounts.google.com/ListA...	HTTP/2	200
8	http://www.google.com:443	HTTP/1.1	200
9	http://optimizationguide-pa.google...	HTTP/1.1	200
10	https://optimizationguide-pa.googl...	HTTP/2	200
11	http://optimizationguide-pa.google...	HTTP/1.1	200
12	https://optimizationguide-pa.googl...	HTTP/2	200
13	https://optimizationguide-pa.googl...	HTTP/2	200
14	https://optimizationguide-pa.googl...	HTTP/2	200
15	https://optimizationguide-pa.googl...	HTTP/2	200
16	https://optimizationguide-pa.googl...	HTTP/2	200
17	https://optimizationguide-pa.googl...	HTTP/2	200
18	https://optimizationguide-pa.googl...	HTTP/2	200
19	https://optimizationguide-pa.googl...	HTTP/2	200
20	http://update.googleapis.com:443	HTTP/1.1	200
21	https://update.googleapis.com/ser...	HTTP/2	200
22	http://edgedl.me.gvt1.com/edgedl/...	HTTP/1.1	200
23	https://update.googleapis.com/ser...	HTTP/2	200
24	http://edgedl.me.gvt1.com/edgedl/...	HTTP/1.1	200
25	http://update.googleapis.com:443	HTTP/1.1	200
26	https://update.googleapis.com/ser...	HTTP/2	200
27	http://edgedl.me.gvt1.com/edgedl/...	HTTP/1.1	200
28	https://update.googleapis.com/ser...	HTTP/2	200
29	http://edgedl.me.gvt1.com/edgedl/...	HTTP/1.1	200

Request https://this.is.fiddler/ TLS 1.3 HTTP/1.1 GET

Headers (14) Params (0) Cookies (0) Raw Body

Key	Value
Host	this.is.fiddler
Connection	keep-alive
sec-ch-ua	"Not A(Brand";v="99", "Google Chrome";v="121", "Chromiu...
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"macOS"
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKi...
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,imag...
Sec-Fetch-Site	none
Sec-Fetch-Mode	navigate

Response BODY: 86.96 KB HTTP/1.1 200

Headers (2) Cookies (0) Raw Preview Body

Text JSON HEX MessagePack XML JavaScript

```
<!DOCTYPE html>
<html lang="en">

<head>
    <link
        href="data:image/png;base64,
```

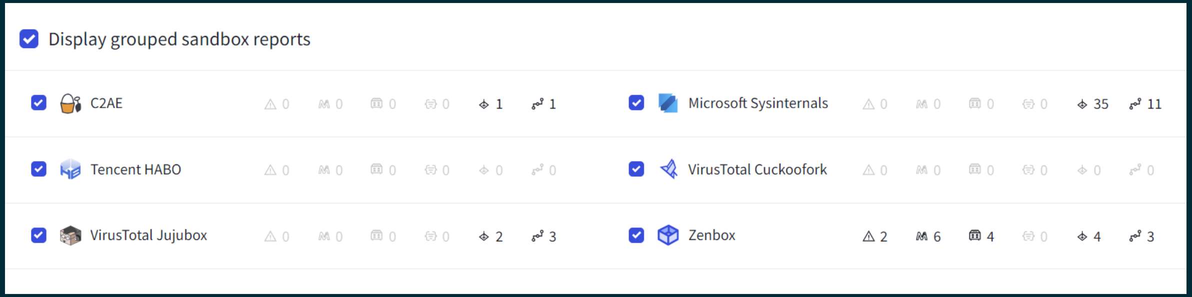
iVBORw0KGgoAAAANSUhEUgAAAGEAAABoCAYAAADhCZSrAAAAAXNSR0IArs4c6QAADEpJREFUeAHtXXuMFdUZ/
83sA45q9YF87llqIqC0NFZqTE0kkdT+U2lL0nYFdnnVFrYIBHksDymwq1gpimAr4aFBhd0FWdM2tWqbdBNMwx/
GmoY/TAhgI7L3bgHBijxcdwd0f9/Iwbu3lzt35s65M7N7J3v3zJw55zvf+X7n
+Z3vnOEOwavmDK6vvIjFhoVJloE7YeGfZjkW7P4a3olgdmBEiokaCZWV5dRT6OsMAzok826BvhaajUFY3jwMnenvwn
4fGRDqDvAAi8zzZHiMg1DPWxae0hPHM28Z6HIIG4rXoQdhWgJ3sIRvJAAT3UiMNeNDnGhoqcJrbuIFETa0INT
+FzeY57CWbf48MlnuVTgE40DKRP2eKrzvlYbueKEDYYKF8ngSc1n6mzLb/QKEkSK9F3tNrNoTw8cF0NESNVQg1HK18
+jFcxT+aR257V/
xKTP8eEccv9tvoEdHG15ohgKEqUnMM527833ASyY8xDnMnrG4uRpveIjre5RAQag5jhsHmWhiuz2XjJT5njsHgky33
UphbusIHHEIqvV1ICDMsVBxeR0PUAD57l+vNYcOxAlEDye9W7qGYG3bjfjUIbiW10UH*VeHJjLjm3S1
+wVI6TSbqNWj4tjeaCBVAB3XUYsGOgDtvmthSAQWkPdNE/N2V+FtTwQ0RNI0AcV/
MzvdJvJWz0SK3u57kIkdhWD0kXOURa0xHPNKI9942kCw2/
0EFnCn20hmrs2XoVCFs90FIDaZZVhH5eB5XbxpAWFKAuPKLLzGdv02XYwXla6FTnYSj7XG0QoLFSuJv5fpL7kvqI2J
4SCZfZLchm526im/BqpMAy/VJfHu9P/gu55o5IikpSao9Op04zpBjl9zCPgoQal0/

~~Lazy mode !~~

Make the most of sandbox !

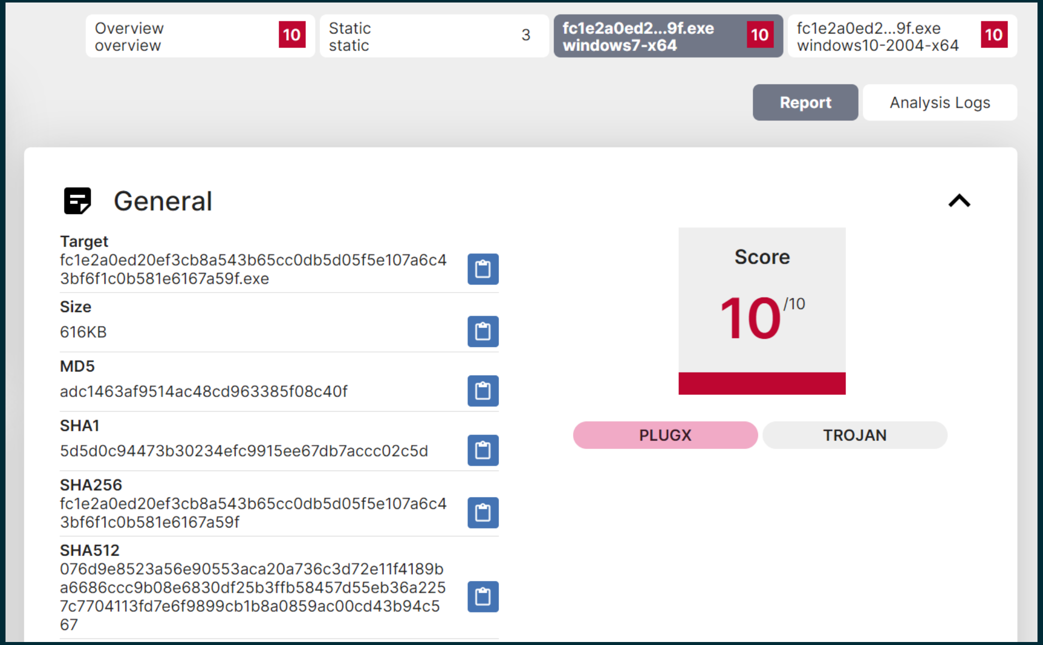
Sandbox

- VT report
  - multiple sandboxes
- Triage
  - new version of cuckoo (?
  - https://tria.ge/240410-sgpmnafd5v/behavioral1
- Remember: don't upload sensitive samples.



☑ Display grouped sandbox reports

☑	C2AE	⚠ 0	0	0	0	1	1	☑	Microsoft Sysinternals	⚠ 0	0	0	0	35	11
☑	Tencent HABO	⚠ 0	0	0	0	0	0	☑	VirusTotal Cuckoofork	⚠ 0	0	0	0	0	0
☑	VirusTotal Jujubox	⚠ 0	0	0	0	2	3	☑	Zenbox	⚠ 2	6	4	0	4	3



General

Target
fc1e2a0ed20ef3cb8a543b65cc0db5d05f5e107a6c43bf6f1c0b581e6167a59f.exe

Size
616KB

MD5
adc1463af9514ac48cd963385f08c40f

SHA1
5d5d0c94473b30234efc9915ee67db7accc02c5d

SHA256
fc1e2a0ed20ef3cb8a543b65cc0db5d05f5e107a6c43bf6f1c0b581e6167a59f

SHA512
076d9e8523a56e90553aca20a736c3d72e11f4189ba6686ccc9b08e6830df25b3ffb58457d55eb36a2257c7704113fd7e6f9899cb1b8a0859ac00cd43b94c567

Score
10 /10

PLUGX TROJAN

Malware Analysis

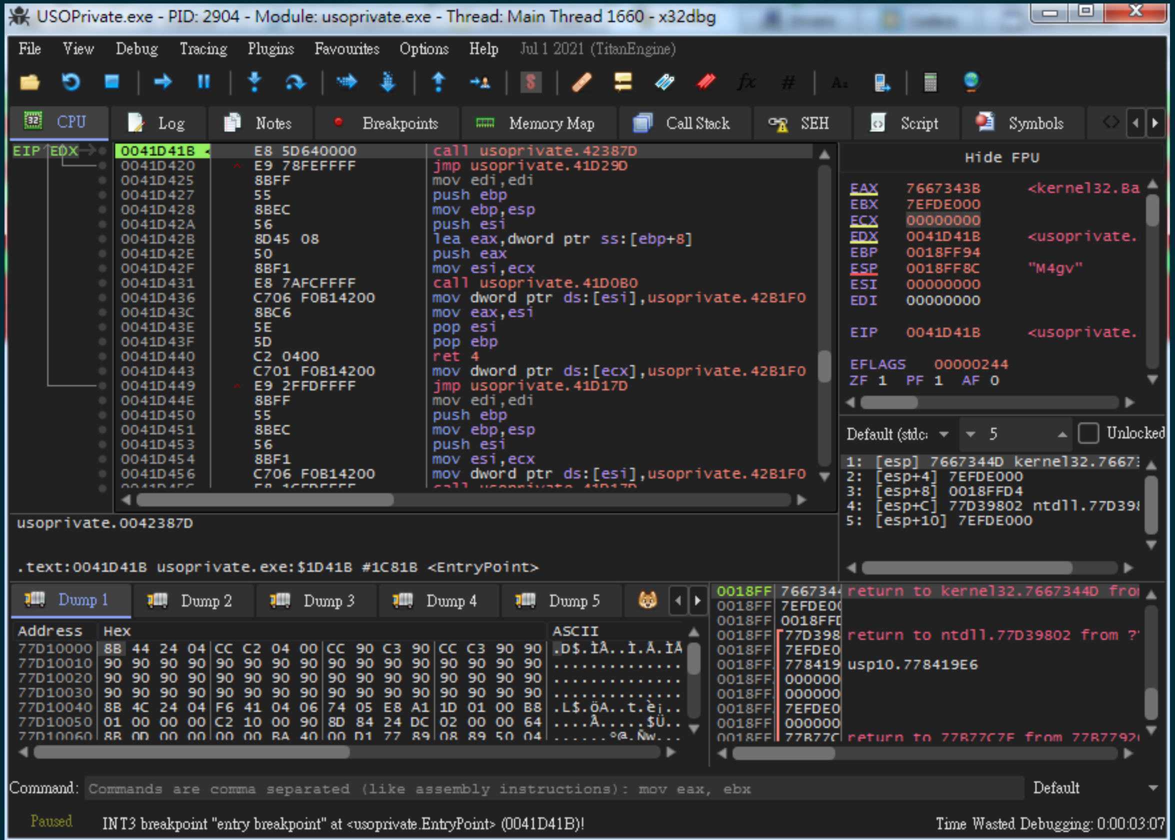
Observation

Dynamic Analysis

Static Analysis

Dynamic Analysis – x64dbg

- Open-source debugger
- Modern rendition of OllyDbg
- Supports both x86 and x64
  - x32dbg.exe and x64dbg.exe
- Supports plugins
- Easy to use interface
- Supports built-in sets of commands
  - bp ➞ breakpoint (Sets a breakpoint)
  - logstack (Prints the current stack)



USOPrivate.exe - PID: 2904 - Module: usoprivate.exe - Thread: Main Thread 1660 - x32dbg

Jul 1 2021 (TitanEngine)

```
EIP EDX
0041D41B   E8 5D640000     call usoprivate.42387D
0041D420   E9 78FEFFFF     jmp usoprivate.41D29D
0041D425   8BFF            mov edi,edi
0041D427   55              push ebp
0041D428   8BEC            mov ebp,esp
0041D42A   56              push esi
0041D42B   8D45 08         lea eax,dword ptr ss:[ebp+8]
0041D42E   50              push eax
0041D42F   8BF1            mov esi,ecx
0041D431   E8 7AFCFFFF     call usoprivate.41D0B0
0041D436   C706 F0B14200   mov dword ptr ds:[esi],usoprivate.42B1F0
0041D43C   8BC6            mov eax,esi
0041D43E   5E              pop esi
0041D43F   5D              pop ebp
0041D440   C2 0400         ret 4
0041D443   C701 F0B14200   mov dword ptr ds:[ecx],usoprivate.42B1F0
0041D449   E9 2FFDFFFF     jmp usoprivate.41D17D
0041D44E   8BFF            mov edi,edi
0041D450   55              push ebp
0041D451   8BEC            mov ebp,esp
0041D453   56              push esi
0041D454   8BF1            mov esi,ecx
0041D456   C706 F0B14200   mov dword ptr ds:[esi],usoprivate.42B1F0
```

```
usoprivate.0042387D

.text:0041D41B usoprivate.exe:$1D41B #1C81B <EntryPoint>
```

```
EAX     7667343B     <kernel32.Ba
EBX     7EFDE000
ECX     00000000
EDX     0041D41B     <usoprivate.
EBP     0018FF94
ESP     0018FF8C     "M4gv"
ESI     00000000
EDI     00000000

EIP     0041D41B     <usoprivate.

EFLAGS   00000244
ZF 1  PF 1  AF 0
```

```
1: [esp] 7667344D kernel32.7667:
2: [esp+4] 7EFDE000
3: [esp+8] 0018FFD4
4: [esp+C] 77D39802 ntdll.77D398
5: [esp+10] 7EFDE000
```

```
Address   Hex                                               ASCII
77D10000  8B 44 24 04 CC C2 04 00 CC 90 C3 90 CC C3 90 90  .D$.ÌÂ..Ì.Ã.ÌÃ
77D10010  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
77D10020  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
77D10030  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
77D10040  8B 4C 24 04 F6 41 04 06 74 05 E8 A1 1D 01 00 B8  .L$.öA..t.è¡..
77D10050  01 00 00 00 C2 10 00 90 8D 84 24 DC 02 00 00 64  ....Â.....$Ü..
```

```
0018FF  766734  return to kernel32.7667344D fro
0018FF  7EFDE0
0018FF  0018FF
0018FF  77D398  return to ntdll.77D39802 from ?'
0018FF  7EFDE0
0018FF  778419  usp10.778419E6
0018FF  000000
0018FF  000000
0018FF  7EFDE0
0018FF  000000
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused INT3 breakpoint "entry breakpoint" at <usoprivate.EntryPoint> (0041D41B)!

Time Wasted Debugging: 0:00:03:07

Dynamic Analysis – x64dbg

- Demo
  - tabs
  - controls
    - step in (F7), step over (F8), run (F9)
    - breakpoint (software, hardware)
  - command: bp

x64dbg Cheat sheet

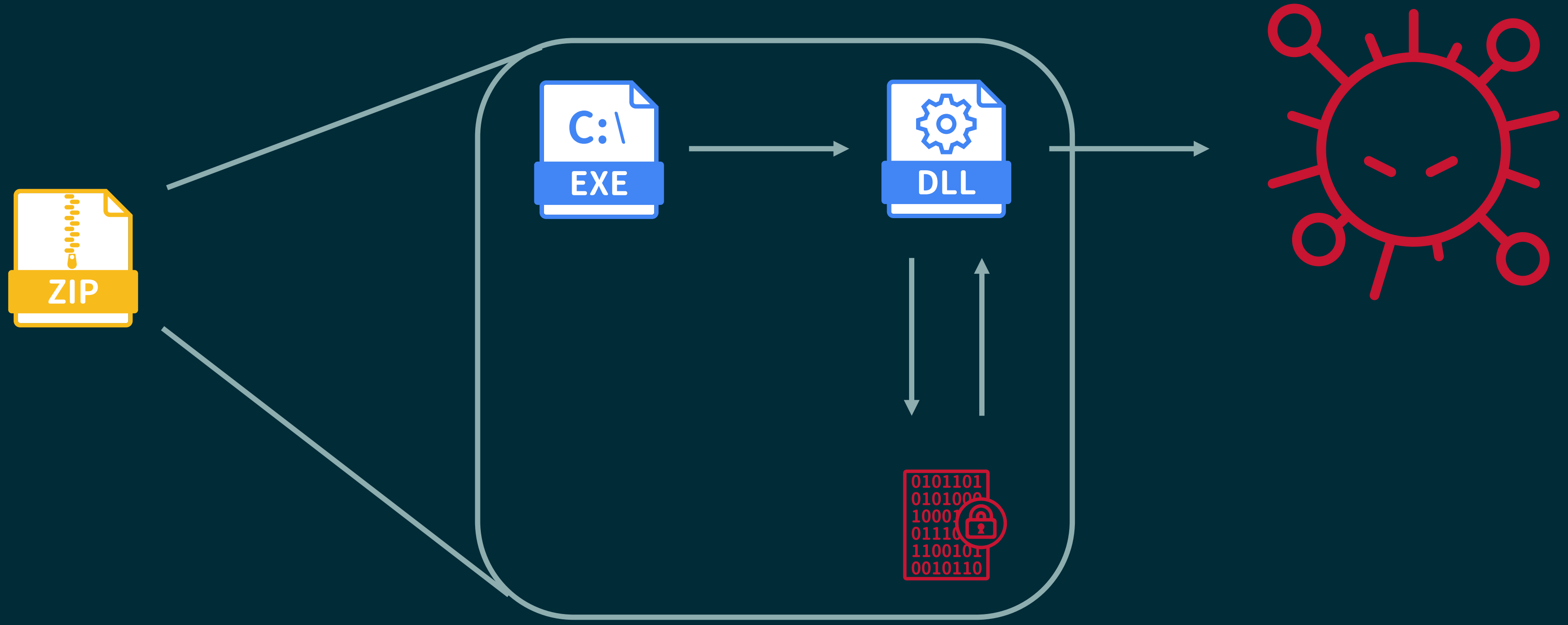
- Plugins
  - Scylla
    - Memory dumping
  - ScyllaHide
    - Anti-anti-debugger
  - OllyDumpEx
    - Memory/PE dumping
- Keyboard Shortcuts
  - F2 = Set breakpoint @ address
  - F7 = Step into
  - F8 = Step over
  - F9 = Run
  - X = xref to selected item
  - Ctrl+G = Go to address
  - - = Go back
  - Ctrl+* = Start from address
  - ; = Comment
- Commands
  - bp <address>

x64dbg

Dynamic Analysis – Breakpoint

- system("pause");
- bp on critical instruction, and observe the result/change
  - encryption
  - decoding
  - hot pach
  - dump memory
  - …

Dynamic Analysis – Breakpoint



WinAPI - Memory

- VirtualAlloc(Ex)
  - Reserves, commits, or changes the state of a region of pages in the virtual address space of the calling process.
  - **Often used to allocate memory for shellcode or PEs.**
  - Watch out for RWX (Read/Write/eXecute) memory allocation.
- VirtualProtect(Ex)
  - Changes the protection on a region of committed pages in the virtual address space of the calling process.
  - Often used to change protection value of malicious memory space.
    - i.e., changing an RW protected memory to RWX.
- WriteProcessMemory
  - Writes data to an area of memory in a specified process.
  - Often used for shellcode injection into another process.

WinAPI - Library

- LoadLibrary(Ex)(A/W)
  - Loads the specified module into the address space of the calling process.
  - Used to load another library
  - Often used to load library as runtime to avoid import table scans.
- GetProcAddress
  - Retrieves the address of an exported function or variable from the specified dynamic-link library (DLL).
  - Used to load an export from a library
  - Often used to load imports at runtime to build its own import table to avoid import table scanning.

WinAPI - Service

- Requires administrative privileges.
- Typically used for persistence or info gathering.
- APIs
  - OpenSCManager(A/W)
  - StartService(A/W)
  - (Open/Control/Delete)Service
  - SetServiceStatus

WinAPI - Crypto

- CryptGetProvParam
- CryptAcquireContext(A/W)
  - Watch out for the provider used
  - e.g., PROV_RSA_FULL, PROV_RSA_AES, etc.
- Crypt(Encrypt/Decrypt)
- Crypt(Derive/Import)Key

WinAPI - File

- (Read/Create/Delete)File(Ex)
- (Create/Delete)Directory(A/W)
- Find(First/Next)File(A/W)
  - Used to enumerate directories
- GetTempPath(A/W)
  - Returns a temporary file to r/w to
  - e.g., %temp%\tmp8F7E.tmp

WinAPI - Process

- CreateToolhelp32Snapshot
  - Creates a snapshot of specified processes.
  - Typically used to get all running processes.
- CreateProcess(A/W)
- TerminateProcess
- CreateRemoteThread(Ex)
  - Can be used to start previously injected shellcode.
- CreateThread

WinAPI - Network

- WSAStartup/WSaCleanup
  - Initializes or terminates Winsock
- accept/connect/recv/send
  - Establish, receive, send information to/from the remote end.
- gethostname/gethostbyname/getaddrinfo
  - DNS resolve
  - Can be used to retrieve local IP/device name
    - e.g.,
      - gethostname(buffer, bufferLen)
      - hostname = gethostbyname(buffer)

WinAPI - Misc

- Sleep
  - Delay process execution
  - Anti-dynamic-analysis or anti-sandbox
- IsDebuggerPresent/CheckRemoteDebuggerPresent
  - Checks if a debugger is attached to the process
- …

Try It

- USOPrivate.exe (MD5: adc1463af9514ac48cd963385f08c40f)
    - unzip this file, you would find three files
- Try to use x64dbg and figure out :
    - Which file will be read ?
    - Try to get the decrypted binary(PE file)
        - Tips: alloc memory + write/? data into the memory

Malware Analysis

Observation

Dynamic Analysis

Static Analysis

Static Analysis - Decompiler

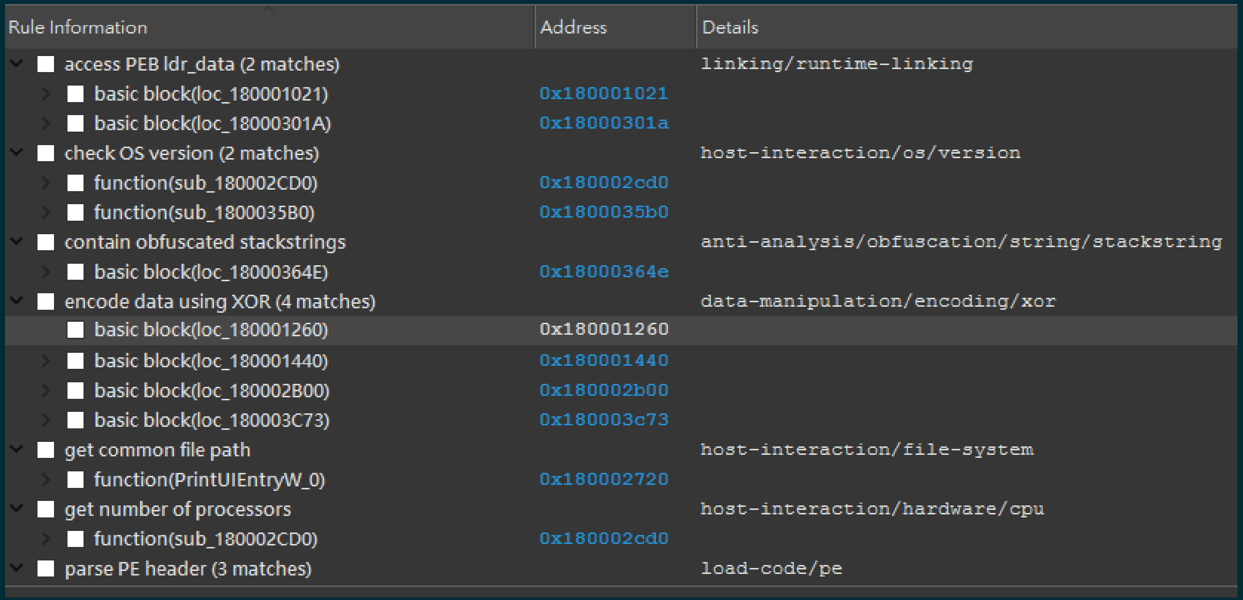
- Ida Pro (~~F5~~)
- Ghidra (~~CTRL + E~~)
- Any thing else ?

Static Analysis – Ida Pro

- In IDA View
  - F5: Go to Pseudocode View
  - U: Undefine selected assembly
    - Useful if IDA accidentally interpreted data as instructions
  - Space: Text View (or Graph View)
- In Pseudocode View
  - X: Show xref
    - Useful when finding other parts of the code that references that specific variable
  - Esc: Go back to last page
  - N = Rename item
  - Y = Set type/definition
  - G = Go to address
- In IDA/Pseudocode/Hex View…
  - Right click -> Synchronize with -> [Other Views]
- General…
  - Shift + F12 = Strings View

Static Analysis - Capa

- https://github.com/mandiant/capa
- Based on function, static analysis
  - behavior
  - signature



Rule Information	Address	Details
□ access PEB ldr_data (2 matches)		linking/runtime-linking
□ basic block(loc_180001021)	0x180001021	
□ basic block(loc_18000301A)	0x18000301a	
□ check OS version (2 matches)		host-interaction/os/version
□ function(sub_180002CD0)	0x180002cd0	
□ function(sub_1800035B0)	0x1800035b0	
□ contain obfuscated stackstrings		anti-analysis/obfuscation/string/stackstring
□ basic block(loc_18000364E)	0x18000364e	
□ encode data using XOR (4 matches)		data-manipulation/encoding/xor
□ basic block(loc_180001260)	0x180001260	
□ basic block(loc_180001440)	0x180001440	
□ basic block(loc_180002B00)	0x180002b00	
□ basic block(loc_180003C73)	0x180003c73	
□ get common file path		host-interaction/file-system
□ function(PrintUIEntryW_0)	0x180002720	
□ get number of processors		host-interaction/hardware/cpu
□ function(sub_180002CD0)	0x180002cd0	
□ parse PE header (3 matches)		load-code/pe

Demo

- EVENT.dll (MD5: 6391ab75ac20f2f59179092446ed5052)

Remember that ?

逆向只是過程

Threat Intelligence

- EVENT.dll (MD5: 6391ab75ac20f2f59179092446ed5052)
- Malware Name: PUBLOAD / TVLoad + NoFive
- C2: 89.38.225.151
- Target: TW
- Actor: Mustang Panda / Earth Preta / Polaris

Q & A

THANK YOU!

Tako

tako@teamt5.org

TEAMT5
杜浦數位安全

Persistent Cyber Threat Hunters