Basics Malware Static and Dynamic Analysis

Intro

What is Malware?

- Malware is a malicious program or software that inserts into a system, with the intention of compromising CIA(Confidentiality, Integrity, Availability).

Types of Malware:

- Virus: Malicious software inserted into a program or data file.
- Trojan: disguised as legitimate files but something else, attacker embedded malicious software into legitimate file.
- Worm: self replicating program, spear over network.
- Backdoor: open backdoor to C&C instruction. Like RAT(remote access tool)
- Ransomware: malicious program that encrypts victim files and asks for money to decrypt.
- APT (Advanced persistent threat): state-sponsored group-create malware to remain undetected for an extended period.

EX:

Rootkits	Bootkits
-Designed to hide the existence of certain processes from normal methods of detection, in order to enable continued access to a computer. EX: flame, stuxnet	-Rootkit + Boot -Are Rootkits in which the first point of control is during the boot process that allow the malicious program to be executed before OS boot.

- PUPs(Potentially unwanted programs): they are programs which don’t do anything good, usually bundled with other useful software.
  - PUPs are not malware because you agree to install it.

Steps for malware analysis:

analysis divided into two techniques Static and Dynamic, simply Static analysis means how to know what is this malware without running it. But Dynamic analysis means running malware and observing behavior.

Note: to do dynamic analysis you need to safe and isolated environment to run malware, so that your device is not infected with this malware.
So we need to setup a VM to run as a sandbox.

Basic Static analysis

To do static analysis you need to follow this steps:

1. Anti-virus scanning
2. Hash scanning
3. Extract strings
4. Analyze PE header
5. Detect packers

1.Anti-virus Scanning

- Antivirus detected based signature or heuristics or behavior or ML
- Antivirus Action: Quarantine or delete
- Scan can be offline by installing any vendor AV or online by searching any virustotal as example.

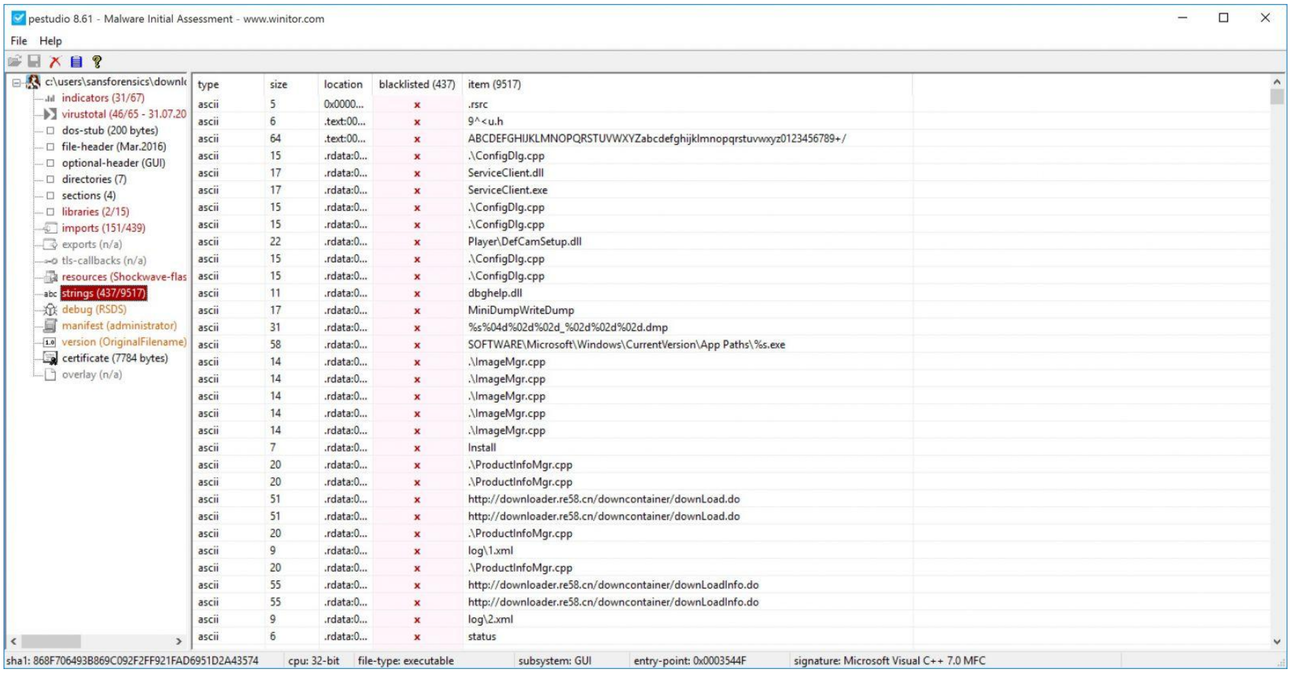
2.Hash Scanning

- Hash: is convert any length of data into fixed length value.
  EX: MD5, SHA-56
- By hash can search for reputation
- To generate hash use hash tools like quickhash or use PEstudio

3.Extract Strings

- Extract strings from file without opening it Searching for file name, URLs, IP, command and embedded files.
- Strings have two types: ASCII and Unicode

- We can extract with many tools like string.exe, floss and PEstudio
- On PEstudio drag and drop file.



type	size	location	blacklisted (437)	item (9517)
ascii	5	0x0000...	x	.rsrc
ascii	6	.text:00...	x	9^<u.h
ascii	64	.text:00...	x	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
ascii	15	.rdata:0...	x	.\ConfigDlg.cpp
ascii	17	.rdata:0...	x	ServiceClient.dll
ascii	17	.rdata:0...	x	ServiceClient.exe
ascii	15	.rdata:0...	x	.\ConfigDlg.cpp
ascii	15	.rdata:0...	x	.\ConfigDlg.cpp
ascii	22	.rdata:0...	x	Player\DefCamSetup.dll
ascii	15	.rdata:0...	x	.\ConfigDlg.cpp
ascii	15	.rdata:0...	x	.\ConfigDlg.cpp
ascii	11	.rdata:0...	x	dbghelp.dll
ascii	17	.rdata:0...	x	MiniDumpWriteDump
ascii	31	.rdata:0...	x	%s%04d%02d%02d_%02d%02d%02d.dmp
ascii	58	.rdata:0...	x	SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\%s.exe
ascii	14	.rdata:0...	x	.\ImageMgr.cpp
ascii	14	.rdata:0...	x	.\ImageMgr.cpp
ascii	14	.rdata:0...	x	.\ImageMgr.cpp
ascii	14	.rdata:0...	x	.\ImageMgr.cpp
ascii	14	.rdata:0...	x	.\ImageMgr.cpp
ascii	7	.rdata:0...	x	Install
ascii	20	.rdata:0...	x	.\ProductInfoMgr.cpp
ascii	20	.rdata:0...	x	.\ProductInfoMgr.cpp
ascii	51	.rdata:0...	x	http://downloader.re58.cn/downcontainer/downLoad.do
ascii	51	.rdata:0...	x	http://downloader.re58.cn/downcontainer/downLoad.do
ascii	20	.rdata:0...	x	.\ProductInfoMgr.cpp
ascii	9	.rdata:0...	x	log\1.xml
ascii	20	.rdata:0...	x	.\ProductInfoMgr.cpp
ascii	55	.rdata:0...	x	http://downloader.re58.cn/downcontainer/downLoadInfo.do
ascii	55	.rdata:0...	x	http://downloader.re58.cn/downcontainer/downLoadInfo.do
ascii	9	.rdata:0...	x	log\2.xml
ascii	6	.rdata:0...	x	status

sha1: 868F706493B869C092F2FF921FAD6951D2A43574 | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x0003544F | signature: Microsoft Visual C++ 7.0 MFC

- Click string tab to look for all strings
- You can use another tool to extract strings like HxD

4.Analyze PE header

- PE: (portable executed file format) is a data structure that contains the information necessary for the windows OS loader to manage the executable code.

  - Most of malware file show as PE file

- Basic structure of PE file:
  - DOS MZ header: 64 byte. Last byte refer to the first point of execution
  - DOS stub
  - PE header: contain function that file should do
  - Section

- PE header contain:
  - Signature: PE -> 50 54
  - File header: number of section, time stamp, characteristics
  - Optional header: address of entry point, image bass, size of image
  - We can analyze PE header by

    PEstudio:

    - ☐ open PEstudio -> drop your file
    - ☐ look for DOS header to know end of header
    - ☐ Optional header contains Address of entry point ->(normal PE.txt)
    - ☐ look for section header and Directory

- Data Directory:
  contains two section: import table and export table
  - Import table: contain function that malware imports from windows libraries
    - Common libraries:
      - user32.dll ->contain all user interface component
      - Gd32.dll -> contain display and manipulate graphic
      - Wsock32.dll -> contain high and low level networking function
  - Export table: export from dll

Note: Naming conventions:

.dll end with A -> ASCII string version
.dll // // W -> Wide char string
.dll // // EX -> updated function

- PE section: contains the executable code.
  - stores global data accessed throughout the program

  - every section have a unique name:
    - text: contain executable code
    - data: stores global data accessed throughout the program
    - rsrc: stores resources needed or any thing else

5.Packed malware and obfuscated malware:

- Malware packed into legal file
- Note: packed malware have a few strings
- Tools to identify packed file and packer:
    - PEID
    - Exeinfo PE
    - DIE
- Then, search for tools to unpack like RL!depacker or AspackDie

---

Note: When using PEstudio look in the Indicators section to know why PEstudio suppose this file is malware.

Basic Dynamic analysis

Dynamic analysis have two technique:

I. Monitoring the malware interaction with environment:
   1. Process
   2. File system
   3. Registry
   4. Network

II. Examining the system after the malware has executed

To do dynamic analysis we need sandbox

We can use online sandbox like any.run or offline sandbox like cuckoo sandbox

But sandboxes have disadvantage:

- Sandbox evasion technique like num of desktop icon, system run time, mouse interaction
- Delaying execution: common technique used to delay the execution

---

Note:

we can run malicious file by double-click if it's .exe but how to run non .exe file

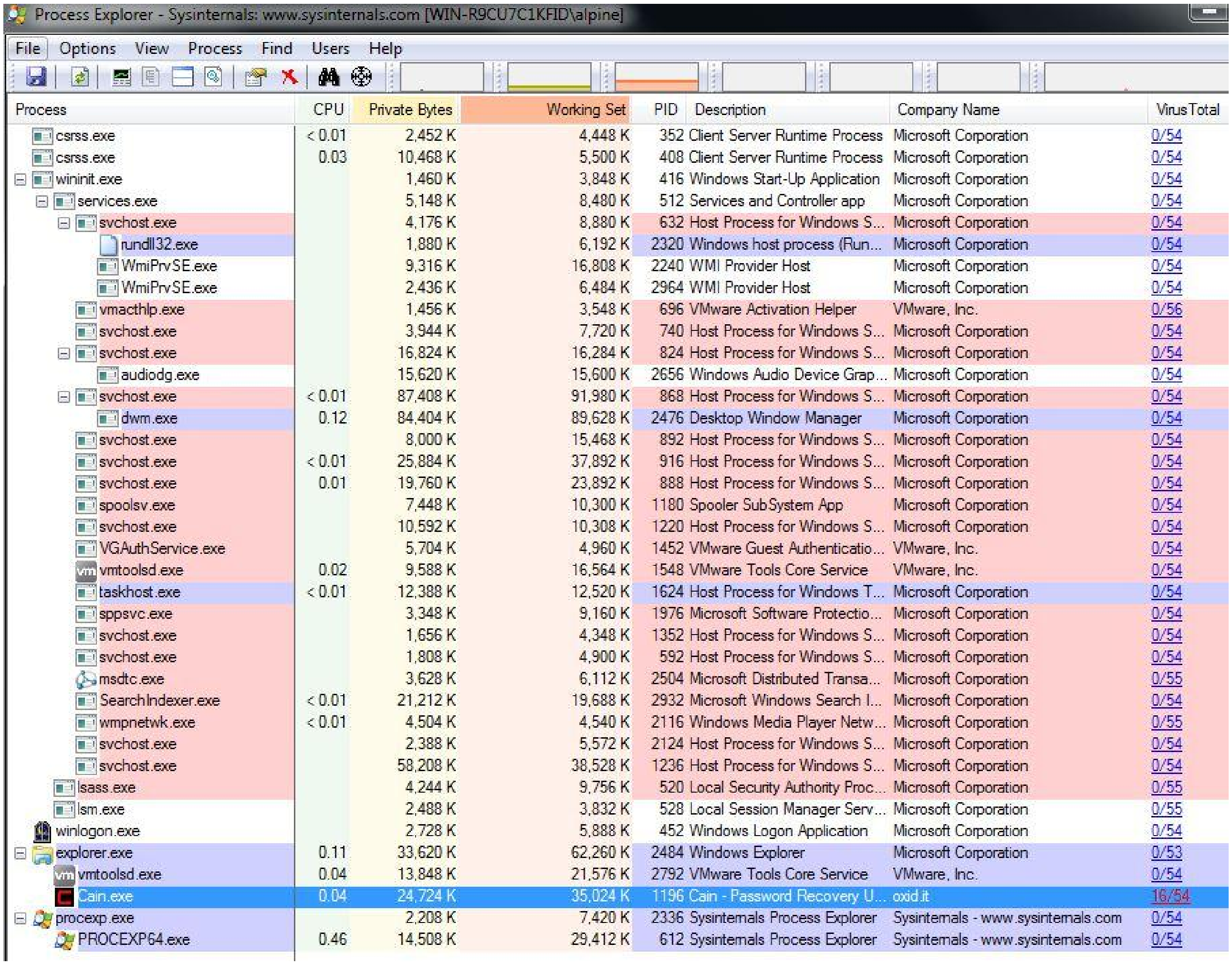
First check its function by PEstudio or CFFexplorer

Then if .dll file open CMD write rundll (file name)

1.Process monitoring

- ➔ Simplest method to show process activity open task manager
- ➔ But useful method is using process hacker / process explorer

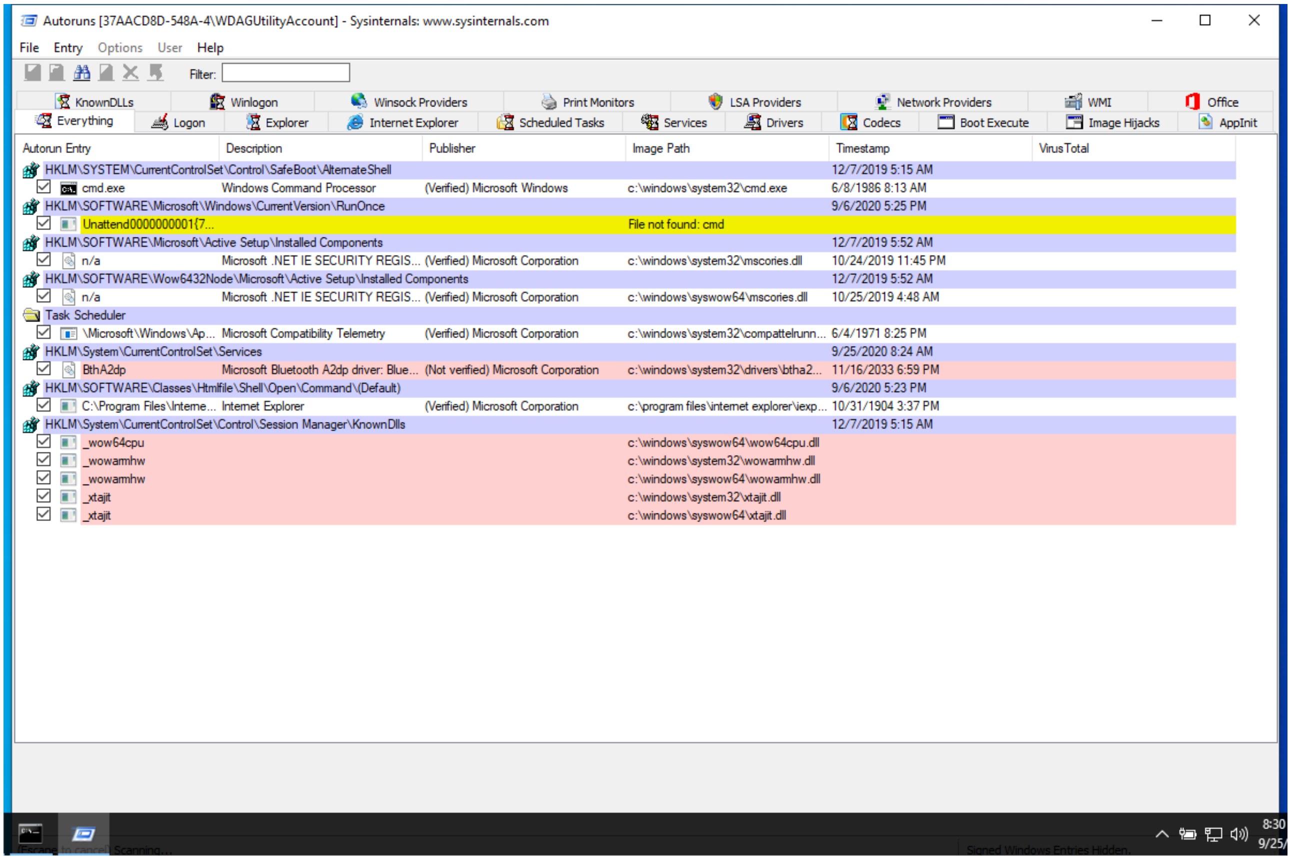
  Useful option in process explorer is verify image signature help us to detect any process malicious or not



Process Explorer - Sysinternals: www.sysinternals.com [WIN-R9CU7C1KFID\alpine]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Virus Total
csrss.exe	< 0.01	2,452 K	4,448 K	352	Client Server Runtime Process	Microsoft Corporation	0/54
csrss.exe	0.03	10,468 K	5,500 K	408	Client Server Runtime Process	Microsoft Corporation	0/54
wininit.exe		1,460 K	3,848 K	416	Windows Start-Up Application	Microsoft Corporation	0/54
services.exe		5,148 K	8,480 K	512	Services and Controller app	Microsoft Corporation	0/54
svchost.exe		4,176 K	8,880 K	632	Host Process for Windows S...	Microsoft Corporation	0/54
rundll32.exe		1,880 K	6,192 K	2320	Windows host process (Run...	Microsoft Corporation	0/54
WmiPrvSE.exe		9,316 K	16,808 K	2240	WMI Provider Host	Microsoft Corporation	0/54
WmiPrvSE.exe		2,436 K	6,484 K	2964	WMI Provider Host	Microsoft Corporation	0/54
vmacthlp.exe		1,456 K	3,548 K	696	VMware Activation Helper	VMware, Inc.	0/56
svchost.exe		3,944 K	7,720 K	740	Host Process for Windows S...	Microsoft Corporation	0/54
svchost.exe		16,824 K	16,284 K	824	Host Process for Windows S...	Microsoft Corporation	0/54
audiodg.exe		15,620 K	15,600 K	2656	Windows Audio Device Grap...	Microsoft Corporation	0/54
svchost.exe	< 0.01	87,408 K	91,980 K	868	Host Process for Windows S...	Microsoft Corporation	0/54
dwm.exe	0.12	84,404 K	89,628 K	2476	Desktop Window Manager	Microsoft Corporation	0/54
svchost.exe		8,000 K	15,468 K	892	Host Process for Windows S...	Microsoft Corporation	0/54
svchost.exe	< 0.01	25,884 K	37,892 K	916	Host Process for Windows S...	Microsoft Corporation	0/54
svchost.exe	0.01	19,760 K	23,892 K	888	Host Process for Windows S...	Microsoft Corporation	0/54
spoolsv.exe		7,448 K	10,300 K	1180	Spooler SubSystem App	Microsoft Corporation	0/54
svchost.exe		10,592 K	10,308 K	1220	Host Process for Windows S...	Microsoft Corporation	0/54
VGAuthService.exe		5,704 K	4,960 K	1452	VMware Guest Authenticatio...	VMware, Inc.	0/54
vmtoolsd.exe	0.02	9,588 K	16,564 K	1548	VMware Tools Core Service	VMware, Inc.	0/54
taskhost.exe	< 0.01	12,388 K	12,520 K	1624	Host Process for Windows T...	Microsoft Corporation	0/54
sppsvc.exe		3,348 K	9,160 K	1976	Microsoft Software Protectio...	Microsoft Corporation	0/54
svchost.exe		1,656 K	4,348 K	1352	Host Process for Windows S...	Microsoft Corporation	0/54
svchost.exe		1,808 K	4,900 K	592	Host Process for Windows S...	Microsoft Corporation	0/54
msdtc.exe		3,628 K	6,112 K	2504	Microsoft Distributed Transa...	Microsoft Corporation	0/55
SearchIndexer.exe	< 0.01	21,212 K	19,688 K	2932	Microsoft Windows Search I...	Microsoft Corporation	0/54
wmpnetwk.exe	< 0.01	4,504 K	4,540 K	2116	Windows Media Player Netw...	Microsoft Corporation	0/55
svchost.exe		2,388 K	5,572 K	2124	Host Process for Windows S...	Microsoft Corporation	0/54
svchost.exe		58,208 K	38,528 K	1236	Host Process for Windows S...	Microsoft Corporation	0/54
lsass.exe		4,244 K	9,756 K	520	Local Security Authority Proc...	Microsoft Corporation	0/55
lsm.exe		2,488 K	3,832 K	528	Local Session Manager Serv...	Microsoft Corporation	0/55
winlogon.exe		2,728 K	5,888 K	452	Windows Logon Application	Microsoft Corporation	0/54
explorer.exe	0.11	33,620 K	62,260 K	2484	Windows Explorer	Microsoft Corporation	0/53
vmtoolsd.exe	0.04	13,848 K	21,576 K	2792	VMware Tools Core Service	VMware, Inc.	0/54
Cain.exe	0.04	24,724 K	35,024 K	1196	Cain - Password Recovery U...	oxid.it	16/54
procexp.exe		2,208 K	7,420 K	2336	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com	0/54
PROCEXP64.exe	0.46	14,508 K	29,412 K	612	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com	0/54

- Malware configured to run during system bootup or login (persistence)
- To detect this malware we use autoruns tool
- Startup malware can be in startup folder, Registry and other location
- Autoruns scan every thing for detect it



Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				12/7/2019 5:15 AM	
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	6/8/1986 8:13 AM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce				9/6/2020 5:25 PM	
☑ Unattend0000000001{7...			File not found: cmd		
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				12/7/2019 5:52 AM	
☑ n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	10/24/2019 11:45 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				12/7/2019 5:52 AM	
☑ n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	10/25/2019 4:48 AM	
Task Scheduler					
☑ \Microsoft\Windows\Ap...	Microsoft Compatibility Telemetry	(Verified) Microsoft Corporation	c:\windows\system32\compattelrunn...	6/4/1971 8:25 PM	
HKLM\System\CurrentControlSet\Services				9/25/2020 8:24 AM	
☑ BthA2dp	Microsoft Bluetooth A2dp driver: Blue...	(Not verified) Microsoft Corporation	c:\windows\system32\drivers\btha2...	11/16/2033 6:59 PM	
HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default)				9/6/2020 5:23 PM	
☑ C:\Program Files\Interne...	Internet Explorer	(Verified) Microsoft Corporation	c:\program files\internet explorer\iexp...	10/31/1904 3:37 PM	
HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls				12/7/2019 5:15 AM	
☑ _wow64cpu			c:\windows\syswow64\wow64cpu.dll		
☑ _wowarmhw			c:\windows\system32\wowarmhw.dll		
☑ _wowarmhw			c:\windows\syswow64\wowarmhw.dll		
☑ _xtajit			c:\windows\system32\xtajit.dll		
☑ _xtajit			c:\windows\syswow64\xtajit.dll		

-Red: suspicious -Yellow: file not found -white: not suspicious

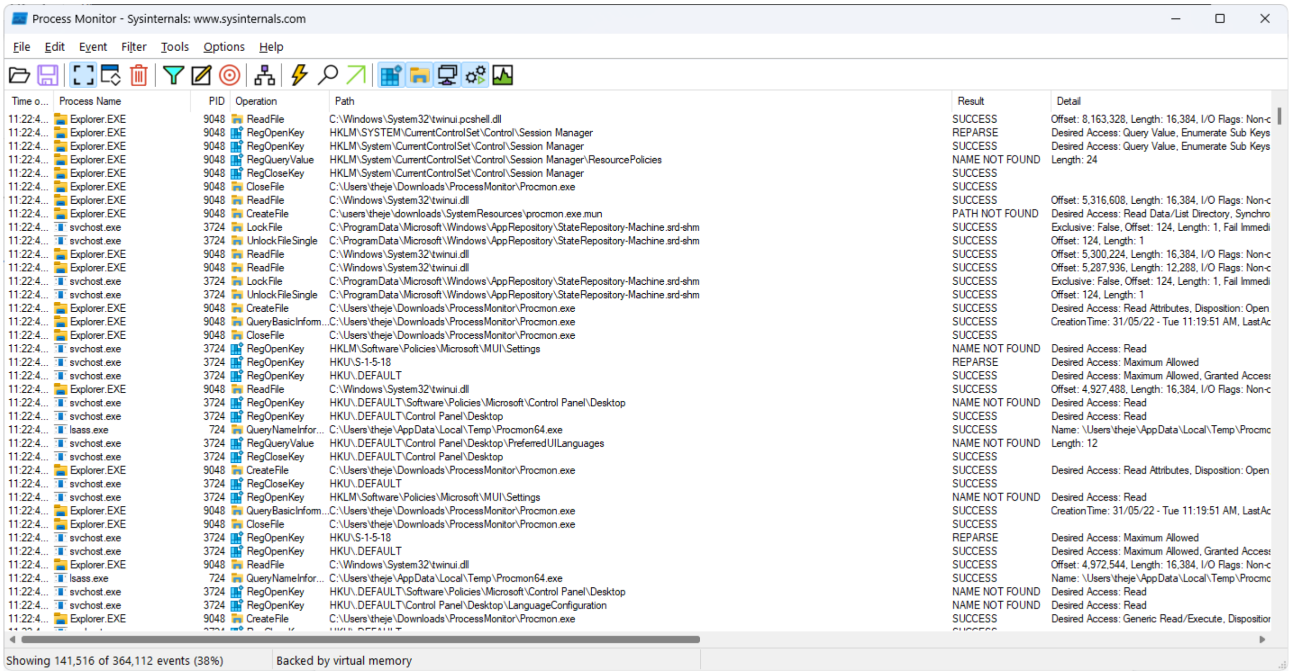
---

- Windows API

  Is a set of functions documented by windows, that allows software to interact with the operating system

  - Malware writers used windows API and we used process monitor tool to detect them

- When you run process monitor reduce background noise like (search indexer - Explorer.exe - svchost.exe)
- We can add filters to detect each process
- Procmon get its event by monitor windows API class



Time o...	Process Name	PID	Operation	Path	Result	Detail
11:22:4...	Explorer.EXE	9048	ReadFile	C:\Windows\System32\twinui.pcshell.dll	SUCCESS	Offset: 8,163,328, Length: 16,384, I/O Flags: Non-c
11:22:4...	Explorer.EXE	9048	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys
11:22:4...	Explorer.EXE	9048	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
11:22:4...	Explorer.EXE	9048	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
11:22:4...	Explorer.EXE	9048	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
11:22:4...	Explorer.EXE	9048	CloseFile	C:\Users\theje\Downloads\ProcessMonitor\Procmon.exe	SUCCESS	
11:22:4...	Explorer.EXE	9048	ReadFile	C:\Windows\System32\twinui.dll	SUCCESS	Offset: 5,316,608, Length: 16,384, I/O Flags: Non-c
11:22:4...	Explorer.EXE	9048	CreateFile	C:\users\theje\downloads\SystemResources\procmon.exe.mun	PATH NOT FOUND	Desired Access: Read Data/List Directory, Synchro
11:22:4...	svchost.exe	3724	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 124, Length: 1, Fail Immedi
11:22:4...	svchost.exe	3724	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 124, Length: 1
11:22:4...	Explorer.EXE	9048	ReadFile	C:\Windows\System32\twinui.dll	SUCCESS	Offset: 5,300,224, Length: 16,384, I/O Flags: Non-c
11:22:4...	Explorer.EXE	9048	ReadFile	C:\Windows\System32\twinui.dll	SUCCESS	Offset: 5,287,936, Length: 12,288, I/O Flags: Non-c
11:22:4...	svchost.exe	3724	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 124, Length: 1, Fail Immedi
11:22:4...	svchost.exe	3724	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 124, Length: 1
11:22:4...	Explorer.EXE	9048	CreateFile	C:\Users\theje\Downloads\ProcessMonitor\Procmon.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open
11:22:4...	Explorer.EXE	9048	QueryBasicInform...	C:\Users\theje\Downloads\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 31/05/22 - Tue 11:19:51 AM, LastAc
11:22:4...	Explorer.EXE	9048	CloseFile	C:\Users\theje\Downloads\ProcessMonitor\Procmon.exe	SUCCESS	
11:22:4...	svchost.exe	3724	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI\Settings	NAME NOT FOUND	Desired Access: Read
11:22:4...	svchost.exe	3724	RegOpenKey	HKU\S-1-5-18	REPARSE	Desired Access: Maximum Allowed
11:22:4...	svchost.exe	3724	RegOpenKey	HKU\.DEFAULT	SUCCESS	Desired Access: Maximum Allowed, Granted Access
11:22:4...	Explorer.EXE	9048	ReadFile	C:\Windows\System32\twinui.dll	SUCCESS	Offset: 4,927,488, Length: 16,384, I/O Flags: Non-c
11:22:4...	svchost.exe	3724	RegOpenKey	HKU\.DEFAULT\Software\Policies\Microsoft\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
11:22:4...	svchost.exe	3724	RegOpenKey	HKU\.DEFAULT\Control Panel\Desktop	SUCCESS	Desired Access: Read
11:22:4...	lsass.exe	724	QueryNameInfor...	C:\Users\theje\AppData\Local\Temp\Procmon64.exe	SUCCESS	Name: \Users\theje\AppData\Local\Temp\Procmc
11:22:4...	svchost.exe	3724	RegQueryValue	HKU\.DEFAULT\Control Panel\Desktop\PreferredUILanguages	NAME NOT FOUND	Length: 12
11:22:4...	svchost.exe	3724	RegCloseKey	HKU\.DEFAULT\Control Panel\Desktop	SUCCESS	
11:22:4...	Explorer.EXE	9048	CreateFile	C:\Users\theje\Downloads\ProcessMonitor\Procmon.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open
11:22:4...	svchost.exe	3724	RegCloseKey	HKU\.DEFAULT	SUCCESS	
11:22:4...	svchost.exe	3724	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI\Settings	NAME NOT FOUND	Desired Access: Read
11:22:4...	Explorer.EXE	9048	QueryBasicInform...	C:\Users\theje\Downloads\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 31/05/22 - Tue 11:19:51 AM, LastAc
11:22:4...	Explorer.EXE	9048	CloseFile	C:\Users\theje\Downloads\ProcessMonitor\Procmon.exe	SUCCESS	
11:22:4...	svchost.exe	3724	RegOpenKey	HKU\S-1-5-18	REPARSE	Desired Access: Maximum Allowed
11:22:4...	svchost.exe	3724	RegOpenKey	HKU\.DEFAULT	SUCCESS	Desired Access: Maximum Allowed, Granted Access
11:22:4...	Explorer.EXE	9048	ReadFile	C:\Windows\System32\twinui.dll	SUCCESS	Offset: 4,972,544, Length: 16,384, I/O Flags: Non-c
11:22:4...	lsass.exe	724	QueryNameInfor...	C:\Users\theje\AppData\Local\Temp\Procmon64.exe	SUCCESS	Name: \Users\theje\AppData\Local\Temp\Procmc
11:22:4...	svchost.exe	3724	RegOpenKey	HKU\.DEFAULT\Software\Policies\Microsoft\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
11:22:4...	svchost.exe	3724	RegOpenKey	HKU\.DEFAULT\Control Panel\Desktop\LanguageConfiguration	NAME NOT FOUND	Desired Access: Read
11:22:4...	Explorer.EXE	9048	CreateFile	C:\Users\theje\Downloads\ProcessMonitor\Procmon.exe	SUCCESS	Desired Access: Generic Read/Execute, Dispositior

Showing 141,516 of 364,112 events (38%)

Backed by virtual memory

Note: to analyze (process/ file system/ registry/ network) we can use the procdot tool.

- install procdot
- install dot.exe and call it in procdot
- Save all event from procmon as .csv without sequence number and with threat ID
- Then choose launcher process

2.File System activity

Why does malware access file system?

- Read:
  - read from its config file
  - read and steal user’s data and machine information

- Write:
  - write to its config file
  - Encryption (Ransomware)

- Delete:
  - delete user’s file or delete itself
  - delete file after encryption (Ransomware)

We can detect all this activity by using ProcMon
Or FileActivity watch
Or Folder Changes view

Note: Some of malware or ransomware close ProcMon after launch but you can bypass this by change ProcMon name

3.Registry Changes

Registry: is collection of database of configuration settings for operating system

- Malware could be read about :
  - OS
  - user
  - language
  - PC uptime
  - installed program
  - enabled service
  - enable/disable windows option

- The malware could be write:
  - its configuration
  - enable/disable some option
  - enable/disable some service

To monitor registry changes we use:

- ProcMon
- Regshot2
- Registry changes view

4.Monitor Network Traffic

Why does malware need network connection?

- Download:
  - download second stage malware or update itself
  - Ads
  - Pay-To-Install
  - DDOS

- Upload:
  - exfiltrate data from the victim
  - send encryption key to the server

- Lateral movement:
  - to infect other machines in the same network

*We detect network traffic using Wireshark

Note:

- nslookup : windows command line to translate domain name into IP
- FakeNet-NG: make fake connection and save all traffic in pcap file

Run wireshark and fakenet, then run malware file

- In normal case we begin analysis from DNS query but some cases malware used direct IP
- When we detect traffic maybe malware close wireshark or ransomware encrypt pcap file
- So, we can redirect sandbox traffic to another VM like REMNUX or another snake hole