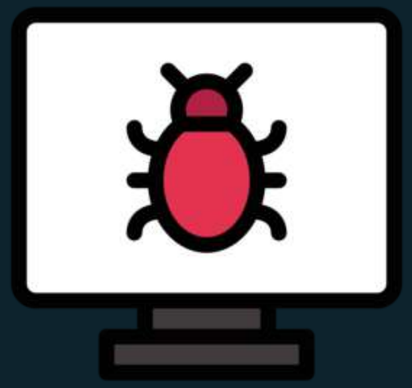
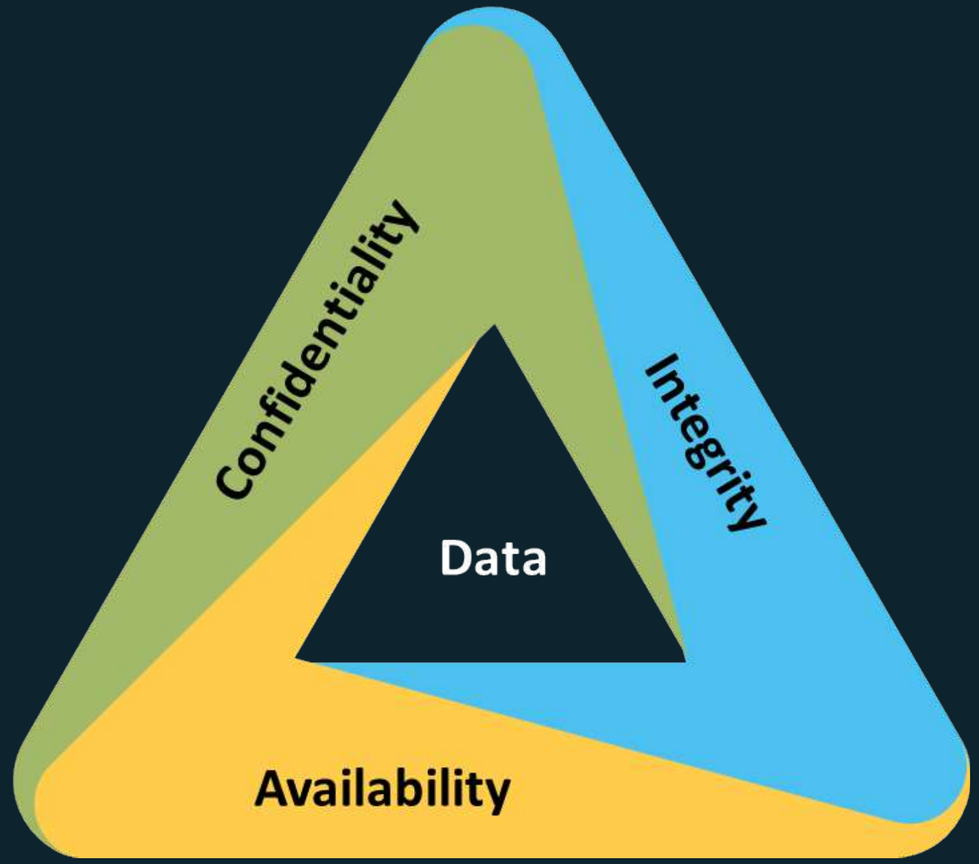

Malware Analysis



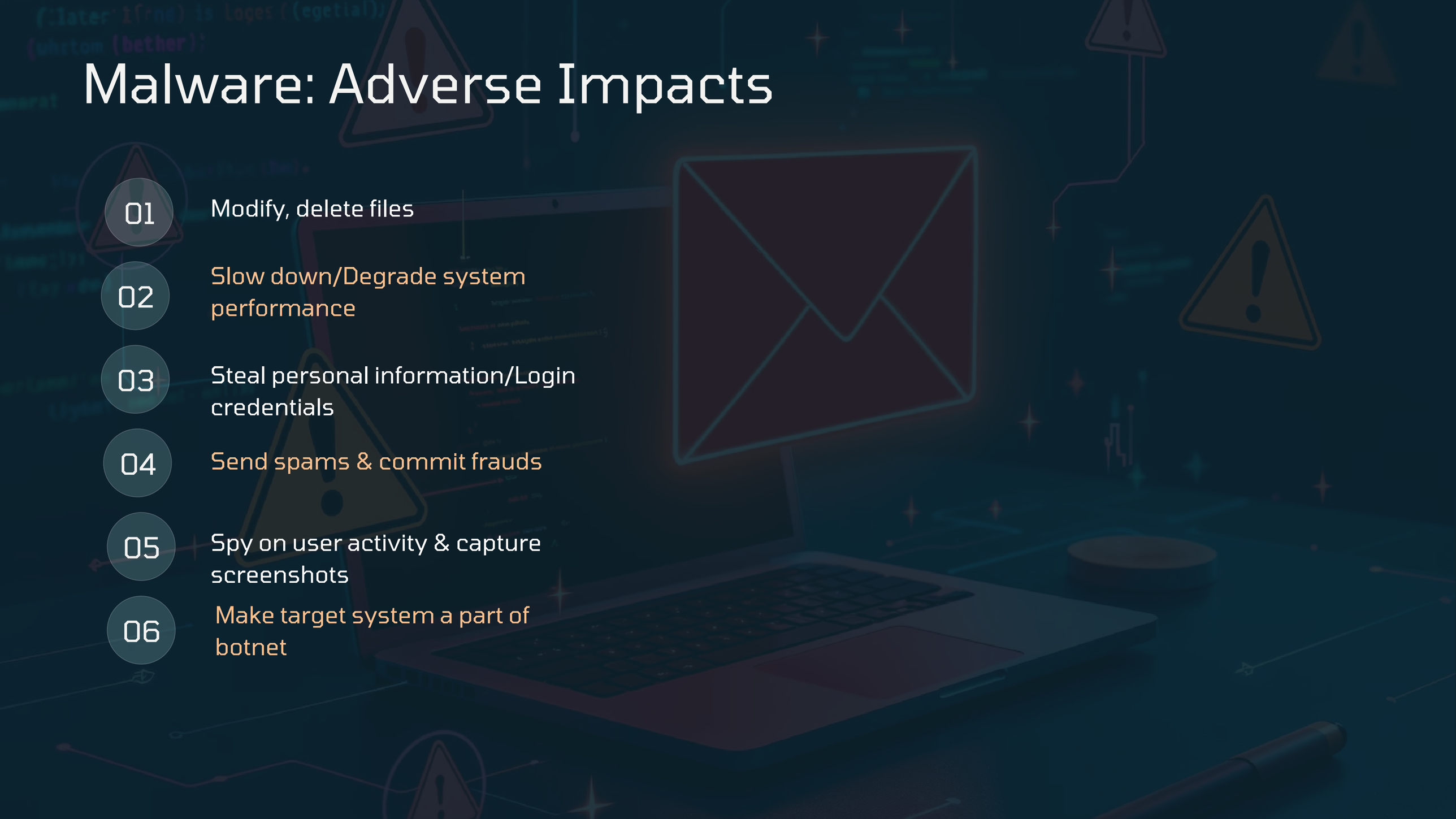
Malware: Definition

According to NIST Special Publication (SP) 800-83:

“Malware is a program that is covertly inserted into a system with the intent of compromising the confidentiality, integrity or availability of the victim’s data, applications or OS”



Malware: Adverse Impacts



01 Modify, delete files

02 Slow down/Degrade system performance

03 Steal personal information/Login credentials

04 Send spams & commit frauds

05 Spy on user activity & capture screenshots

06 Make target system a part of botnet

How Malware Enters?

- Instant messenger applications like WhatsApp, Instagram, LinkedIn
- Portable Hardware Media/Removable devices like USB flash drives - Enabled autorun function makes a system vulnerable
- Browser & Email software bugs - using outdated versions
- Unpatched software stealing of confidential files & company credentials
- Access untrusted sites and download free web application/software
- Network propagation due to inappropriate network security and vulnerable network protocols
- Email attachment: Email header and sender's email not legitimate
- File sharing services such as NetBIOS, FTP, SMB etc. are open
- Connecting to open Bluetooth & Wireless Networks
- Compromised supply chain

Malware: Components

nponent	Description
pter	Encrypts or obfuscates malware to evade antivirus detection.
vnloader	Fetches and installs additional malicious components from the internet.
pper	Delivers and executes the main malware payload on the target system.
loit	Takes advantage of software vulnerabilities to gain unauthorized access.
ctor	Injects malicious code into legitimate processes to evade detection.
uscator	Scrambles code to make analysis and detection by security tools difficult.
load	The core malicious function, such as data theft or system disruption.
icious Code	Any harmful program or script designed to damage, steal, or disrupt.

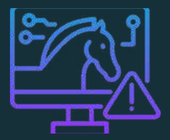
Malware: Types

VIRUS

Spread between computers

WORM

Spread between computers in one copany or location



TROJAN

Sneaks malware onto your computer

SPYWARE

Steals your data

ADWARE

Spams your Ads

RANSOMWARE

Encrypts files and blackmails you

FILELESS MALWARE

Operates in your system's memory

ROOTKIT

Gives remote access to your device

BOTNET

Turns on your PC into a puppet

KEYLOGGER

Records user activity

Malware Type: Adware

- Generates unsolicited pop ups
- Display advertisement while the program is launched

Impacts

Malware Type: APTs

01 Obtains unauthorized access & remains in the network for a long time

02 Exploits specific vulnerability

03 Persistently contacts an external C2 center

04 Well-crafted malicious code with multiple zero-day exploits

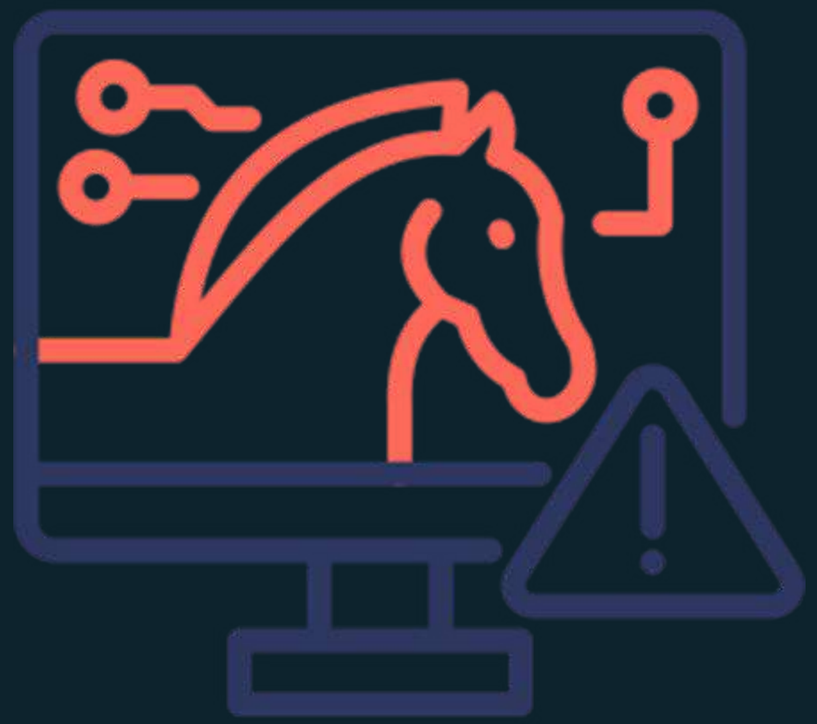
05 Sophisticated C2 obfuscates itself and avoids detection

06 Bypass checks of AV, Firewall, IDS/IPS, spam filters etc.

07 Highly targeted. For example, military institution

08 Exfiltrate sensitive information

Malware Type: Trojan



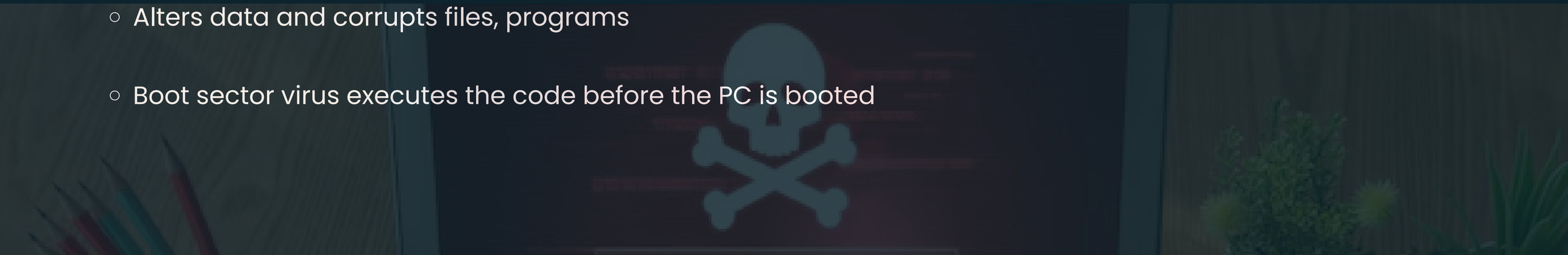
- Program appears to be benign but contains a malicious or h code.
- Delivers virus, worms, spyware etc.
- Trojans work at the same level of privileges as the victims
- May escalate privileges to install more malicious codes victim's system.
- Usually enters through E-mail attachments, downloads & IM app

Trojan: Types

Remote Access Trojan(RAT)	**Backdoor Trojan**	Rootkit Trojan
E banking Trojan	Mobile Trojan	Command Shell Trojan

Malware Type: Virus

- Transmitted through Email attachment, downloads & infected USB drive
- Attaches itself to an executable system application program
- Infects other system only with assistance of a user
- Usually targets source code, batch file & script file
- Transforms, Encrypts & Replicates itself
- Alters data and corrupts files, programs
- Boot sector virus executes the code before the PC is booted



Malware Type: Worms

1. Malware that replicates, executes and spreads across the network independent of human intervention.

2. Consume resources and degrades system performance. Subsequently, the device may stop responding

3. Worm may also carry payloads to install backdoor on the target and/or turn them into bots.

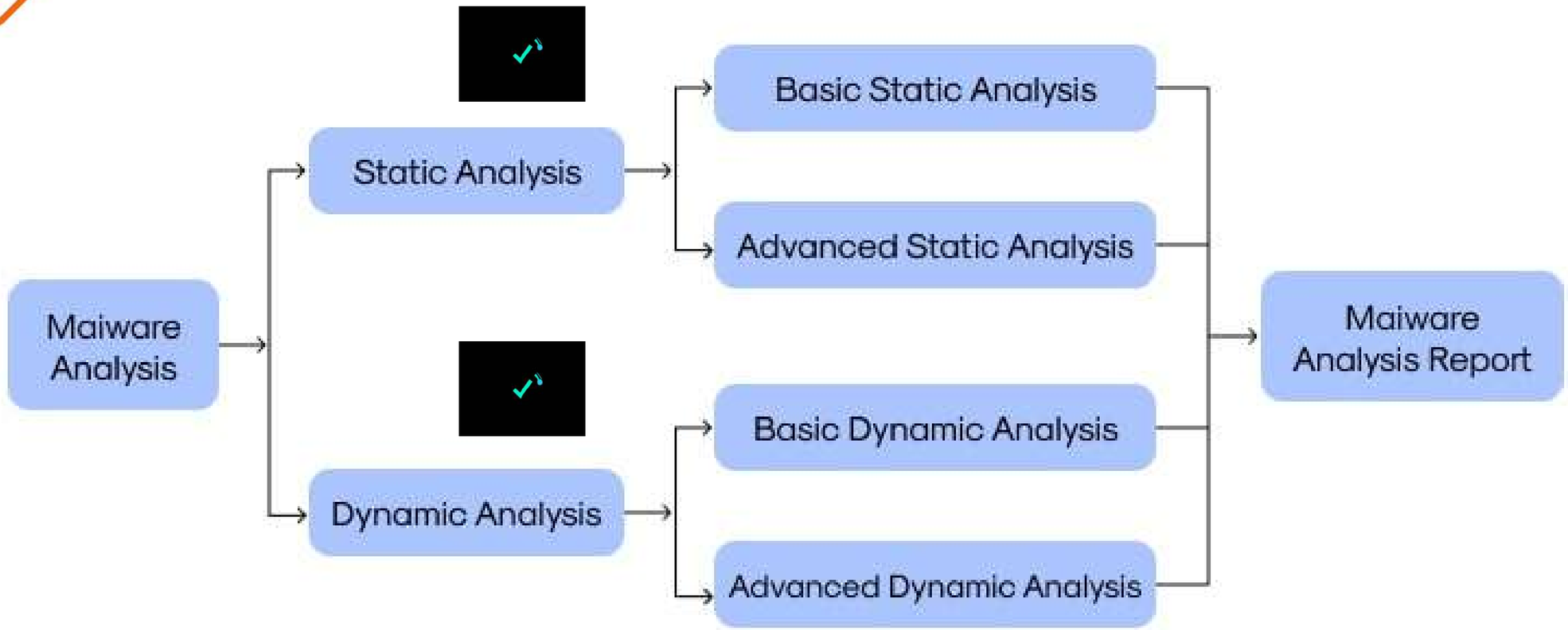
4. Alters system settings to remain active and continuously exfiltrate data from infected device.

📌 Example - **Stuxnet** infected the SCADA systems at Iran's nuclear power plant

Malware Analysis

1. Process of **Reverse Engineering** a specific piece of malware to determine its origin, functionality and impact.
2. Identify IOCs
3. Determine malicious intent
4. Identify exploited vulnerability
5. Identify damage/impact
6. Find signatures for host & network-based IDS
7. Find out the duration of infection
8. Determine preventive measures
9. Different approaches & tools are used, as single approach may not suffice.

Malware Analysis Method



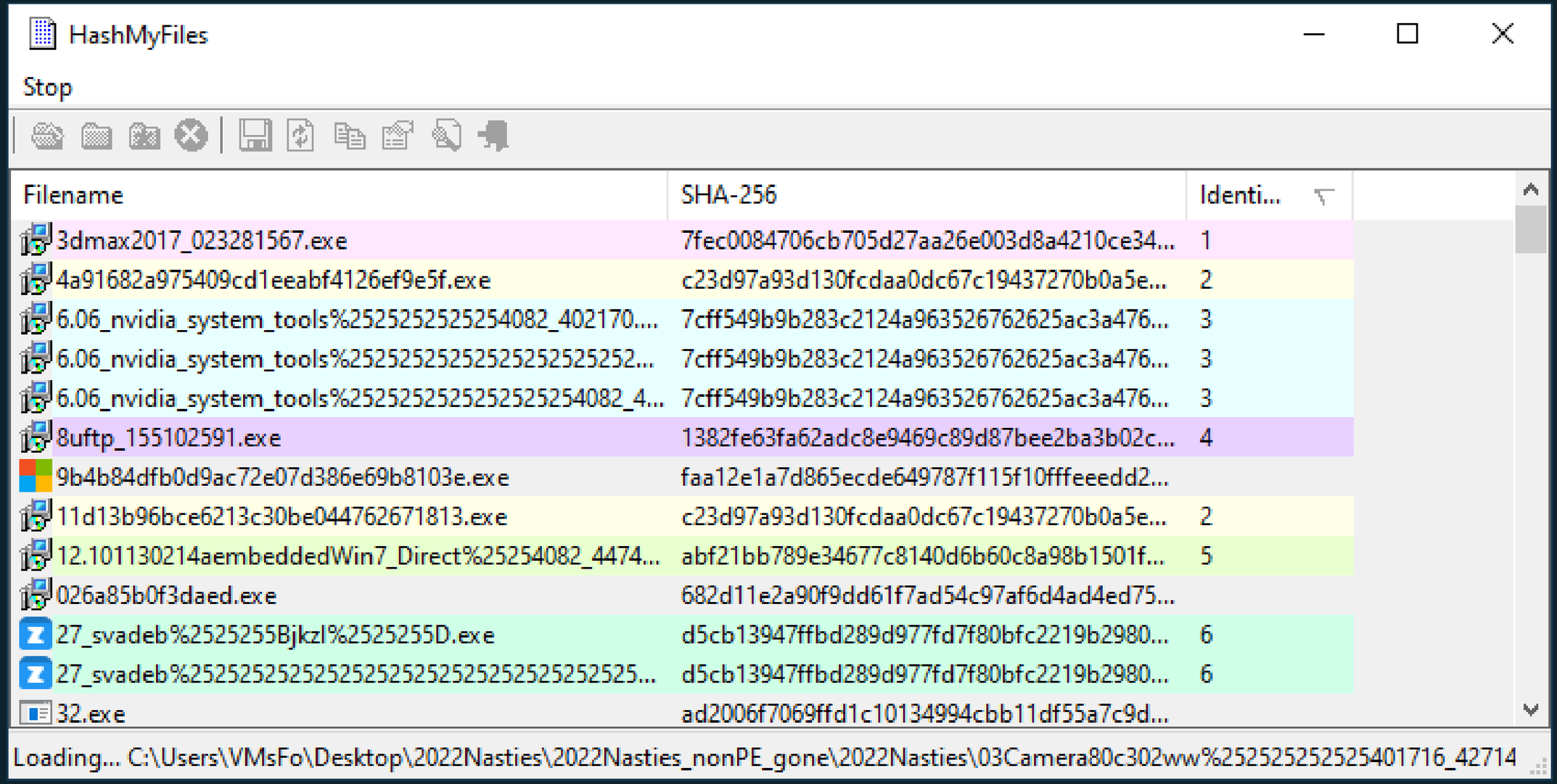
Static Malware Analysis

- Analyze code, instructions or executable binary without actually executing
- Determine the malicious part of the sample/program with help of tools
- Collect information w.r.t functionality, technical pointers or simple signatures of the malware
- Technical Pointers - File name, hash, file type, file size etc.
- Advised to perform static analysis in a controlled environment because some malwares perform malicious activities even without installation
- Find malicious behavior by analyzing the data structure, function calls, call graphs etc. of a given binary executable. This is mostly manual
- Find exploit packing technique and dependencies

Static Analysis: File Fingerprinting

- Cryptographic hash value of a given binary code is used to uniquely identify the malware.
- Fingerprint can identify similar programs from a database.
- Won’t help with encrypted or password secured files, images, audio etc.
- MD5, SHA1 and SHA2 are most commonly used.
- Tool - HashMyFiles, a free GUI based tool available at https://www.nirsoft.net

Tool: HashMyFiles



Static Analysis: Malware Scan

- VirusTotal is a free service that analyzes suspicious files, calculates hash and compares them online and offline with malware database to determine the existence of recognized malware code.
- Generates report that provide the total number of AV engines that have marked the file as malicious, the malware name, type of file, entry point, target machine, IP address accessed etc.

Community Score

62 security vendors and no sandboxes flagged this file as malicious

Follow | Reanalyze | Download | Similar | More

43486586e97095c4139a12a921e3f1cfdb06172624b123b7bf123765371386ef

olacweegim.exe

peexe | upatre | spreader | upx | overlay

Size
51.65 KB

Last Analysis Date
2 hours ago

EXE

PDF

DETECTION | DETAILS | RELATIONS | BEHAVIOR | CONTENT | TELEMETRY | COMMUNITY

Strings | Hex

Search in strings

All | ASCII | Wide | Download

```
C:\Users\admin\Downloads\29824edb55d108de9562ef3987eb29bec544390361fda8ae1f31a84a68de50bc.exe
C:\Users\admin\Downloads\3cfdb4f0d7995b55f3bddbc440c43f63ce1b02fe4bab898f5d874846b077c99b.exe
C:\Users\admin\Downloads\b54a848e3fd1ac7c50c86d732d3ce282d80dff03e883d0a690f6af962d78a428.exe
C:\Users\admin\Downloads\57d5ac02cb28b497c9fe04a3ca89b08bfa91b736e2312789ced62de5e390f621.exe
C:\Users\admin\Downloads\a95351787028c04e82dbe659988a8f313a776a8d2318c135bb2a718a062c040f.exe
C:\Users\admin\Downloads\0199a4c370eda14bf6a02f540e541835859f8e674c6a7da5eb3cfbc7bf0c1d7f.exe
C:\Users\admin\Downloads\e06cbf3d0104fa88fe7085cbef847734bb43c6704105122b95208ed7476615ec.exe
C:\Users\azure\Downloads\175fdfea80579e166668d9332f50d1d8.virus.exe
C:\Users\admin\Downloads\7dfd8916b6d071bb_olacweegim.exe
C:\Users\Petra\AppData\Local\Temp\olacweegim.pe32
C:\8ef1df7b3d6b8dd72091045662d94c0776841318.exe
C:\Users\admin\Downloads\olacweegim.exe
```

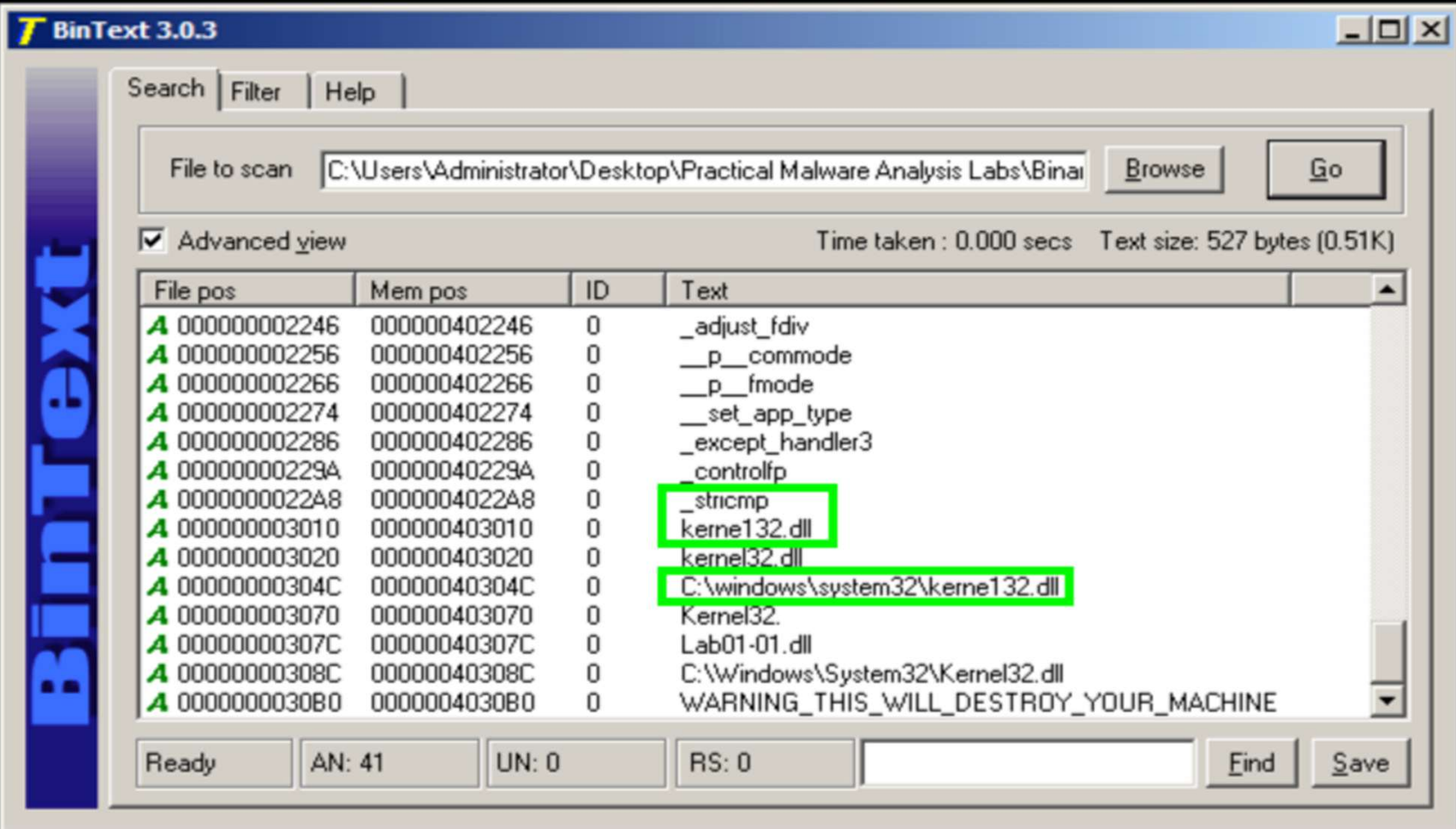
Static Analysis: String Search

01 Every program has strings which can communicate information about malicious intent

02 Various strings representing malicious intent such as reading internal memory or cookie data, may be embedded in the compiled binary code

03 For example, a program may access a particular URL

04 Tools such as **BinText** can extract embedded strings from an executable file. It can scan and display both ASCII & Unicode strings. It copies all strings to text file for searching malicious strings.


BinText 3.0.3
Search
Filter
Help
File to scan
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Binar
Browse
Go
Advanced view
Time taken : 0.000 secs
Text size: 527 bytes (0.51K)
File pos
Mem pos
ID
Text
A 000000002246 000000402246 0 _adjust_fdiv
A 000000002256 000000402256 0 __p__commode
A 000000002266 000000402266 0 __p__fmode
A 000000002274 000000402274 0 __set_app_type
A 000000002286 000000402286 0 _except_handler3
A 00000000229A 00000040229A 0 _controlfp
A 0000000022A8 0000004022A8 0 _stricmp
A 000000003010 000000403010 0 kerne132.dll
A 000000003020 000000403020 0 kernel32.dll
A 00000000304C 00000040304C 0 C:\windows\system32\kerne132.dll
A 000000003070 000000403070 0 Kernel32.
A 00000000307C 00000040307C 0 Lab01-01.dll
A 00000000308C 00000040308C 0 C:\Windows\System32\Kernel32.dll
A 0000000030B0 0000004030B0 0 WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
Ready
AN: 41
UN: 0
RS: 0
Find
Save

bp6.ex_

1 ❹

❶
❸
❷

m DLL is invalid.!Send Mail failed to send message. ❺

Static Analysis: Identify Obfuscation

01 Attackers compress, encrypt & modify the malware executable files to avoid detection

02 This complicates our attempt of RE

03 PEiD is a free tool which is used to find the Packer, Cryptor & Compiler used for PE executable file. Finding packer will ease the task of unpacking the code.

04 It can identify signature associated with over 600 different packers & compilers

05 Detect it Easy (DIE) is an application used for determining type of files. It is available for Windows, Linux & macOS.

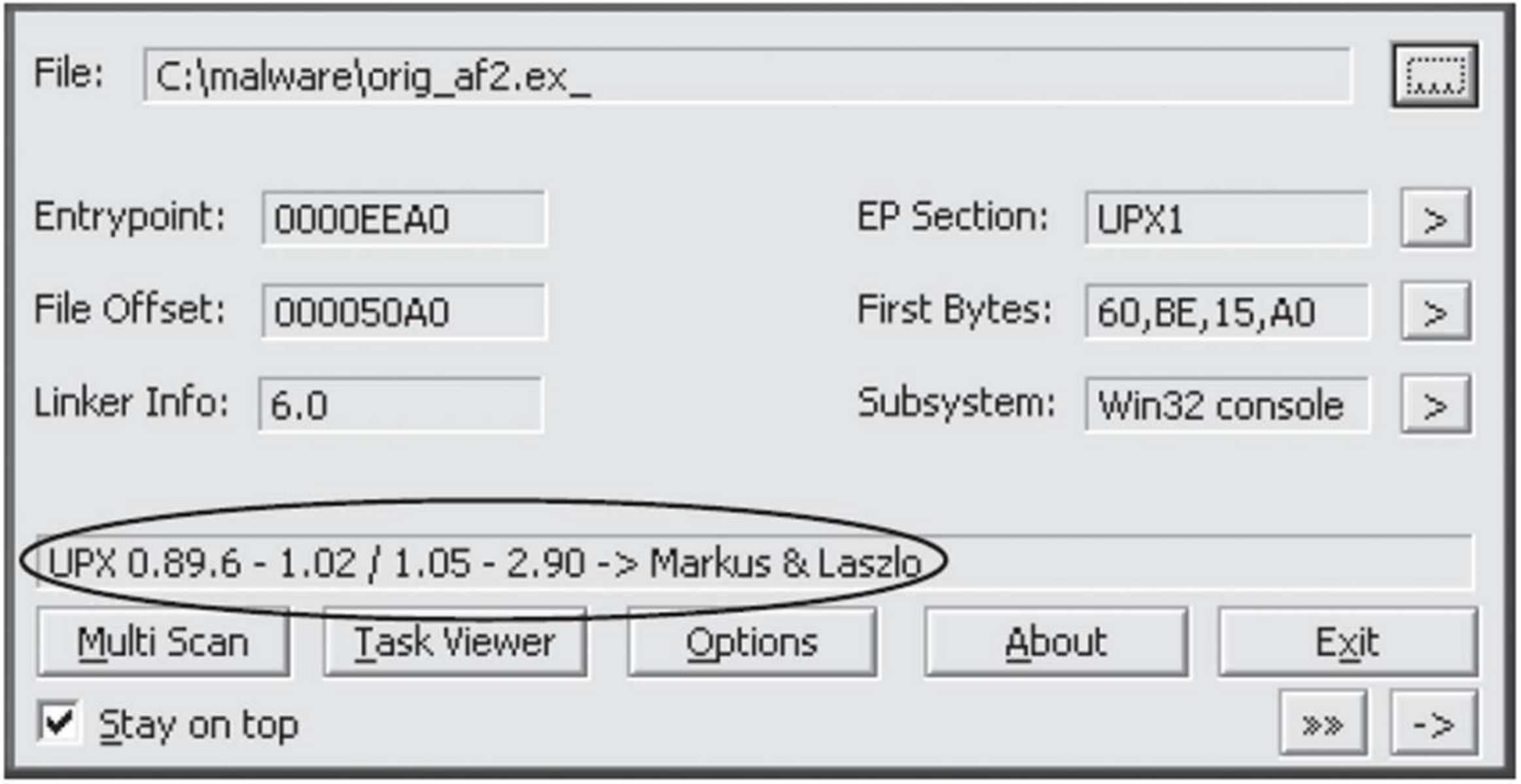


Figure 1-5: The PEiD program

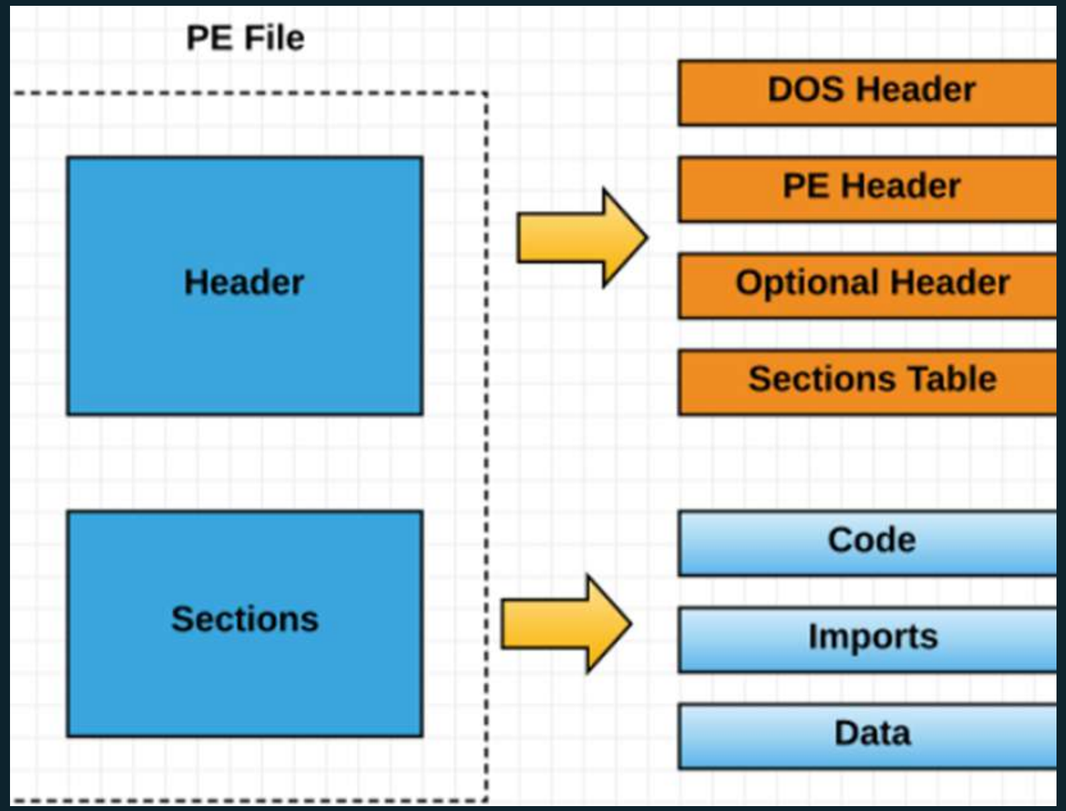
Static Analysis: PE Information

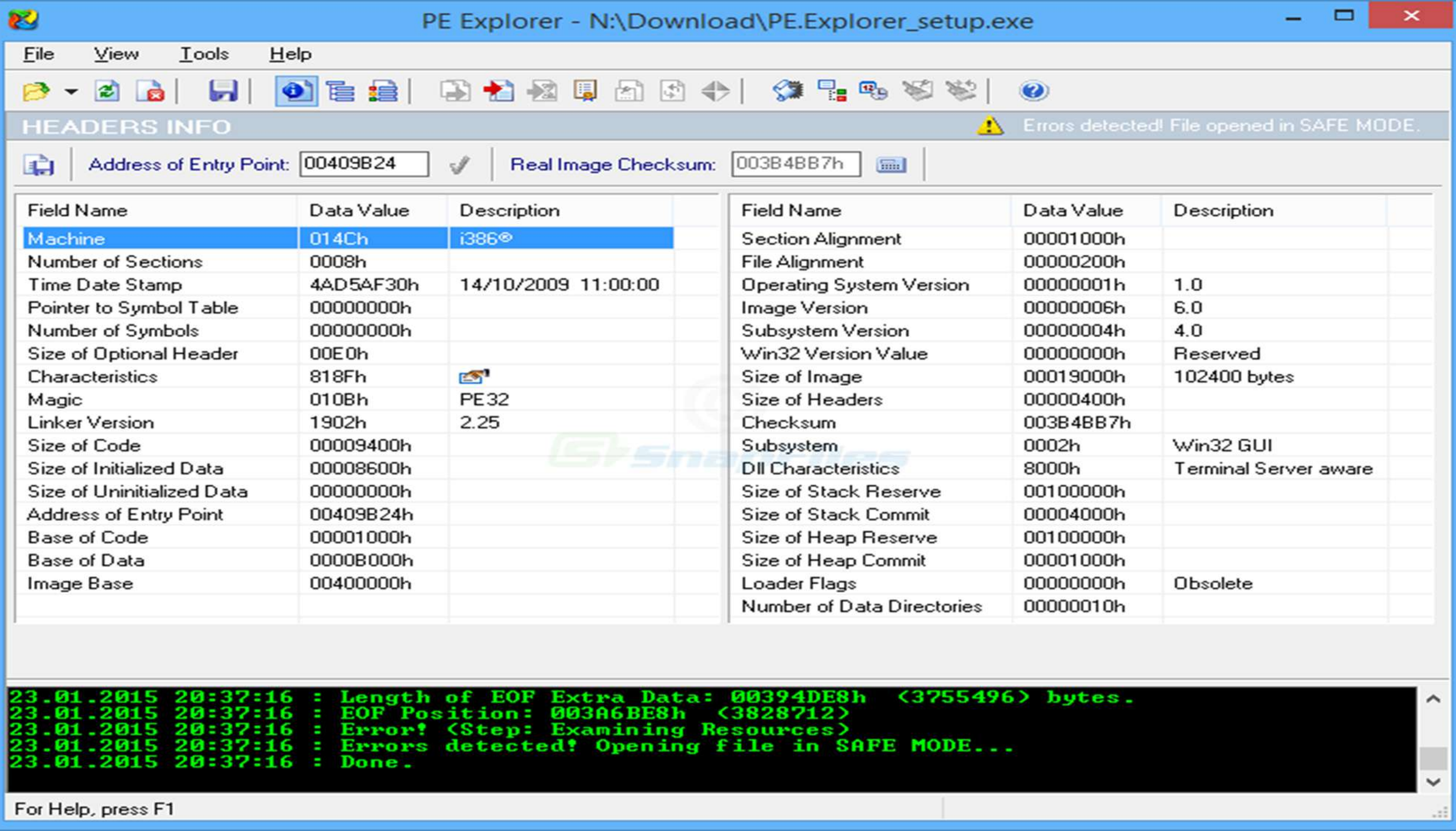
01 PE is a file format that Windows OS use for executable files

02 PE format contains header and sections that store metadata about file and code mapping in an OS

03 PE of a file contains instructions & program code, import/export information, programs global data, resources such as icons, images, menus, strings etc.

04 Tool: **PE Explorer tools** allow us to Reverse Engineer, open, view, edit a variety of 32-bit windows executable file types




PE Explorer - N:\Download\PE.Explorer_setup.exe
File View Tools Help
HEADERS INFO
Errors detected! File opened in SAFE MODE.
Address of Entry Point: 00409B24
Real Image Checksum: 003B4BB7h
Field Name Data Value Description
Machine 014Ch i386®
Number of Sections 0008h
Time Date Stamp 4AD5AF30h 14/10/2009 11:00:00
Pointer to Symbol Table 00000000h
Number of Symbols 00000000h
Size of Optional Header 00E0h
Characteristics 818Fh
Magic 010Bh PE32
Linker Version 1902h 2.25
Size of Code 00009400h
Size of Initialized Data 00008600h
Size of Uninitialized Data 00000000h
Address of Entry Point 00409B24h
Base of Code 00001000h
Base of Data 0000B000h
Image Base 00400000h
Field Name Data Value Description
Section Alignment 00001000h
File Alignment 00000200h
Operating System Version 00000001h 1.0
Image Version 00000006h 6.0
Subsystem Version 00000004h 4.0
Win32 Version Value 00000000h Reserved
Size of Image 00019000h 102400 bytes
Size of Headers 00000400h
Checksum 003B4BB7h
Subsystem 0002h Win32 GUI
Dll Characteristics 8000h Terminal Server aware
Size of Stack Reserve 00100000h
Size of Stack Commit 00004000h
Size of Heap Reserve 00100000h
Size of Heap Commit 00001000h
Loader Flags 00000000h Obsolete
Number of Data Directories 00000010h
23.01.2015 20:37:16 : Length of EOF Extra Data: 00394DE8h (3755496) bytes.
23.01.2015 20:37:16 : EOF Position: 003A6BE8h (3828712)
23.01.2015 20:37:16 : Error! (Step: Examining Resources)
23.01.2015 20:37:16 : Errors detected! Opening file in SAFE MODE...
23.01.2015 20:37:16 : Done.
For Help, press F1

Static Analysis: ELF files

ELF is a general executable file format in LINUX

`readelf -s <malware-sample>`

Displays info about ELF objects and extract static artifacts from ELF executable such as functions and variables used in source code.

`readelf -h <malware-sample>`

Identify ELF executable file header. Determine file architecture and machine for which file is designed to run

`readelf -l <malware-sample>`

Identify program headers in ELF executable file. Reveals memory layout of the binary code and helps determine whether ELF executable file is properly packed or not.

Static Analysis: File Dependency

01 Find information about libraries & file dependencies as they contain information about run time requirements of an application.

02 File dependencies include linked libraries, functions and function calls.

03 Kernel32.dll, Advapi32.dll, User32.dll etc. are some standard DLLs

04 Tool: Dependency Walker lists all dependent modules of an executable file and builds hierarchical tree diagram.

05 It also records all the functions of each module's exports and calls

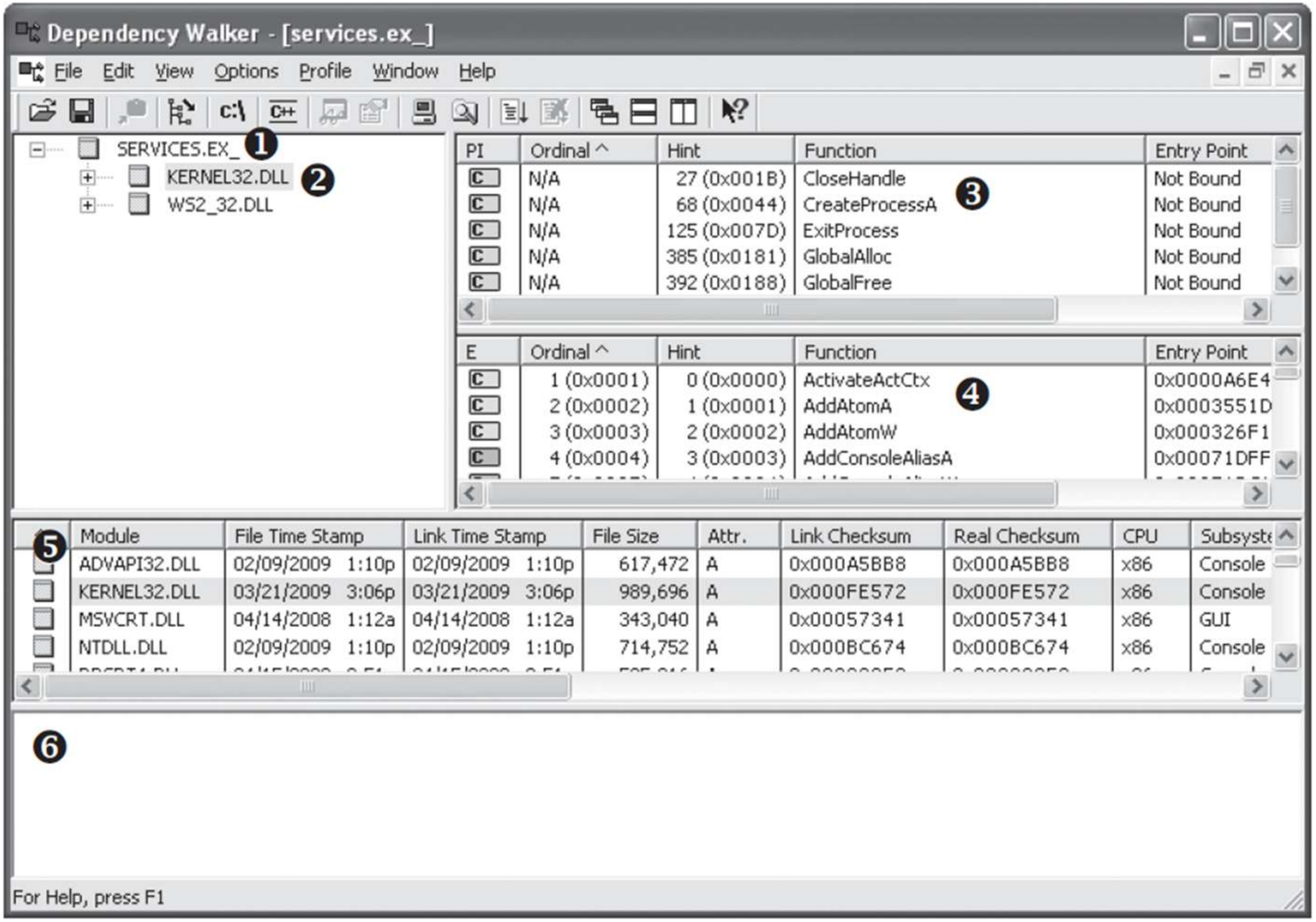


Figure 1-6: The Dependency Walker program

Static Analysis: Malware Disassembly

01 Converts raw binary instructions into assembly code

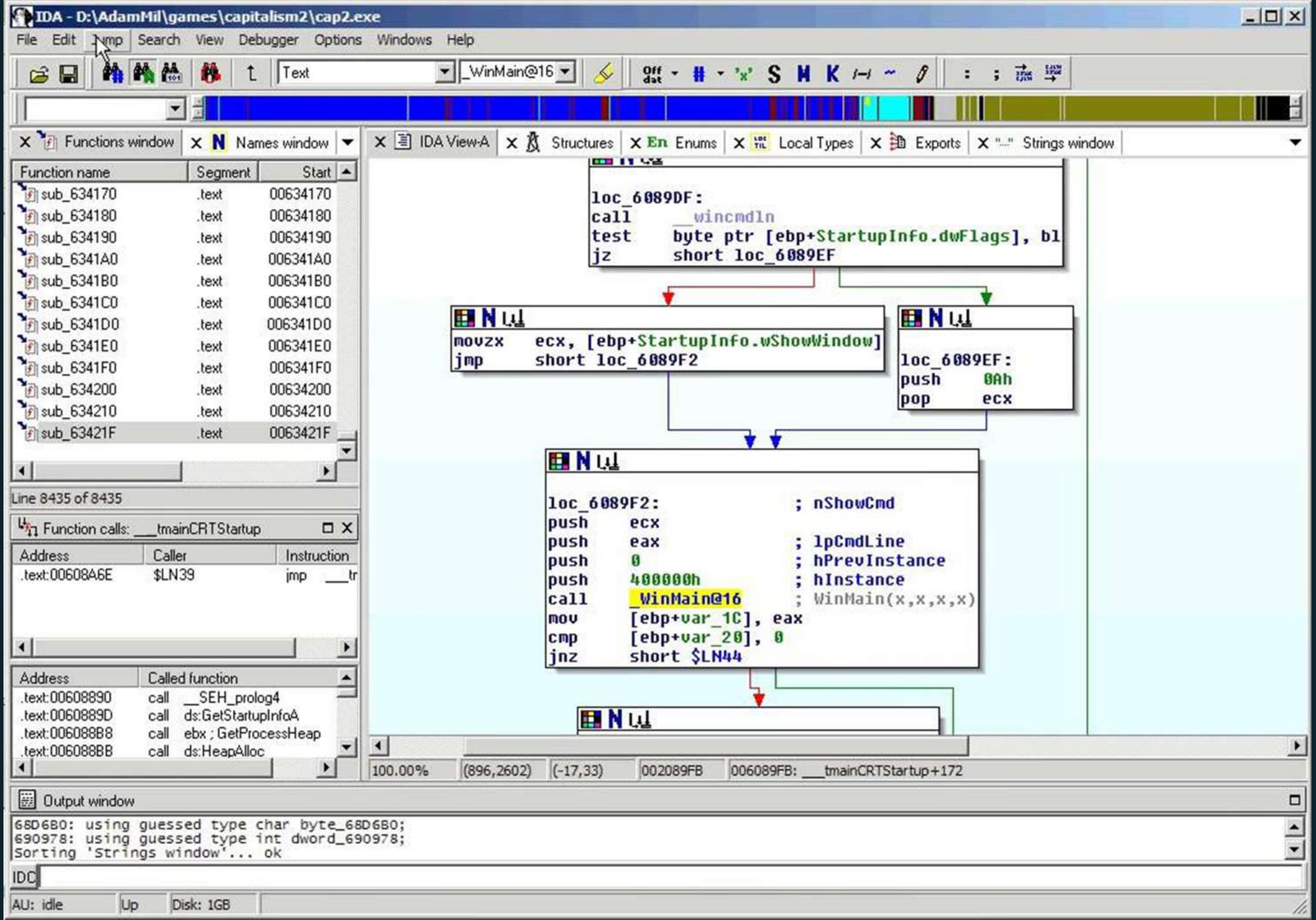
02 Malware is examined without executing it, reducing the risk of infection

03 **Identify system calls, API imports, and encryption routines**

04 Examining the entry point, function calls, and loops helps determine if the malware performs keylogging, network communication, or privilege escalation.

05 Unpack & reverse-engineering obfuscation

07 Tools: IDA Pro, Ghidra etc


IDA - D:\AdamMil\games\capitalism2\cap2.exe
File Edit Jump Search View Debugger Options Windows Help
Text
_WinMain@16
Functions window
Names window
Function name Segment Start
sub_634170 .text 00634170
sub_634180 .text 00634180
sub_634190 .text 00634190
sub_6341A0 .text 006341A0
sub_6341B0 .text 006341B0
sub_6341C0 .text 006341C0
sub_6341D0 .text 006341D0
sub_6341E0 .text 006341E0
sub_6341F0 .text 006341F0
sub_634200 .text 00634200
sub_634210 .text 00634210
sub_63421F .text 0063421F
Line 8435 of 8435
Function calls: ___tmainCRTStartup
Address Caller Instruction
.text:00608A6E $LN39 jmp ___tr
Address Called function
.text:00608890 call __SEH_prolog4
.text:0060889D call ds:GetStartupInfoA
.text:006088B8 call ebx ; GetProcessHeap
.text:006088BB call ds:HeapAlloc
IDA View-A
Structures
Enums
Local Types
Exports
Strings window
loc_6089DF:
call __wincmdln
test byte ptr [ebp+StartupInfo.dwFlags], bl
jz short loc_6089EF
movzx ecx, [ebp+StartupInfo.wShowWindow]
jmp short loc_6089F2
loc_6089EF:
push 0Ah
pop ecx
loc_6089F2: ; nShowCmd
push ecx
push eax ; lpCmdLine
push 0 ; hPrevInstance
push 400000h ; hInstance
call _WinMain@16 ; WinMain(x,x,x,x)
mov [ebp+var_1C], eax
cmp [ebp+var_20], 0
jnz short $LN44
100.00% (896,2602) (-17,33) 002089FB 006089FB: ___tmainCRTStartup+172
Output window
68D6B0: using guessed type char byte_68D6B0;
690978: using guessed type int dword_690978;
Sorting 'Strings window'... ok
IDC
AU: idle Up Disk: 1GB

Dynamic Malware Analysis

Malware file is actually executed in an isolated environment so that it does not propagate to production environment.

System Baselining

- Take snapshot of system before executing the malware and compare with system’s state after executing it.
- Help understand changes that malware has made across the system.
- Check file system, registry, open ports, network activity etc.

Host Integrity Check

- Port monitor
- Process monitor
- Registry monitor
- Start-up program monitor etc.

Dynamic Analysis: Port Monitor

Malware may try to access a particular port and try to establish connection with remote C2 Center

Port Monitoring Tools:

TCPView

1.Free tool developed by Microsoft. It is used to monitor real-time TCP & UDP connections on a Windows system, showing details like remote/local addresses, ports, and process associations.

Netstat - Windows command line utility

1.Free tool developed by Microsoft. It is used to monitor real-time TCP & UDP connections on a Windows system, showing details like remote/local addresses, ports, and process associations.

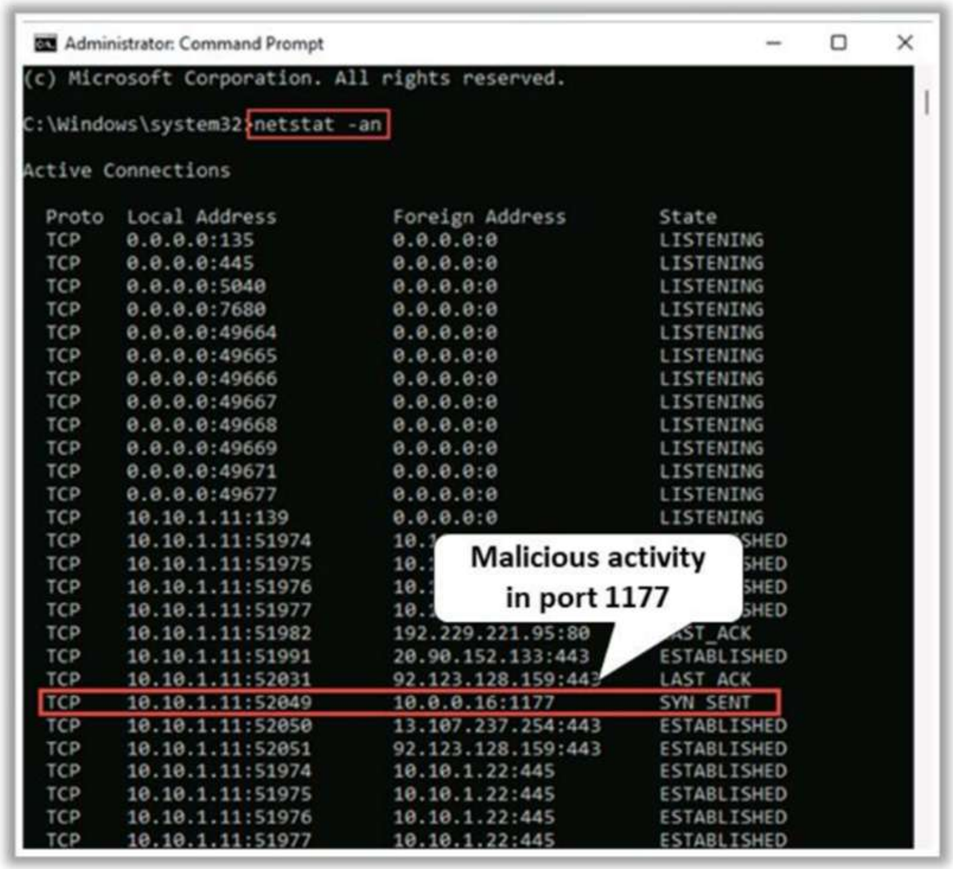


Figure 7.113: Screenshot of Netstat

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
QualysAgent.exe	1512	TCP	Established	host.docker.internal	1131	qagpublic.qg3.apps.qua...	https	03/19/21 21:05:35.149	QualysAgent	4
OUTLOOK.EXE	27004	TCP	Established	host.docker.internal	1129	40.101.92.194	https	03/19/21 21:05:35.649	OUTLOOK.EXE	3
devenv.exe	15256	TCP	Established	host.docker.internal	1126	51.107.59.180	https	03/19/21 21:05:31.734	devenv.exe	
Teams.exe	26092	TCP	Established	host.docker.internal	1123	52.114.92.151	https	03/19/21 21:05:16.124	Teams.exe	7
OUTLOOK.EXE	27004	TCP	Established	host.docker.internal	1117	52.114.128.71	https	03/19/21 21:05:04.083	OUTLOOK.EXE	6
devenv.exe	15256	TCP	Established	host.docker.internal	1116	lb-140-82-121-5-fra.gith...	https	03/19/21 21:05:03.265	devenv.exe	3
devenv.exe	15256	TCP	Close Wait	kubernetes.docker.inter...	1106	kubernetes.docker.inter...	1112	03/19/21 21:05:01.430	devenv.exe	6
Microsoft.Alm.Shared...	50384	TCP	Fin Wait 2	kubernetes.docker.inter...	1112	kubernetes.docker.inter...	1106	03/19/21 21:05:01.010	Microsoft.Alm.Shared....	6
Microsoft.Alm.Shared...	50384	TCP	Listen	kubernetes.docker.inter...	1111	0.0.0.0	0	03/19/21 21:05:01.680	Microsoft.Alm.Shared....	
devenv.exe	15256	TCP	Listen	kubernetes.docker.inter...	1106	0.0.0.0	0	03/19/21 21:04:58.789	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1105	13.66.38.99	https	03/19/21 21:04:55.470	devenv.exe	5
devenv.exe	15256	TCP	Established	host.docker.internal	1104	13.66.241.134	https	03/19/21 21:04:54.104	devenv.exe	5
devenv.exe	15256	TCP	Established	host.docker.internal	1103	13.77.157.133	https	03/19/21 21:04:53.935	devenv.exe	5
ServiceHub.IdentityH...	17188	TCP	Established	host.docker.internal	1102	51.107.59.180	https	03/19/21 21:04:52.098	ServiceHub.IdentityHo...	8
firefox.exe	3604	TCP	Established	host.docker.internal	1101	51.107.59.180	https	03/19/21 21:04:52.682	firefox.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1099	13.107.42.18	https	03/19/21 21:04:51.587	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1098	13.107.42.20	https	03/19/21 21:04:51.107	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1097	13.107.42.18	https	03/19/21 21:04:50.454	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1096	13.107.42.20	https	03/19/21 21:04:50.869	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1095	13.107.42.18	https	03/19/21 21:04:50.445	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1093	13.107.42.20	https	03/19/21 21:04:50.260	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1092	13.107.42.18	https	03/19/21 21:04:50.460	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1091	13.107.42.20	https	03/19/21 21:04:49.818	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1090	13.107.42.18	https	03/19/21 21:04:49.227	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1089	13.107.42.20	https	03/19/21 21:04:49.767	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1088	13.107.42.18	https	03/19/21 21:04:49.681	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1087	13.107.42.18	https	03/19/21 21:04:49.352	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1084	13.107.42.20	https	03/19/21 21:04:48.252	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1083	13.107.42.18	https	03/19/21 21:04:48.793	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1082	13.107.42.18	https	03/19/21 21:04:48.682	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1081	13.107.42.20	https	03/19/21 21:04:48.775	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1080	13.107.42.18	https	03/19/21 21:04:48.580	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1079	13.107.42.20	https	03/19/21 21:04:48.957	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1078	13.107.42.18	https	03/19/21 21:04:48.994	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1077	13.107.42.18	https	03/19/21 21:04:47.460	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1076	13.107.42.20	https	03/19/21 21:04:47.063	devenv.exe	

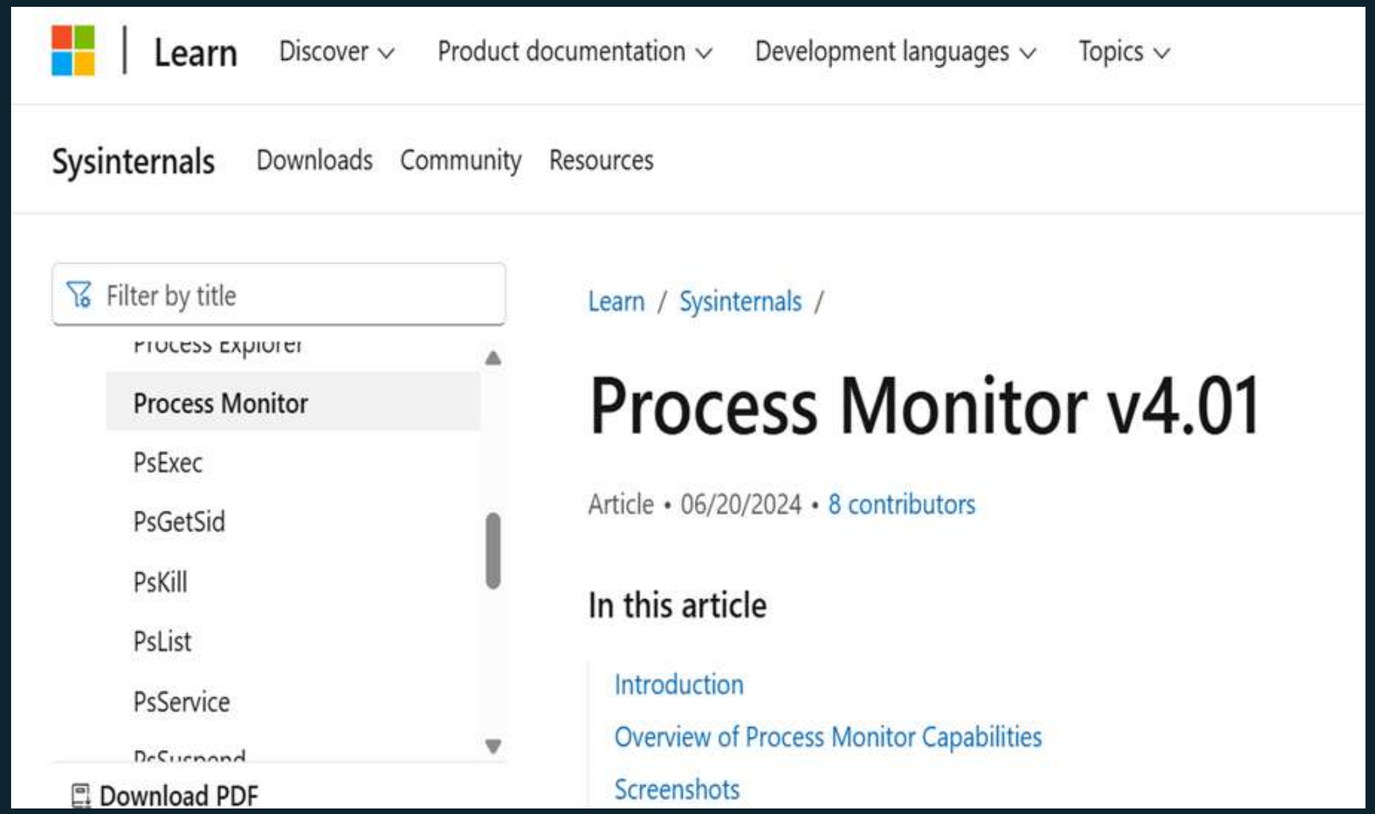
Endpoints: 256 Established: 175 Listening: 64 Time Wait: 9 Close Wait: 6 Update: 2 sec

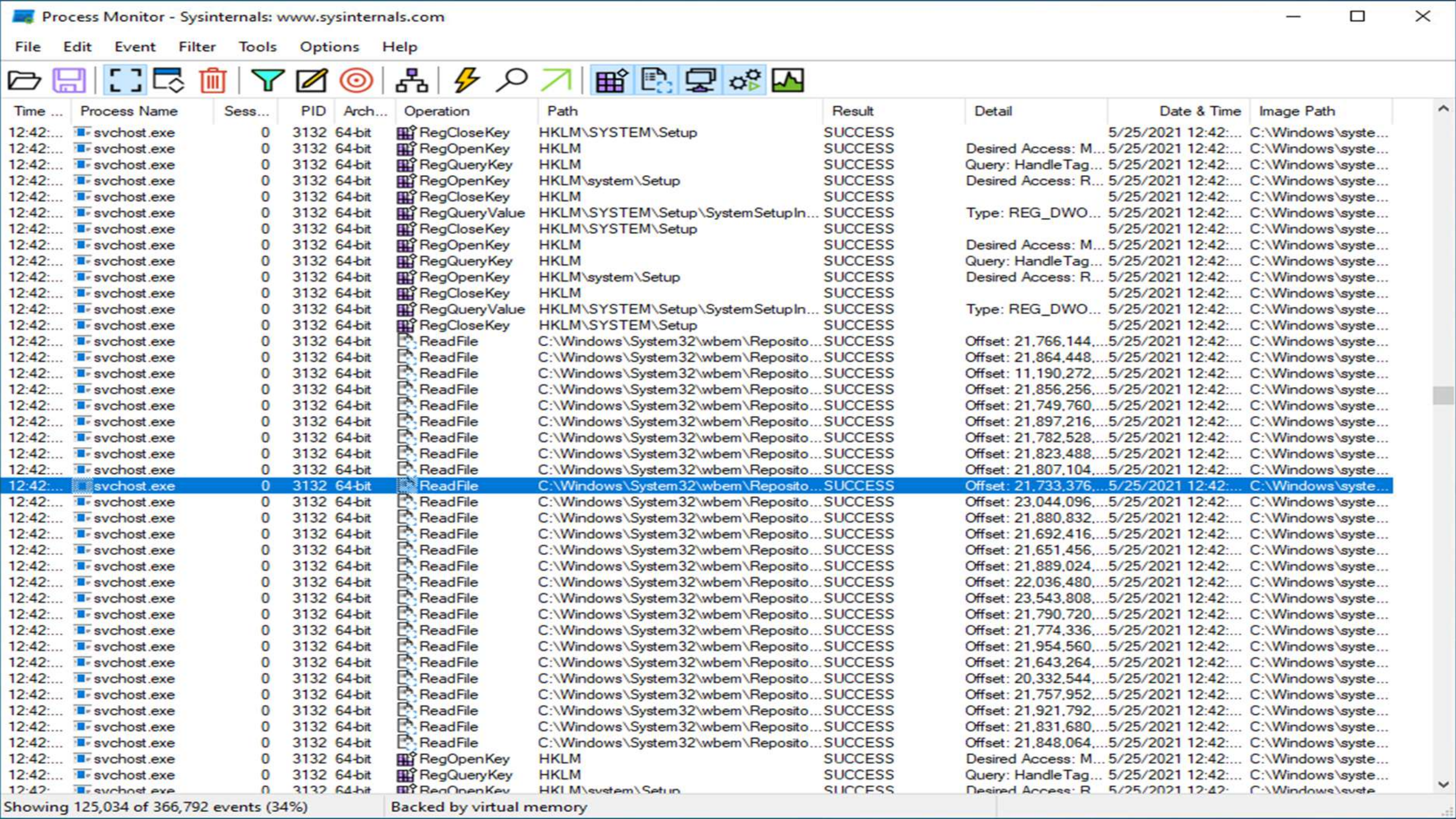
Dynamic Analysis: Process Monitor

- Identify and understand the process that malware initiates after execution
- Observe child process, associated handles, loaded libraries, functions and execution flow of booth time processes.
- Compare the processes before and after execution.

Tool: Process Monitor

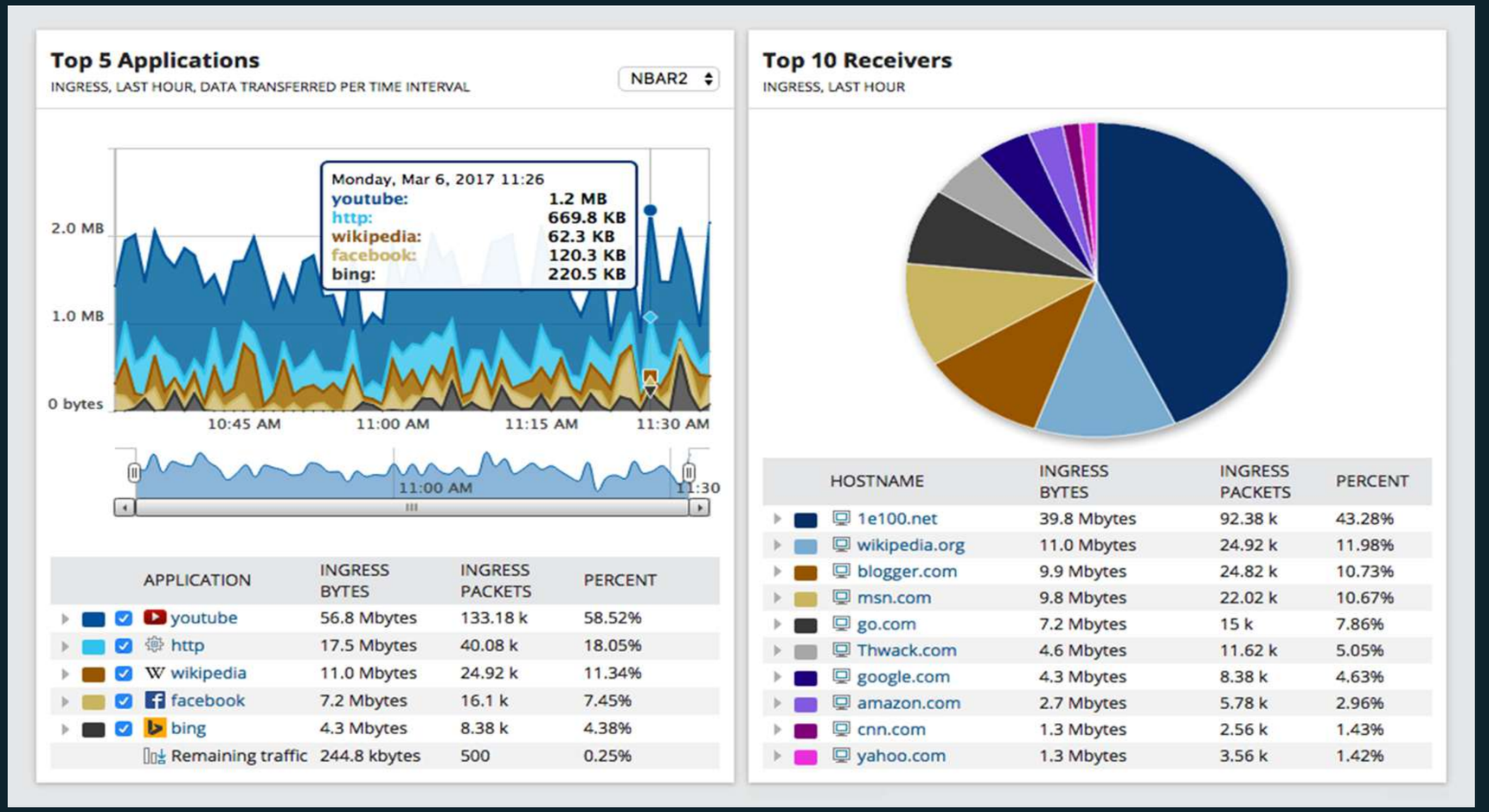
- Reliably captures process details, including image path, command line, user and session ID
- Captures tens to millions of events and GBs of log data




Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name Sess... PID Arch... Operation Path Result Detail Date & Time Image Path
12:42:... svchost.exe 0 3132 64-bit RegCloseKey HKLM\SYSTEM\Setup SUCCESS 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegOpenKey HKLM SUCCESS Desired Access: M... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegQueryKey HKLM SUCCESS Query: HandleTag... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegOpenKey HKLM\system\Setup SUCCESS Desired Access: R... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegCloseKey HKLM SUCCESS 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegQueryValue HKLM\SYSTEM\Setup\SystemSetupIn... SUCCESS Type: REG_DWO... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegCloseKey HKLM\SYSTEM\Setup SUCCESS 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegOpenKey HKLM SUCCESS Desired Access: M... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegQueryKey HKLM SUCCESS Query: HandleTag... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegOpenKey HKLM\system\Setup SUCCESS Desired Access: R... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegCloseKey HKLM SUCCESS 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegQueryValue HKLM\SYSTEM\Setup\SystemSetupIn... SUCCESS Type: REG_DWO... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegCloseKey HKLM\SYSTEM\Setup SUCCESS 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,766,144,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,864,448,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 11,190,272,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,856,256,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,749,760,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,897,216,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,782,528,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,823,488,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,807,104,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,733,376,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 23,044,096,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,880,832,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,692,416,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,651,456,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,889,024,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 22,036,480,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 23,543,808,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,790,720,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,774,336,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,954,560,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,643,264,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 20,332,544,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,757,952,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,921,792,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,831,680,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,848,064,... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegOpenKey HKLM SUCCESS Desired Access: M... 5/25/2021 12:42:... C:\Windows\syste...
12:42:... svchost.exe 0 3132 64-bit RegQueryKey HKLM SUCCESS Query: HandleTag... 5/25/2021 12:42:... C:\Windows\syste...
Showing 125,034 of 366,792 events (34%)
Backed by virtual memory

Dynamic Analysis: Network Traffic Monitor

- Capture network traffic and analyze it carefully
- Tools: Wireshark, CAPSA Network analyzer, PRTG Network Monitor, Solar Wind NetFlow Traffic Analyzer



Start-up Program Monitor

Malware may add itself to start up menu to perform malicious activity whenever the system starts.

Scan for suspicious start up program manually or use tool such as Autoruns for windows.

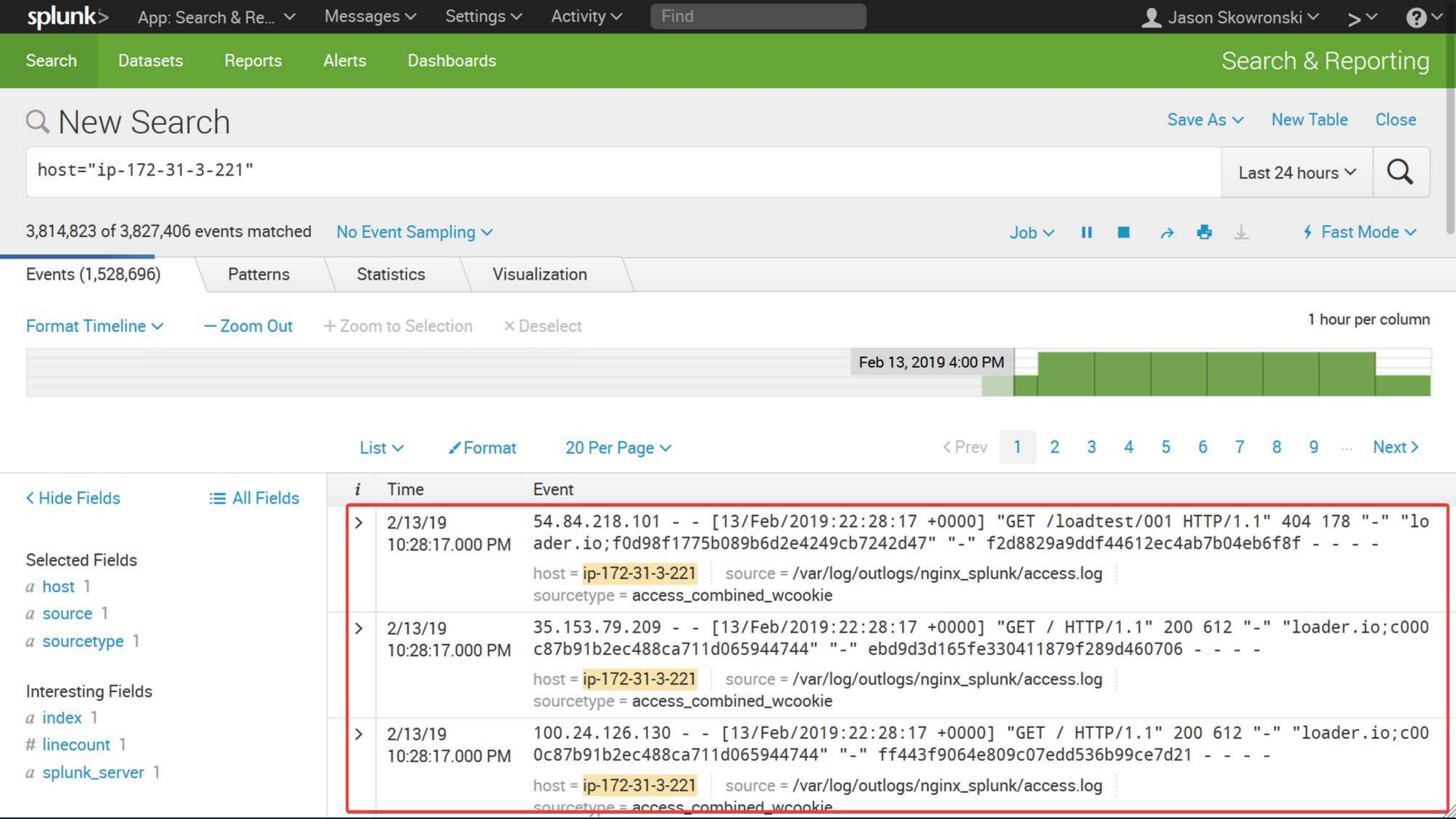
- Check all the start-up program entries in registry
- Check device drivers automatically loaded
- Check boot manager entries
- Check services that start automatically
- Check start-up folder

Event Logs Monitoring

Logs are the primary source of information and help in identifying attacks and security gaps.

Logs of Firewall, IDS/IPS, web servers & authentication servers are monitored.

Tool: Splunk collects all event logs, conducts real time monitoring and generates alerts. Both free and paid versions are available


splunk> App: Search & Re... Messages Settings Activity Find Jason Skowronski
Search Datasets Reports Alerts Dashboards Search & Reporting
New Search
Save As New Table Close
host="ip-172-31-3-221"
Last 24 hours
3,814,823 of 3,827,406 events matched No Event Sampling
Job Fast Mode
Events (1,528,696) Patterns Statistics Visualization
Format Timeline Zoom Out Zoom to Selection Deselect
1 hour per column
Feb 13, 2019 4:00 PM
List Format 20 Per Page
Prev 1 2 3 4 5 6 7 8 9 Next
Hide Fields All Fields
Selected Fields
a host 1
a source 1
a sourcetype 1
Interesting Fields
a index 1
linecount 1
a splunk_server 1
i Time Event
2/13/19 10:28:17.000 PM
54.84.218.101 - - [13/Feb/2019:22:28:17 +0000] "GET /loadtest/001 HTTP/1.1" 404 178 "-" "loader.io;f0d98f1775b089b6d2e4249cb7242d47" "-" f2d8829a9ddf44612ec4ab7b04eb6f8f - - - -
host = ip-172-31-3-221 source = /var/log/outlogs/nginx_splunk/access.log
sourcetype = access_combined_wcookie
2/13/19 10:28:17.000 PM
35.153.79.209 - - [13/Feb/2019:22:28:17 +0000] "GET / HTTP/1.1" 200 612 "-" "loader.io;c000c87b91b2ec488ca711d065944744" "-" ebd9d3d165fe330411879f289d460706 - - - -
host = ip-172-31-3-221 source = /var/log/outlogs/nginx_splunk/access.log
sourcetype = access_combined_wcookie
2/13/19 10:28:17.000 PM
100.24.126.130 - - [13/Feb/2019:22:28:17 +0000] "GET / HTTP/1.1" 200 612 "-" "loader.io;c000c87b91b2ec488ca711d065944744" "-" ff443f9064e809c07edd536b99ce7d21 - - - -
host = ip-172-31-3-221 source = /var/log/outlogs/nginx_splunk/access.log
sourcetype = access_combined_wcookie

Installation Monitor

Detect hidden & background installation performed by malware. Traces of the application data may remain on the system after system or user installs or uninstalls any software application.

There is a need to detect files and folders modified and created during the process.

Tool:

Mirekusoft monitors resources that are created when program is installed. Provides information such as disk, CPU and memory consumption of the program.

Files and Folder Monitor

Find files and folders that malware creates and analyze them to collect relevant information. These may contain hidden program code or malicious strings that malware may execute later.

Tools: PA File Sight & Tripwire File Integrity

Device Driver Monitor

A user may download malware along with an infected driver from untrusted sources.

Tools: Driver View and Driver Detective

DNS Monitor

Determine whether malware changes DNS server and redirects the victim to a fraud web pag

Tool: DNS Query Sniffer verifies the DNS servers that malware tries to connect to & identi the type of connection. Provides DNS query information such as host name, port numbe equest type, time, duration etc. for every DNS query

API Call Monitor

Malware programs make use of APIs to access OS information such as file systems, thread errors, registry, kernel, mouse pointers etc.

Tool: API monitor , Postman

System Call Monitor

- System call acts as an interface between application & kernel.
- Such calls are generated by application when it requires to access specific resources from the OS.
- Monitoring of system calls can reveal type of damage caused by malware.

Tools: strace in Linux is used to extract system calls from a sample file

Scheduled Task Monitor

Malware such as logic bomb may trigger at a specific time using the windows task scheduler.

Tools: schtasks a command line tool is sued to display list of all system scheduled tasks

1.3.4 Known Malware Check

Requirement:

- Vendor shall submit Software Test Document (STD) of the network product proving that the network product is free from known malware/spyware to lab for scrutiny

The test document may comprise of:

1. Introduction
2. Test Objective
3. Test Scope
4. Testing Methodology
5. Result Summary
6. Conclusion
7. Recommendations

Test Case	Method	Tools Used	Expected Outcome	Result
Firmware Analysis	Extract and analyze firmware for malicious components	Binwalk, Firmware Mod Kit	No suspicious binaries or scripts found	Pass/Fail
Signature-based Scan	Scan firmware and router OS for known malware signatures	ClamAV, VirusTotal	No known malware signatures detected	Pass/Fail
Heuristic Analysis	Identify suspicious patterns and behavior in software	YARA, Cuckoo Sandbox	No abnormal patterns detected	Pass/Fail
Network Traffic Analysis	Monitor network traffic for unusual behavior	Wireshark, Zeek (Bro)	No unauthorized outbound connections	Pass/Fail
Process and Service Analysis	List and analyze running processes	Procmon, ps (Linux)	No suspicious processes	Pass/Fail
File Integrity Check	Verify file hashes with known good versions	Tripwire, HashMyFiles	No unauthorized modifications	Pass/Fail
Memory Analysis	Dump and scan memory for malware indicators	Volatility, Rekall	No malicious code in memory	Pass/Fail


Thank
You