



Malware Sandboxing

(Build your own Sandbox)

for SOC Analysts, Information security Analysts,
and investigators who want to learn how to
perform initial both static and dynamic malware
analysis



1

by\ Mostafa Yahia

<https://t.me/learningnets>

Table of Contents

Introduction:	3
Sandbox Definition:.....	3
Installation Requirements:.....	4
<i>Hardware Requirements:</i>	4
<i>Software Requirements:</i>	4
Tools Required for Analysis	4
Static analysis tools:	4
Dynamic analysis tools:.....	5
Guest Preparation:	6
Guest Preparation Steps:.....	6
Tips to evade the Sandbox Detection.....	6
Put them All together:.....	7
Static analysis phase:.....	7
Dynamic analysis Phase:	9
Demo Lab:	12
File Identification phase (YARA)	12
Static analysis Phase:.....	13
Dynamic Analysis Phase:	17

Introduction:

Due to the increase of the malwares that spread many ways like USB or phishing mail attacks against the enterprise environments or even targeting the individuals, you will hope to test every file you suspect on SandBox to analyze the file before running it on a real environment to make sure that this file is not malicious or harmful. During this Guide, you will learn a little of the static and dynamic malware analysis tools and techniques used to find the malicious artifacts.

Sandbox Definition:

In cybersecurity, the sandbox technology is an isolated test environment that looks like end-user operating environments, to safely execute the suspicious files and know its behavior. It is better if you deal with Zero-day malware.

Installation Requirements:

to build your Sandbox it should have the basic installation requirements whether hardware Requirements or software Requirements.

Hardware Requirements:

- 2.4 GHz CPU minimum or higher
- 6 GB RAM or higher
- 100 GB free hard drive space or higher

Software Requirements:

- VMware or Virtual Box
- The Host Operating system (Linux, MacOS, WIN 10, Win 8, etc..)
- The Guest Operating system (WIN 10, Win 8, etc..)

Tools Required for Analysis

Static analysis tools:

- **YARA:** YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples, we will use YARA to identify the malware family (ransomware, Trojan, etc...) by look for certain characteristics.
Download the tool from here(<https://virustotal.github.io/yara/>)
You can find some of YARA Rules repository here (<https://github.com/Yara-Rules/rules>)
- **EXEinfo:** great GUI tool to analyze the PE header information, we will use it to verify if we are dealing with the packer or not, and if so how to unpack it.
Download the tool from here (<https://exeinfo-pe.en.uptodown.com/windows>)

- **Compute hash:** a suggested tool to calculate the file hash (feel free to use any other tool).
Download the tool from here
(<http://www.subisoft.net/ComputeHash.aspx>)
- **PEstudio:** very useful tool has been made specifically for static malware Analysis. To looking for the malicious malware strings, functions, etc. We will explore it in more details later.
Download the tool from here (<https://www.winitor.com/features>)

Dynamic analysis tools:

- **FakeNet:** tool that aids in the dynamic analysis of malicious software. The tool simulates a network so that malware interacting with a remote host continues to run allowing the analyst to observe the malware's network activity from within a safe environment.
Download the tool from here
(<https://www.fireeye.com/services/freeware/fakenet-ng.html>)
- **RegShot:** Registry and file system integrity monitor tool.
Download the tool from here
(<https://sourceforge.net/projects/regshot/>)
- **ProcMon:** record the real-time system activity like process create, register edited or added, touch files, network connection, etc. with a great filtering capability.
Download the tool from here
(<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>)
- **ProcDot:** visualize the ProcMon output.
Download the tool from here
(<https://cert.at/en/downloads/software/software-procdot>)
- **Autoruns:** very useful free tool from Microsoft that check the code signing certificate on the persistence locations like the Registry paths, scheduled tasks.
Download the tool from here (<https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>)

Guest Preparation:

WARNING: you will be dealing with a very dangerous malware samples, so please be careful and follow below instructions.

Guest Preparation Steps:

- Create new windows Virtual machine on either VMware or Virtual Box.
- Download all of the above tools.
- **Setup a host-only network and Isolate the Guest by preventing the Drag & Drop and Copy & Paste from, or to the machine.** This step to isolate the VM from the internet or network access. (you don't want to infect your host during analyzing a malware)
- Apply all of the below **Tips to evade the Sandbox Detection**
- Now take a snapshot. (Clean Snapshot to revert it after finish malware analyzing)

Tips to evade the Sandbox Detection.

Before malware running on the victim machine it may check for the presence of a virtual machine environment (sandbox) or search for any Malware analysis tools exist on the VM like (Wireshark, PEStudio, etc.), if it detected any presence of a VM or tools it will change the real intended Actions or maybe delete itself to evade the detection and analysis of tools and activities.

What I should do to evade the SandBox Detection?

- Keep the VM Hard Disk large as you can (higher than 100 GB).
- Increase the RAM memory of the VM (4 GB or higher).
- Don't Install VM Guest tools, if it is required to install it, make sure to uninstall it before executing the malware.
- Install the common End-user tools (Adobe, Excel, Firefox, etc.), put many random Files on the Desktop and the hard Disk partitions like Pictures, Videos or even small games and don't install any of the VM guest tools.
- Open many files and Applications before executing the malware to increase VM Recent Activity.

- Use Two or more vCPU cores on a VM.
- Change all the Malware analysis name to games or Music, for example, change “PEstudio” tool name to “hello”.
- Use normal logging username like (Mostafa Yahia, will smith, etc..), the same for the machine name.

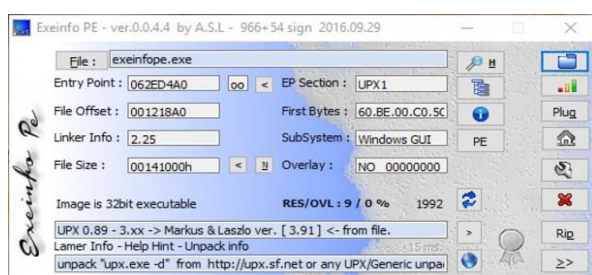
Put them All together:

now you should have downloaded the required tools and Prepared your guest to analyze your first malware, we will analyze the malware during Two phases: static analysis phase and Dynamic Analysis Phase.

Static analysis phase:

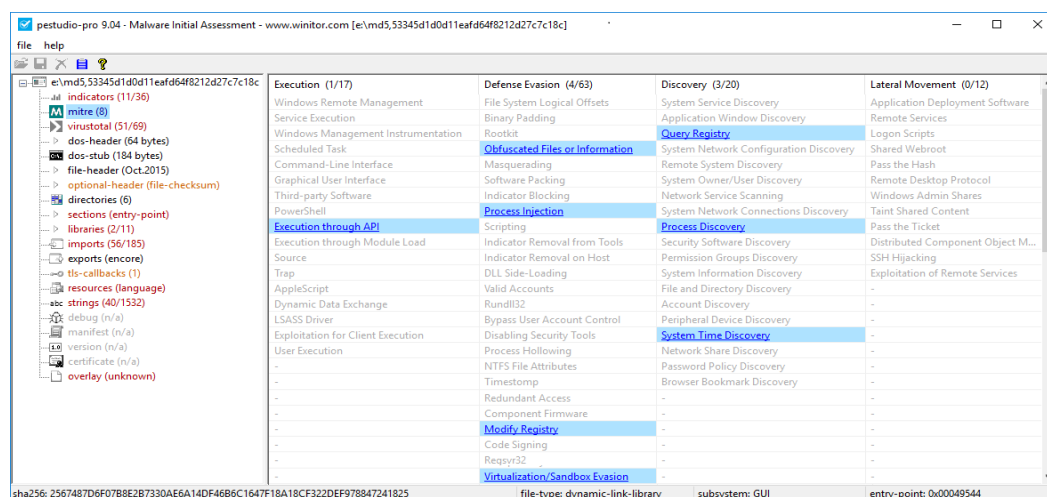
During this phase we intend to identify the malware type by using YARA tool and analyze the malware without executing it, such phase requires little experience on the malware analysis field but we will easily try to extract some useful info during this phase by using easy tools like: (EXEinfo, PEstudio).

- 1- **compute hash:** Run the compute hash tool to collect the file hashes then search for such hashes on the threat intelligence platforms such as Virustotal, X-Force or even google, if the malware has seen before you will find a lot of useful info on the communities.
- 2- **YARA:** Run YARA rules against the file to identify the malware family, use this command Syntax to test the rules against the target file `[yara [OPTIONS] -C RULES_FILE TARGET_FILE]`, to understand YARA command line syntax follow the below URL. (<https://yara.readthedocs.io/en/stable/commandline.html>)
- 3- **EXEinfo PE:** we will use this tool to tell us if we are dealing with packed file or not, if so the last two labels include all the info that needed like what is the packer that Attacker has used and how to unpack it.



4- **PEstudio**: if you are intended to use just one tool during the static analysis phase this tool will be the PEStudio, it's really an amazing tool that made specifically for static malware analysis, the tool has integrated with MITRE ATT&CK and VirusTotal.

As we said before this phase requires a little experience in the malware analysis field, so we will focus on some features that easy to use.

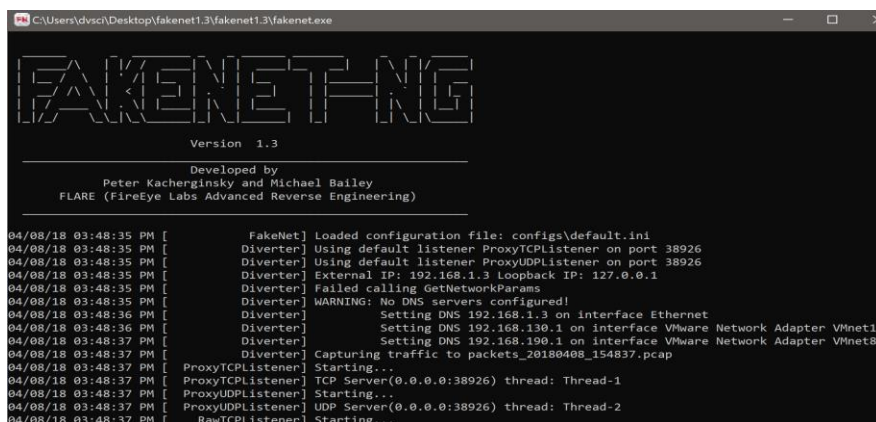


- **indicators**: this tab includes all suspicious Indicators like bad reputation on virustotal, the perform function that blacklisted on the PEstudio, and more.
- **VirusTotal**: PEstudio will send an MD5 hash of the file to Virustotal and retrieve the results.
- **File header**: contain the file made date and the malware author computer language.
- **Imports**: PEstudio has a list of blacklisted functions and libraries which are often used by malware.
- **Strings**: PEstudio will list all the suspicious strings those found on the analyzed file.
- **Version**: show you the original file name, the company name, the language of the author, and file type.

Dynamic analysis Phase:

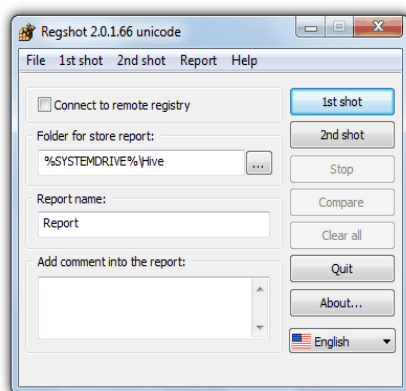
During this phase we will run all the Dynamic analysis tools that we will explore later with admin privilege to give the running tools vision on the entire system then execute the malware and watch the malware behavior e.g. network communication, registry editing, downloading additional payload, etc..., at the first, we will run all the tools together then we will execute the Malware.

- 1- **FakeNet:** as you remember we have denied the VM from the network and the internet communications, but as you know the malwares are usually tending to communicate with their C&C server for more payload or for more instructions, so the FakeNet will introduce all of the internet services HTTP, DNS, SMTP, etc... then log all activities in a log file and PCAP File for all captured network traffic.



```
C:\Users\dvsc\Desktop\Fakenet1.3\Fakenet1.3\Fakenet.exe
FAKENET-NG
Version 1.3
Developed by
Peter Kacherginsky and Michael Bailey
FLARE (FireEye Labs Advanced Reverse Engineering)
04/08/18 03:48:35 PM [ FakeNet] Loaded configuration file: configs/default.ini
04/08/18 03:48:35 PM [ Diverter] Using default listener ProxyTCPListener on port 38926
04/08/18 03:48:35 PM [ Diverter] Using default listener ProxyUDPListener on port 38926
04/08/18 03:48:35 PM [ Diverter] External IP: 192.168.1.3 Loopback IP: 127.0.0.1
04/08/18 03:48:35 PM [ Diverter] Failed calling GetNetworkParams
04/08/18 03:48:35 PM [ Diverter] WARNING: No DNS servers configured!
04/08/18 03:48:36 PM [ Diverter] Setting DNS 192.168.1.3 on interface Ethernet
04/08/18 03:48:36 PM [ Diverter] Setting DNS 192.168.130.1 on interface VMware Network Adapter VMnet1
04/08/18 03:48:37 PM [ Diverter] Setting DNS 192.168.190.1 on interface VMware Network Adapter VMnet8
04/08/18 03:48:37 PM [ Diverter] Capturing traffic to packets_20180408_154837.pcap
04/08/18 03:48:37 PM [ ProxyTCPListener] Starting...
04/08/18 03:48:37 PM [ ProxyTCPListener] TCP Server(0.0.0.0:38926) thread: Thread-1
04/08/18 03:48:37 PM [ ProxyUDPListener] Starting...
04/08/18 03:48:37 PM [ ProxyUDPListener] UDP Server(0.0.0.0:38926) thread: Thread-2
04/08/18 03:48:37 PM [ RawTCPListener] Starting...
```

- 2- **RegShot:** file system and registry monitor tool, the tool job is simple just take first shot from entire the system and after running the malware we will take the second shot then compare them to show what are the files or registries were modified, added or deleted after running the malware.

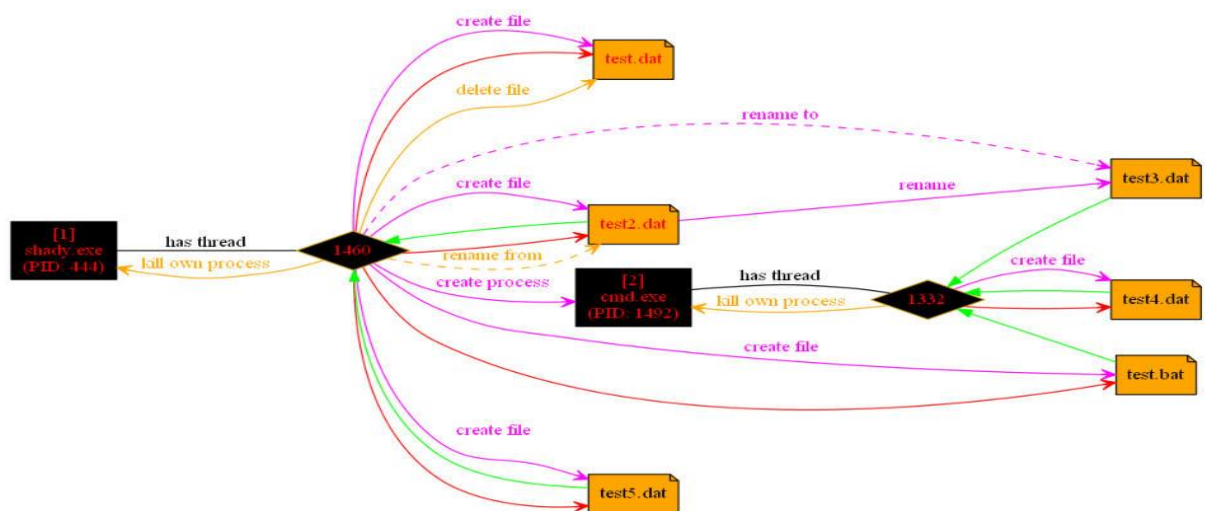


- 3- **ProcMon:** also known as process monitor tool which monitors the process behavior like registry edit, create a child process, file creation or deletion, etc...., also ProcMon has a great filter capability.

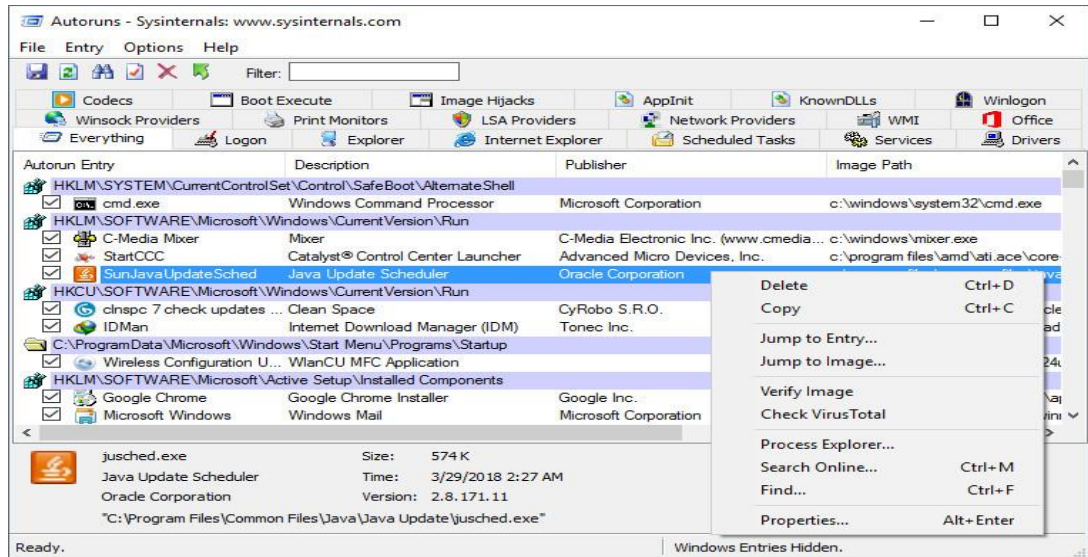
Time o...	Process Name	PID	Operation	Path	Result	Detail
10:01:51...	Isass.exe	832	CreateFile	C:\Windows\System32\Microsoft\Protect...	SUCCESS	Desired Access: G...
10:01:51...	Isass.exe	832	CloseFile	C:\Windows\System32\Microsoft\Protect...	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegQueryKey	HKLM	SUCCESS	Query: Handle Tag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_DWO...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ, Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ, Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ, Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ, Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ, Le...
10:01:51...	sw2_service.exe	3732	RegQueryKey	HKLM	SUCCESS	Query: Handle Tag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\Software\Microsoft\Cryptograp...	SUCCESS	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	KeySetInformation...
10:01:51...	sw2_service.exe	3732	RegSetInfoValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ, Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ, Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ, Le...
10:01:51...	sw2_service.exe	3732	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegQueryKey	HKLM	SUCCESS	Query: Handle Tag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\Software\Microsoft\Cryptograp...	NAME NOT FOUND	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegQueryKey	HKLM	SUCCESS	Query: Handle Tag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\Software\Microsoft\Cryptograp...	NAME NOT FOUND	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegCloseKey	HKLM\SOFTWARE\SecureW2\License	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Serv...	REPARSE	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\System\CurrentControlSet\Servic...	NAME NOT FOUND	Length: 144
10:01:51...	sw2_service.exe	3732	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	

Showing 460,776 of 956,665 events (48%) Backed by virtual memory

- 4- **ProcDot:** we will use this tool to Visualize the ProcMon Data in smart charts which give more visibility on the process behavior and activity



- 5- **Autoruns:** the tool that Knows every auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login and check the Application signed certificates then alerts you for any suspicious or unverified certificates.



Demo Lab:

WARNING: you will run a real malware so please be careful with the previous Guide instructions to avoid getting infected.

We will analyze a malware called Kenora.exe

File Identification phase (YARA)

Run the YARA using the CMD command line which located at (D:\YARA\yara64.exe) using the pre-created YARA rules repo those we are previously downloaded which located at (d:\YARA\rules-YARA) against the suspected file "Kenora.exe" which located at (d:\Malware\Kenora.exe).

The Final Command is: d:\YARA\yara64.exe -w d:\YARA\rules-YARA\index.yar d:\Malware\Kenora.exe

By executing the above command line we will have the below result:

```
C:\Users\Securemisr>d:\YARA\yara64.exe -w d:\YARA\rules-YARA\index.yar d:\Malware\Kenora.exe
DebuggerCheck_QueryInfo d:\Malware\Kenora.exe
DebuggerCheck_RemoteAPI d:\Malware\Kenora.exe
anti_dbg d:\Malware\Kenora.exe
Inject_thread d:\Malware\Kenora.exe
network_udp_sock d:\Malware\Kenora.exe
network_tcp_listen d:\Malware\Kenora.exe
network_dyn dns d:\Malware\Kenora.exe
network_smtp_raw d:\Malware\Kenora.exe
network_tcp_socket d:\Malware\Kenora.exe
network_dns d:\Malware\Kenora.exe
network_ssl d:\Malware\Kenora.exe
escalate_priv d:\Malware\Kenora.exe
screenshot d:\Malware\Kenora.exe
keylogger d:\Malware\Kenora.exe
spreading_file d:\Malware\Kenora.exe
win_mutex d:\Malware\Kenora.exe
win_registry d:\Malware\Kenora.exe
win_token d:\Malware\Kenora.exe
win_private_profile d:\Malware\Kenora.exe
win_files_operation d:\Malware\Kenora.exe
Str_Win32_Winsock2_Library d:\Malware\Kenora.exe
Str_Win32_Wininet_Library d:\Malware\Kenora.exe
Str_Win32_Internet_ApE d:\Malware\Kenora.exe
Big_Numbers1 d:\Malware\Kenora.exe
Big_Numbers3 d:\Malware\Kenora.exe
CRC32_poly_Constant d:\Malware\Kenora.exe
BASE64_table d:\Malware\Kenora.exe
Delphi_Random d:\Malware\Kenora.exe
Delphi_FormShow d:\Malware\Kenora.exe
Delphi_Comparecall d:\Malware\Kenora.exe
Delphi_Copy d:\Malware\Kenora.exe
Delphi_StrToInt d:\Malware\Kenora.exe
Delphi_DecodeDate d:\Malware\Kenora.exe
CookieTools d:\Malware\Kenora.exe
Borland d:\Malware\Kenora.exe
BobSoftMiniDelphiBobBobSoft d:\Malware\Kenora.exe
DISIGv11betaD1N d:\Malware\Kenora.exe
ISPE32 d:\Malware\Kenora.exe
ISWindowsGUI d:\Malware\Kenora.exe
ISPacked d:\Malware\Kenora.exe
borland_delphi d:\Malware\Kenora.exe
borland_delphi_dll d:\Malware\Kenora.exe
borland_delphi_40_additional d:\Malware\Kenora.exe
Microsoft_Visual_Cpp_v50v60_MFC d:\Malware\Kenora.exe
Borland_Delphi_30_additional d:\Malware\Kenora.exe
Borland_Delphi_30_ d:\Malware\Kenora.exe
Borland_Delphi_Setup_Module d:\Malware\Kenora.exe
Borland_Delphi_40 d:\Malware\Kenora.exe
Borland_Delphi_v40_v50 d:\Malware\Kenora.exe
BobSoft_Min_Delphi_Bob_BobSoft_additional d:\Malware\Kenora.exe
Borland_Delphi_v60_v70 d:\Malware\Kenora.exe
Borland_Delphi_v50 d:\Malware\Kenora.exe
Borland_Delphi_DLL d:\Malware\Kenora.exe
```

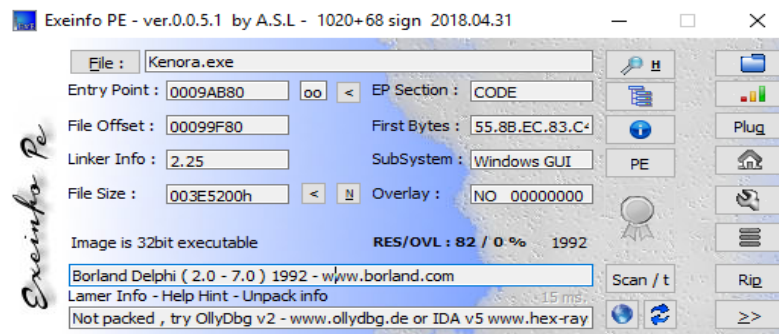
After reviewing the result, on the left, you will find the matched signature name and on the right is the file name, now you have known the malware type and the matched strings.

The malware is a keylogger and the malware was packed by using Delphi packer and more other..., also you must notice many matched strings, for example, the malware will use a Dynamic DNS Domain, anti-Debug and more others...Now you may have expected the results that you will get during the static and dynamic malware analysis.

Static analysis Phase:

- **EXEinfo PE:**

Drag and Drop the malicious file to know if you are dealing with Packed file or not, and if so, what is the packer type and how to unpack it.



The Result is the file is packed and the packer's name is Borland Delphi.

Libraries tab:

library (12)	blacklist (3)	type (1)	imports (161)	description
kernel32.dll	-	implicit	48	Windows NT BASE API Client DLL
user32.dll	-	implicit	4	Multi-User Windows USER API Client DLL
advapi32.dll	-	implicit	3	Advanced Windows 32 Base API
oleaut32.dll	-	implicit	3	OLEAUT32.DLL
version.dll	-	implicit	3	Version Checking and File Installation Libraries
gdi32.dll	-	implicit	64	GDI Client DLL
ole32.dll	-	implicit	1	Microsoft OLE for Windows
comctl32.dll	-	implicit	22	Common Controls Library
shell32.dll	-	implicit	2	Windows Shell Common Dll
wininet.dll	x	implicit	5	Internet Extensions for Win32
wsock32.dll	x	implicit	5	Windows Socket 32-Bit DLL
netapi32.dll	x	implicit	1	Net Win32 API DLL

The malware calls twelve windows libraries, but the interesting is calling three blacklisted Libraries which usually is used to communicate through the Internet.

Imports tab:

name (161)	group (12)	mitre-technique (7)	mitre-tactic (5)	type (1)	anonymous (0)	blacklist (22)	anti-debug (0)	undocumented (0)	deprecated (8)	library (12)
GetFileVersionInfoSizeW	system-information	-	-	implicit	-	x	-	-	-	version.dll
GetFileVersionInfoExW	system-information	-	-	implicit	-	x	-	-	-	version.dll
GetCurrentDirectoryW	storage	-	-	implicit	-	x	-	-	-	kernel32.dll
InternetGetConnectedState	network	-	-	implicit	-	x	-	-	-	wininet.dll
InternetGetFileUrl	network	-	-	implicit	-	x	-	-	-	wininet.dll
InternetOpenUrlA	network	-	-	implicit	-	x	-	-	-	wininet.dll
InternetOpenA	network	-	-	implicit	-	x	-	-	-	wininet.dll
InternetCloseHandle	network	-	-	implicit	-	x	-	-	-	wininet.dll
WSACleanup	network	-	-	implicit	-	x	-	-	-	wsock32.dll
WSAStartup	network	-	-	implicit	-	x	-	-	-	wsock32.dll
gethostbyname	network	-	-	implicit	-	x	-	-	-	wsock32.dll
gethostbynameA	network	-	-	implicit	-	x	-	-	x	wsock32.dll
inet_ntoa	network	-	-	implicit	-	x	-	-	-	netapi32.dll
Netbios	network	-	-	implicit	-	x	-	-	x	netapi32.dll
GetKeyboardType	keyboard-and-mouse	-	-	implicit	-	x	-	-	-	user32.dll
FindFirstFile	file	-	-	implicit	-	x	-	-	-	kernel32.dll
FindClose	file	-	-	implicit	-	x	-	-	-	kernel32.dll
GetCurrentThreadId	execution	-	-	implicit	-	x	-	-	-	kernel32.dll
ShellExecuteEx	execution	Execution through API	Execution	implicit	-	x	-	-	-	shell32.dll
ParseException	exception-handling	-	-	implicit	-	x	-	-	-	kernel32.dll
GetModuleFileNameA	dynamic-library	-	-	implicit	-	x	-	-	-	kernel32.dll
GetThreadLocale	-	-	-	implicit	-	x	-	-	-	kernel32.dll
GetTickCount	system-information	System Time Discov.	Discovery	implicit	-	-	-	-	-	kernel32.dll
QueryPerformanceCounter	system-information	-	-	implicit	-	-	-	-	-	kernel32.dll
GetCurrentProcess	system-information	-	-	implicit	-	-	-	-	-	kernel32.dll
DeleteCriticalSection	synchronization	-	-	implicit	-	-	-	-	-	kernel32.dll

The malware calls many Blacklisted Functions like gethostname, gethostbyname to get info about the victim machine. As an example.

For details about function usage, google is your friend.

Dynamic Analysis Phase:

firstly, run as an administrator all of the Dynamic Analysis tools as arranged below.

- 1- Run FakeNet as an administrator.
- 2- Run RegShot as an administrator and take the first shot.
- 3- Run procMon as an administrator.
- 4- Execute the malware as an administrator.
- 5- After 5 minutes, Take the second shot by using RegShot.

Analysis steps:

- 1- The FakeNet will view on the black screen all malware network activities like C&C Communication, DNS queries, Data Exfiltration. Also, will create a log file and PCAP file that you can analyze by using the Wireshark. When analyzing the PCAP file, you will be able to collect a lot of malware Network IOCs as shown in the below screenshots.

DNS Queries to malicious hostname.

```
> Frame 95: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0
Raw packet data
> Internet Protocol Version 4, Src: 192.168.68.129, Dst: 192.168.68.129
> User Datagram Protocol, Src Port: 55843, Dst Port: 53
v Domain Name System (query)
  Transaction ID: 0xdda7
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  v Queries
    v xred.mooc.com: type A, class IN
      Name: xred.mooc.com
      [Name Length: 13]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 96]
```

Discover and exfiltrate the System info.

```
> Frame 102: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0
Raw packet data
> Internet Protocol Version 4, Src: 192.168.68.129, Dst: 192.0.2.123
> Transmission Control Protocol, Src Port: 49676, Dst Port: 1199, Seq: 1, Ack: 1, Len: 67
v Data (67 bytes)
  Data: 5365637572656d6973727c4445534b544f502d4753564452...
  [Length: 67]

0000  45 00 00 6b 31 c6 40 00 80 0c 01 22 c0 a8 44 81  E: k1 @ . . . . D
0010  c0 00 02 7b c2 0c 04 af 52 b5 b5 d5 a5 45 47 c0  . . . . X . . . .
0020  58 38 01 08 8a 4a 00 00 53 55 53 75 77 45 01 00  P: . . . . S . . . .
0030  73 72 7c 44 45 53 4b 54 4f 50 2d 47 53 56 44 52  r[ DESKT OP-GSVDR
0040  88 33 76 33 39 32 2e 31 36 39 28 36 38 26 31 32  l[192.3.0.0.0.10
0050  39 7c 38 7c 41 30 36 7c 30 30 2d 30 43 2d 32 30  9[8196] 00-0c-20
0060  2d 42 33 2d 4c 37 2d 45 36 3d 0a
```