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

by\ Mostafa Yahia

Table of Contents

Introduction: 3

Sandbox Definition: 3

Installation Requirements: 4

Hardware Requirements: 4

Software Requirements: 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.

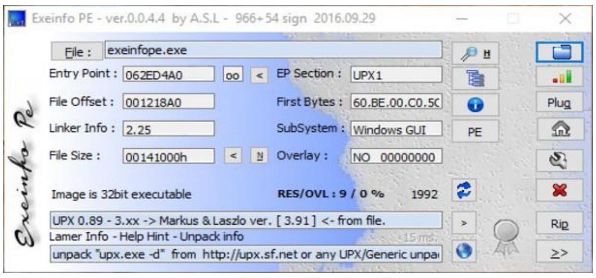
Static analysis phase:

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_FILETARGET_FILE], to understand YARA command line syntax follow the below URL. (https://yara.readthedocs.io/en/stable/commandline.html)

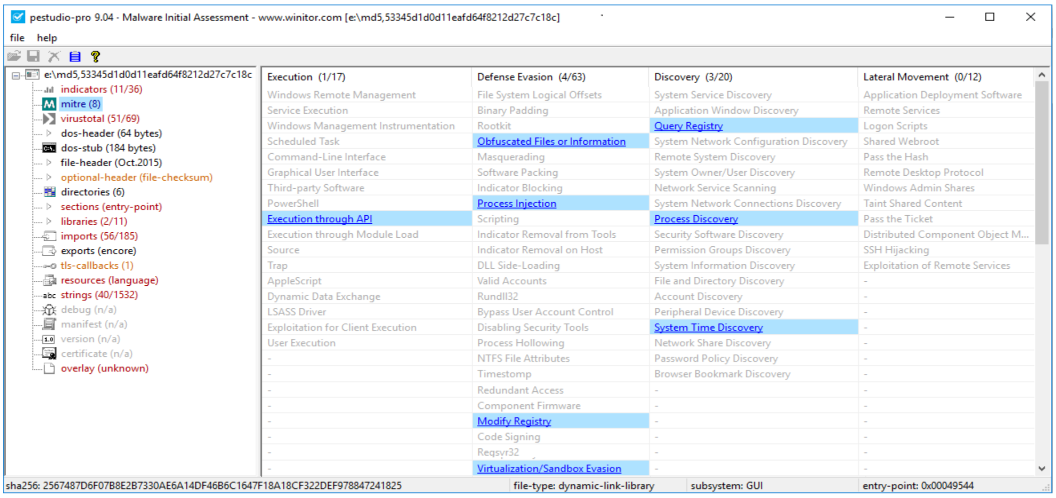
3- **EXEinfo PE:** we will use this tool to tell us if we are dealing with packed file or not, if so the last two labels include all the info that needed like what is the packer that Attacker has used and how to unpack it.



Exeinfo PE - ver.0.0.4.4 by A.S.L - 966+54 sign 2016.09.29

File : exeinfope.exe
Entry Point : 062ED4A0
EP Section : UPX1
File Offset : 001218A0
First Bytes : 60.BE.00.C0.5C
Linker Info : 2.25
SubSystem : Windows GUI
File Size : 00141000h
Overlay : NO 00000000
Image is 32bit executable
RES/OVL : 9 / 0 % 1992
UPX 0.89 - 3.xx -> Markus & Laszlo ver. [3.91] <- from file.
Lamer Info - Help Hint - Unpack info
15 ms.
unpack "upx.exe -d" from http://upx.sf.net or any UPX/Generic unpa

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.



pestudio-pro 9.04 - Malware Initial Assessment - www.winitor.com [e:\md5,53345d1d0d11eafd64f8212d27c7c18c]

e:\md5,53345d1d0d11eafd64f8212d27c7c18c
- indicators (11/36)
- mitre (8)
- virustotal (51/69)
- dos-header (64 bytes)
- dos-stub (184 bytes)
- file-header (Oct.2015)
- optional-header (file-checksum)
- directories (6)
- sections (entry-point)
- libraries (2/11)
- imports (56/185)
- exports (encore)
- tls-callbacks (1)
- resources (language)
- strings (40/1532)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (unknown)

Execution (1/17)	Defense Evasion (4/63)	Discovery (3/20)	Lateral Movement (0/12)
Windows Remote Management	File System Logical Offsets	System Service Discovery	Application Deployment Software
Service Execution	Binary Padding	Application Window Discovery	Remote Services
Windows Management Instrumentation	Rootkit	Query Registry	Logon Scripts
Scheduled Task	Obfuscated Files or Information	System Network Configuration Discovery	Shared Webroot
Command-Line Interface	Masquerading	Remote System Discovery	Pass the Hash
Graphical User Interface	Software Packing	System Owner/User Discovery	Remote Desktop Protocol
Third-party Software	Indicator Blocking	Network Service Scanning	Windows Admin Shares
PowerShell	Process Injection	System Network Connections Discovery	Taint Shared Content
Execution through API	Scripting	Process Discovery	Pass the Ticket
Execution through Module Load	Indicator Removal from Tools	Security Software Discovery	Distributed Component Object M...
Source	Indicator Removal on Host	Permission Groups Discovery	SSH Hijacking
Trap	DLL Side-Loading	System Information Discovery	Exploitation of Remote Services
AppleScript	Valid Accounts	File and Directory Discovery	-
Dynamic Data Exchange	Rundll32	Account Discovery	-
LSASS Driver	Bypass User Account Control	Peripheral Device Discovery	-
Exploitation for Client Execution	Disabling Security Tools	System Time Discovery	-
User Execution	Process Hollowing	Network Share Discovery	-
-	NTFS File Attributes	Password Policy Discovery	-
-	Timestomp	Browser Bookmark Discovery	-
-	Redundant Access	-	-
-	Component Firmware	-	-
-	Modify Registry	-	-
-	Code Signing	-	-
-	Regsvr32	-	-
-	Virtualization/Sandbox Evasion	-	-

sha256: 2567487D6F07B8E2B7330AE6A14DF46B6C1647F18A18CF322DEF978847241825 file-type: dynamic-link-library subsystem: GUI entry-point: 0x00049544

- **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.

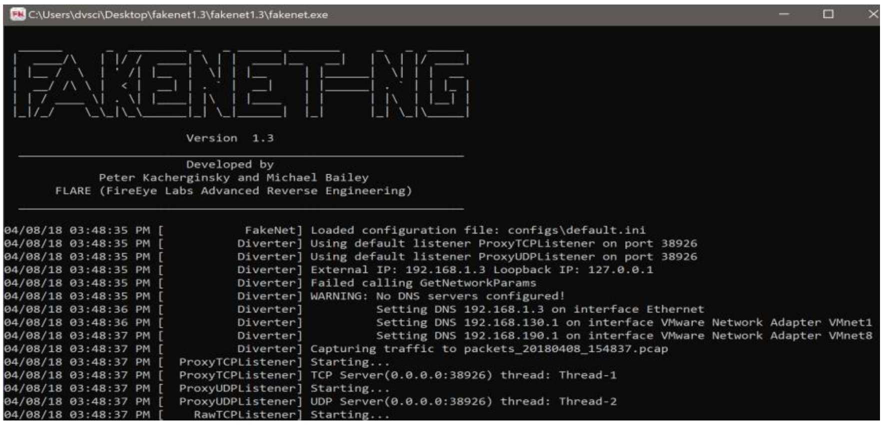
- **Strings:** PEstudio will list all the suspicious strings those found on the analyzed file.

- **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.

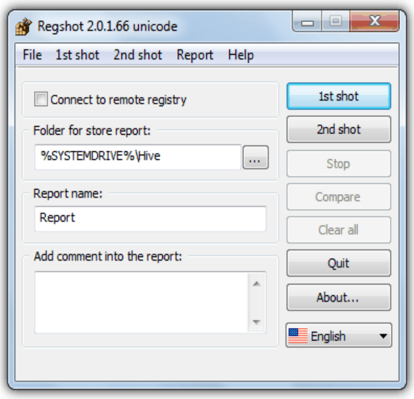
1- **FakeNet:** as you remember we have denied the VM from the network and the internet communications, but as you know the malwares are usually tending to communicate with their C&C server for more payload or for more instructions, so the FakeNet will introduce all of the internet services HTTP, DNS,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



```
                        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.



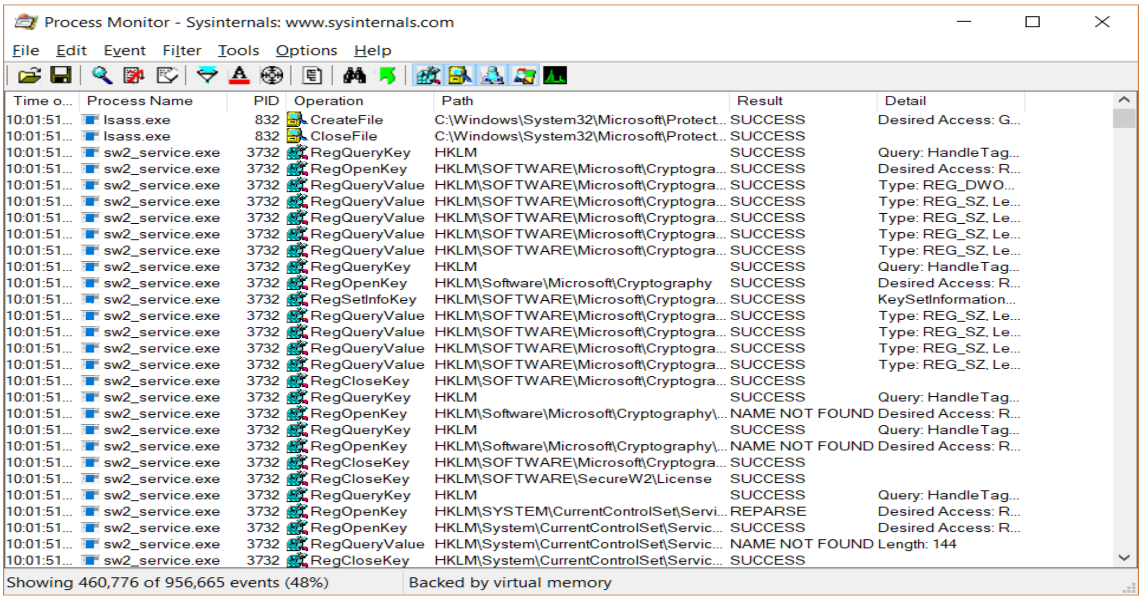
□ Connect to remote registry

Folder for store report: %SYSTEMDRIVE%\Hive

Report name: Report

Add comment into the report:

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.

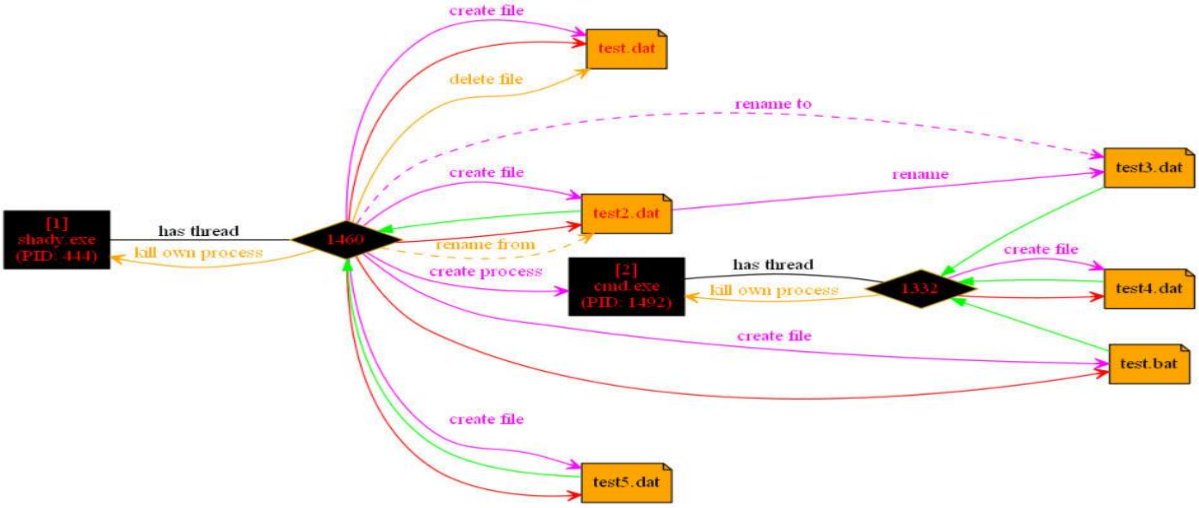


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
10:01:51...	lsass.exe	832	CreateFile	C:\Windows\System32\Microsoft\Protect...	SUCCESS	Desired Access: G...
10:01:51...	lsass.exe	832	CloseFile	C:\Windows\System32\Microsoft\Protect...	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegQueryValue	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	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\Software\Microsoft\Cryptography	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	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	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\Software\Microsoft\Cryptography\...	NAME NOT FOUND	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\Software\Microsoft\Cryptography\...	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\Servi...	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	

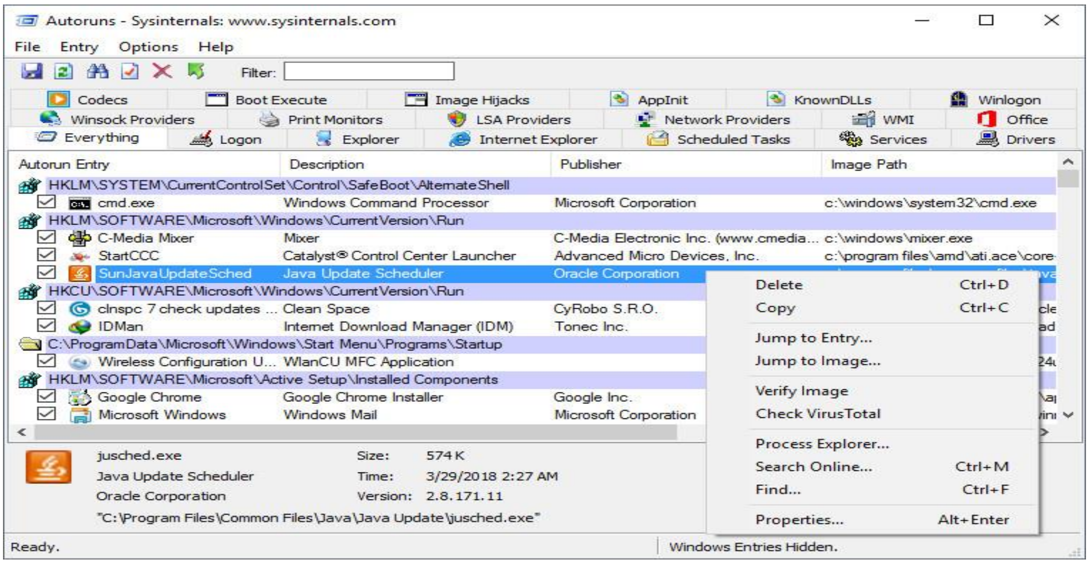
Showing 460,776 of 956,665 events (48%) Backed by virtual memory

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



Mostafa Yahia
E-Mail: Mostafayahia753@gmail.com
LinkedIn: https://www.linkedin.com/in/mostafa-yahia-701b4b15a/

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 singed certificates then alerts you for any suspicious or unverified certificates.



Autorun Entry	Description	Publisher	Image Path
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
☑ cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ C-Media Mixer	Mixer	C-Media Electronic Inc. (www.cmedia...	c:\windows\mixer.exe
☑ StartCCC	Catalyst® Control Center Launcher	Advanced Micro Devices, Inc.	c:\program files\amd\ati.ace\core-
☑ SunJavaUpdateSched	Java Update Scheduler	Oracle Corporation	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ clnspc 7 check updates ...	Clean Space	CyRobo S.R.O.	
☑ IDMan	Internet Download Manager (IDM)	Tonec Inc.	
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup			
☑ Wireless Configuration U...	WlanCU MFC Application		
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
☑ Google Chrome	Google Chrome Installer	Google Inc.	
☑ Microsoft Windows	Windows Mail	Microsoft Corporation	

jusched.exe — Size: 574 K
Java Update Scheduler — Time: 3/29/2018 2:27 AM
Oracle Corporation — Version: 2.8.171.11
"C:\Program Files\Common Files\Java\Java Update\jusched.exe"

Ready. | Windows Entries Hidden.

Mostafa Yahia
E-Mail: Mostafayahia753@gmail.com
LinkedIn: https://www.linkedin.com/in/mostafa-yahia-701b4b15a/

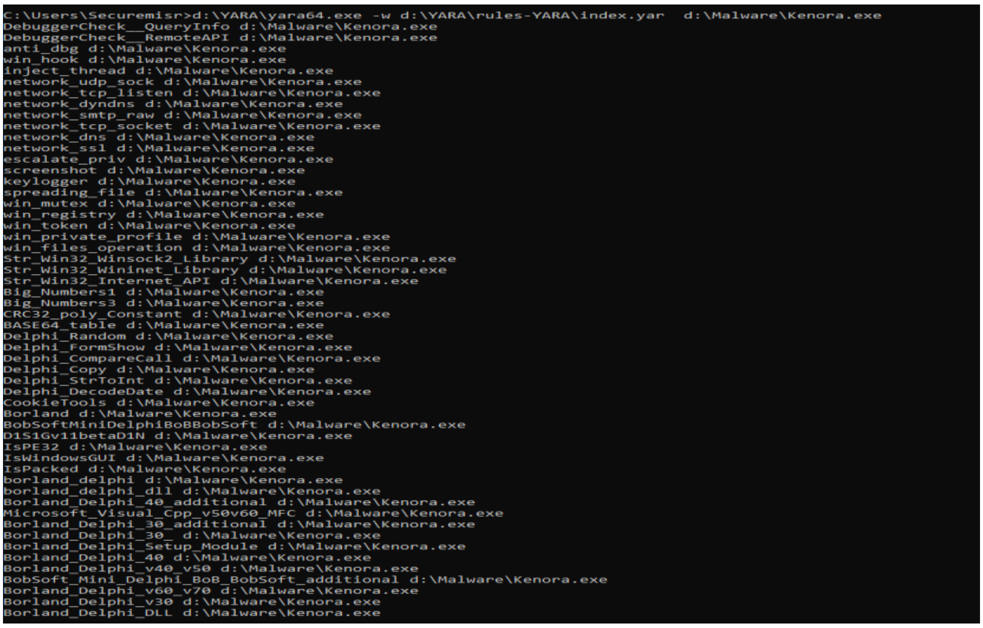
Demo Lab:

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
win_hook 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_dyndns 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_API 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
D1S1Gv11betaD1N 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_Mini_Delphi_BoB_BobSoft_additional d:\Malware\Kenora.exe
Borland_Delphi_v60_v70 d:\Malware\Kenora.exe
Borland_Delphi_v30 d:\Malware\Kenora.exe
Borland_Delphi_DLL d:\Malware\Kenora.exe
```

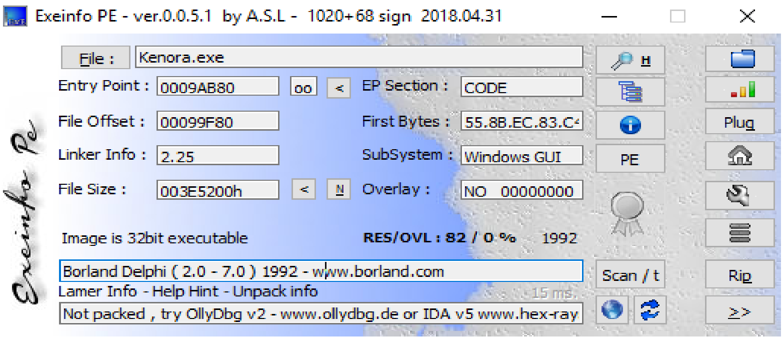
After reviewing the result, on the left, you will find the matched signature name and on the right is the file name, now you have known the malware type and the matched strings.

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.



Exeinfo PE - ver.0.0.5.1 by A.S.L - 1020+68 sign 2018.04.31

File : Kenora.exe

Entry Point : 0009AB80

EP Section : CODE

File Offset : 00099F80

First Bytes : 55.8B.EC.83.C

Linker Info : 2.25

SubSystem : Windows GUI

File Size : 003E5200h

Overlay : NO 00000000

Image is 32bit executable

RES/OVL : 82 / 0 % 1992

Borland Delphi (2.0 - 7.0) 1992 - www.borland.com

Lamer Info - Help Hint - Unpack info

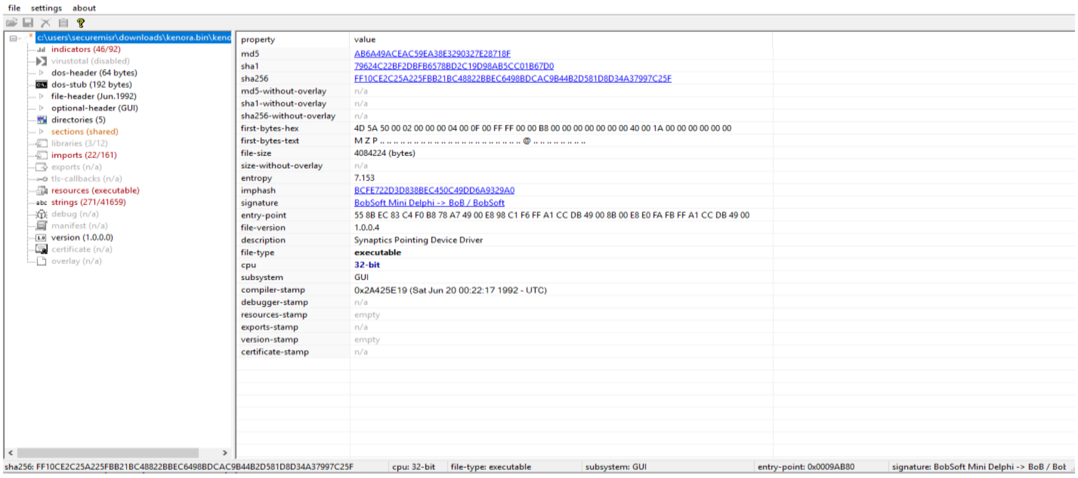
15 ms.

Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-ray

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

- **PE Studio:**

  Open the tool then Drag and Drop the file or (file >> open file).
  Now you observe a quick info about the file like: file hashes, Magic Bytes/Num, file Size, File Type and signature.



c:\users\securemisr\downloads\kenora.bin\keno
indicators (46/92)
virustotal (disabled)
dos-header (64 bytes)
dos-stub (192 bytes)
file-header (Jun.1992)
optional-header (GUI)
directories (5)
sections (shared)
libraries (3/12)
imports (22/161)
exports (n/a)
tls-callbacks (n/a)
resources (executable)
strings (271/41659)
debug (n/a)
manifest (n/a)
version (1.0.0.0)
certificate (n/a)
overlay (n/a)

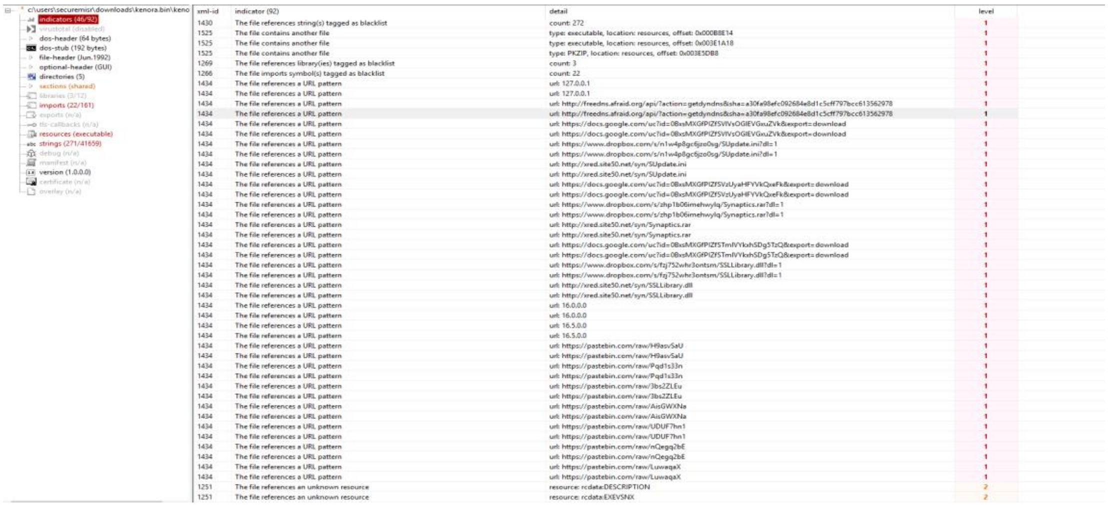
property	value
md5	AB6A49ACEAC59EA38E3290327E28718F
sha1	79624C22BF2DBFB6578BD2C19D98AB5CC01B67D0
sha256	FF10CE2C25A225FBB21BC48822BBEC6498BDCAC9B44B2D581D8D34A37997C25F
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00 00
first-bytes-text	M Z P .. .. @ .. ..
file-size	4084224 (bytes)
size-without-overlay	n/a
entropy	7.153
imphash	BCFE722D3D838BEC450C49DD6A9329A0
signature	BobSoft Mini Delphi -> BoB / BobSoft
entry-point	55 8B EC 83 C4 F0 B8 78 A7 49 00 E8 98 C1 F6 FF A1 CC DB 49 00 8B 00 E8 E0 FA FB FF A1 CC DB 49 00
file-version	1.0.0.4
description	Synaptics Pointing Device Driver
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x2A425E19 (Sat Jun 20 00:22:17 1992 - UTC)
debugger-stamp	n/a
resources-stamp	empty
exports-stamp	n/a
version-stamp	empty
certificate-stamp	n/a

sha256: FF10CE2C25A225FBB21BC48822BBEC6498BDCAC9B44B2D581D8D34A37997C25F cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x0009AB80 signature: BobSoft Mini Delphi -> BoB / Bot

  PE studio has detected a Use of a Delphi Packer as shown on the Signature field (BobSoft Mini Delphi ->BoB / BobSoft).

PEstudio tabs NAVIGATION:

Indicators tab:



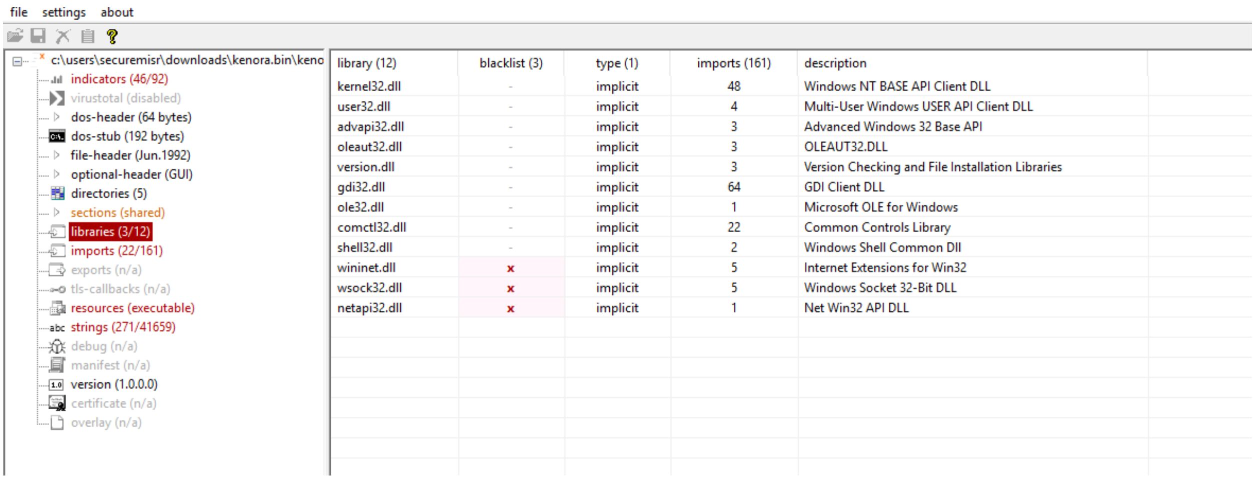
c:\users\securemisr\downloads\kenora.bin\keno
indicators (46/92)
virustotal (disabled)
dos-header (64 bytes)
dos-stub (192 bytes)
file-header (Jun.1992)
optional-header (GUI)
directories (5)
sections (shared)
libraries (3/12)
imports (22/161)
exports (n/a)
tls-callbacks (n/a)
resources (executable)
strings (271/41659)
debug (n/a)
manifest (n/a)
version (1.0.0.0)
certificate (n/a)
overlay (n/a)

xml-id	indicator (92)	detail	level
1430	The file references string(s) tagged as blacklist	count: 272	1
1525	The file contains another file	type: executable, location: resources, offset: 0x000B8E14	1
1525	The file contains another file	type: executable, location: resources, offset: 0x003E1A18	1
1525	The file contains another file	type: PKZIP, location: resources, offset: 0x003E5DB8	1
1269	The file references library(ies) tagged as blacklist	count: 3	1
1266	The file imports symbol(s) tagged as blacklist	count: 22	1
1434	The file references a URL pattern	url: 127.0.0.1	1
1434	The file references a URL pattern	url: 127.0.0.1	1
1434	The file references a URL pattern	url: http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978	1
1434	The file references a URL pattern	url: http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978	1
1434	The file references a URL pattern	url: https://docs.google.com/uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download	1
1434	The file references a URL pattern	url: https://docs.google.com/uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download	1
1434	The file references a URL pattern	url: https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl=1	1
1434	The file references a URL pattern	url: https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl=1	1
1434	The file references a URL pattern	url: http://xred.site50.net/syn/SUpdate.ini	1
1434	The file references a URL pattern	url: http://xred.site50.net/syn/SUpdate.ini	1
1434	The file references a URL pattern	url: https://docs.google.com/uc?id=0BxsMXGfPIZfSVzUyaHFVVkQxeFk&export=download	1
1434	The file references a URL pattern	url: https://docs.google.com/uc?id=0BxsMXGfPIZfSVzUyaHFVVkQxeFk&export=download	1
1434	The file references a URL pattern	url: https://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1	1
1434	The file references a URL pattern	url: https://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1	1
1434	The file references a URL pattern	url: http://xred.site50.net/syn/Synaptics.rar	1
1434	The file references a URL pattern	url: http://xred.site50.net/syn/Synaptics.rar	1
1434	The file references a URL pattern	url: https://docs.google.com/uc?id=0BxsMXGfPIZfSTmlVYkxhSDg5TzQ&export=download	1
1434	The file references a URL pattern	url: https://docs.google.com/uc?id=0BxsMXGfPIZfSTmlVYkxhSDg5TzQ&export=download	1
1434	The file references a URL pattern	url: https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=1	1
1434	The file references a URL pattern	url: https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=1	1
1434	The file references a URL pattern	url: http://xred.site50.net/syn/SSLLibrary.dll	1
1434	The file references a URL pattern	url: http://xred.site50.net/syn/SSLLibrary.dll	1
1434	The file references a URL pattern	url: 16.0.0.0	1
1434	The file references a URL pattern	url: 16.0.0.0	1
1434	The file references a URL pattern	url: 16.5.0.0	1
1434	The file references a URL pattern	url: 16.5.0.0	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/H9asvSaU	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/H9asvSaU	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/Pqd1s33n	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/Pqd1s33n	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/3bs2ZLEu	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/3bs2ZLEu	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/AisGWXNa	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/AisGWXNa	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/UDUF7hn1	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/UDUF7hn1	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/nQegq2bE	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/nQegq2bE	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/LuwaqaX	1
1434	The file references a URL pattern	url: https://pastebin.com/raw/LuwaqaX	1
1251	The file references an unknown resource	resource: rcdata:DESCRIPTION	2
1251	The file references an unknown resource	resource: rcdata:EXEVSNX	2

There are many malicious Communication maybe the malware tries to Download extra payload, Communicate with C&C server or Exfiltrate Data.

Mostafa Yahia
E-Mail: Mostafayahia753@gmail.com
LinkedIn: https://www.linkedin.com/in/mostafa-yahia-701b4b15a/

Libraries tab:

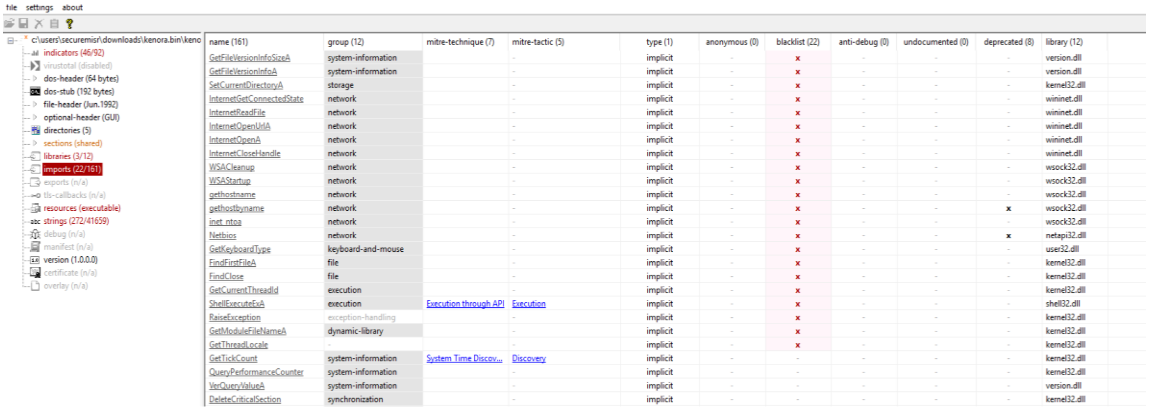


c:\users\securemisr\downloads\kenora.bin\keno
- indicators (46/92)
- virustotal (disabled)
- dos-header (64 bytes)
- dos-stub (192 bytes)
- file-header (Jun.1992)
- optional-header (GUI)
- directories (5)
- sections (shared)
- libraries (3/12)
- imports (22/161)
- exports (n/a)
- tls-callbacks (n/a)
- resources (executable)
- strings (271/41659)
- debug (n/a)
- manifest (n/a)
- version (1.0.0.0)
- certificate (n/a)
- overlay (n/a)

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:



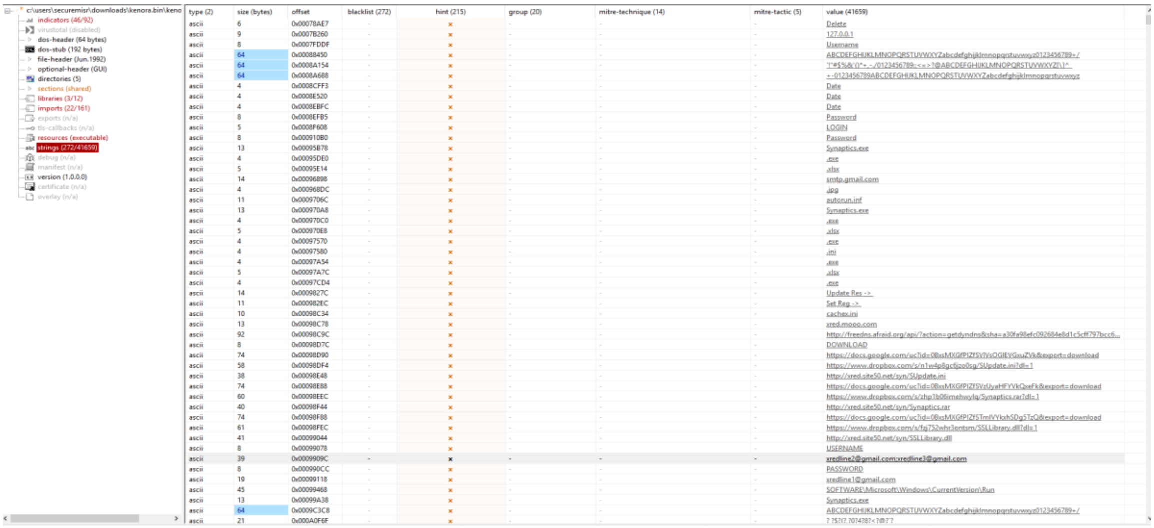
c:\users\securemisr\downloads\kenora.bin\keno
- indicators (46/92)
- virustotal (disabled)
- dos-header (64 bytes)
- dos-stub (192 bytes)
- file-header (Jun.1992)
- optional-header (GUI)
- directories (5)
- sections (shared)
- libraries (3/12)
- imports (22/161)
- exports (n/a)
- tls-callbacks (n/a)
- resources (executable)
- strings (272/41659)
- debug (n/a)
- manifest (n/a)
- version (1.0.0.0)
- certificate (n/a)
- overlay (n/a)

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)
GetFileVersionInfoSizeA	system-information		-	implicit	-	x	-	-	-	version.dll
GetFileVersionInfoA	system-information		-	implicit	-	x	-	-	-	version.dll
SetCurrentDirectoryA	storage		-	implicit	-	x	-	-	-	kernel32.dll
InternetGetConnectedState	network		-	implicit	-	x	-	-	-	wininet.dll
InternetReadFile	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
gethostname	network		-	implicit	-	x	-	-	-	wsock32.dll
gethostbyname	network		-	implicit	-	x	-	-	x	wsock32.dll
inet_ntoa	network		-	implicit	-	x	-	-	-	wsock32.dll
Netbios	network		-	implicit	-	x	-	-	x	netapi32.dll
GetKeyboardType	keyboard-and-mouse		-	implicit	-	x	-	-	-	user32.dll
FindFirstFileA	file		-	implicit	-	x	-	-	-	kernel32.dll
FindClose	file		-	implicit	-	x	-	-	-	kernel32.dll
GetCurrentThreadId	execution		-	implicit	-	x	-	-	-	kernel32.dll
ShellExecuteExA	execution	Execution through API	Execution	implicit	-	x	-	-	-	shell32.dll
RaiseException	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
VerQueryValueA	system-information		-	implicit	-	-	-	-	-	version.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.

Strings tab:



c:\users\securemisr\downloads\kenora.bin\keno

- indicators (46/92)
- virustotal (disabled)
- dos-header (64 bytes)
- dos-stub (192 bytes)
- file-header (Jun.1992)
- optional-header (GUI)
- directories (5)
- sections (shared)
- libraries (3/12)
- imports (22/161)
- exports (n/a)
- tls-callbacks (n/a)
- resources (executable)
- strings (272/41659)
- debug (n/a)
- manifest (n/a)
- version (1.0.0.0)
- certificate (n/a)
- overlay (n/a)

type (2)	size (bytes)	offset	blacklist (272)	hint (215)	group (20)	mitre-technique (14)	mitre-tactic (5)	value (41659)
ascii	6	0x00078AE7	-	x	-	-	-	Delete
ascii	9	0x0007B260	-	x	-	-	-	127.0.0.1
ascii	8	0x0007FDDF	-	x	-	-	-	Username
ascii	64	0x00088450	-	x	-	-	-	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
ascii	64	0x0008A154	-	x	-	-	-	!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_
ascii	64	0x0008A688	-	x	-	-	-	+-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
ascii	4	0x0008CFF3	-	x	-	-	-	Date
ascii	4	0x0008E520	-	x	-	-	-	Date
ascii	4	0x0008EBFC	-	x	-	-	-	Date
ascii	8	0x0008EFB5	-	x	-	-	-	Password
ascii	5	0x0008F608	-	x	-	-	-	LOGIN
ascii	8	0x000910B0	-	x	-	-	-	Password
ascii	13	0x00095B78	-	x	-	-	-	Synaptics.exe
ascii	4	0x00095DE0	-	x	-	-	-	.exe
ascii	5	0x00095E14	-	x	-	-	-	.xlsx
ascii	14	0x00096898	-	x	-	-	-	smtp.gmail.com
ascii	4	0x000968DC	-	x	-	-	-	.jpg
ascii	11	0x0009706C	-	x	-	-	-	autorun.inf
ascii	13	0x000970A8	-	x	-	-	-	Synaptics.exe
ascii	4	0x000970C0	-	x	-	-	-	.exe
ascii	5	0x000970E8	-	x	-	-	-	.xlsx
ascii	4	0x00097570	-	x	-	-	-	.exe
ascii	4	0x00097580	-	x	-	-	-	.ini
ascii	4	0x00097A54	-	x	-	-	-	.exe
ascii	5	0x00097A7C	-	x	-	-	-	.xlsx
ascii	4	0x00097CD4	-	x	-	-	-	.exe
ascii	14	0x0009827C	-	x	-	-	-	Update Res ->
ascii	11	0x000982EC	-	x	-	-	-	Set Reg ->
ascii	10	0x00098C34	-	x	-	-	-	cachex.ini
ascii	13	0x00098C78	-	x	-	-	-	xred.mooo.com
ascii	92	0x00098C9C	-	x	-	-	-	http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc6...
ascii	8	0x00098D7C	-	x	-	-	-	DOWNLOAD
ascii	74	0x00098D90	-	x	-	-	-	https://docs.google.com/uc?id=0BxsMXGfPIZfSVlVsOGIEVGxuZVk&export=download
ascii	58	0x00098DF4	-	x	-	-	-	https://www.dropbox.com/s/n1w4p8gcfjzo0sg/SUpdate.ini?dl=1
ascii	38	0x00098E48	-	x	-	-	-	http://xred.site50.net/syn/SUpdate.ini
ascii	74	0x00098E88	-	x	-	-	-	https://docs.google.com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=download
ascii	60	0x00098EEC	-	x	-	-	-	https://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1
ascii	40	0x00098F44	-	x	-	-	-	http://xred.site50.net/syn/Synaptics.rar
ascii	74	0x00098F88	-	x	-	-	-	https://docs.google.com/uc?id=0BxsMXGfPIZfSTmlVYkxhSDg5TzQ&export=download
ascii	61	0x00098FEC	-	x	-	-	-	https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=1
ascii	41	0x00099044	-	x	-	-	-	http://xred.site50.net/syn/SSLLibrary.dll
ascii	8	0x00099078	-	x	-	-	-	USERNAME
ascii	39	0x0009909C	-	x	-	-	-	xredline2@gmail.com:xredline3@gmail.com
ascii	8	0x000990CC	-	x	-	-	-	PASSWORD
ascii	19	0x00099118	-	x	-	-	-	xredline1@gmail.com
ascii	45	0x00099468	-	x	-	-	-	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
ascii	13	0x00099A38	-	x	-	-	-	Synaptics.exe
ascii	64	0x0009C3C8	-	x	-	-	-	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
ascii	21	0x000A0F6F	-	x	-	-	-	? ?$?(?.?0?4?8?<?@?"?

The Most interesting Tab, strings tell you about every malicious and suspicious strings found on the malware, As you can see on the above screenshot, it seems that malware intends to use the Gmail SMTP Server to exfiltrate the Data and the Attacker mails are : xredline*@gmail.com , Also you could notice that the attacker intends to use the RUN registry key (**SOFTWARE\Microsoft\Windows\CurrentVersion\Run**) for persistence, and many others you will find on this wonderful tap.

Dynamic Analysis Phase:

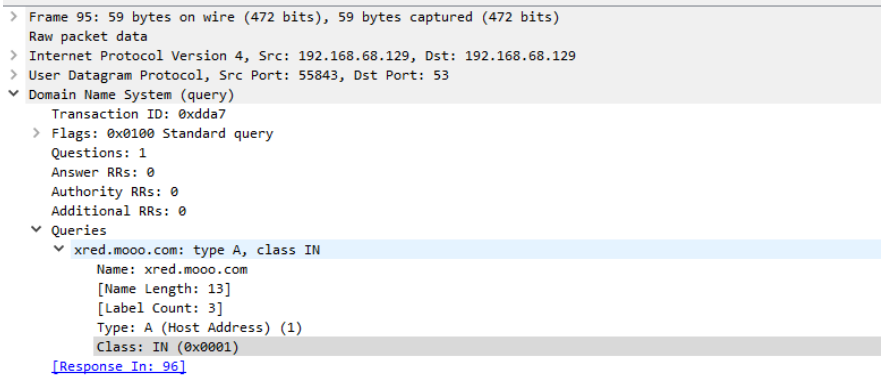
firstly, run as an administrator all of the Dynamic Analysis tools as arranged below.

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:

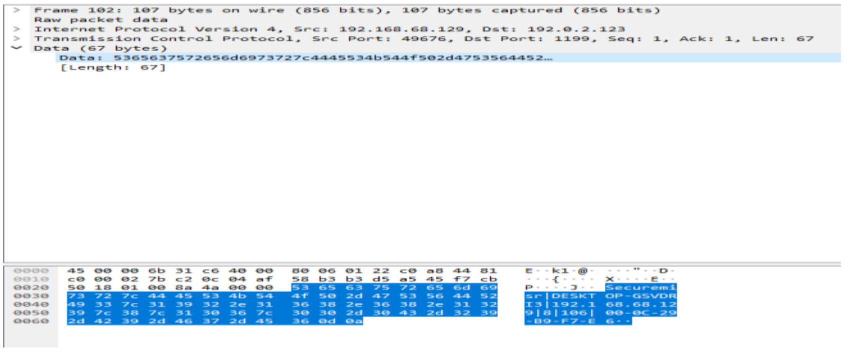
1- The FakeNet will view on the black screen all malware network activities like C&C Communication, DNS queries, Data Exfiltration. Also, will create a log file and PCAP file that you can analyze by using the Wireshark. When analyzing the PCAP file, you will be able to collect a lot of malware Network 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)
  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.mooo.com: type A, class IN
        Name: xred.mooo.com
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 96]
```

- Discover and exfiltrate the System info.

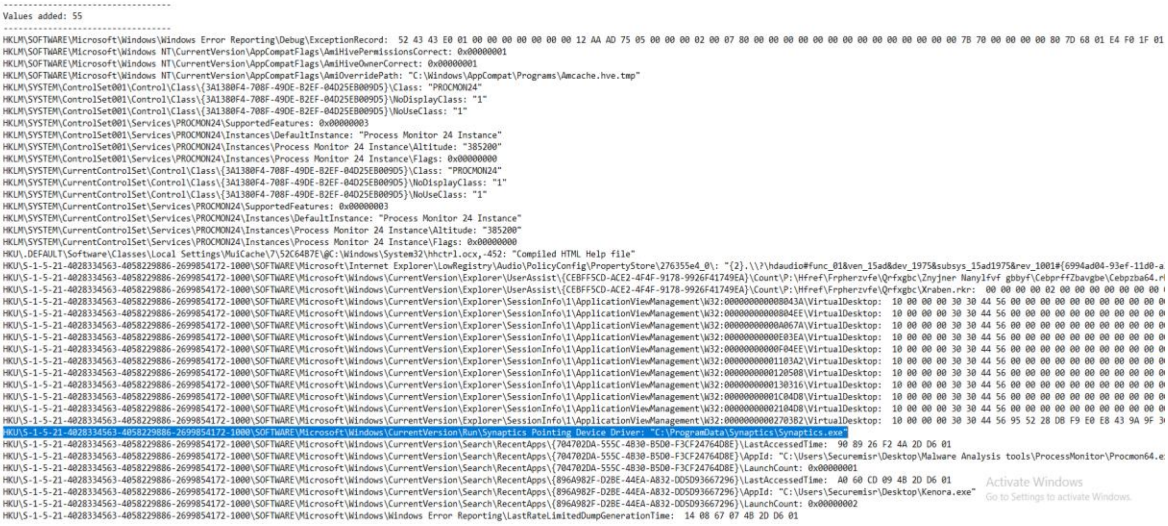


```
> Frame 102: 107 bytes on wire (856 bits), 107 bytes captured (856 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 192.168.68.129, Dst: 192.0.2.123
> Transmission Control Protocol, Src Port: 49676, Dst Port: 1199, Seq: 1, Ack: 1, Len: 67
v Data (67 bytes)
    Data: 5365637572656d6973727c4445534b544f502d4753564452…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

0000  45 00 00 6b 31 c6 40 00  80 06 01 22 c0 a8 44 81   E··k1·@· ···"··D·
0010  c0 00 02 7b c2 0c 04 af  58 b3 b3 d5 a5 45 f7 cb   ···{···· X····E··
0020  50 18 01 00 8a 4a 00 00  53 65 63 75 72 65 6d 69   P····J·· Securemi
0030  73 72 7c 44 45 53 4b 54  4f 50 2d 47 53 56 44 52   sr|DESKT OP-GSVDR
0040  49 33 7c 31 39 32 2e 31  36 38 2e 36 38 2e 31 32   I3|192.1 68.68.12
0050  39 7c 38 7c 31 30 36 7c  30 30 2d 30 43 2d 32 39   9|8|106| 00-0C-29
0060  2d 42 39 2d 46 37 2d 45  36 0d 0a                  -B9-F7-E 6··
```

Note: the above Screenshots is just a sample, you could go more to find more

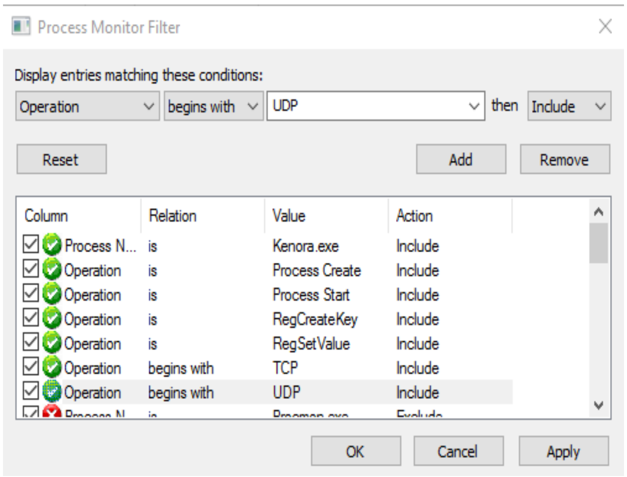
2- On the **RegShot** click compare, after showing the comparing file you will find a lot of deleted, added, modified values and keys. We are mainly interested in the added keys and Values.



```
----------------------------------
Values added: 55
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug\ExceptionRecord:  52 43 43 E0 01 00 00 00 00 00 00 00 12 AA AD 75 05 00 00 00 02 00 07 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7B 70 00 00 00 00 80 7D 68 01 E4 F0 1F 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\AmiHivePermissionsCorrect: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\AmiHiveOwnerCorrect: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\AmiOverridePath: "C:\Windows\AppCompat\Programs\Amcache.hve.tmp"
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}\Class: "PROCMON24"
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}\NoDisplayClass: "1"
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}\NoUseClass: "1"
HKLM\SYSTEM\ControlSet001\Services\PROCMON24\SupportedFeatures: 0x00000003
HKLM\SYSTEM\ControlSet001\Services\PROCMON24\Instances\DefaultInstance: "Process Monitor 24 Instance"
HKLM\SYSTEM\ControlSet001\Services\PROCMON24\Instances\Process Monitor 24 Instance\Altitude: "385200"
HKLM\SYSTEM\ControlSet001\Services\PROCMON24\Instances\Process Monitor 24 Instance\Flags: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}\Class: "PROCMON24"
HKLM\SYSTEM\CurrentControlSet\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}\NoDisplayClass: "1"
HKLM\SYSTEM\CurrentControlSet\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}\NoUseClass: "1"
HKLM\SYSTEM\CurrentControlSet\Services\PROCMON24\SupportedFeatures: 0x00000003
HKLM\SYSTEM\CurrentControlSet\Services\PROCMON24\Instances\DefaultInstance: "Process Monitor 24 Instance"
HKLM\SYSTEM\CurrentControlSet\Services\PROCMON24\Instances\Process Monitor 24 Instance\Altitude: "385200"
HKLM\SYSTEM\CurrentControlSet\Services\PROCMON24\Instances\Process Monitor 24 Instance\Flags: 0x00000000
HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\7\52C64B7E\@C:\Windows\System32\hhctrl.ocx,-452: "Compiled HTML Help file"
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Internet Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\276355e4_0\: "{2}.\\?\hdaudio#func_01&ven_15ad&dev_1975&subsys_15ad1975&rev_1001#{6994ad04-93ef-11d0-a
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Frpherzvfe\Qrfxgbc\Znyjner Nanylfvf gbbyf\CebprffZbavgbe\Cebpzba64.r
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Frpherzvfe\Qrfxgbc\Xraben.rkr:  00 00 00 00 02 00 00 00 00 00 00 00
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000008043A\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000804EE\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000A067A\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000E03EA\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000F04EE\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001103A2\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000120508\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000130316\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001C04D8\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000002104D8\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000002703B2\VirtualDesktop:  10 00 00 00 30 30 44 56 95 52 28 DB F9 E0 E8 43 9A 9F 3
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Synaptics Pointing Device Driver: "C:\ProgramData\Synaptics\Synaptics.exe"
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{704702DA-555C-4B30-B5D0-F3CF24764D8E}\LastAccessedTime:  90 89 26 F2 4A 2D D6 01
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{704702DA-555C-4B30-B5D0-F3CF24764D8E}\AppId: "C:\Users\Securemisr\Desktop\Malware Analysis tools\ProcessMonitor\Procmon64.e
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{704702DA-555C-4B30-B5D0-F3CF24764D8E}\LaunchCount: 0x00000001
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{896A982F-D2BE-44EA-A832-DD5D93667296}\LastAccessedTime:  A0 60 CD 09 4B 2D D6 01
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{896A982F-D2BE-44EA-A832-DD5D93667296}\AppId: "C:\Users\Securemisr\Desktop\Kenora.exe"
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{896A982F-D2BE-44EA-A832-DD5D93667296}\LaunchCount: 0x00000002
HKU\S-1-5-21-4028334563-4058229886-2699854172-1000\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LastRateLimitedDumpGenerationTime:  14 08 67 07 4B 2D D6 01
```

After checking the Values added you can see that the malware has created on the RUN key, and the file name is Synaptics.exe which located in c:\ProgramData\Synaptics\Synaptics.exe

3- Now deploy filters on the ProcMon tool to obtain an effective result, click on this button ⛛ then filter for the malware process name "Kenora.exe", then choose the suspicious operations like process created, RegcreateKey, RegSetValue, etc…



Process Monitor Filter

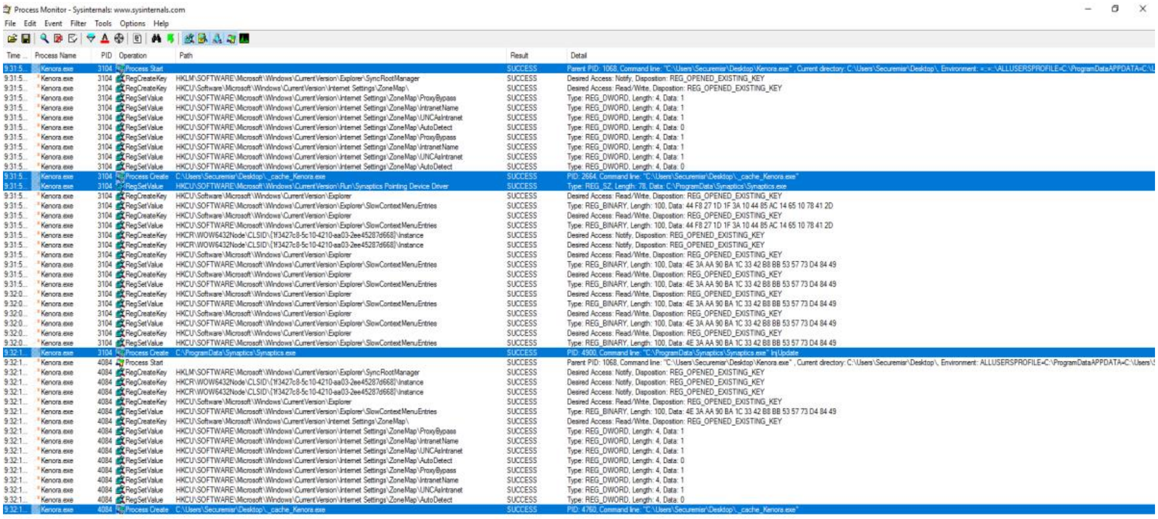
Display entries matching these conditions:

Operation | begins with | UDP | then | Include

Column	Relation	Value	Action
☑ Process N...	is	Kenora.exe	Include
☑ Operation	is	Process Create	Include
☑ Operation	is	Process Start	Include
☑ Operation	is	RegCreateKey	Include
☑ Operation	is	RegSetValue	Include
☑ Operation	begins with	TCP	Include
☑ Operation	begins with	UDP	Include
☑ Process N...	is	Procmon.exe	Exclude

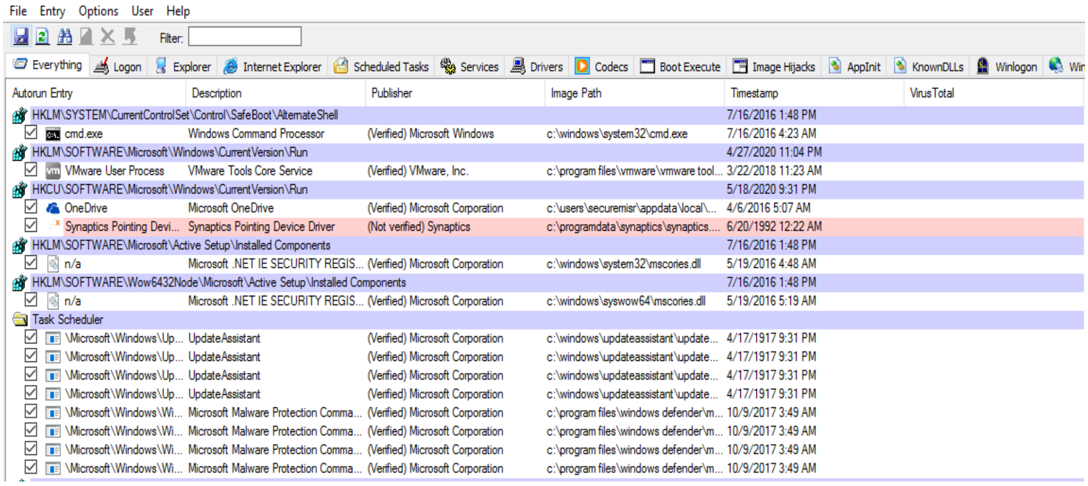
Mostafa Yahia
E-Mail: Mostafayahia753@gmail.com
LinkedIn: https://www.linkedin.com/in/mostafa-yahia-701b4b15a/

Based on the above filter we have observed the below malicious Activities like Discover the system by using the command line, create new process, etc…
Apply more filters, get more results.



Time ...	Process Name	PID	Operation	Path	Result	Detail
9:31:5...	Kenora.exe	3104	Process Start		SUCCESS	Parent PID: 1068, Command line: "C:\Users\Securemisr\Desktop\Kenora.exe" , Current directory: C:\Users\Securemisr\Desktop\, Environment: =::=::\ALLUSERSPROFILE=C:\ProgramDataAPPDATA=C:\U
9:31:5...	Kenora.exe	3104	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SyncRootManager	SUCCESS	Desired Access: Notify, Disposition: REG_OPENED_EXISTING_KEY
9:31:5...	Kenora.exe	3104	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	SUCCESS	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
9:31:5...	Kenora.exe	3104	Process Create	C:\Users\Securemisr\Desktop_cache_Kenora.exe	SUCCESS	PID: 2664, Command line: "C:\Users\Securemisr\Desktop_cache_Kenora.exe"
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Synaptics Pointing Device Driver	SUCCESS	Type: REG_SZ, Length: 78, Data: C:\ProgramData\Synaptics\Synaptics.exe
9:31:5...	Kenora.exe	3104	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	Type: REG_BINARY, Length: 100, Data: 44 F8 27 1D 1F 3A 10 44 85 AC 14 65 10 78 41 2D
9:31:5...	Kenora.exe	3104	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	Type: REG_BINARY, Length: 100, Data: 44 F8 27 1D 1F 3A 10 44 85 AC 14 65 10 78 41 2D
9:31:5...	Kenora.exe	3104	RegCreateKey	HKCR\WOW6432Node\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance	SUCCESS	Desired Access: Notify, Disposition: REG_OPENED_EXISTING_KEY
9:31:5...	Kenora.exe	3104	RegCreateKey	HKCR\WOW6432Node\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance	SUCCESS	Desired Access: Notify, Disposition: REG_OPENED_EXISTING_KEY
9:31:5...	Kenora.exe	3104	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	Type: REG_BINARY, Length: 100, Data: 4E 3A AA 90 BA 1C 33 42 B8 BB 53 57 73 D4 84 49
9:31:5...	Kenora.exe	3104	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
9:31:5...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	Type: REG_BINARY, Length: 100, Data: 4E 3A AA 90 BA 1C 33 42 B8 BB 53 57 73 D4 84 49
9:32:0...	Kenora.exe	3104	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
9:32:0...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	Type: REG_BINARY, Length: 100, Data: 4E 3A AA 90 BA 1C 33 42 B8 BB 53 57 73 D4 84 49
9:32:0...	Kenora.exe	3104	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
9:32:0...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	Type: REG_BINARY, Length: 100, Data: 4E 3A AA 90 BA 1C 33 42 B8 BB 53 57 73 D4 84 49
9:32:0...	Kenora.exe	3104	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
9:32:0...	Kenora.exe	3104	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	Type: REG_BINARY, Length: 100, Data: 4E 3A AA 90 BA 1C 33 42 B8 BB 53 57 73 D4 84 49
9:32:1...	Kenora.exe	3104	Process Create	C:\ProgramData\Synaptics\Synaptics.exe	SUCCESS	PID: 4900, Command line: "C:\ProgramData\Synaptics\Synaptics.exe" InjUpdate
9:32:1...	Kenora.exe	4084	Process Start		SUCCESS	Parent PID: 1068, Command line: "C:\Users\Securemisr\Desktop\Kenora.exe" , Current directory: C:\Users\Securemisr\Desktop\, Environment: ALLUSERSPROFILE=C:\ProgramDataAPPDATA=C:\Users\S
9:32:1...	Kenora.exe	4084	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SyncRootManager	SUCCESS	Desired Access: Notify, Disposition: REG_OPENED_EXISTING_KEY
9:32:1...	Kenora.exe	4084	RegCreateKey	HKCR\WOW6432Node\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance	SUCCESS	Desired Access: Notify, Disposition: REG_OPENED_EXISTING_KEY
9:32:1...	Kenora.exe	4084	RegCreateKey	HKCR\WOW6432Node\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance	SUCCESS	Desired Access: Notify, Disposition: REG_OPENED_EXISTING_KEY
9:32:1...	Kenora.exe	4084	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
9:32:1...	Kenora.exe	4084	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	Type: REG_BINARY, Length: 100, Data: 4E 3A AA 90 BA 1C 33 42 B8 BB 53 57 73 D4 84 49
9:32:1...	Kenora.exe	4084	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	SUCCESS	Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
9:32:1...	Kenora.exe	4084	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:32:1...	Kenora.exe	4084	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:32:1...	Kenora.exe	4084	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:32:1...	Kenora.exe	4084	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
9:32:1...	Kenora.exe	4084	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:32:1...	Kenora.exe	4084	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:32:1...	Kenora.exe	4084	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
9:32:1...	Kenora.exe	4084	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
9:32:1...	Kenora.exe	4084	Process Create	C:\Users\Securemisr\Desktop_cache_Kenora.exe	SUCCESS	PID: 4760, Command line: "C:\Users\Securemisr\Desktop_cache_Kenora.exe"

4- Finally run the Autoruns tool to check all of the persistence locations.



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/16/2016 1:48 PM	
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	7/16/2016 4:23 AM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				4/27/2020 11:04 PM	
☑ VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	c:\program files\vmware\vmware tool...	3/22/2018 11:23 AM	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				5/18/2020 9:31 PM	
☑ OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\securemisr\appdata\local\...	4/6/2016 5:07 AM	
☑ Synaptics Pointing Devi...	Synaptics Pointing Device Driver	(Not verified) Synaptics	c:\programdata\synaptics\synaptics....	6/20/1992 12:22 AM	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				7/16/2016 1:48 PM	
☑ n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	5/19/2016 4:48 AM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				7/16/2016 1:48 PM	
☑ n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	5/19/2016 5:19 AM	
Task Scheduler					
☑ \Microsoft\Windows\Up...	UpdateAssistant	(Verified) Microsoft Corporation	c:\windows\updateassistant\update...	4/17/1917 9:31 PM	
☑ \Microsoft\Windows\Up...	UpdateAssistant	(Verified) Microsoft Corporation	c:\windows\updateassistant\update...	4/17/1917 9:31 PM	
☑ \Microsoft\Windows\Up...	UpdateAssistant	(Verified) Microsoft Corporation	c:\windows\updateassistant\update...	4/17/1917 9:31 PM	
☑ \Microsoft\Windows\Up...	UpdateAssistant	(Verified) Microsoft Corporation	c:\windows\updateassistant\update...	4/17/1917 9:31 PM	
☑ \Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Verified) Microsoft Corporation	c:\program files\windows defender\m...	10/9/2017 3:49 AM	
☑ \Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Verified) Microsoft Corporation	c:\program files\windows defender\m...	10/9/2017 3:49 AM	
☑ \Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Verified) Microsoft Corporation	c:\program files\windows defender\m...	10/9/2017 3:49 AM	
☑ \Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Verified) Microsoft Corporation	c:\program files\windows defender\m...	10/9/2017 3:49 AM	

the tool has detected the UNSIGNED Value (red highlighted), feel free to navigate the rest of Tabs.

NOW revert to the clean snapshot

Mostafa Yahia
E-Mail: Mostafayahia753@gmail.com
LinkedIn: https://www.linkedin.com/in/mostafa-yahia-701b4b15a/