



TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM

KHOA CÔNG NGHỆ THÔNG TIN

Môn: Thực Hành Phân Tích Mã Độc

Họ Và Tên: Trần Hân Nhi

MSSV: 2011770131

Lớp: 20DATA1

Báo Cáo Tuần 2

- Thực hiện phân tích tĩnh để kiểm tra mẫu mã độc, dùng md5sum xác định giá trị hàm băm của file sales.bin

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ ls
sales.bin
(kali@kali)-[~/Desktop]
$ file sales.bin
sales.bin: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
(kali@kali)-[~/Desktop]
$ md5sum sales.bin
51d9e2993d203bd43a502a2b1e1193da sales.bin
```

- Dùng strings kiểm tra

```
GetFileAttributes
SizeofResource
WinExec
WriteFile
lstrcatA
lstrcmpiA
lstrlenA
kernel32.dll
SHGetPathFromIDListA
SHGetSpecialFolderLocation
ShellExecuteA
shell32.dll
RegCloseKey
RegCreateKeyA
RegSetValueExA
advapi32.dll
kernel32.dll
Software\Microsoft\Windows\CurrentVersion\Run
ShellExecuteA
shell32.dll
RegCloseKey
RegCreateKeyA
RegSetValueExA
advapi32.dll
```

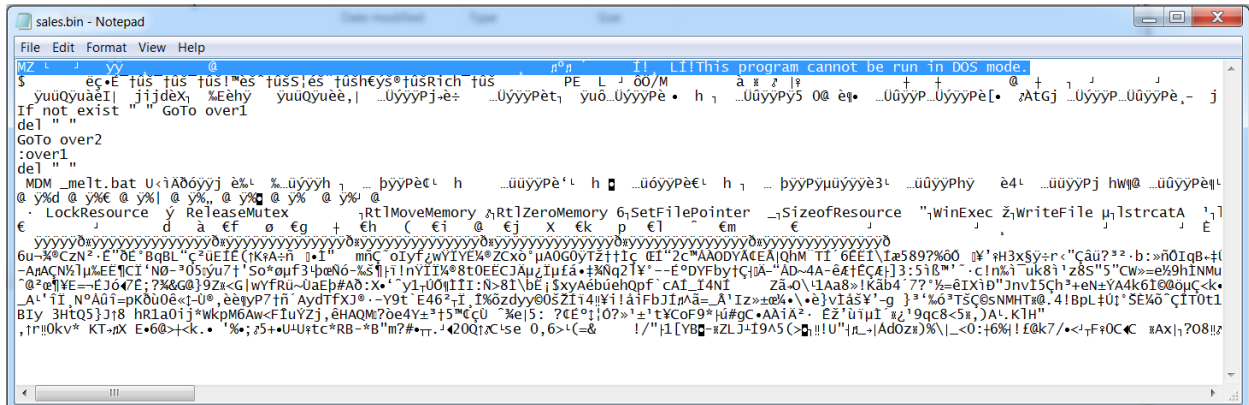
```
WinExec
WriteFile
12da398350fd1a2cd7d95e9f2c7248c3b8f87683

(kali@kali)-[~/Desktop]
$ python3 APIVirustotal.py 12da398350fd1a2cd7d95e9f2c7248c3b8f87683
Detection: 65/72
VirusTotal Results:
/tBkav ==> W32.AIDetectMalware
/tLionic ==> Trojan.Win32.Small.l60l
/tElastic ==> malicious (high confidence)
/tCynet ==> Malicious (score: 100)
/tCMC ==> None
/tCAT-QuickHeal ==> Backdoor.Poisonivy.EX4
/tSkyhigh ==> BehavesLike.Win32.PWSZbot.lh
/tALYac ==> Backdoor.Generic.474970
/tCylance ==> unsafe
/tZillya ==> Dropper.Agent.Win32.242906
/tSangfor ==> Suspicious.Win32.Save.a
/tK7AntiVirus ==> Trojan ( 004c4a601 )
/tAlibaba ==> Ransom:Win32/Kisucrypt.64021cc3
/tK7GW ==> Trojan ( 004c4a601 )
/tCybereason ==> malicious.350fd1
/tBaidu ==> None
/tVirIT ==> None
/tSymantec ==> ML.Attribute.HighConfidence
/ttehtris ==> None
/tESET-NOD32 ==> Win32/TrojanDropper.Agent.PEH
/tAPEX ==> Malicious
/tPaloalto ==> None
/tClamAV ==> Win.Trojan.Poison-1487
/tKaspersky ==> Trojan.Win32.Agentb.jan
/tBitDefender ==> Backdoor.Generic.474970
```

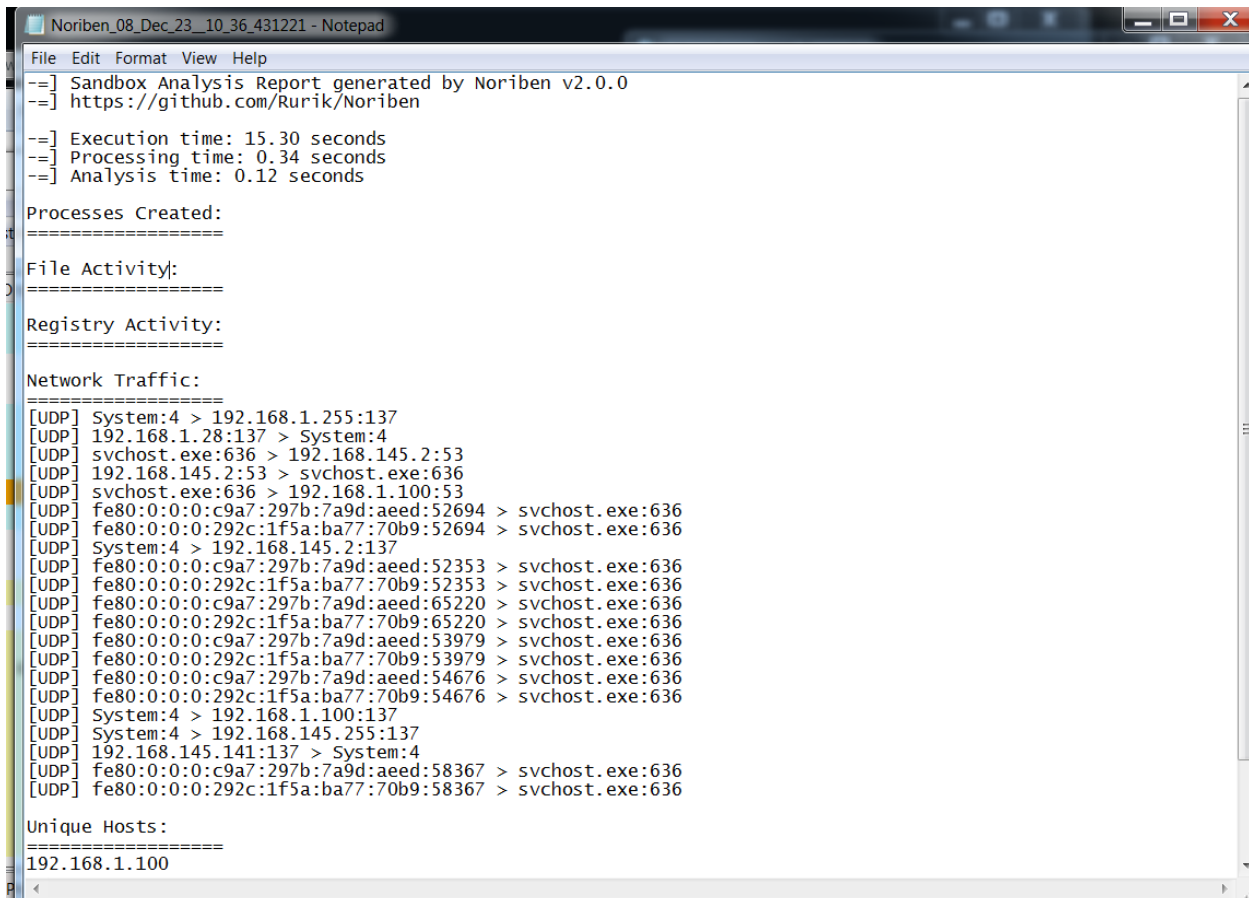
- Dùng inetsim mô phỏng port đánh lạc hướng mã độc.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== INetSim main process started (PID 9972) ==
Session ID: 9972
Listening on: 127.0.0.1
Real Date/Time: 2023-12-07 22:56:45
Fake Date/Time: 2023-12-07 22:56:45 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 9974)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm l
ine 399.
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm l
ine 399.
* https_443_tcp - started (PID 9976)
* http_80_tcp - started (PID 9975)
* ident_113_tcp - started (PID 9987)
* pop3_110_tcp - started (PID 9979)
* ftp_21_tcp - started (PID 9981)
* daytime_13_tcp - started (PID 9993)
* irc_6667_tcp - started (PID 9984)
* time_37_tcp - started (PID 9989)
* ftps_990_tcp - started (PID 9982)
* echo_7_tcp - started (PID 9995)
* tftp_69_udp - started (PID 9983)
* discard_9_udp - started (PID 9998)
* daytime_13_udp - started (PID 9994)
* finger_79_tcp - started (PID 9986)
* discard_9_tcp - started (PID 9997)
* pop3s_995_tcp - started (PID 9980)
* syslog_514_udp - started (PID 9988)
* echo_7_udp - started (PID 9996)
* smtps_465_tcp - started (PID 9978)
* time_37_udp - started (PID 9992)
* quotd_17_udp - started (PID 10000)
* quotd_17_tcp - started (PID 9999)
```

- Xác định tệp thực thi bằng notepad. File hiện dòng MZ, ta xác định được đây là tệp thực thi EXE PE.



- Chạy Noriben khởi động Process Monitor. Khi hoàn tất giám sát, lưu kết quả vào một tệp văn bản (.txt) và tệp CSV (.csv) trong cùng thư mục.



- Khi thực thi file mã độc, Process Hacker hiện 1 tiến trình lạ. Ta tiến hành kiểm tra thông tin của chương trình lạ.

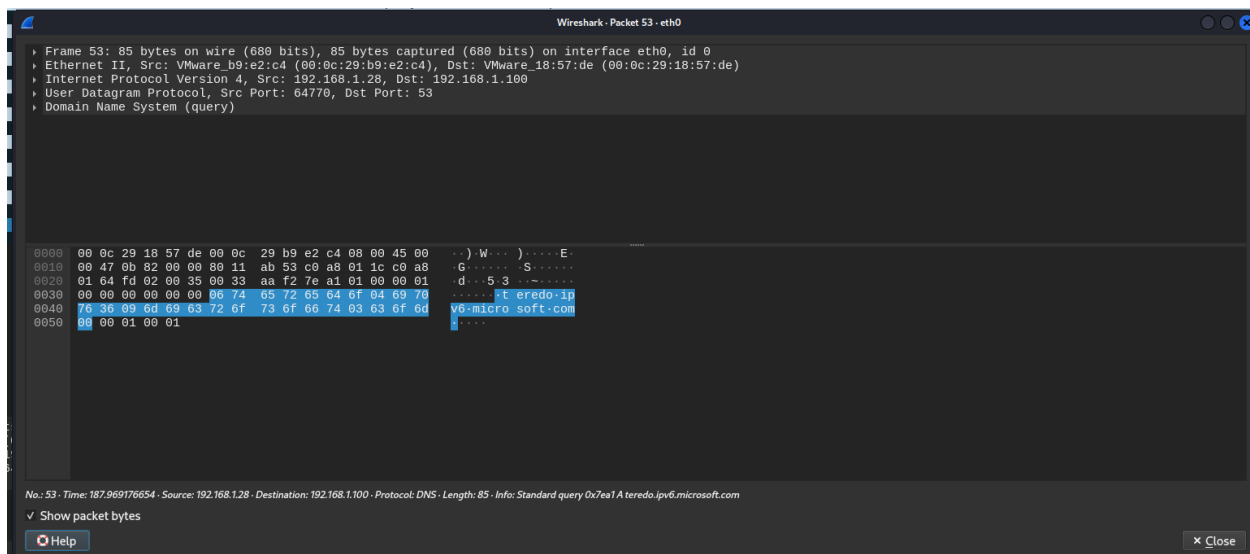
The screenshot displays a Windows 7 desktop environment. In the foreground, the Process Hacker application is open, showing a list of running processes. The process explorer.exe is highlighted. To the right, the Properties window for explorer.exe is open, showing the File tab. The process is identified as explorer.exe (2004) with a version of N/A. The command line is "C:\Users\DHTT\AppData\Roaming\explorer.exe". The current directory is "C:\Users\Public\New folder(Bui2)". The process started 13 seconds ago at 10:44:17 AM on 12/8/2023. The PEB address is 0x7efdf000 (32-bit: 0x7efdf000) and the image type is 32-bit. The parent is Non-existent process (2228). The mitigation is None and the protection is None. Below the Process Hacker window, a Wireshark packet capture is visible, showing a DNS query from 192.168.1.28 to 192.168.1.100. The packet details show a Standard query type for www.webserver.proxydns.com. The packet bytes are displayed in hexadecimal and ASCII.

Name	PID	CPU	I/O total r...	Private by...	User name	Description
SearchIndexer.exe	2488			24.29 MB		Microsoft Windows Search Ind...
SearchProtocolHo...	3996			2.33 MB		Microsoft Windows Search Pro...
SearchFilterHost.exe	1260			1.96 MB		Microsoft Windows Search Fil...
svchost.exe	2796			3.4 MB		Host Process for Windows Serv...
spssvc.exe	2584			7.43 MB		Microsoft Software Protection ...
svchost.exe	196			67.33 MB		Host Process for Windows Serv...
taskhost.exe	3020			4.45 MB	DHTT-PC\DHTT	Host Process for Windows Task...
lsass.exe	460			4.28 MB		Local Security Authority Process
lsm.exe	468			2.23 MB		Local Session Manager Service
csrss.exe	404	0.09		8.86 MB		Client Server Runtime Process
conhost.exe	2840			1.33 MB	DHTT-PC\DHTT	Console Window Host
winlogon.exe	496			2.8 MB		Windows Logon Application
explorer.exe	2064	0.04		41.39 MB	DHTT-PC\DHTT	Windows Explorer
idnity.exe	1572			1.4 MB	DHTT-PC\DHTT	Windows Device Installation
Process Hacker.exe	3160	0.46		11.41 MB	DHTT-PC\DHTT	Process Hacker
vmtoolsd.exe	1532	0.17	760 B/s	21.14 MB	DHTT-PC\DHTT	VMware Tools Core Service
cmd.exe	2732			3.63 MB	DHTT-PC\DHTT	Windows Command Processor
py.exe	2860			1.95 MB	DHTT-PC\DHTT	Python
python.exe	2144			9.14 MB	DHTT-PC\DHTT	Python
Procmon.exe	3344			5.36 MB	DHTT-PC\DHTT	Process Monitor
procmon64.exe	2440	0.37	30.08 kB/s	67.9 MB	DHTT-PC\DHTT	Process Monitor
explorer.exe	2064			1.59 MB	DHTT-PC\DHTT	Process Monitor

No.	Time	Source	Destination	Protocol	Length	Info
0	0.3.253865895	192.168.1.28	192.168.1.100	DNS	88	Standard query 0x5688 A teredo.ipv6.microsoft.com
1	0.3.253865895	192.168.1.100	192.168.1.28	ICMP	113	Destination unreachable (Port unreachable)
11	25.822582768	192.168.1.28	192.168.1.100	DNS	88	Standard query 0x1469 A www.webserver.proxydns.com
12	25.822555735	192.168.1.100	192.168.1.28	ICMP	114	Destination unreachable (Port unreachable)
14	40.824005452	192.168.1.28	192.168.1.100	DNS	85	Standard query 0xd2a2 A teredo.ipv6.microsoft.com
15	40.824005452	192.168.1.100	192.168.1.28	ICMP	113	Destination unreachable (Port unreachable)
23	83.262518234	192.168.1.28	192.168.1.100	DNS	85	Standard query 0x984a A teredo.ipv6.microsoft.com
24	83.262518234	192.168.1.100	192.168.1.28	ICMP	114	Destination unreachable (Port unreachable)
26	85.835468771	192.168.1.28	192.168.1.100	DNS	88	Standard query 0xdcc2 A www.webserver.proxydns.com
27	85.835468771	192.168.1.100	192.168.1.28	ICMP	114	Destination unreachable (Port unreachable)
30	126.606030360	192.168.1.28	192.168.1.100	DNS	85	Standard query 0x489a A teredo.ipv6.microsoft.com
30	126.606030360	192.168.1.100	192.168.1.28	ICMP	113	Destination unreachable (Port unreachable)
46	145.849428962	192.168.1.28	192.168.1.100	DNS	88	Standard query 0x489b A www.webserver.proxydns.com
47	145.849428962	192.168.1.100	192.168.1.28	ICMP	114	Destination unreachable (Port unreachable)
50	156.276211373	192.168.1.28	192.168.1.100	DNS	85	Standard query 0x4832 A teredo.ipv6.microsoft.com
51	156.276211373	192.168.1.100	192.168.1.28	ICMP	113	Destination unreachable (Port unreachable)

Frame 5: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface eth0, id 0
Ethernet II, Src: VMware b0:22:c4 (00:0c:29:b9:c2:c4), Dst: VMware 18:57:de (00:0c:29:18:57:de)
Internet Protocol Version 4, Src: 192.168.1.28, Dst: 192.168.1.100
User Datagram Protocol, Src Port: 61416, Dst Port: 53
Domain Name System (query)

Wireshark_eth0G8Y2.pcapng
Packets: 52 - Displayed: 16 (30.8%)
Profile: Default



- So sánh giá trị băm md5 của file mã độc và tiến trình lạ.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ ls
APIVirustotal.py iexplorer.exe sales.bin
(kali@kali)-[~/Desktop]
$ md5sum iexplorer.exe sales.bin
51d9e2993d203bd43a502a2b1e1193da iexplorer.exe
51d9e2993d203bd43a502a2b1e1193da sales.bin
```

- File iexplorer.exe không cần triển khai chức năng xóa file trong mã nguồn. Nó chỉ cần nhập và gọi hàm DeleteFile.

CFF Explorer VIII - [explorer.exe]

File Settings ?

File: explorer.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Module Name Imports OFTs TimeDateStamp ForwarderChain Name RVA FTs (IAT)

000010F6	N/A	00000E8C	00000E90	00000E94	00000E98	00000E9C
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
kernel32.dll	26	000020EC	00000000	00000000	000022F6	00002010
shell32.dll	3	00002158	00000000	00000000	0000234A	0000207C
advapi32.dll	3	000020DC	00000000	00000000	00002386	00002000

OFTs FTs (IAT) Hint Name

Dword	Dword	Word	szAnsi
000021A0	000021A0	0053	DeleteFileA
000021AE	000021AE	0080	ExitProcess
000021BC	000021BC	00A2	FindResourceA
000021CC	000021CC	00B5	FreeResource
000021DC	000021DC	00FD	GetLastError
000021EC	000021EC	0107	GetModuleFileNameA

11:58 AM 12/8/2023