



FPT UNIVERSITY

Malware Analysis Report

Dương Hàn Nam
SE161443

SET UP

I. Set up các tools

A. Các tools phân tích

- Virustotal: <https://www.virustotal.com/gui/home/upload>
- Wireshark(free tool): <https://www.wireshark.org/#download>
- Exeinfo PE: <https://softfamous.com/exeinfo-pe/>
- UPX: <https://windows-1.com/upx-for-pc.html>
- Ida pro 7.3 (có bản quyền)
- Tất cả các tools là (64bits) theo máy phân tích

B. Mẫu malware

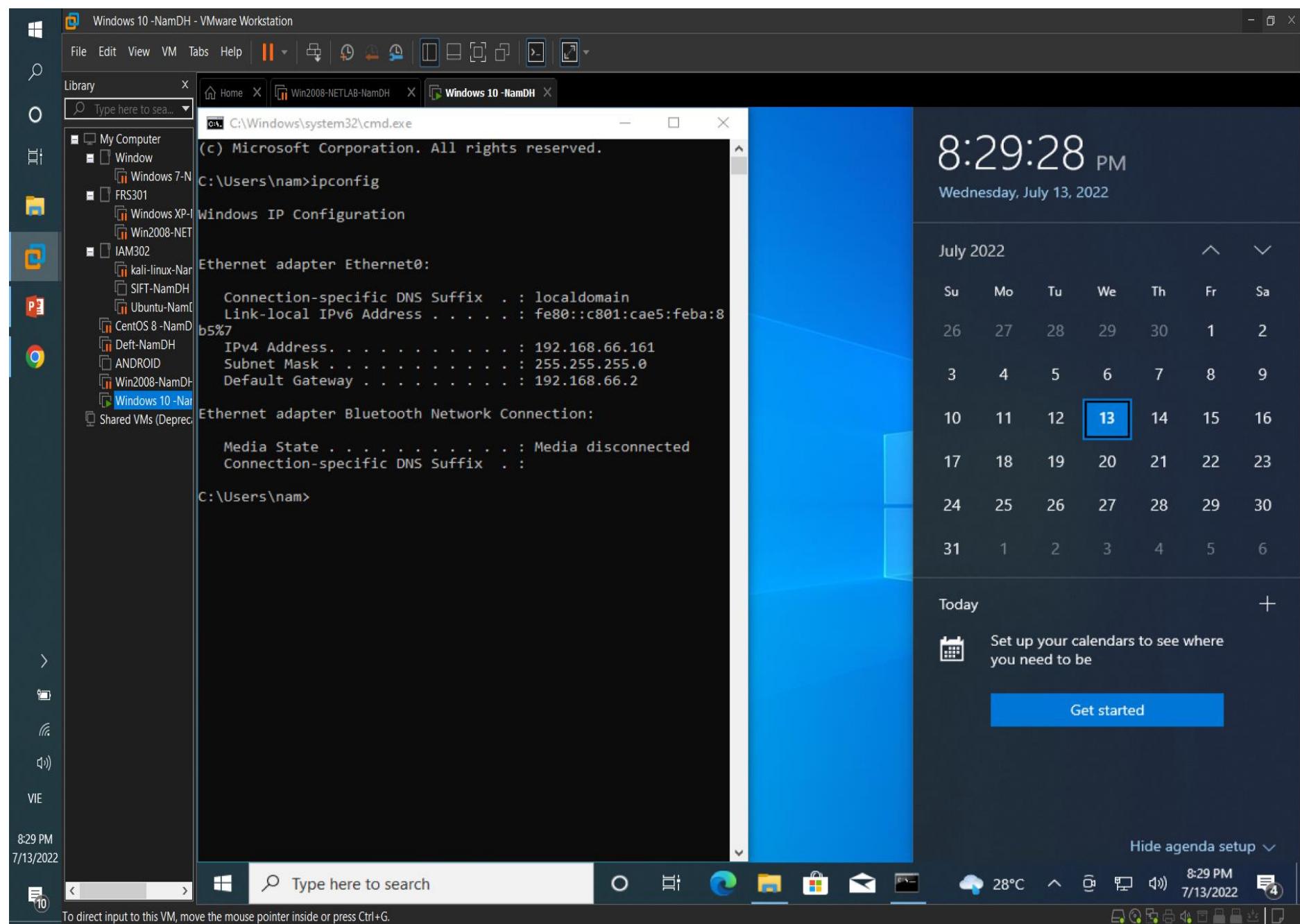
- Đây là mẫu malware về adware sẽ được phân tích trong report này
- Link web tải:
<https://dasmalwerk.eu/?fbclid=IwAR3qo1J0voS48iDJTa9FYQjN0UA83rPBrZ9qQuDYIpl5aGJgriIMcfJUXo>
- Chọn mẫu: Malware Name: Adware (004f7c2e1)

Dropped:Trojan.Dropper.Agent.VOE 'Adware (004f7c2e1)	Download Dropped:Trojan.Dropper.Agent.VOE sample Download 'Adware (004f7c2e1) sample	91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a
Trojan.GenericKD.40445486 Trojan.GenericKD.40455512	Download Trojan.GenericKD.40445486 sample Download Trojan.GenericKD.40455512 sample	e796e64c5f9a7568773bd2924e992172f222957e039ab7b41ade448e e523418670b4ef66754a610bf18a60d31a8a17020028ad3f1431712

II. Set up máy ảo

Máy bị nhiễm có những đặc điểm sau:

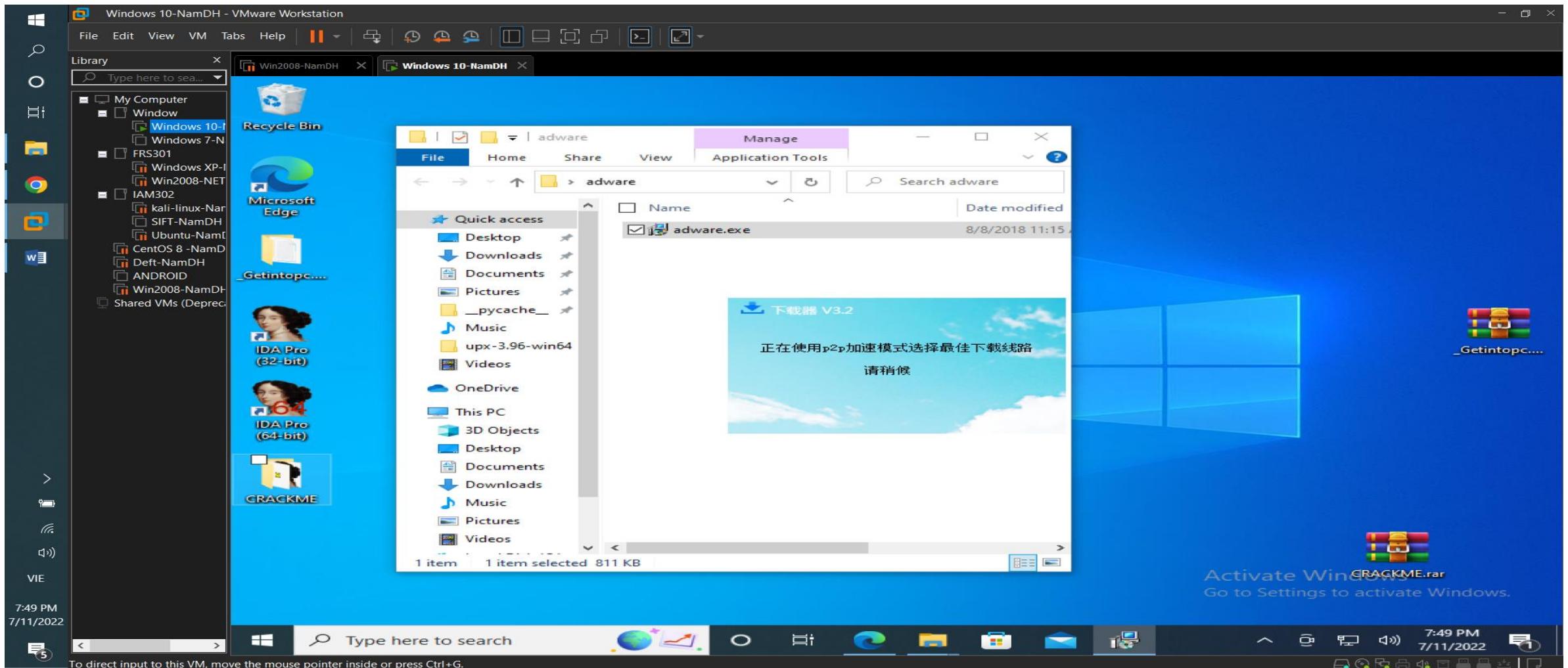
- Win 10
- Ipv4: 192.168.66.161
- Thời gian thực hiện trên máy ảo



Analysis

I. Biểu hiện

- Khi file malware được khởi động. Một quảng cáo về tải một app lạ liền pop-up lên màn hình



II. Phân tích

Đưa mẫu malware lên virustotal để phân tích, dựa trên những thông tin mà virustotal cung cấp ta sẽ phân tích và kiểm tra mẫu mã độc

<https://www.virustotal.com/gui/file/37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9>

The screenshot shows the Virustotal analysis interface for the file hash `37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9`. The main page displays a red circular icon with the number "57 / 66" indicating vendor detections. A prominent message states: "57 security vendors and no sandboxes flagged this file as malicious". Below this, the file details are shown: size 811.26 KB, last analyzed on 2022-06-30 19:50:49 UTC, and it was uploaded 10 days ago. The file type is identified as EXE. The "DETECTION" tab is selected, showing a table of vendor analysis results:

Security Vendor	Detection	Analysis	
Ad-Aware	Gen:Variant.Doina.21780	AhnLab-V3	PUP/Win32.Qjwmonkey.R187306
Alibaba	Downloader:Win32/Bazload.3a998326	ALYac	Gen:Variant.Doina.21780
Arcabit	Trojan.Doina.D5514	Avast	FileRepMalware [Misc]
AVG	FileRepMalware [Misc]	Avira (no cloud)	ADWARE/Adware.Gen7
BitDefender	Gen:Variant.Doina.21780	BitDefenderTheta	Gen:NN.Zexaf.84742.YmMfaCxl@F
Bkav Pro	W32.AIDetect.malware1	ClamAV	Win.Trojan.Agent-1824051

The interface also includes tabs for "DETAILS", "RELATIONS", "BEHAVIOR", and "COMMUNITY". The bottom of the screen shows the Windows taskbar with various pinned icons and the date/time as 8:07 PM 7/11/2022.

Đây là mẫu malware đã được biết đến và định danh, virustotal đã cung cấp những thông tin quan trọng sau:

- Các thông tin về mã hash như MD5, SHA-1, SHA-256 vv...
- File type: [Win32 EXE](#)
- File size: [811.26 KB](#)
- PEID packer:
[UPX v0.89.6 –v1.02 / v1.05 –v1.24](#)
-> Markus & Laszlo [overlay] (Có thể file đã bị packed)

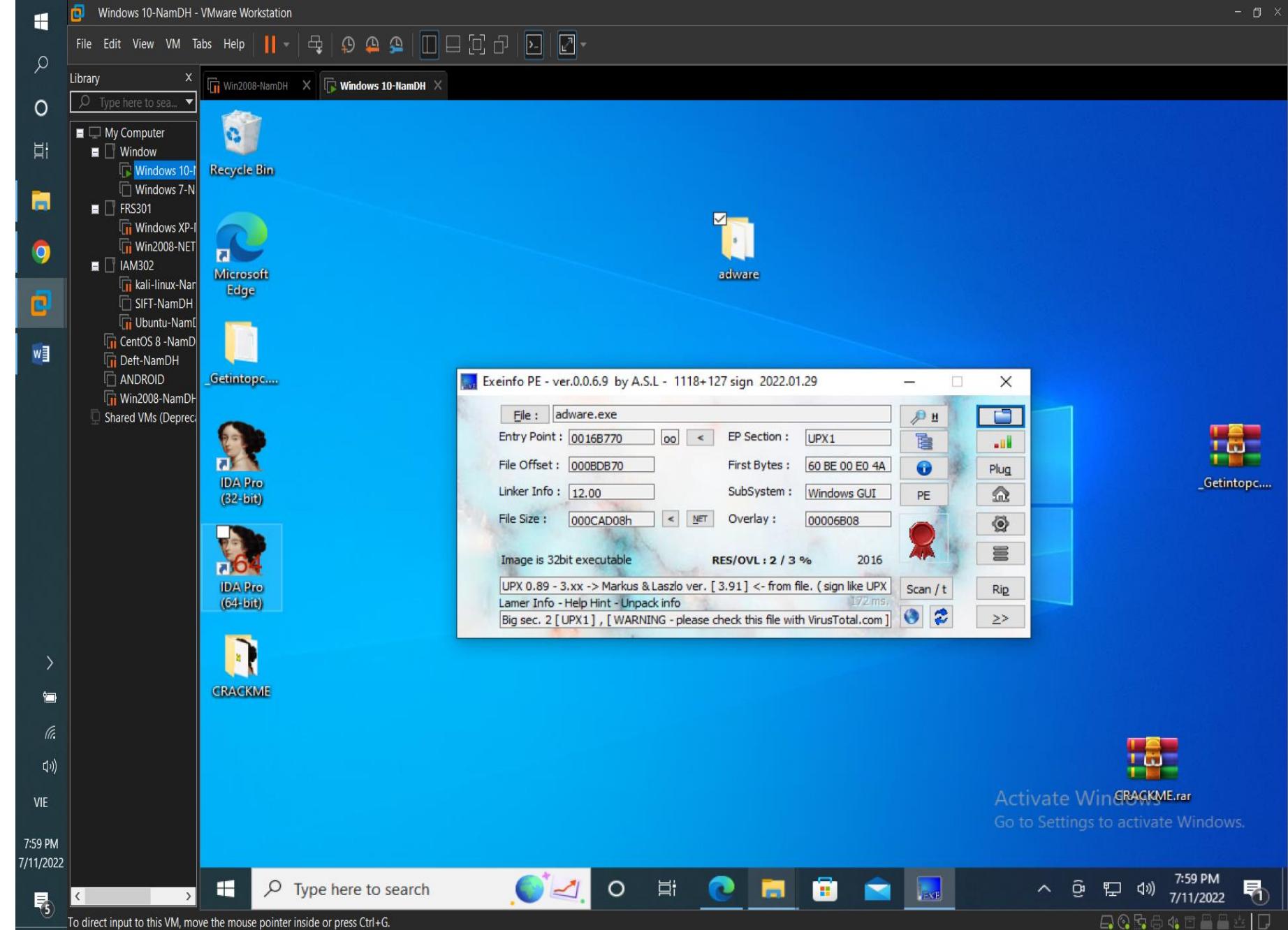
The screenshot shows the VirusTotal analysis interface for the file `37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9`. The 'DETAILS' tab is selected. Below it, the 'Basic Properties' section lists the following information:

Property	Value
MD5	b315c590c3ad691604597ea41f8dd84e
SHA-1	6d15e7f0bb54df5b27a093f20186773ab0af7707
SHA-256	37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9
Vhash	08503e0f7d1015z11z67z1015z1010101013z17z
Authentihash	c2b5080cb65af153e72e0eafaa4f32ee961f72d1ec0d772564cdf171c221d935
Imphash	365100121d9e63d60ff044587bff9a5
Rich PE header hash	c554b8575fc9e6157a0607263dea05a0
SSDEEP	24576:kKWhaKj3uHJ3iekCUWCWbJxVjMJ4fNgGxFR24d7:LWhJjw9fkCUW9I0JO7xn24d
TLSH	T150052323EA004447E615EC36FB55D7B61C10BD02BAE46A646EC5FCE770BD6A03B64A0F
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	UPX compressed Win32 Executable (39.1%)
TrID	Win32 EXE Yoda's Crypter (38.3%)
TrID	Win16 NE executable (generic) (7.2%)
TrID	Win32 Executable (generic) (6.5%)
TrID	OS/2 Executable (generic) (2.9%)
File size	811.26 KB (830728 bytes)
PEiD packer	UPX v0.89.6 - v1.02 / v1.05 - v1.24 -> Markus & Laszlo [overlay]
Cyren packer	UPX
F-PROT packer	UPX

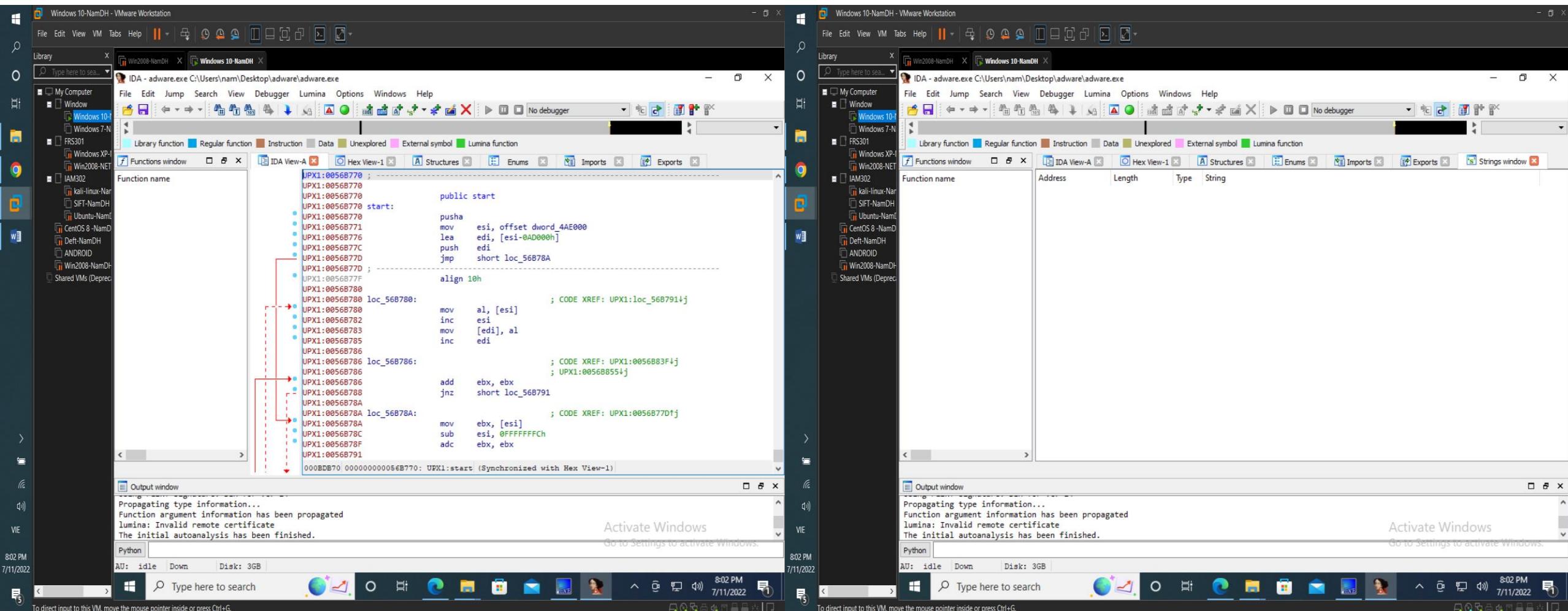
At the bottom right of the browser window, there is a watermark for Microsoft Windows: "Activate Windows Go to Settings to activate Windows".

Ta dùng công cụ Exeinfo PE để kiểm tra malware adware.exe, nó cung cấp rất nhiều thông tin nhưng quan trọng là:

- Ep Section: **UPX1**
(file đã bị packed upx)
- Image is 32bit executable: UPX 0.89 – 3.xx -> Markus & Laszlo ver. [3.91]
(version của upx giống như thông tin virustotal cung cấp)



Nếu ta mở file adware.exe bằng IDA pro để kiểm tra, ta sẽ thấy nó sẽ ở dạng upx1, và ta sẽ không thể xem Imports, hay chuỗi nhúng Strings của file



- Để unpacke đã packed dạng upx, ta dùng upx.exe tools
- Mở cmd và thực hiện câu lệnh sau:
Upx -d -o adware-unpacked.exe adware.exe
 (để trách tồn hại, ghi đè file gốc, ta unpacked file thành file mới adware-unpacked)
- File đã unpacked

```

Windows 10-NamDH - VMware Workstation
File Edit View VM Tabs Help ||| Library Type here to search... Manage upx-3.96-win64
File Home Share View Application Tools
This PC > Downloads > upx-3.96-win64 > upx-3.96-win64
C:\Windows\system32\cmd.exe
*file.. executables to (de)compress
Type 'upx --help' for more detailed help.

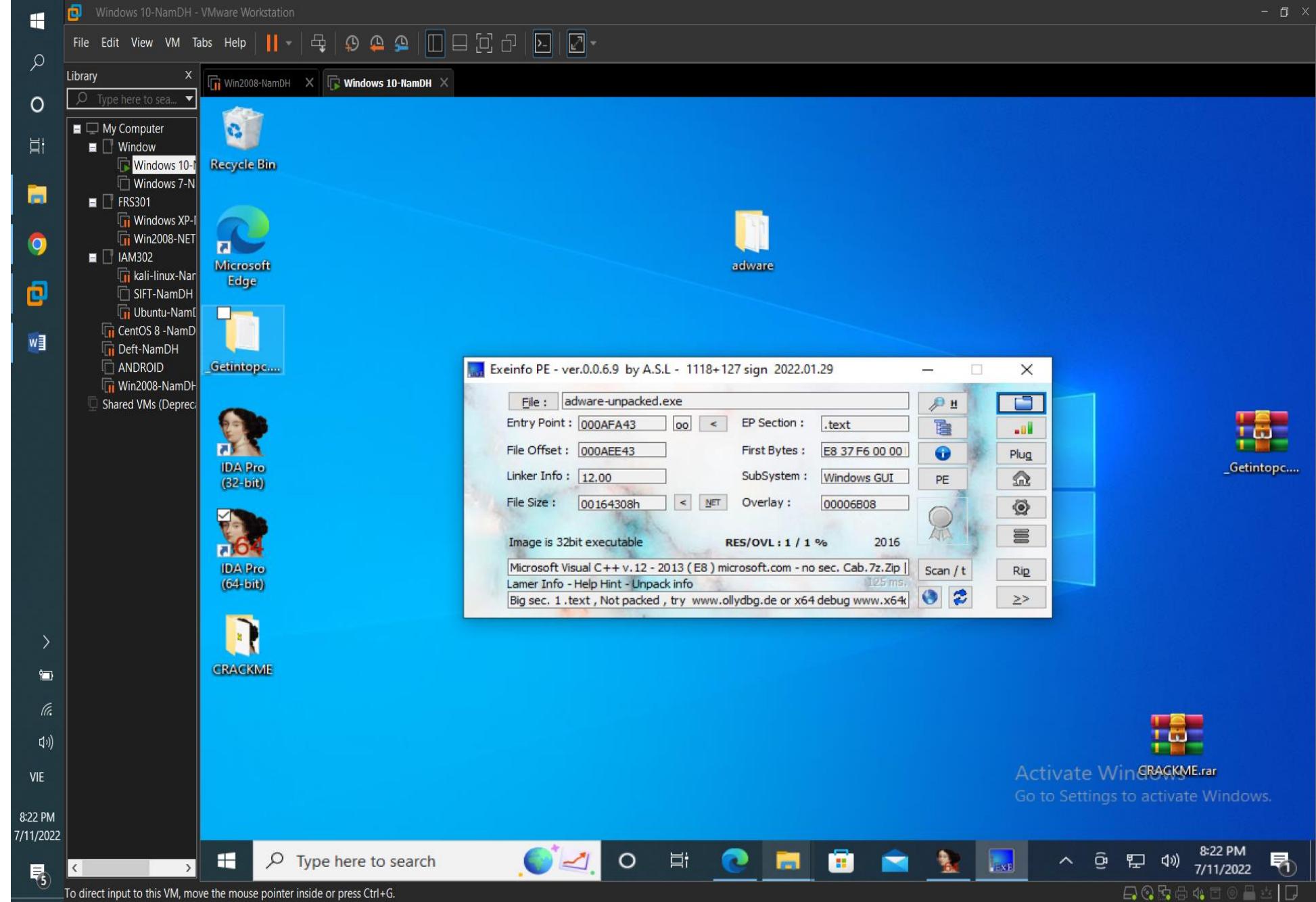
UPX comes with ABSOLUTELY NO WARRANTY; for details visit https://upx.github.io
E:\Users\nam\Downloads\upx-3.96-win64\upx-3.96-win64>upx -d -o adware-unpacked.exe adware.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020
File size      Ratio      Format      Name
-----<-     -----<-      -----<-      -----
1458952 <- 830728 56.94% win32/pe adware-unpacked.exe
Unpacked 1 file.
E:\Users\nam\Downloads\upx-3.96-win64\upx-3.96-win64>

```

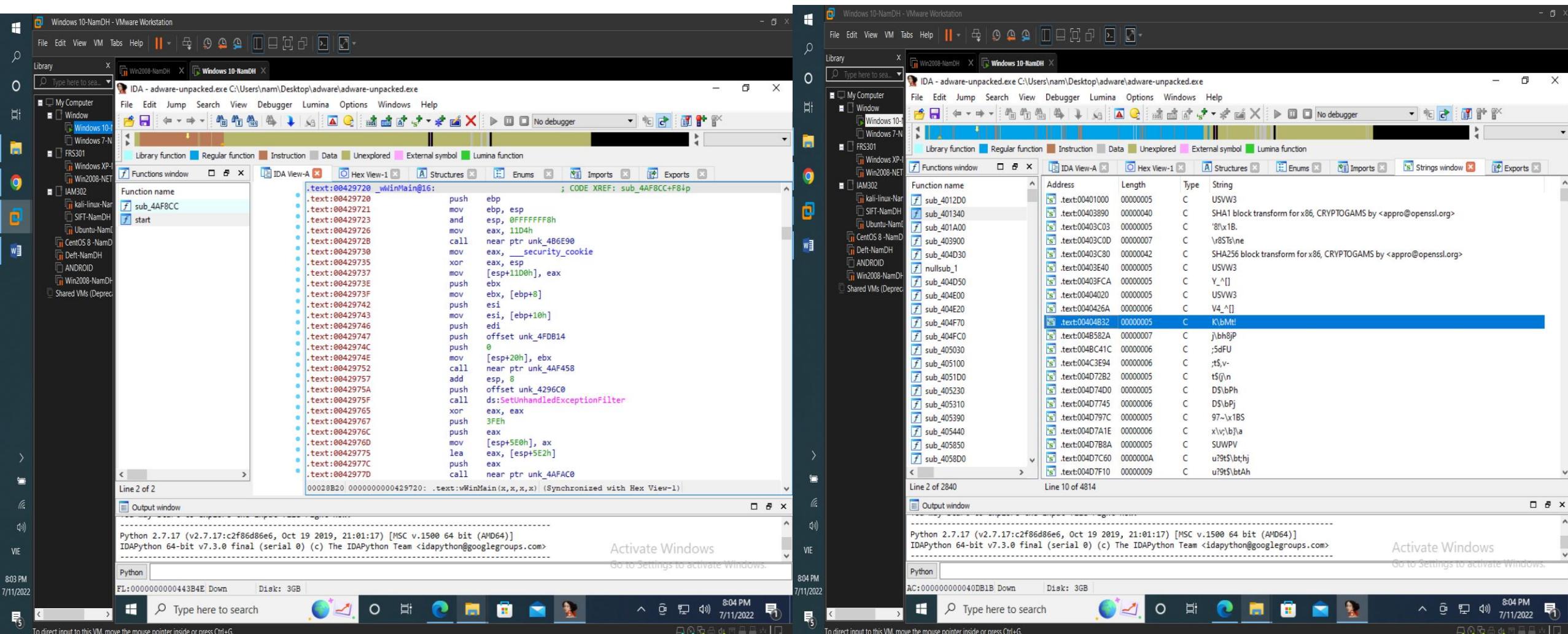
Activate Windows
Go to Settings to activate Windows.

Kiểm tra file adware-unpacked.exe vừa mới unpacked ta thấy:

- Ep section: .text
- Microsoft Visual C++
(Mã nguồn thực thi của Malware)



Bật IDA pro kiểm tra lại file unpacked adware-unpacked.exe ta thấy định dạng file là .text và ta có thể xem được thông tin Imports hay chuỗi nhúng Strings của file



- Chúng ta có thể thấy thông tin về ngôn ngữ biên dịch (chủ yếu là C++ và C)
- Ở mục header: ta có thể thấy thời gian malware được tạo ra (lưu ý nó có thể được chỉnh sửa)
- Ta cũng có thể thấy những thông tin về imports mà malware đã sử dụng

Portable Executable Info

Compiler Products

- [ASM] VS2013 UPD5 build 40629 count=5
- [C] VS2013 UPD5 build 40629 count=23
- [C++] VS2013 UPD5 build 40629 count=3
- [ASM] VS2013 build 21005 count=35
- [C++] VS2013 build 21005 count=79
- [C] VS2013 build 21005 count=233
- id: 225, version: 20806 count=7
- [C] VS2008 SP1 build 30729 count=13
- [IMP] VS2008 SP1 build 30729 count=35
- [--] Unmarked objects count=344

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2016-09-08 12:07:40 UTC
Entry Point	1488752
Contained Sections	3

Sections

Activate Windows
Go to Settings to activate Windows

Contained Resources By Type

RT_ICON	6
RT_GROUP_ICON	1
RT_VERSION	1
RT_DIALOG	1
RT_MENU	1
RT_MANIFEST	1

Activate Windows
Go to Settings to activate Windows

Ở đây ta thấy ở phần
Language: Chinese
⇒ Có thể malware
này được tạo bởi
người Trung Quốc

Windows 10-NamDH - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

Win2008-NamDH Windows 10-NamDH

https://www.virustotal.com/gui/file/37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9

Contained Resources By Language

Language	Count
CHINESE SIMPLIFIED	10
ENGLISH US	1

Contained Resources

SHA-256	Type	Language	Entropy	Chi2
d374d231f40ffe2da7c71bbf1b2dfd78a0e66ad603e851121df1c71051f80203	RT_ICO	CHINESE	3.27	279047.0
	N	SIMPLIFIED	3	
0a4d783c14704c963d417cfab8ad1f66a47866d79b106668cd3432786e442d	RT_ICO	CHINESE	4.29	53109.8
48	N	SIMPLIFIED		
22c113e4cab4b01d0a348ba8bb75fa32c57dc62fb3f52c372e486d8feeb5af2	RT_ICO	CHINESE	3.47	66022.38
0	N	SIMPLIFIED		
f9d16c7942ac9ab18b0600667e591acd1da35aaec7c6c3cad7479c96d8cef6	RT_ICO	CHINESE	3.03	530522.6
b2	N	SIMPLIFIED	9	
1fc972ea11bf0494ab62f7a8ca6f66ad4c6366e0e1377e4aeb570e82cc212ae	RT_ICO	CHINESE	2.82	254554.4
f	N	SIMPLIFIED	1	

Overlay

entropy	offset	chi2
7.5269694328308105	803328	31789.68

Activate Windows
Go to Settings to activate Windows.

8:10 PM 7/11/2022

Type here to search

16

Ta có thể thấy URLs và domains mà malware liên kết. Hãy chú ý tới http://api.baizhu.cc URLs xuất hiện rất nhiều và có thể là malware sẽ gửi thông tin kết nối đến địa chỉ này.

Ngoài ra ở phần người đăng ký (Registrar): Ta có thể thấy tên Alibaba (là một tập đoàn lớn của Trung Quốc) => Có thể đây là adware của họ, đúng với việc đây là malware do người Trung Quốc tạo ra

Windows 10-NamDH - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

0 Win2008-NamDH Windows 10-NamDH

My Computer Window Windows 10-N

FRS301 Windows XP-I Win2008-NET IAM302 kali-linux-Nar SIFT-NamDH Ubuntu-NamD CentOS 8-NamD Delt-NamDH ANDROID Win2008-NamD Shared VMs (Deprec)

37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9 &showp=1360x768&t=&h=1&md=1731771022

Contacted Domains

Domain	Detections	Created	Registrar
15.38.102.47.in-addr.arpa	0 / 93	-	-
212.161.61.168.in-addr.arpa	0 / 94	-	-
api.baizhu.cc	2 / 94	2012-08-08	Alibaba Cloud Computing (Beijing) Co., Ltd.
baizhu.cc	2 / 94	2012-08-08	Alibaba Cloud Computing (Beijing) Co., Ltd.
c.cnzz.com	0 / 94	2000-04-13	Alibaba Cloud Computing (Beijing) Co., Ltd.
cdn.baizhu.cc	3 / 94	2012-08-08	Alibaba Cloud Computing (Beijing) Co., Ltd.
crl.startcom.org	0 / 94	2000-10-12	Webcentral Group Limited dba Melbourne IT (Australia)
down.360safe.com	0 / 94	2006-05-17	GoDaddy.com, LLC
ocsp.startssl.com	0 / 94	2006-09-10	GoDaddy.com, LLC
s4.cnzz.com	0 / 94	2000-04-13	Alibaba Cloud Computing (Beijing) Co., Ltd.

Contacted IP Addresses

IP	Detections	Autonomous System	Country
104.192.108.18	1 / 93	55992	US
113.105.245.109	0 / 93	4134	CN
120.76.122.200	1 / 94	37963	CN

37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9

https://www.virustotal.com/gui/file/37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9

Contacted URLs

Scanned	Detections	Status	URL
2022-01-12	3 / 93	403	http://api.baizhu.cc/
2021-11-02	1 / 92	200	http://s95.cnzz.com/z_stat.php?id=1257656622&web_id=1257656622
2021-11-11	5 / 93	200	http://down.360safe.com/360/inst.exe
2016-09-12	0 / 68	200	http://z4.cnzz.com/stat.htm?id=1257656622&r=&lg=en-us&ntime=none&cnzz_eid=1712393167-1473712574-&showp=1360x768&t=&h=1&rnd=2115144766
2022-04-27	3 / 92	503	http://api.baizhu.cc/api/getdown
2019-04-03	3 / 66	200	http://cdn.baizhu.cc/youxi/index_1_1.htm
2019-12-07	0 / 72	200	http://c.cnzz.com/core.php?web_id=1257656622&t=z
2018-01-08	0 / 66	200	http://s4.cnzz.com/z_stat.php?id=1259684196&web_id=1259684196
2019-04-05	3 / 66	200	http://cdn.baizhu.cc/baizhu.zip
2016-09-12	0 / 68	200	http://z11.cnzz.com/stat.htm?id=1259684196&r=&lg=en-us&ntime=none&cnzz_eid=992716535-1473712947-&showp=1360x768&t=&h=1&rnd=1731771022

Contacted Domains

Domain	Detections	Created	Registrar
15.38.102.47.in-addr.arpa	0 / 93	-	-
212.161.61.168.in-addr.arpa	0 / 94	-	-

Nhìn thấy nguồn ip là CN hoặc có thể là US ngoài ra DNS resolutions xác định rõ tên miền api.baizhu.cc

Windows 10-NamDH - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search... My Computer

- My Computer
- Windows
- Windows 10-1
- Windows 7-N
- FRS301
- Windows XP-I
- Win2008-NET
- IAM302
 - kali-linux-Nar
 - SIFT-NamDH
 - Ubuntu-NamD
- CentOS 8 - NamD
- Deft-NamDH
- ANDROID
- Win2008-NamD
- Shared VMS (Deprec)

37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9

57 / 66

① 57 security vendors and no sandboxes flagged this file as malicious

37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9

811.26 KB | 2022-06-30 19:50:49 UTC

10 days ago

downloader

checks-user-input direct-cpu-clock-access overlay peexe runtime-modules spreader upx

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Microsoft Sysinternals 6

Network Communication

DNS Resolutions + api.baizhu.cc

IP Traffic

23.216.147.64.443 (TCP)
20.99.132.105.443 (TCP)

Activate Windows Go to Settings to activate Windows

8:12 PM 7/11/2022

Type here to search

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

Windows 10-NamDH - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search... Win2008-NamDH Windows 10-NamDH

https://www.virustotal.com/gui/file/37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9

IP	Detections	Autonomous System	Country
104.192.108.18	1 / 93	55992	US
113.105.245.109	0 / 93	4134	CN
120.76.122.200	1 / 94	37963	CN
123.138.67.81	0 / 93	4837	CN
20.99.132.105	0 / 94	8075	US
23.216.147.64	0 / 94	20940	US
39.108.27.173	0 / 93	37963	CN
39.97.130.28	2 / 94	37963	CN
42.156.140.84	0 / 93	37963	CN
47.102.38.15	2 / 94	37963	CN

Execution Parents

Scanned	Detections	Type	Name
2022-02-04	50 / 61	ZIP	Malware.zip
2022-04-28	25 / 50	Macintosh Disk Image	DeadlyNightShadeIII.iso

PE Resource Children

Scanned	Detections	File type	Name
2016-09-12	0 / 56	?	

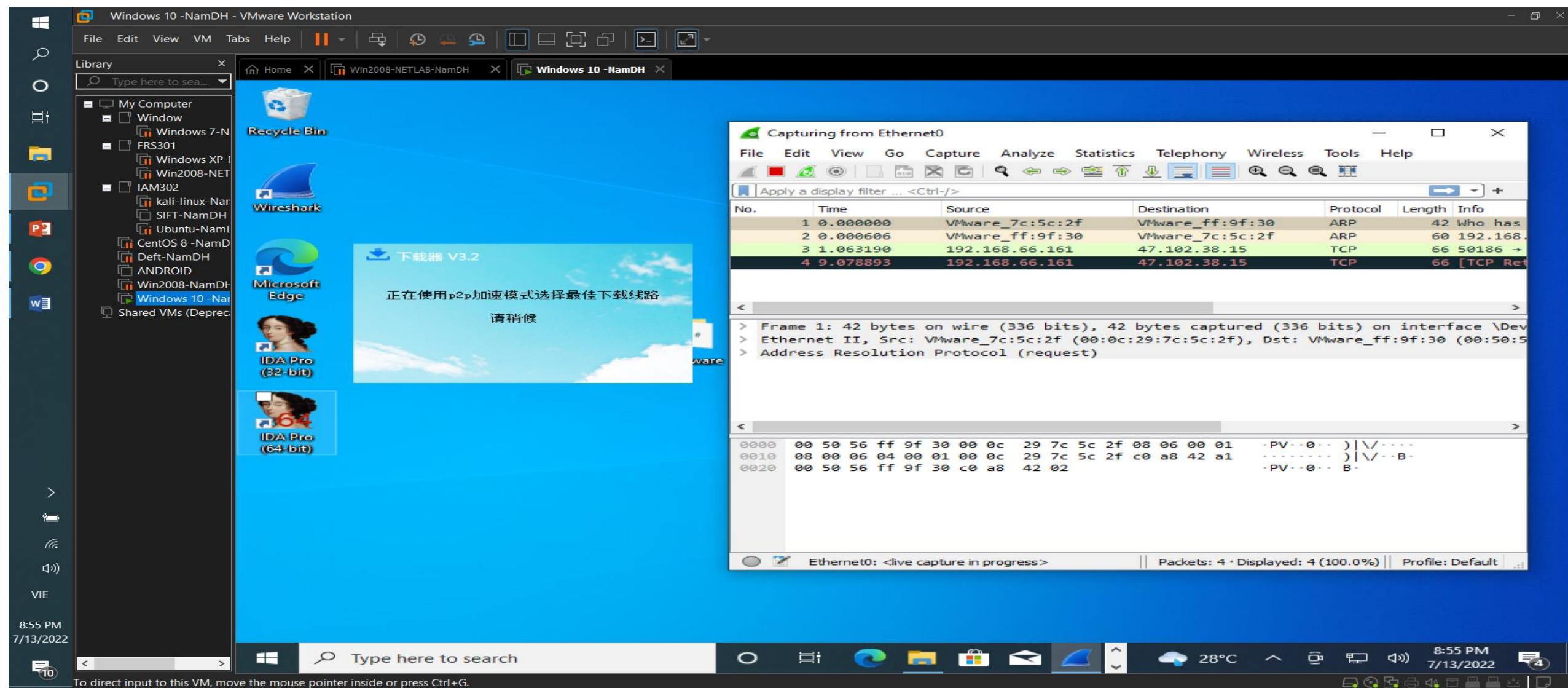
Activate Windows Go to Settings to activate Windows

8:11 PM 7/11/2022

Type here to search

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

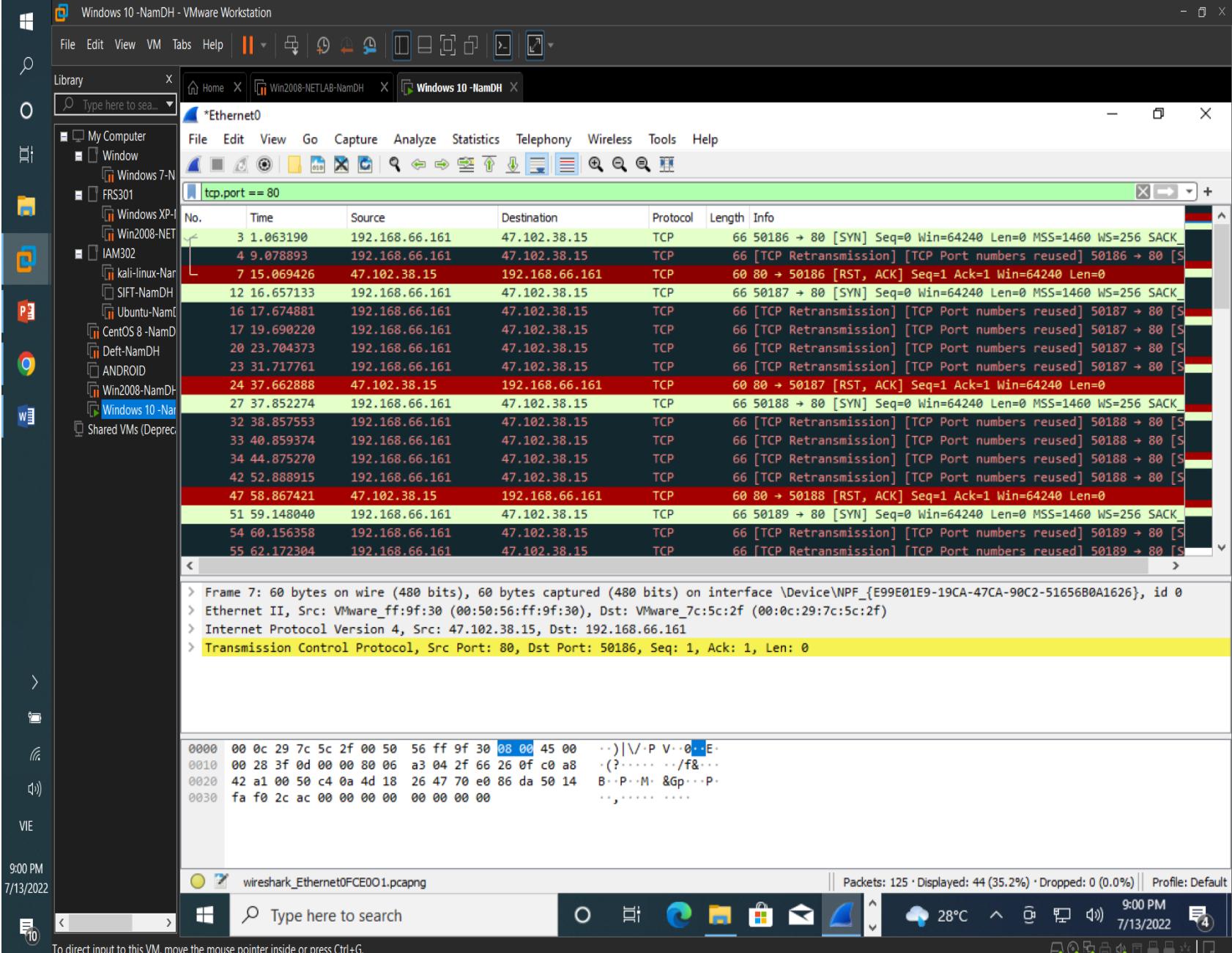
Để kiểm tra về ip trên virustotal có đúng không , ta sẽ dùng wireshark để capture lại khi malware đang chạy

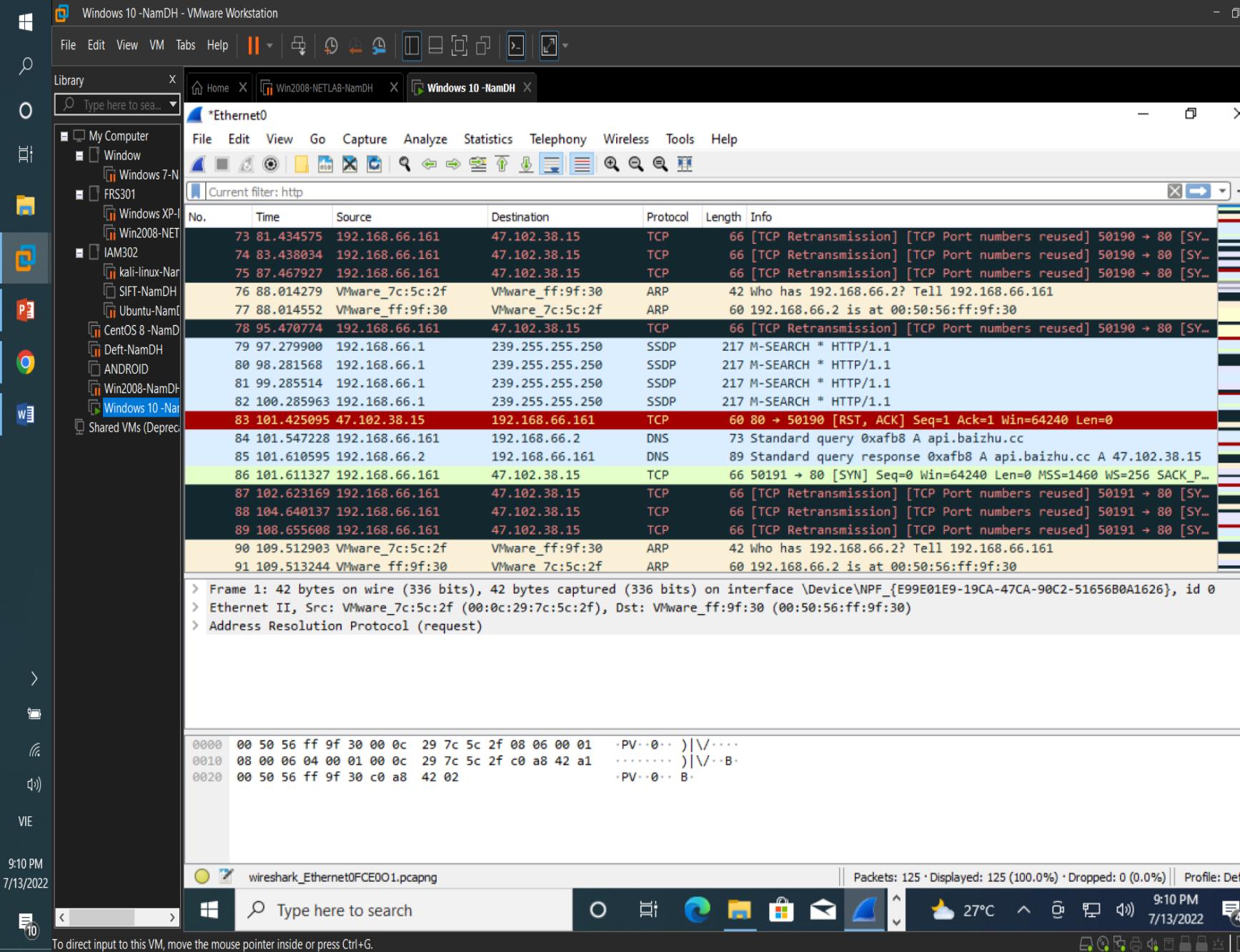


- Như ở phần đầu, máy bị nhiễm malware có ip: 192.168.66.161

- Ip: 47.102.38.15 được virustotal phát hiện khi phân tích file malware

=> Khi dùng wireshark capture ta có thể thấy khi chạy malware, thì giao tiếp giữa hai ip trên thực sự xảy ra (port 80)





Wireshark còn capture được giao thức SSDP (Simple Service Discovery Protocol): là một giao thức mạng dựa trên bộ giao thức Internet để quảng cáo và khám phá các dịch vụ mạng và thông tin hiện diện

Summary:

Đây là một malware dạng adware, khi click sẽ pop-up và xảy ra giao tiếp với máy chủ tại Trung Quốc, có các giao thức để quảng cáo trên nó. Ngoài ra nó đã được packed để không thể nhìn thấy được nội dung bên trong.