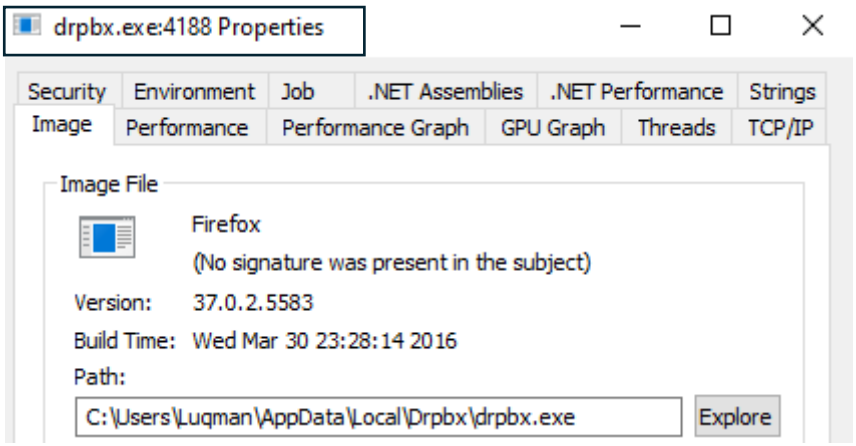
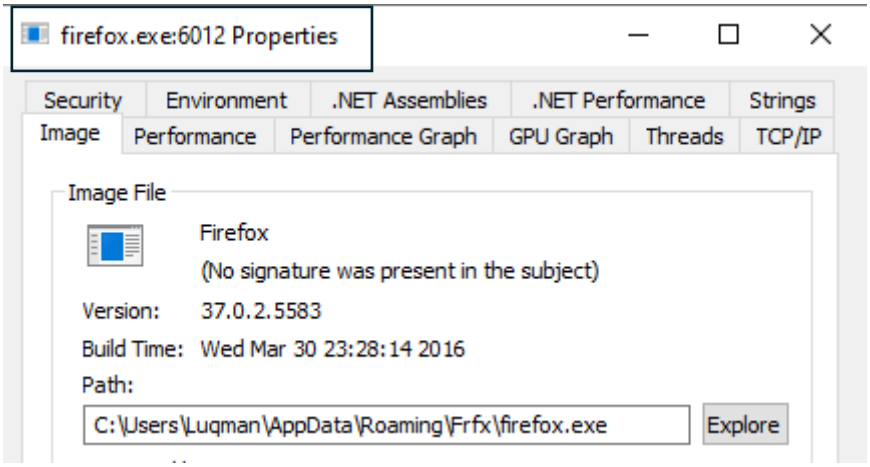
- Mention the names of the malicious processes, and provide explanations that point out why they are malicious.

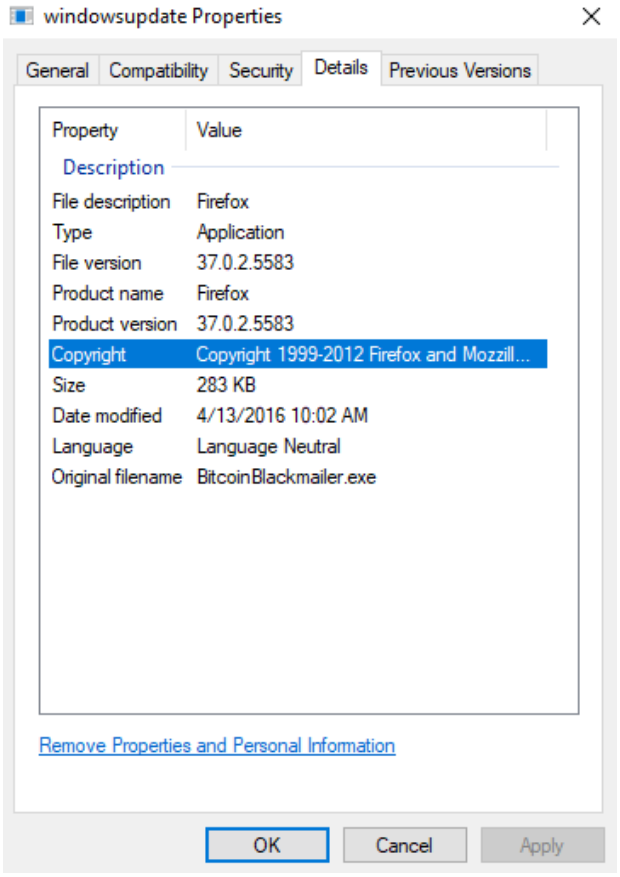
The name of the malicious processes is firefox.exe (PID 5712) and drpbx.exe (PID 5872 and 5880). There are no Windows signature for those two processes. They are not digitaly signed.



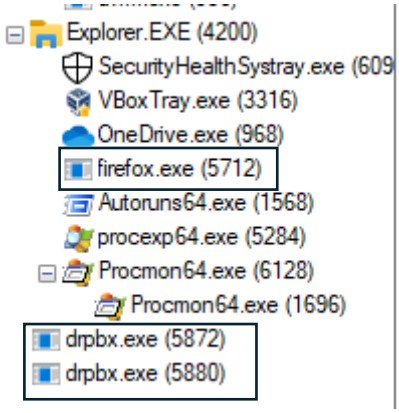


Those two processes runs automatically during the system boots. After killing that process firefox.exe in a task manager below window disappear 😉

The real name of this file is BitcoinBlackmailer.exe



- Specify the directory of the infected process.



For a firefox.exe PID 5712 directory is C:\Users\Luqman\AppData\Roaming\Frfx

For a drpbx.exe PID 5872 and 5880 the directory is C:\Users\Luqman\AppData\Local\drpbx

For windowsupdate.exe C:\Users\Luqman\Documents\WindowsUpdate.exe

- List files that are infected.

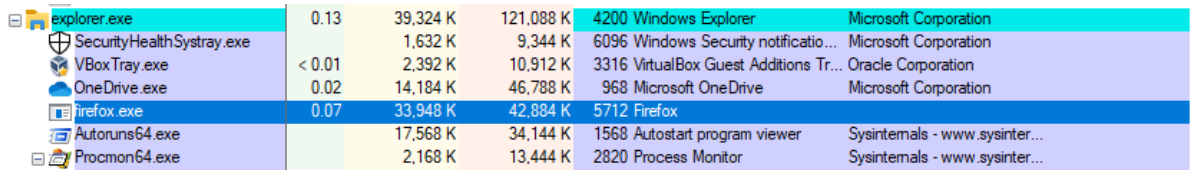
Firefox.exe

drpbx.exe

windowsupdate.exe

- Prove that the malicious process and the "Welcome" screen are the same.

If I drag Find Window's Process (drag over window) on a popped up window then Process Explorer Point Firefox.exe as a owner of this window.



- Add three strings that indicate that this is malware.

```
C:\Users\Luqman\Desktop\FinalToolkit Part 1\SysinternalsSuite>strings.exe C:\Users\Luqman\AppData\Roaming\Frfx\firefox.e
xe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

In a strings we have mentioned infected processes

```
Drpbx\drpbx.exe
Frfx\firefox.exe
System32Work\
```

Different real name of a file:

```
InternalName
BitcoinBlackmailer.exe
```

We can find same message in a strings:

```
Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.
If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal.
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypted files will be returned to normal.
       Thank you
Please, send $
 worth of Bitcoin here:
```

- Find the associated website and IP of the malware.

In a strings we can find this website:

http://btc.blockr.io/api/v1/

According to https://otx.alienvault.com/ below we can find related IP addresses:

HOSTNAME

btc.blockr.io Add to Pulse +

Passive DNS

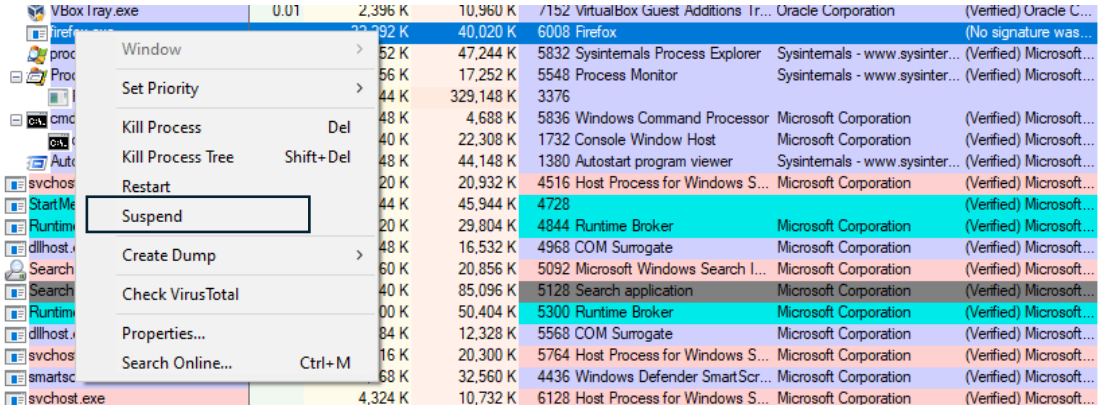
Show 10 entries Search:

STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
Unknown	btc.blockr.io	A	NXDOMAIN	2021-10-18 12:36	2024-06-22 08:44		
Unknown	btc.blockr.io	A	91.121.71.36	2021-07-27 02:18	2021-09-08 11:34	AS16276 ovh sas	France
Unknown	btc.blockr.io	A	52.90.150.224	2019-07-28 12:41	2019-08-13 09:29	AS14618 amazon.com inc.	United States
Unknown	btc.blockr.io	AAAA	2606:4700:30::6818:6099	2019-06-10 07:27	2019-07-23 09:00	AS13335 cloudflare	United States
Unknown	btc.blockr.io	AAAA	2606:4700:30::6818:6199	2019-06-10 07:27	2019-07-23 09:00	AS13335 cloudflare	United States
Unknown	btc.blockr.io	A	104.24.96.153	2019-02-13 07:01	2019-07-26 02:17	AS13335 cloudflare	United States
Unknown	btc.blockr.io	A	104.24.97.153	2019-02-13 07:01	2019-07-26 02:17	AS13335 cloudflare	United States
Unknown	btc.blockr.io	A	104.16.150.172	2016-12-28 01:39	2019-01-12 11:00	AS13335 cloudflare	United States
Unknown	btc.blockr.io	A	104.16.148.172	2016-12-28 01:39	2018-10-10 10:00	AS13335 cloudflare	United States
Unknown	btc.blockr.io	A	104.16.152.172	2016-12-28 01:39	2018-12-22 11:00	AS13335 cloudflare	United States

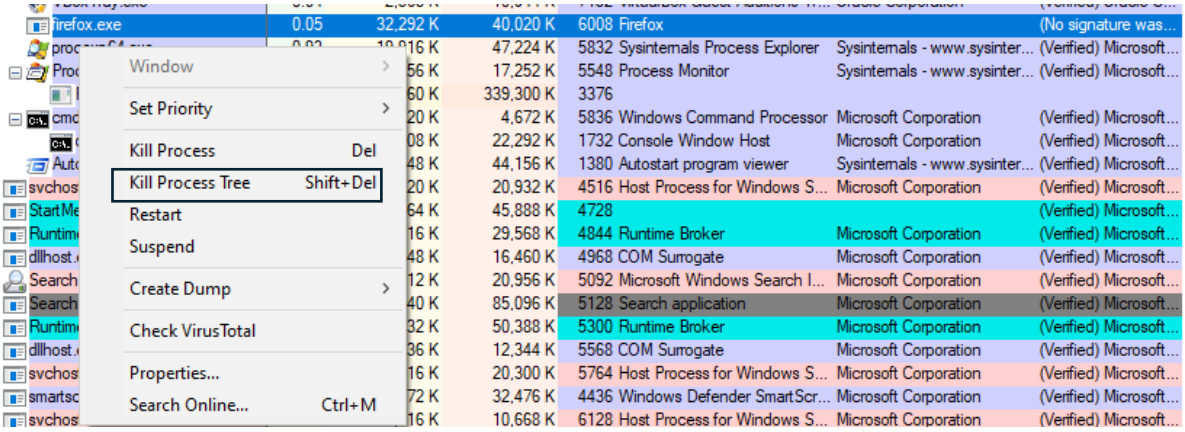
SHOWING 1 TO 10 OF 14 ENTRIES 1 2 NEXT >

- Terminate the malware permanently when done, and explain why it works.

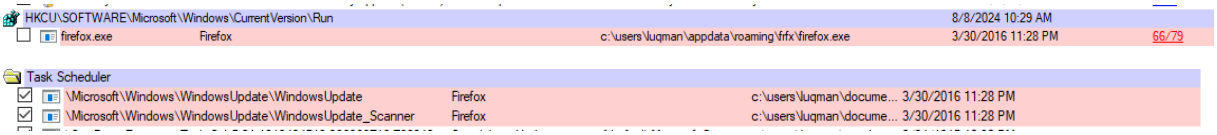
First I suspend malicious process in Process Explorer



Next I kill the process tree:



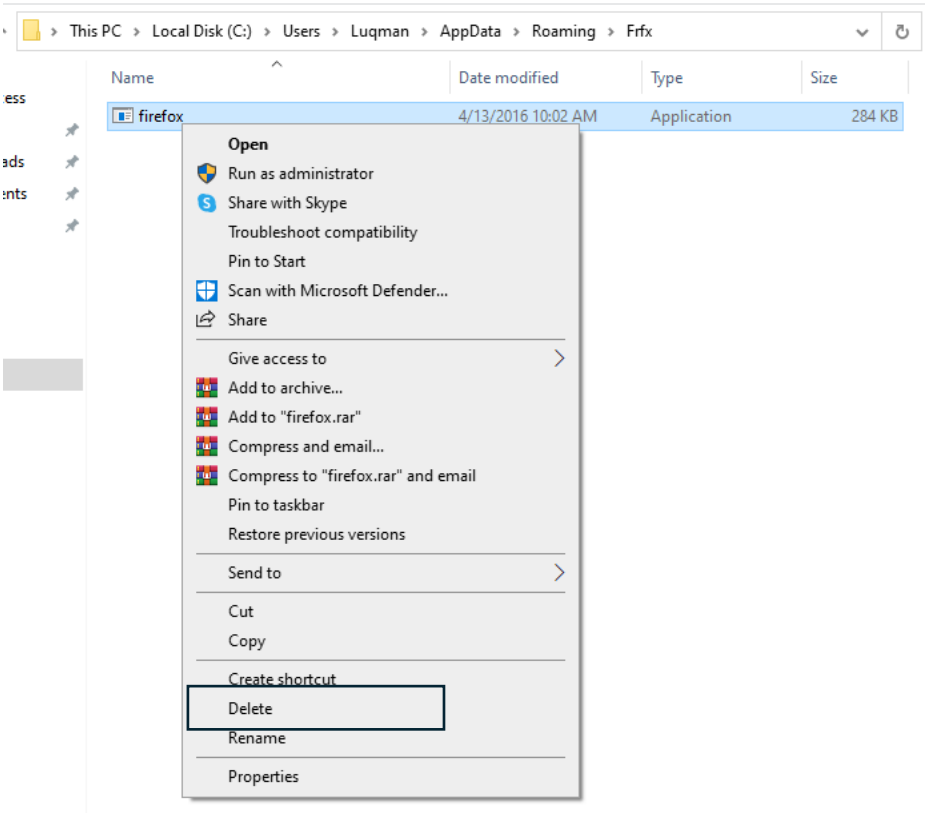
And then I unchecked processes in Autoruns for Firefox.exe and Windowsupdate_Scanner and WindowsUpdate.



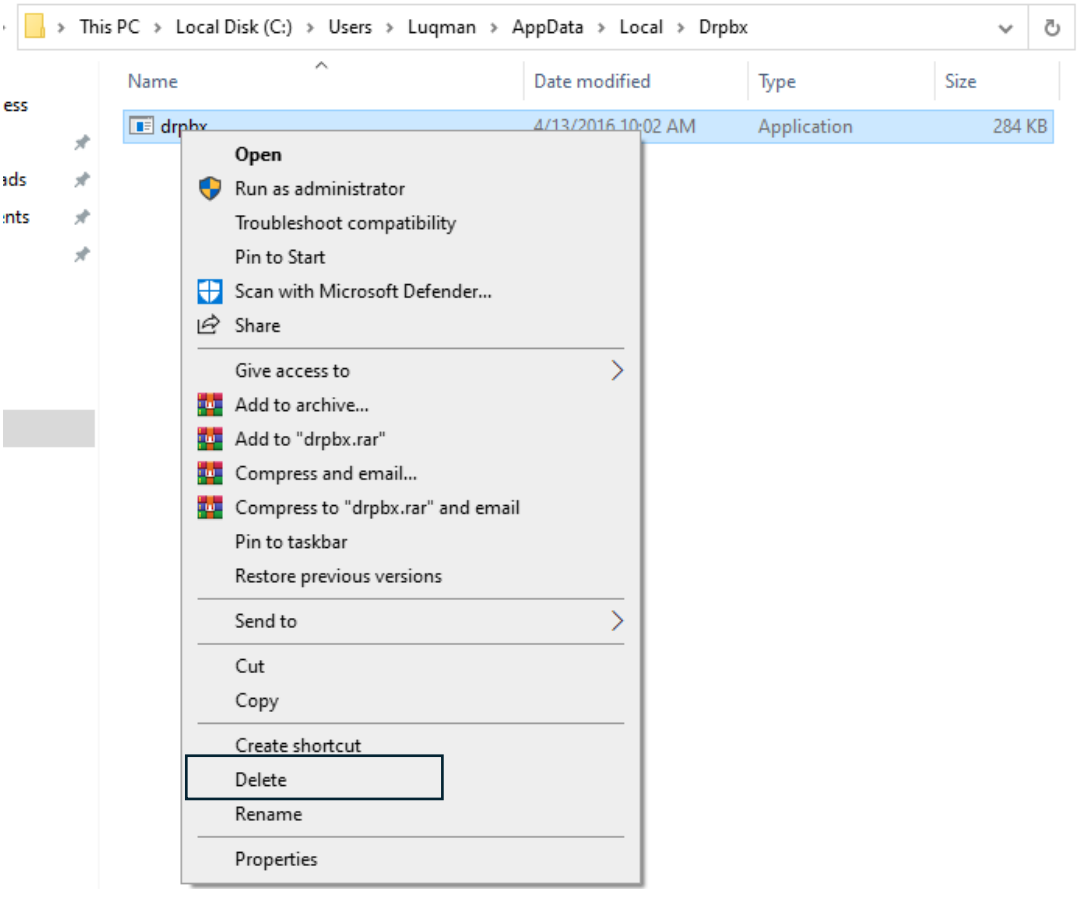
And then delete Firefox.exe from the HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and WindowsUpdate_Scanner and WindowsUpdate from Task Scheduler in the Autoruns.

Next I deleted all files from the mentioned previous directories.

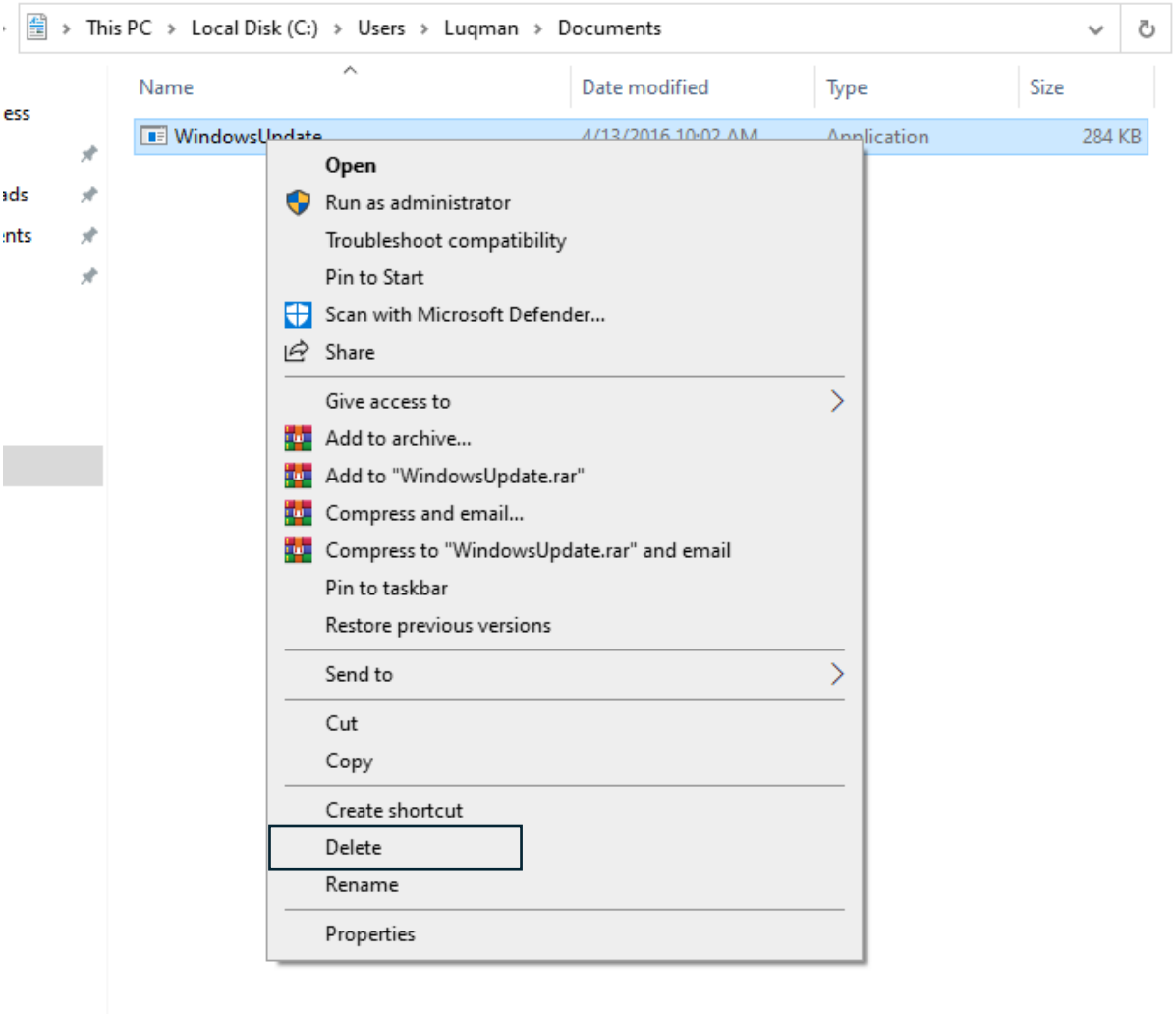
Firefox.exe



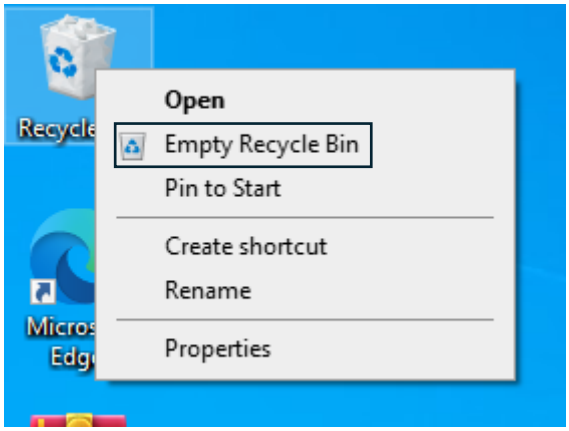
Drpbx.exe



WindowsUpdate.exe



Empty recycle bin



After reboot all malicious processes disappear! 😊

This malware was created for encrypt data on the disc and demand for a ransom. That's why we can categorize it as a ransomware. It runs automatically during the system booting process. It infects such a processes as windows update which is included in task scheduler and use such a files as firefox.exe, drpbx.exe windows update.exe which might not seems suspicious on the first

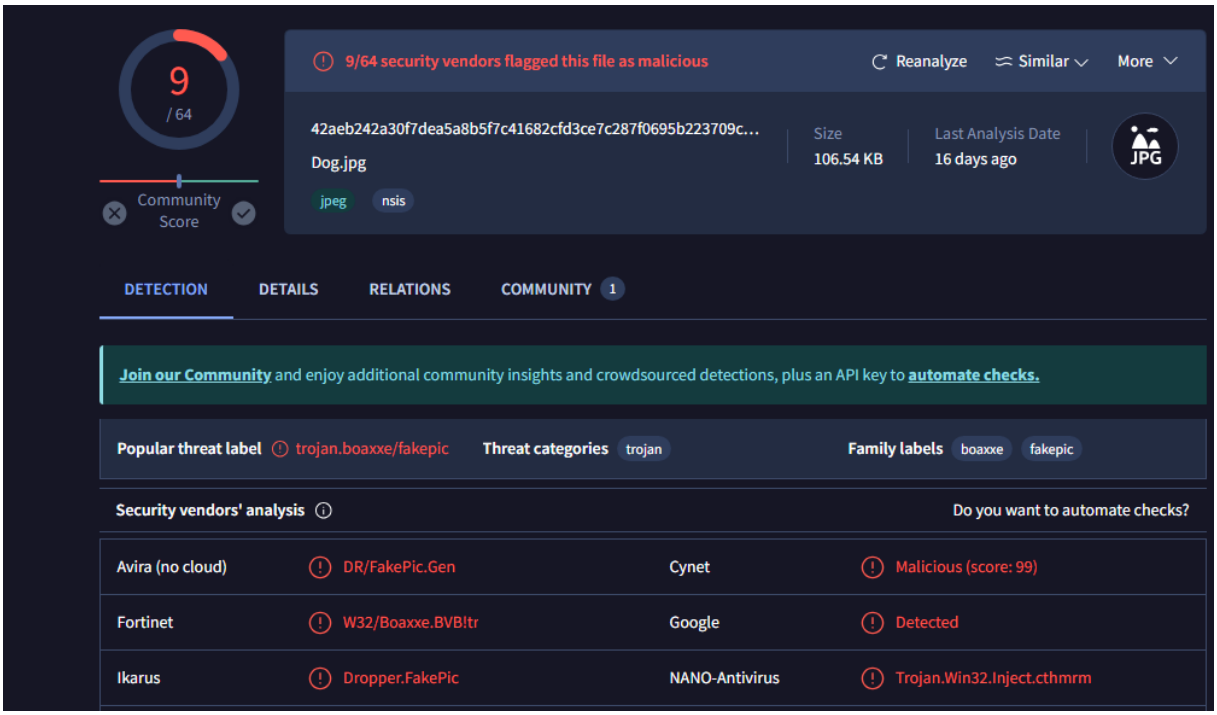
sight. We can also see in event viewer that settings of Windows Defender are changed and logs for Applications and Services for Internet Explorer are empty.

PART 2 - SIEM & SOC - Final Project

- Write at least two reasons that prove it is malware, only through static analysis.

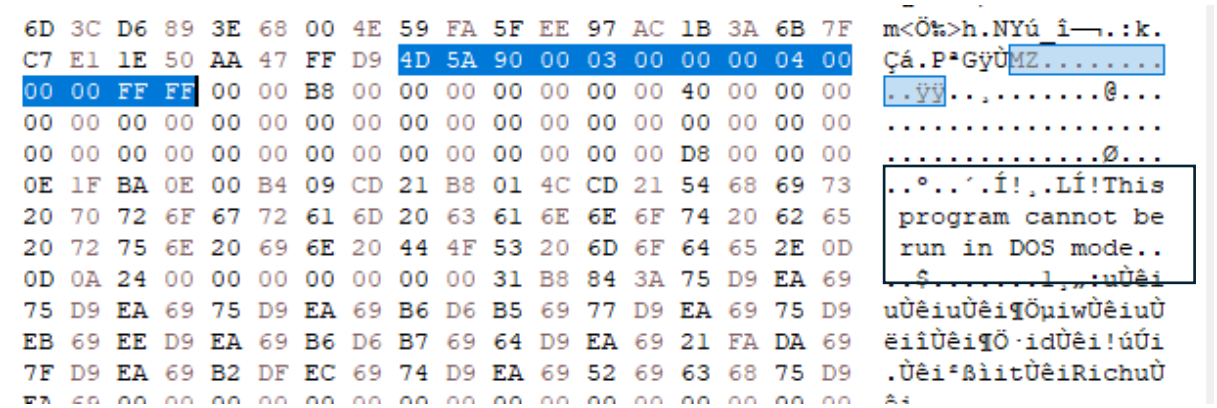
I have created a hash of dog.jpg file with certutil and check it on virus total:

```
C:\Users\Luqman\Desktop\SysinternalsSuite>certutil -hashfile C:\Users\Luqman\Desktop\Dog.jpg
SHA1 hash of C:\Users\Luqman\Desktop\Dog.jpg:
0c6bbb2054403daaba4fcdac316ff33e852ea411
CertUtil: -hashfile command completed successfully.
```



As we can see almost every vendor detected this file as a malicious.

Second thing is that we can find in raw data bytes that inform us about that file is executable.



According to website https://www.garykessler.net/library/file_sigs.html bytes which starts with 4D 5A are Windows/DOS executable files. What is more as we can see in the frame “This program cannot be run in DOS mode” that is another sign that it’s not usual jpg file.

I have also checked if that file is verified using a Sigcheck

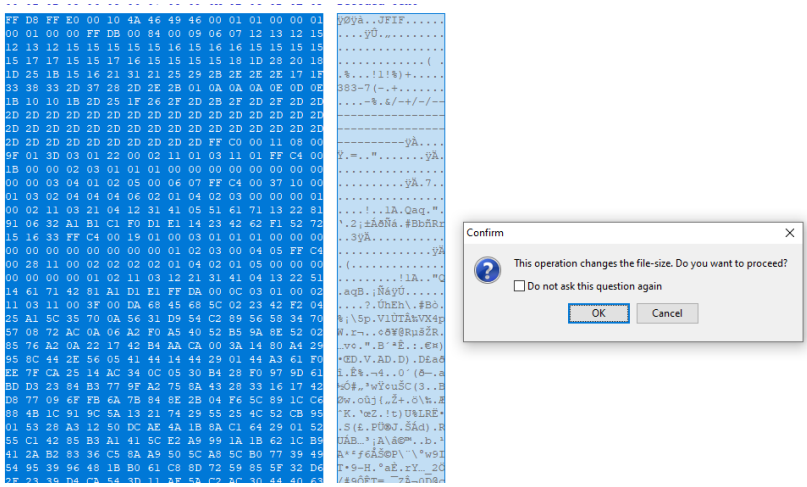
```
C:\Users\Luqman\Desktop\SysinternalsSuite>sigcheck -a -i -h C:\Users\Luqman\Desktop\Dog.jpg

Sigcheck v2.80 - File version and signature viewer
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\users\luqman\desktop\Dog.jpg:
        Verified:       Unsigned
        File date:      12:12 AM 12/20/2020
        Publisher:      n/a
        Company:        n/a
        Description:    n/a
        Product:        n/a
        Prod version:   n/a
        File version:   n/a
        MachineType:    n/a
        Binary Version: n/a
        Original Name:  n/a
        Internal Name:  n/a
        Copyright:      n/a
        Comments:       n/a
        Entropy:        7.715
        MD5:    79BF480968F4B4BE28A39FE3AFA4B0D7
        SHA1:   0C6BBB2054403DAABA4FCDAC316FF33E852EA411
        PESHA1: 0C6BBB2054403DAABA4FCDAC316FF33E852EA411
        PE256:  42AEB242A30F7DEA5A8B5F7C41682CFD3CE7C287F0695B223709C8A8F721532B
        SHA256: 42AEB242A30F7DEA5A8B5F7C41682CFD3CE7C287F0695B223709C8A8F721532B
        IMP:    n/a
```

- Mention at least one DLL that the program uses, which is not found.

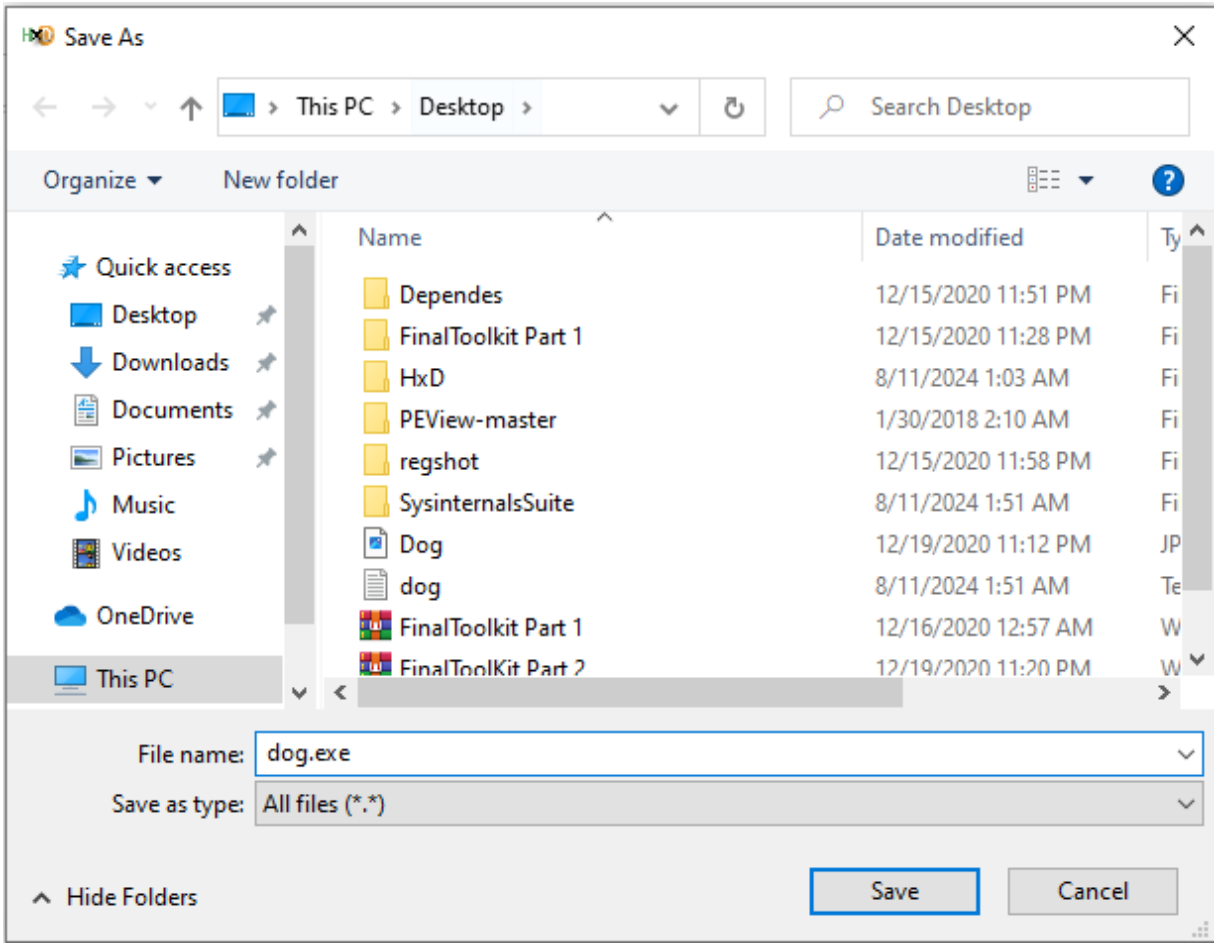
In the strings we can find few dlls as follows:

- Version.dll
- Ole32.dll
- COMCTL32.dll
- ADVAPI32.dll
- GDI32.dll
- USERS32.dll
- KERNEL32.dll
- SHELL32.dll

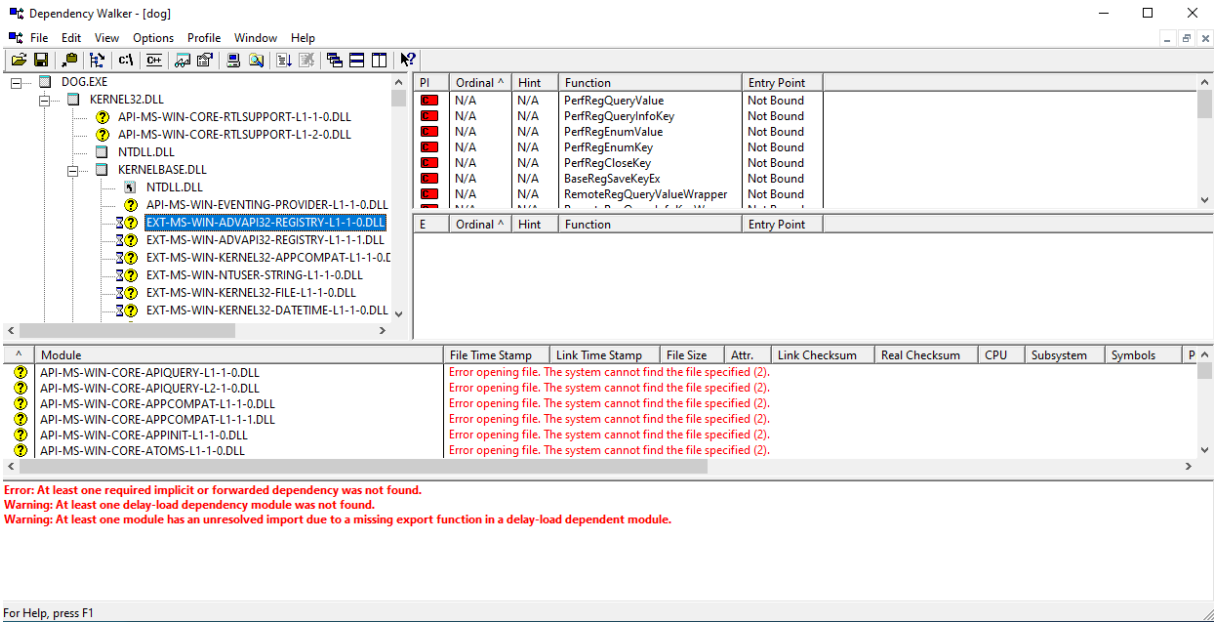
I have edited dog.jpg in Hex Editor to extract executable file from dog.jpg. I was searching for 4D 5A bytes and deleted all the bytes that are coming before that.



Now we have executable file and we can save it as with an .exe extension.



Then we can proceed with Dependency Walker Analysis:



According to the dlls that we have found in a strings here we also can find same dlls such as:

ADVAPI32.DLL, KERNEL32.DLL, SHELL32.dll