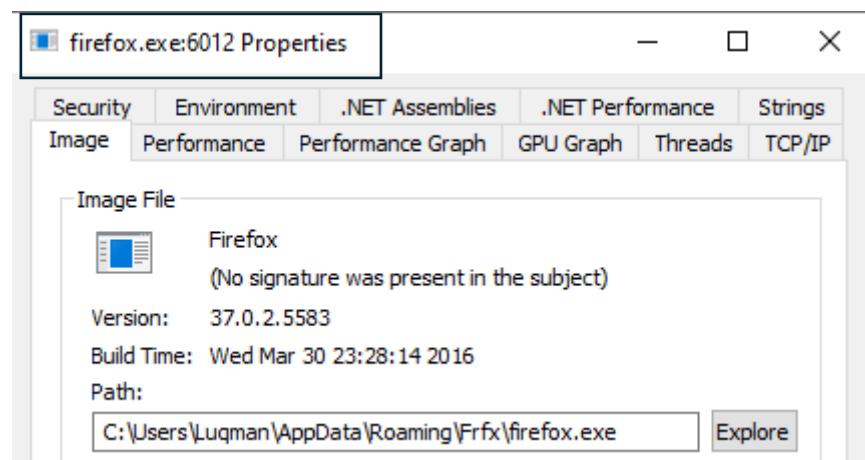
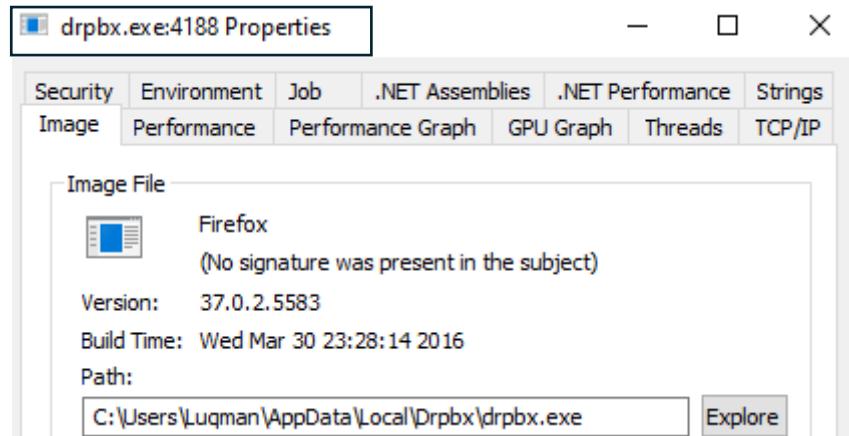


## PART 1 - SIEM & SOC - Final Project

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

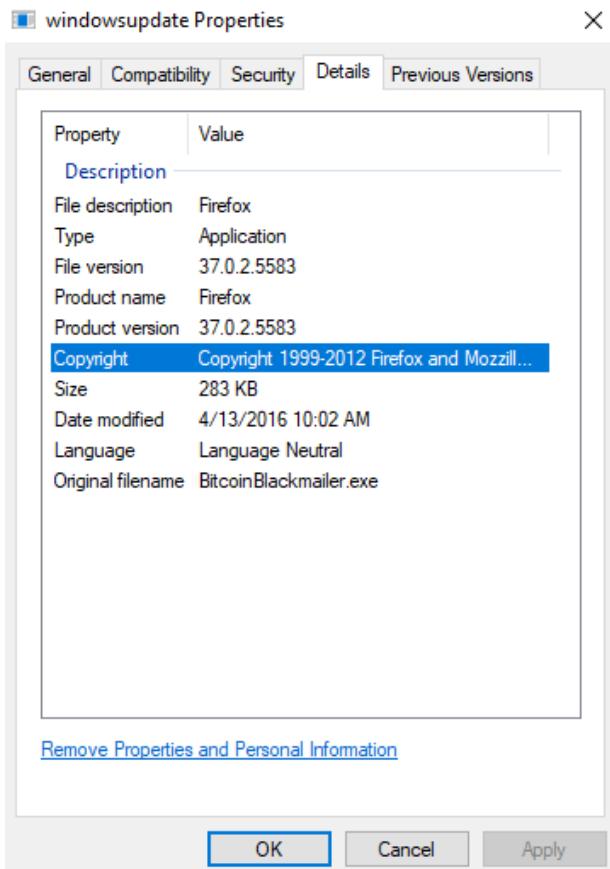
The name of the malicious processes is firefox.exe (PID 5712) and drpbx.exe (PID 5872 and 5880). There are no Windows signature for those two processes. They are not digitally signed.



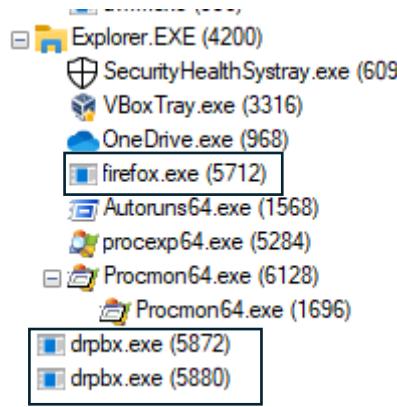
Those two processes runs automatically during the system boots. After killing that process firefox.exe in a task manager below window disappear 😊



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\FrFrx

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.

explorer.exe	0.13	39,324 K	121,088 K	4200 Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,632 K	9,344 K	6096 Windows Security notificatio...	Microsoft Corporation
VBoxTray.exe	< 0.01	2,392 K	10,912 K	3316 VirtualBox Guest Additions Tr...	Oracle Corporation
OneDrive.exe	0.02	14,184 K	46,788 K	968 Microsoft OneDrive	Microsoft Corporation
firefox.exe	0.07	33,948 K	42,884 K	5712 Firefox	
Autoruns64.exe		17,568 K	34,144 K	1568 Autostart program viewer	Sysinternals - www.sysinter...
Procmon64.exe		2,168 K	13,444 K	2820 Process Monitor	Sysinternals - www.sysinter...

- Add three strings that indicate that this is malware.

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

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
FrFrx\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  						
Passive DNS						
Show <input type="button" value="10"/> entries	STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN
						ASN
Unknown	btc.blockr.io		A	NXDOMAIN	2021-10-16 12:36	2024-06-22 08:44
Unknown	btc.blockr.io		A	91.21.71.36	2021-07-27 02:18	2021-09-08 11:34
Unknown	btc.blockr.io		A	62.90.150.224	2019-07-28 12:41	2019-08-13 09:29
Unknown	btc.blockr.io		AAAA	2606:4700:30::6818:6099	2019-06-10 07:27	2019-07-23 09:00
Unknown	btc.blockr.io		AAAA	2606:4700:30::6818:6199	2019-06-10 07:27	2019-07-23 09:00
Unknown	btc.blockr.io		A	104.24.96.153	2019-02-13 07:01	2019-07-26 02:17
Unknown	btc.blockr.io		A	104.24.97.153	2019-02-13 07:01	2019-07-26 02:17
Unknown	btc.blockr.io		A	104.16.150.172	2016-12-28 01:39	2019-01-12 11:00
Unknown	btc.blockr.io		A	104.16.148.172	2016-12-28 01:39	2018-10-10 10:00
Unknown	btc.blockr.io		A	104.16.152.172	2016-12-28 01:39	2018-12-22 11:00

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

VBoxTray.exe	0.01	2,396 K	10,960 K	/152 VirtualBox Guest Additions Tr...	Oracle Corporation	(Verified) Oracle C...
firefo...	0.01	32,292 K	40,020 K	6008 Firefox		(No signature was...
proc...	0.02	10,016 K	47,224 K	5832 Sysinternals Process Explorer	Sysinternals - www.sysinter...	(Verified) Microsoft...
cmd...	0.02	56 K	17,252 K	5548 Process Monitor	Sysinternals - www.sysinter...	(Verified) Microsoft...
c:\cmd...	0.02	44 K	329,148 K	3376		
Auto...	0.02	48 K	4,688 K	5836 Windows Command Processor	Microsoft Corporation	(Verified) Microsoft...
svchost...	0.02	40 K	22,308 K	1732 Console Window Host	Microsoft Corporation	(Verified) Microsoft...
StartMe...	0.02	48 K	44,148 K	1380 Autostart program viewer	Sysinternals - www.sysinter...	(Verified) Microsoft...
Runtim...	0.02	20 K	20,932 K	4516 Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
dllhost...	0.02	44 K	45,944 K	4728		
Search...	0.02	20 K	29,804 K	4844 Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
Search...	0.02	48 K	16,532 K	4968 COM Surrogate	Microsoft Corporation	(Verified) Microsoft...
Runtim...	0.02	60 K	20,856 K	5092 Microsoft Windows Search I...	Microsoft Corporation	(Verified) Microsoft...
dllhost...	0.02	40 K	85,096 K	5128 Search application	Microsoft Corporation	(Verified) Microsoft...
svchost...	0.02	00 K	50,404 K	5300 Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
smarts...	0.02	84 K	12,328 K	5568 COM Surrogate	Microsoft Corporation	(Verified) Microsoft...
svchost...	0.02	16 K	20,300 K	5764 Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost...	0.02	68 K	32,560 K	4436 Windows Defender SmartScr...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	0.02	16 K	10,732 K	6128 Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	0.02	4,324 K	10,732 K	6128 Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...

Next I kill the process tree:

firefo...	0.05	32,292 K	40,020 K	6008 Firefox		(No signature was...
proc...	0.02	10,016 K	47,224 K	5832 Sysinternals Process Explorer	Sysinternals - www.sysinter...	(Verified) Microsoft...
cmd...	0.02	56 K	17,252 K	5548 Process Monitor	Sysinternals - www.sysinter...	(Verified) Microsoft...
c:\cmd...	0.02	60 K	339,300 K	3376		
Auto...	0.02	20 K	4,672 K	5836 Windows Command Processor	Microsoft Corporation	(Verified) Microsoft...
svchost...	0.02	08 K	22,292 K	1732 Console Window Host	Microsoft Corporation	(Verified) Microsoft...
StartMe...	0.02	48 K	44,156 K	1380 Autostart program viewer	Sysinternals - www.sysinter...	(Verified) Microsoft...
Runtim...	0.02	20 K	20,932 K	4516 Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
dllhost...	0.02	64 K	45,888 K	4728		
Search...	0.02	16 K	29,568 K	4844 Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
Search...	0.02	48 K	16,460 K	4968 COM Surrogate	Microsoft Corporation	(Verified) Microsoft...
Runtim...	0.02	12 K	20,956 K	5092 Microsoft Windows Search I...	Microsoft Corporation	(Verified) Microsoft...
dllhost...	0.02	40 K	85,096 K	5128 Search application	Microsoft Corporation	(Verified) Microsoft...
svchost...	0.02	32 K	50,388 K	5300 Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
smarts...	0.02	36 K	12,344 K	5568 COM Surrogate	Microsoft Corporation	(Verified) Microsoft...
svchost...	0.02	16 K	20,300 K	5764 Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost...	0.02	72 K	32,476 K	4436 Windows Defender SmartScr...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	0.02	16 K	10,668 K	6128 Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...

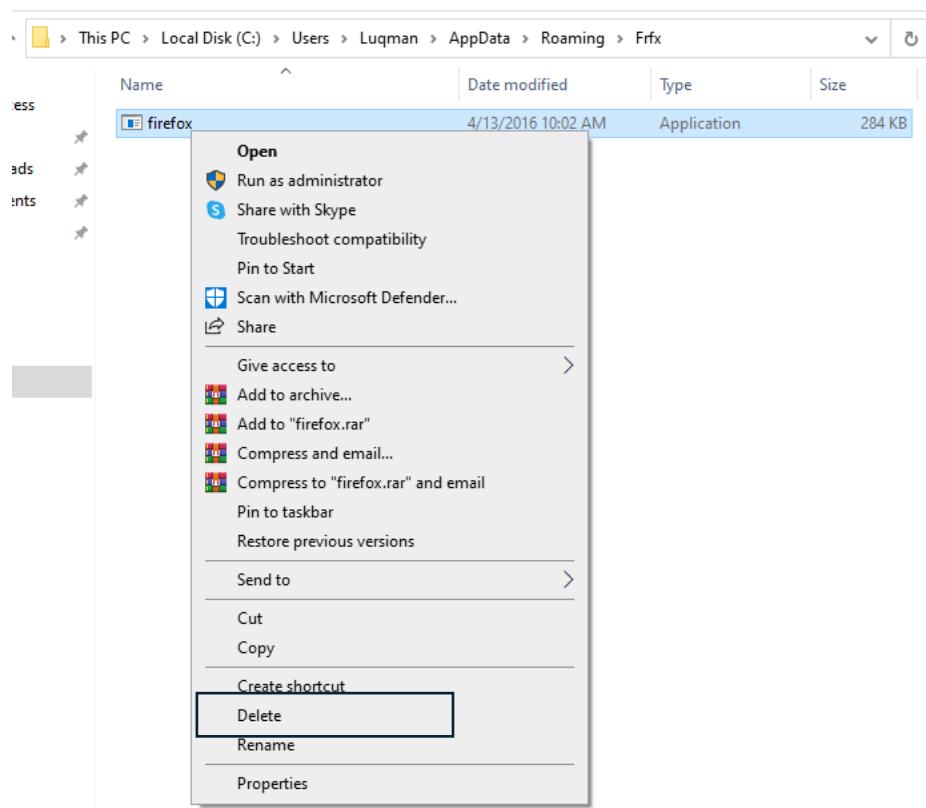
And then I unchecked processes in Autoruns for Firefox.exe and Windowsupdate\_Scanner and WindowsUpdate.

HCU\Software\Microsoft\Windows\CurrentVersion\Run	8/8/2024 10:29 AM
firefox.exe	Firefox
	c:\users\luqman\appdata\roaming\firfx\firefox.exe
	8/8/2024 10:29 AM
	3/30/2016 11:28 PM
	66/79
Task Scheduler	
<input checked="" type="checkbox"/> \Microsoft\Windows\WindowsUpdate\WindowsUpdate	Firefox
<input checked="" type="checkbox"/> \Microsoft\Windows\WindowsUpdate\WindowsUpdate_Scanner	Firefox
	c:\users\luqman\documents\3/30/2016 11:28 PM
	c:\users\luqman\documents\3/30/2016 11:28 PM

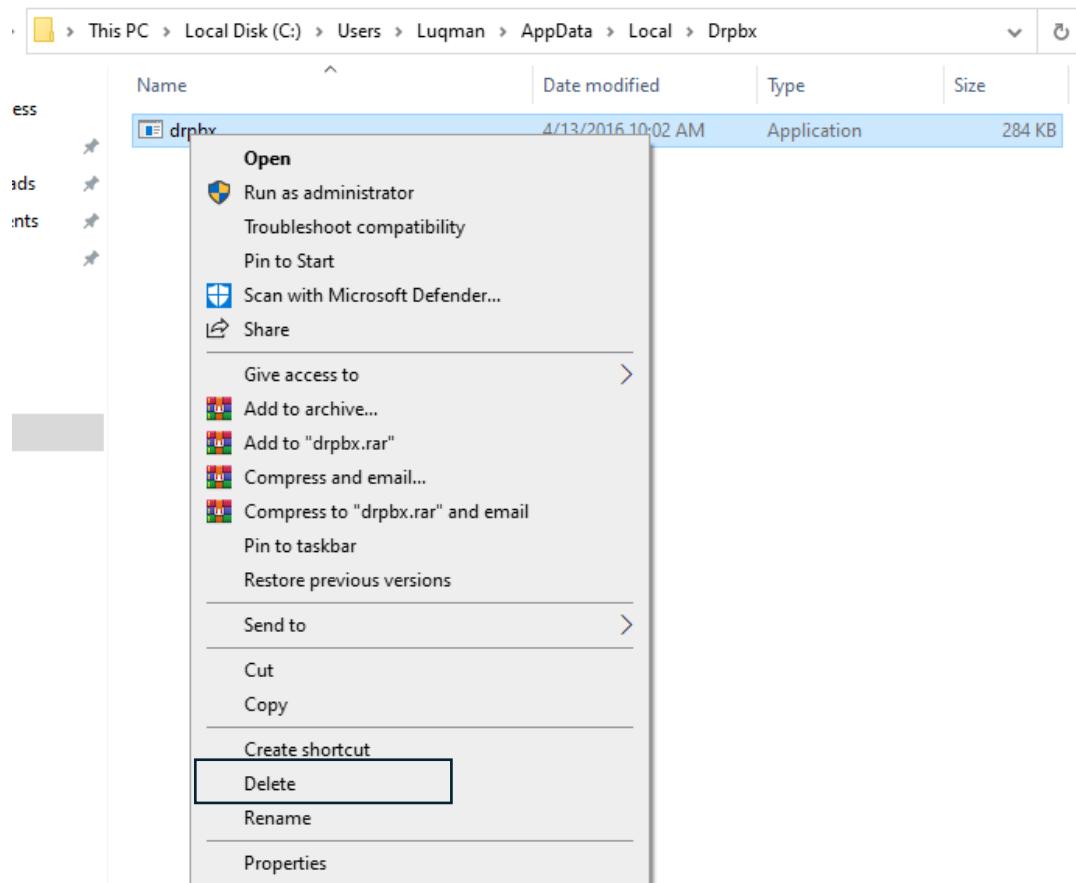
And then delete Firefox.exe from the HCU\Software\Microsoft\Windows\CurrentVersion\Run and WindowsUpdate\_Scanner and WindowsUpdate from Task Scheduler in the Autoruns.

Next I deleted all files from the mentioned previous directories.

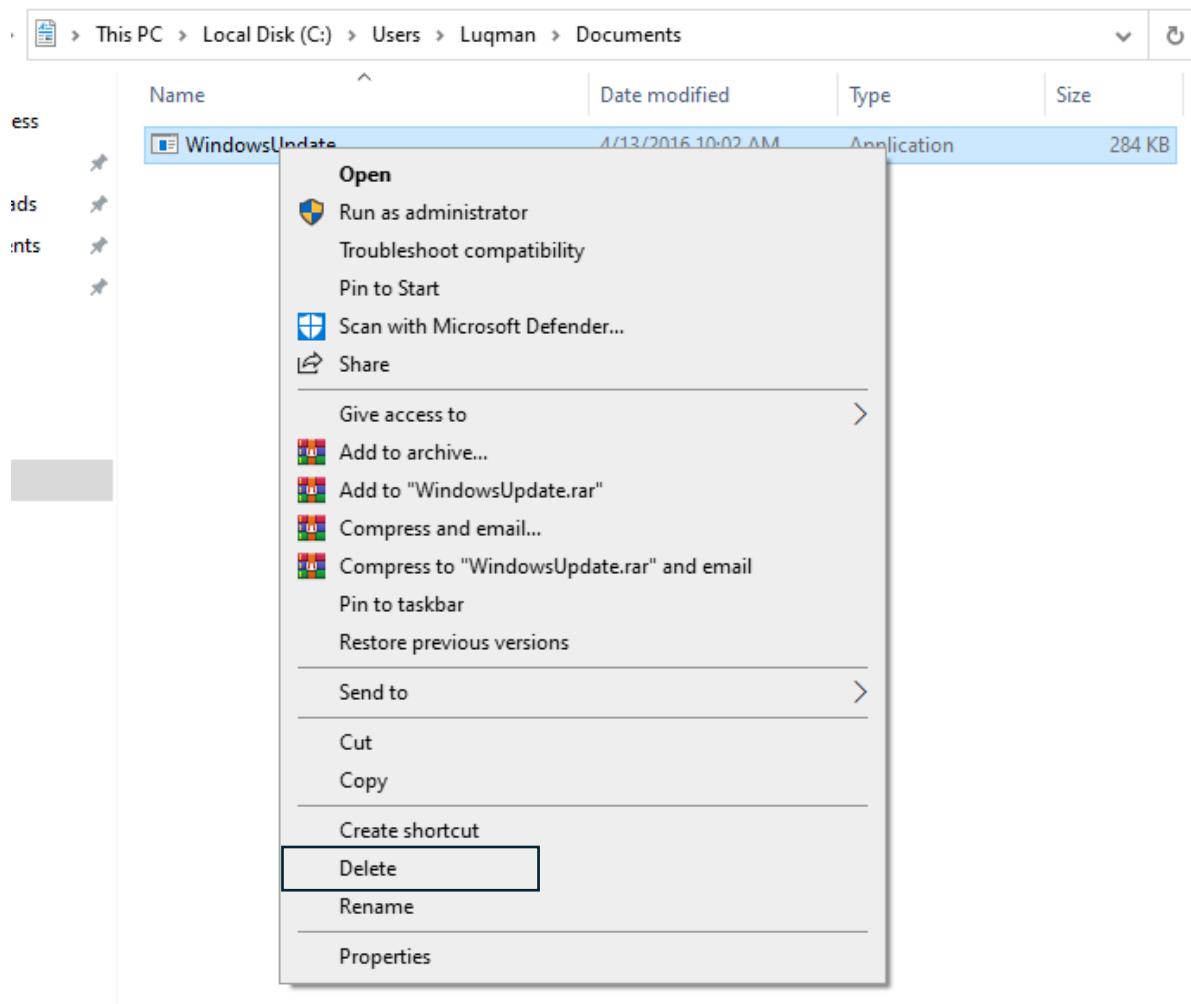
## Firefox.exe



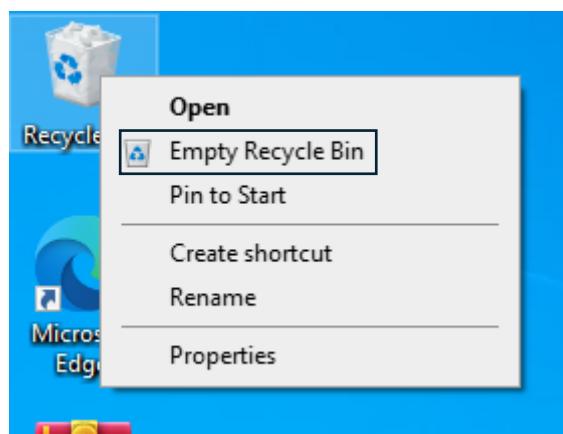
## Drpbx.exe



## 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.
```

The screenshot shows the VirusTotal analysis interface for a file named 'Dog.jpg'. The top bar indicates a 'Community Score' of 9 / 64. Below this, a summary box states '9/64 security vendors flagged this file as malicious'. The file details include the SHA1 hash: 42aeb242a30f7dea5a8b5f7c41682cf3ce7c287f0695b223709c..., a size of 106.54 KB, and a last analysis date of 16 days ago. The file is identified as a 'jpeg' file. A 'JPG' icon is present. Below the summary, tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY (1) are visible. A callout encourages joining the community. Under 'Popular threat label', 'trojan.boaxxe/fakepic' is listed. Threat categories include 'trojan'. Family labels include 'boaxxe' and 'fakepic'. The 'Security vendors' analysis' section lists findings from Avira, Fortinet, and Ikarus, all marking the file as malicious. A 'Do you want to automate checks?' button is shown. The right side of the interface displays the raw hex dump of the file's contents, starting with 6D 3C D6 89 3E 68 00 4E 59 FA 5F EE 97 AC 1B 3A 6B 7F and ending with a warning message: '...°..!..Lí!This program cannot be run in DOS mode..'. The entire dump is approximately 1000 bytes long.

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.

The screenshot shows a hex editor displaying the raw bytes of the 'Dog.jpg' file. The bytes are shown in pairs of hex values. A specific sequence of bytes, 4D 5A, is highlighted in blue. This sequence is known as the DOS executable signature, which typically starts with the ASCII characters 'MZ'. To the right of the hex dump, there is a vertical column of text in a non-Latin script, likely Cyrillic, which includes the string 'This program cannot be run in DOS mode..'. This text is enclosed in a rectangular box, indicating it is a part of the file's data.

According to website [https://www.garykessler.net/library/file\\_sigs.html](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

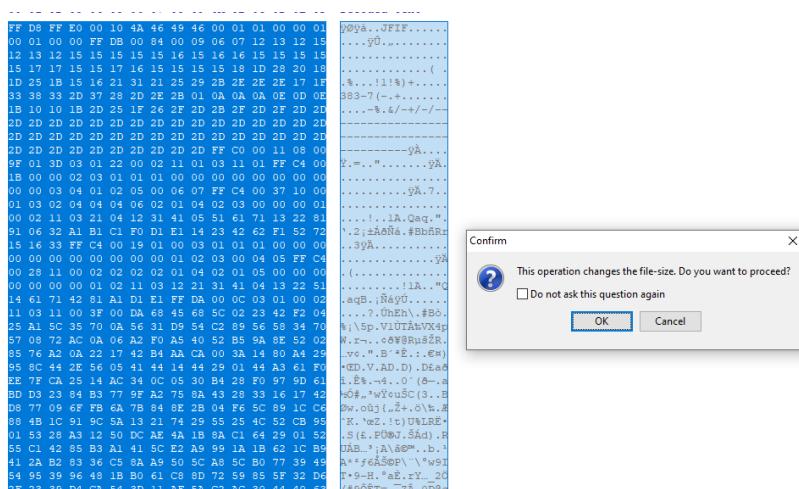
c:\users\luqman\desktop\Dog.jpg:
    Verified: Unsigned
    File date: 12:12 AM 12/20/2020
    Publisher: n/a
    Company: n/a
    Description: n/a
    Product: n/a
    Prod version: n/a
    File version: n/a
    MachineType: n/a
    Binary Version: n/a
    Original Name: n/a
    Internal Name: n/a
    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.

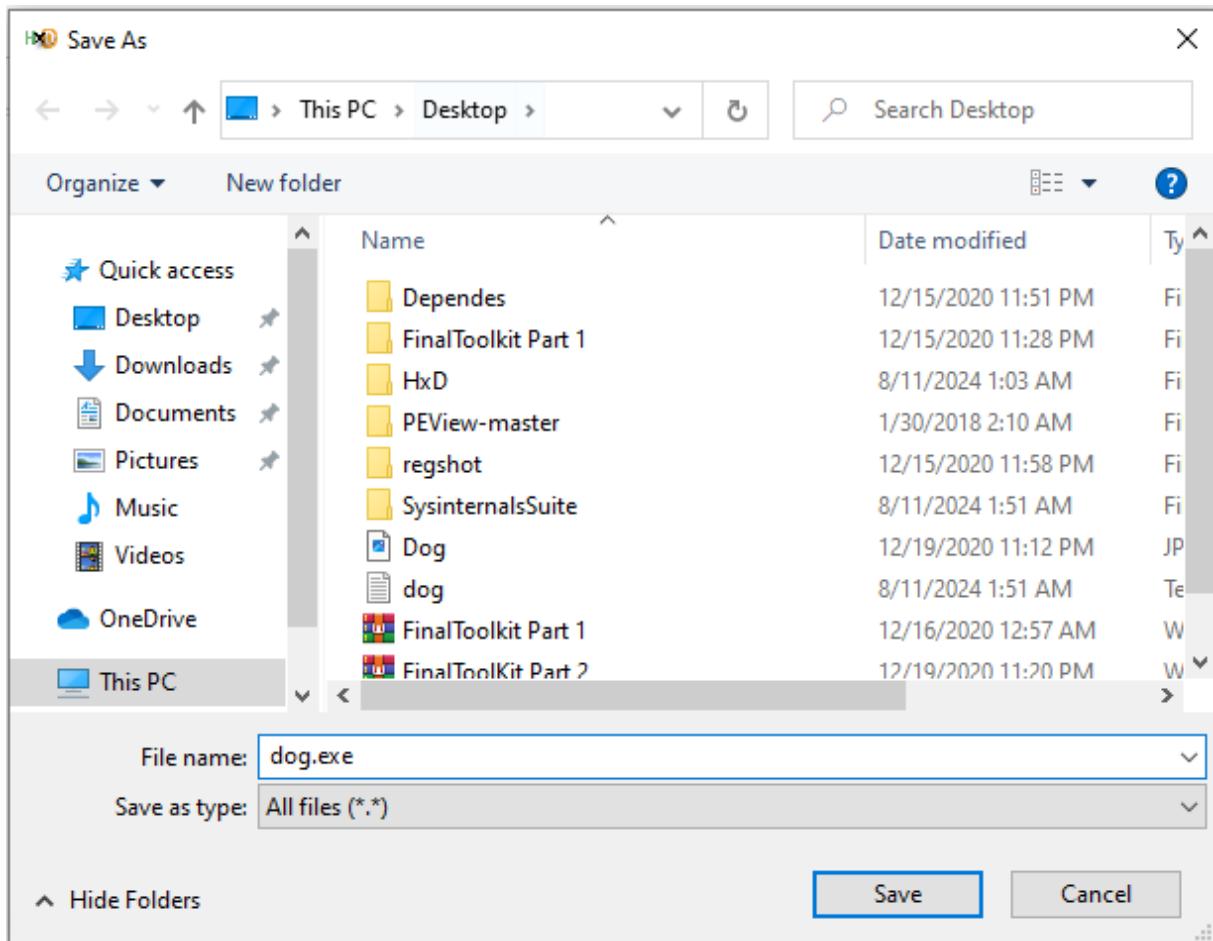
In the strings we can find few dlls as follows:

- 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:

The screenshot shows the Dependency Walker application window. The main pane displays the dependency tree for the 'DOG.EXE' file. Under 'DOG.EXE', there are entries for 'KERNEL32.DLL', 'NTDLL.DLL', and 'KERNELBASE.DLL'. The 'KERNEL32.DLL' entry shows imports from 'API-MS-WIN-CORE-RTLSUPPORT-L1-1.0.DLL', 'EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1.0.DLL', 'EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1.DLL', 'EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1.0.DLL', 'EXT-MS-WIN-NTUSER-STRING-L1-1.0.DLL', 'EXT-MS-WIN-KERNEL32-FILE-L1-1.0.DLL', and 'EXT-MS-WIN-KERNEL32-DATETIME-L1-1.0.DLL'. The 'NTDLL.DLL' and 'KERNELBASE.DLL' entries also show imports from various system DLLs. Below the dependency tree, a table lists the imported functions with their ordinal, hint, function name, and entry point. At the bottom of the application window, there is a table of modules with their file time stamp, link time stamp, file size, attributes, link checksum, real checksum, CPU, subsystem, and symbols. Error messages are displayed at the bottom of the application window, indicating that some required implicit or forwarded dependencies were not found.

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