

## SIEM & SOC FINAL PROJECT

### Part 1

#### Project Overview:

#### Lab Task

An end-user in an organization felt that his computer became slower after the last Windows update. As time passed, he noticed that the internet connection became slower as well and that files took time to load. He suspects that malware was installed in his machine.

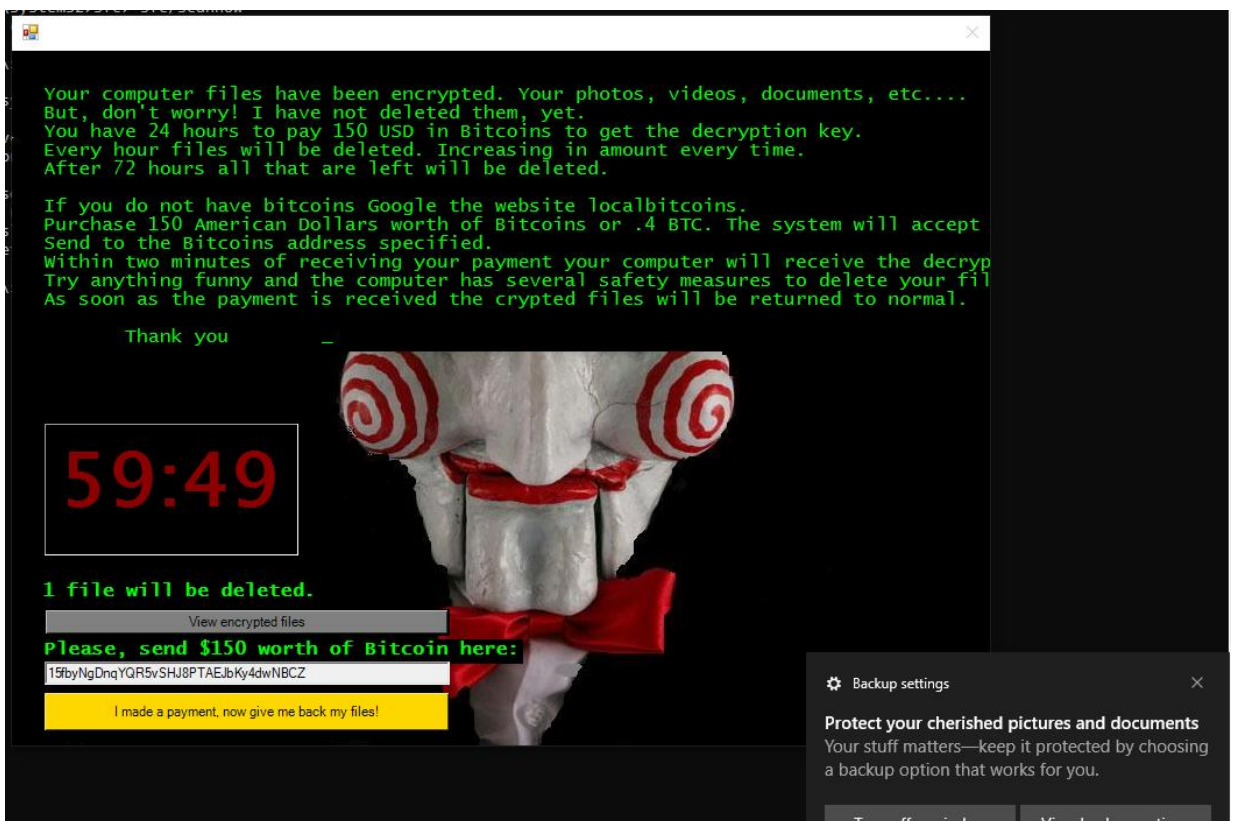
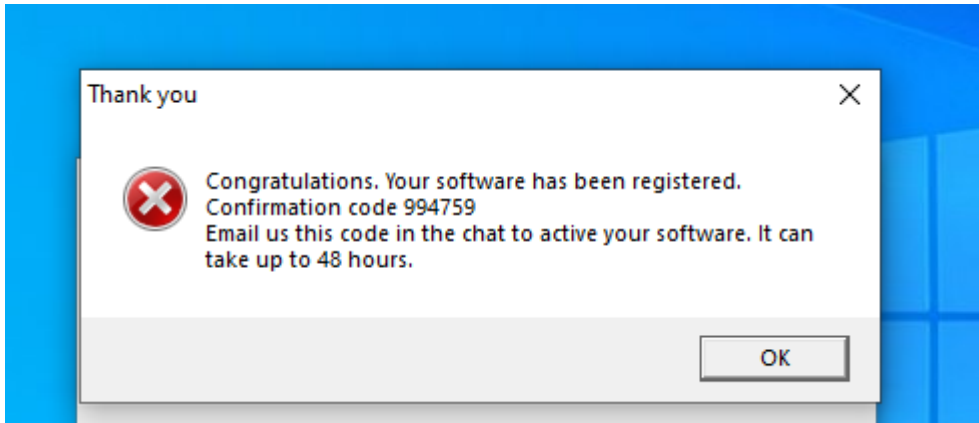
Investigate the environment and write a report that includes the guidelines below. Terminate the malware after the report is complete.

The following are guidelines for writing the report. Don't forget to take screenshots.

- Mention the names of the malicious processes, and provide explanations that point out why they are malicious.
- Specify the directory of the infected process.
- List files that are infected.
- Prove that the malicious process and the "Welcome" screen are the same.
- Add three strings that indicate that this is malware.
- Find the associated website and IP of the malware.
- Terminate the malware permanently when done, and explain why it works.

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

When we turn on the machine and Windows has been loaded, after a few minutes we have a very unpleasant surprise, two pop-ups are visible on the screen:



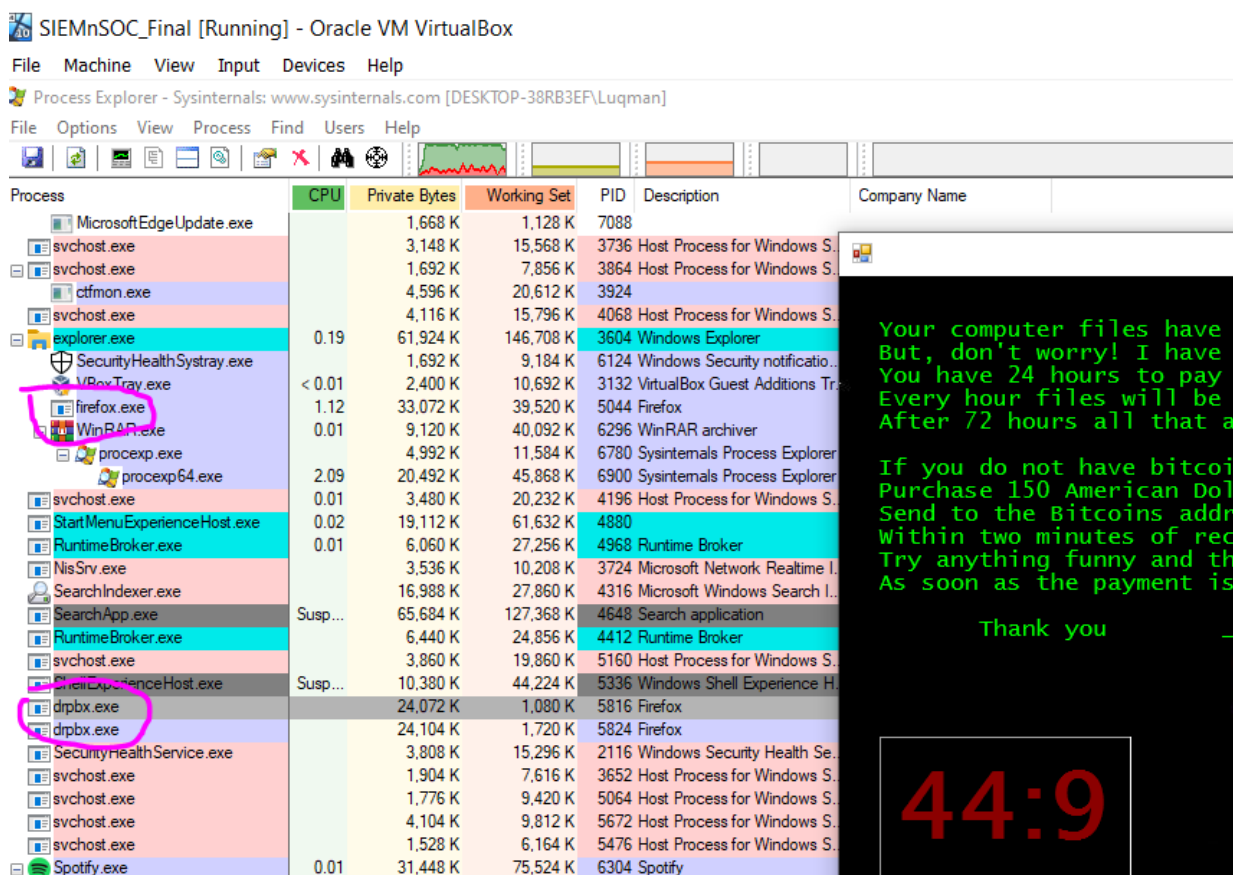
We're dealing with malware here, precisely ransomware, known as **Jigsaw Ransomware** or **BitcoinBlackmailer.exe**.

This malicious software encrypts files and demand to pay ransom worth 150\$ in bitcoins to pass decryption key. If victim didn't pay the ransom on time, Jigsaw deletes files after files every one hour.

BitcoinBlackmailer.exe is distributed via spam emails with malicious attachments, porn sites and part of potentially unwanted program. As we can see in further part of the report, it pretends to be other processes: Firefox and Dropbox.

## 2. Specify the directory of the infected process

How we can find the directory of the infected process? Using Process Explorer. First point malicious process, then check for details and find out path of directory



SIEMnSOC\_Final [Running] - Oracle VM VirtualBox

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38RB3EF\Luqman]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
MicrosoftEdgeUpdate.exe		1,668 K	1,128 K	7088		
svchost.exe		3,148 K	15,568 K	3736	Host Process for Windows S...	
svchost.exe		1,692 K	7,856 K	3864	Host Process for Windows S...	
ctfmon.exe		4,596 K	20,612 K	3924		
svchost.exe		4,116 K	15,796 K	4068	Host Process for Windows S...	
explorer.exe	0.19	61,924 K	146,708 K	3604	Windows Explorer	
SecurityHealthSystray.exe		1,692 K	9,184 K	6124	Windows Security notificatio...	
VBTray.exe	< 0.01	2,400 K	10,692 K	3132	VirtualBox Guest Additions Tr...	
firefox.exe	1.12	33,072 K	39,520 K	5044	Firefox	
WinRAR.exe	0.01	9,120 K	40,092 K	6296	WinRAR archiver	
procexp.exe		4,992 K	11,584 K	6780	Sysinternals Process Explorer	
procexp64.exe	2.09	20,492 K	45,868 K	6900	Sysinternals Process Explorer	
svchost.exe	0.01	3,480 K	20,232 K	4196	Host Process for Windows S...	
StartMenuExperienceHost.exe	0.02	19,112 K	61,632 K	4880		
RuntimeBroker.exe	0.01	6,060 K	27,256 K	4968	Runtime Broker	
NisSrv.exe		3,536 K	10,208 K	3724	Microsoft Network Realtime I...	
SearchIndexer.exe		16,988 K	27,860 K	4316	Microsoft Windows Search I...	
SearchApp.exe	Susp...	65,684 K	127,368 K	4648	Search application	
RuntimeBroker.exe		6,440 K	24,856 K	4412	Runtime Broker	
svchost.exe		3,860 K	19,860 K	5160	Host Process for Windows S...	
StartMenuExperienceHost.exe	Susp...	10,380 K	44,224 K	5336	Windows Shell Experience H...	
dropbox.exe		24,072 K	1,080 K	5816	Firefox	
dropbox.exe		24,104 K	1,720 K	5824	Firefox	
SecurityHealthService.exe		3,808 K	15,296 K	2116	Windows Security Health Se...	
svchost.exe		1,904 K	7,616 K	3652	Host Process for Windows S...	
svchost.exe		1,776 K	9,420 K	5064	Host Process for Windows S...	
svchost.exe		4,104 K	9,812 K	5672	Host Process for Windows S...	
svchost.exe		1,528 K	6,164 K	5476	Host Process for Windows S...	
Spotify.exe	0.01	31,448 K	75,524 K	6304	Spotify	

Your computer files have  
But, don't worry! I have  
You have 24 hours to pay  
Every hour files will be  
After 72 hours all that a

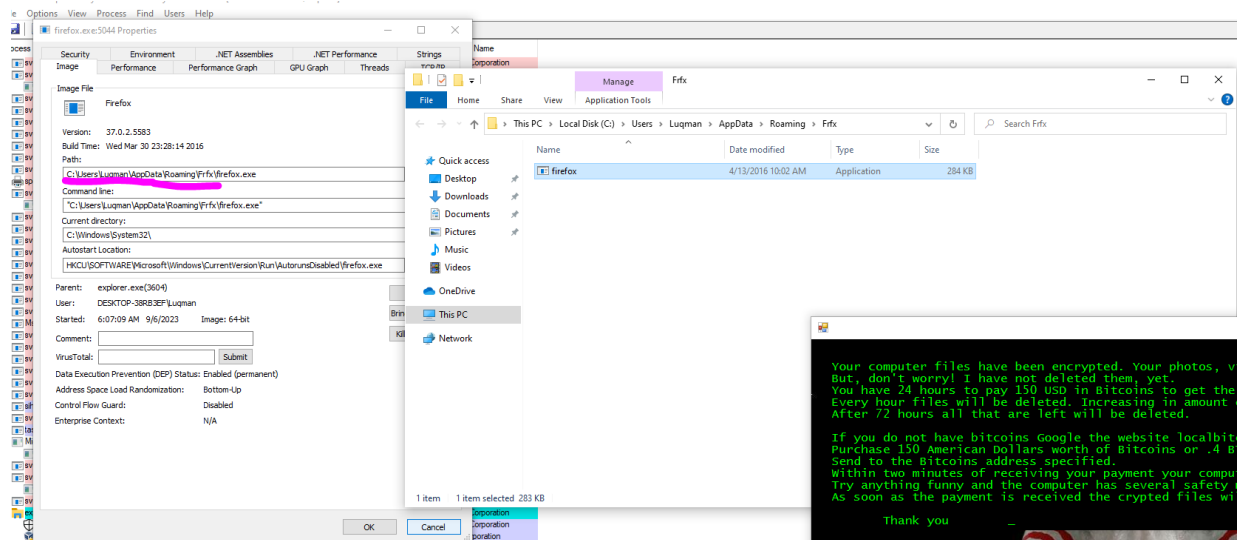
If you do not have bitcoi  
Purchase 150 American Dol  
Send to the Bitcoins addr  
Within two minutes of rec  
Try anything funny and th  
As soon as the payment is

Thank you

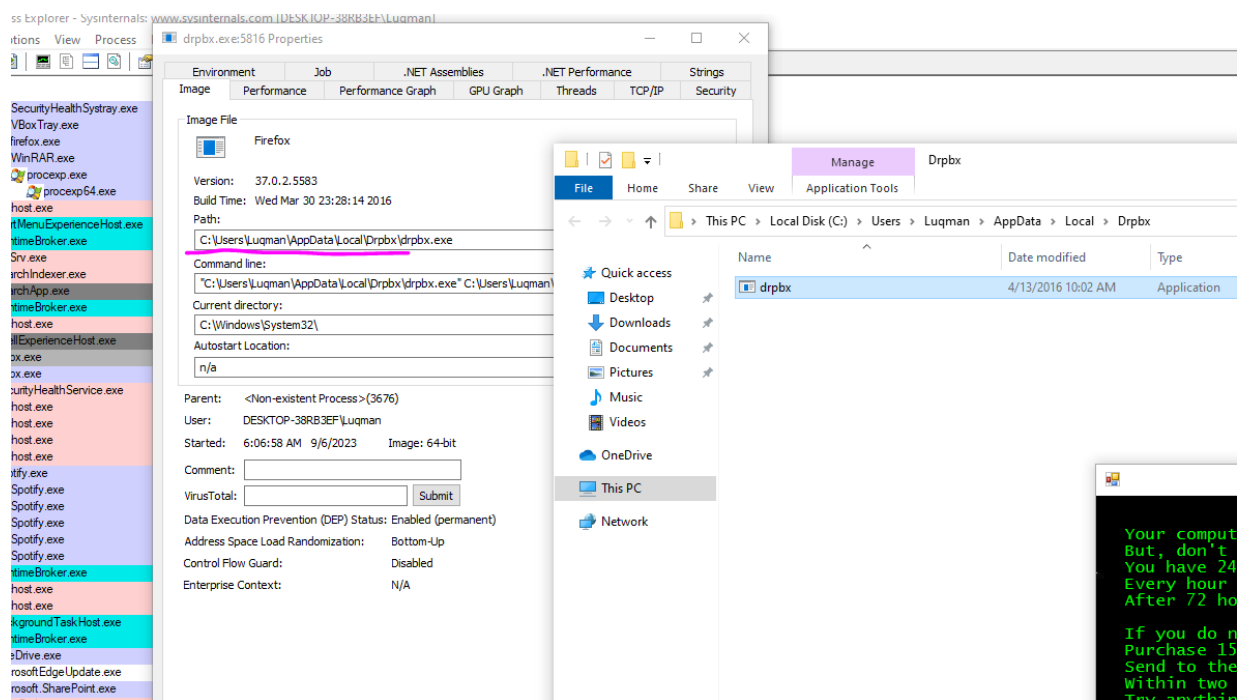
44:9

Infected directory is C:\Users\Luqman\AppData, more precisely:

## a) C:\Users\Luqman\AppData\Roaming\Frfox

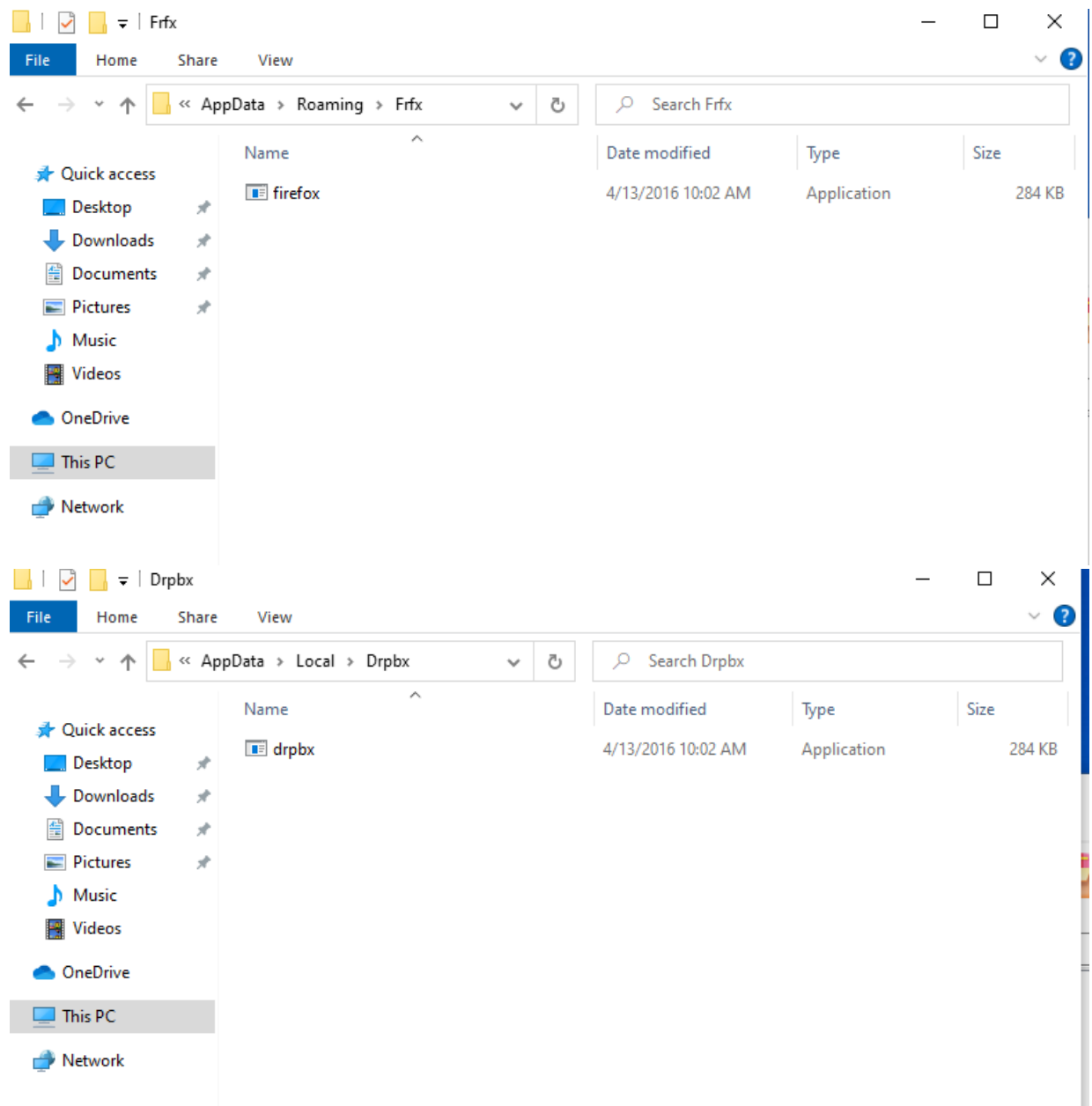


## b) C:\Users\Luqman\AppData\Local\Drpbx



## 3. List files that are infected

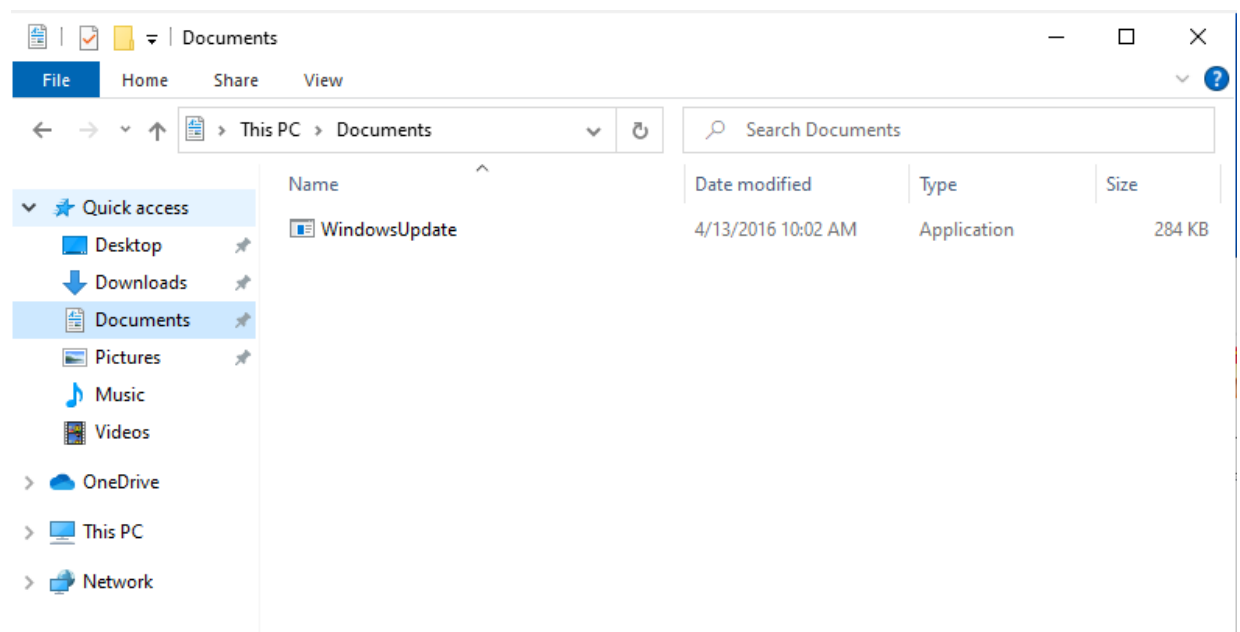
If we find directory, we can find infected files. As we can see on the screen below, we've got infected files: Firefox.exe and drpbx.exe. The path was given in the screenshots in the permanent in the previous point



The rest of the report will mention one more infected file, but at this stage of my analysis it has not been visible yet. It's WindowsUpdate – in:

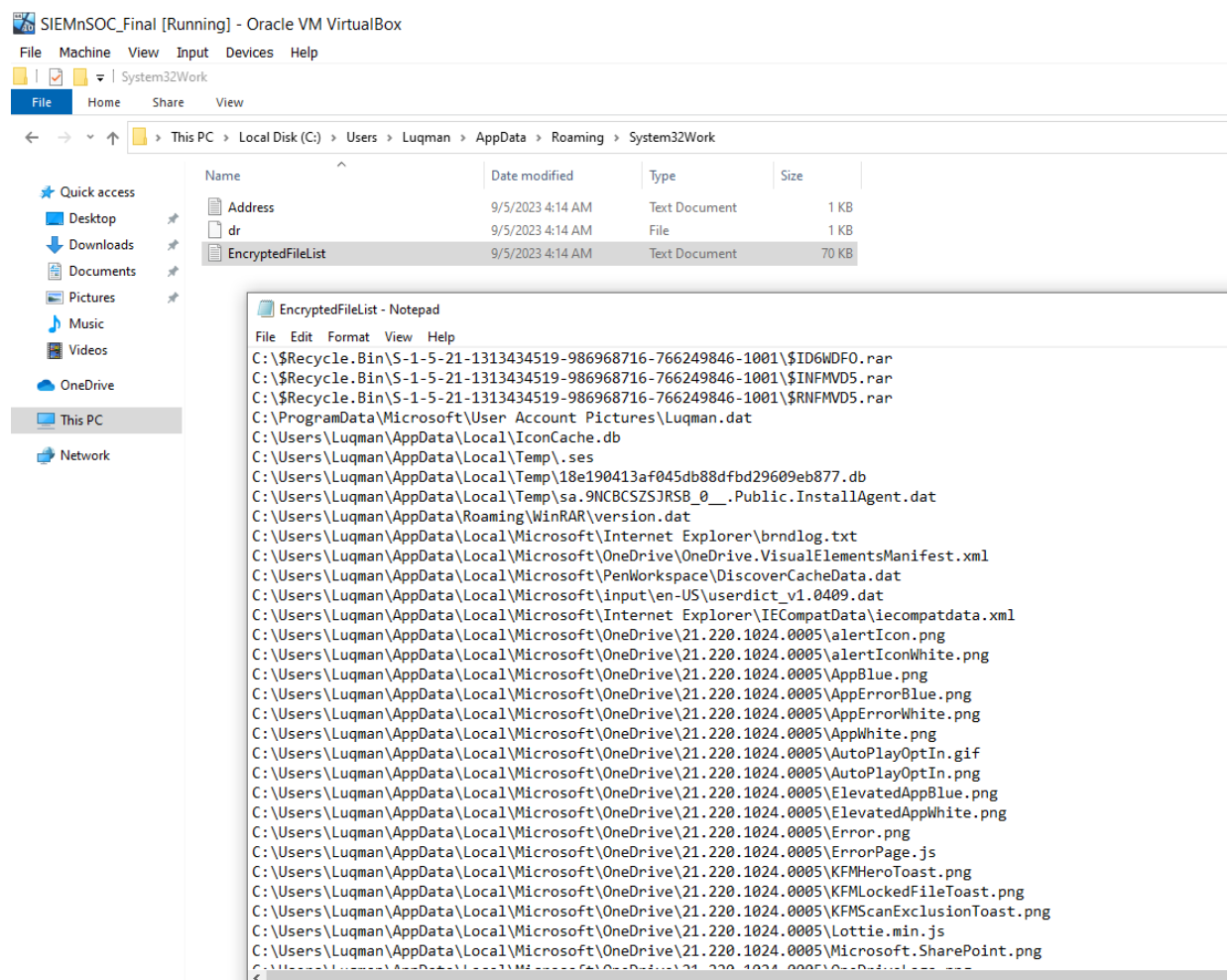
C:\Users\Luqman\Documents\WindowsUpdate.exe

I described how to find it in point 7.



And as extra screen:

if we would like to know which files were affected and encrypted by the virus, their list can be found here:

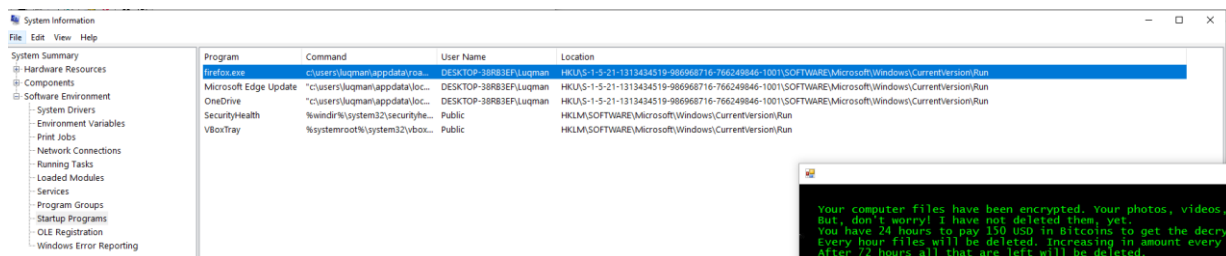


#### 4. Prove that the malicious process and the “Welcome” screen are the same

Answer depends on what you understand as “Welcome screen”. Two answers can be given here:

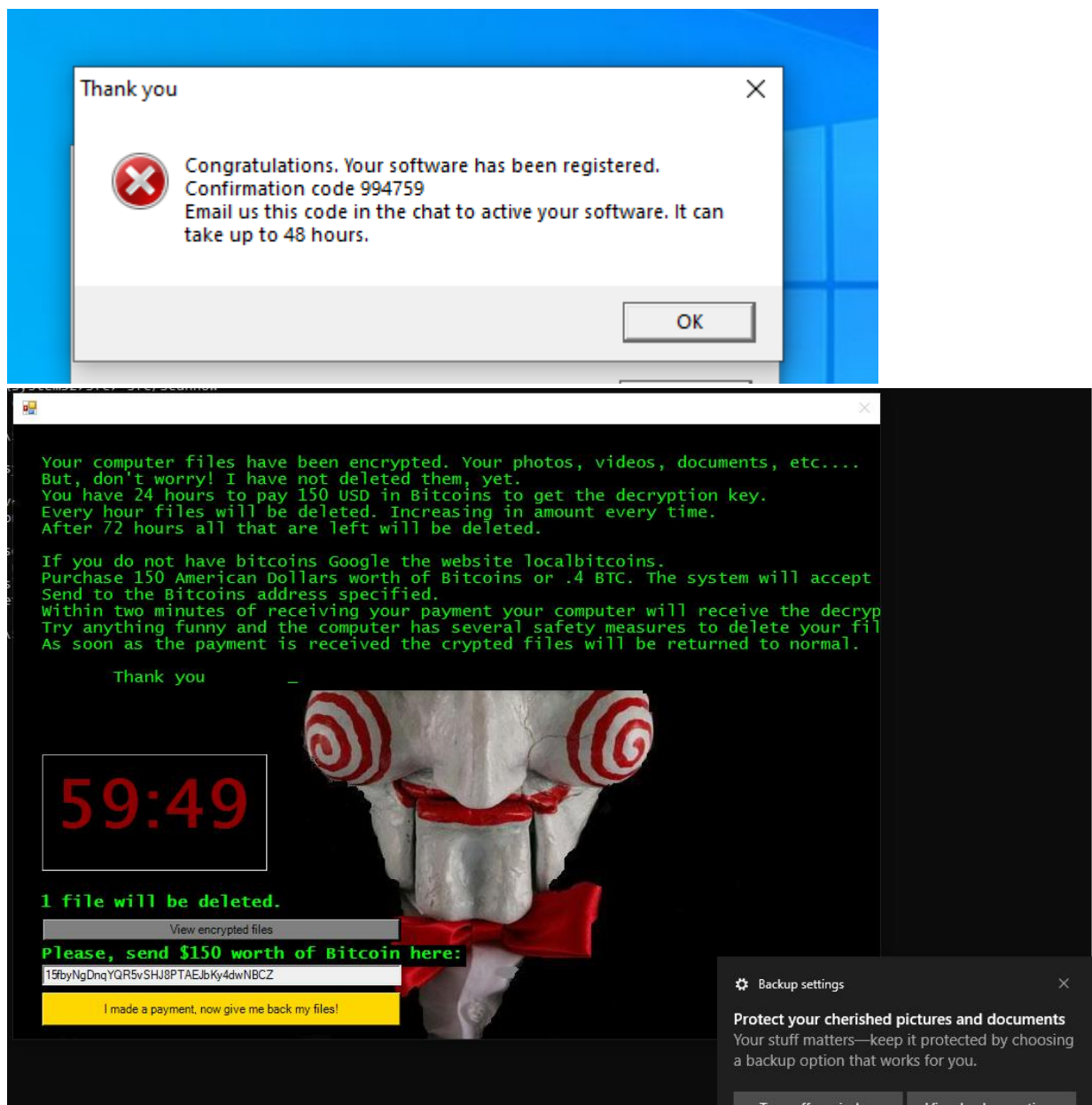
1) What is a “Welcome screen”? It’s an introduction page as program or computer is loading or booting. When Microsoft Window computer is loading, there is a Window welcome screen displayed. It includes logo, company name etc. In simple words: it’s screen with a nice picture you can look at, when all complicated processes go on behind the scene to ensure machine works properly and the necessary software can be loaded. When booting, the computer performs tasks, mostly in the background. Among them are additional software programs configured to start with the operating system, known as startup programs.

Startup Programs can be checked via msconfig. And here we go: our Firefox.exe is there! It means, that it’s activated when computer displays Welcome screen.



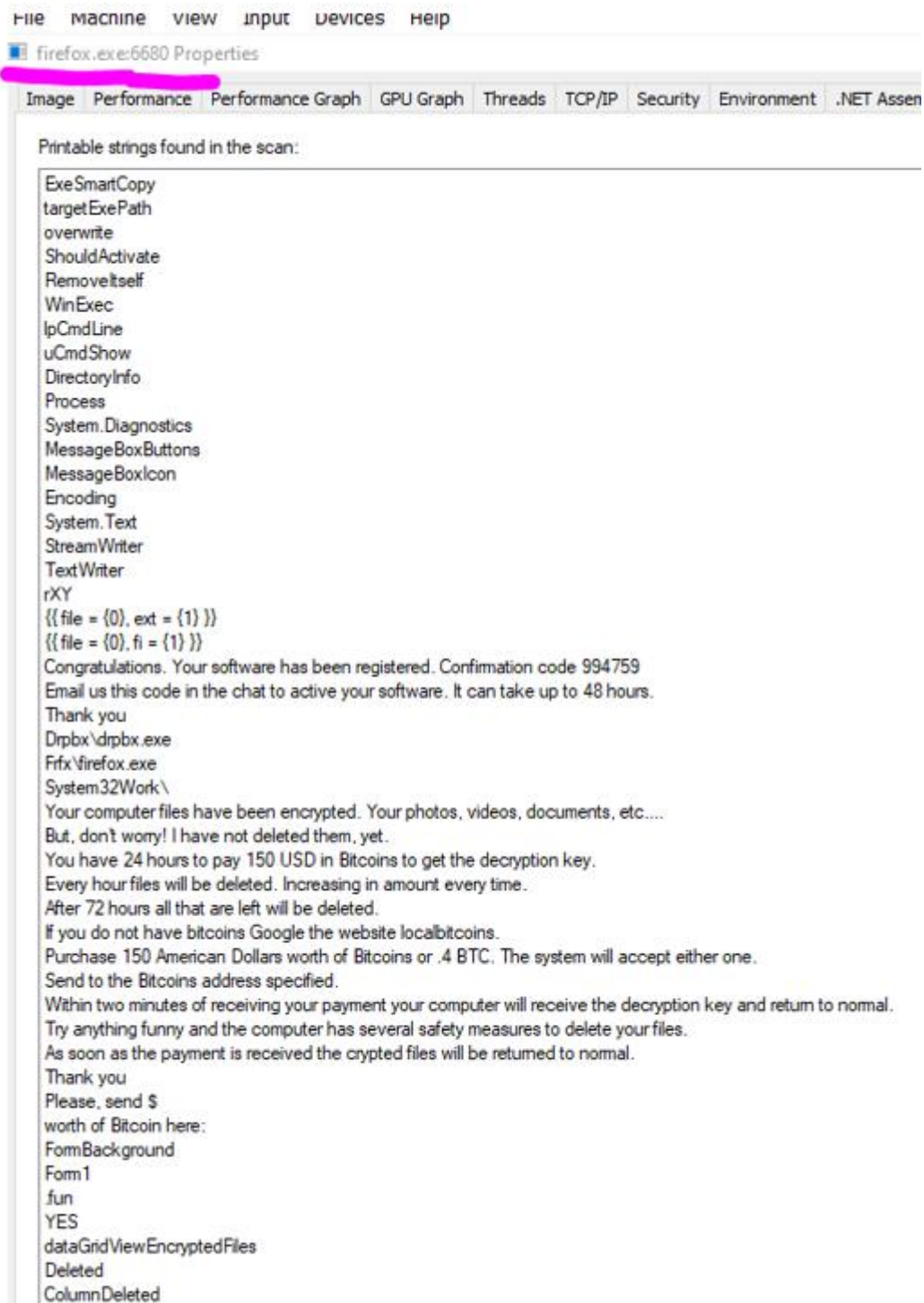
2) But when you think about “welcome screen” as the first view Lugkman meet when he opens windows machine after loading, we can assume that it is popup with our malware:





The text is identical to the text saved in the file firefox.exe strings:





## 5. Add three strings that indicate that is a malware

```

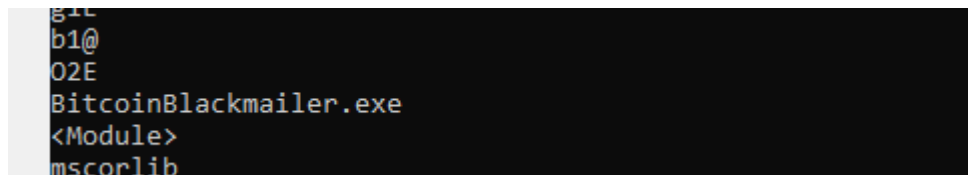
C:\Users\Luqman>C:\Users\Luqman\Desktop\strings.exe C:\Users\Luqman\AppData\Roaming\Frfx\firefox.exe

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

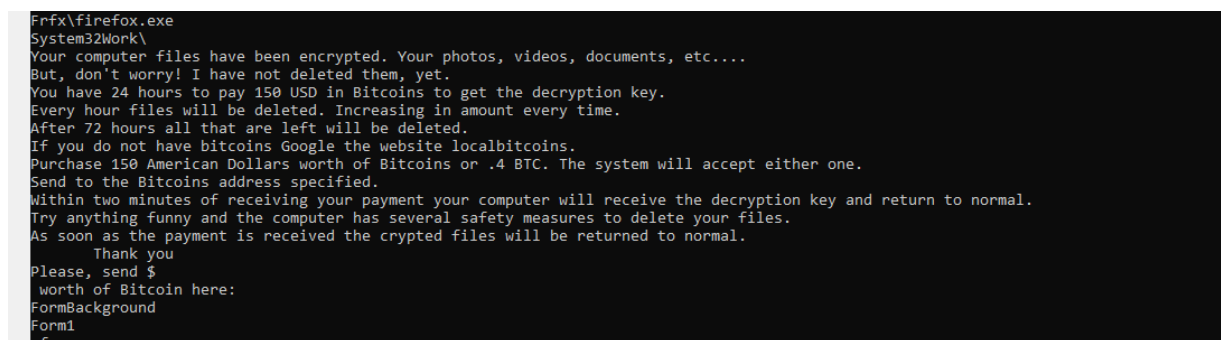
This program cannot be run in DOS mode.

```

“This program cannot be run in DOS mode” - Sometimes the malware or virus infection also causes the error. This happens because the malware or the virus has already infected the system file or program you need to run. This can lead you to malfunction or fail to run altogether.



signed with the name of the malicious program



Text in strings is the same as text on popup

Below I mentioned some other malware indicators presented using others tools:

#### a) Firefox.exe:

- Original name is different than displayed
- There is no verified file's signature
- Among strings are words relating to text displayed on pop-up
- On virus total website it is detected as trojan

Process	CPU	Private
MicrosoftEdgeUpdate.exe		
svchost.exe		
svchost.exe		
ctfmon.exe		
svchost.exe	< 0.01	
explorer.exe	0.22	
SecurityHealthSystray.exe		
VBoxTray.exe	0.04	
firefox.exe	0.04	
WinRAR.exe	0.01	
proceXP.exe		
proceXP64.exe	2.80	
regedit.exe		
svchost.exe	0.01	
StartMenuExperienceHost.exe		
RuntimeBroker.exe		
NisSrv.exe		
SearchIndexer.exe		
SearchApp.exe	Susp...	
RuntimeBroker.exe		
svchost.exe		
ShellExperienceHost.exe	Susp...	
drpbx.exe		
drpbx.exe		
SecurityHealthService.exe		
svchost.exe		
svchost.exe		
svchost.exe		
Spotify.exe	0.02	
Spotify.exe		
Spotify.exe	0.01	
Spotify.exe		
Spotify.exe		
Spotify.exe	< 0.01	
RuntimeBroker.exe		
svchost.exe		

Security

Environment

.NET Assemblies

.NET Performance

Strings

Image

Performance

Performance Graph

GPU Graph

Threads

TCP/IP

Count: 4

TID	CPU	Cycles Delta	Suspend Count	Start Address
5776	0.04	1,121,050		firefox.exe+0x4e00a
5940				mscorlib.dll!Meta...
5800				mscorlib.dll!Initial...
4240				gdiplus.dll!Gdiplus...

Thread ID: 5776

Start Time: 6:07:09 AM 9/6/2023

State: Wait:WnUserRequest Base Pri...

Kernel Time: 0:00:08.578 Dynamic

User Time: 0:00:13.734 I/O Prior...

Context Switches: 59,156 Memory

Cycles: 72,365,776,183 Ideal Pro...

General

Compatibility

Security

Details

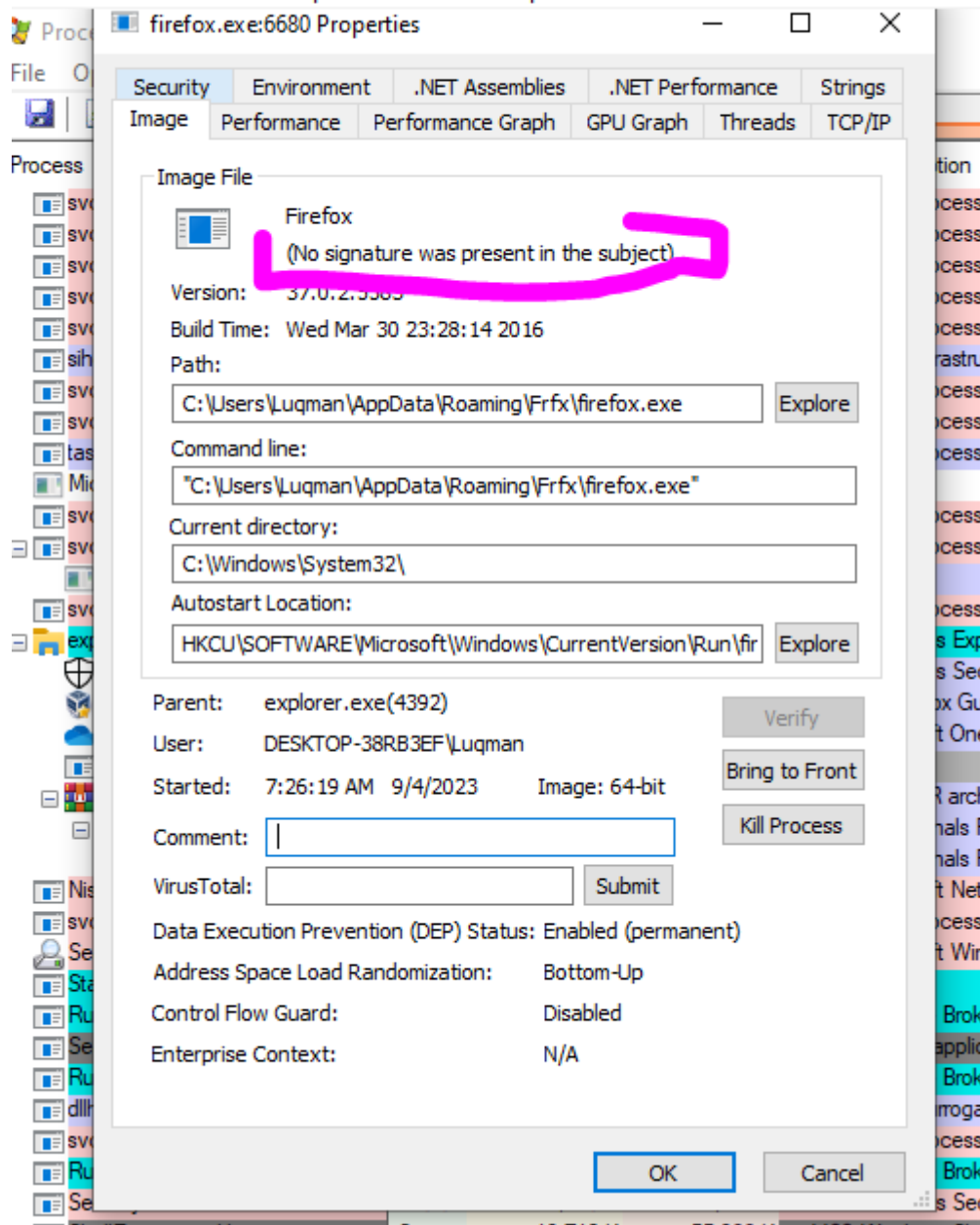
Previous Versions

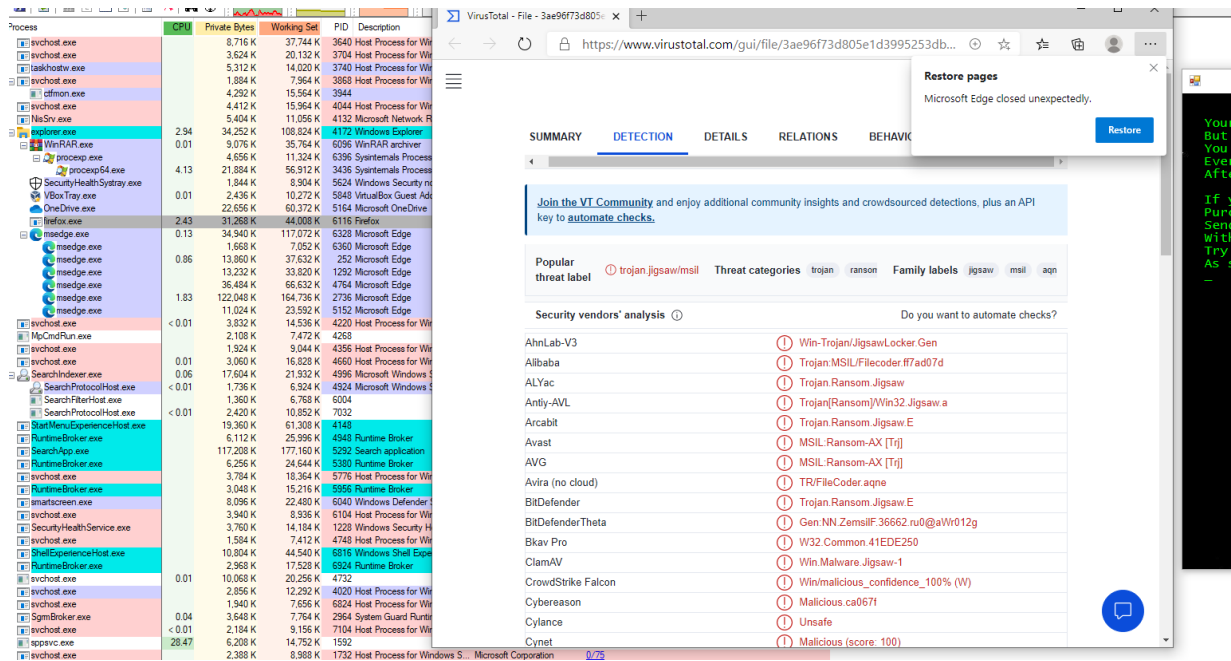
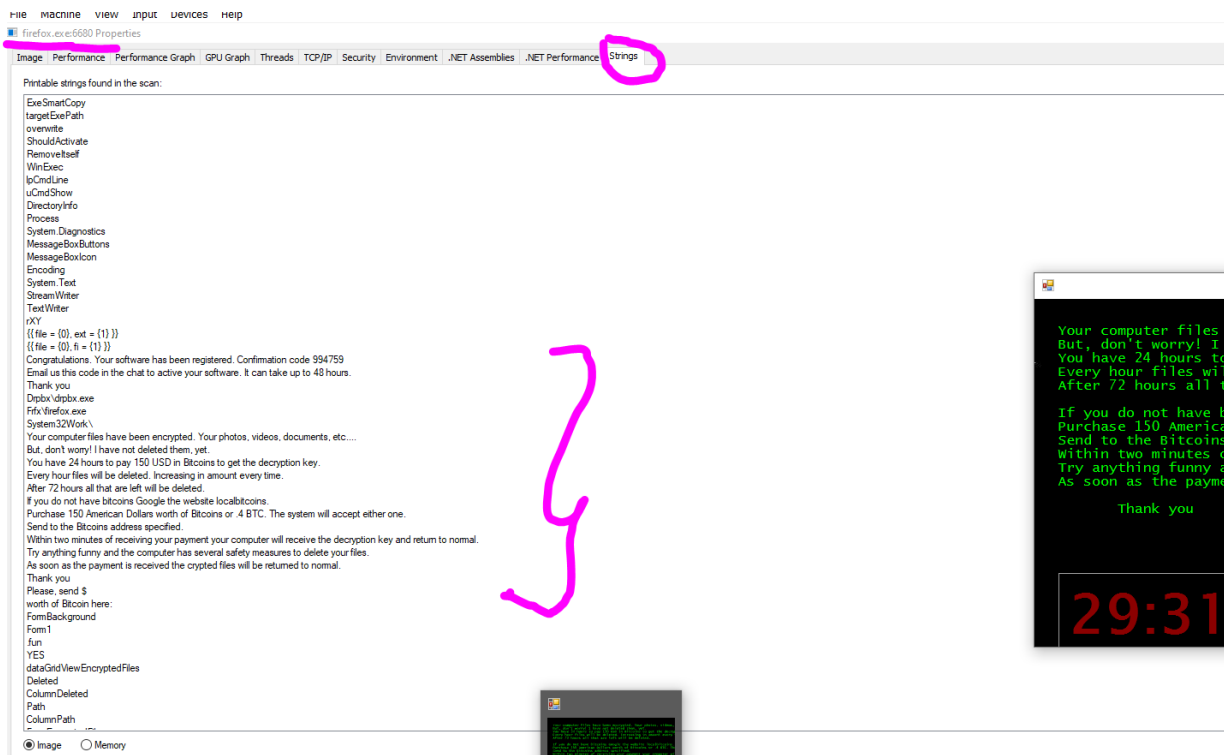
Property	Value
Description	
File description	Firefox
Type	Application
File version	37.0.2.5583
Product name	Firefox
Product version	37.0.2.5583
Copyright	Copyright 1999-2012 Firefox and Mozzill...
Size	283 KB
Date modified	4/13/2016 10:02 AM
Language	Language Neutral
Original filename	BitcoinBlackmailer.exe

[Remove Properties and Personal Information](#)

# SIEMnSOC\_Final [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help





## b) Drpbx.exe:

- Original name is different than displayed
- There is no verified signature with file
- Among strings are words with text displayed with virus popup
- On virus total website it is detected as trojan

File Options View Process Find Users Help

Process CPU Private

MicrosoftEdgeUpdate.exe  
svchost.exe  
svchost.exe  
ctfmon.exe  
svchost.exe  
explorer.exe  
SecurityHealthSystray.exe  
VBoxTray.exe  
firefox.exe  
WinRAR.exe  
procexp.exe  
procexp64.exe  
svchost.exe  
StartMenuExperienceHost.exe  
RuntimeBroker.exe  
NisSrv.exe  
SearchIndexer.exe  
SearchApp.exe  
RuntimeBroker.exe  
svchost.exe  
ShellExperienceHost.exe  
drpbx.exe  
drpbx.exe  
SecurityHealthService.exe  
svchost.exe  
svchost.exe  
svchost.exe  
svchost.exe  
Spotify.exe  
Spotify.exe  
Spotify.exe  
Spotify.exe  
Spotify.exe  
Spotify.exe  
RuntimeBroker.exe  
svchost.exe  
svchost.exe  
RuntimeBroker.exe  
OneDrive.exe  
MicrosoftEdgeUpdate.exe  
SgmnBroker.exe  
svchost.exe

3.068 K 11.056 K 6764 Host Process for Windows S... Microsoft Corporation

drpbx.exe:5824 Properties

Environment Job .NET Assemblies .NET Performance Strings  
Image Performance Performance Graph GPU Graph Threads TCP/IP Security

Image File

Firefox  
(No signature was present in the subject)

Version: 37.0.2.5583  
Build Time: Wed Mar 30 23:28:14 2016  
Path: C:\Users\Luqman\AppData\Local\Drpbx\drpbx.exe  
Command line: "C:\Users\Luqman\AppData\Local\Drpbx\drpbx.exe" C:\Users\Luqman\Documents\WindowsUpdate.EXE  
Current directory: C:\Windows\System32\  
Autostart Location: n/a  
Parent: <Non-existent Process>(3652)  
User: DESKTOP-38RB3EF\Luqman  
Started: 6:06:59 AM 9/6/2023 Image: 64-bit  
Comment:  
VirusTotal: Submit  
Data Execution Prevention (DEP) Status: Enabled (permanent)  
Address Space Load Randomization: Bottom-Up  
Control Flow Guard: Disabled  
Enterprise Context: N/A

OK Cancel





Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38RB3EF\Lugman]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
svchost.exe		2,612 K	10,496 K	3400	Host Process for Windows S...	Microsoft Corporation	0/75
WmiPrvSE.exe	3.35	5,016 K	13,364 K	3480			The system cannot find the file specified.
svchost.exe		3,824 K	13,272 K	3572	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe	0.60	17,116 K	34,288 K	3600	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe		8,756 K	17,104 K	3632	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe	0.06	2,328 K	9,020 K	3668	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe		1,228 K	5,596 K	3752	Host Process for Windows S...	Microsoft Corporation	0/75
MsMpEng.exe	0.72	146,100 K	104,192 K	3760	Antimalware Service Execut...	Microsoft Corporation	0/75
MpCmdRun.exe		2,740 K	10,244 K	4872			The system cannot find the file specified.
conhost.exe	0.01	6,644 K	12,884 K	4884			The system cannot find the file specified.
svchost.exe	0.01	3,008 K	16,840 K	3768	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe		4,400 K	20,572 K	3776	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe		2,644 K	10,820 K	3928	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe		1,248 K	5,404 K	3992	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe		2,240 K	7,128 K	2768	Host Process for Windows S...	Microsoft Corporation	0/75
NlsSrv.exe	0.12	5,460 K	11,560 K	4800	Microsoft Network Realtime I...	Microsoft Corporation	0/75
MpCmdRun.exe		2,124 K	7,492 K	4832			The system cannot find the file specified.
StartMenuExperienceHost.exe		19,388 K	61,556 K	4940			0/74
RuntimeBroker.exe		6,412 K	28,012 K	5012	Runtime Broker	Microsoft Corporation	0/74
SearchApp.exe		80,032 K	143,908 K	5116	Search application	Microsoft Corporation	0/75
RuntimeBroker.exe		6,484 K	25,856 K	4424	Runtime Broker	Microsoft Corporation	0/74
SearchIndexer.exe	0.01	17,588 K	22,672 K	2480	Microsoft Windows Search I...	Microsoft Corporation	0/73
svchost.exe	< 0.01	4,044 K	15,124 K	5152	Host Process for Windows S...	Microsoft Corporation	0/75
RuntimeBroker.exe		3,068 K	15,372 K	5712	Runtime Broker	Microsoft Corporation	0/74
svchost.exe		4,008 K	19,992 K	5952	Host Process for Windows S...	Microsoft Corporation	0/75
smartscreen.exe		8,096 K	23,612 K	1808	Windows Defender SmartScr...	Microsoft Corporation	0/75
svchost.exe	0.05	10,908 K	21,312 K	4556	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe		1,980 K	7,324 K	4544	Host Process for Windows S...	Microsoft Corporation	0/75
dpbpx.exe		18,136 K	2,492 K	6180	Firefox		63/75
dpbpx.exe		18,084 K	2,488 K	6228	Firefox		63/75
svchost.exe		1,132 K	5,936 K	6720	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe		4,184 K	10,584 K	6908	Host Process for Windows S...	Microsoft Corporation	0/75
ShellExperienceHost.exe		12,000 K	53,244 K	6984	Windows Shell Experience H...	Microsoft Corporation	0/73
RuntimeBroker.exe		3,884 K	22,076 K	7100	Runtime Broker	Microsoft Corporation	0/74
svchost.exe		1,548 K	7,080 K	7148	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe		3,288 K	12,828 K	2216	Host Process for Windows S...	Microsoft Corporation	0/75
MicrosoftEdgeUpdate.exe	0.92	3,792 K	15,644 K	5584	Microsoft Edge Update	Microsoft Corporation	0/75
svchost.exe		2,836 K	12,344 K	252	Host Process for Windows S...	Microsoft Corporation	0/75
SgmBroker.exe		3,784 K	6,872 K	6592	System Guard Runtime Monit...	Microsoft Corporation	0/74
svchost.exe		4,256 K	16,040 K	5800	Host Process for Windows S...	Microsoft Corporation	0/75
MoUsoCoreWorker.exe		19,236 K	30,752 K	2940			
svchost.exe	3.13	2,288 K	10,012 K	2436	Host Process for Windows S...	Microsoft Corporation	0/75
svchost.exe		10,036 K	29,912 K	3036	Host Process for Windows S...	Microsoft Corporation	0/75
SecurityHealthService.exe		2,396 K	10,880 K	3940	Windows Security Health Se...	Microsoft Corporation	0/74

CPU Usage: 100.00% | Commit Charge: 32.04% | Processes: 141 | Physical Usage: 44.85%

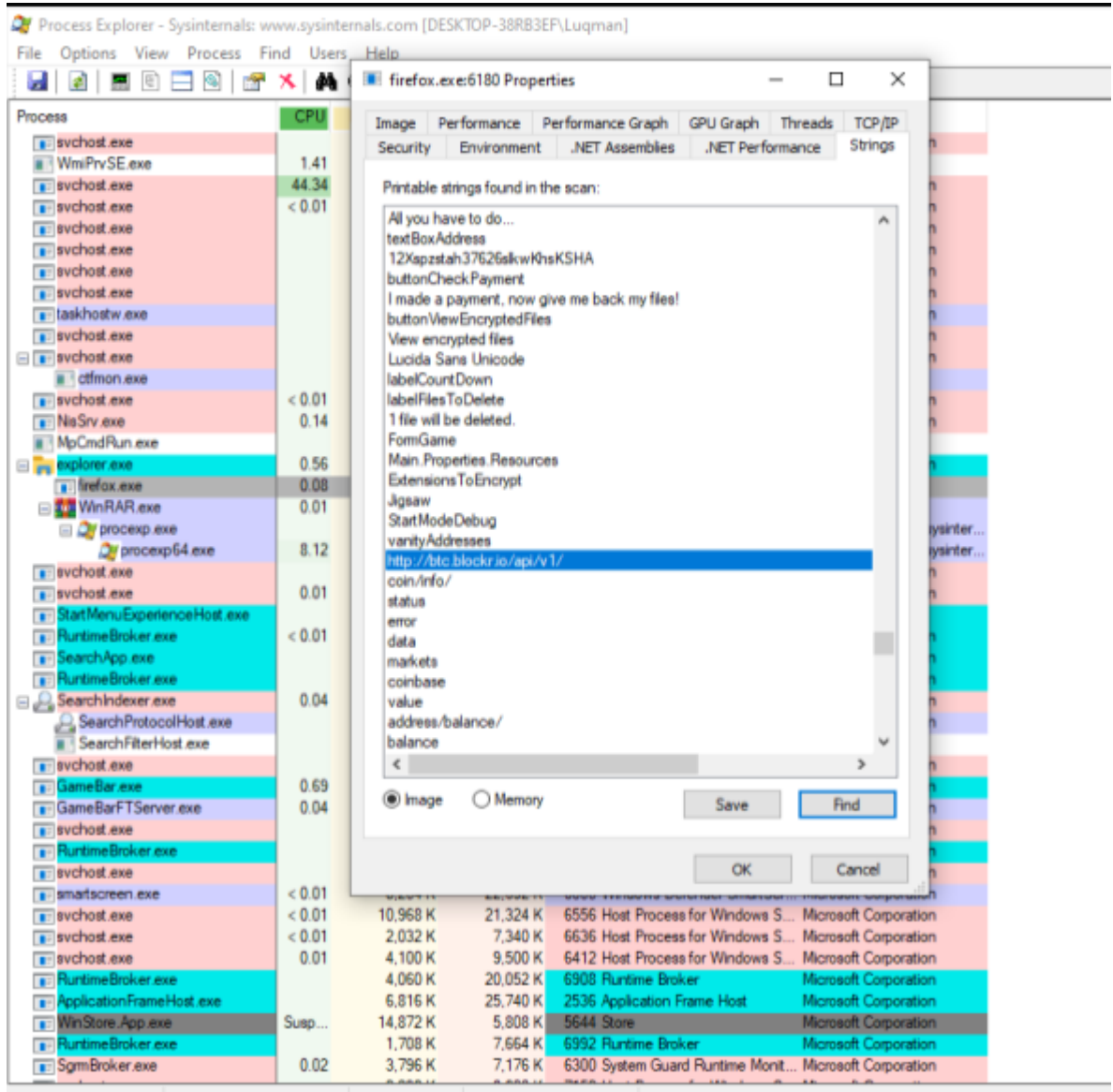
Type here to search

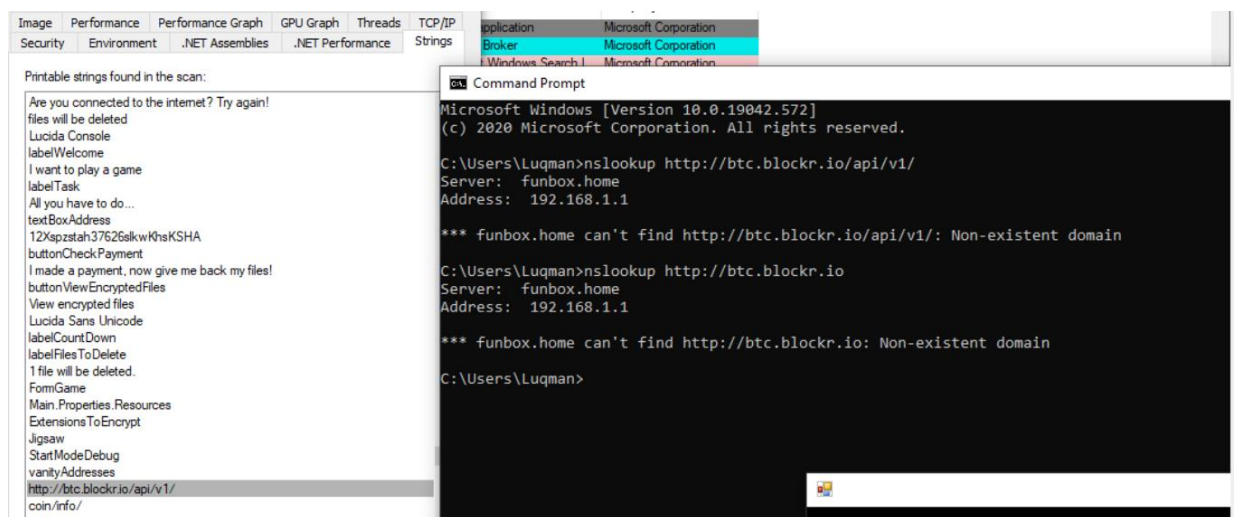
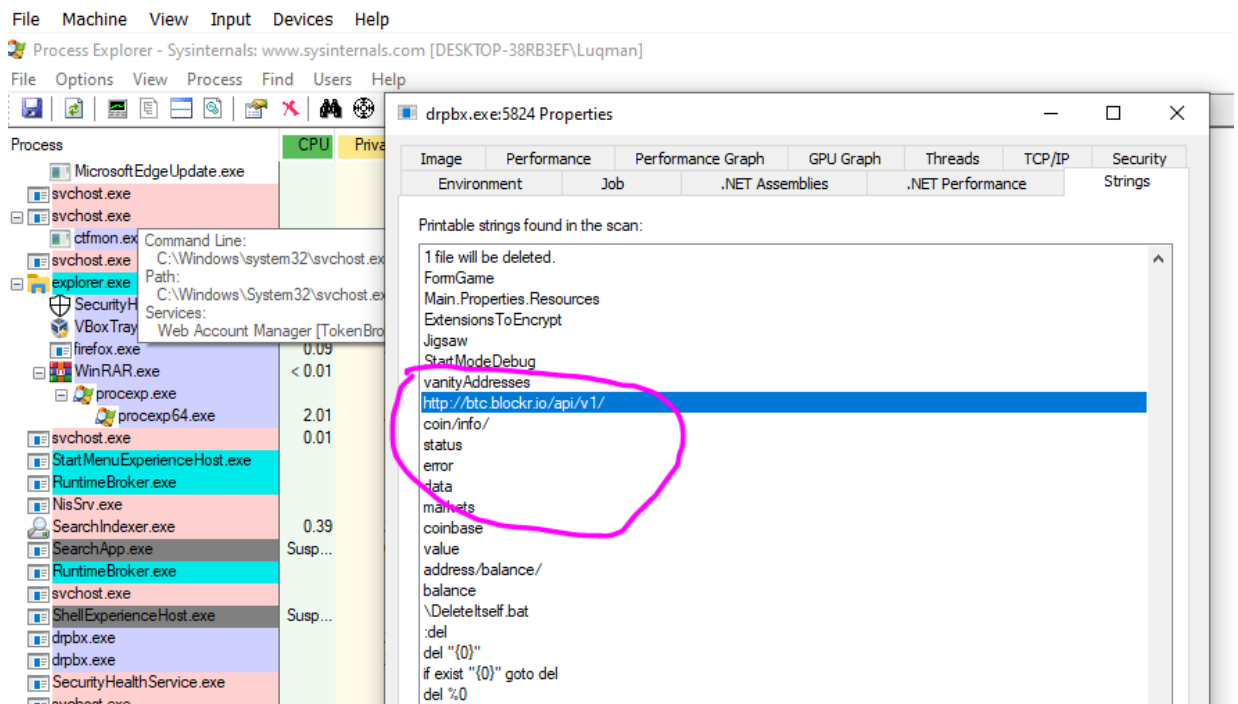
1:05 AM 9/5/2023

The screenshot displays a Windows desktop environment. On the left, the Process Explorer window is open, showing a list of running processes. The columns visible are Process, CPU, Private Bytes, Working Set, and PID. Processes include msedge.exe, svchost.exe, WmiPrvSE.exe, MpCmdRun.exe, conhost.exe, SearchApp.exe, SearchIndexer.exe, SearchProtocolHost.exe, SearchFilterHost.exe, RuntimeBroker.exe, smartscreen.exe, ShellExperienceHost.exe, and several instances of svchost.exe. The CPU usage is 100.00% and the commit charge is 37.89%.

On the right, the VirusTotal website is open in a web browser. The URL is <https://www.virustotal.com/gui/file/3ae96f73d805e1d3995253db...>. The 'DETECTION' tab is selected, showing a summary of security vendors' analysis. The file is identified as a Trojan.JigsawLocker.Gen with a score of 100 (Malicious). The analysis includes detections from AhnLab-V3, Alibaba, ALYac, Antiy-AVL, Arcabit, Avast, AVG, Avira (no cloud), BitDefender, BitDefenderTheta, Bkav Pro, ClamAV, CrowdStrike Falcon, Cybereason, Cylance, and Cynet.

## 6. Find the associated website and IP of the malware





IP found -> source: virustotal 52.90.150.224

<https://www.virustotal.com/gui/url/edbb69e0ef35f728abb7dc40aab1613a9a7d4b80aa2d6c1f04f5087d3804a05c/details>

http://btc.blockr.io/

Last Submission	2023-08-17 04:16:11 UTC
Last Analysis	2023-08-17 04:16:11 UTC

---

**HTTP Response** ⓘ

---

**Final URL**  
http://btc.blockr.io/

**Serving IP Address**  
52.90.150.224

**Status Code**  
200

**Body Length**  
8.26 KB

**Body SHA-256**  
e0484a8fa0ba5ce43090f97ac2052768c78454463439fd42ea1d673b4daa2442

Analyse

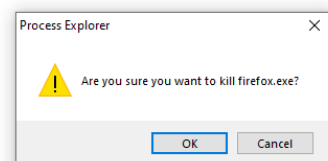
## 7. Terminate the malware permanently when done and explain why it works.

Steps:

- Suspend first, then kill processes: firefox.exe and drpbx.exe (x2)

MicrosoftEdgeUpdate.exe	2,416 K	212 K	6028	
MicrosoftEdgeUpdate.exe	1,600 K	156 K	7088	
MicrosoftEdgeUpdate.exe	1,600 K	152 K	3448	
MicrosoftEdgeUpdate.exe	1,660 K	9,300 K	2516	
svchost.exe	2,936 K	13,992 K	3736	Host Process for Windows S... Microsoft Corporation
svchost.exe	1,692 K	7,268 K	3864	Host Process for Windows S... Microsoft Corporation
ctfmon.exe	7,952 K	21,288 K	3924	
svchost.exe	0.01	4,116 K	14,216 K	4068 Host Process for Windows S... Microsoft Corporation
explorer.exe	0.13	56,348 K	129,480 K	3604 Windows Explorer Microsoft Corporation
SecurityHealthService.exe		8,780 K	6124	Windows Security notificatio... Microsoft Corporation
VBoxTray.exe		10,240 K	3132	VirtualBox Guest Additions Tr... Oracle Corporation
firefox.exe		36,948 K	5044	Firefox
WinRAR.exe		64,080 K	5452	WinRAR archiver Alexander Roshal
Regshot.exe		144,680 K	5752	
svchost.exe		18,092 K	4196	Host Process for Windows S... Microsoft Corporation
StartMenuExperienceHost.exe		65,204 K	4880	
RuntimeBroker.exe		28,144 K	4968	Runtime Broker Microsoft Corporation
NisSrv.exe		8,588 K	3724	Microsoft Network Realtime I... Microsoft Corporation
SearchIndexer.exe		33,932 K	4316	Microsoft Windows Search I... Microsoft Corporation
SearchProtocolHost.exe		7,264 K	6488	Microsoft Windows Search P... Microsoft Corporation
SearchApp.exe		145,940 K	4648	Search application Microsoft Corporation
RuntimeBroker.exe		23,832 K	4412	Runtime Broker Microsoft Corporation
svchost.exe		18,660 K	5160	Host Process for Windows S... Microsoft Corporation
ShellExperienceHost.exe		37,500 K	5336	Windows Shell Experience H... Microsoft Corporation
drpbx.exe		4,304 K	5816	Firefox
drpbx.exe		60,248 K	4,016 K	5824 Firefox
SecurityHealthService.exe		3,700 K	13,516 K	2116 Windows Security Health Se... Microsoft Corporation
svchost.exe		1,860 K	6,908 K	3652 Host Process for Windows S... Microsoft Corporation
svchost.exe		1,896 K	9,256 K	5064 Host Process for Windows S... Microsoft Corporation
svchost.exe		4,368 K	10,512 K	5672 Host Process for Windows S... Microsoft Corporation
svchost.exe		1,400 K	5,768 K	5476 Host Process for Windows S... Microsoft Corporation
RuntimeBroker.exe		2,472 K	15,804 K	6752 Runtime Broker Microsoft Corporation
svchost.exe		1,588 K	10,832 K	6932 Host Process for Windows S... Microsoft Corporation
OneDrive.exe		36,624 K	83,396 K	6672 Microsoft OneDrive Microsoft Corporation
MicrosoftEdgeUpdate.exe		1,532 K	7,560 K	5464
SgmBroker.exe		3,656 K	6,704 K	4220 System Guard Runtime Monit... Microsoft Corporation
svchost.exe		4,568 K	15,776 K	6764 Host Process for Windows S... Microsoft Corporation
svchost.exe		1,720 K	6,916 K	5900 Host Process for Windows S... Microsoft Corporation
svchost.exe		2,432 K	9,240 K	5708 Host Process for Windows S... Microsoft Corporation

svchost.exe	2,668 K	10,684 K	2800	Host Process for Windows S... Microsoft Corporation
svchost.exe	1,292 K	4,964 K	2852	Host Process for Windows S... Microsoft Corporation
svchost.exe	1,932 K	7,396 K	3176	Host Process for Windows S... Microsoft Corporation
svchost.exe	4,392 K	15,648 K	3504	Host Process for Windows S... Microsoft Corporation
shost.exe	5,916 K	24,404 K	3516	Shell Infrastructure Host Microsoft Corporation
svchost.exe	8,312 K	35,812 K	3528	Host Process for Windows S... Microsoft Corporation
taskhostw.exe	6,660 K	16,816 K	3700	Host Process for Windows T... Microsoft Corporation
MicrosoftEdgeUpdate.exe	0.01	1,992 K	3,052 K	3708
MicrosoftEdgeUpdate.exe		2,216 K	212 K	6028
MicrosoftEdgeUpdate.exe		1,600 K	156 K	7088
MicrosoftEdgeUpdate.exe		1,600 K	152 K	3448
MicrosoftEdgeUpdate.exe	0.01	1,732 K	8,648 K	2516
svchost.exe		2,992 K	14,012 K	3736 Host Process for Windows S... Microsoft Corporation
svchost.exe		1,748 K	7,284 K	3864 Host Process for Windows S... Microsoft Corporation
ctfmon.exe		7,968 K	21,292 K	3924
svchost.exe		4,168 K	14,232 K	4068 Host Process for Windows S... Microsoft Corporation
explorer.exe	0.10	56,008 K	128,944 K	3604 Windows Explorer Microsoft Corporation
SecurityHealthSystay.exe		1,660 K	8,780 K	6124 Windows Security notificatio... Microsoft Corporation
VBoxTray.exe	0.03	2,376 K	10,240 K	3132 VirtualBox Guest Additions Tr... Oracle Corporation
firefox.exe		32,364 K	36,964 K	5044 Firefox
WinRAR.exe	< 0.01	15,120 K	64,088 K	5452 WinRAR archiver Alexander Roshal
Regshot.exe		140,340 K	144,680 K	5752
svchost.exe	0.01	3,392 K	18,108 K	4196 Host Process for Windows S... Microsoft Corporation
StartMenuExperienceHost.exe		23,016 K	65,192 K	4880
RuntimeBroker.exe		6,644 K	28,108 K	4968 Runtime Broker Microsoft Corporation
NisSrv.exe		3,536 K	8,588 K	3724 Microsoft Network Realtime I... Microsoft Corporation
SearchIndexer.exe		29,320 K	33,944 K	4316 Microsoft Windows Search I... Microsoft Corporation
SearchProtocolHost.exe		1,644 K	7,252 K	6488 Microsoft Windows Search P... Microsoft Corporation
SearchApp.exe	Susp...	82,828 K	145,940 K	4648 Search application Microsoft Corporation
RuntimeBroker.exe		6,132 K	23,832 K	4412 Runtime Broker Microsoft Corporation
svchost.exe		4,128 K	18,660 K	5160 Host Process for Windows S... Microsoft Corporation
ShellExperienceHost.exe	Susp...	10,380 K	37,500 K	5336 Windows Shell Experience H... Microsoft Corporation
drpbx.exe	Susp...	60,160 K	3,040 K	5816 Firefox
drpbx.exe	Susp...	60,248 K	2,804 K	5824 Firefox
SecurityHealthService.exe		3,700 K	13,516 K	2116 Windows Security Health Se... Microsoft Corporation
svchost.exe		1,964 K	6,936 K	3652 Host Process for Windows S... Microsoft Corporation
svchost.exe		1,788 K	9,212 K	5064 Host Process for Windows S... Microsoft Corporation



The screenshot shows the Windows Task Manager interface with a list of running processes. A pink arrow points to the 'drpbx.exe' process, which is highlighted in blue. To the right, a 'Process Explorer' dialog box is open, asking 'Are you sure you want to kill drpbx.exe?' with 'OK' and 'Cancel' buttons.

b) Delete: directories: System32Work, Frfx, Drpbx and everything what was possible to delete in Temp

The screenshot shows a Windows File Explorer window with the address bar displaying the path: This PC > Local Disk (C:) > Users > Luqman > AppData > Roaming > System32Work. The file list shows three items:

Name	Date modified	Type	Size
Address	9/5/2023 4:14 AM	Text Document	1 KB
dr	9/5/2023 4:14 AM	File	1 KB
EncryptedFileList	9/5/2023 4:14 AM	Text Document	70 KB



Roaming

Home Share View

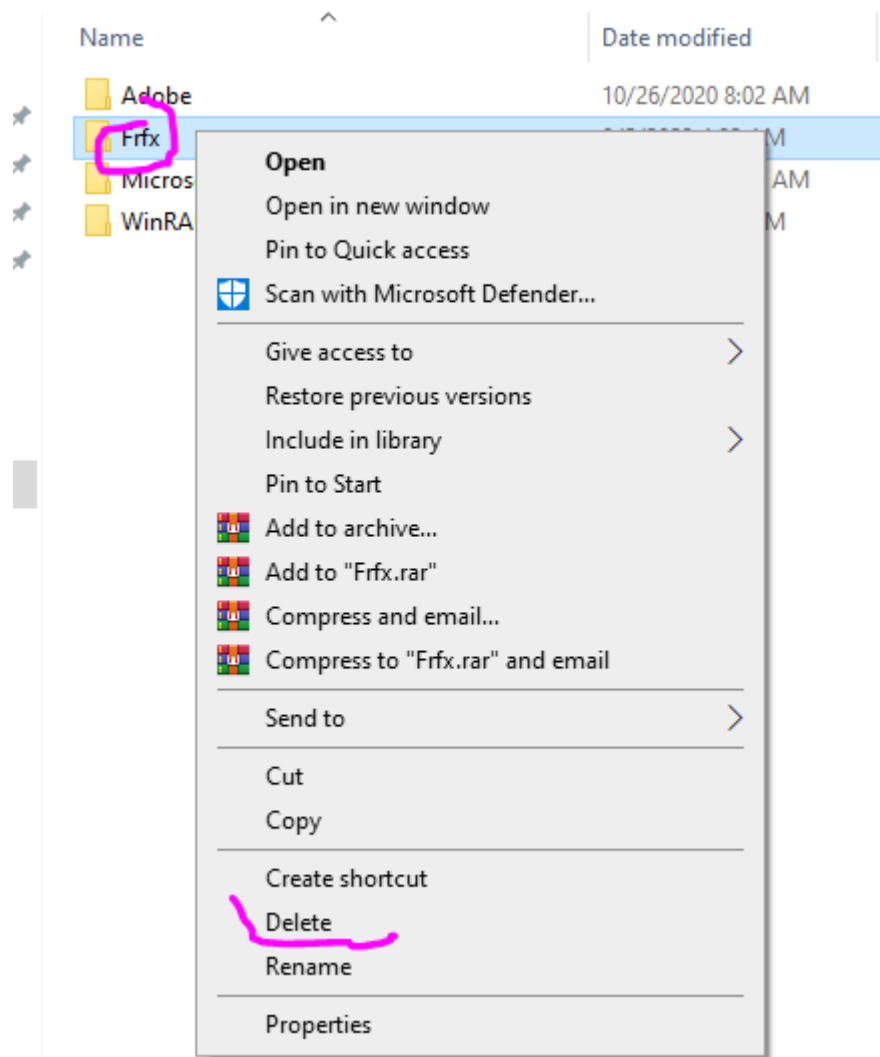
This PC > Local Disk (C:) > Users > Luqman > AppData > Roaming >

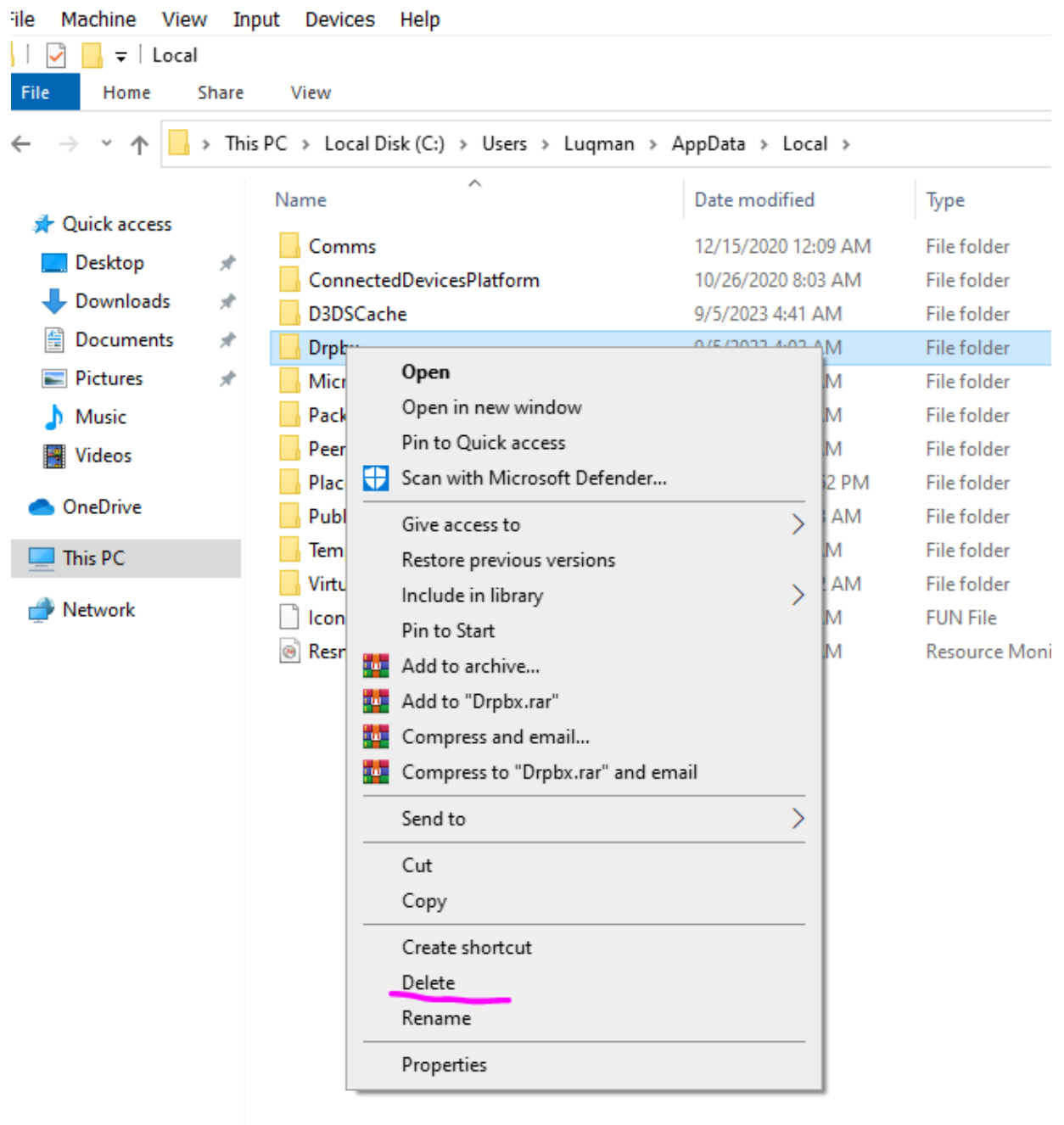
Name	Date modified	Type	Size
Adobe	10/26/2020 8:02 AM	File folder	
Firefox	9/5/2023 4:02 AM	File folder	
Microsoft	12/16/2020 1:04 AM	File folder	
System32Work	0/5/2022 4:14 AM	File folder	
Windows		File folder	

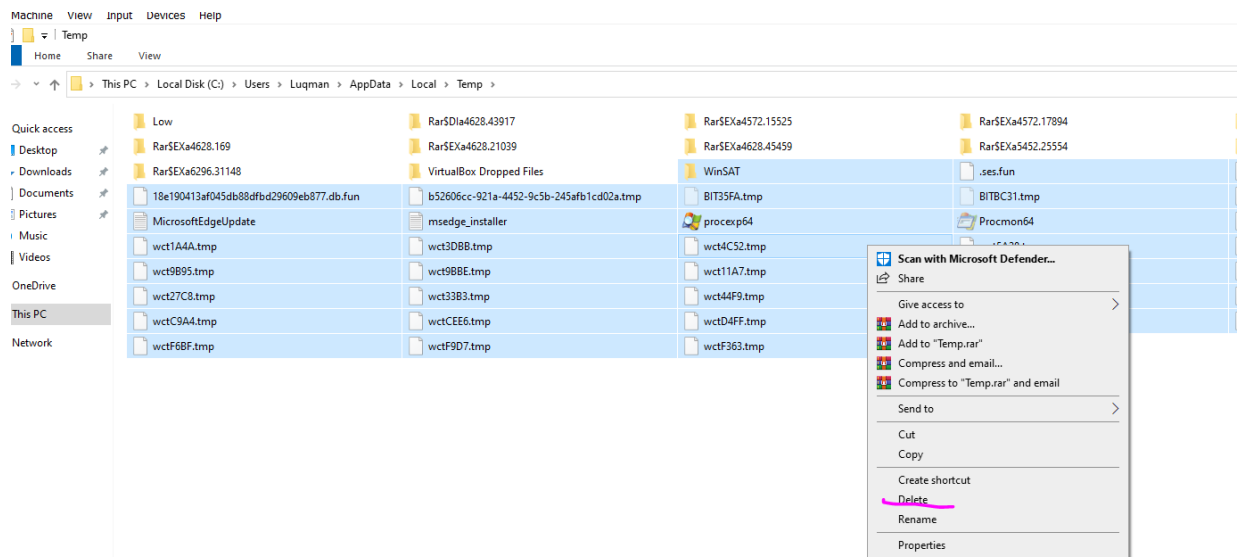
Left sidebar: Quick access, Desktop, Downloads, Documents, Pictures, Music, Videos, This PC, Work

Context menu for 'System32Work':

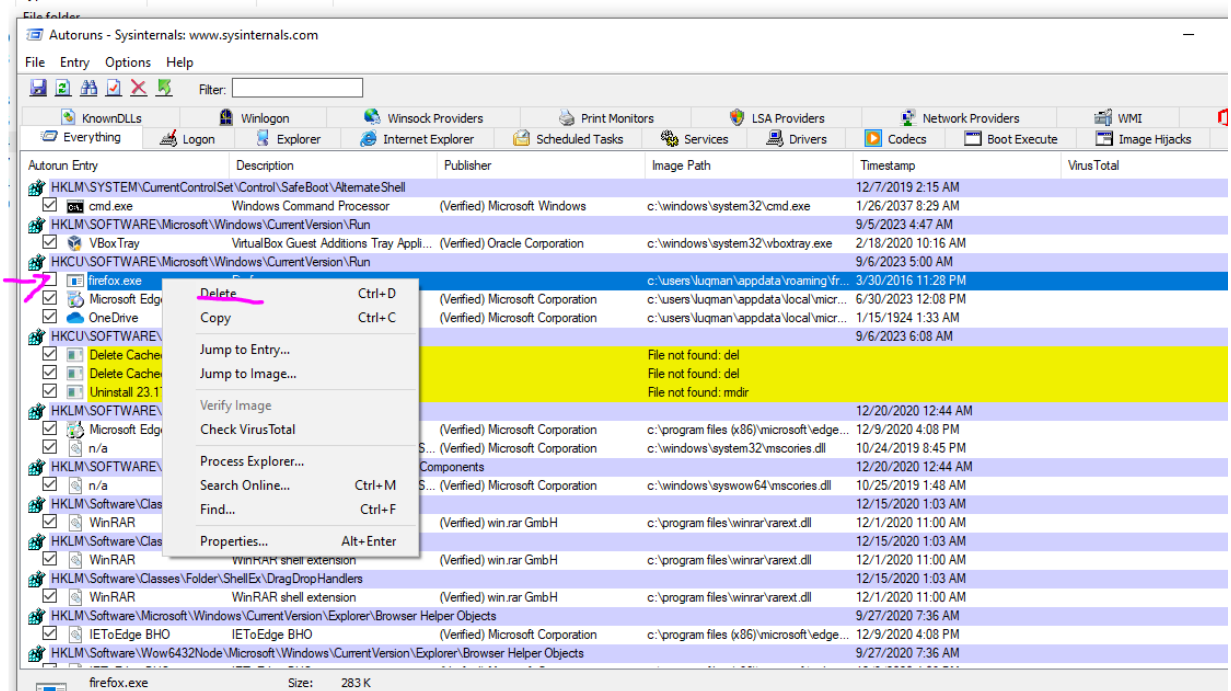
- Open
- Open in new window
- Pin to Quick access
- Scan with Microsoft Defender...
- Give access to >
- Restore previous versions
- Include in library >
- Pin to Start
- Add to archive...
- Add to "System32Work.rar"
- Compress and email...
- Compress to "System32Work.rar" and email
- Send to >
- Cut
- Copy
- Create shortcut
- Delete
- Rename
- Properties





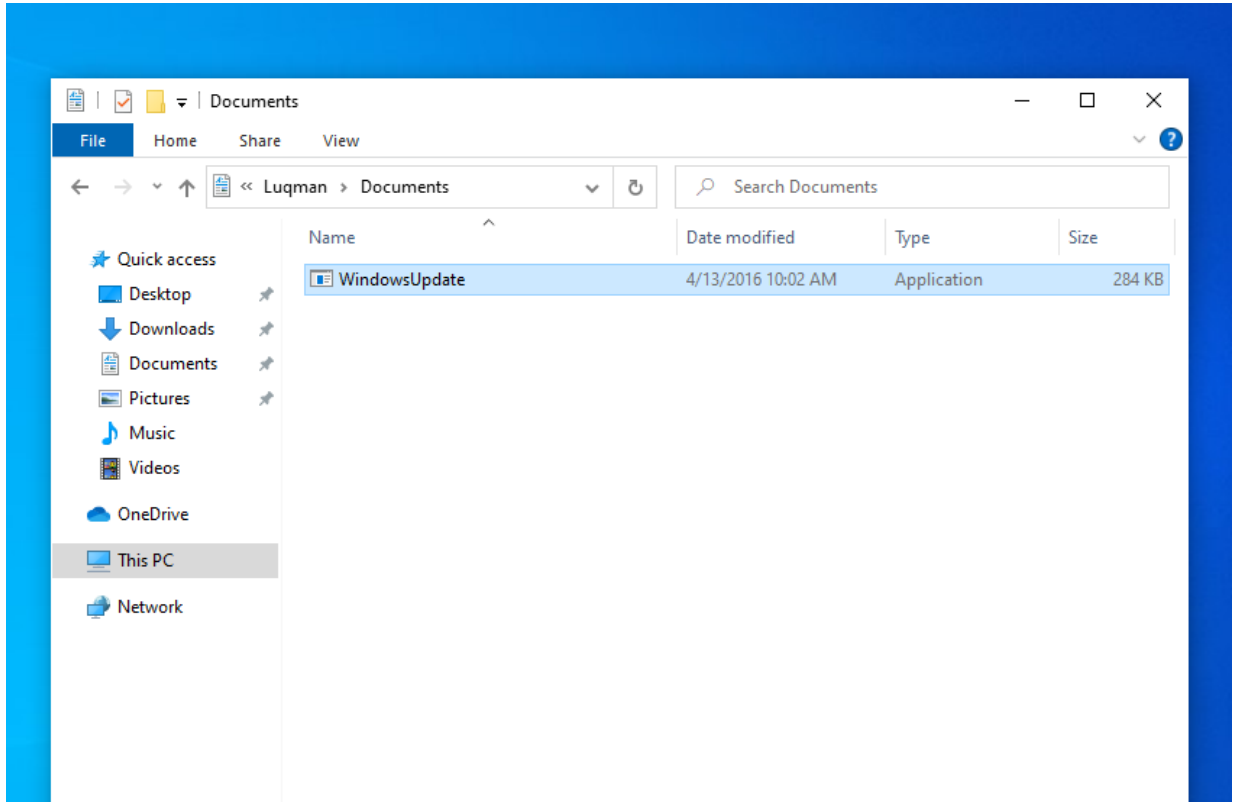
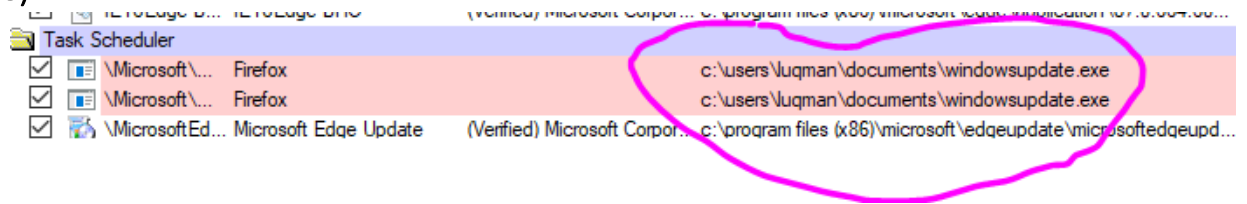


c) Uncheck and kill processes in Autoruns: firefox.exe

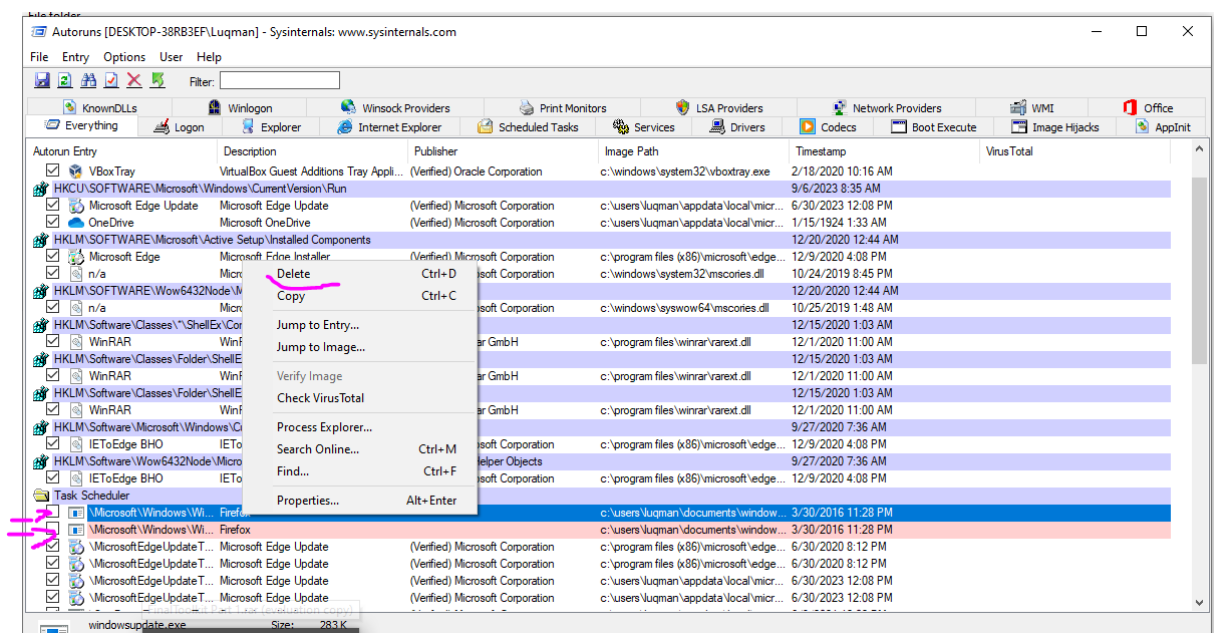


d) And we can see here, there is one more infected file (as was mentioned in point 3.): windowsupdate.exe

e)



After we deleted file windowsupdate.exe, we unchecked and delete tasks as shown below:



Regshot's report shows changes in Registry Editor after removing malware:



```
HKU\S-1-5-21-1313434519-986968716-766249846-1001_Classes\Local Settings\Software\Microsoft\W
HKU\S-1-5-21-1313434519-986968716-766249846-1001_Classes\Local Settings\Software\Microsoft\W
HKU\S-1-5-21-1313434519-986968716-766249846-1001_Classes\Local Settings\Software\Microsoft\W
HKU\S-1-5-21-1313434519-986968716-766249846-1001_Classes\Local Settings\Software\Microsoft\W
HKU\S-1-5-21-1313434519-986968716-766249846-1001_Classes\Local Settings\Software\Microsoft\W
```

Total changes: 343



After rebooting there is no malware any more. The procedure was successful because not only processes were killed but also files were removed and process were deleted from Registry Editor. They don't load during booting.

The image shows a Windows Task Manager window on the left, displaying a list of running processes. The processes are sorted by name, and the columns show the process name, PID, PPID, Name, Description, and Publisher. The processes listed include svchost.exe, csrss.exe, winlogon.exe, fontdrvhost.exe, dwm.exe, explorer.exe, WinRAR.exe, procexp.exe, procexp64.exe, Autoruns.exe, SecurityHealthSystray.exe, VBoxTray.exe, and OneDrive.exe. The Task Manager window is overlaid on top of the Autoruns application window.

The Autoruns application window is open, showing a list of registry entries. The entries are sorted by name, and the columns show the entry name, description, and publisher. The entries listed include HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, Microsoft Edge Update, OneDrive, HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components, Microsoft Edge, n/a, HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components, n/a, HKLM\Software\Classes\\*\ShellEx\ContextMenuHandlers, WinRAR, HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers, WinRAR, HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers, WinRAR, HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects, IEToEdge BHO, HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects, IEToEdge BHO, Task Scheduler, \MicrosoftEdgeUpdateT..., \MicrosoftEdgeUpdateT..., and \OneDrive Reporting Ta... Standalone Updater.