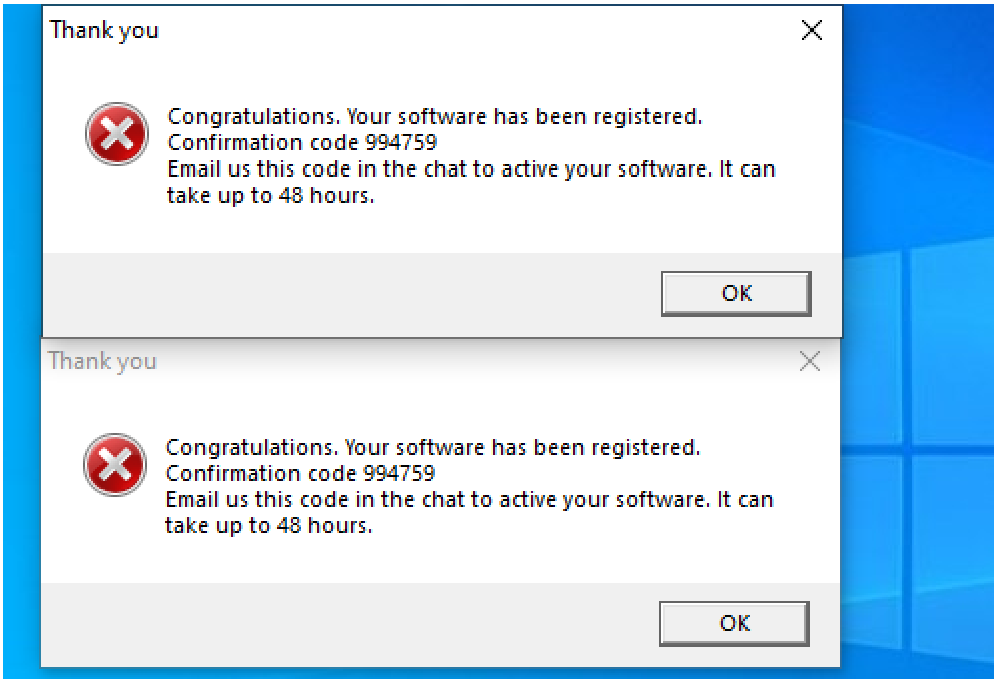
SIEM &SOC Final Project

Author Mateusz Łagocki



Congratulations. Your software has been registered.
Confirmation code 994759
Email us this code in the chat to active your software. It can take up to 48 hours.

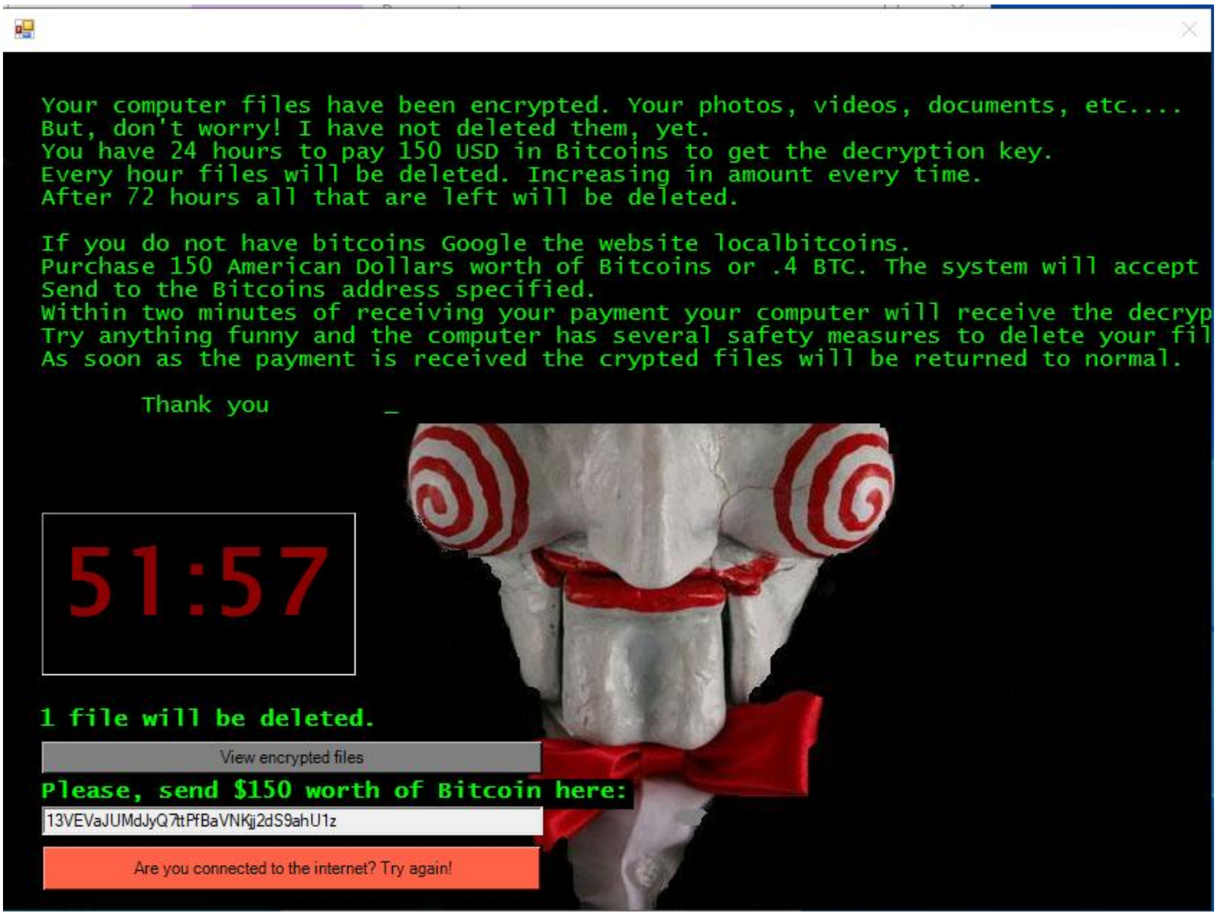
Thank you

Congratulations. Your software has been registered.
Confirmation code 994759
Email us this code in the chat to active your software. It can take up to 48 hours.

OK

What It Means:

- The message appears to be a **fake notification**, possibly part of a **scam or ransomware** attempt.
- It claims that software has been "registered," but then asks the user to send a confirmation code via chat to "active" the software (note the grammatical error – it should be "activate").
- The message is generic, does not mention any specific software, and uses suspicious language, which is common in malicious popups.
- The fact that two identical windows appeared simultaneously suggests **automated or malicious behavior**, which is a strong sign of malware activity.



```
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
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryp
Try anything funny and the computer has several safety measures to delete your fil
As soon as the payment is received the crypted files will be returned to normal.

       Thank you
```

51:57

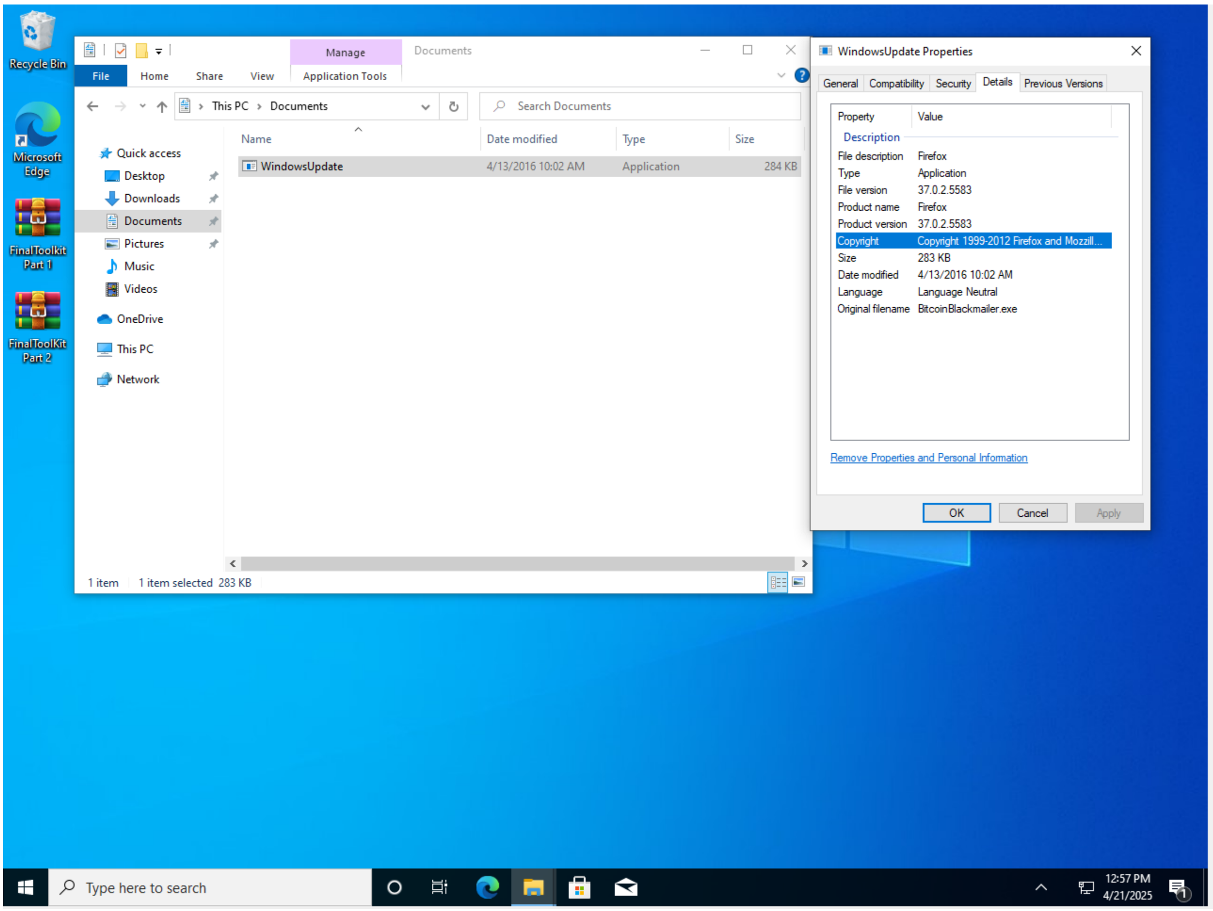
1 file will be deleted.

Please, send $150 worth of Bitcoin here:

13VEVaJUMdJyQ7ttPfBaVNKjj2dS9ahU1z

In the picture above, we can see the effect if an unaware user overrides the ok (which is, unfortunately, the only choice).

We can see that we are dealing with a typical ransomware whose purpose is to force us to pay a ransom under the threat of deleting already encrypted files and all files on the user's computer.



Name	Date modified	Type	Size
WindowsUpdate	4/13/2016 10:02 AM	Application	284 KB

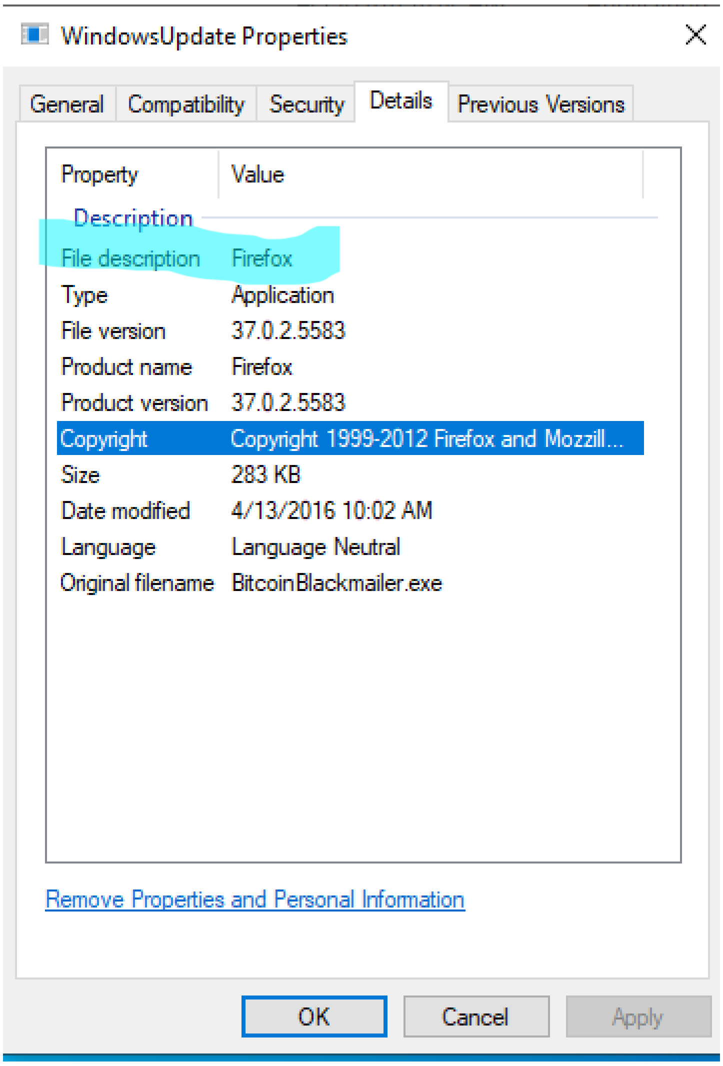
1 item 1 item selected 283 KB

WindowsUpdate Properties

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

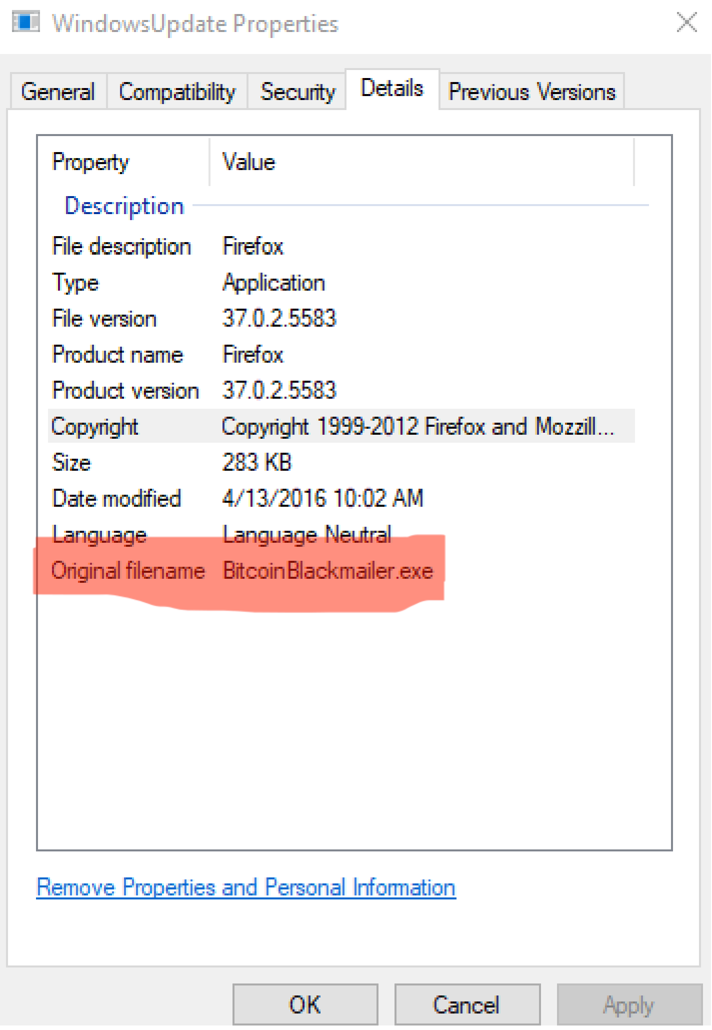
In the above screenshot, we see a potential file that is a threat to our user.

At first, it may seem like a simple system update file, but after delving into the properties, it turns out that it is malware that has infected the computer and probably slowed down its performance by overloading processes responsible for the speed of operation.



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

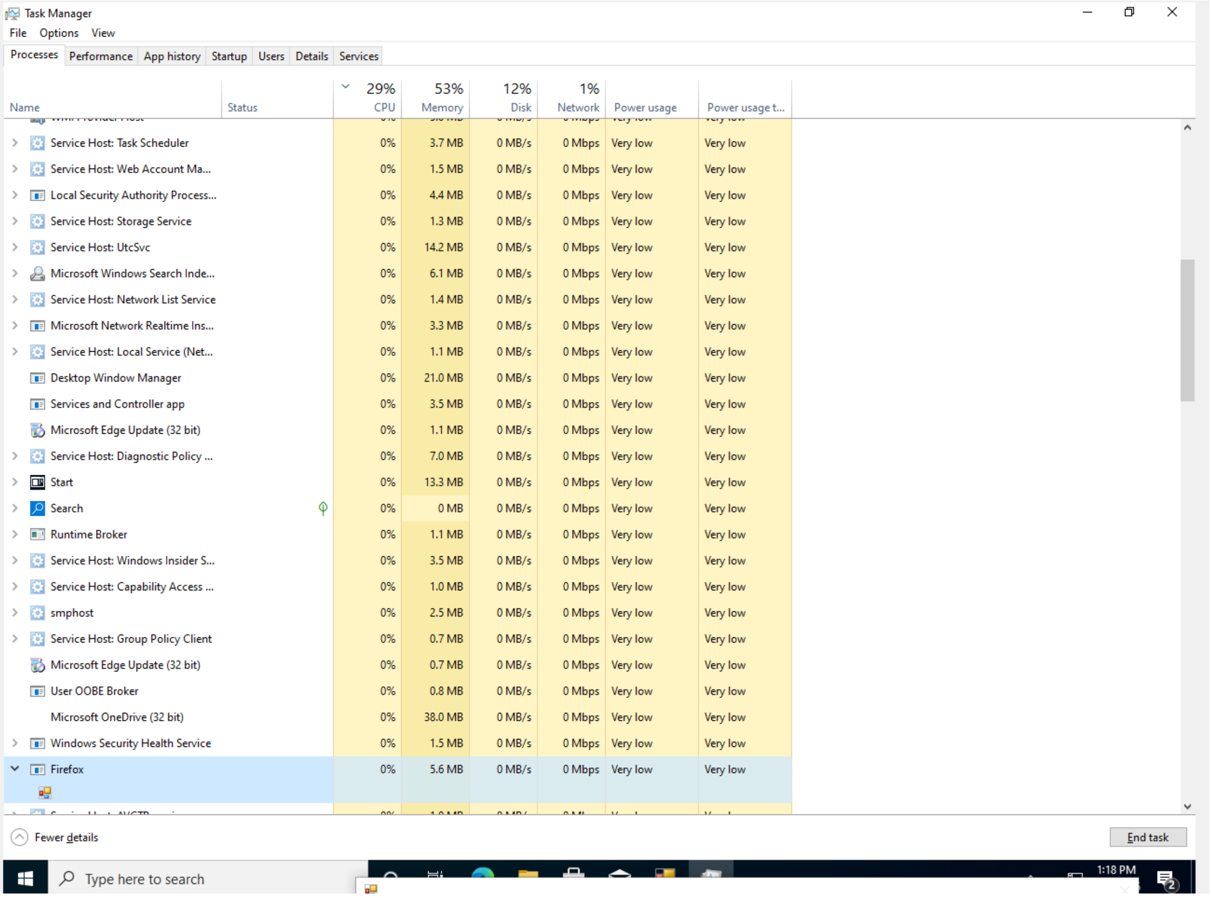
In the file description section, we see the program that the malware is impersonating. At first glance, firefox itself does not seem suspicious because it is the name of an ordinary web browser, but ...



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

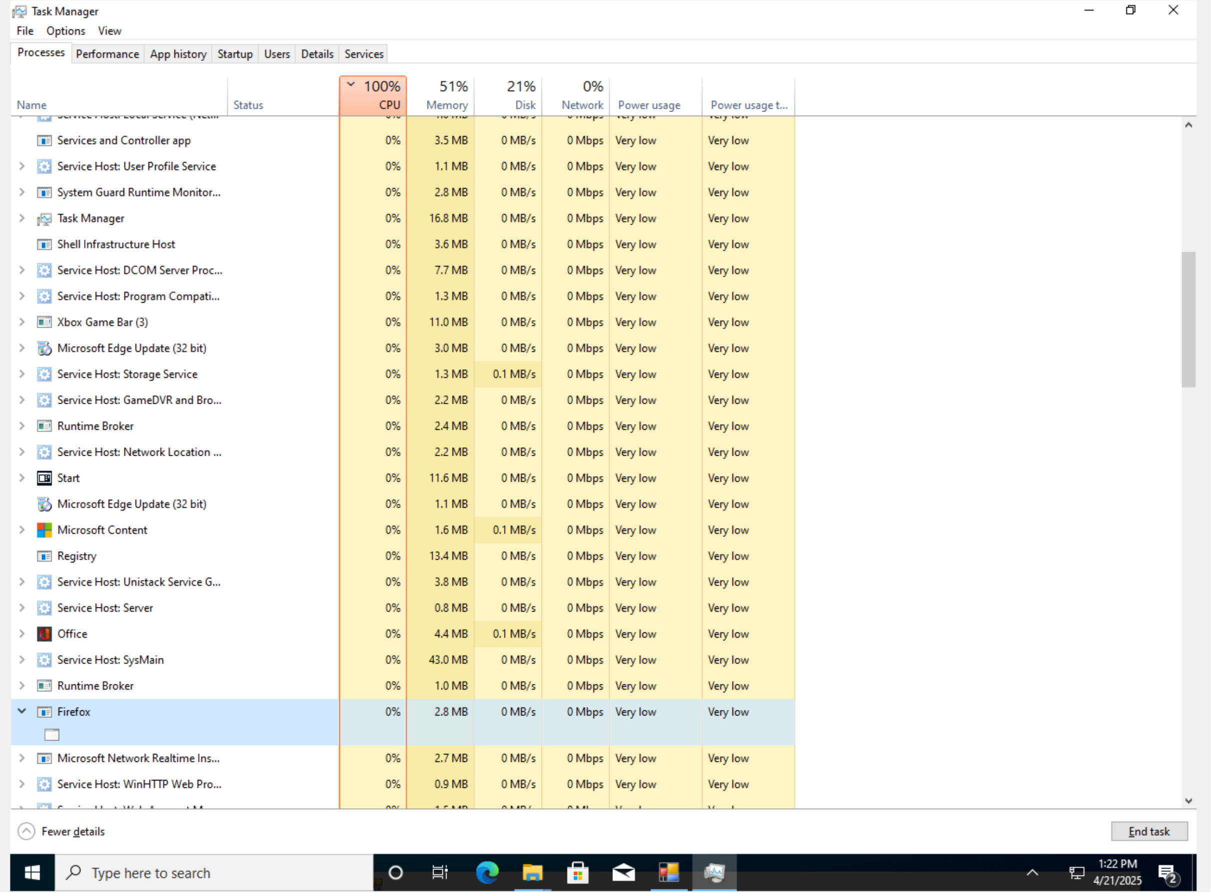
In the Original file name section, we see the real name of the application that is overwritten as the browser.

After reconnaissance on the Internet or available sources, we can find information that BitcoinBlackmailer is malware, and according to the definition of malware, such software can impersonate other programs to deceive the vigilance of the attacked user.



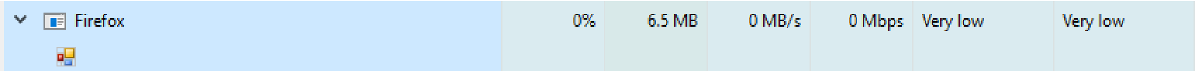
Name	Status	29% CPU	53% Memory	12% Disk	1% Network	Power usage	Power usage t...
Service Host: Task Scheduler		0%	3.7 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Web Account Ma...		0%	1.5 MB	0 MB/s	0 Mbps	Very low	Very low
Local Security Authority Process...		0%	4.4 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Storage Service		0%	1.3 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: UtcSvc		0%	14.2 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Windows Search Inde...		0%	6.1 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Network List Service		0%	1.4 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Network Realtime Ins...		0%	3.3 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Local Service (Net...		0%	1.1 MB	0 MB/s	0 Mbps	Very low	Very low
Desktop Window Manager		0%	21.0 MB	0 MB/s	0 Mbps	Very low	Very low
Services and Controller app		0%	3.5 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Edge Update (32 bit)		0%	1.1 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Diagnostic Policy ...		0%	7.0 MB	0 MB/s	0 Mbps	Very low	Very low
Start		0%	13.3 MB	0 MB/s	0 Mbps	Very low	Very low
Search	φ	0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker		0%	1.1 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Windows Insider S...		0%	3.5 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Capability Access ...		0%	1.0 MB	0 MB/s	0 Mbps	Very low	Very low
smphost		0%	2.5 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Group Policy Client		0%	0.7 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Edge Update (32 bit)		0%	0.7 MB	0 MB/s	0 Mbps	Very low	Very low
User OOBE Broker		0%	0.8 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft OneDrive (32 bit)		0%	38.0 MB	0 MB/s	0 Mbps	Very low	Very low
Windows Security Health Service		0%	1.5 MB	0 MB/s	0 Mbps	Very low	Very low
Firefox		0%	5.6 MB	0 MB/s	0 Mbps	Very low	Very low

Now let's go to the task manager to see what happened there.



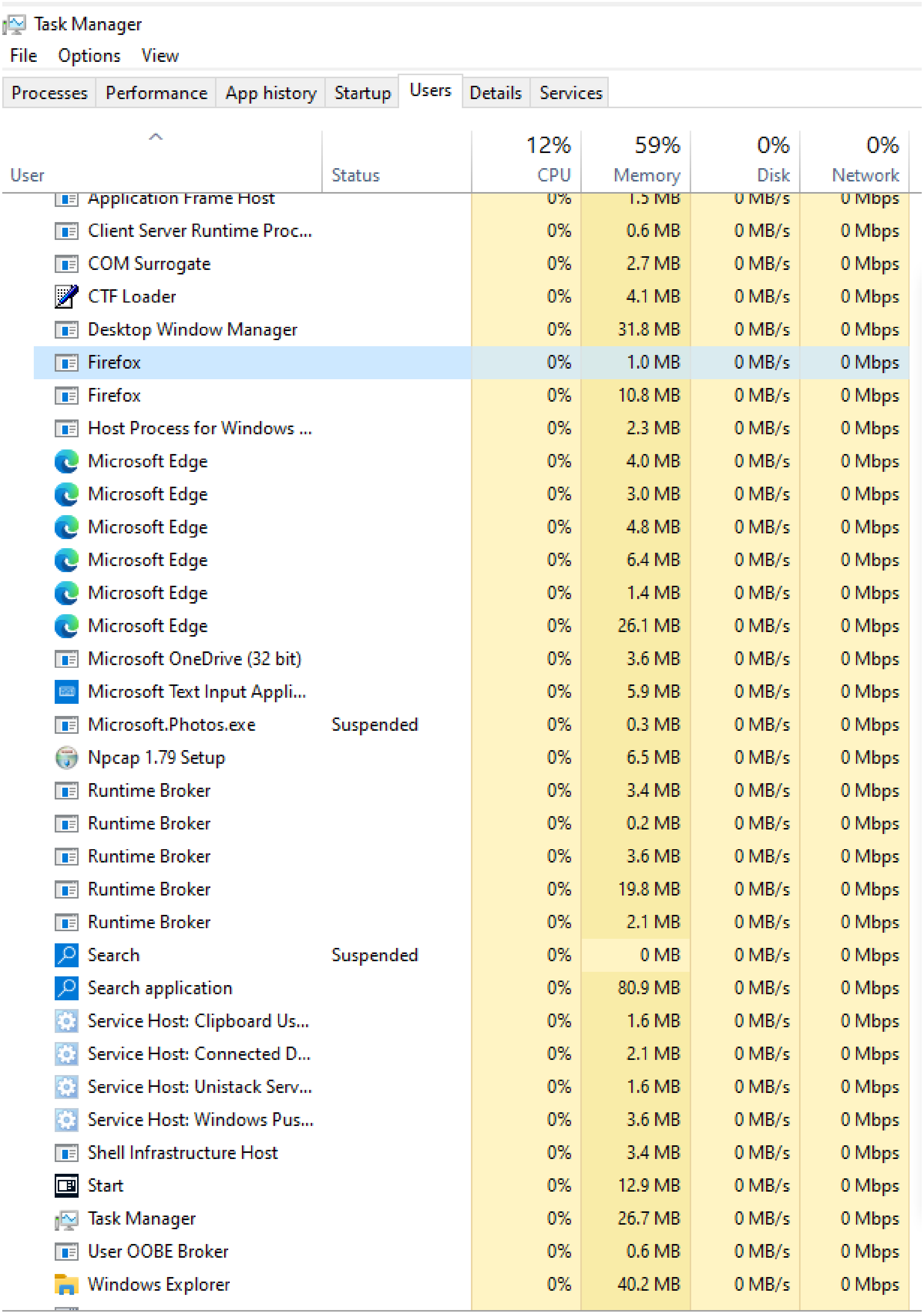
Name	Status	100% CPU	51% Memory	21% Disk	0% Network	Power usage	Power usage t...
Services and Controller app		0%	3.5 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: User Profile Service		0%	1.1 MB	0 MB/s	0 Mbps	Very low	Very low
System Guard Runtime Monitor...		0%	2.8 MB	0 MB/s	0 Mbps	Very low	Very low
Task Manager		0%	16.8 MB	0 MB/s	0 Mbps	Very low	Very low
Shell Infrastructure Host		0%	3.6 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: DCOM Server Proc...		0%	7.7 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Program Compati...		0%	1.3 MB	0 MB/s	0 Mbps	Very low	Very low
Xbox Game Bar (3)		0%	11.0 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Edge Update (32 bit)		0%	3.0 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Storage Service		0%	1.3 MB	0.1 MB/s	0 Mbps	Very low	Very low
Service Host: GameDVR and Bro...		0%	2.2 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker		0%	2.4 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Network Location ...		0%	2.2 MB	0 MB/s	0 Mbps	Very low	Very low
Start		0%	11.6 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Edge Update (32 bit)		0%	1.1 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Content		0%	1.6 MB	0.1 MB/s	0 Mbps	Very low	Very low
Registry		0%	13.4 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Unistack Service G...		0%	3.8 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: Server		0%	0.8 MB	0 MB/s	0 Mbps	Very low	Very low
Office		0%	4.4 MB	0.1 MB/s	0 Mbps	Very low	Very low
Service Host: SysMain		0%	43.0 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker		0%	1.0 MB	0 MB/s	0 Mbps	Very low	Very low
Firefox		0%	2.8 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Network Realtime Ins...		0%	2.7 MB	0 MB/s	0 Mbps	Very low	Very low
Service Host: WinHTTP Web Pro...		0%	0.9 MB	0 MB/s	0 Mbps	Very low	Very low

We can notice that every now and then it loads the processor and memory to a significant degree. We can see that firefox itself does not load the components, but the ransomware we are interested in does not give results or information regarding the load on the computer.



Name	CPU	Memory	Disk	Network	Power usage	Power usage t...
Firefox	0%	6.5 MB	0 MB/s	0 Mbps	Very low	Very low

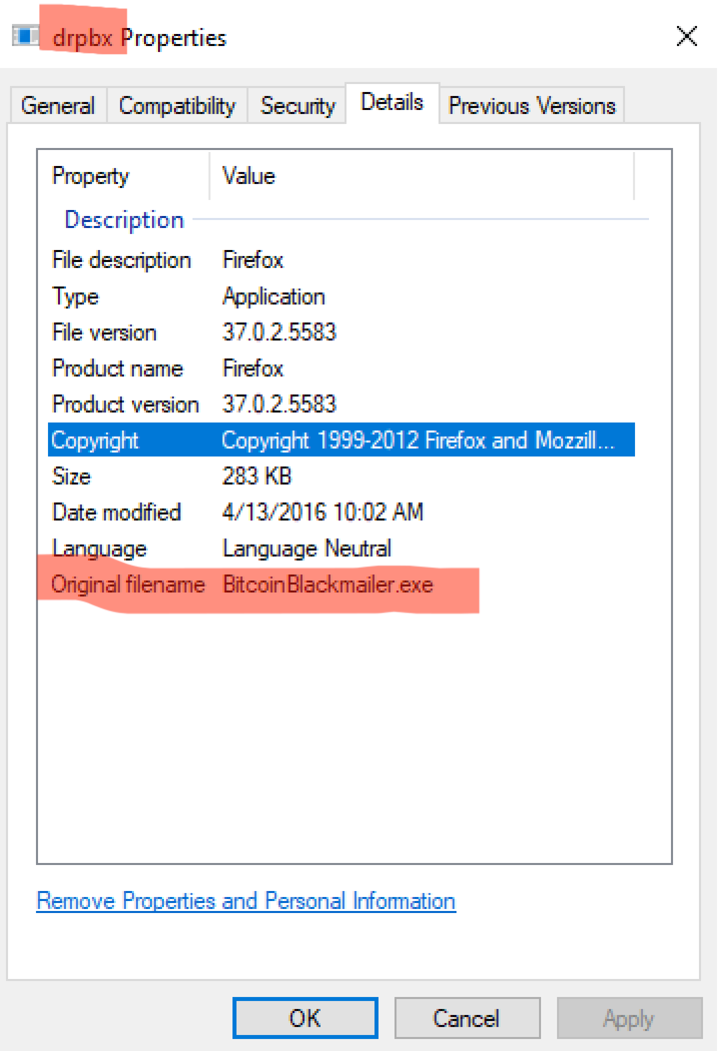
The screenshot above shows the program and the malware impersonating it.



User	Status	12% CPU	59% Memory	0% Disk	0% Network
Application Frame Host		0%	1.5 MB	0 MB/s	0 Mbps
Client Server Runtime Proc...		0%	0.6 MB	0 MB/s	0 Mbps
COM Surrogate		0%	2.7 MB	0 MB/s	0 Mbps
CTF Loader		0%	4.1 MB	0 MB/s	0 Mbps
Desktop Window Manager		0%	31.8 MB	0 MB/s	0 Mbps
Firefox		0%	1.0 MB	0 MB/s	0 Mbps
Firefox		0%	10.8 MB	0 MB/s	0 Mbps
Host Process for Windows ...		0%	2.3 MB	0 MB/s	0 Mbps
Microsoft Edge		0%	4.0 MB	0 MB/s	0 Mbps
Microsoft Edge		0%	3.0 MB	0 MB/s	0 Mbps
Microsoft Edge		0%	4.8 MB	0 MB/s	0 Mbps
Microsoft Edge		0%	6.4 MB	0 MB/s	0 Mbps
Microsoft Edge		0%	1.4 MB	0 MB/s	0 Mbps
Microsoft Edge		0%	26.1 MB	0 MB/s	0 Mbps
Microsoft OneDrive (32 bit)		0%	3.6 MB	0 MB/s	0 Mbps
Microsoft Text Input Appli...		0%	5.9 MB	0 MB/s	0 Mbps
Microsoft.Photos.exe	Suspended	0%	0.3 MB	0 MB/s	0 Mbps
Npcap 1.79 Setup		0%	6.5 MB	0 MB/s	0 Mbps
Runtime Broker		0%	3.4 MB	0 MB/s	0 Mbps
Runtime Broker		0%	0.2 MB	0 MB/s	0 Mbps
Runtime Broker		0%	3.6 MB	0 MB/s	0 Mbps
Runtime Broker		0%	19.8 MB	0 MB/s	0 Mbps
Runtime Broker		0%	2.1 MB	0 MB/s	0 Mbps
Search	Suspended	0%	0 MB	0 MB/s	0 Mbps
Search application		0%	80.9 MB	0 MB/s	0 Mbps
Service Host: Clipboard Us...		0%	1.6 MB	0 MB/s	0 Mbps
Service Host: Connected D...		0%	2.1 MB	0 MB/s	0 Mbps
Service Host: Unistack Serv...		0%	1.6 MB	0 MB/s	0 Mbps
Service Host: Windows Pus...		0%	3.6 MB	0 MB/s	0 Mbps
Shell Infrastructure Host		0%	3.4 MB	0 MB/s	0 Mbps
Start		0%	12.9 MB	0 MB/s	0 Mbps
Task Manager		0%	26.7 MB	0 MB/s	0 Mbps
User OOBE Broker		0%	0.6 MB	0 MB/s	0 Mbps
Windows Explorer		0%	40.2 MB	0 MB/s	0 Mbps

In the Users tab, we see several firefoxes fired up even though they are not physically running on the computer. Of course, we are talking about our only user here.

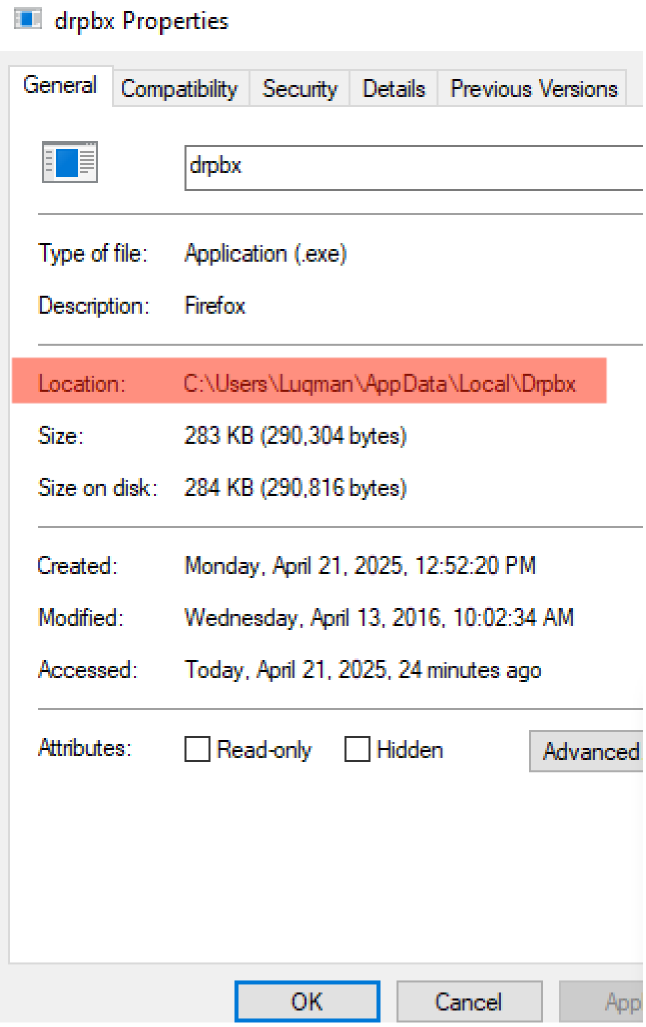
Let's see what's hidden in these running applications.



drpbx Properties

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

In the areas highlighted in red, we see more disturbing incidents. One that has been detected before and drpbx which is rather inconsistent with web browsers.



drpbx Properties

drpbx

Type of file: Application (.exe)

Description: Firefox

Location: C:\Users\Luqman\AppData\Local\Drpbx

Size: 283 KB (290,304 bytes)

Size on disk: 284 KB (290,816 bytes)

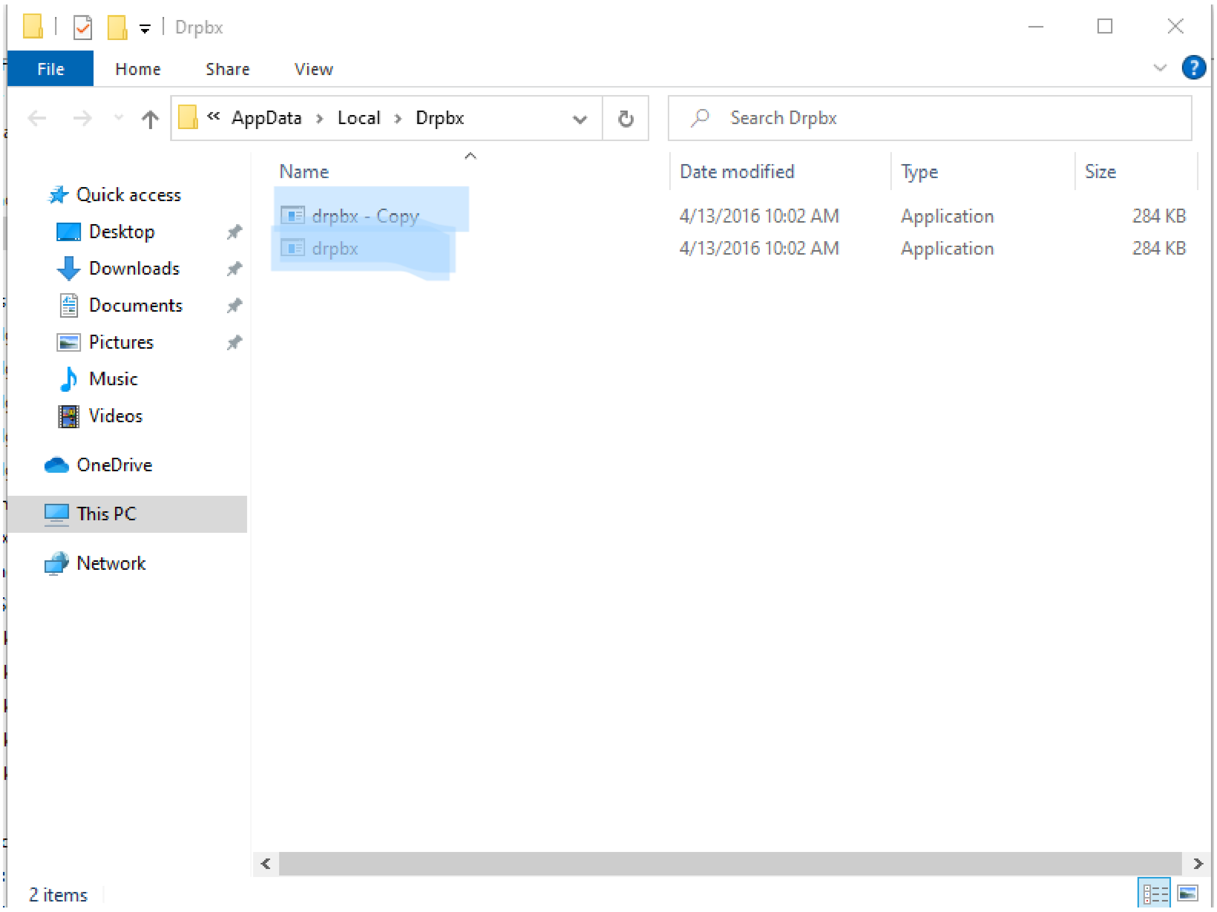
Created: Monday, April 21, 2025, 12:52:20 PM

Modified: Wednesday, April 13, 2016, 10:02:34 AM

Accessed: Today, April 21, 2025, 24 minutes ago

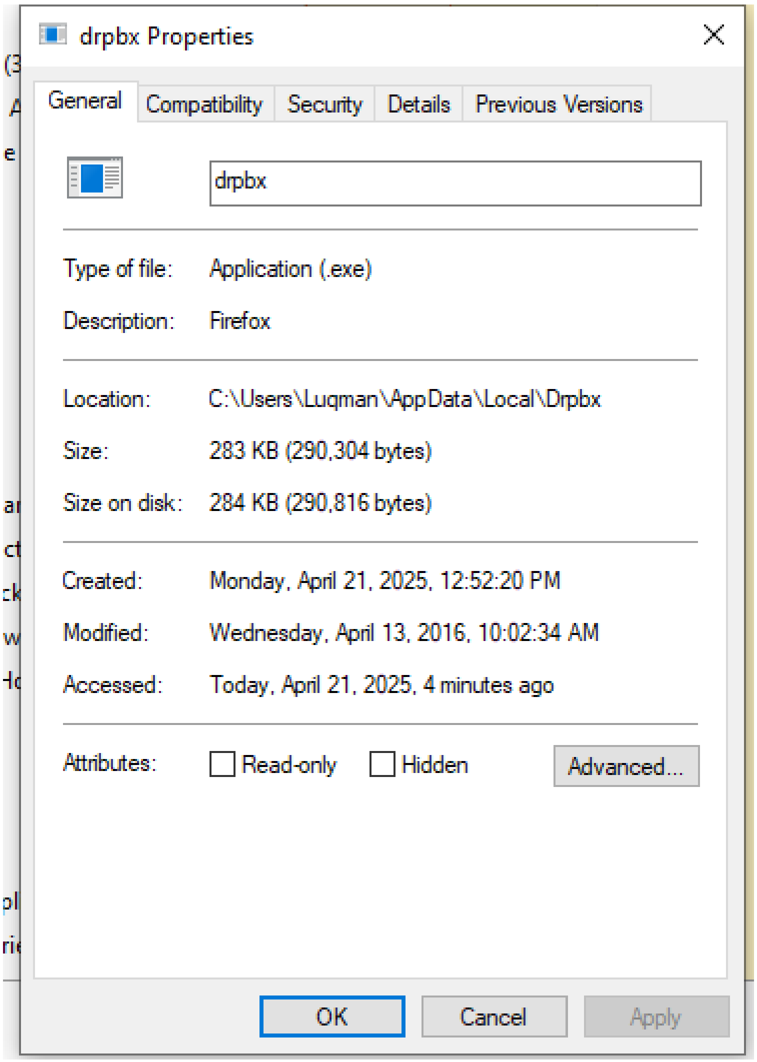
Attributes: □ Read-only □ Hidden

We see the location of the suspected file let's check it.



Name	Date modified	Type	Size
drpbx - Copy	4/13/2016 10:02 AM	Application	284 KB
drpbx	4/13/2016 10:02 AM	Application	284 KB

We see two more infected files in this location.



drpbx

Type of file: Application (.exe)

Description: Firefox

Location: C:\Users\Luqman\AppData\Local\Drpbx

Size: 283 KB (290,304 bytes)

Size on disk: 284 KB (290,816 bytes)

Created: Monday, April 21, 2025, 12:52:20 PM

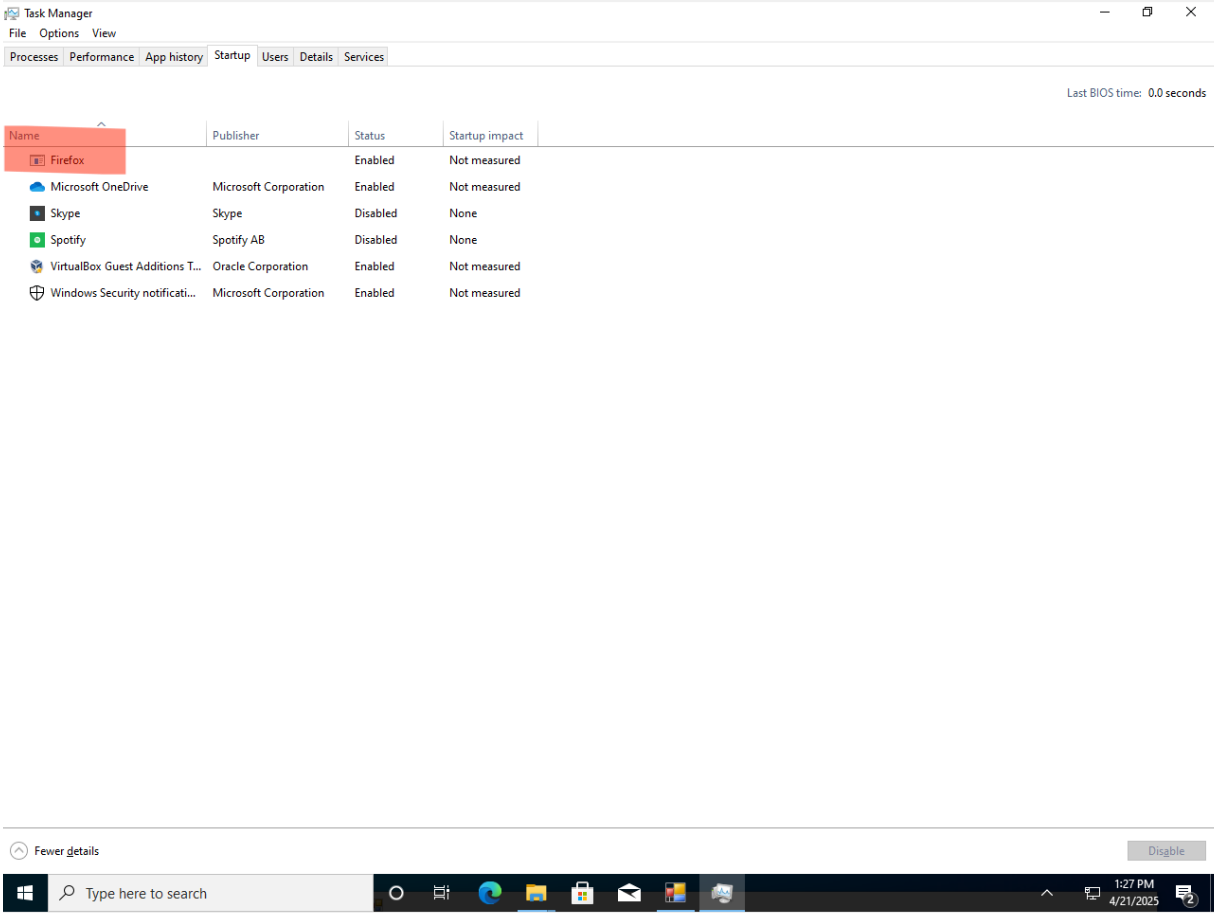
Modified: Wednesday, April 13, 2016, 10:02:34 AM

Accessed: Today, April 21, 2025, 4 minutes ago

Attributes: □ Read-only □ Hidden

In the second case, we have the same situation.

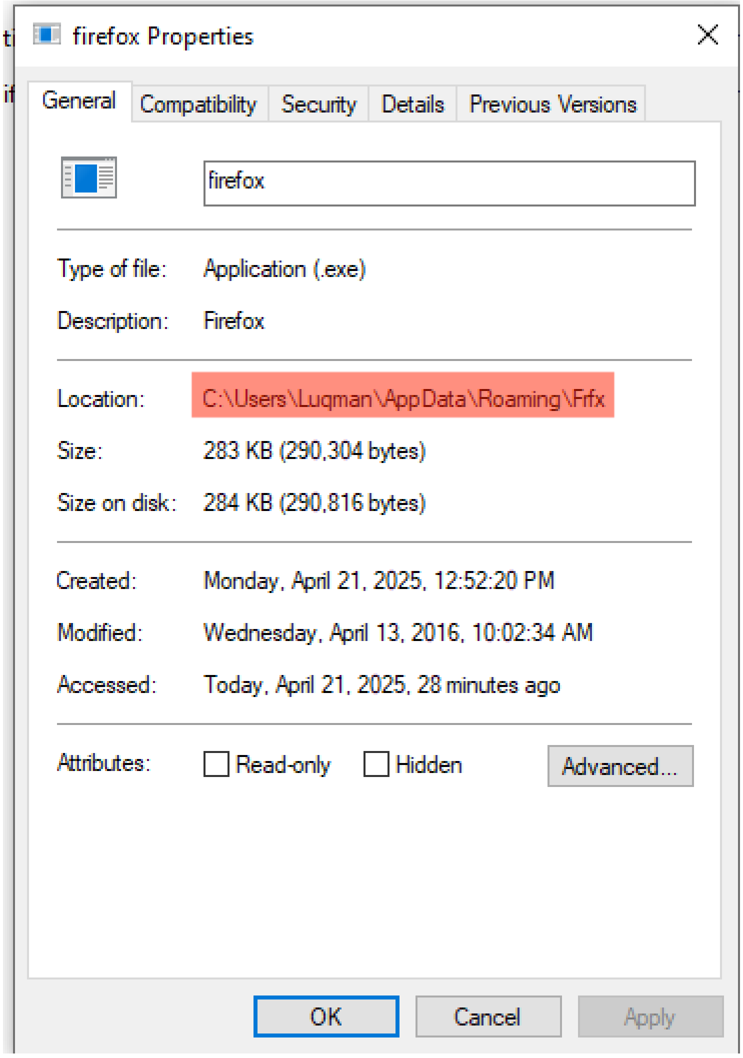
It refers again to dprbx which is just infected.



Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Last BIOS time: 0.0 seconds
Fewer details
Disable
Type here to search
1:27 PM
4/21/2025

Name	Publisher	Status	Startup impact
Firefox		Enabled	Not measured
Microsoft OneDrive	Microsoft Corporation	Enabled	Not measured
Skype	Skype	Disabled	None
Spotify	Spotify AB	Disabled	None
VirtualBox Guest Additions T...	Oracle Corporation	Enabled	Not measured
Windows Security notificati...	Microsoft Corporation	Enabled	Not measured

In the Startup section, we see our potential malware infection.



firefox

Type of file: Application (.exe)

Description: Firefox

Location: C:\Users\Luqman\AppData\Roaming\Frfx

Size: 283 KB (290,304 bytes)

Size on disk: 284 KB (290,816 bytes)

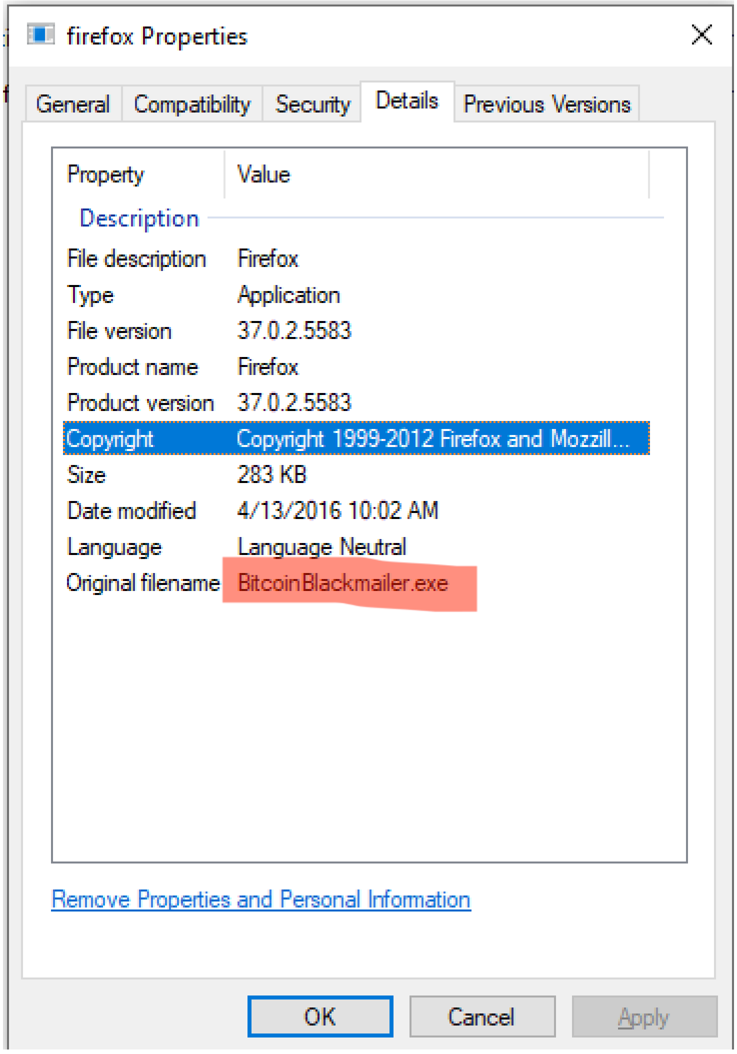
Created: Monday, April 21, 2025, 12:52:20 PM

Modified: Wednesday, April 13, 2016, 10:02:34 AM

Accessed: Today, April 21, 2025, 28 minutes ago

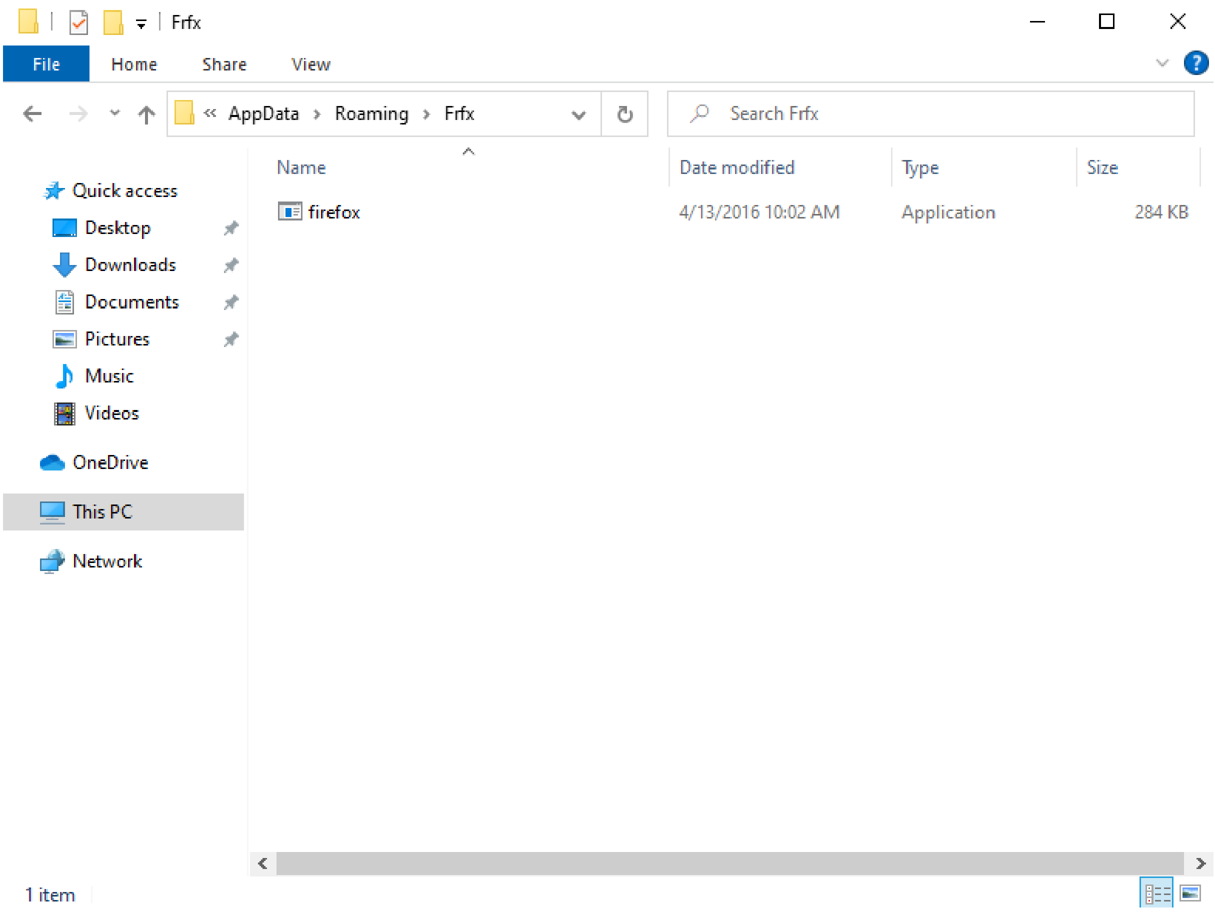
Attributes: □ Read-only □ Hidden

After checking in the properties section, we can find the location of this software



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

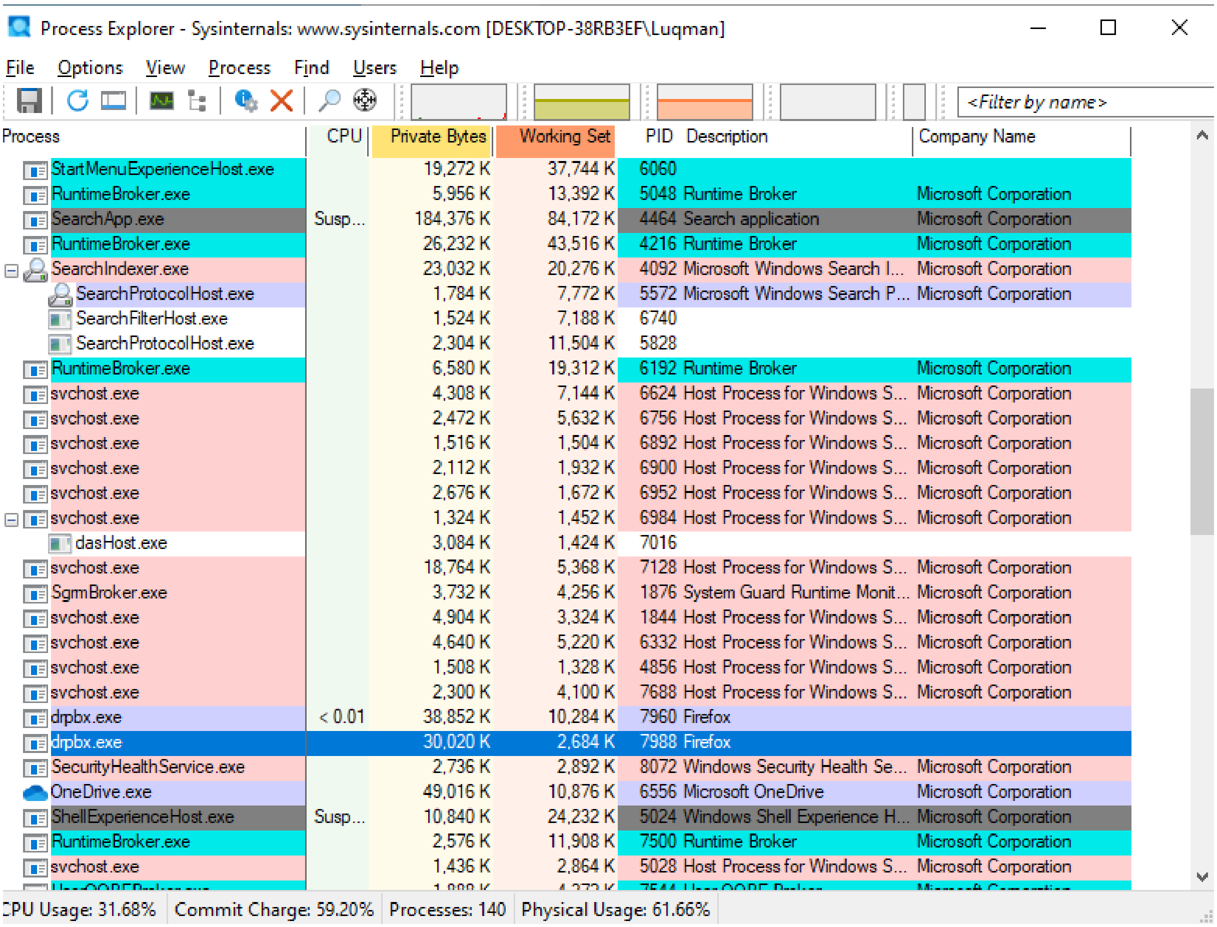
To make sure and confirm that I am dealing with the same thing, I check the program information in detail and everything agrees with the original findings found at the very beginning.



Name	Date modified	Type	Size
firefox	4/13/2016 10:02 AM	Application	284 KB

After checking the location found in the details, we find only one file which is just malicious.

At this point we have the culprit of this user's troubles with the computer.



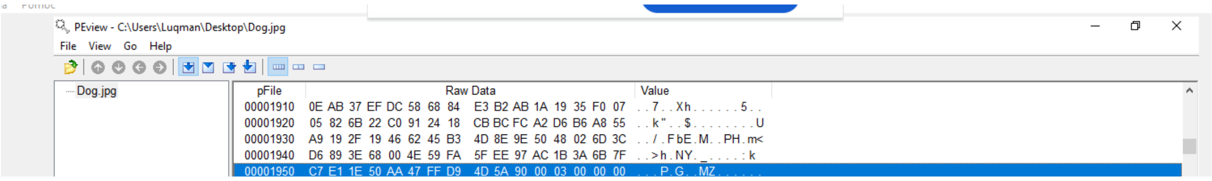
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38RB3EF\Luqman]
File
Options
View
Process
Find
Users
Help
<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
StartMenuExperienceHost.exe		19,272 K	37,744 K	6060		
RuntimeBroker.exe		5,956 K	13,392 K	5048	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	184,376 K	84,172 K	4464	Search application	Microsoft Corporation
RuntimeBroker.exe		26,232 K	43,516 K	4216	Runtime Broker	Microsoft Corporation
⊟ SearchIndexer.exe		23,032 K	20,276 K	4092	Microsoft Windows Search I...	Microsoft Corporation
SearchProtocolHost.exe		1,784 K	7,772 K	5572	Microsoft Windows Search P...	Microsoft Corporation
SearchFilterHost.exe		1,524 K	7,188 K	6740		
SearchProtocolHost.exe		2,304 K	11,504 K	5828		
RuntimeBroker.exe		6,580 K	19,312 K	6192	Runtime Broker	Microsoft Corporation
svchost.exe		4,308 K	7,144 K	6624	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,472 K	5,632 K	6756	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,516 K	1,504 K	6892	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,112 K	1,932 K	6900	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,676 K	1,672 K	6952	Host Process for Windows S...	Microsoft Corporation
⊟ svchost.exe		1,324 K	1,452 K	6984	Host Process for Windows S...	Microsoft Corporation
dasHost.exe		3,084 K	1,424 K	7016		
svchost.exe		18,764 K	5,368 K	7128	Host Process for Windows S...	Microsoft Corporation
SgrmBroker.exe		3,732 K	4,256 K	1876	System Guard Runtime Monit...	Microsoft Corporation
svchost.exe		4,904 K	3,324 K	1844	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,640 K	5,220 K	6332	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,508 K	1,328 K	4856	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,300 K	4,100 K	7688	Host Process for Windows S...	Microsoft Corporation
drpbx.exe	< 0.01	38,852 K	10,284 K	7960	Firefox	
drpbx.exe		30,020 K	2,684 K	7988	Firefox	
SecurityHealthService.exe		2,736 K	2,892 K	8072	Windows Security Health Se...	Microsoft Corporation
OneDrive.exe		49,016 K	10,876 K	6556	Microsoft OneDrive	Microsoft Corporation
ShellExperienceHost.exe	Susp...	10,840 K	24,232 K	5024	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		2,576 K	11,908 K	7500	Runtime Broker	Microsoft Corporation
svchost.exe		1,436 K	2,864 K	5028	Host Process for Windows S...	Microsoft Corporation
UserOOBEBroker.exe		1,888 K	4,372 K	7544	User OOBE Broker	Microsoft Corporation

CPU Usage: 31.68% Commit Charge: 59.20% Processes: 140 Physical Usage: 61.66%

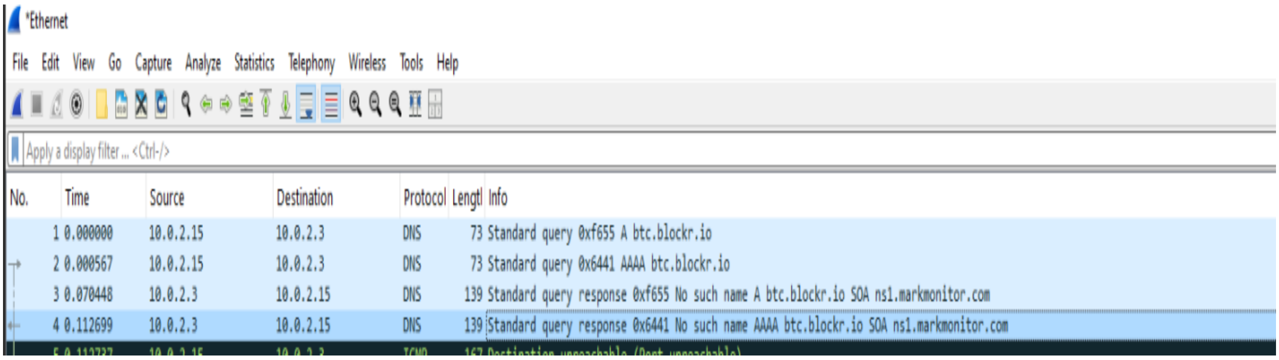
When we start explorer process we see two processes:

dpbx.exe despite the fact that they have a different PID they refer to our infected file.



```
pFile     Raw Data                                          Value
00001910  0E AB 37 EF DC 58 68 84  E3 B2 AB 1A 19 35 F0 07  ..7..Xh.......5..
00001920  05 82 6B 22 C0 91 24 18  CB BC FC A2 D6 B6 A8 55  ..k"..$.........U
00001930  A9 19 2F 19 46 62 45 B3  4D 8E 9E 50 48 02 6D 3C  ../.FbE.M..PH.m<
00001940  D6 89 3E 68 00 4E 59 FA  5F EE 97 AC 1B 3A 6B 7F  ..>h.NY._.....:k
00001950  C7 E1 1E 50 AA 47 FF D9  4D 5A 90 00 03 00 00 00  ...P.G..MZ......
```

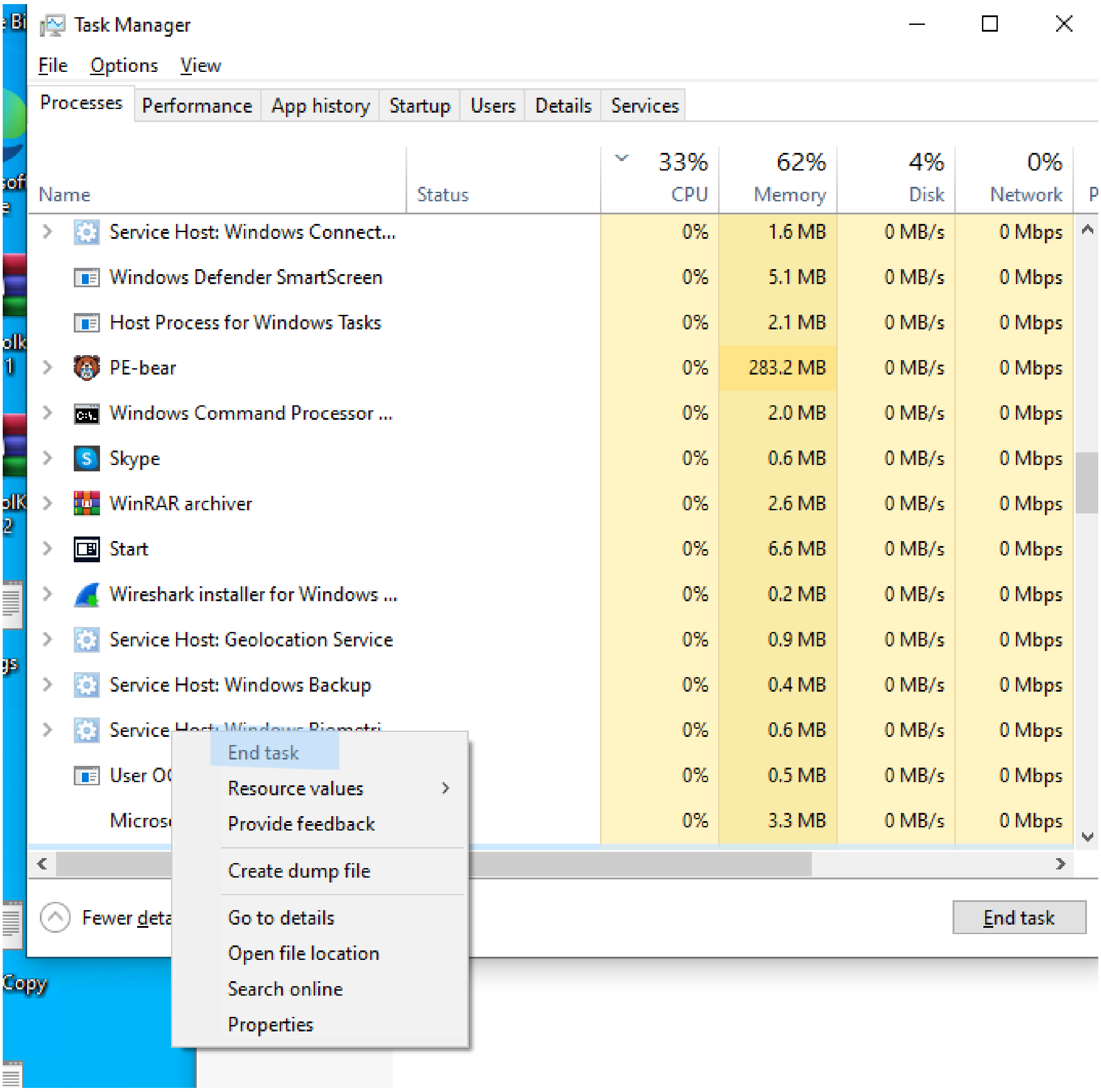
Here are the strings indicating the infection



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

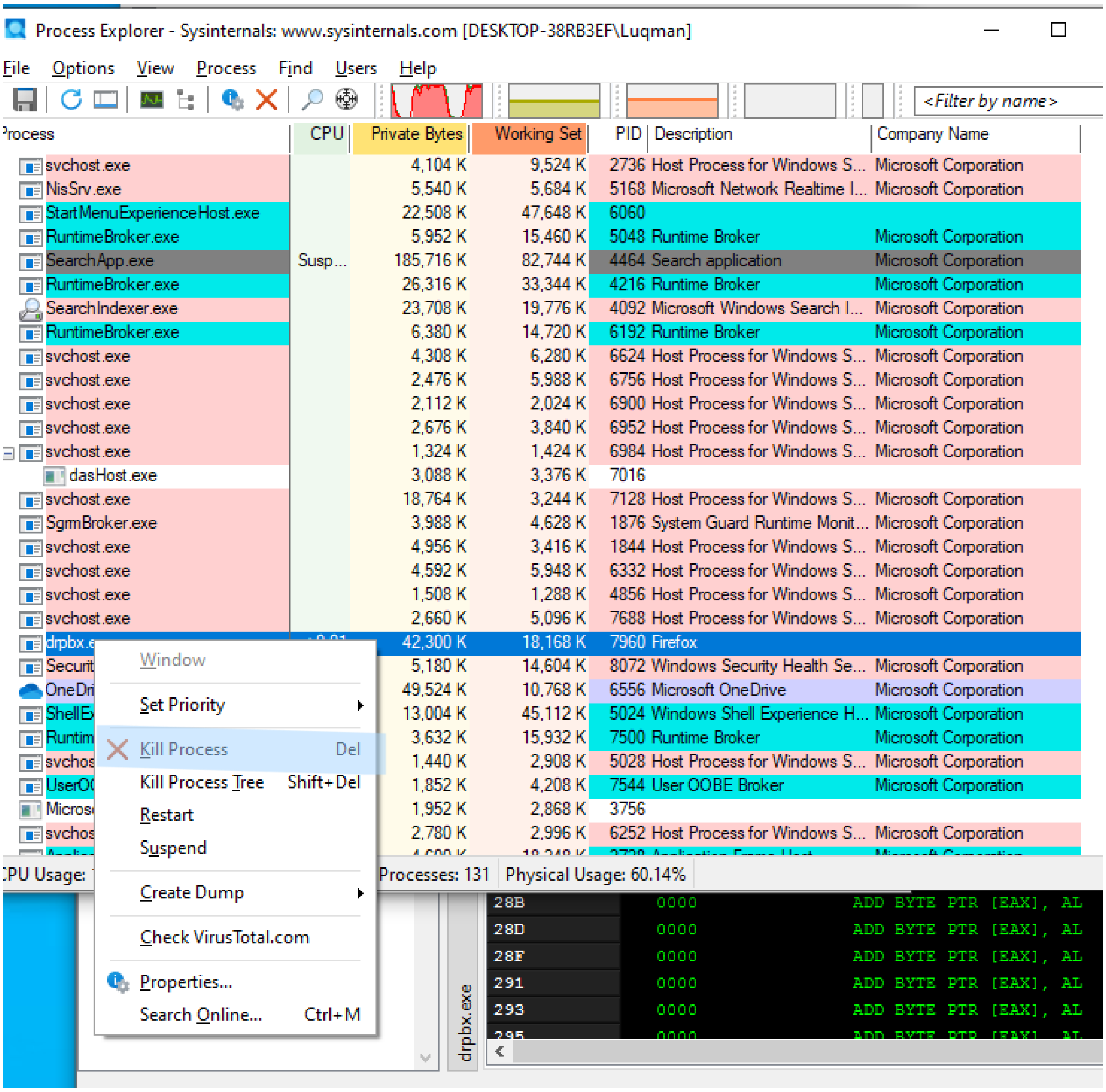
```
No. Time      Source     Destination  Protocol Lengtl Info
  1 0.000000  10.0.2.15  10.0.2.3     DNS       73 Standard query 0xf655 A btc.blockr.io
  2 0.000567  10.0.2.15  10.0.2.3     DNS       73 Standard query 0x6441 AAAA btc.blockr.io
  3 0.070448  10.0.2.3   10.0.2.15    DNS      139 Standard query response 0xf655 No such name A btc.blockr.io SOA ns1.markmonitor.com
  4 0.112699  10.0.2.3   10.0.2.15    DNS      139 Standard query response 0x6441 No such name AAAA btc.blockr.io SOA ns1.markmonitor.com
  5 0.112737  10.0.2.15  10.0.2.3     ICMP     167 Destination unreachable (Port unreachable)
```

Its confirm from wireshark.



Name	Status	33% CPU	62% Memory	4% Disk	0% Network
Service Host: Windows Connect...		0%	1.6 MB	0 MB/s	0 Mbps
Windows Defender SmartScreen		0%	5.1 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	2.1 MB	0 MB/s	0 Mbps
PE-bear		0%	283.2 MB	0 MB/s	0 Mbps
Windows Command Processor ...		0%	2.0 MB	0 MB/s	0 Mbps
Skype		0%	0.6 MB	0 MB/s	0 Mbps
WinRAR archiver		0%	2.6 MB	0 MB/s	0 Mbps
Start		0%	6.6 MB	0 MB/s	0 Mbps
Wireshark installer for Windows ...		0%	0.2 MB	0 MB/s	0 Mbps
Service Host: Geolocation Service		0%	0.9 MB	0 MB/s	0 Mbps
Service Host: Windows Backup		0%	0.4 MB	0 MB/s	0 Mbps
Service Host: Windows Biometri		0%	0.6 MB	0 MB/s	0 Mbps
User O		0%	0.5 MB	0 MB/s	0 Mbps
Micros		0%	3.3 MB	0 MB/s	0 Mbps

First Step: I choose to complete the task



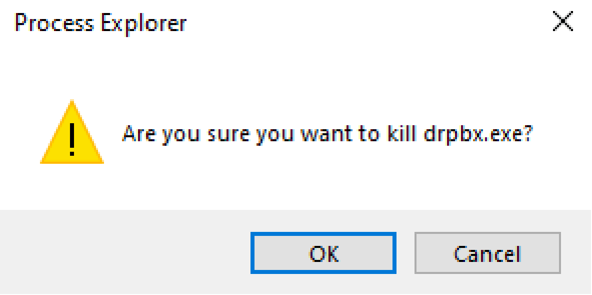
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38RB3EF\Luqman]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		4,104 K	9,524 K	2736	Host Process for Windows S...	Microsoft Corporation
NisSrv.exe		5,540 K	5,684 K	5168	Microsoft Network Realtime I...	Microsoft Corporation
StartMenuExperienceHost.exe		22,508 K	47,648 K	6060		
RuntimeBroker.exe		5,952 K	15,460 K	5048	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	185,716 K	82,744 K	4464	Search application	Microsoft Corporation
RuntimeBroker.exe		26,316 K	33,344 K	4216	Runtime Broker	Microsoft Corporation
SearchIndexer.exe		23,708 K	19,776 K	4092	Microsoft Windows Search I...	Microsoft Corporation
RuntimeBroker.exe		6,380 K	14,720 K	6192	Runtime Broker	Microsoft Corporation
svchost.exe		4,308 K	6,280 K	6624	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,476 K	5,988 K	6756	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,112 K	2,024 K	6900	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,676 K	3,840 K	6952	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,324 K	1,424 K	6984	Host Process for Windows S...	Microsoft Corporation
dasHost.exe		3,088 K	3,376 K	7016		
svchost.exe		18,764 K	3,244 K	7128	Host Process for Windows S...	Microsoft Corporation
SgrmBroker.exe		3,988 K	4,628 K	1876	System Guard Runtime Monit...	Microsoft Corporation
svchost.exe		4,956 K	3,416 K	1844	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,592 K	5,948 K	6332	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,508 K	1,288 K	4856	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,660 K	5,096 K	7688	Host Process for Windows S...	Microsoft Corporation
drpbx.e	< 0.01	42,300 K	18,168 K	7960	Firefox	
Securit		5,180 K	14,604 K	8072	Windows Security Health Se...	Microsoft Corporation
OneDri		49,524 K	10,768 K	6556	Microsoft OneDrive	Microsoft Corporation
ShellEx		13,004 K	45,112 K	5024	Windows Shell Experience H...	Microsoft Corporation
Runtim		3,632 K	15,932 K	7500	Runtime Broker	Microsoft Corporation
svchos		1,440 K	2,908 K	5028	Host Process for Windows S...	Microsoft Corporation
UserO(		1,852 K	4,208 K	7544	User OOBE Broker	Microsoft Corporation
Micros		1,952 K	2,868 K	3756		
svchos		2,780 K	2,996 K	6252	Host Process for Windows S...	Microsoft Corporation

CPU Usage: Processes: 131 Physical Usage: 60.14%

```
28B   0000   ADD BYTE PTR [EAX], AL
28D   0000   ADD BYTE PTR [EAX], AL
28F   0000   ADD BYTE PTR [EAX], AL
291   0000   ADD BYTE PTR [EAX], AL
293   0000   ADD BYTE PTR [EAX], AL
```

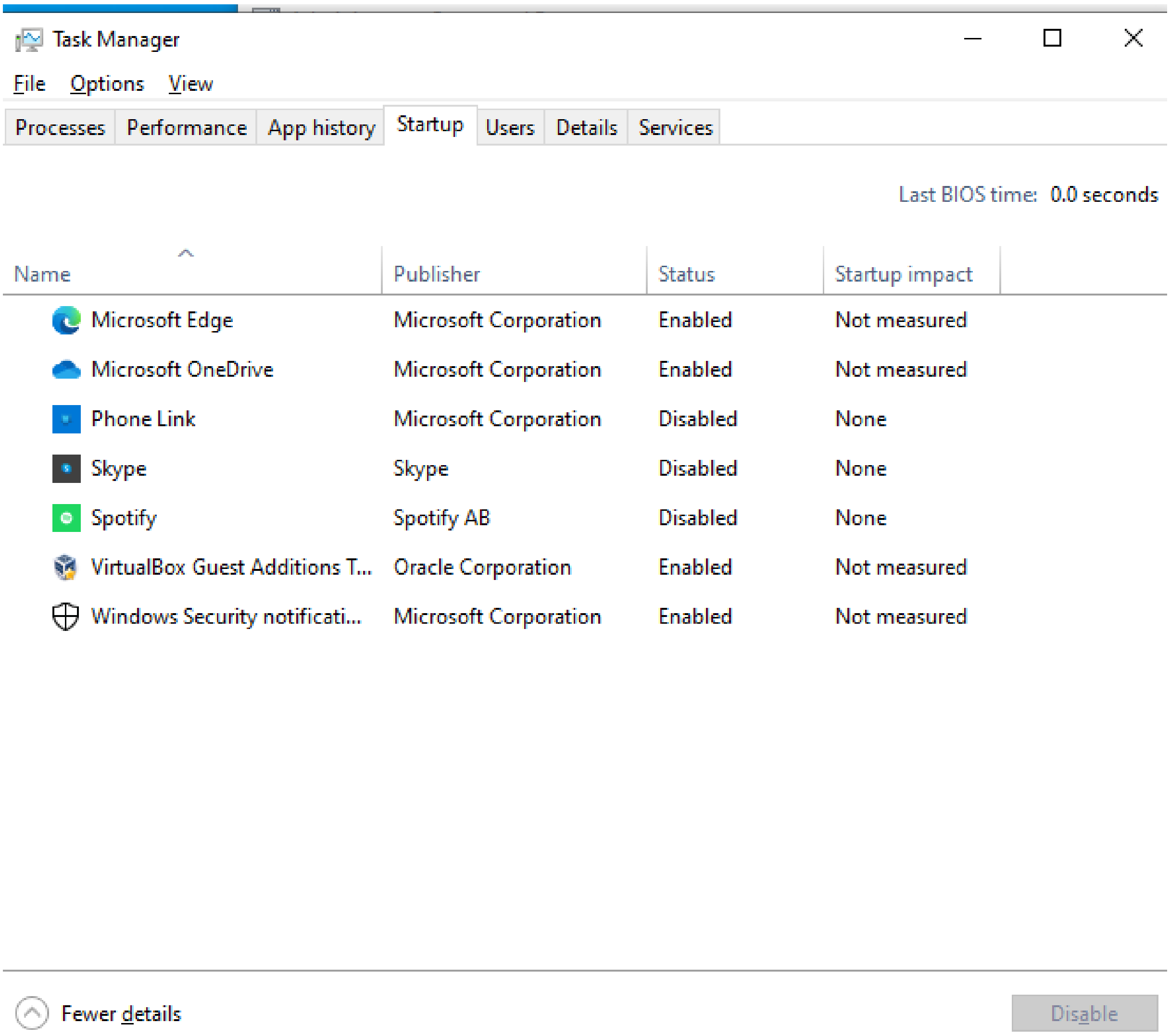
Second step: in process explorer finds infected processes and selects kill process option



Process Explorer

Are you sure you want to kill drpbx.exe?

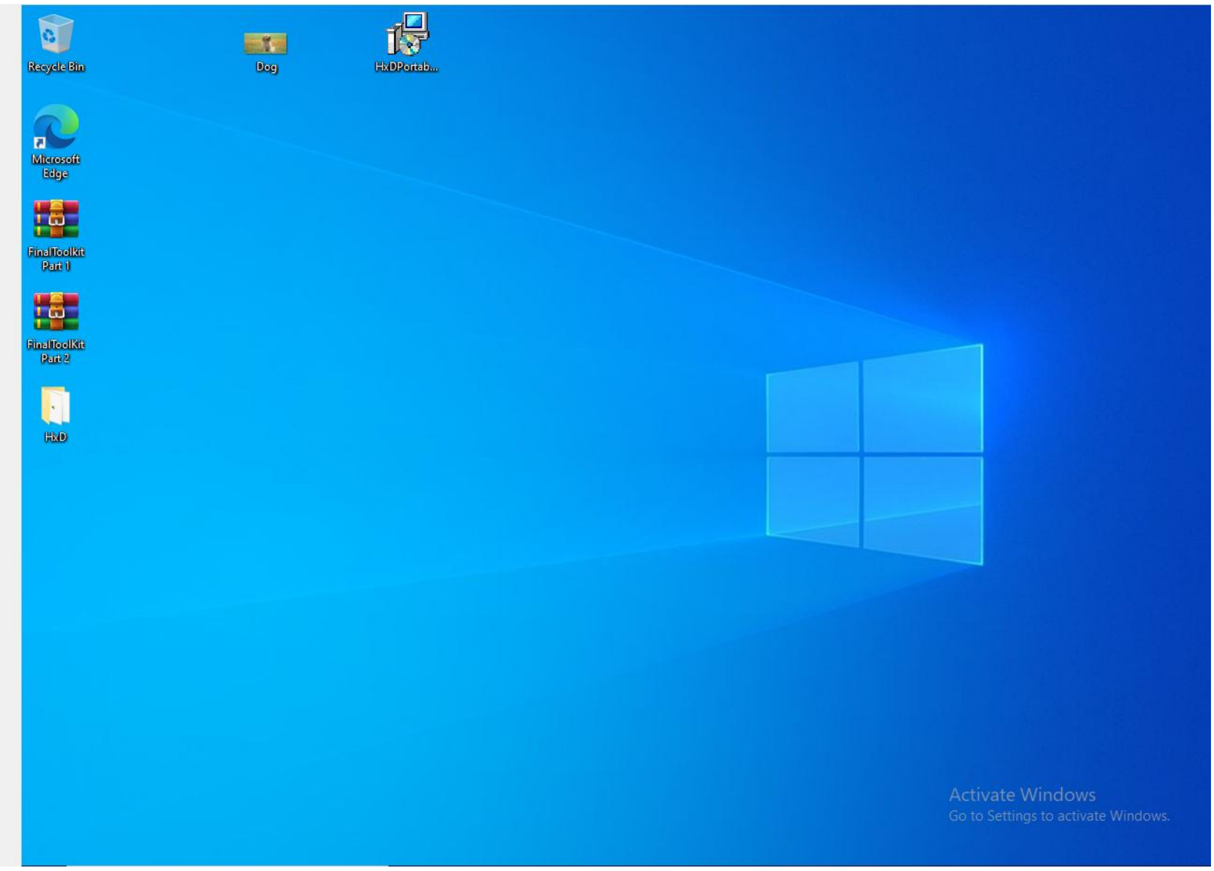
Third step: I confirm my willingness to remove the harmful proces


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
Disable

Last BIOS time: 0.0 seconds

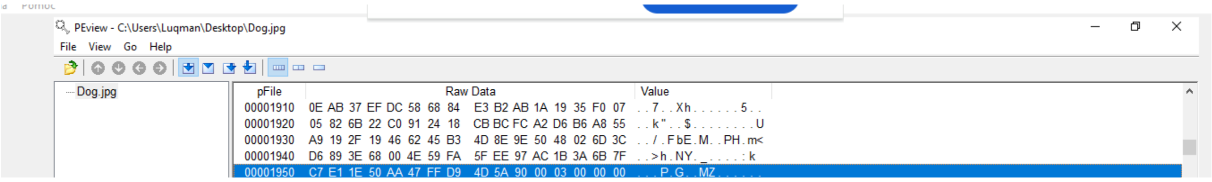
Name	Publisher	Status	Startup impact
Microsoft Edge	Microsoft Corporation	Enabled	Not measured
Microsoft OneDrive	Microsoft Corporation	Enabled	Not measured
Phone Link	Microsoft Corporation	Disabled	None
Skype	Skype	Disabled	None
Spotify	Spotify AB	Disabled	None
VirtualBox Guest Additions T...	Oracle Corporation	Enabled	Not measured
Windows Security notificati...	Microsoft Corporation	Enabled	Not measured

And final confirmation of the removal of harmful processes



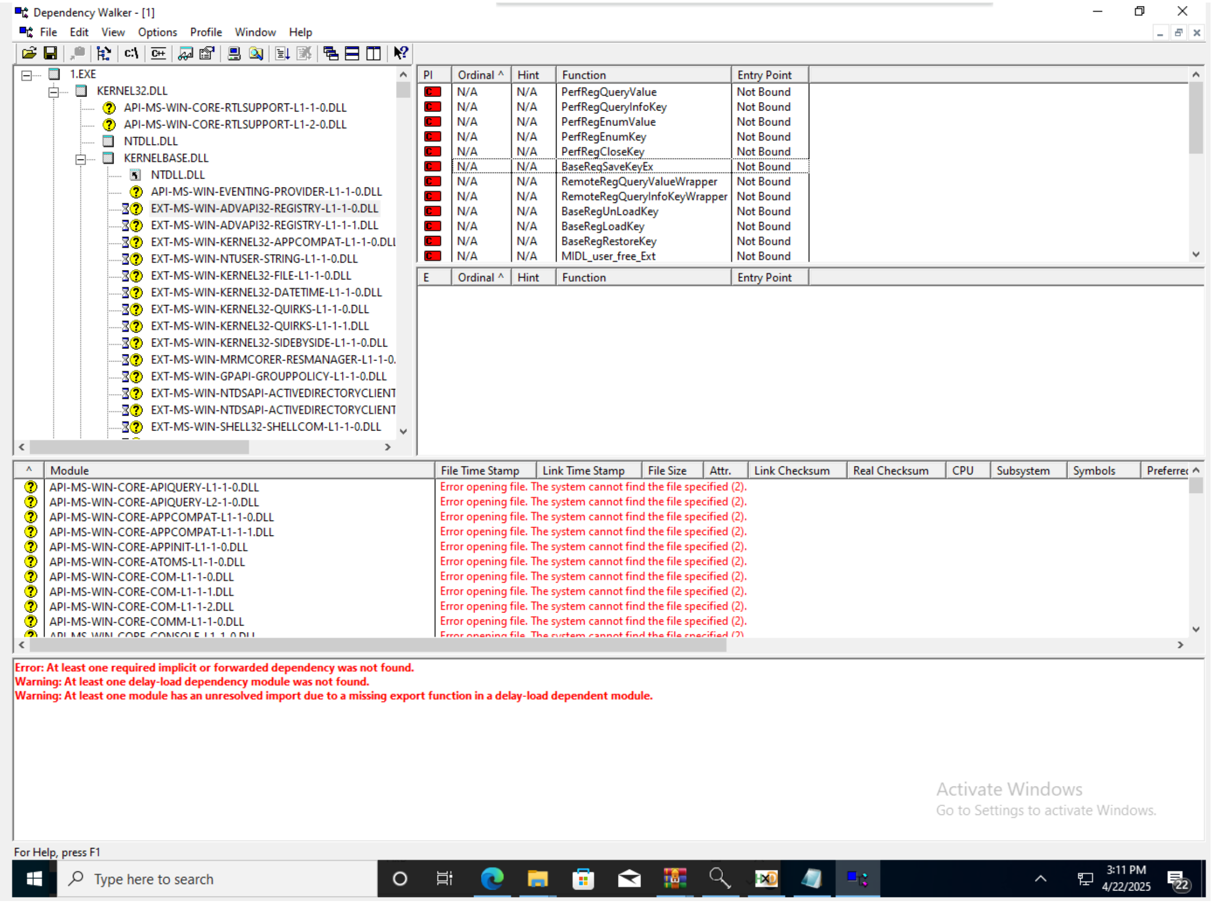
The malicious software operated by disguising the ransomware as the Firefox browser. While the process appeared to be Firefox and was visible in the system's process list, the actual browser window was not shown to the user. Instead, only the ransomware screen was displayed on the screen, making the deception invisible to the user.

Part 2



```
pFile     Raw Data                                         Value
00001910  0E AB 37 EF DC 58 68 84  E3 B2 AB 1A 19 35 F0 07  ..7..Xh.......5..
00001920  05 82 6B 22 C0 91 24 18  CB BC FC A2 D6 B6 A8 55  ..k"..$.........U
00001930  A9 19 2F 19 46 62 45 B3  4D 8E 9E 50 48 02 6D 3C  ../.FbE.M..PH.m<
00001940  D6 89 3E 68 00 4E 59 FA  5F EE 97 AC 1B 3A 6B 7F  ..>h.NY._.....:k
00001950  C7 E1 1E 50 AA 47 FF D9  4D 5A 90 00 03 00 00 00  ...P.G..MZ......
```

This image has increased magic bytes which indicates a nested program. 4D5A are magic bytes for .exe files.



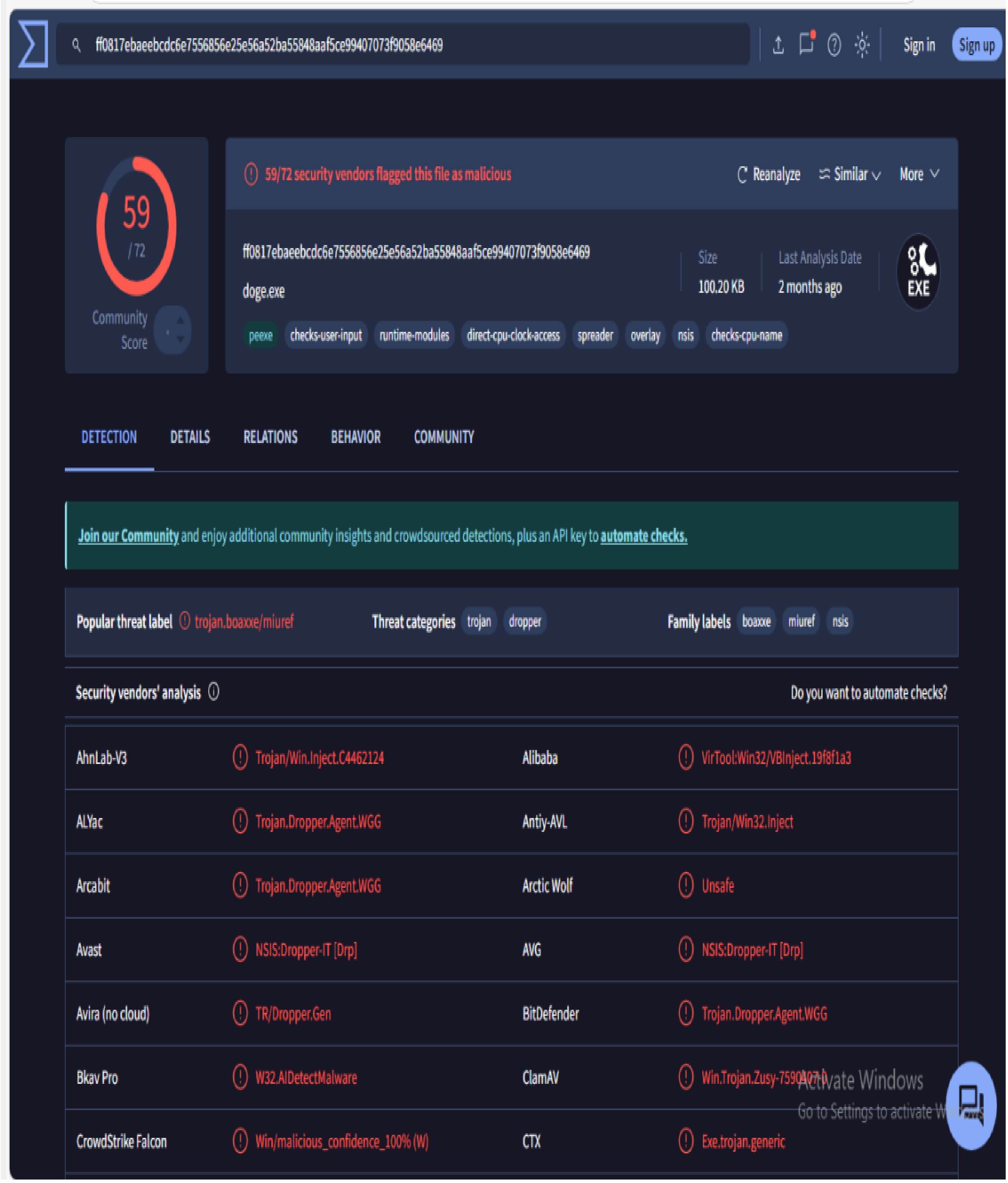
```
1.EXE
  KERNEL32.DLL
    API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
    API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
    NTDLL.DLL
    KERNELBASE.DLL
      NTDLL.DLL
      API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
      EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
      EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
      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
      EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
      EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
      EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL
      EXT-MS-WIN-KERNEL32-SIDEBYSIDE-L1-1-0.DLL
      EXT-MS-WIN-MRMCORER-RESMANAGER-L1-1-0.
      EXT-MS-WIN-GPAPI-GROUPPOLICY-L1-1-0.DLL
      EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT
      EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT
      EXT-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	N/A	PerfRegQueryValue	Not Bound
C	N/A	N/A	PerfRegQueryInfoKey	Not Bound
C	N/A	N/A	PerfRegEnumValue	Not Bound
C	N/A	N/A	PerfRegEnumKey	Not Bound
C	N/A	N/A	PerfRegCloseKey	Not Bound
C	N/A	N/A	BaseRegSaveKeyEx	Not Bound
C	N/A	N/A	RemoteRegQueryValueWrapper	Not Bound
C	N/A	N/A	RemoteRegQueryInfoKeyWrapper	Not Bound
C	N/A	N/A	BaseRegUnLoadKey	Not Bound
C	N/A	N/A	BaseRegLoadKey	Not Bound
C	N/A	N/A	BaseRegRestoreKey	Not Bound
C	N/A	N/A	MIDL_user_free_Ext	Not Bound

E	Ordinal ^	Hint	Function	Entry Point

```
^  Module                                  File Time Stamp  Link Time Stamp  File Size  Attr.  Link Checksum  Real Checksum  CPU  Subsystem  Symbols  Preferre
?  API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL     Error opening file. The system cannot find the file specified (2).
?  API-MS-WIN-CORE-APIQUERY-L2-1-0.DLL     Error opening file. The system cannot find the file specified (2).
?  API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL    Error opening file. The system cannot find the file specified (2).
?  API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL    Error opening file. The system cannot find the file specified (2).
?  API-MS-WIN-CORE-APPINIT-L1-1-0.DLL      Error opening file. The system cannot find the file specified (2).
?  API-MS-WIN-CORE-ATOMS-L1-1-0.DLL        Error opening file. The system cannot find the file specified (2).
?  API-MS-WIN-CORE-COM-L1-1-0.DLL          Error opening file. The system cannot find the file specified (2).
?  API-MS-WIN-CORE-COM-L1-1-1.DLL          Error opening file. The system cannot find the file specified (2).
?  API-MS-WIN-CORE-COM-L1-1-2.DLL          Error opening file. The system cannot find the file specified (2).
?  API-MS-WIN-CORE-COMM-L1-1-0.DLL         Error opening file. The system cannot find the file specified (2).
?  API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL      Error opening file. The system cannot find the file specified (2).
```

```
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```



ff0817ebaeebcdc6e7556856e25e56a52ba55848aaf5ce99407073f9058e6469

59
/ 72
Community Score

59/72 security vendors flagged this file as malicious

ff0817ebaeebcdc6e7556856e25e56a52ba55848aaf5ce99407073f9058e6469

doge.exe

Size: 100.20 KB

Last Analysis Date: 2 months ago

EXE

peexe · checks-user-input · runtime-modules · direct-cpu-clock-access · spreader · overlay · nsis · checks-cpu-name

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.boaxxe/miuref

Threat categories: trojan · dropper

Family labels: boaxxe · miuref · nsis

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win.Inject.C4462124	Alibaba	VirTool:Win32/VBInject.19f8f1a3
ALYac	Trojan.Dropper.Agent.WGG	Antiy-AVL	Trojan/Win32.Inject
Arcabit	Trojan.Dropper.Agent.WGG	Arctic Wolf	Unsafe
Avast	NSIS:Dropper-IT [Drp]	AVG	NSIS:Dropper-IT [Drp]
Avira (no cloud)	TR/Dropper.Gen	BitDefender	Trojan.Dropper.Agent.WGG
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Zusy-7590407-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.generic

This is confirm from totalvirus