**Malware Analysis Report: Jigsaw Ransomware - by Michał Botuliński**

*Prepared by: Michał Botuliński*
*Date:5.08.2023*

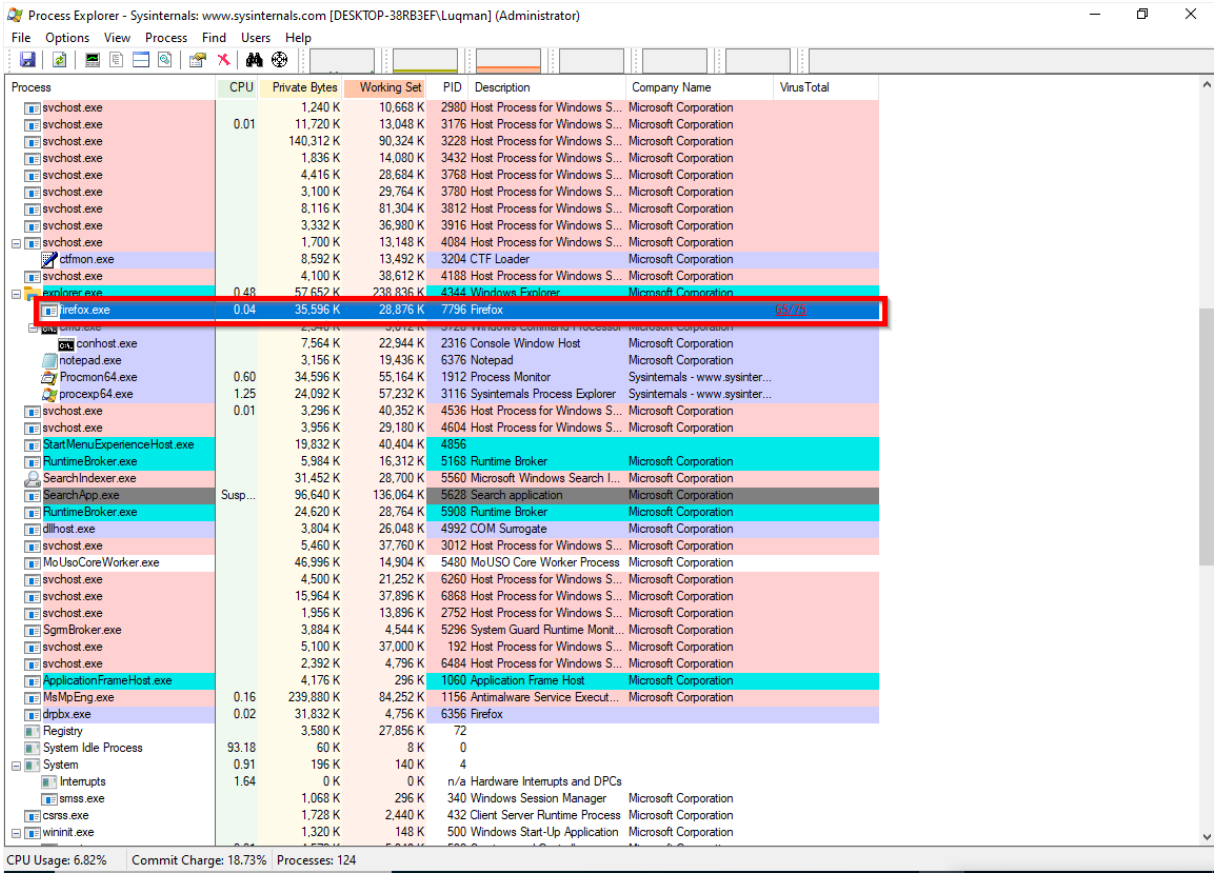
**Executive Summary:**

This collaborative report presents a comprehensive analysis of the Jigsaw ransomware, highlighting the steps taken by Michał Botuliński to dissect its malicious behavior and permanently terminate its actions. The analysis encompasses process termination, identification of malicious activities, file and directory analysis, evidence of malware behavior, and recommendations for effective termination and prevention.

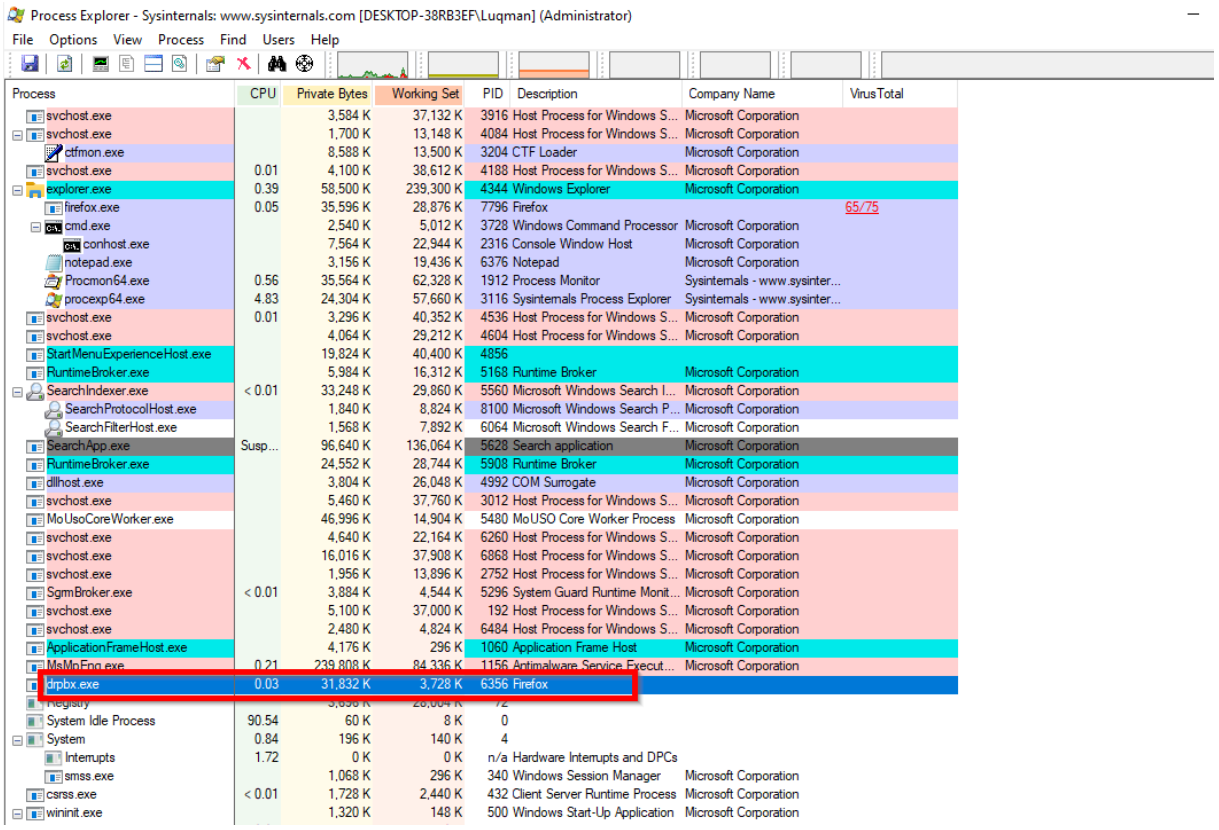
1. **Malicious Process Identification:**

   The analysis identified two malicious processes associated with the Jigsaw ransomware:

   A) "firefox.exe"



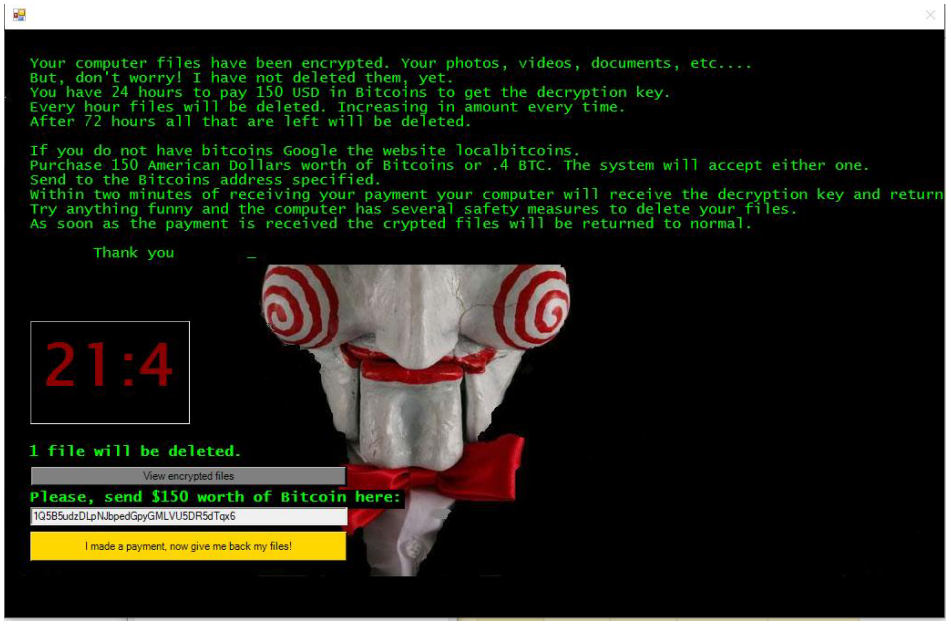
B) "drpbx.exe"



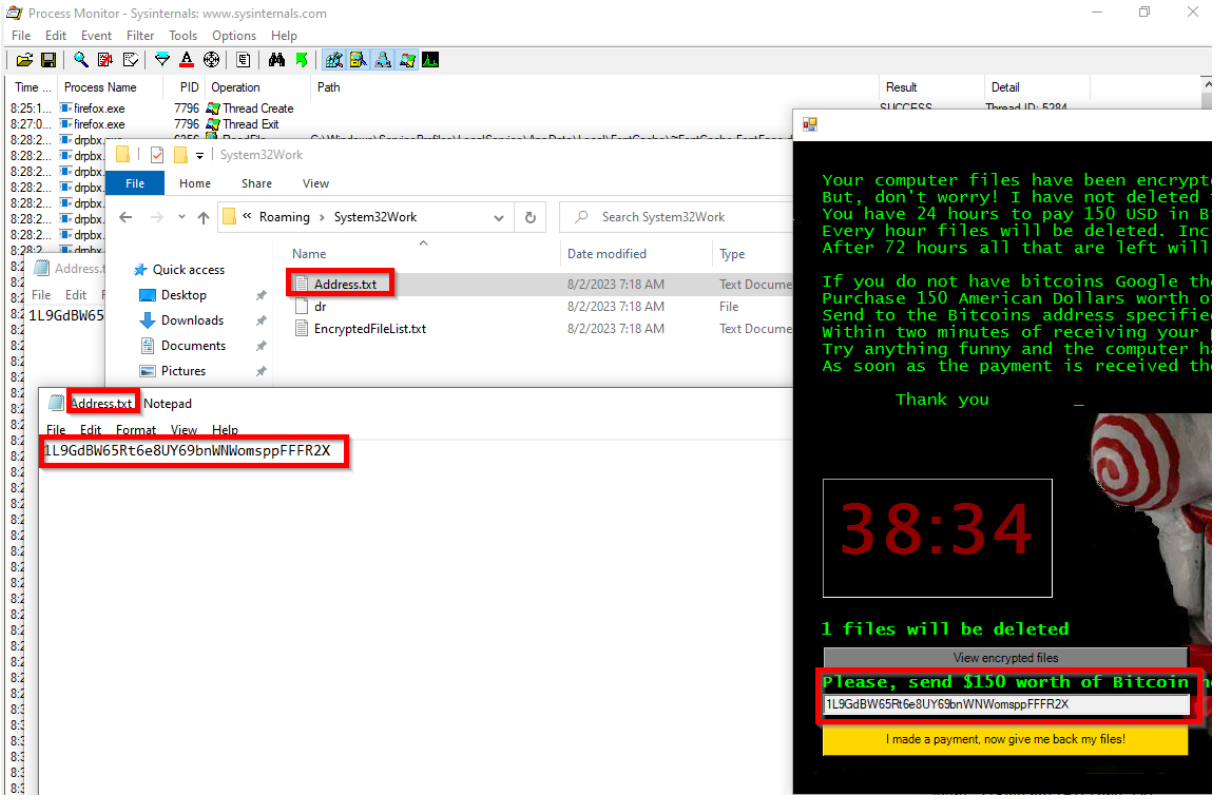

## 2. Malware Behavior and Activities:

The Jigsaw ransomware exhibits several malicious behaviors, including:

A) Displaying threatening messages to victims into paying ransoms.

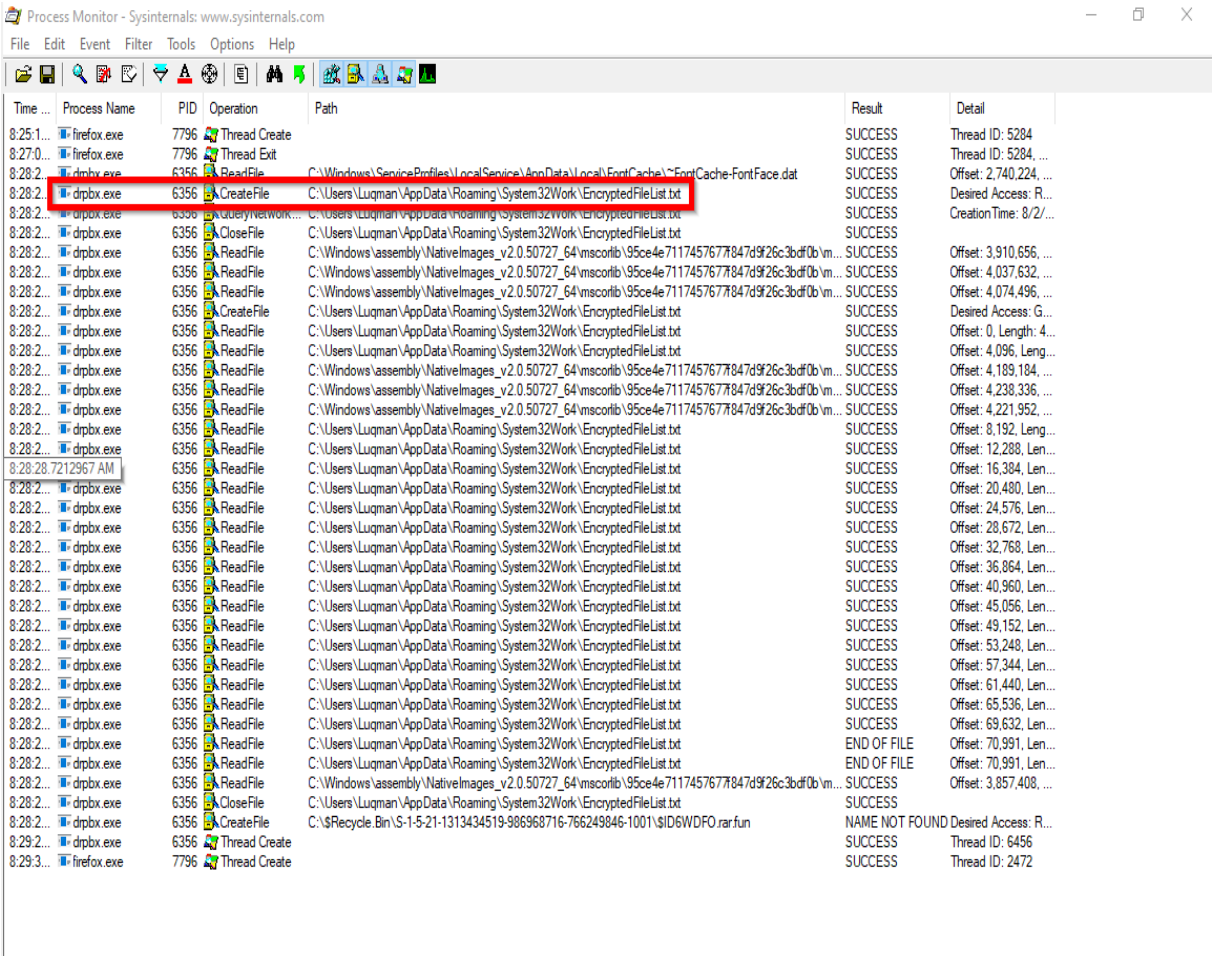


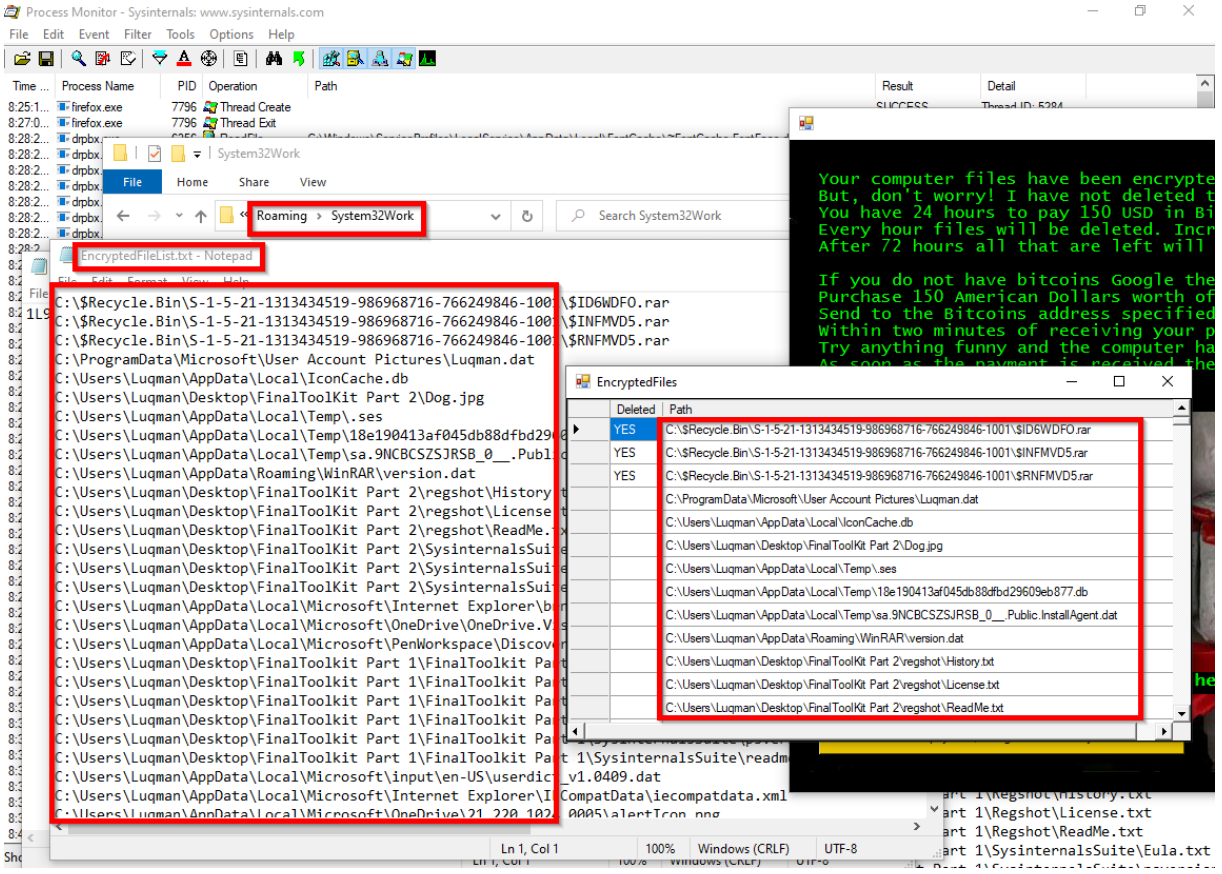
B) Creating essential files for ransome payment and encrypted file tracking.
Address.txt located at C:\Users\Luqman\AppData\Roamin\System32Work
File is related to address where victim should send Bitcoins for decrypt files.



EncryptedFileList.txt located at C:\Users\Luqman\AppData\Roamin\System32Work

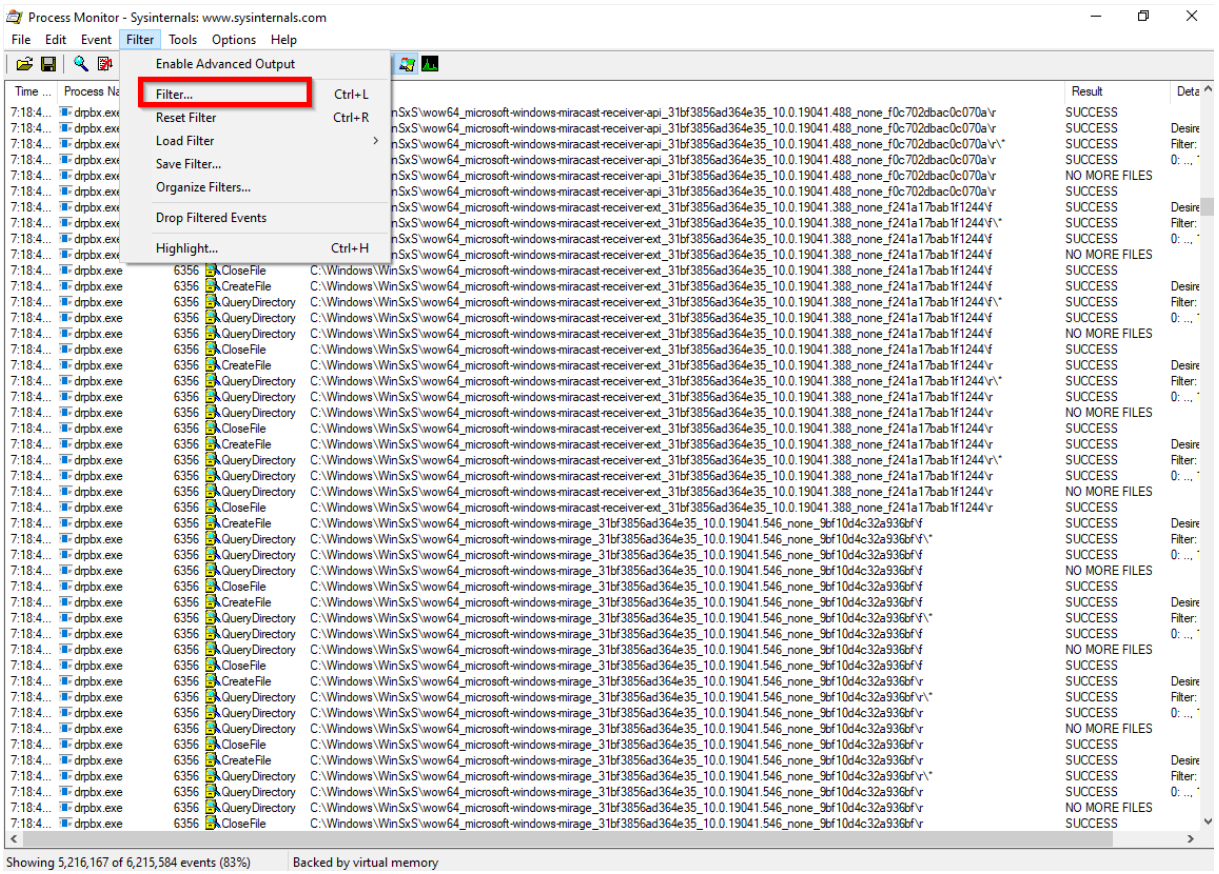
File is related to files and them locations which been already encrypted by ransomware "Jigsaw".



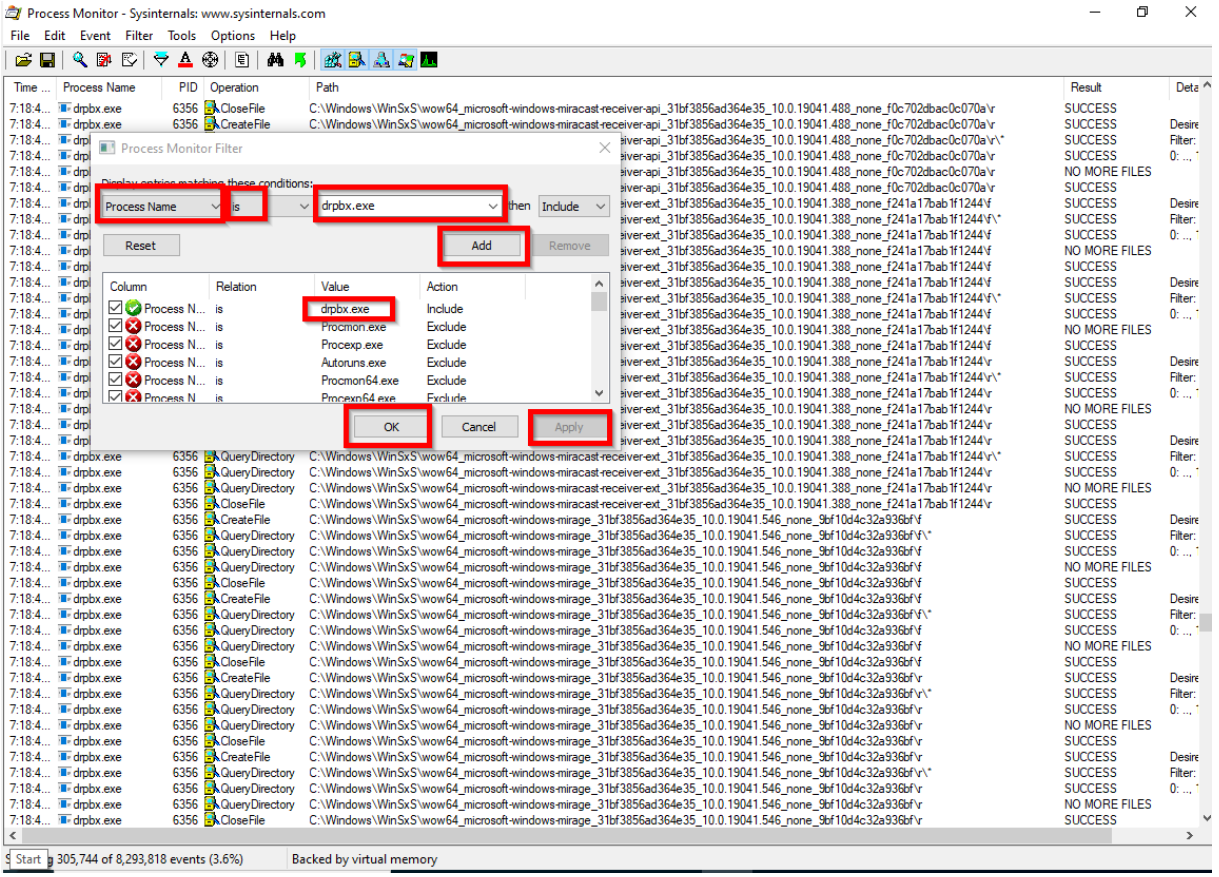

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
firefox.exe 7796 Thread Create
firefox.exe 7796 Thread Exit
System32Work
File Home Share View
Roaming › System32Work
Search System32Work
EncryptedFileList.txt - Notepad
C:\$Recycle.Bin\S-1-5-21-1313434519-986968716-766249846-1001\$ID6WDFO.rar
C:\$Recycle.Bin\S-1-5-21-1313434519-986968716-766249846-1001\$INFMVD5.rar
C:\$Recycle.Bin\S-1-5-21-1313434519-986968716-766249846-1001\$RNFMVD5.rar
C:\ProgramData\Microsoft\User Account Pictures\Luqman.dat
C:\Users\Luqman\AppData\Local\IconCache.db
C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg
C:\Users\Luqman\AppData\Local\Temp\.ses
C:\Users\Luqman\AppData\Local\Temp\18e190413af045db88dfbd29
C:\Users\Luqman\AppData\Local\Temp\sa.9NCBCSZSJRSB_0__.Publ
C:\Users\Luqman\AppData\Roaming\WinRAR\version.dat
C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\History
C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\License
C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\ReadMe.
C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite
C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite
C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite
C:\Users\Luqman\AppData\Local\Microsoft\Internet Explorer\br
C:\Users\Luqman\AppData\Local\Microsoft\OneDrive\OneDrive.V
C:\Users\Luqman\AppData\Local\Microsoft\PenWorkspace\Discov
C:\Users\Luqman\Desktop\FinalToolkit Part 1\FinalToolkit Pa
C:\Users\Luqman\Desktop\FinalToolkit Part 1\FinalToolkit Pa
C:\Users\Luqman\Desktop\FinalToolkit Part 1\FinalToolkit Pa
C:\Users\Luqman\Desktop\FinalToolkit Part 1\FinalToolkit Pa
C:\Users\Luqman\Desktop\FinalToolkit Part 1\FinalToolkit Pa
C:\Users\Luqman\Desktop\FinalToolkit Part 1\FinalToolkit Pa
C:\Users\Luqman\AppData\Local\Microsoft\input\en-US\userdict_v1.0409.dat
C:\Users\Luqman\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml
Ln 1, Col 1 100% Windows (CRLF) UTF-8
Your computer files have been encrypte
But, don't worry! I have not deleted t
You have 24 hours to pay 150 USD in Bi
Every hour files will be deleted. Incr
After 72 hours all that are left will
If you do not have bitcoins Google the
Purchase 150 American Dollars worth of
Send to the Bitcoins address specified
Within two minutes of receiving your p
Try anything funny and the computer ha
EncryptedFiles
Deleted Path
YES C:\$Recycle.Bin\S-1-5-21-1313434519-986968716-766249846-1001\$ID6WDFO.rar
YES C:\$Recycle.Bin\S-1-5-21-1313434519-986968716-766249846-1001\$INFMVD5.rar
YES C:\$Recycle.Bin\S-1-5-21-1313434519-986968716-766249846-1001\$RNFMVD5.rar
C:\ProgramData\Microsoft\User Account Pictures\Luqman.dat
C:\Users\Luqman\AppData\Local\IconCache.db
C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg
C:\Users\Luqman\AppData\Local\Temp\.ses
C:\Users\Luqman\AppData\Local\Temp\18e190413af045db88dfbd29609eb877.db
C:\Users\Luqman\AppData\Local\Temp\sa.9NCBCSZSJRSB_0__.Public.InstallAgent.dat
C:\Users\Luqman\AppData\Roaming\WinRAR\version.dat
C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\History.txt
C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\License.txt
C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\ReadMe.txt
art 1\Regshot\History.txt
art 1\Regshot\License.txt
art 1\Regshot\ReadMe.txt
art 1\SysinternalsSuite\Eula.txt

C) Encrypting files with the ".fun" extension, rendering them inaccessible.

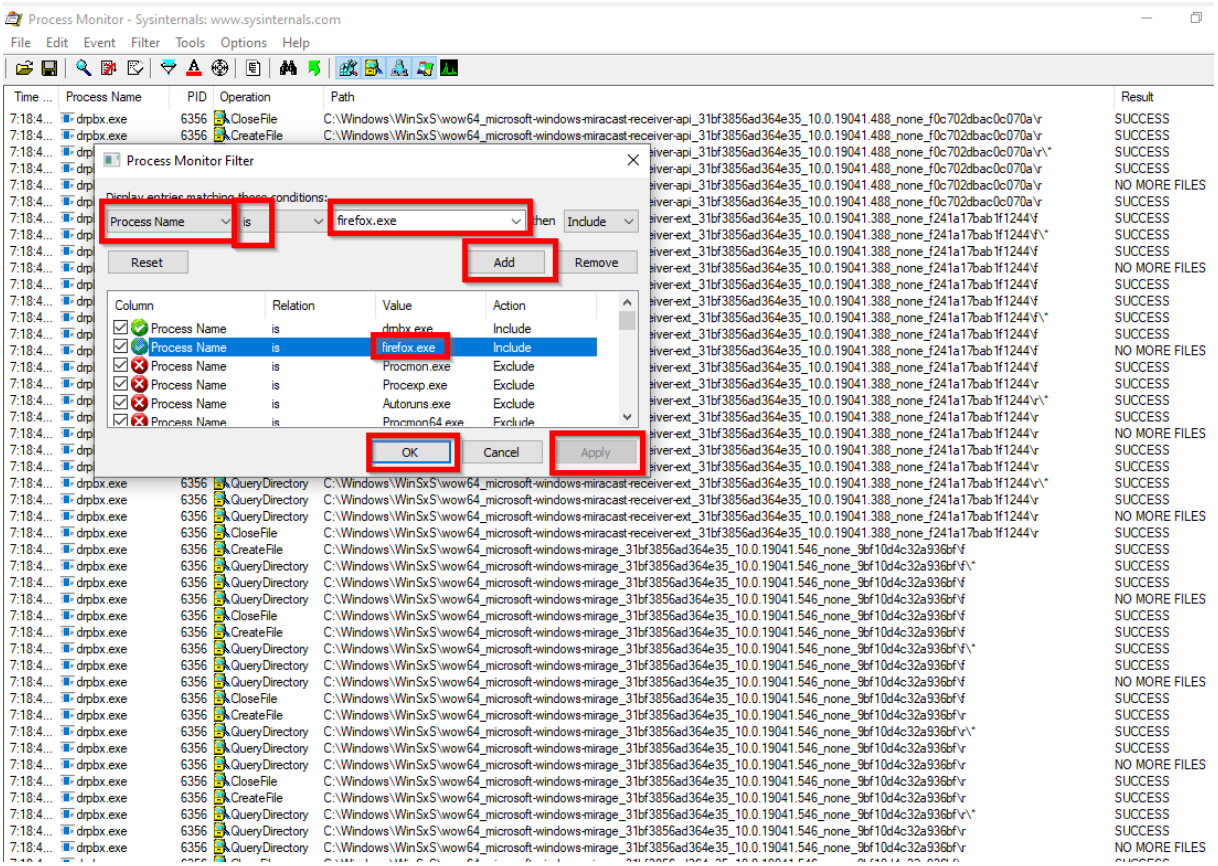
1.



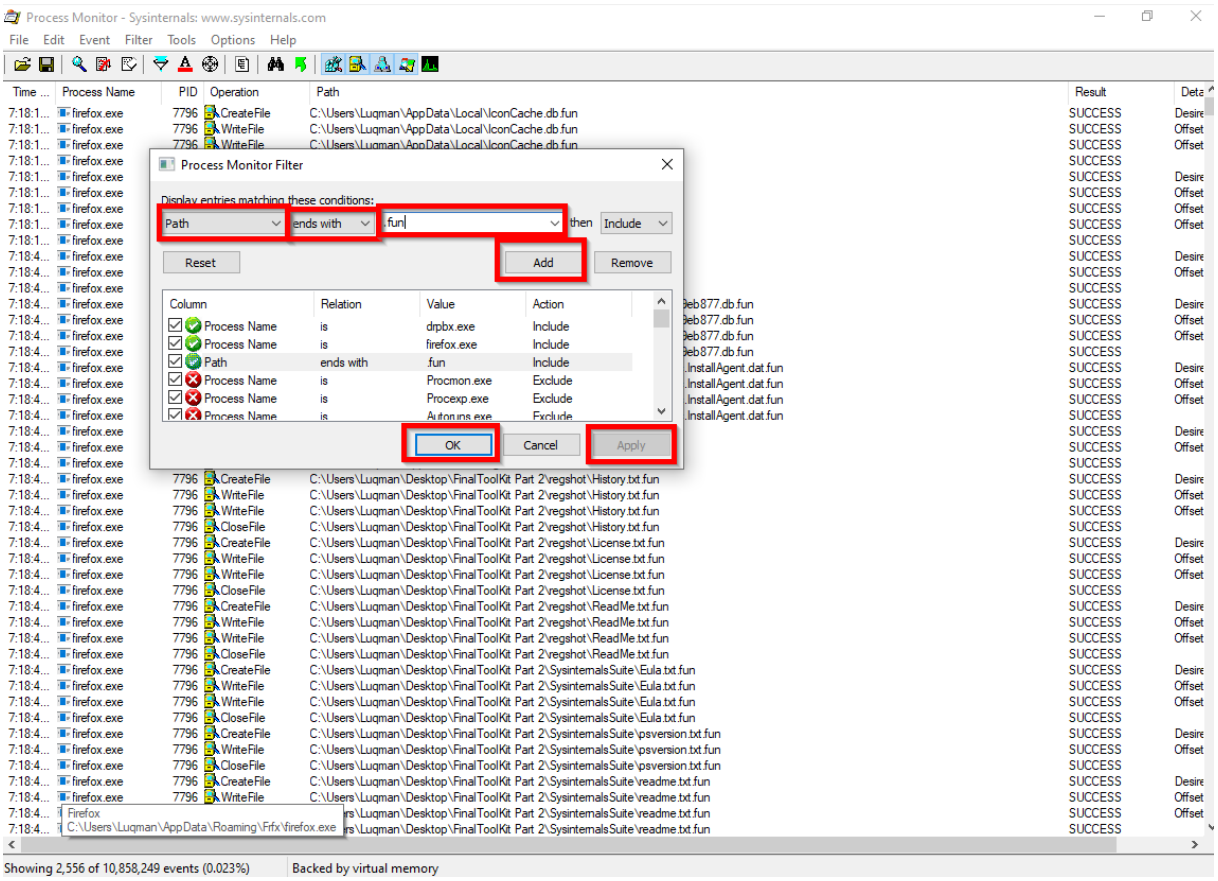
2.

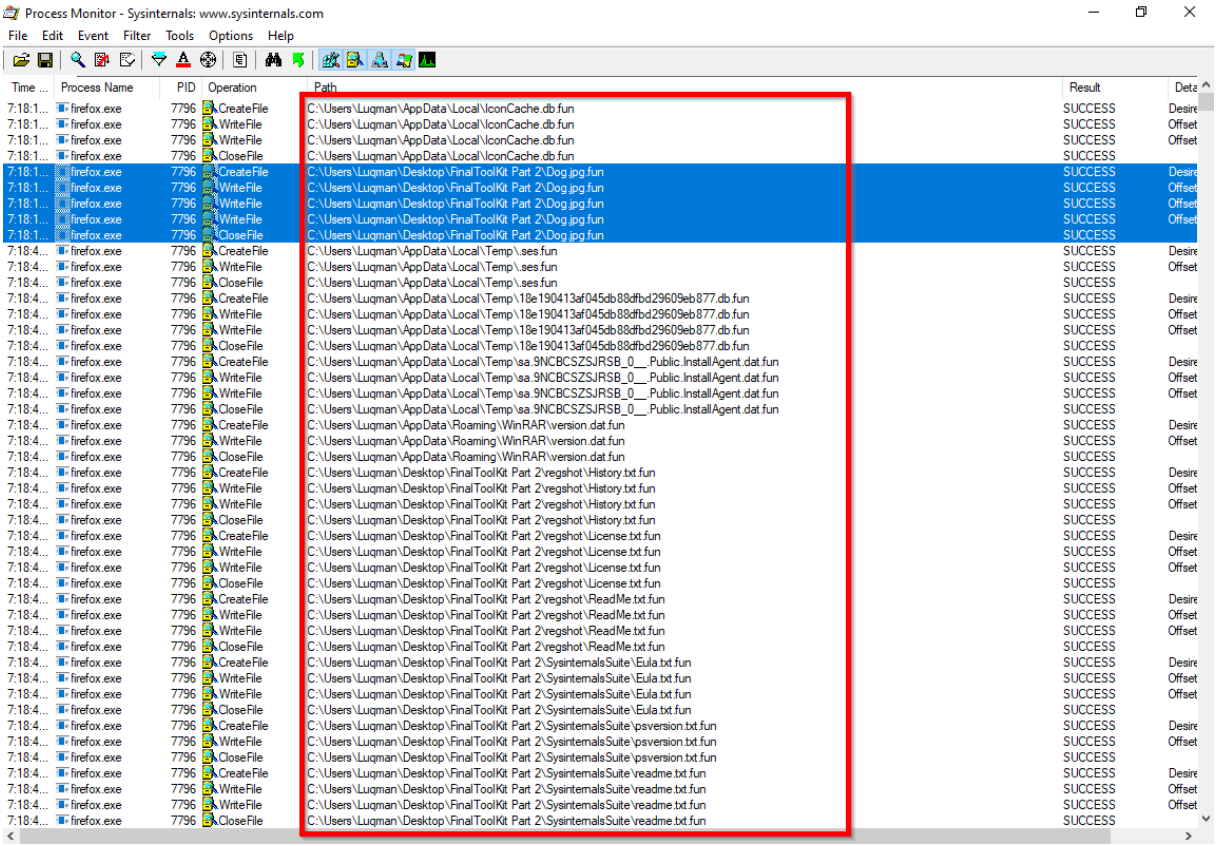

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Process Monitor Filter
Process Name is drpbx.exe then Include
Reset Add Remove
Column Relation Value Action
Process N... is drpbx.exe Include
Process N... is Procmon.exe Exclude
Process N... is Procexp.exe Exclude
Process N... is Autoruns.exe Exclude
Process N... is Procmon64.exe Exclude
OK Cancel Apply
Start 305,744 of 8,293,818 events (3.6%)
Backed by virtual memory

3.

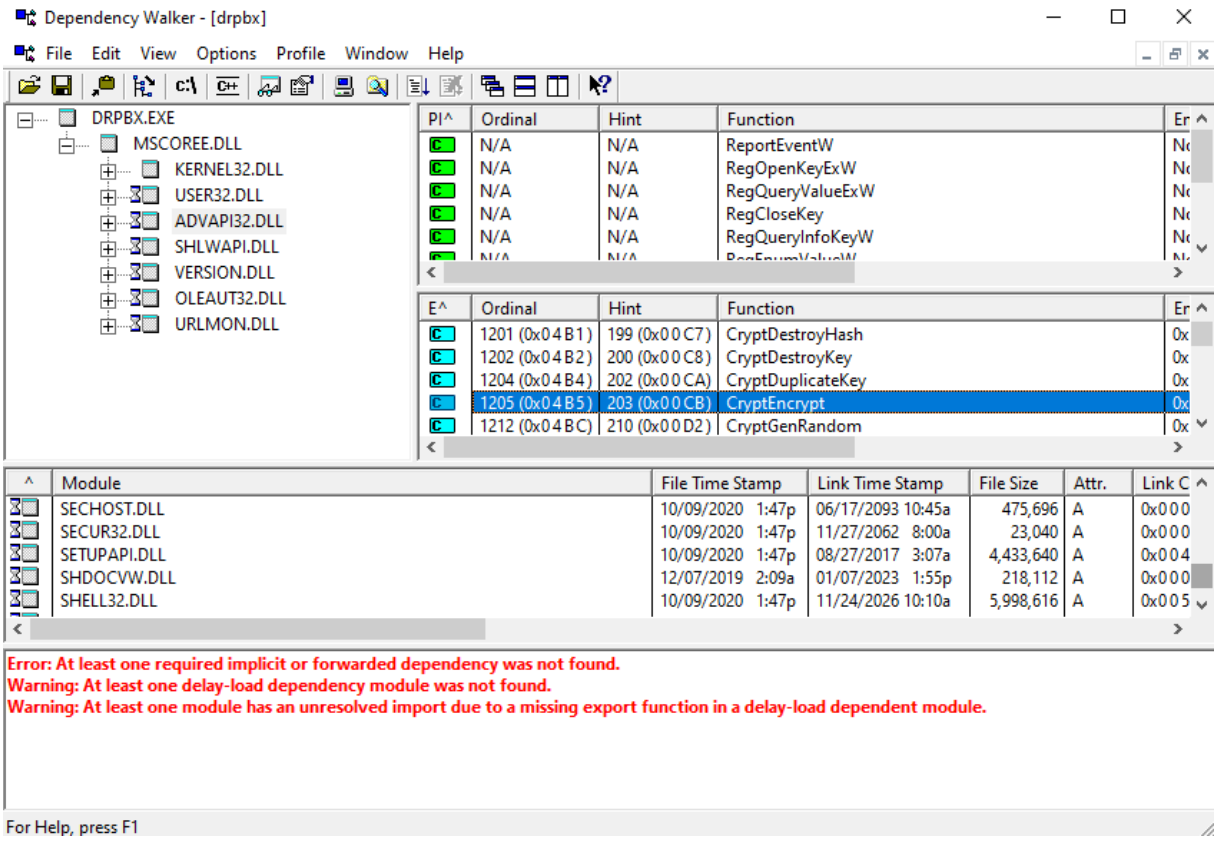

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Process Monitor Filter
Process Name is firefox.exe then Include
Reset Add Remove
Column Relation Value Action
Process Name is drpbx.exe Include
Process Name is firefox.exe Include
Process Name is Procmon.exe Exclude
Process Name is Procexp.exe Exclude
Process Name is Autoruns.exe Exclude
Process Name is Procmon64.exe Exclude
OK Cancel Apply

4.

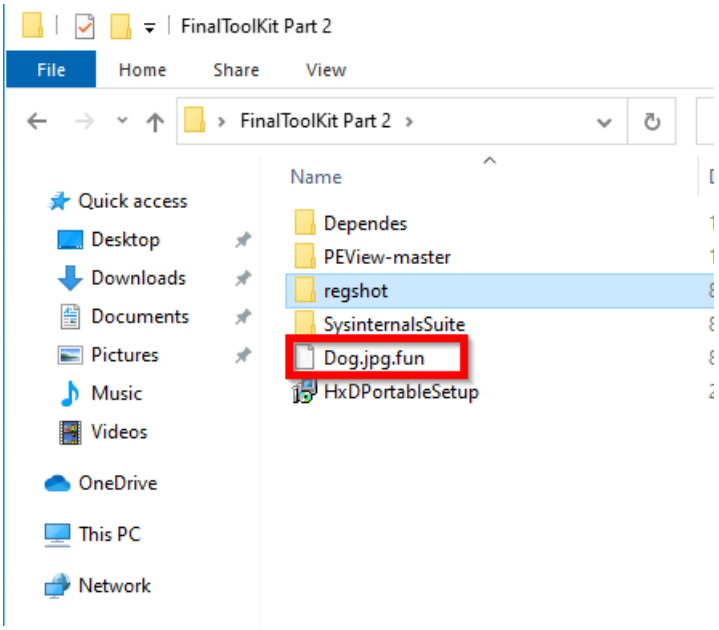

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Process Monitor Filter
Display entries matching these conditions:
Path
ends with
.fun
then
Include
Reset
Add
Remove
Column
Relation
Value
Action
Process Name is drpbx.exe Include
Process Name is firefox.exe Include
Path ends with .fun Include
Process Name is Procmon.exe Exclude
Process Name is Procexp.exe Exclude
OK
Cancel
Apply
Showing 2,556 of 10,858,249 events (0.023%)
Backed by virtual memory


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Deta
7:18:1... firefox.exe 7796 CreateFile C:\Users\Luqman\AppData\Local\IconCache.db.fun SUCCESS Desire
7:18:1... firefox.exe 7796 WriteFile C:\Users\Luqman\AppData\Local\IconCache.db.fun SUCCESS Offset
7:18:1... firefox.exe 7796 WriteFile C:\Users\Luqman\AppData\Local\IconCache.db.fun SUCCESS Offset
7:18:1... firefox.exe 7796 CloseFile C:\Users\Luqman\AppData\Local\IconCache.db.fun SUCCESS
7:18:1... firefox.exe 7796 CreateFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg.fun SUCCESS Desire
7:18:1... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg.fun SUCCESS Offset
7:18:1... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg.fun SUCCESS Offset
7:18:1... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg.fun SUCCESS Offset
7:18:1... firefox.exe 7796 CloseFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\Dog.jpg.fun SUCCESS
7:18:4... firefox.exe 7796 CreateFile C:\Users\Luqman\AppData\Local\Temp\.ses.fun SUCCESS Desire
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\AppData\Local\Temp\.ses.fun SUCCESS Offset
7:18:4... firefox.exe 7796 CloseFile C:\Users\Luqman\AppData\Local\Temp\.ses.fun SUCCESS
7:18:4... firefox.exe 7796 CreateFile C:\Users\Luqman\AppData\Local\Temp\18e190413af045db88dfbd29609eb877.db.fun SUCCESS Desire
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\AppData\Local\Temp\18e190413af045db88dfbd29609eb877.db.fun SUCCESS Offset
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\AppData\Local\Temp\18e190413af045db88dfbd29609eb877.db.fun SUCCESS Offset
7:18:4... firefox.exe 7796 CloseFile C:\Users\Luqman\AppData\Local\Temp\18e190413af045db88dfbd29609eb877.db.fun SUCCESS
7:18:4... firefox.exe 7796 CreateFile C:\Users\Luqman\AppData\Local\Temp\sa.9NCBCSZSJRSB_0__Public.InstallAgent.dat.fun SUCCESS Desire
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\AppData\Local\Temp\sa.9NCBCSZSJRSB_0__Public.InstallAgent.dat.fun SUCCESS Offset
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\AppData\Local\Temp\sa.9NCBCSZSJRSB_0__Public.InstallAgent.dat.fun SUCCESS Offset
7:18:4... firefox.exe 7796 CloseFile C:\Users\Luqman\AppData\Local\Temp\sa.9NCBCSZSJRSB_0__Public.InstallAgent.dat.fun SUCCESS
7:18:4... firefox.exe 7796 CreateFile C:\Users\Luqman\AppData\Roaming\WinRAR\version.dat.fun SUCCESS Desire
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\AppData\Roaming\WinRAR\version.dat.fun SUCCESS Offset
7:18:4... firefox.exe 7796 CloseFile C:\Users\Luqman\AppData\Roaming\WinRAR\version.dat.fun SUCCESS
7:18:4... firefox.exe 7796 CreateFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\History.txt.fun SUCCESS Desire
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\History.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\History.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 CloseFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\History.txt.fun SUCCESS
7:18:4... firefox.exe 7796 CreateFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\License.txt.fun SUCCESS Desire
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\License.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\License.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 CloseFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\License.txt.fun SUCCESS
7:18:4... firefox.exe 7796 CreateFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\ReadMe.txt.fun SUCCESS Desire
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\ReadMe.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\ReadMe.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 CloseFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\regshot\ReadMe.txt.fun SUCCESS
7:18:4... firefox.exe 7796 CreateFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\Eula.txt.fun SUCCESS Desire
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\Eula.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\Eula.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 CloseFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\Eula.txt.fun SUCCESS
7:18:4... firefox.exe 7796 CreateFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\psversion.txt.fun SUCCESS Desire
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\psversion.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 CloseFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\psversion.txt.fun SUCCESS
7:18:4... firefox.exe 7796 CreateFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\readme.txt.fun SUCCESS Desire
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\readme.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 WriteFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\readme.txt.fun SUCCESS Offset
7:18:4... firefox.exe 7796 CloseFile C:\Users\Luqman\Desktop\FinalToolKit Part 2\SysinternalsSuite\readme.txt.fun SUCCESS

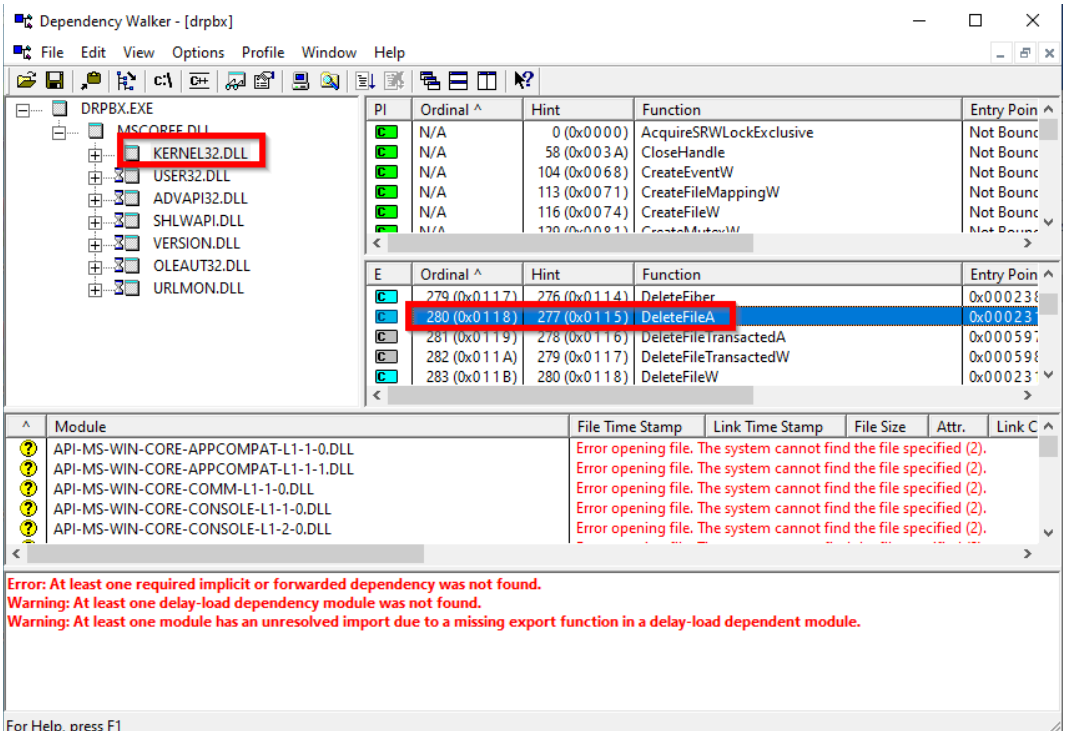
5.

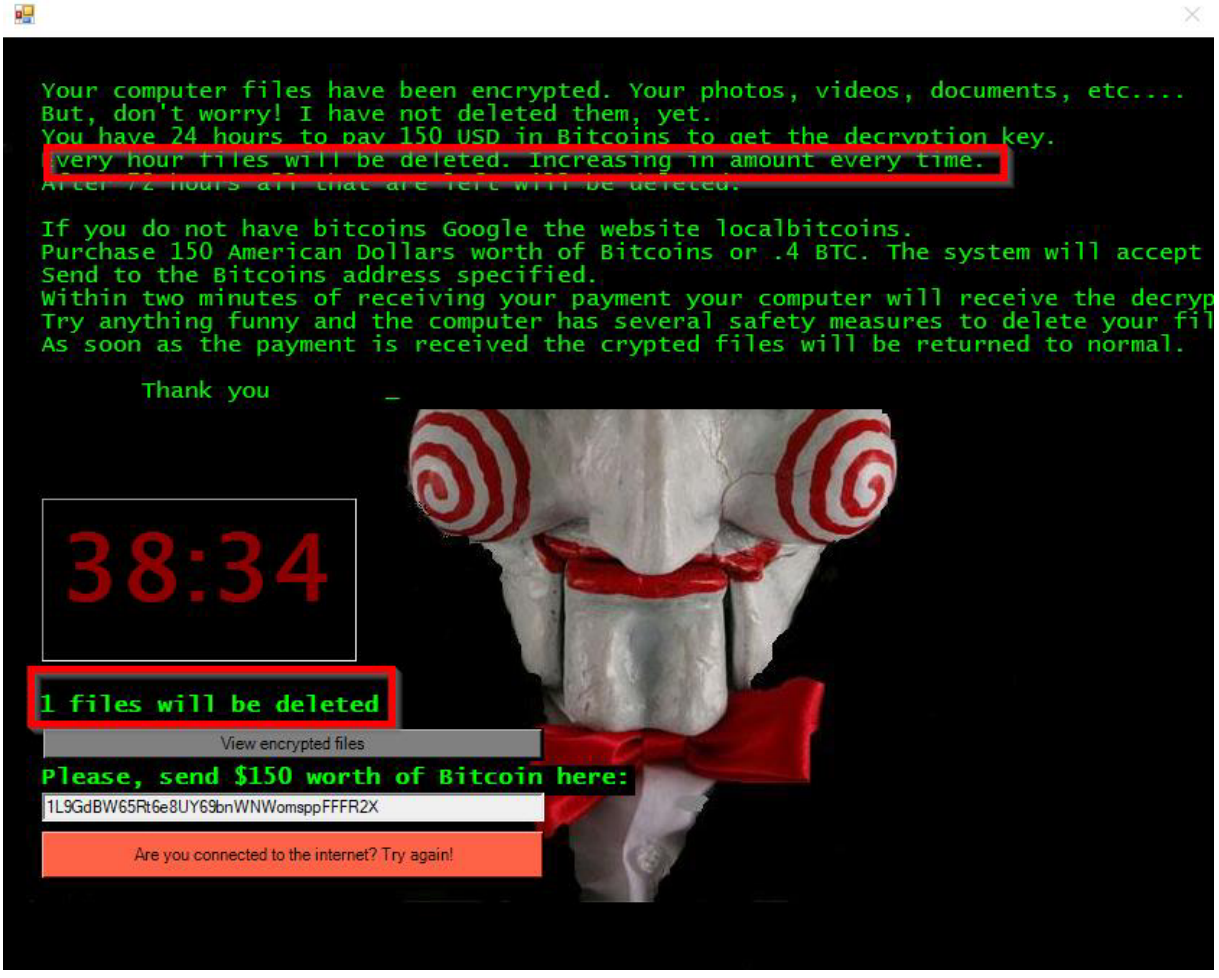

Dependency Walker - [drpbx]
File Edit View Options Profile Window Help
DRPBX.EXE
MSCOREE.DLL
KERNEL32.DLL
USER32.DLL
ADVAPI32.DLL
SHLWAPI.DLL
VERSION.DLL
OLEAUT32.DLL
URLMON.DLL
PI^ Ordinal Hint Function
N/A N/A ReportEventW
N/A N/A RegOpenKeyExW
N/A N/A RegQueryValueExW
N/A N/A RegCloseKey
N/A N/A RegQueryInfoKeyW
E^ Ordinal Hint Function
1201 (0x04B1) 199 (0x00C7) CryptDestroyHash
1202 (0x04B2) 200 (0x00C8) CryptDestroyKey
1204 (0x04B4) 202 (0x00CA) CryptDuplicateKey
1205 (0x04B5) 203 (0x00CB) CryptEncrypt
1212 (0x04BC) 210 (0x00D2) CryptGenRandom
Module File Time Stamp Link Time Stamp File Size Attr. Link C
SECHOST.DLL 10/09/2020 1:47p 06/17/2093 10:45a 475,696 A 0x000
SECUR32.DLL 10/09/2020 1:47p 11/27/2062 8:00a 23,040 A 0x000
SETUPAPI.DLL 10/09/2020 1:47p 08/27/2017 3:07a 4,433,640 A 0x004
SHDOCVW.DLL 12/07/2019 2:09a 01/07/2023 1:55p 218,112 A 0x000
SHELL32.DLL 10/09/2020 1:47p 11/24/2026 10:10a 5,998,616 A 0x005
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.
For Help, press F1

6.


FinalToolKit Part 2
File Home Share View
FinalToolKit Part 2
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Dependes
PEView-master
regshot
SysinternalsSuite
Dog.jpg.fun
HxDPortableSetup

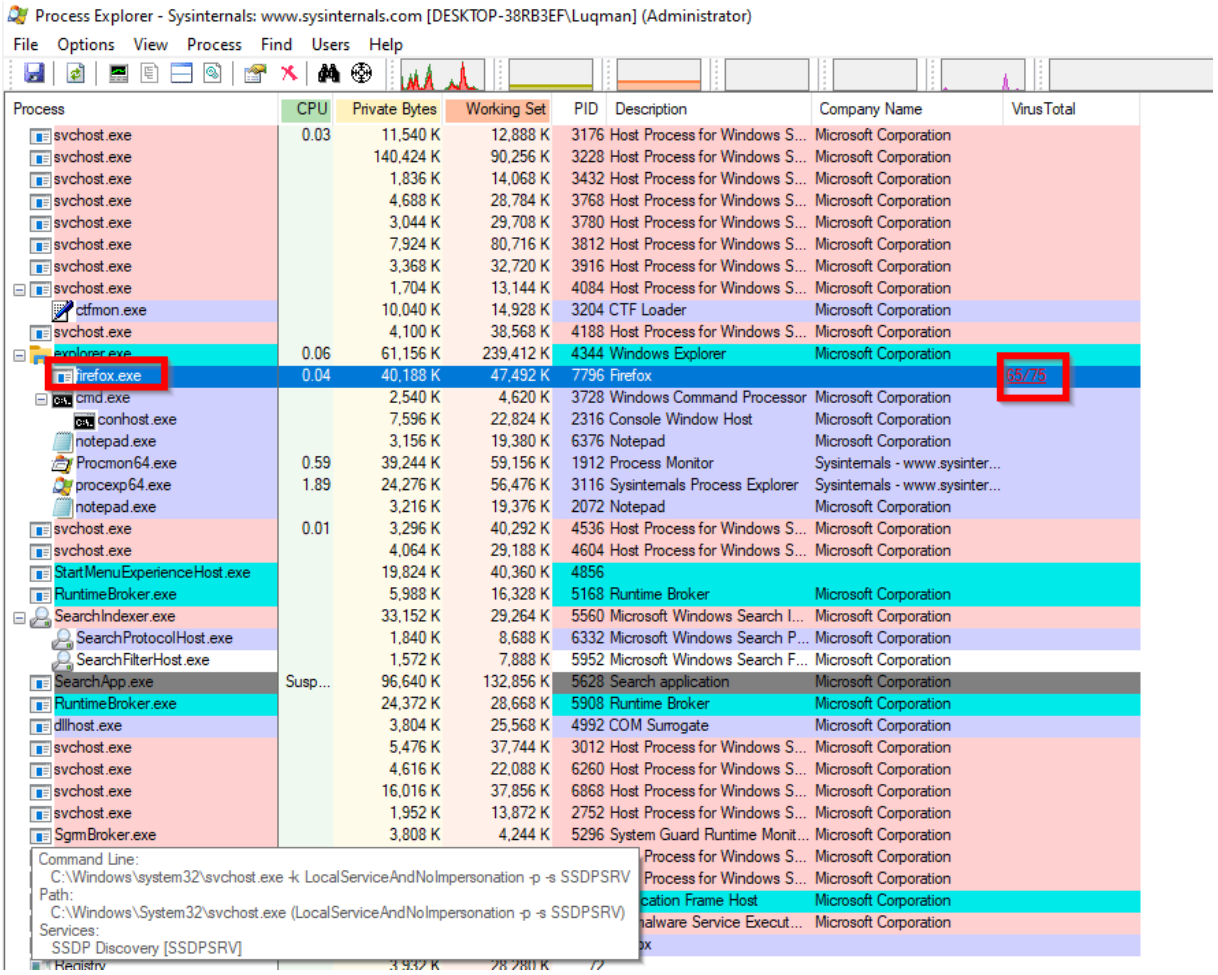
D) Deletion of files in the event of non-payment. (Screenshot from Dependency Walker)



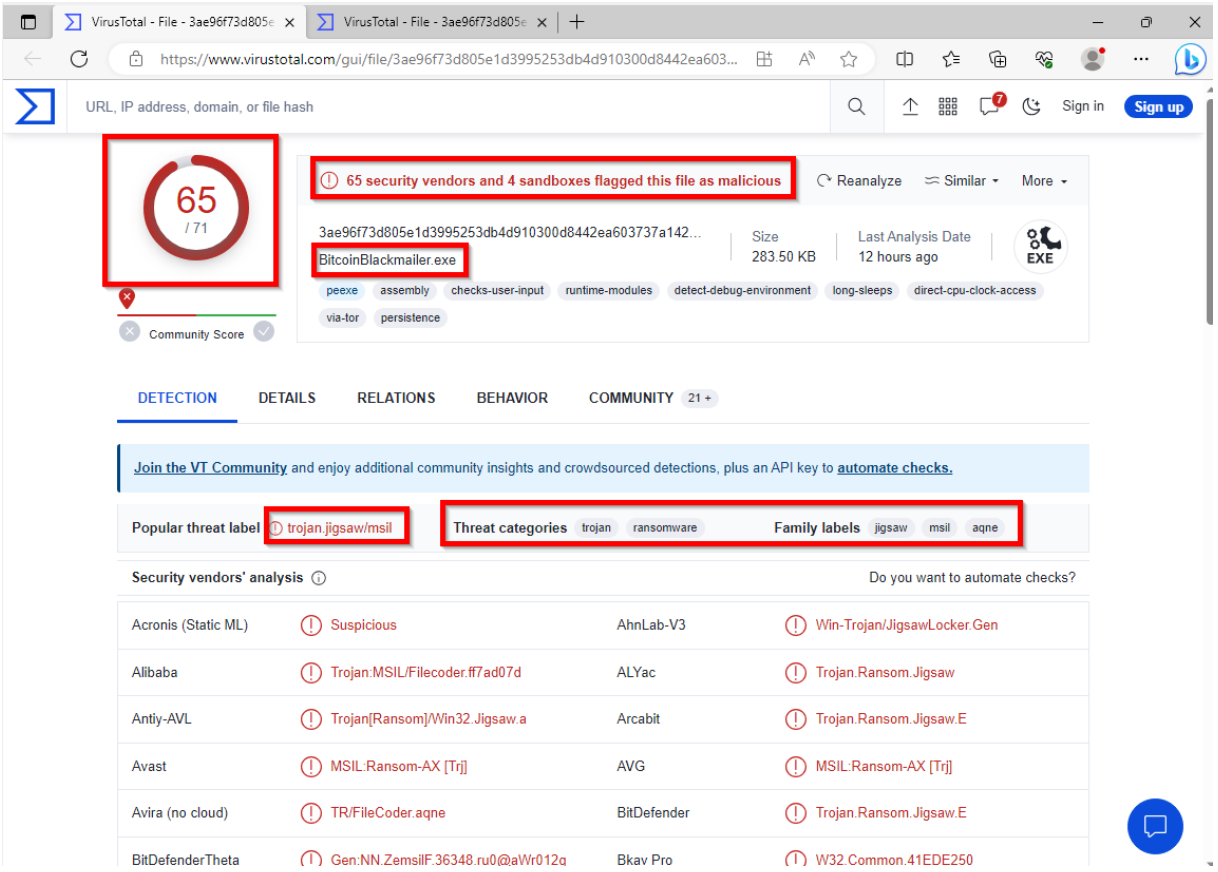



E) Analyze firefox.exe by program “Process Explorer” shown that is a malicious process.

1.



2.




### 3. Infected Directories and Files:

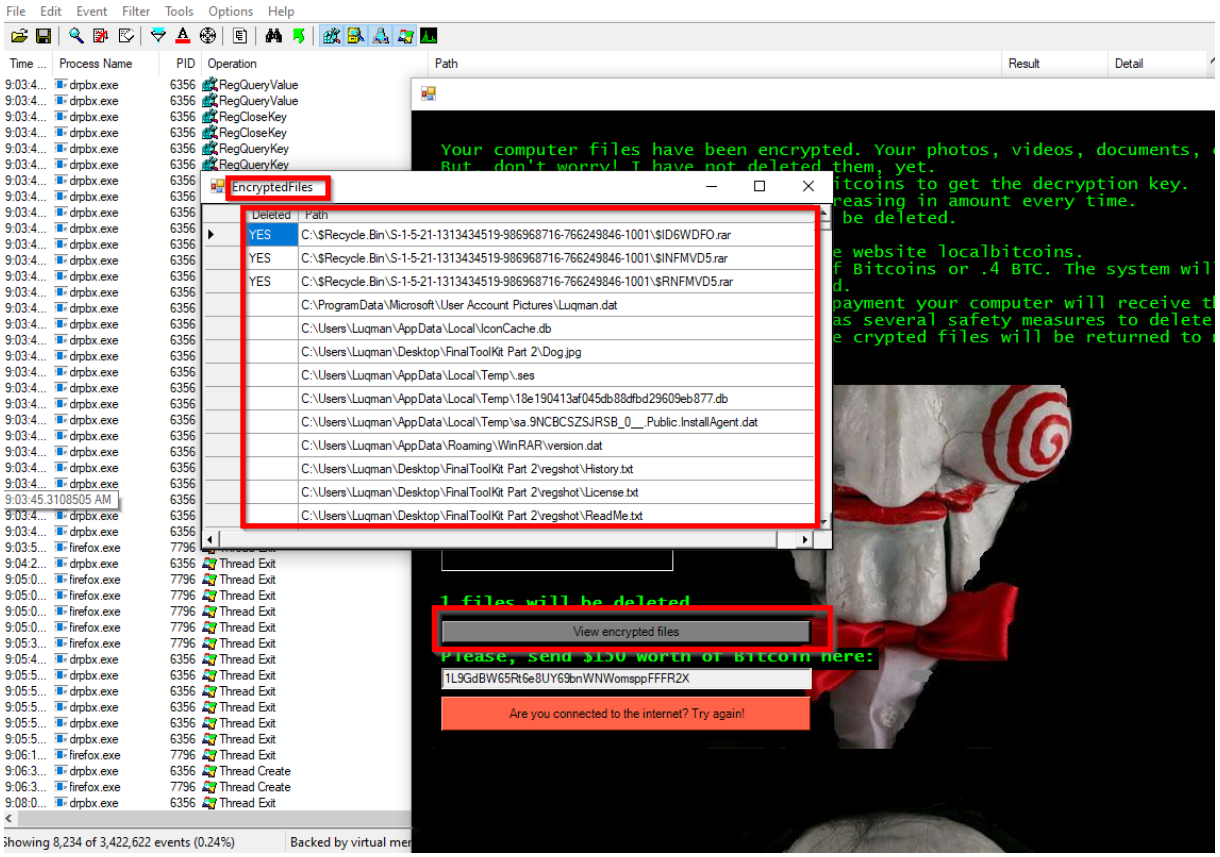
The ransomware infects specific directories and creates crucial files:

A) C:\Users\Luqman\App\Roaming\Frfx

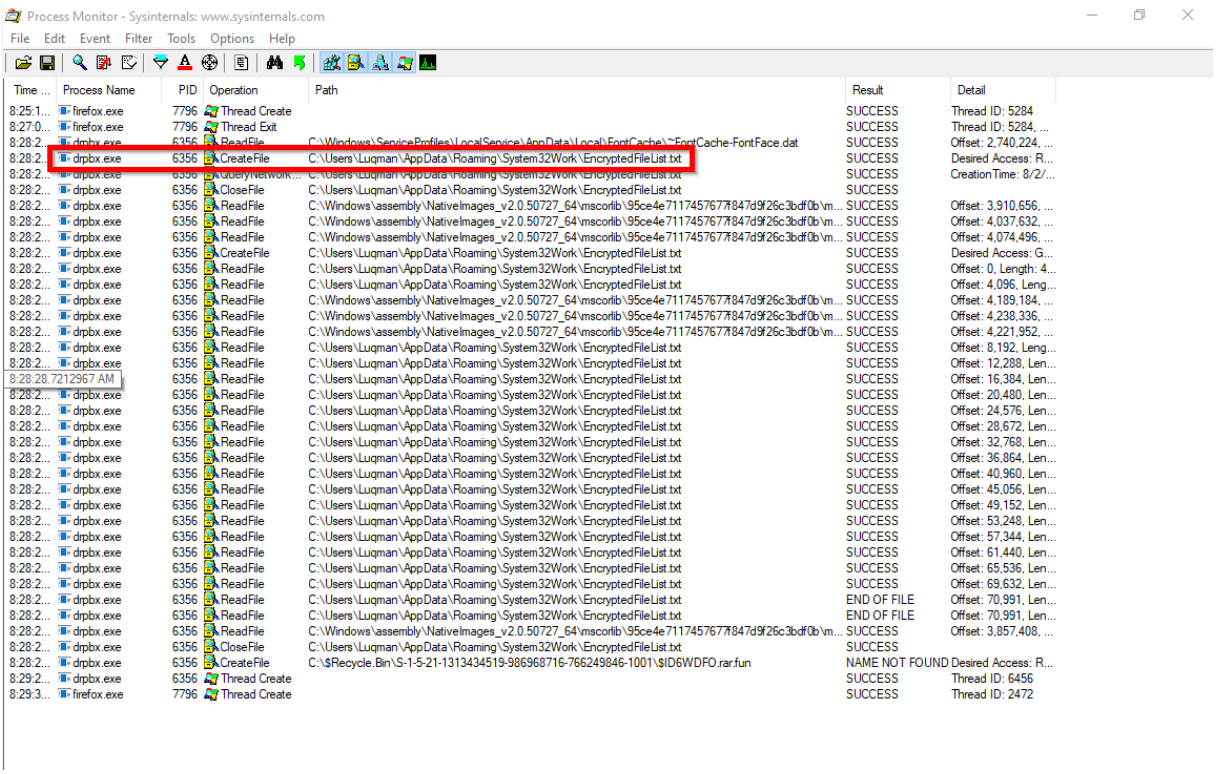
B) C:\Users\Luqman\AppData\Local\Drpbx

## 3. List of files that are infected.

A)



B) Ransomware during process CreateFile creates a file EncryptedFileList.txt in directory : C:\Users\Luqman\AppData\Roaming\System32Work

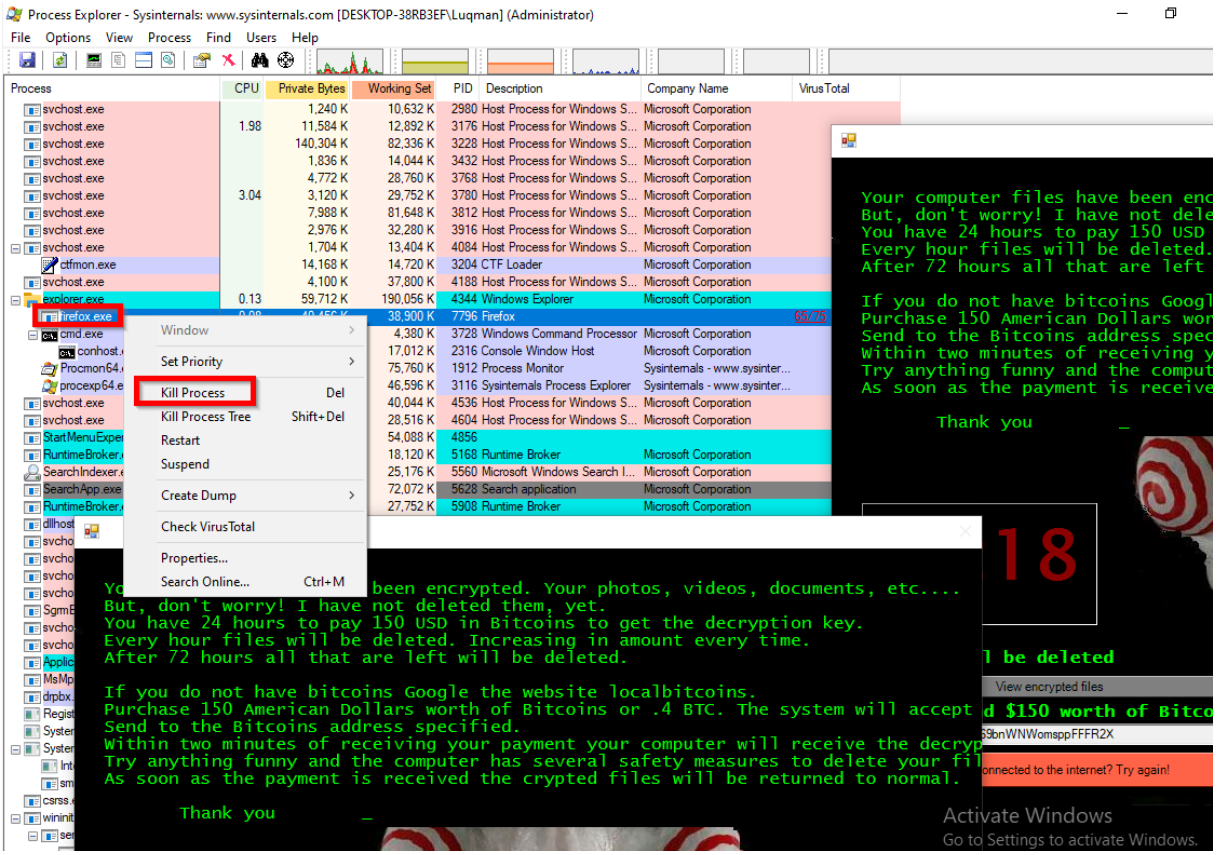


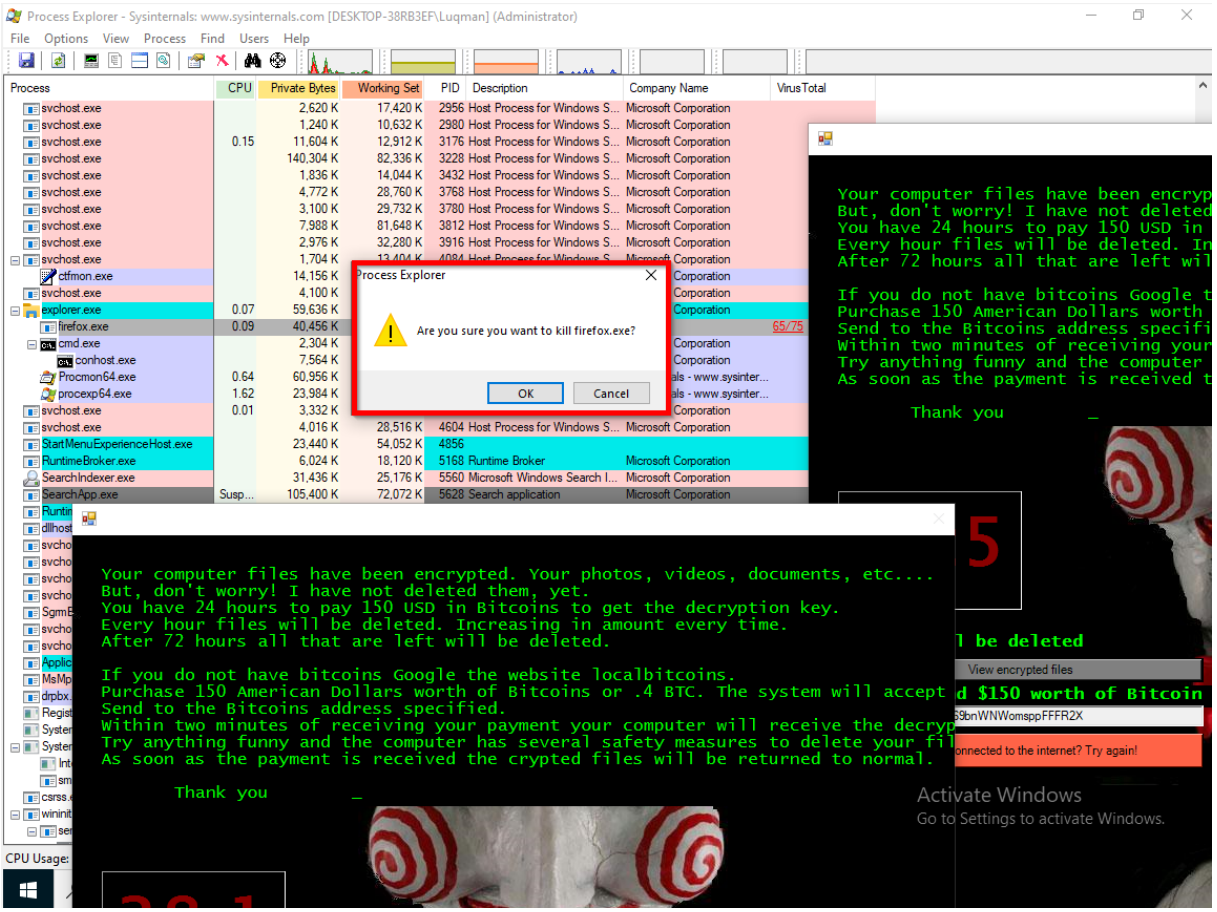

| Time ... | Process Name | PID | Operation | Path | Result | Detail |
|---|---|---|---|---|---|---|
| 8:25:1... | firefox.exe | 7796 | Thread Create | | SUCCESS | Thread ID: 5284 |
| 8:27:0... | firefox.exe | 7796 | Thread Exit | | SUCCESS | Thread ID: 5284, ... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\~FontCache-FontFace.dat | SUCCESS | Offset: 2,740,224, ... |
| 8:28:2... | dropbx.exe | 6356 | CreateFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Desired Access: R... |
| 8:28:2... | dropbx.exe | 6356 | QueryNetwork... | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | CreationTime: 8/2/... |
| 8:28:2... | dropbx.exe | 6356 | CloseFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677f847d9f26c3bdf0b\m... | SUCCESS | Offset: 3,910,656, ... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677f847d9f26c3bdf0b\m... | SUCCESS | Offset: 4,037,632, ... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677f847d9f26c3bdf0b\m... | SUCCESS | Offset: 4,074,496, ... |
| 8:28:2... | dropbx.exe | 6356 | CreateFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Desired Access: G... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 0, Length: 4... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 4,096, Leng... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677f847d9f26c3bdf0b\m... | SUCCESS | Offset: 4,189,184, ... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677f847d9f26c3bdf0b\m... | SUCCESS | Offset: 4,238,336, ... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677f847d9f26c3bdf0b\m... | SUCCESS | Offset: 4,221,952, ... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 8,192, Leng... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 12,288, Len... |
| 8:28:28.7212967 AM | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 16,384, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 20,480, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 24,576, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 28,672, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 32,768, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 36,864, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 40,960, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 45,056, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 49,152, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 53,248, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 57,344, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 61,440, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 65,536, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | Offset: 69,632, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | END OF FILE | Offset: 70,991, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | END OF FILE | Offset: 70,991, Len... |
| 8:28:2... | dropbx.exe | 6356 | ReadFile | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677f847d9f26c3bdf0b\m... | SUCCESS | Offset: 3,857,408, ... |
| 8:28:2... | dropbx.exe | 6356 | CloseFile | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt | SUCCESS | |
| 8:28:2... | dropbx.exe | 6356 | CreateFile | C:\$Recycle.Bin\S-1-5-21-1313434519-986968716-766249846-1001\$ID6WDFO.rar.fun | NAME NOT FOUND | Desired Access: R... |
| 8:29:2... | dropbx.exe | 6356 | Thread Create | | SUCCESS | Thread ID: 6456 |
| 8:29:3... | firefox.exe | 7796 | Thread Create | | SUCCESS | Thread ID: 2472 |

## 4. Evidence of Malware Activity:

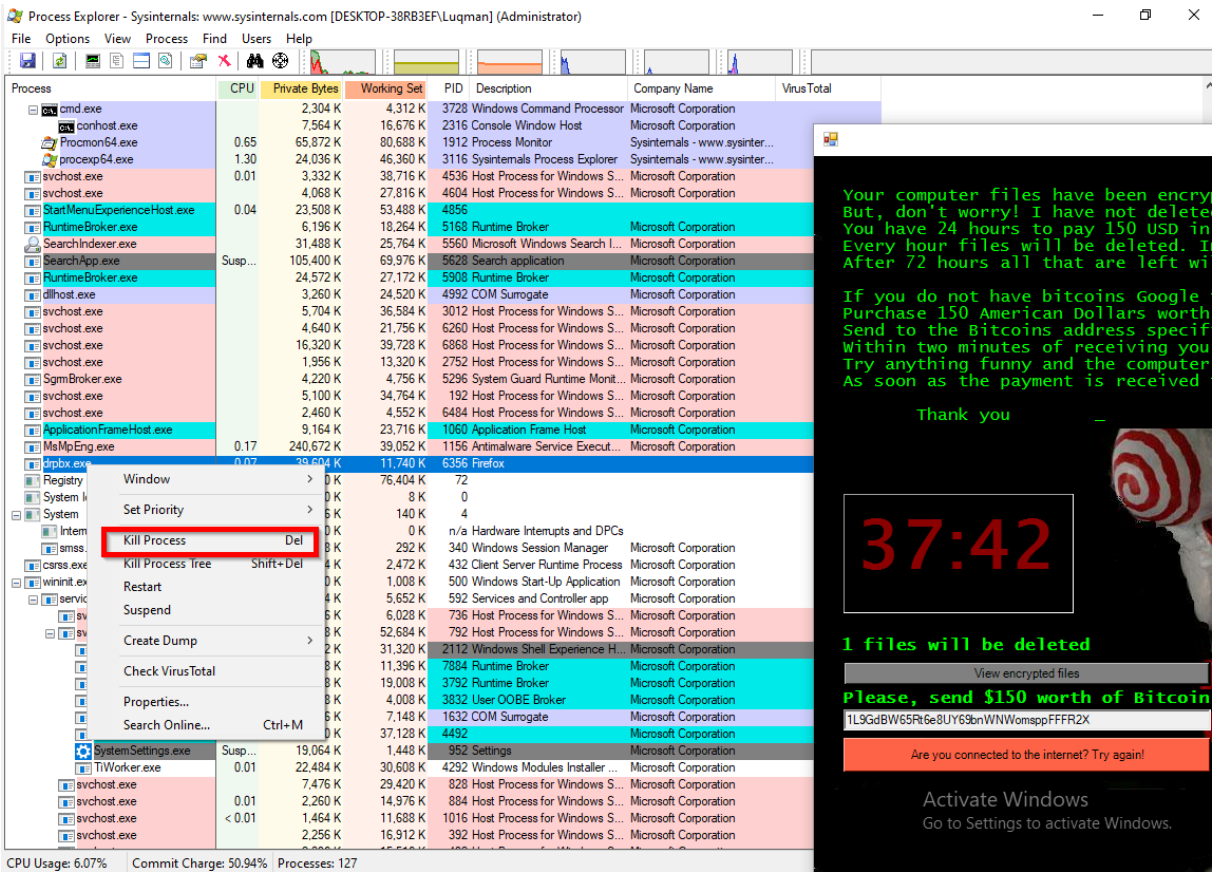
The analysis provides evidence of the malware's actions and its correlation with the "Welcome" screen:

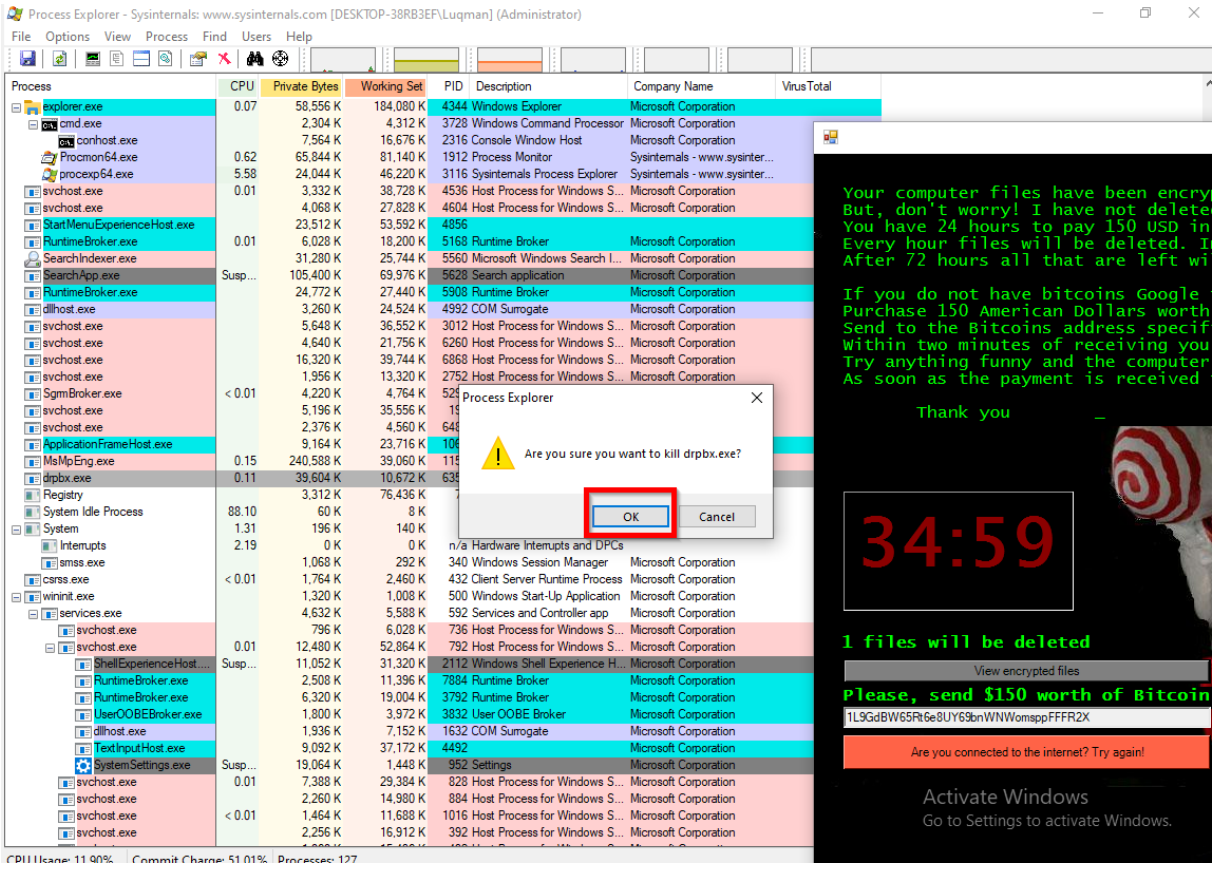
A) Killing "firefox.exe" terminates the "Welcome" screen.

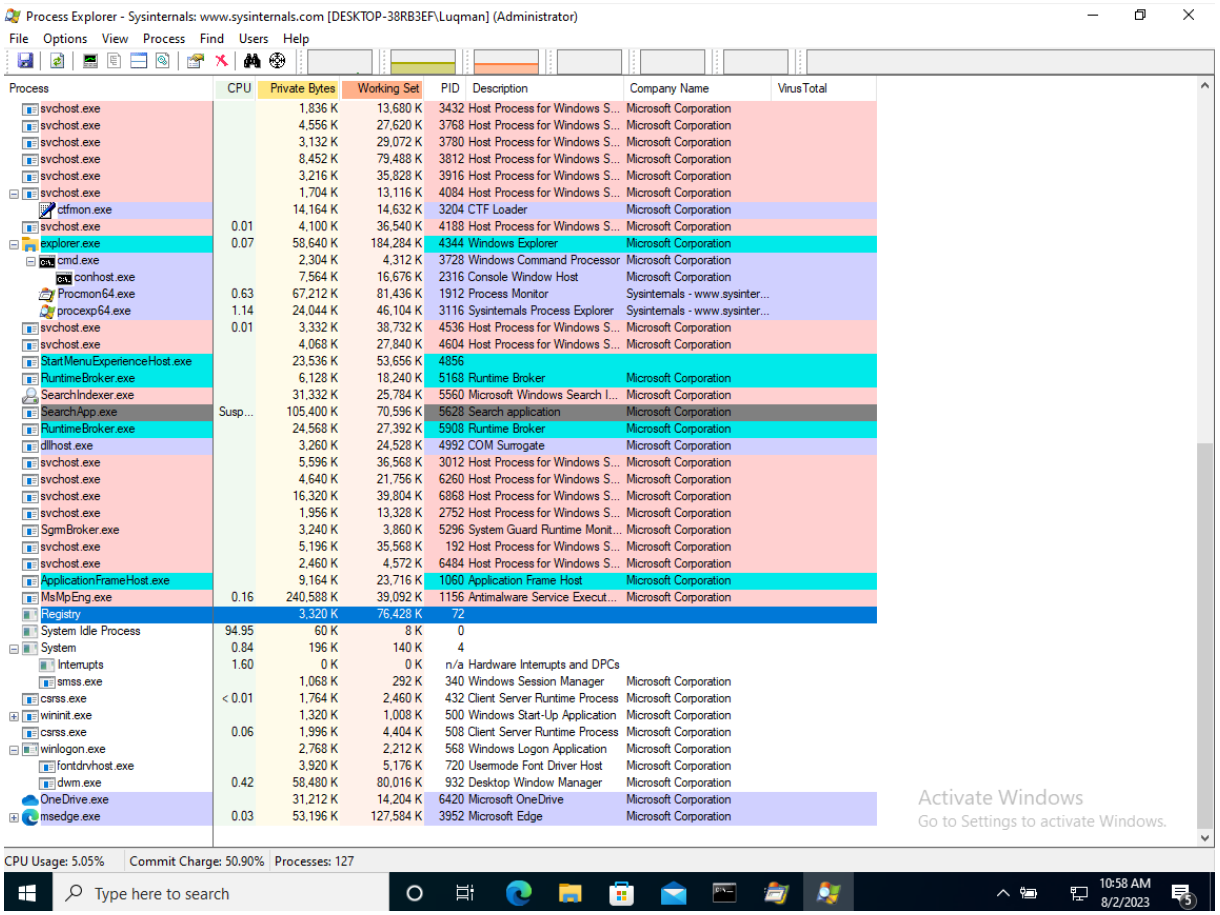



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38RB3EF\Luqman] (Administrator)
File Options View Process Find Users Help
Process
CPU
Private Bytes
Working Set
PID
Description
Company Name
VirusTotal
Process Explorer
Are you sure you want to kill firefox.exe?
OK
Cancel
Your computer files 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 fi
As soon as the payment is received the crypted files will be returned to normal.
Thank you
Activate Windows
Go to Settings to activate Windows.

B) Killing "drpbx.exe" terminates another instance of the "Welcome" screen.

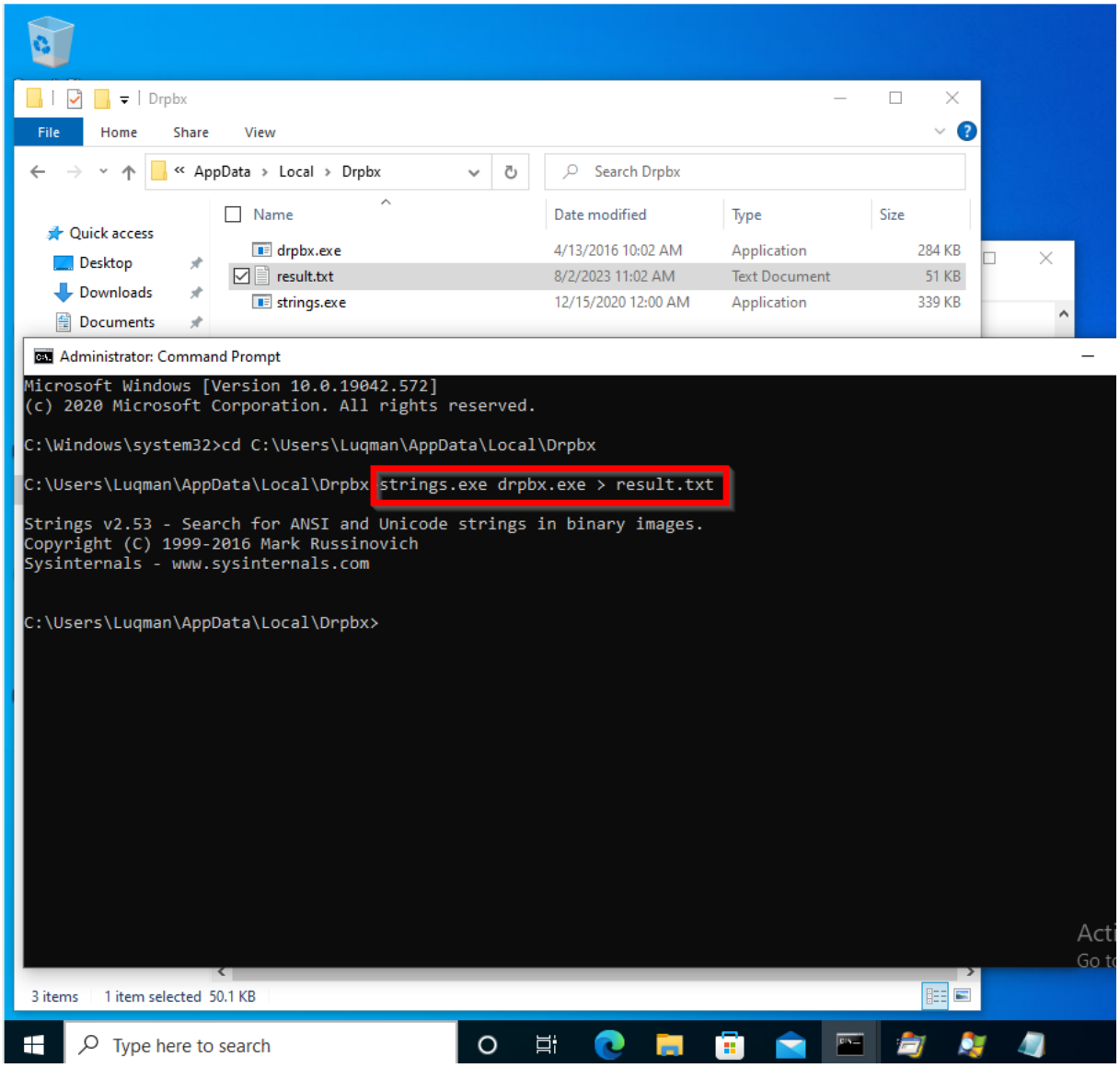


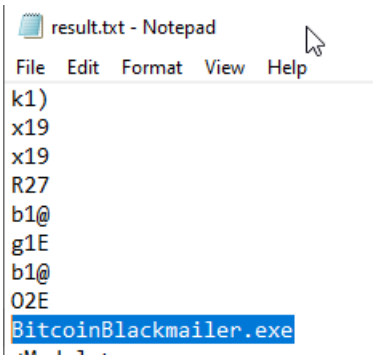




Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38RB3EF\Luqman] (Administrator)
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name VirusTotal
svchost.exe 1,836 K 13,680 K 3432 Host Process for Windows S... Microsoft Corporation
svchost.exe 4,556 K 27,620 K 3768 Host Process for Windows S... Microsoft Corporation
svchost.exe 3,132 K 29,072 K 3780 Host Process for Windows S... Microsoft Corporation
svchost.exe 8,452 K 79,488 K 3812 Host Process for Windows S... Microsoft Corporation
svchost.exe 3,216 K 35,828 K 3916 Host Process for Windows S... Microsoft Corporation
svchost.exe 1,704 K 13,116 K 4084 Host Process for Windows S... Microsoft Corporation
ctfmon.exe 14,164 K 14,632 K 3204 CTF Loader Microsoft Corporation
svchost.exe 0.01 4,100 K 36,540 K 4188 Host Process for Windows S... Microsoft Corporation
explorer.exe 0.07 58,640 K 184,284 K 4344 Windows Explorer Microsoft Corporation
cmd.exe 2,304 K 4,312 K 3728 Windows Command Processor Microsoft Corporation
conhost.exe 7,564 K 16,676 K 2316 Console Window Host Microsoft Corporation
Procmon64.exe 0.63 67,212 K 81,436 K 1912 Process Monitor Sysinternals - www.sysinter...
procexp64.exe 1.14 24,044 K 46,104 K 3116 Sysinternals Process Explorer Sysinternals - www.sysinter...
svchost.exe 0.01 3,332 K 38,732 K 4536 Host Process for Windows S... Microsoft Corporation
svchost.exe 4,068 K 27,840 K 4604 Host Process for Windows S... Microsoft Corporation
StartMenuExperienceHost.exe 23,536 K 53,656 K 4856
RuntimeBroker.exe 6,128 K 18,240 K 5168 Runtime Broker Microsoft Corporation
SearchIndexer.exe 31,332 K 25,784 K 5560 Microsoft Windows Search I... Microsoft Corporation
SearchApp.exe Susp... 105,400 K 70,596 K 5628 Search application Microsoft Corporation
RuntimeBroker.exe 24,568 K 27,392 K 5908 Runtime Broker Microsoft Corporation
dllhost.exe 3,260 K 24,528 K 4992 COM Surrogate Microsoft Corporation
svchost.exe 5,596 K 36,568 K 3012 Host Process for Windows S... Microsoft Corporation
svchost.exe 4,640 K 21,756 K 6260 Host Process for Windows S... Microsoft Corporation
svchost.exe 16,320 K 39,804 K 6868 Host Process for Windows S... Microsoft Corporation
svchost.exe 1,956 K 13,328 K 2752 Host Process for Windows S... Microsoft Corporation
SgrmBroker.exe 3,240 K 3,860 K 5296 System Guard Runtime Monit... Microsoft Corporation
svchost.exe 5,196 K 35,568 K 192 Host Process for Windows S... Microsoft Corporation
svchost.exe 2,460 K 4,572 K 6484 Host Process for Windows S... Microsoft Corporation
ApplicationFrameHost.exe 9,164 K 23,716 K 1060 Application Frame Host Microsoft Corporation
MsMpEng.exe 0.16 240,588 K 39,092 K 1156 Antimalware Service Execut... Microsoft Corporation
Registry 3,320 K 76,428 K 72
System Idle Process 94.95 60 K 8 K 0
System 0.84 196 K 140 K 4
Interrupts 1.60 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 1,068 K 292 K 340 Windows Session Manager Microsoft Corporation
csrss.exe < 0.01 1,764 K 2,460 K 432 Client Server Runtime Process Microsoft Corporation
wininit.exe 1,320 K 1,008 K 500 Windows Start-Up Application Microsoft Corporation
csrss.exe 0.06 1,996 K 4,404 K 508 Client Server Runtime Process Microsoft Corporation
winlogon.exe 2,768 K 2,212 K 568 Windows Logon Application Microsoft Corporation
fontdrvhost.exe 3,920 K 5,176 K 720 Usermode Font Driver Host Microsoft Corporation
dwm.exe 0.42 58,480 K 80,016 K 932 Desktop Window Manager Microsoft Corporation
OneDrive.exe 31,212 K 14,204 K 6420 Microsoft OneDrive Microsoft Corporation
msedge.exe 0.03 53,196 K 127,584 K 3952 Microsoft Edge Microsoft Corporation
Activate Windows
Go to Settings to activate Windows.
CPU Usage: 5.05% Commit Charge: 50.90% Processes: 127
Type here to search
10:58 AM
8/2/2023

## 5. Indicators of Malware:

The following strings serve as indicators of the malware's malicious nature:



result.txt - Notepad

File Edit Format View Help

```
path
EncryptFiles
dirPath
encryptionExtension
extensionsToEncrypt
DecryptFiles
EncryptFile
DecryptFile
SymmetricAlgorithm
System.Security.Cryptography
alg
inputFile
outputFile
DriveInfo
IEnumerator
System.Collections
StringComparison
AesCryptoServiceProvider
Array
RuntimeFieldHandle
FileStream
FileMode
ICryptoTransform
CryptoStream
CryptoStreamMode
<>9__4_0
<>9__9_1
```

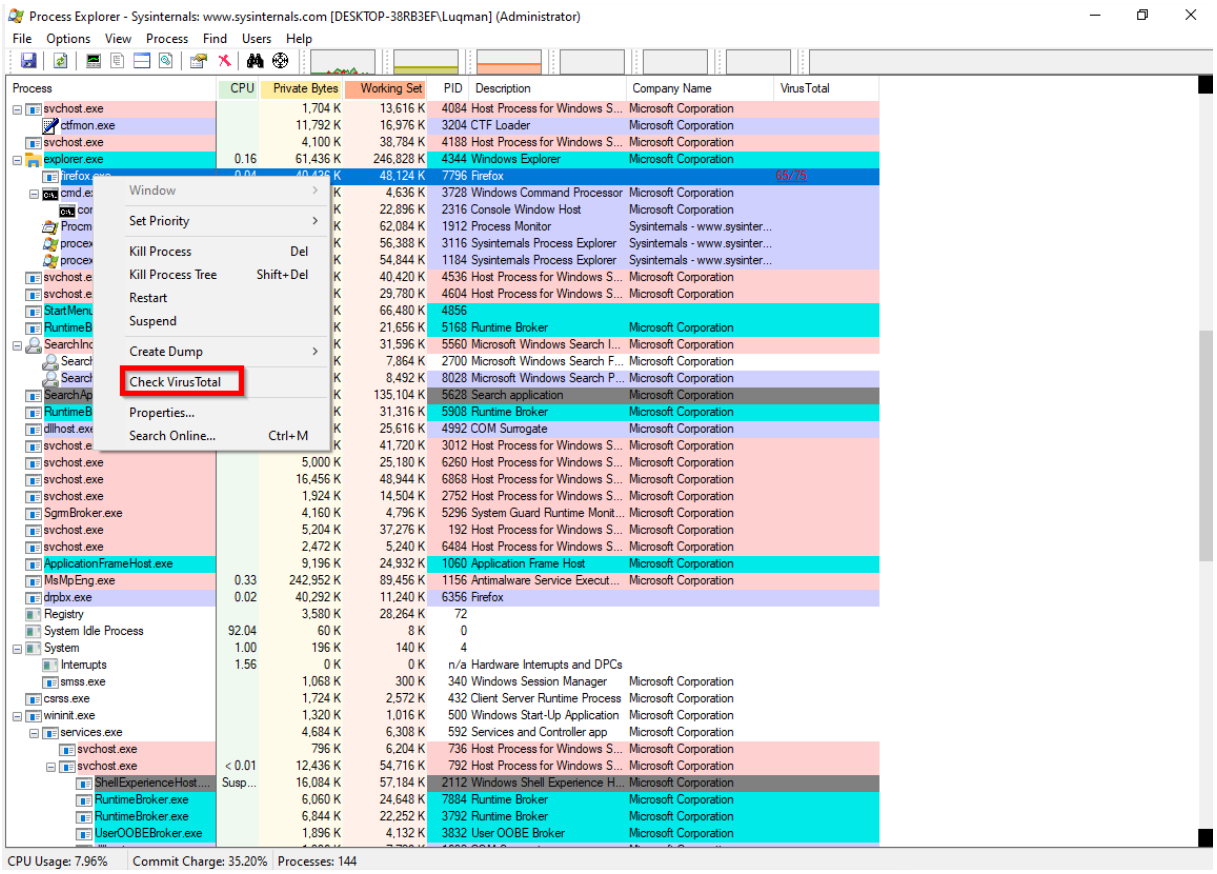
result.txt - Notepad

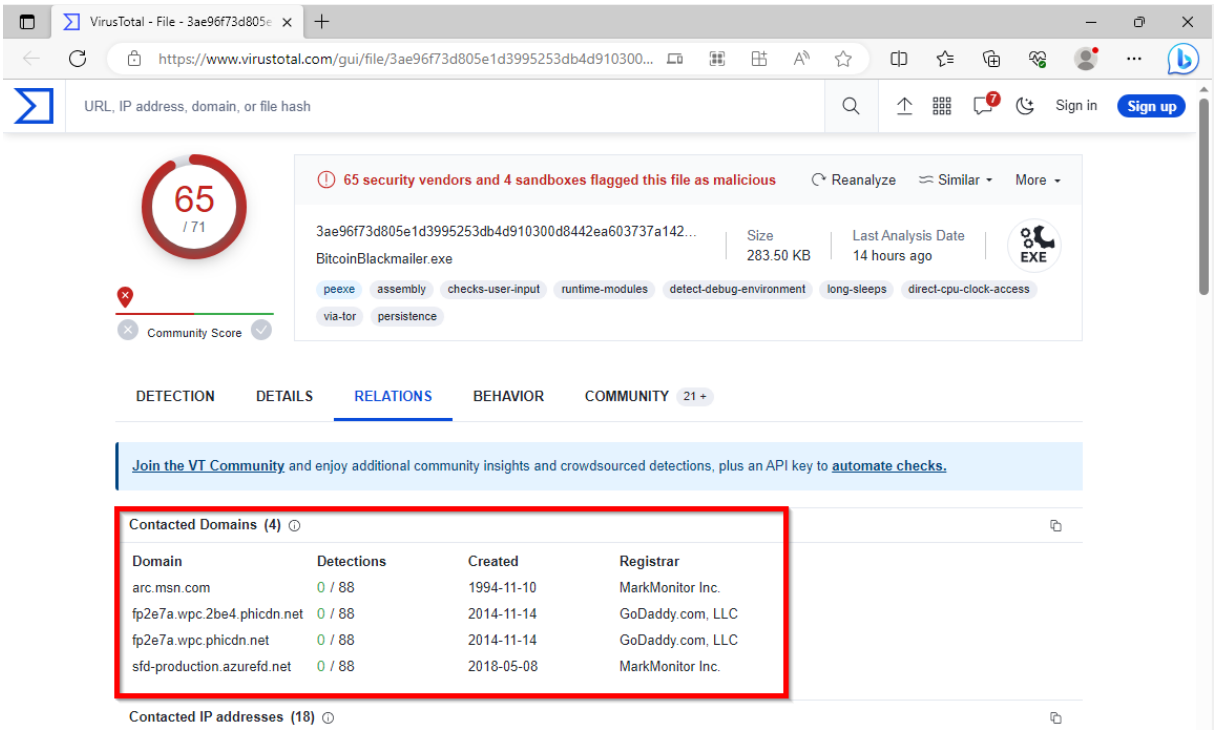
File Edit Format View Help

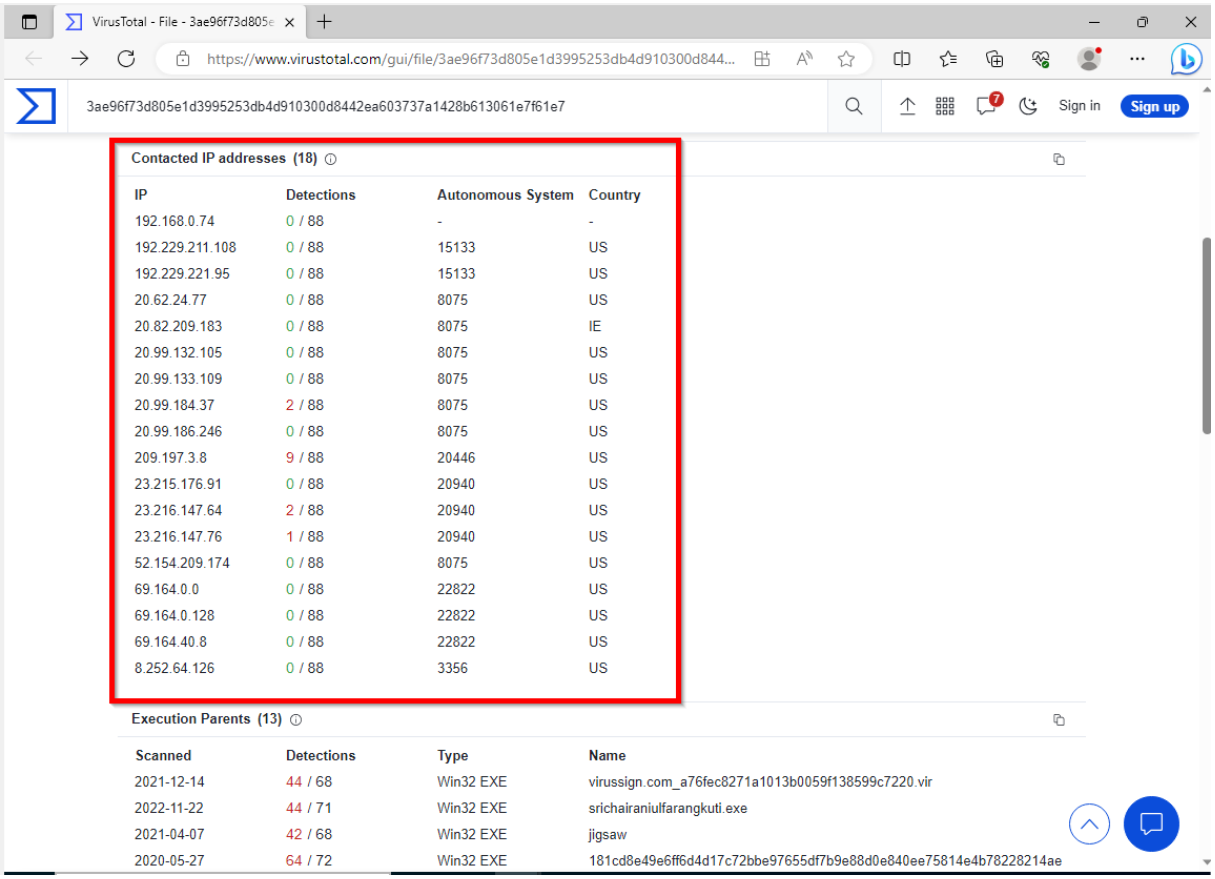
```
If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return
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:
FormBackground
Form1
.fun
YES
dataGridViewEncryptedFiles
Deleted
ColumnDeleted
Path
ColumnPath
FormEncryptedFiles
EncryptedFiles
Address.txt
You are about to make a very bad decision. Are you sure about it?
Great job, I'm decrypting your files...
Decrypting your files. It will take for a while. After done I will close and completely remove myself
Great job
You did not sent me enough! Try again!
You haven't made payment yet! Try again!
Are you connected to the internet? Try again!
```

## 6. Associated Domains and IPs:

IP addresses and associated domains linked to the malware were discovered on VirusTotal:



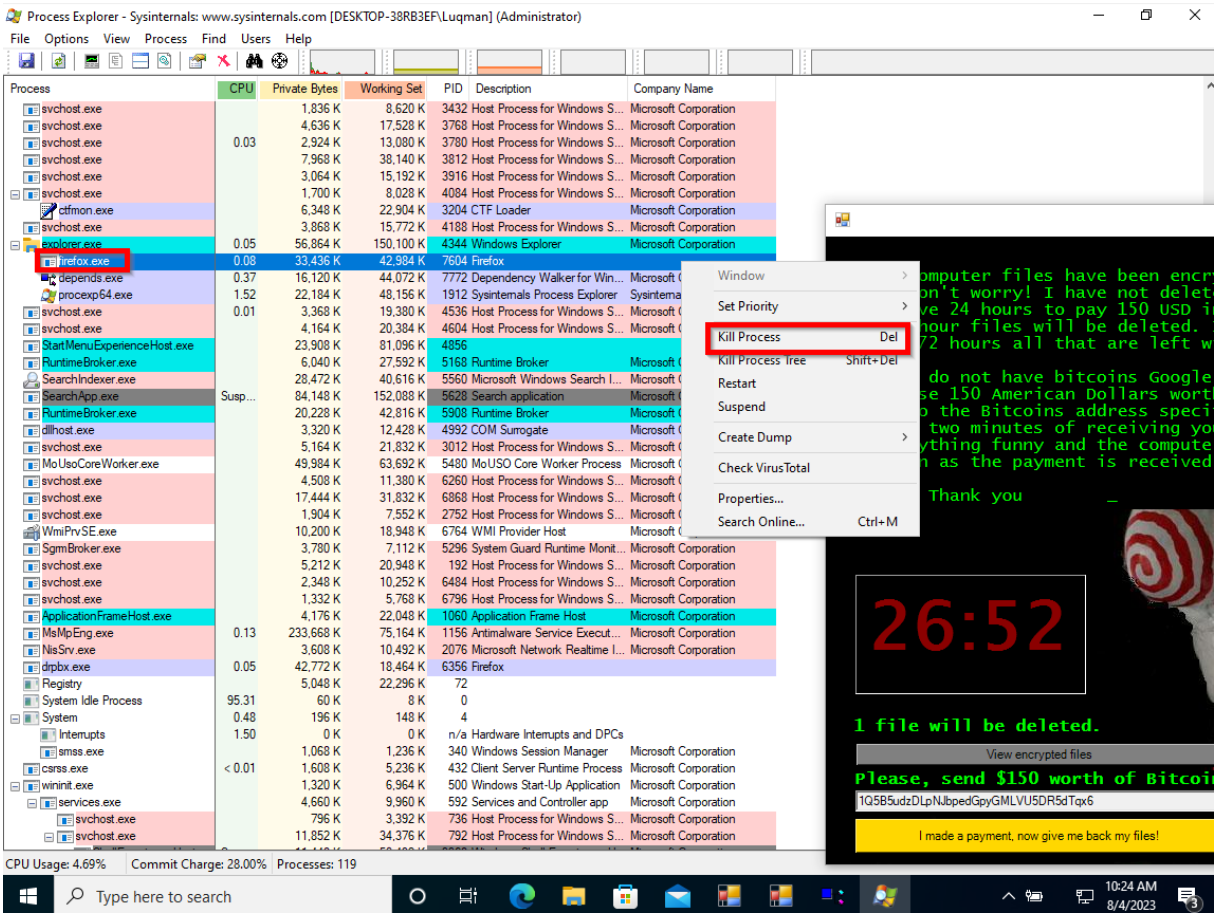



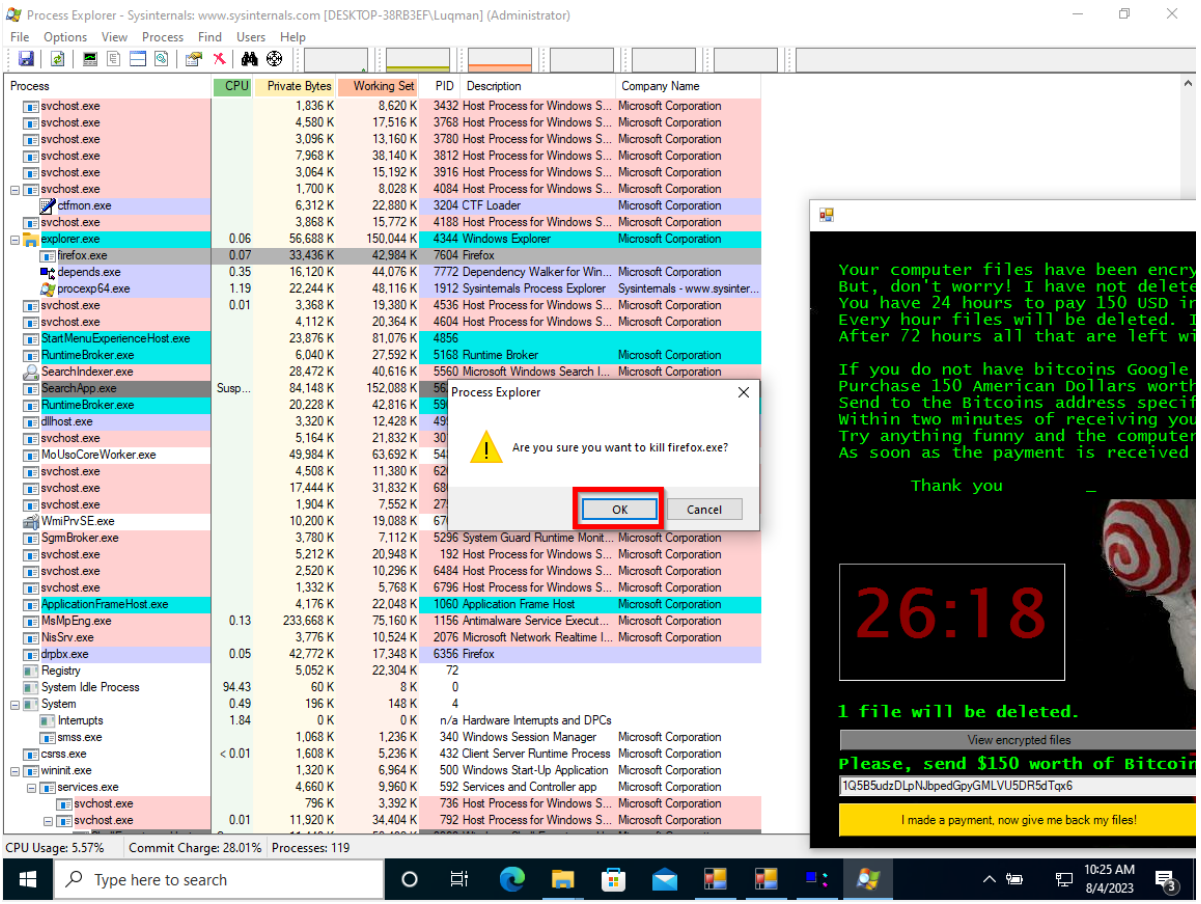

VirusTotal - File - 3ae96f73d805e
https://www.virustotal.com/gui/file/3ae96f73d805e1d3995253db4d910300d844...
3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7
Sign in
Sign up
Contacted IP addresses (18)
IP Detections Autonomous System Country
192.168.0.74 0 / 88 - -
192.229.211.108 0 / 88 15133 US
192.229.221.95 0 / 88 15133 US
20.62.24.77 0 / 88 8075 US
20.82.209.183 0 / 88 8075 IE
20.99.132.105 0 / 88 8075 US
20.99.133.109 0 / 88 8075 US
20.99.184.37 2 / 88 8075 US
20.99.186.246 0 / 88 8075 US
209.197.3.8 9 / 88 20446 US
23.215.176.91 0 / 88 20940 US
23.216.147.64 2 / 88 20940 US
23.216.147.76 1 / 88 20940 US
52.154.209.174 0 / 88 8075 US
69.164.0.0 0 / 88 22822 US
69.164.0.128 0 / 88 22822 US
69.164.40.8 0 / 88 22822 US
8.252.64.126 0 / 88 3356 US
Execution Parents (13)
Scanned Detections Type Name
2021-12-14 44 / 68 Win32 EXE virussign.com_a76fec8271a1013b0059f138599c7220.vir
2022-11-22 44 / 71 Win32 EXE srichairaniulfarangkuti.exe
2021-04-07 42 / 68 Win32 EXE jigsaw
2020-05-27 64 / 72 Win32 EXE 181cd8e49e6ff6d4d17c72bbe97655df7b9e88d0e840ee75814e4b78228214ae

**7. Termination of Malicious Processes:**

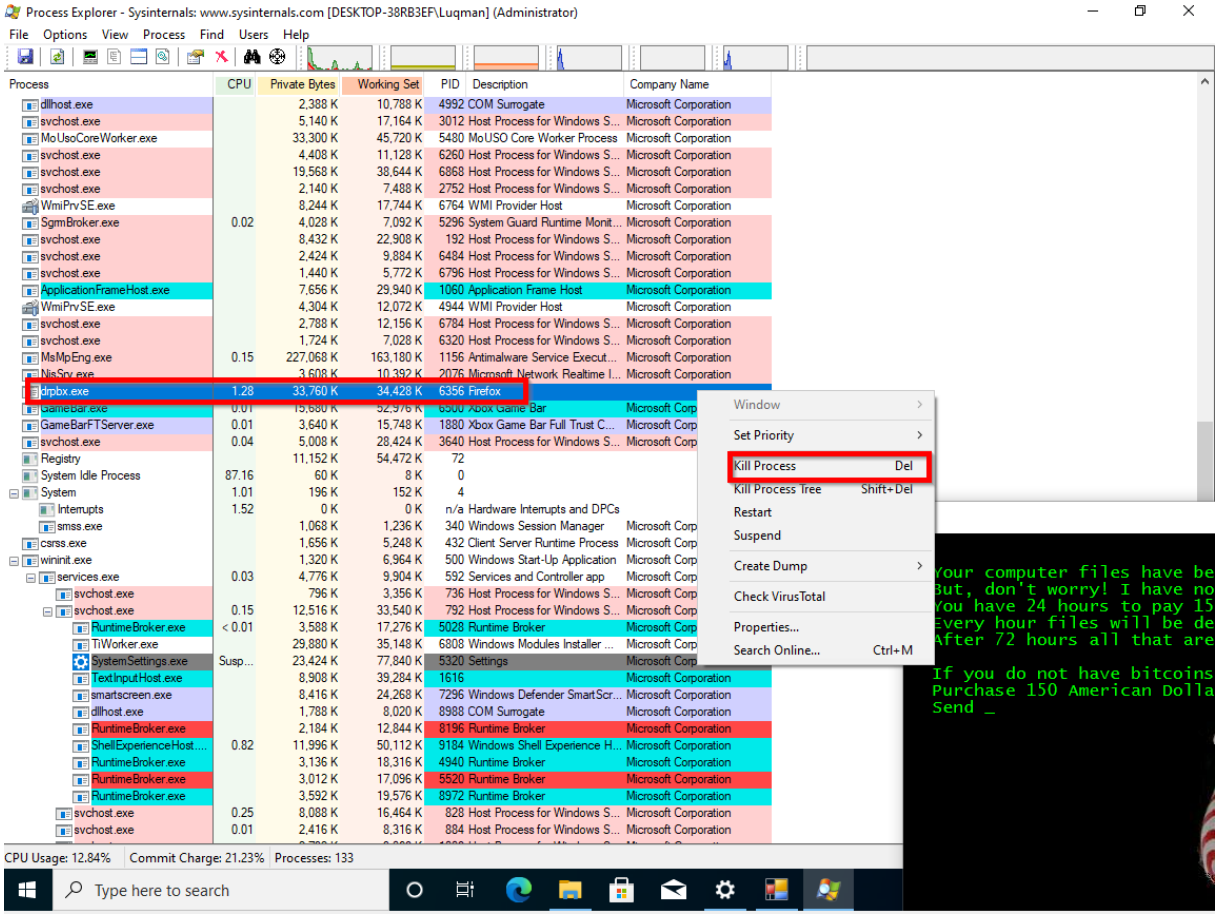
1.I identified and put a kill to two processes, 'firefox.exe' and 'drpbx.exe', within the Process Explorer utility. This deliberate intervention effectively severed the ransomware's ability to further encrypt files and propagate its malevolent actions.

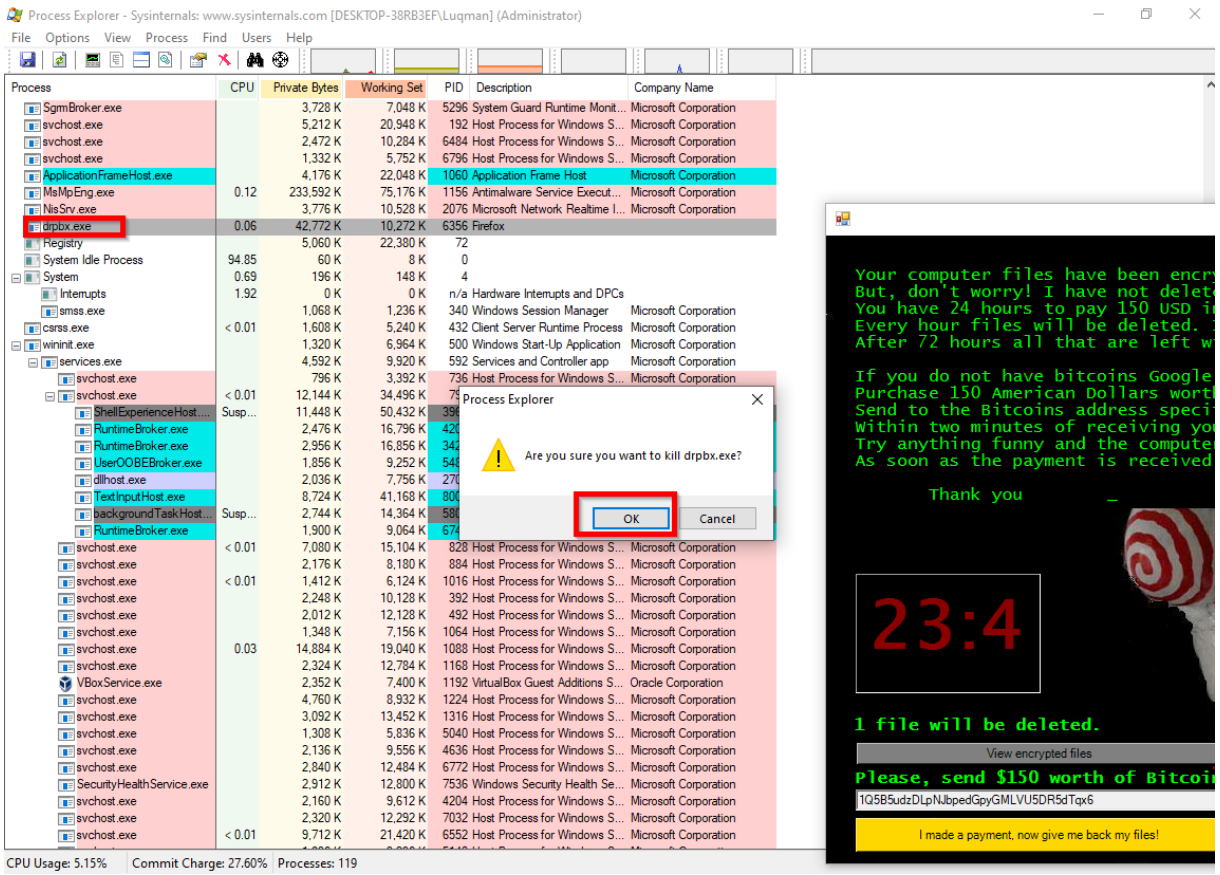
A) firefox.exe




Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38RB3EF\Luqman] (Administrator)
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name
Process Explorer
Are you sure you want to kill firefox.exe?
OK
Cancel
Your computer files have been encry
But, don't worry! I have not delete
You have 24 hours to pay 150 USD in
Every hour files will be deleted. I
After 72 hours all that are left wi
If you do not have bitcoins Google
Purchase 150 American Dollars worth
Send to the Bitcoins address specif
Within two minutes of receiving you
Try anything funny and the computer
As soon as the payment is received
Thank you
26:18
1 file will be deleted.
View encrypted files
Please, send $150 worth of Bitcoin
1Q5B5udzDLpNJbpedGpyGMLVU5DR5dTqx6
I made a payment, now give me back my files!
CPU Usage: 5.57% Commit Charge: 28.01% Processes: 119
Type here to search
10:25 AM
8/4/2023

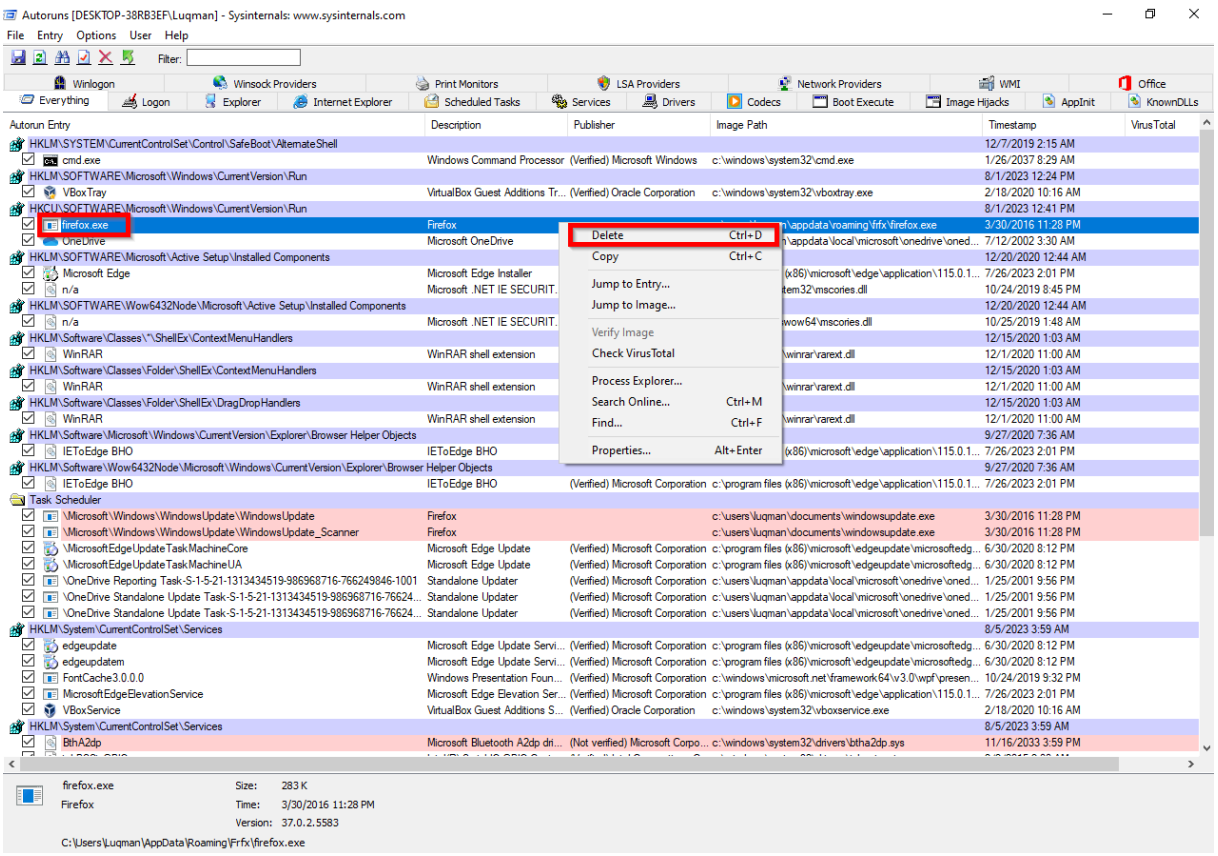
## B) Drpbx.exe

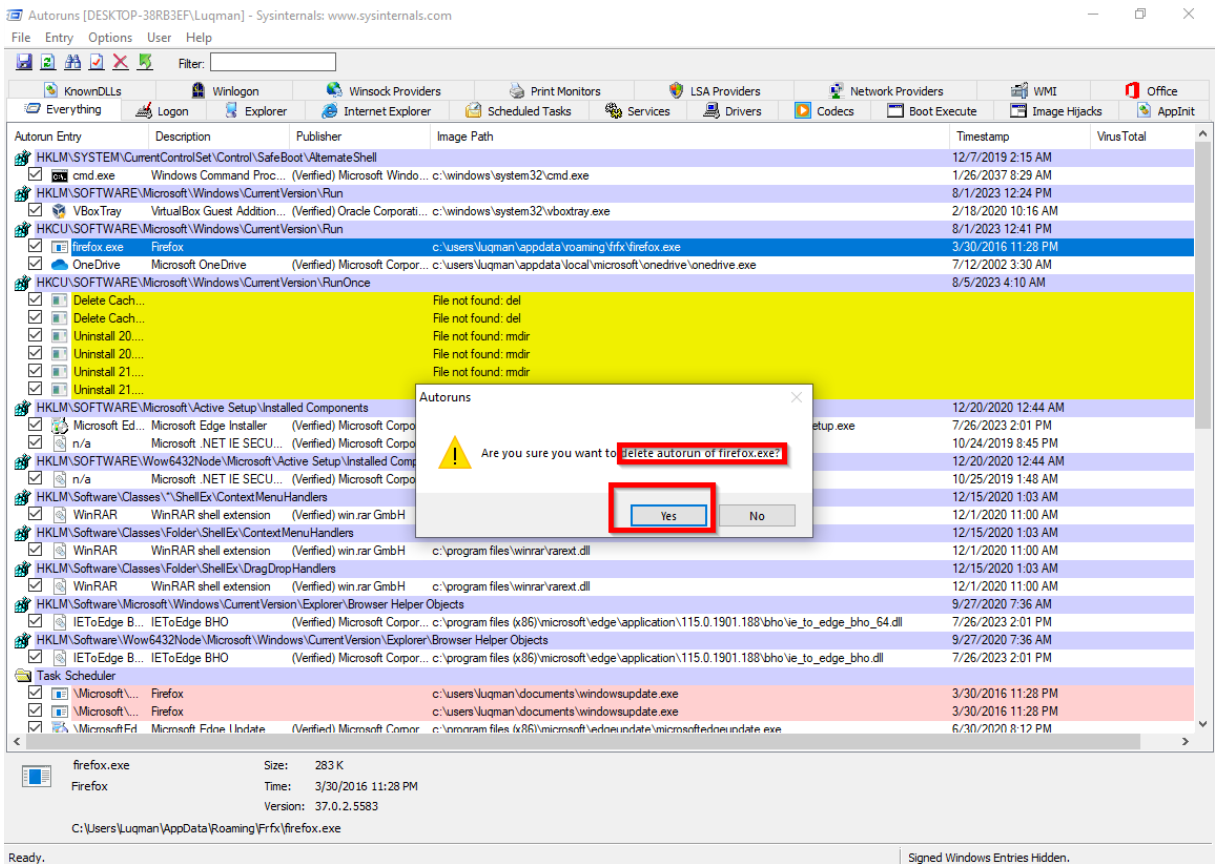

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38RB3EF\Luqman] (Administrator)
File Options View Process Find Users Help
dropbx.exe 1.28 33,760 K 34,428 K 6356 Firefox
Window
Set Priority
Kill Process Del
Kill Process Tree Shift+Del
Restart
Suspend
Create Dump
Check VirusTotal
Properties...
Search Online... Ctrl+M
Your computer files have be
But, don't worry! I have no
You have 24 hours to pay 15
Every hour files will be de
After 72 hours all that are
If you do not have bitcoins
Purchase 150 American Dolla
Send _
CPU Usage: 12.84% Commit Charge: 21.23% Processes: 133
Type here to search


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38RB3EF\Luqman] (Administrator)
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name
drpbx.exe 0.06 42,772 K 10,272 K 6356 Firefox
Process Explorer
Are you sure you want to kill drpbx.exe?
OK
Cancel
Your computer files have been encr
But, don't worry! I have not delet
You have 24 hours to pay 150 USD i
Every hour files will be deleted.
After 72 hours all that are left w
If you do not have bitcoins Google
Purchase 150 American Dollars wort
Send to the Bitcoins address speci
Within two minutes of receiving yo
Try anything funny and the compute
As soon as the payment is received
Thank you
23:4
1 file will be deleted.
View encrypted files
Please, send $150 worth of Bitcoi
1Q5B5udzDLpNJbpedGpyGMLVU5DR5dTqx6
I made a payment, now give me back my files!
CPU Usage: 5.15% Commit Charge: 27.60% Processes: 119

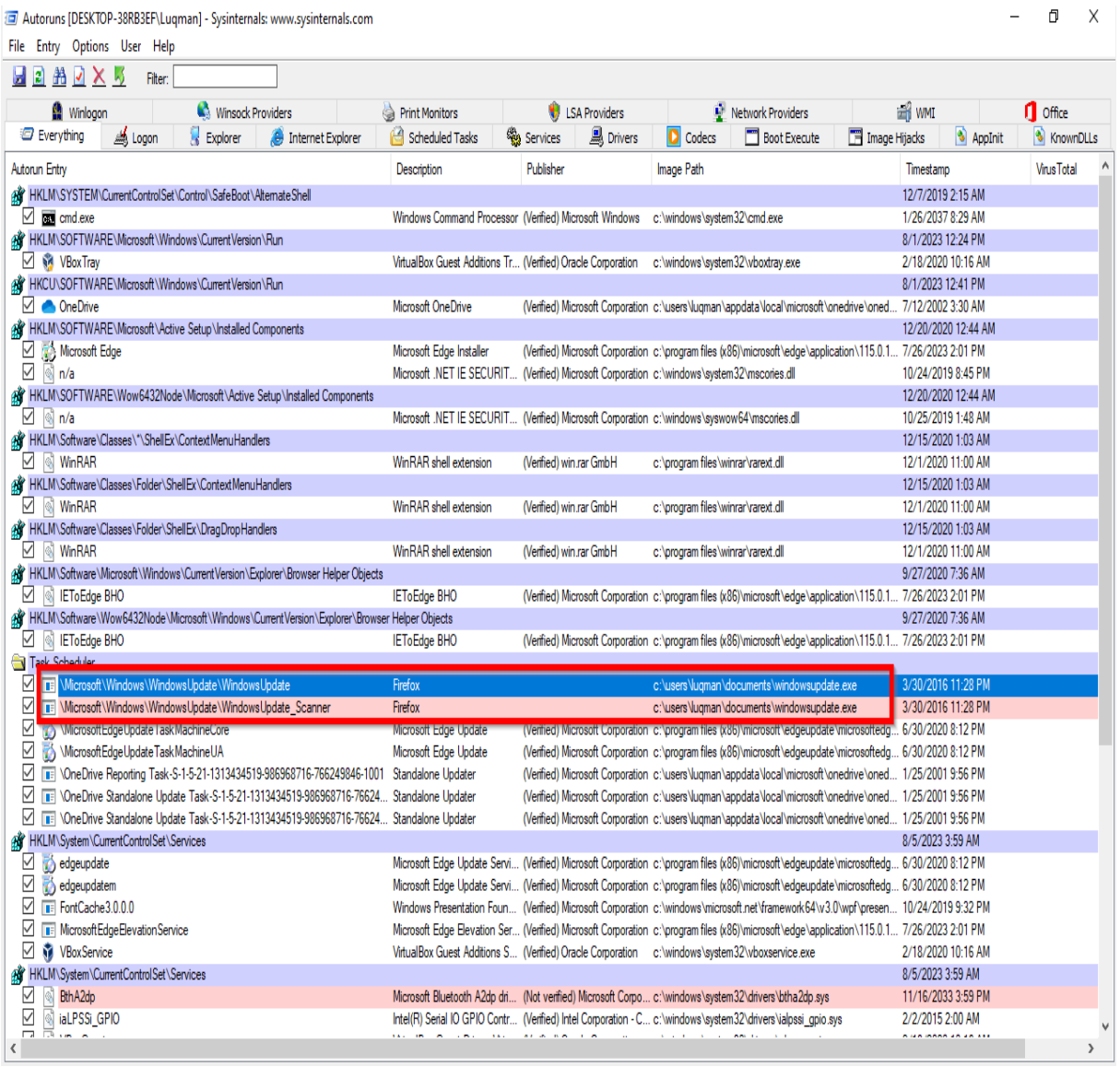
2. **Investigation and Prudent Removal:** Delving deeper, I turned my attention to 'Autoruns62.exe', a tool for managing startup entries. My meticulous scrutiny led me to discern suspicious entries, named 'firefox.exe' located at ‘C:\Users\Luqman\AppData\Roamin\Frfx’ , 'WindowsUpdate.', and 'WindowsUpdate_Scanner.', a localized within the 'C:\Users\Luqman\Documents' directory. Notably, 'WindowsUpdate.' and 'WindowsUpdate_Scanner', Alarming patterns emerged that those two processes doesn’t exists in Windows 10 system. Originally are named as **wuauserv.exe** and **UsoClient.exe** . When I started the 'strings.exe' program, revealing stark resemblances to the strings associated with 'firefox.exe' and 'drpbx.exe'.

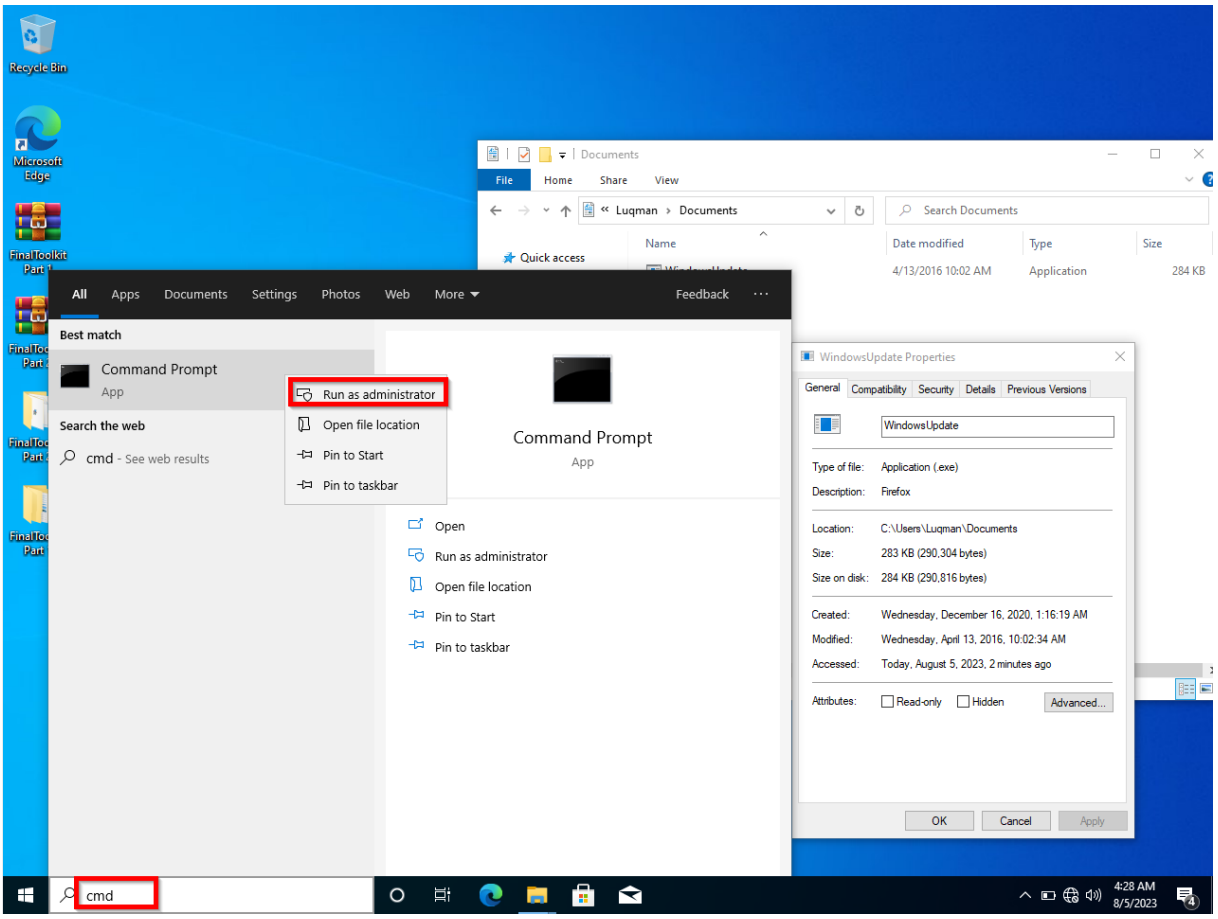
Armed with this newfound insight, I executed a decisive course of action. I promptly eliminated the aforementioned entries, thereby obliterating the presence of 'firefox.exe', 'drpbx.exe', 'WindowsUpdate', and 'WindowsUpdate_Scanner' from the system.

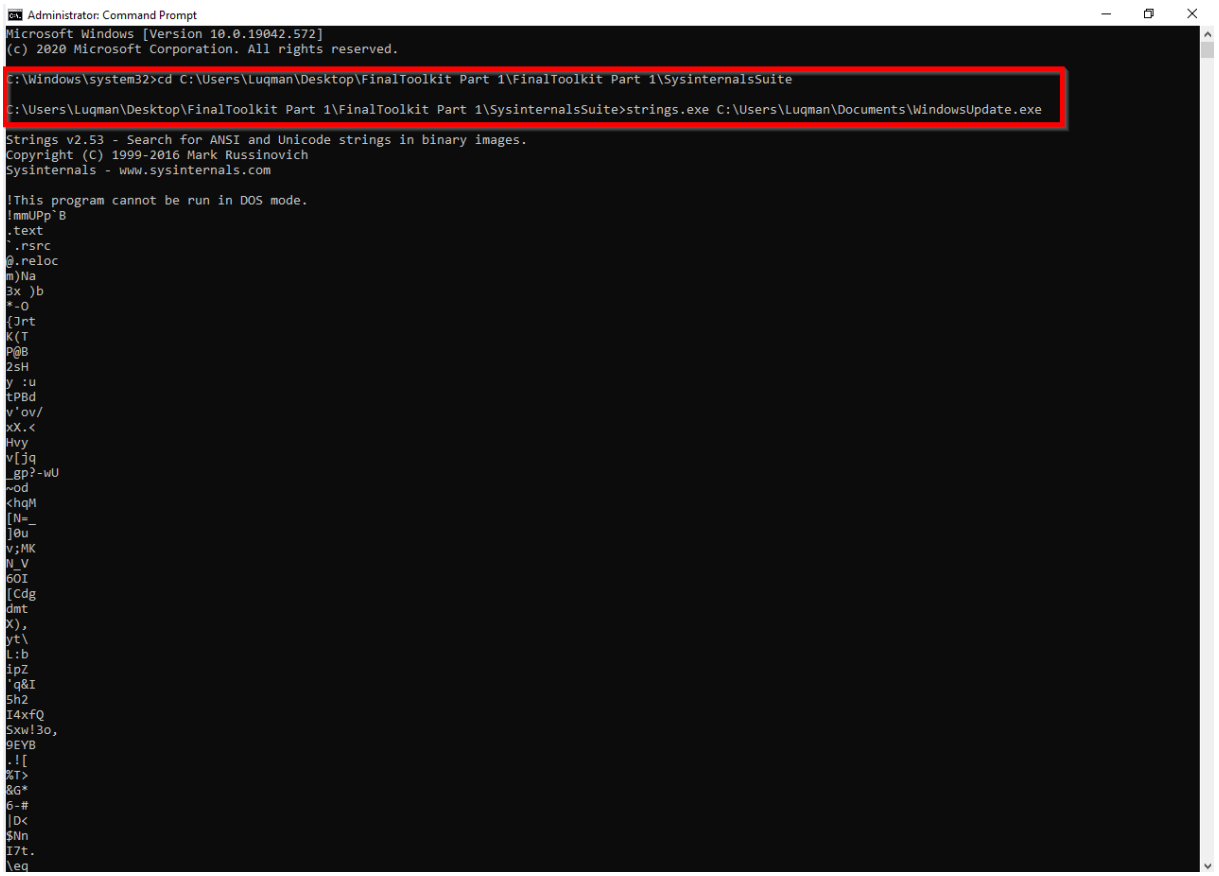


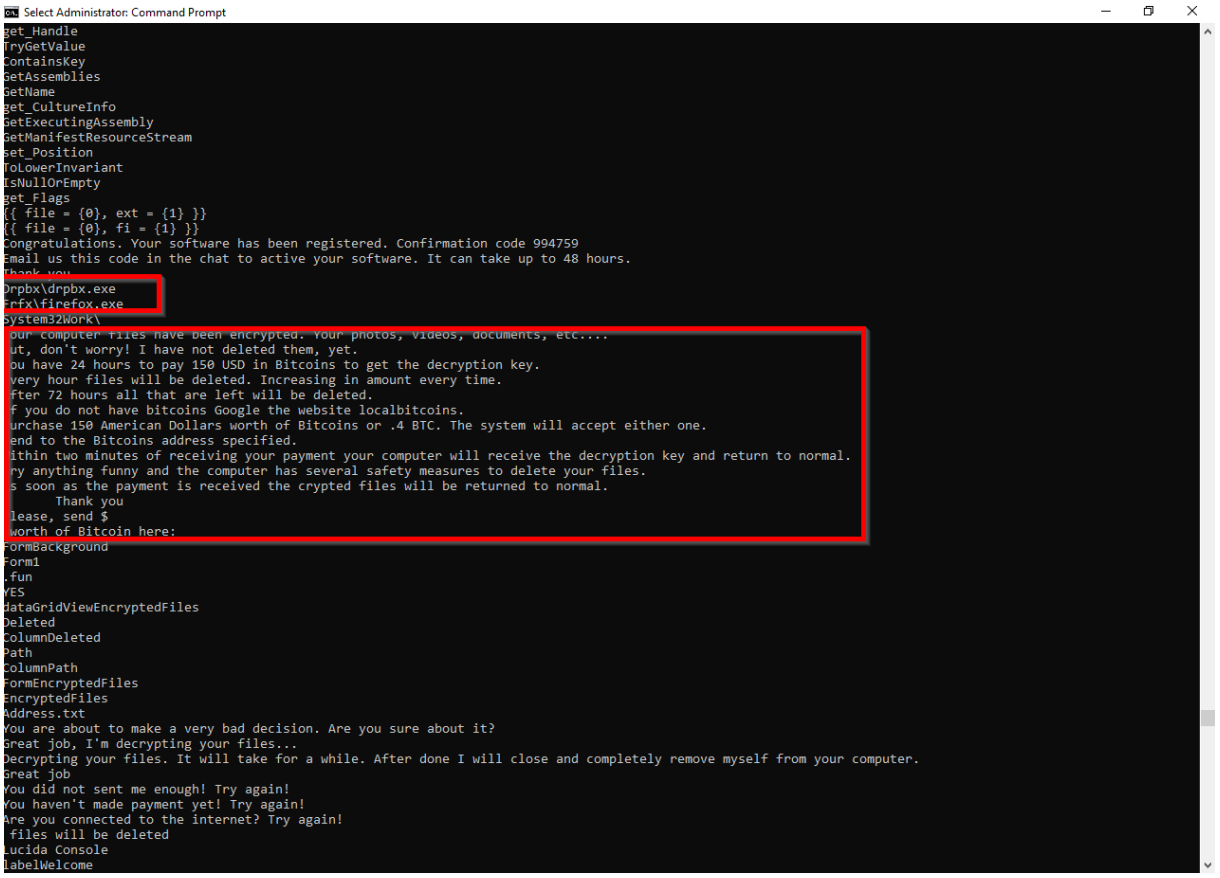

Autoruns [DESKTOP-38RB3EF\Luqman] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell 12/7/2019 2:15 AM
cmd.exe Windows Command Proc... (Verified) Microsoft Windo... c:\windows\system32\cmd.exe 1/26/2037 8:29 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 8/1/2023 12:24 PM
VBoxTray VirtualBox Guest Addition... (Verified) Oracle Corporati... c:\windows\system32\vboxtray.exe 2/18/2020 10:16 AM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 8/1/2023 12:41 PM
firefox.exe Firefox c:\users\luqman\appdata\roaming\frfx\firefox.exe 3/30/2016 11:28 PM
OneDrive Microsoft OneDrive (Verified) Microsoft Corpor... c:\users\luqman\appdata\local\microsoft\onedrive\onedrive.exe 7/12/2002 3:30 AM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 8/5/2023 4:10 AM
Delete Cach... File not found: del
Delete Cach... File not found: del
Uninstall 20... File not found: rmdir
Uninstall 20... File not found: rmdir
Uninstall 21... File not found: rmdir
Uninstall 21...
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components 12/20/2020 12:44 AM
Microsoft Ed... Microsoft Edge Installer (Verified) Microsoft Corpo 7/26/2023 2:01 PM
n/a Microsoft .NET IE SECU... (Verified) Microsoft Corpo 10/24/2019 8:45 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Comp 12/20/2020 12:44 AM
n/a Microsoft .NET IE SECU... (Verified) Microsoft Corpo 10/25/2019 1:48 AM
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers 12/15/2020 1:03 AM
WinRAR WinRAR shell extension (Verified) win.rar GmbH 12/1/2020 11:00 AM
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers 12/15/2020 1:03 AM
WinRAR WinRAR shell extension (Verified) win.rar GmbH c:\program files\winrar\rarext.dll 12/1/2020 11:00 AM
HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers 12/15/2020 1:03 AM
WinRAR WinRAR shell extension (Verified) win.rar GmbH c:\program files\winrar\rarext.dll 12/1/2020 11:00 AM
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects 9/27/2020 7:36 AM
IEToEdge B... IEToEdge BHO (Verified) Microsoft Corpor... c:\program files (x86)\microsoft\edge\application\115.0.1901.188\bho\ie_to_edge_bho_64.dll 7/26/2023 2:01 PM
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects 9/27/2020 7:36 AM
IEToEdge B... IEToEdge BHO (Verified) Microsoft Corpor... c:\program files (x86)\microsoft\edge\application\115.0.1901.188\bho\ie_to_edge_bho.dll 7/26/2023 2:01 PM
Task Scheduler
\Microsoft\... Firefox c:\users\luqman\documents\windowsupdate.exe 3/30/2016 11:28 PM
\Microsoft\... Firefox c:\users\luqman\documents\windowsupdate.exe 3/30/2016 11:28 PM
Autoruns
Are you sure you want to delete autorun of firefox.exe?
Yes
No
firefox.exe
Firefox
Size: 283 K
Time: 3/30/2016 11:28 PM
Version: 37.0.2.5583
C:\Users\Luqman\AppData\Roaming\Frfx\firefox.exe
Ready.
Signed Windows Entries Hidden.

Identified autoruns entry WindowsUpdate and WindowsUpdate_Scaner. Related to a file windowsupdate.exe and identified strings from WindowsUpdate.exe



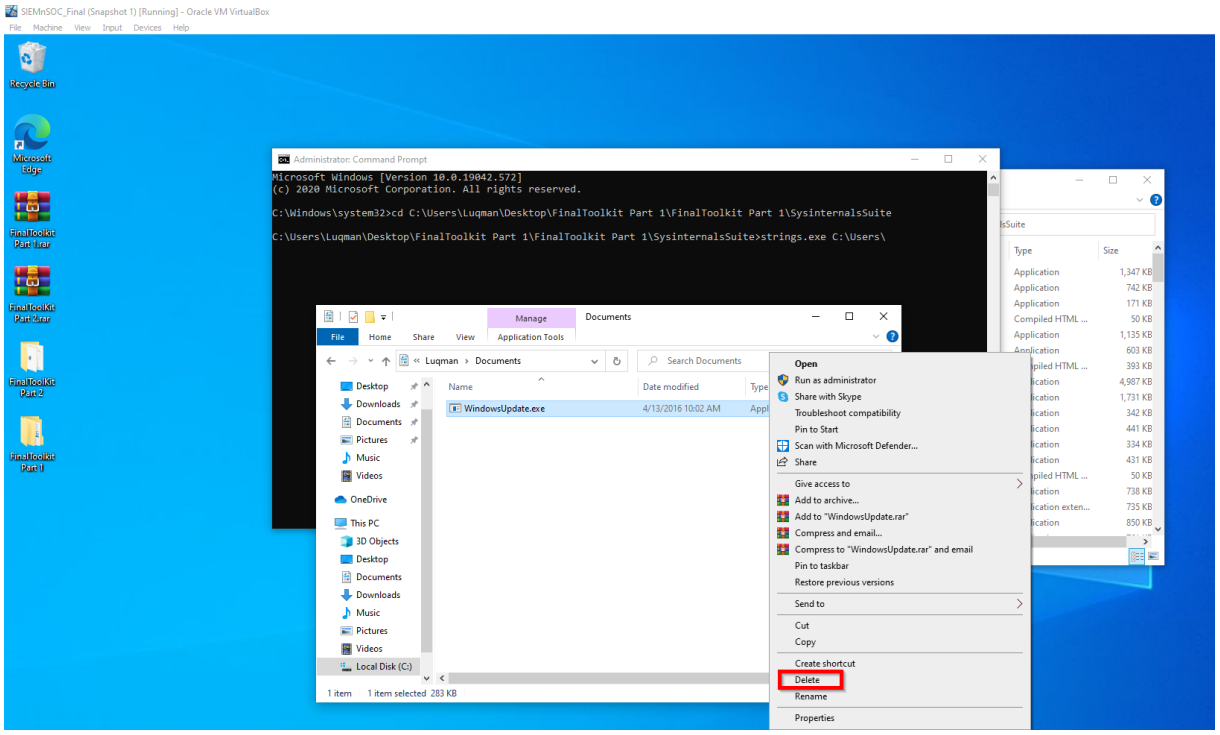

Recycle Bin
Microsoft Edge
FinalToolkit Part 1
Documents
File
Home
Share
View
Luqman › Documents
Search Documents
Quick access
Name
Date modified
Type
Size
4/13/2016 10:02 AM
Application
284 KB
All
Apps
Documents
Settings
Photos
Web
More
Feedback
Best match
Command Prompt
App
Search the web
cmd - See web results
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Command Prompt
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
WindowsUpdate Properties
General
Compatibility
Security
Details
Previous Versions
WindowsUpdate
Type of file: Application (.exe)
Description: Firefox
Location: C:\Users\Luqman\Documents
Size: 283 KB (290,304 bytes)
Size on disk: 284 KB (290,816 bytes)
Created: Wednesday, December 16, 2020, 1:16:19 AM
Modified: Wednesday, April 13, 2016, 10:02:34 AM
Accessed: Today, August 5, 2023, 2 minutes ago
Attributes: Read-only Hidden Advanced...
OK
Cancel
Apply
cmd
4:28 AM
8/5/2023


Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.572]
(c) 2020 Microsoft Corporation. All rights reserved.
c:\Windows\system32>cd C:\Users\Luqman\Desktop\FinalToolkit Part 1\FinalToolkit Part 1\SysinternalsSuite
C:\Users\Luqman\Desktop\FinalToolkit Part 1\FinalToolkit Part 1\SysinternalsSuite>strings.exe C:\Users\Luqman\Documents\WindowsUpdate.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.
!mmUPp`B
.text
`.rsrc
@.reloc
m)Na
3x )b
*-O
{Jrt
K(T
P@B
2sH
y :u
tPBd
v'ov/
xX.<
Hvy
v[jq
_gp?-wU
~od
<hqM
[N=_
]0u
v;MK
N_V
6OI
[Cdg
dmt
X),
yt\
L:b
ipZ
'q&I
5h2
I4xfQ
Sxw!3o,
9EYB
.![
%T>
&G*
6-#
|D<
$Nn
I7t.
\eq

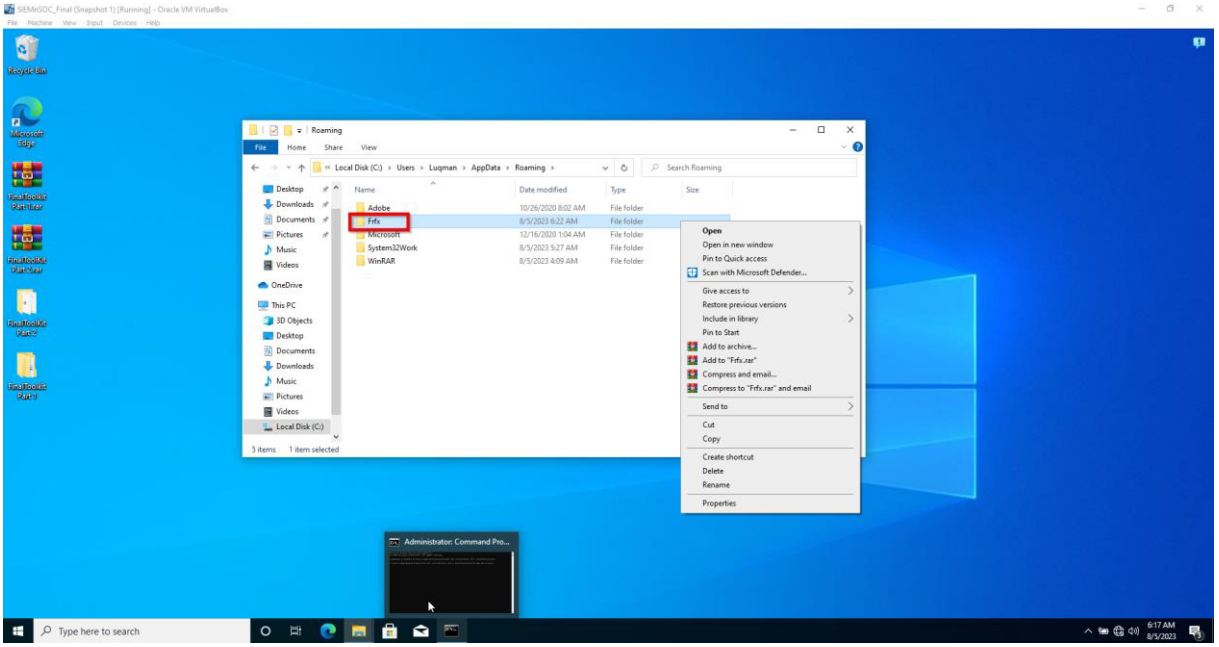



At the end I delete manually infected files and Directories which is :

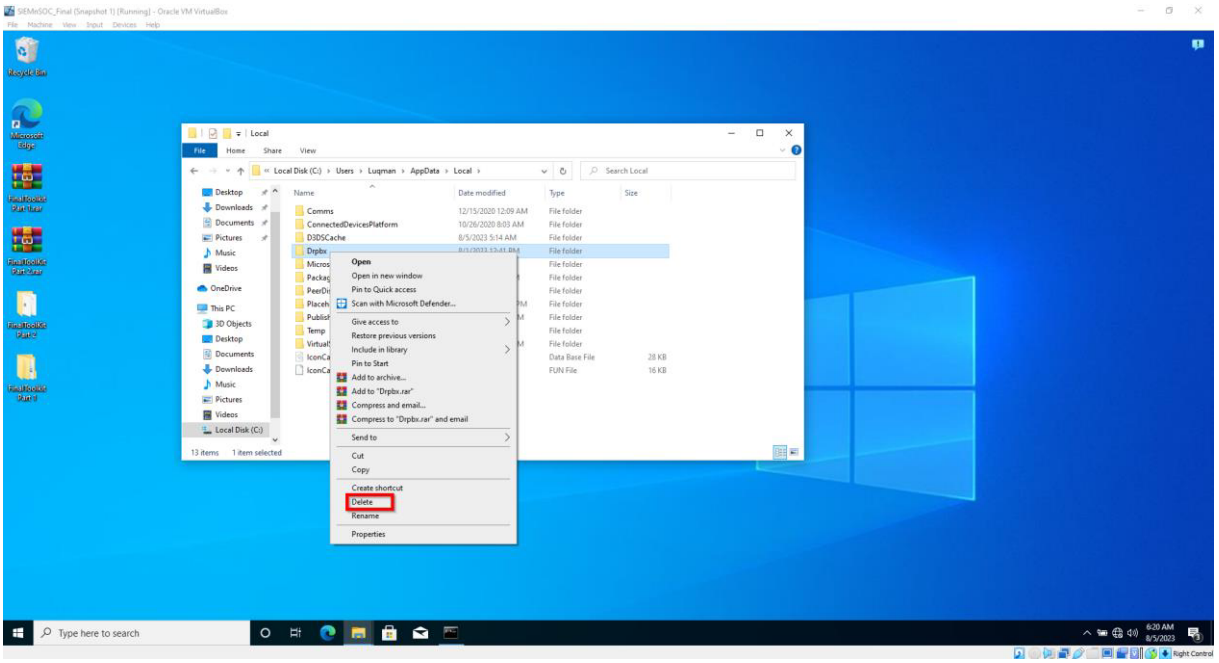
WindowsUpdate located at C:\Users\Luqman\Documents



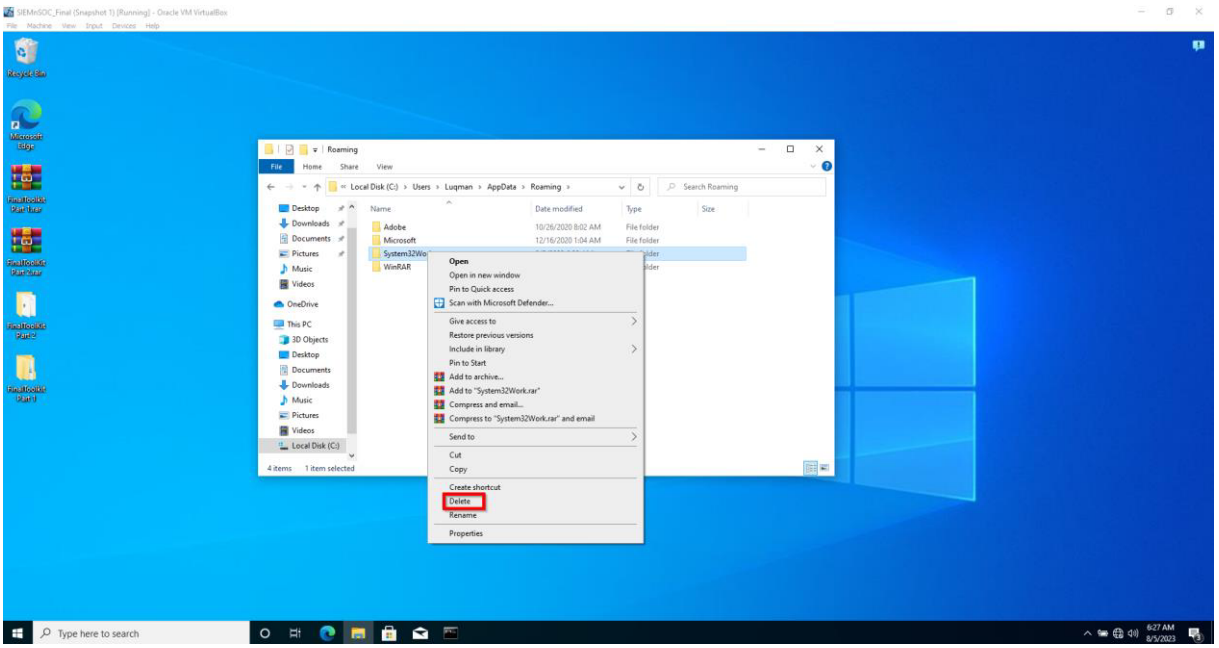
Firefox.exe located at C:\Users\Luqman\AppData\Roamin\Frfx



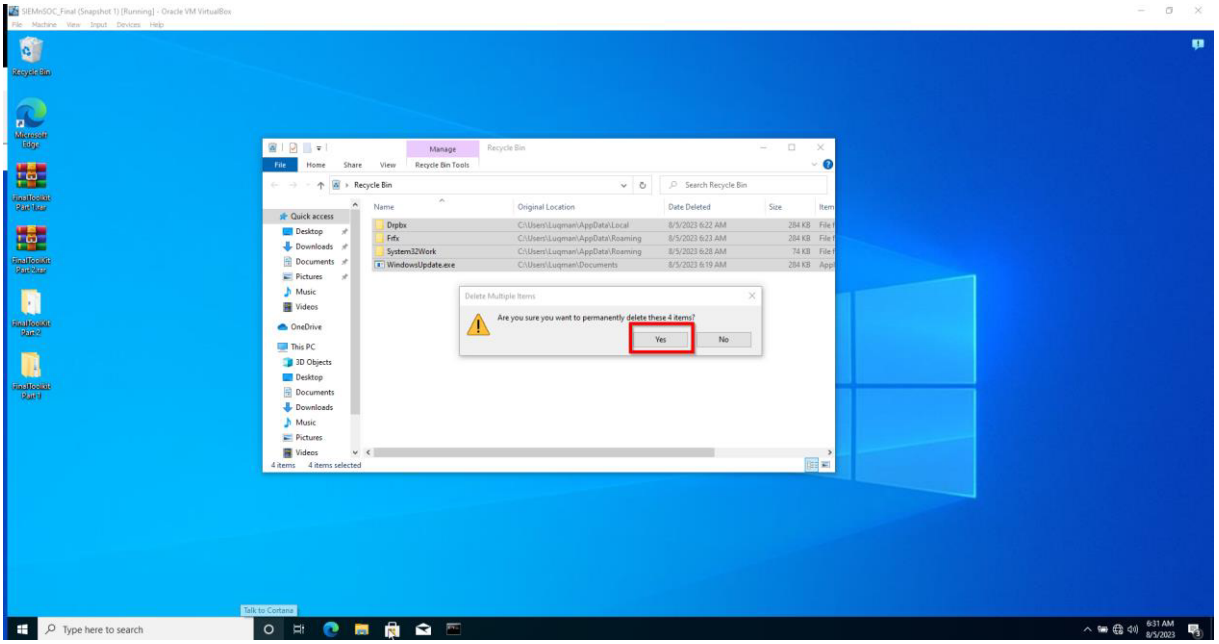
drpbx.exe locate at C:\Users\Luqman\AppData\Local\Drpbx




Also I deleted directory System32Work with contain files generated by ransomware “Jigsaw” Address.txt , dr , EncryptedFileList.txt located at C: \Users\Luqman\AppData\Roamin\System32Work



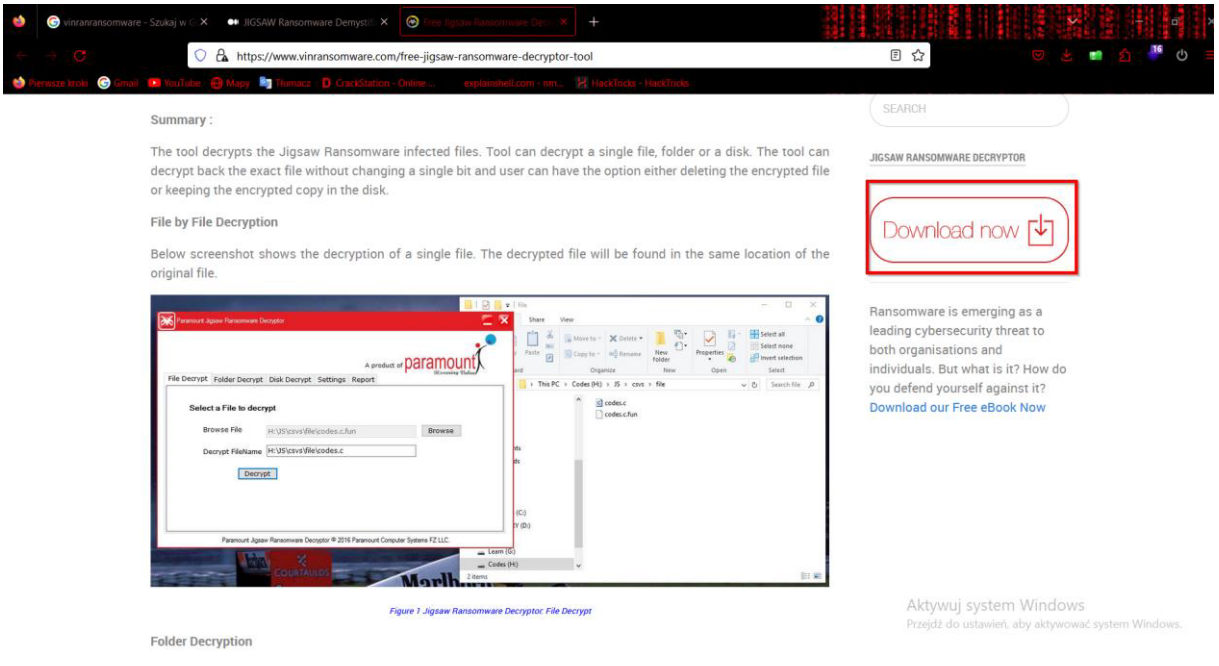
At the end I deleted those files and directories permanently by use Recycle bin.

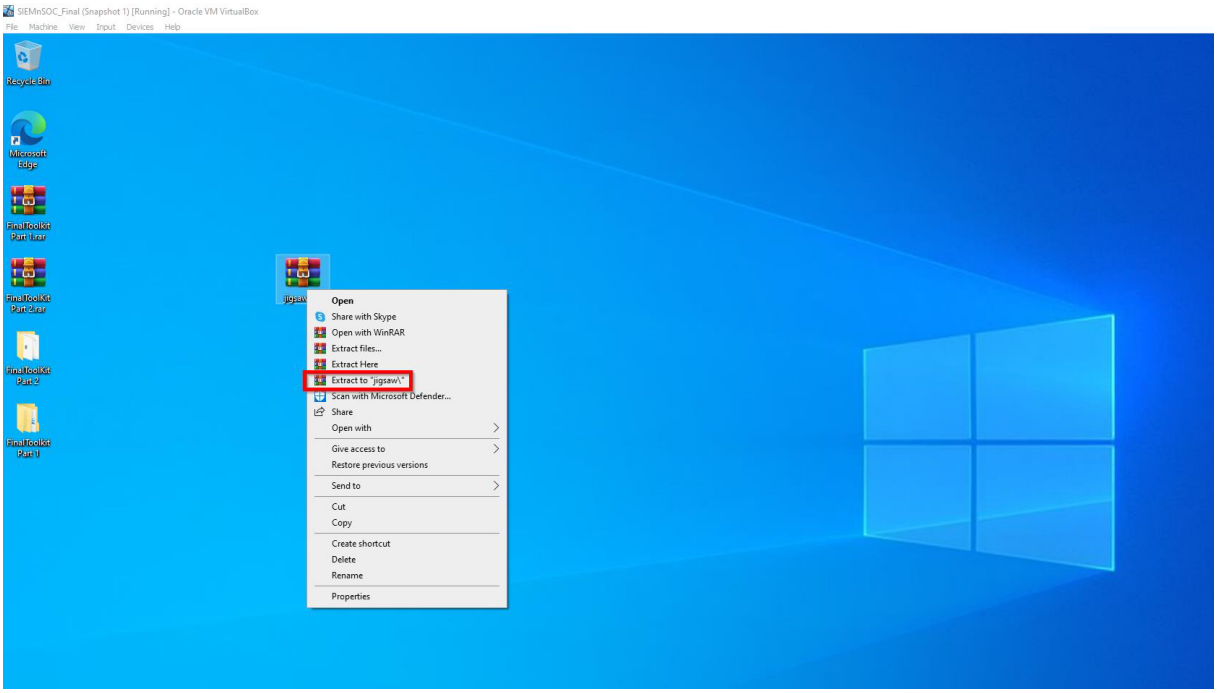



3. Decryption of Files Encrypted by "Jigsaw" Ransomware

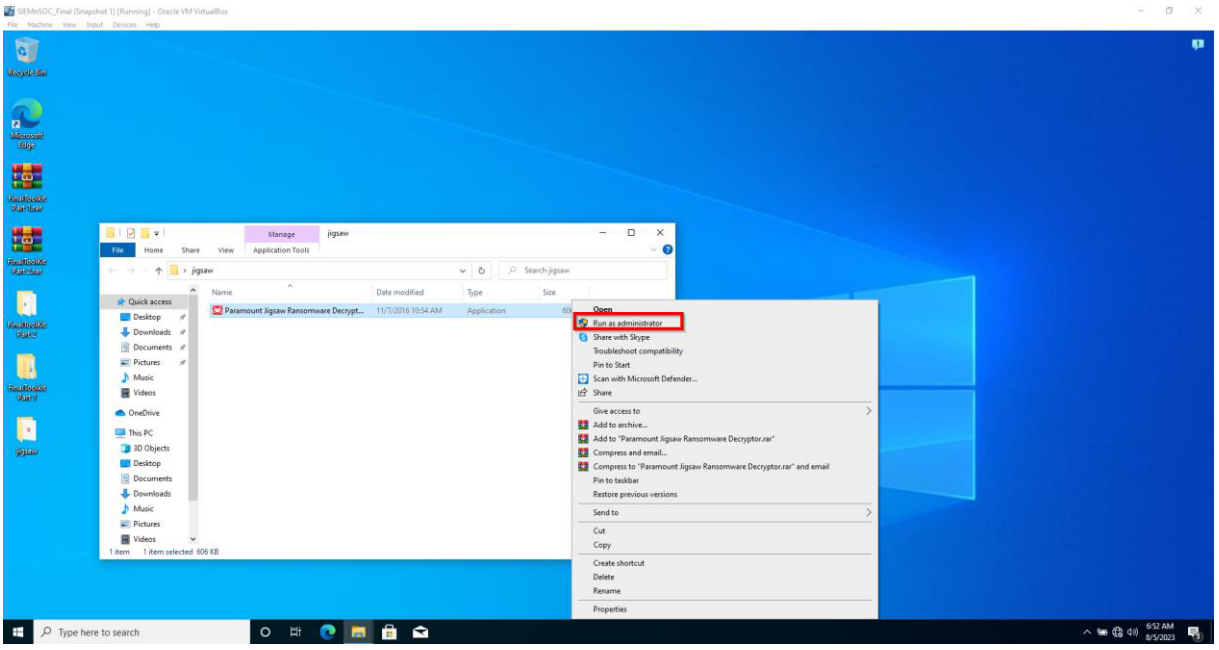
In the final phase of our comprehensive response, the successful decryption of files that had fallen victim to the "Jigsaw" ransomware was achieved through a strategic and systematic approach.

**Download and Preparation:** To initiate the decryption process, the "Jigsaw Ransomware Decryptor Tool" was acquired from the reputable website https://www.vinransomware.com/free-jigsaw-ransomware-decryptor-tool. The tool was then extracted from the provided zip archive.

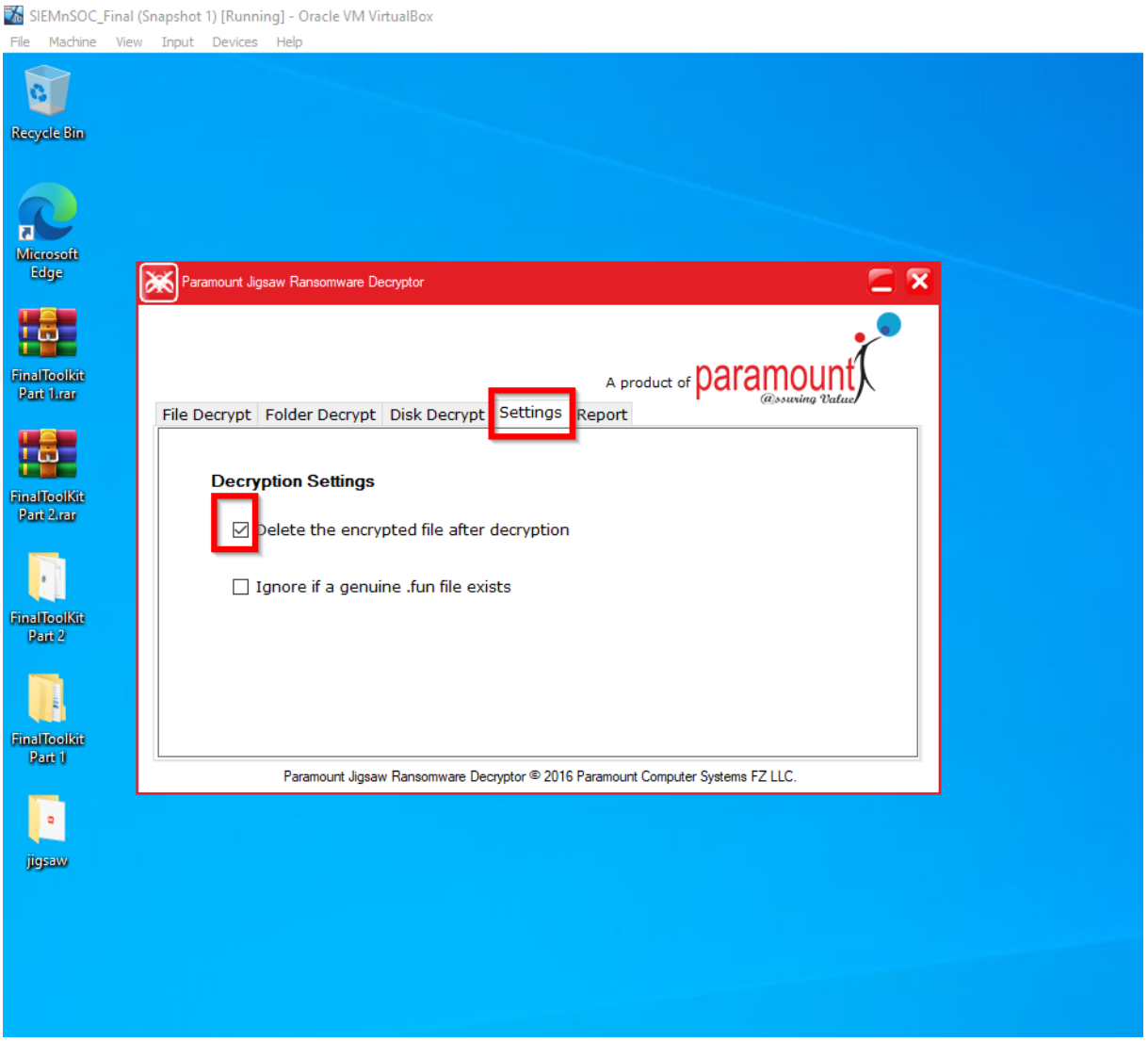




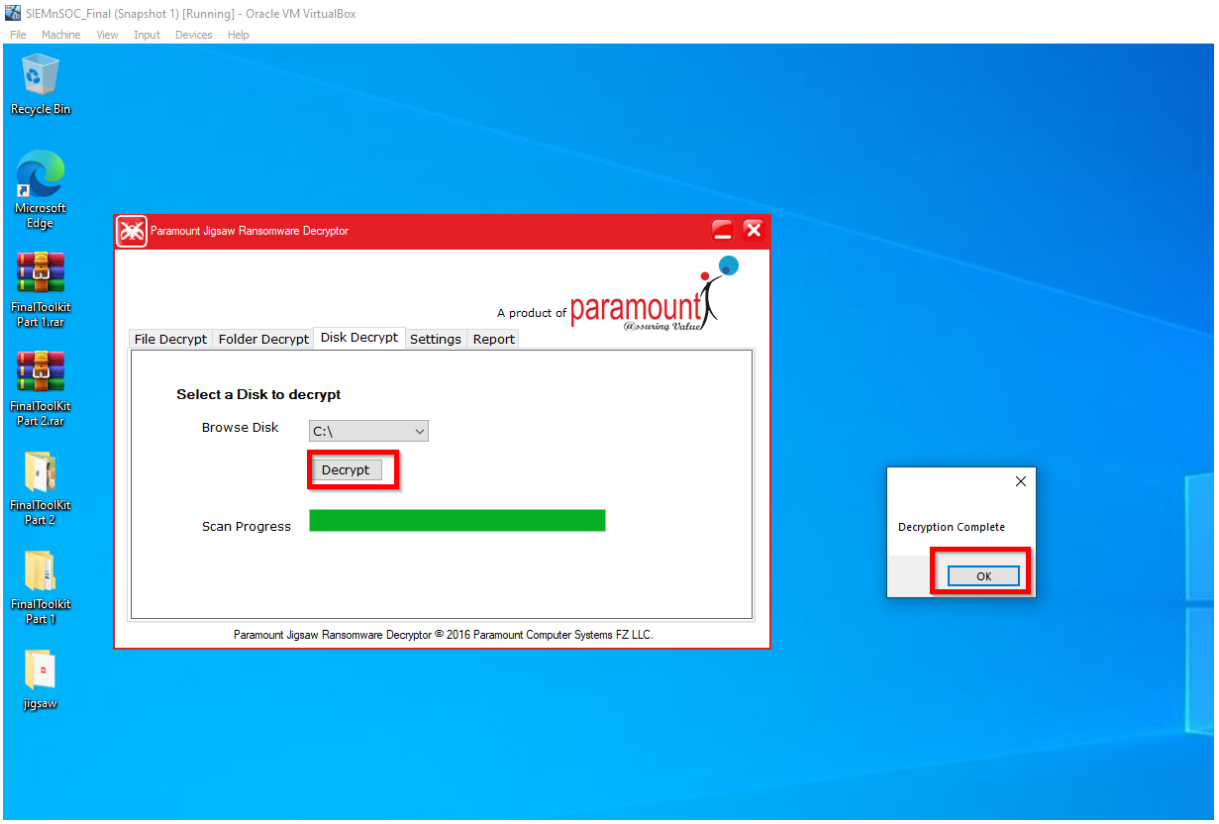

**Tool Execution:** Executing the tool as an administrator was a critical step. The program named "Paramount Jigsaw Ransomware Decryptor.exe" was launched, and immediate attention was directed to the "Settings" tab.



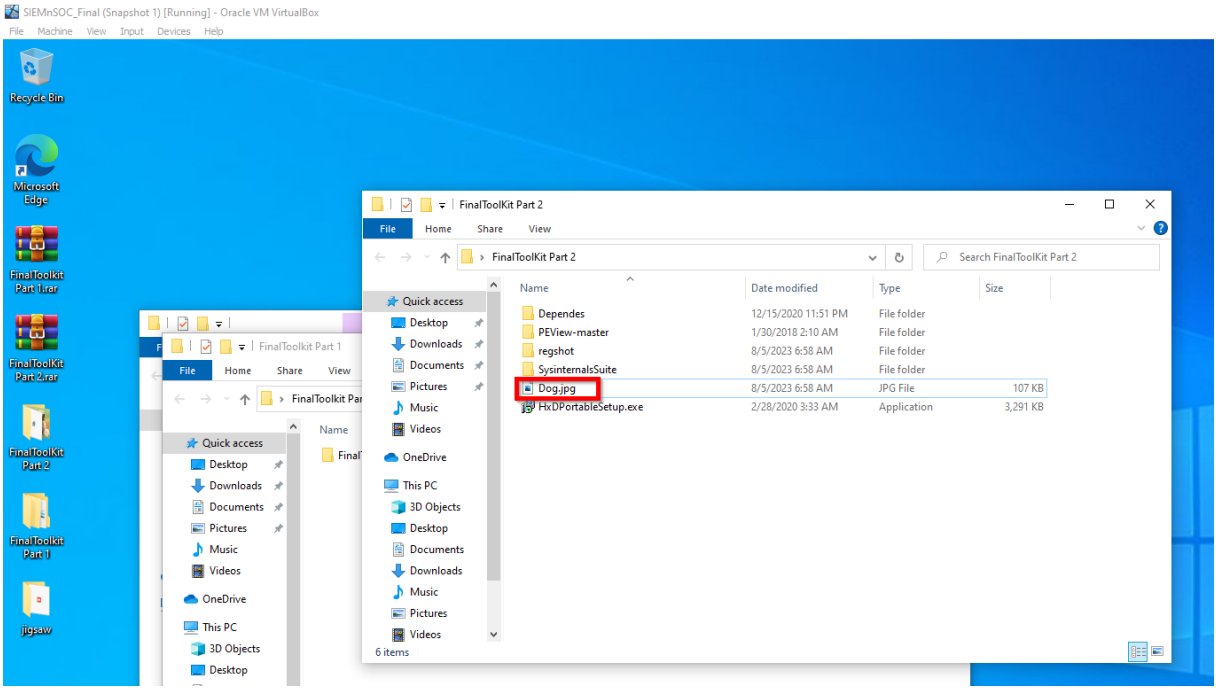
**Optimal Settings Configuration:** Within the "Settings" tab, a pivotal setting was configured. Specifically, the option "Delete the encrypted file after decryption" was selected. This setting ensured not only the recovery of the encrypted files but also the removal of the encrypted duplicates.



**Decryption Process:** The heart of the operation lay within the "Disk Decrypt" tab. Here, the target disk for decryption was meticulously chosen. With precision, the decryption process was initiated by selecting the "Decrypt" option. Upon completion, an affirmative "OK" signal marked the successful decryption.



**Verification of Success:** As validation of the process, a comprehensive assessment of the files on Disk C was undertaken. This step provided tangible evidence of the restoration and decryption of the previously compromised files.




Summary:

The successful mitigation of the "Jigsaw" ransomware threat stands as a testament to our meticulous approach, swift actions, and unwavering commitment to safeguarding the integrity of the system. This comprehensive response has effectively neutralized the threat, ensuring that the organization can continue its operations with minimized disruption.