

# 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"

| Process                     | CPU   | Private Bytes | Working Set | PID   | Description                     | Company Name                   | VirusTotal |
|-----------------------------|-------|---------------|-------------|-------|---------------------------------|--------------------------------|------------|
| svchost.exe                 | 0.01  | 1,240 K       | 10,668 K    | 2980  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 11,720 K      | 13,048 K    | 3176  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 140,312 K     | 90,324 K    | 3228  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 1,836 K       | 14,080 K    | 3432  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 4,416 K       | 28,684 K    | 3768  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 3,100 K       | 29,764 K    | 3780  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 8,116 K       | 81,304 K    | 3812  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 3,332 K       | 36,980 K    | 3916  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 1,700 K       | 13,148 K    | 4084  | Host Process for Windows S...   | Microsoft Corporation          |            |
| ctfmon.exe                  |       | 8,592 K       | 13,492 K    | 3204  | CTF Loader                      | Microsoft Corporation          |            |
| svchost.exe                 |       | 4,100 K       | 38,612 K    | 4188  | Host Process for Windows S...   | Microsoft Corporation          |            |
| explorer.exe                | 0.48  | 57,652 K      | 238,836 K   | 4344  | Windows Explorer                | Microsoft Corporation          |            |
| firefox.exe                 | 0.04  | 35,596 K      | 28,876 K    | 7796  | Firefox                         | Mozilla Corporation            |            |
| cmd.exe                     |       | 25,940 K      | 35,016 K    | 3720  | Windows Command Processor       | Microsoft Corporation          |            |
| conhost.exe                 |       | 7,564 K       | 22,944 K    | 2316  | Console Window Host             | Microsoft Corporation          |            |
| notepad.exe                 |       | 3,156 K       | 6,376 K     | 6376  | Notepad                         | Microsoft Corporation          |            |
| Procmon64.exe               | 0.60  | 34,596 K      | 55,164 K    | 1912  | Process Monitor                 | Sysinternals - www.sysinter... |            |
| procexp64.exe               | 1.25  | 24,092 K      | 57,232 K    | 3116  | Sysinternals Process Explorer   | Sysinternals - www.sysinter... |            |
| svchost.exe                 | 0.01  | 3,296 K       | 40,352 K    | 4536  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 3,956 K       | 29,180 K    | 4604  | Host Process for Windows S...   | Microsoft Corporation          |            |
| StartMenuExperienceHost.exe |       | 19,832 K      | 40,404 K    | 4956  |                                 |                                |            |
| RuntimeBroker.exe           |       | 5,984 K       | 16,312 K    | 5168  | Runtime Broker                  | Microsoft Corporation          |            |
| SearchIndexer.exe           |       | 31,452 K      | 28,700 K    | 5560  | Microsoft Windows Search I...   | Microsoft Corporation          |            |
| SearchApp.exe               |       | 96,640 K      | 136,064 K   | 5628  | Search application              | Microsoft Corporation          |            |
| RuntimeBroker.exe           |       | 24,620 K      | 28,764 K    | 5908  | Runtime Broker                  | Microsoft Corporation          |            |
| dllhost.exe                 |       | 3,804 K       | 26,048 K    | 4992  | COM Surrogate                   | Microsoft Corporation          |            |
| svchost.exe                 |       | 5,460 K       | 37,760 K    | 3012  | Host Process for Windows S...   | Microsoft Corporation          |            |
| MoUsCoreWorker.exe          |       | 46,996 K      | 14,904 K    | 5480  | MoUSO Core Worker Process       | Microsoft Corporation          |            |
| svchost.exe                 |       | 4,500 K       | 21,252 K    | 6260  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 15,964 K      | 37,896 K    | 6568  | Host Process for Windows S...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 1,956 K       | 13,896 K    | 2752  | Host Process for Windows S...   | Microsoft Corporation          |            |
| SgmBroker.exe               |       | 3,894 K       | 4,544 K     | 5296  | System Guard Runtime Monit...   | Microsoft Corporation          |            |
| svchost.exe                 |       | 5,100 K       | 37,000 K    | 192   | Host Process for Windows S...   | Microsoft Corporation          |            |
| ApplicationFrameHost.exe    |       | 2,392 K       | 4,796 K     | 6484  | Host Process for Windows S...   | Microsoft Corporation          |            |
| MsMpEng.exe                 | 0.16  | 239,880 K     | 84,252 K    | 296   | 1060 Application Frame Host     | Microsoft Corporation          |            |
| drpbx.exe                   | 0.02  | 31,832 K      | 4,756 K     | 1156  | Antimalware Service Execut...   | Microsoft Corporation          |            |
| Registry                    |       | 3,580 K       | 27,856 K    | 72    |                                 |                                |            |
| System Idle Process         | 93.18 | 60 K          | 8 K         | 0     |                                 |                                |            |
| System                      |       | 0.91          | 196 K       | 140 K | 4                               |                                |            |
| Interrups                   |       | 1.64          | 0 K         | 0 K   | n/a Hardware Interrups and DPCs |                                |            |
| smss.exe                    |       | 1,068 K       | 296 K       | 340   | Windows Session Manager         | Microsoft Corporation          |            |
| css.exe                     |       | 1,728 K       | 2,440 K     | 432   | Client Server Runtime Process   | Microsoft Corporation          |            |
| wininit.exe                 |       | 1,320 K       | 148 K       | 500   | Windows Start-Up Application    | Microsoft Corporation          |            |

CPU Usage: 6.82% Commit Charge: 18.73% Processes: 124

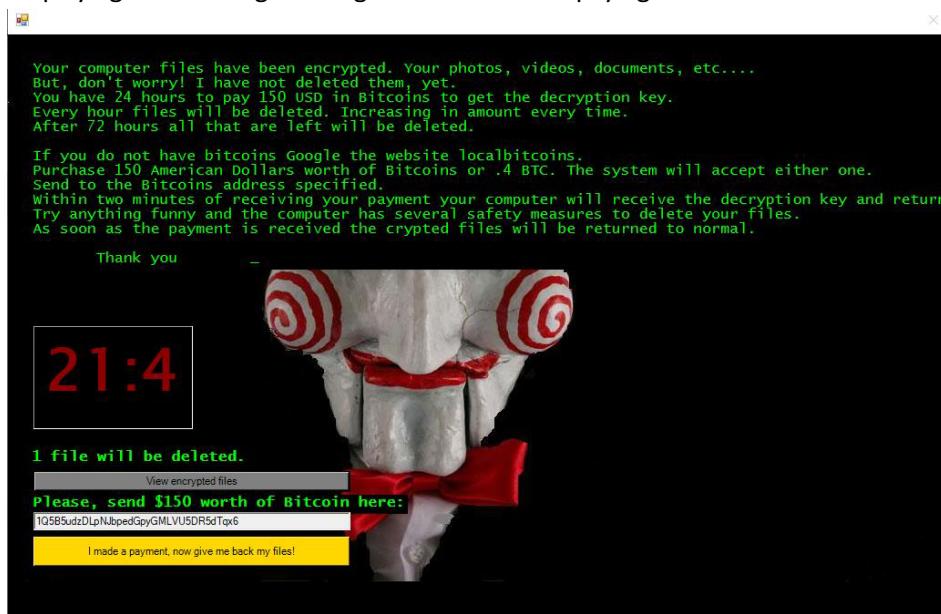
B) "drpbx.exe"

| Process                     | CPU     | Private Bytes | Working Set | PID  | Description                   | Company Name                   | VirusTotal |
|-----------------------------|---------|---------------|-------------|------|-------------------------------|--------------------------------|------------|
| svchost.exe                 |         | 3,584 K       | 37,132 K    | 3916 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe                 |         | 1,700 K       | 13,148 K    | 4084 | Host Process for Windows S... | Microsoft Corporation          |            |
| ctfmon.exe                  |         | 8,588 K       | 13,500 K    | 3204 | CTF Loader                    | Microsoft Corporation          |            |
| svchost.exe                 | 0.01    | 4,100 K       | 38,612 K    | 4188 | Host Process for Windows S... | Microsoft Corporation          |            |
| explorer.exe                | 0.39    | 58,500 K      | 239,300 K   | 4344 | Windows Explorer              | Microsoft Corporation          |            |
| firefox.exe                 | 0.05    | 35,596 K      | 28,876 K    | 7796 | Firefox                       | 65/75                          |            |
| cmd.exe                     |         | 2,540 K       | 5,012 K     | 3728 | Windows Command Processor     | Microsoft Corporation          |            |
| c:\host.exe                 |         | 7,564 K       | 22,944 K    | 2316 | Console Window Host           | Microsoft Corporation          |            |
| notepad.exe                 |         | 3,156 K       | 19,436 K    | 6376 | Notepad                       | Microsoft Corporation          |            |
| Procmon64.exe               | 0.56    | 35,564 K      | 62,328 K    | 1912 | Process Monitor               | Sysinternals - www.sysinter... |            |
| procexp64.exe               | 4.83    | 24,304 K      | 57,660 K    | 3116 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |            |
| svchost.exe                 | 0.01    | 3,296 K       | 40,352 K    | 4536 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe                 |         | 4,064 K       | 29,212 K    | 4604 | Host Process for Windows S... | Microsoft Corporation          |            |
| StartMenuExperienceHost.exe |         | 19,824 K      | 40,400 K    | 4856 |                               |                                |            |
| RuntimeBroker.exe           |         | 5,984 K       | 16,312 K    | 5168 | Runtime Broker                | Microsoft Corporation          |            |
| SearchIndexer.exe           | < 0.01  | 33,248 K      | 29,860 K    | 5560 | Microsoft Windows Search I... | Microsoft Corporation          |            |
| SearchProtocolHost.exe      |         | 1,840 K       | 8,824 K     | 8100 | Microsoft Windows Search P... | Microsoft Corporation          |            |
| SearchFilterHost.exe        |         | 1,568 K       | 7,892 K     | 6064 | Microsoft Windows Search F... | Microsoft Corporation          |            |
| SearchApp.exe               | Susp... | 96,640 K      | 136,064 K   | 5628 | Search application            | Microsoft Corporation          |            |
| RuntimeBroker.exe           |         | 24,552 K      | 28,744 K    | 5908 | Runtime Broker                | Microsoft Corporation          |            |
| dlhost.exe                  |         | 3,804 K       | 26,048 K    | 4992 | COM Surrogate                 | Microsoft Corporation          |            |
| svchost.exe                 |         | 5,460 K       | 37,760 K    | 3012 | Host Process for Windows S... | Microsoft Corporation          |            |
| MoUsCoreWorker.exe          |         | 46,996 K      | 14,904 K    | 5480 | MoUSO Core Worker Process     | Microsoft Corporation          |            |
| svchost.exe                 |         | 4,640 K       | 22,164 K    | 6260 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe                 |         | 16,016 K      | 37,908 K    | 6868 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe                 |         | 1,956 K       | 13,896 K    | 2752 | Host Process for Windows S... | Microsoft Corporation          |            |
| SgmBroker.exe               | < 0.01  | 3,884 K       | 4,544 K     | 5296 | System Guard Runtime Monit... | Microsoft Corporation          |            |
| svchost.exe                 |         | 5,100 K       | 37,000 K    | 192  | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe                 |         | 2,480 K       | 4,824 K     | 6484 | Host Process for Windows S... | Microsoft Corporation          |            |
| ApplicationFrameHost.exe    |         | 4,176 K       | 296 K       | 1060 | Application Frame Host        | Microsoft Corporation          |            |
| MsMpEng.exe                 | 0.21    | 239,808 K     | 84,336 K    | 1156 | Antimalware Service Execut... | Microsoft Corporation          |            |
| drpbx.exe                   | 0.03    | 31,832 K      | 3,728 K     | 6356 | Firefox                       |                                |            |
| Ntdll.dll                   |         | 3,556 K       | 26,004 K    | 72   |                               |                                |            |
| System Idle Process         | 90.54   | 60 K          | 8 K         | 0    |                               |                                |            |
| System                      | 0.84    | 196 K         | 140 K       | 4    |                               |                                |            |
| Interrups                   | 1.72    | 0 K           | 0 K         | n/a  | Hardware Interrupts and DPCs  |                                |            |
| smss.exe                    |         | 1,068 K       | 296 K       | 340  | Windows Session Manager       | Microsoft Corporation          |            |
| csrss.exe                   | < 0.01  | 1,728 K       | 2,440 K     | 432  | Client Server Runtime Process | Microsoft Corporation          |            |
| wininit.exe                 |         | 1,320 K       | 148 K       | 500  | Windows Start-Up Application  | Microsoft Corporation          |            |

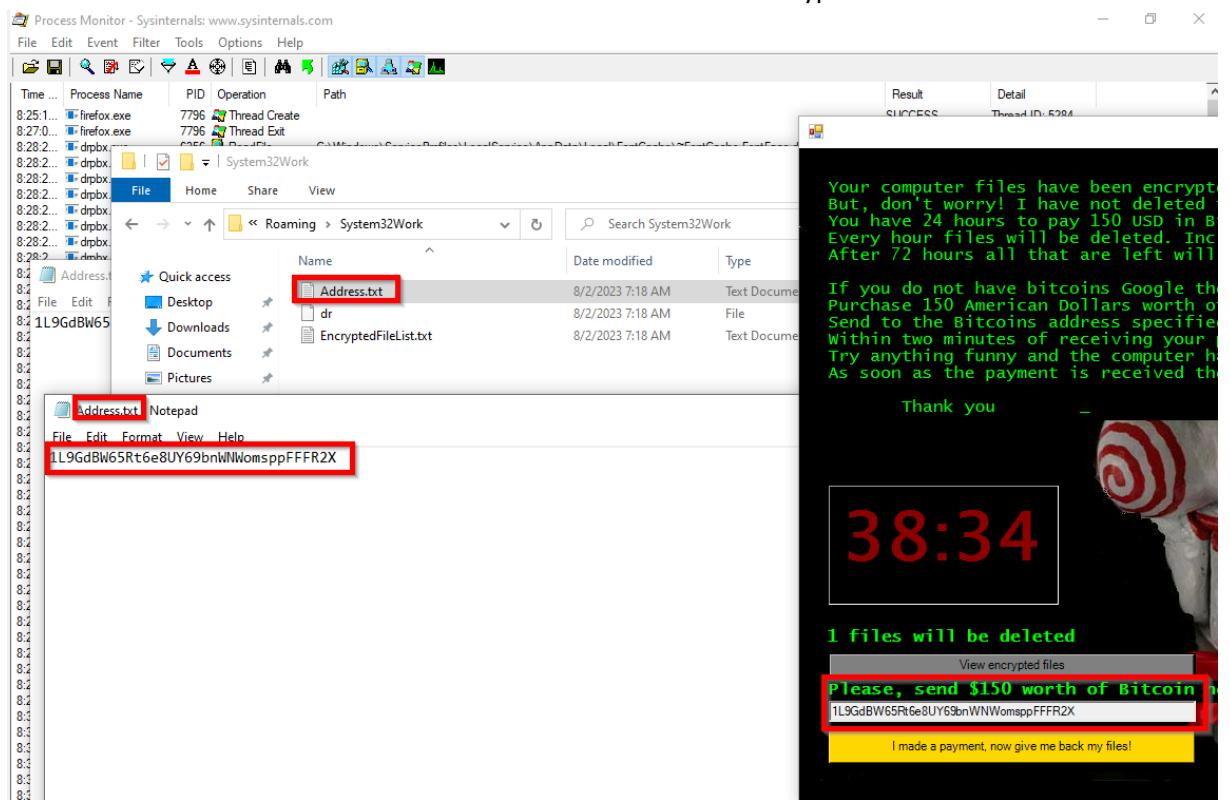
## 2. Malware Behavior and Activities:

The Jigsaw ransomware exhibits several malicious behaviors, including:

- A) Displaying threatening messages to victims into paying ransoms.



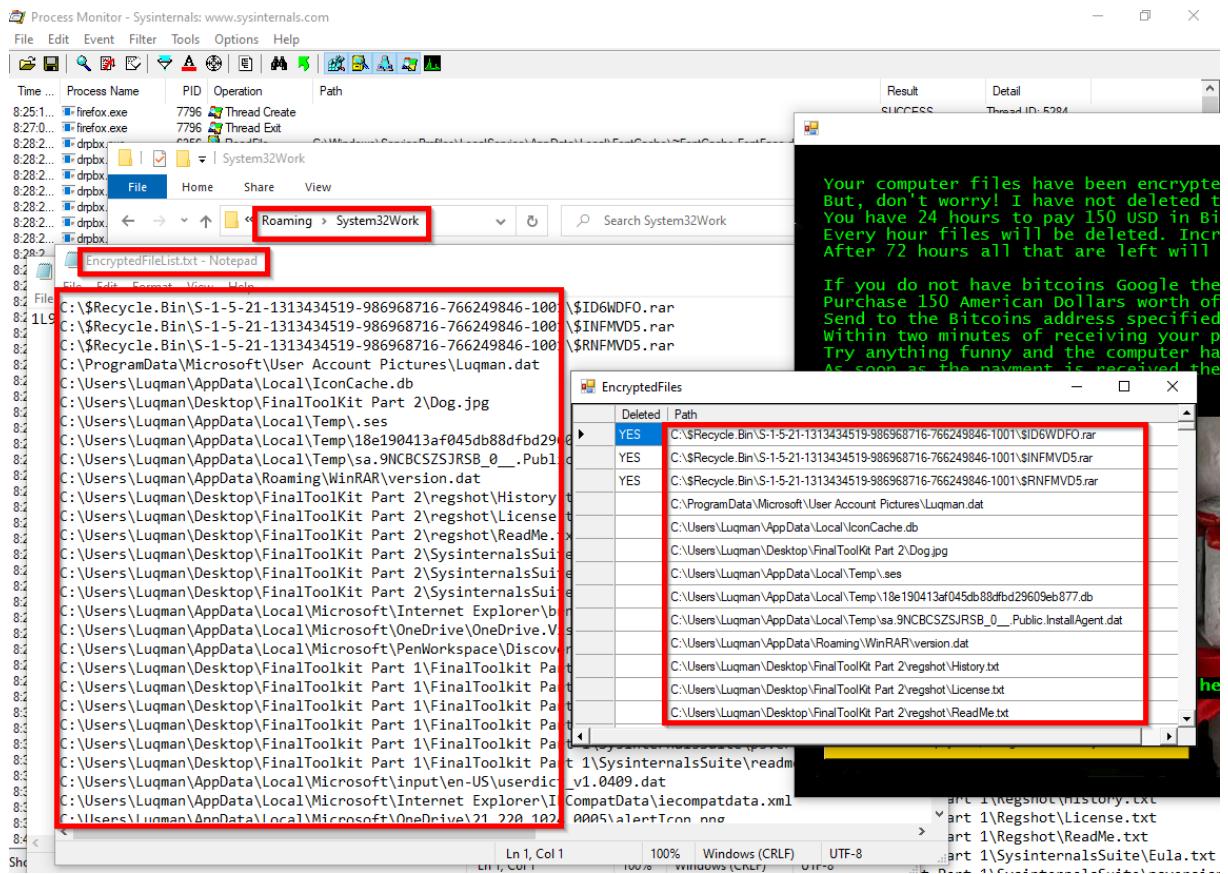
- B) Creating essential files for ransom payment and encrypted file tracking.  
Address.txt located at C:\Users\Luqman\AppData\Roaming\System32Work  
File is related to address where victim should send Bitcoins for decrypt files.



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

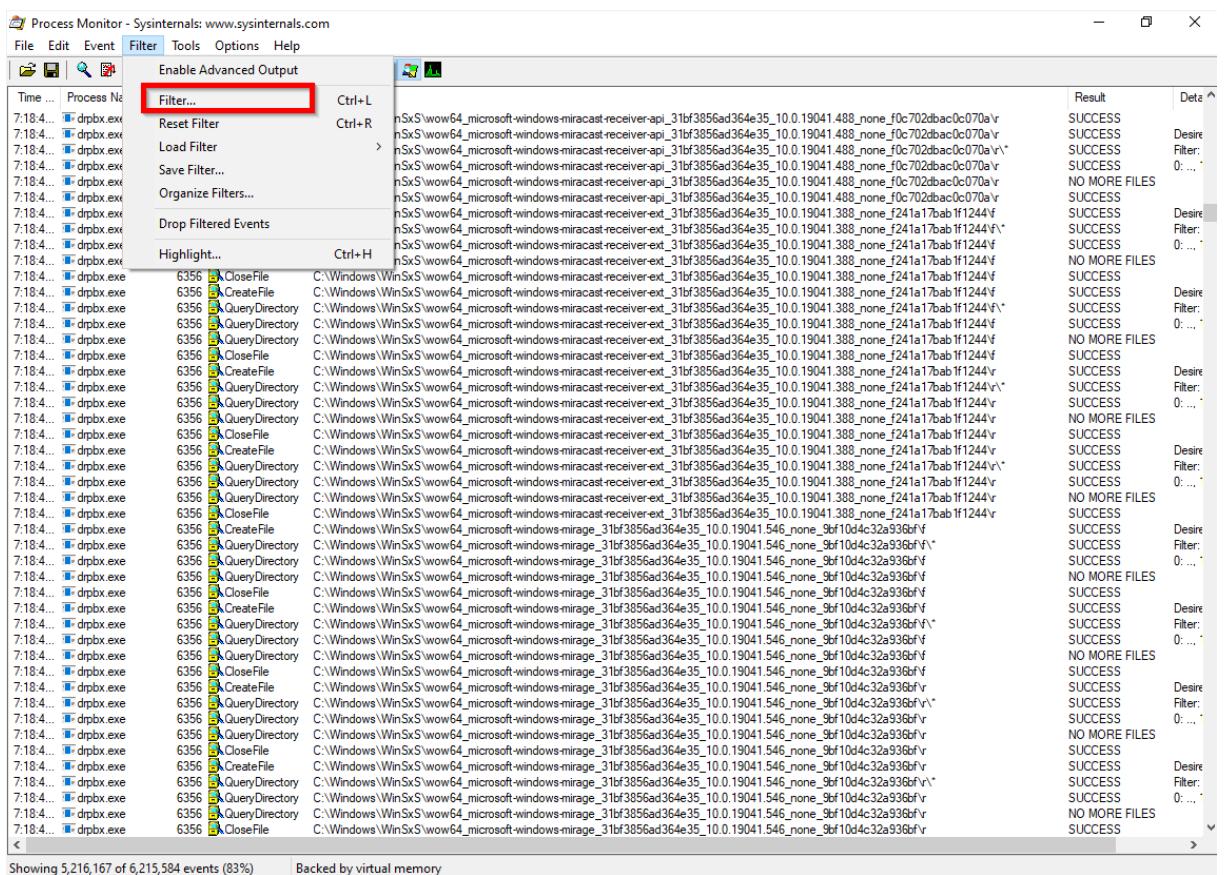
File is related to files and them locations which been already encrypted by ransomware "Jigsaw".

| 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...          | drpbx.exe    | 6356 | ReadFile          | C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\FontCache-FontFace.dat      | SUCCESS                             | Offset: 2,740,224, ...                        |
| 8:28:2...          | drpbx.exe    | 6356 | CreateFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Desired Access: R...<br>CreationTime: 8/2/... |
| 8:28:2...          | drpbx.exe    | 6356 | QueryVirtualAlloc | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             |   |
| 8:28:2...          | drpbx.exe    | 6356 | CloseFile         | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             |   |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 3,910,656, ...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 4,037,632, ...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 4,074,496, ...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 4,189,184, ...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 4,238,336, ...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 4,221,952, ...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 8,192, Len...                         |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 12,288, Len...                        |
| 8:28:28.7212567 AM | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 16,384, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 20,490, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 24,576, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 28,672, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 32,768, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 36,864, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 40,960, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 45,056, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 49,152, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 53,248, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 57,344, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 61,440, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 65,536, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 69,632, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | END OF FILE                         | Offset: 70,991, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile          | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | END OF FILE                         | Offset: 70,991, Len...                        |
| 8:28:2...          | drpbx.exe    | 6356 | CloseFile         | C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 3,857,408, ...                        |
| 8:28:2...          | drpbx.exe    | 6356 | CreateFile        | C:\\$Recycle.Bin\\$1-5-21-1313434519-986968716-766249846-1001\\$ID6WDF0.rarfun              | NAME NOT FOUND Desired Access: R... |   |
| 8:29:2...          | drpbx.exe    | 6356 | Thread Create     |   | SUCCESS                             | Thread ID: 6456                               |
| 8:29:3...          | drpbx.exe    | 7796 | Thread Create     |   | SUCCESS                             | Thread ID: 2472                               |

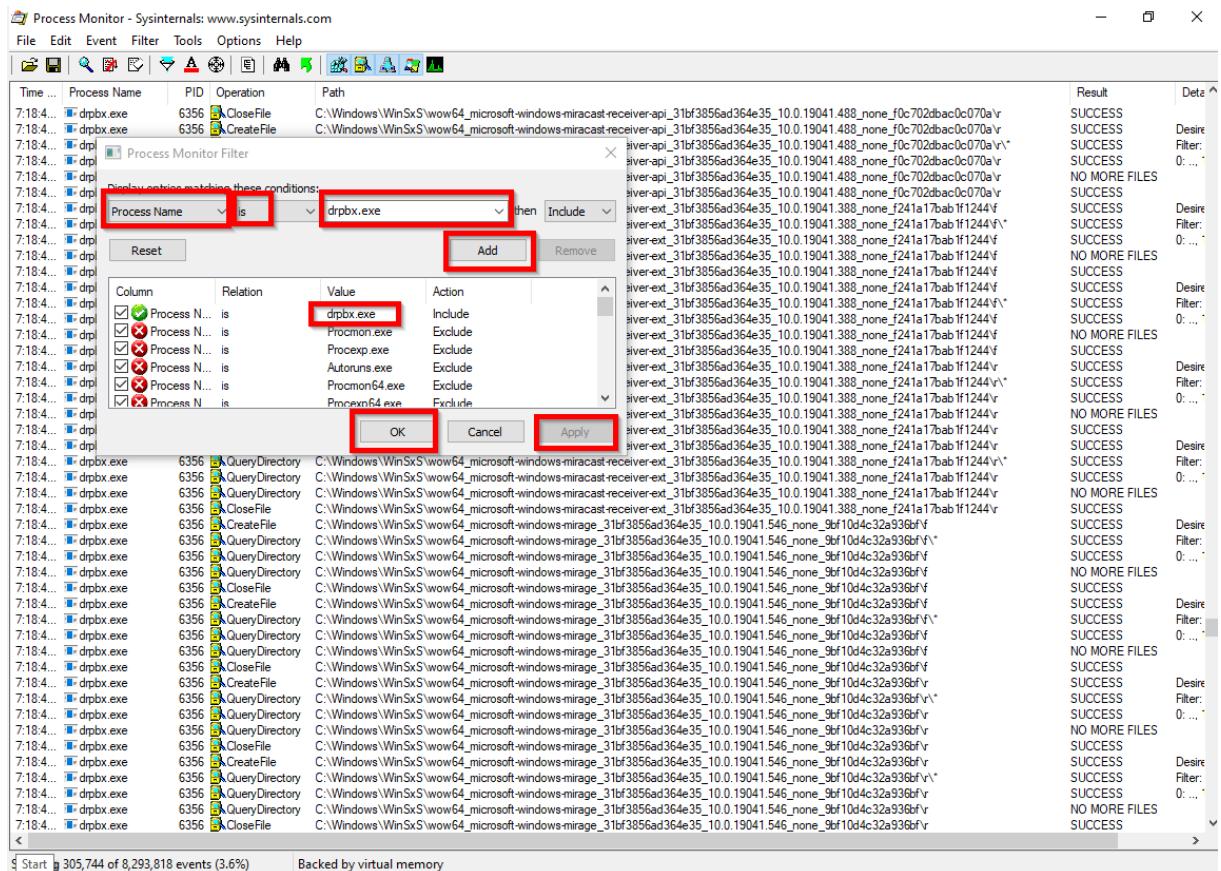


C) Encrypting files with the ".fun" extension, rendering them inaccessible.

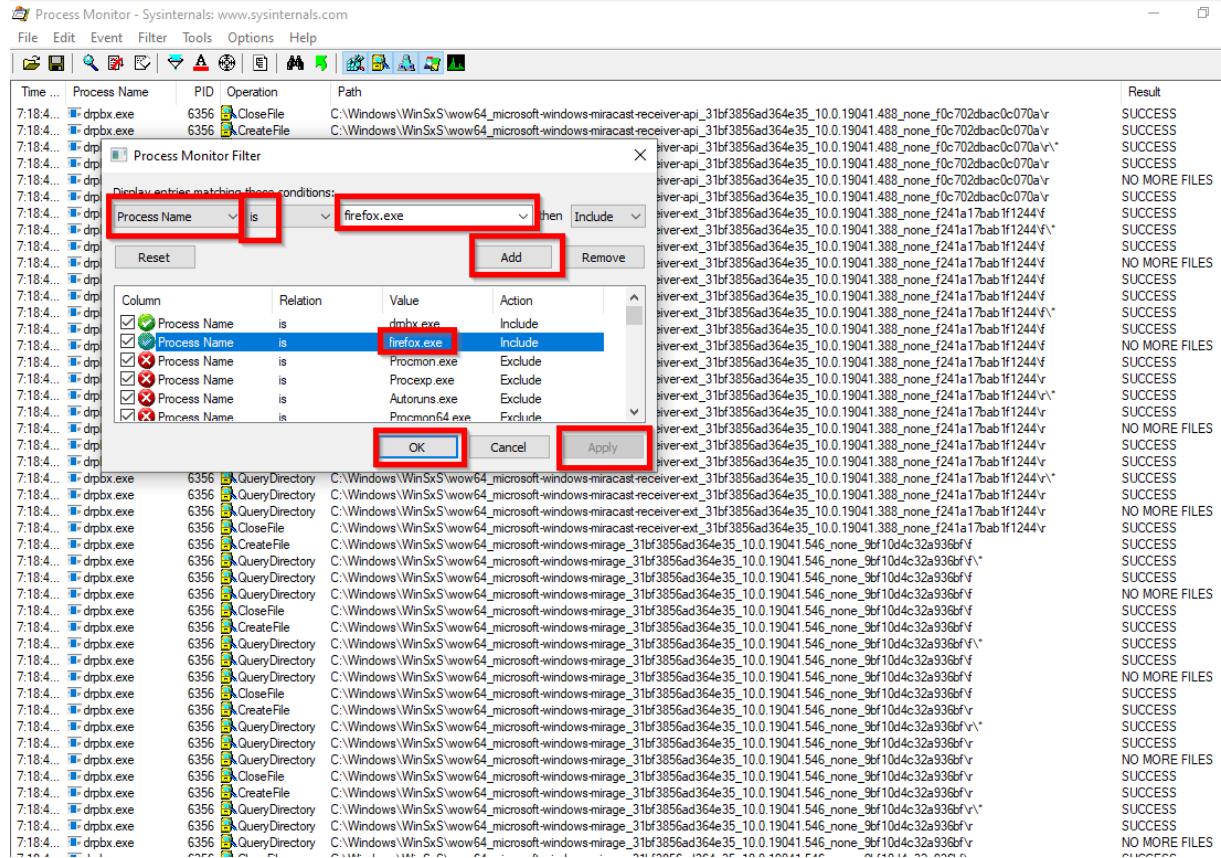
1.



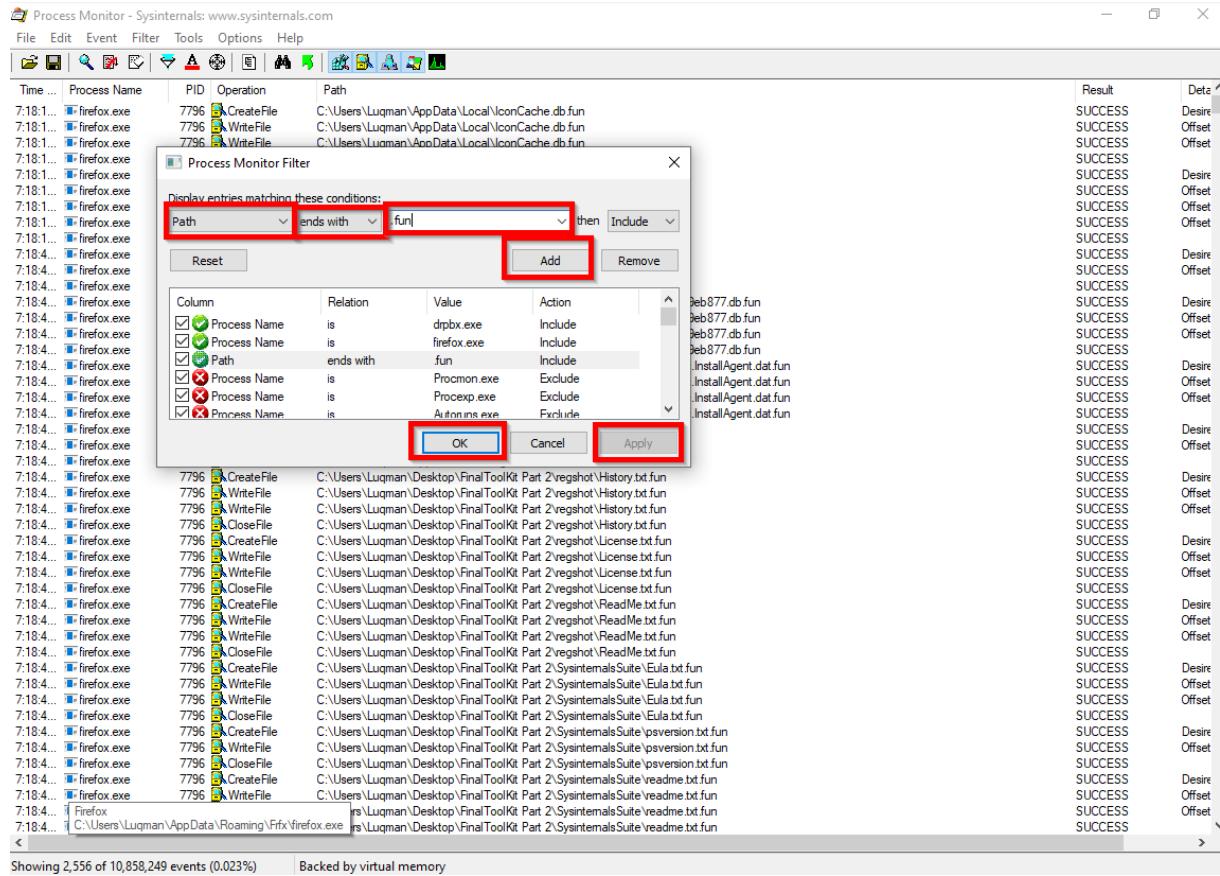
2.



### 3.



4.





5.

The screenshot shows the Dependency Walker interface. On the left, a tree view lists the modules loaded by DRPBX.EXE, including DRPBX.EXE itself, MSCOREE.DLL, KERNEL32.DLL, USER32.DLL, ADVAPI32.DLL, SHLWAPI.DLL, VERSION.DLL, OLEAUT32.DLL, and URLMON.DLL. On the right, two tables show imported functions. The top table lists functions from MSCOREE.DLL, and the bottom table lists functions from ADVAPI32.DLL. A specific entry in the bottom table, 'CryptEncrypt' (Ordinal 1205), is highlighted. Below these tables is a module list table:

| Module       | File Time Stamp  | Link Time Stamp   | File Size | Attr. | Link C |
|--------------|------------------|-------------------|-----------|-------|--------|
| SEHOST.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  |

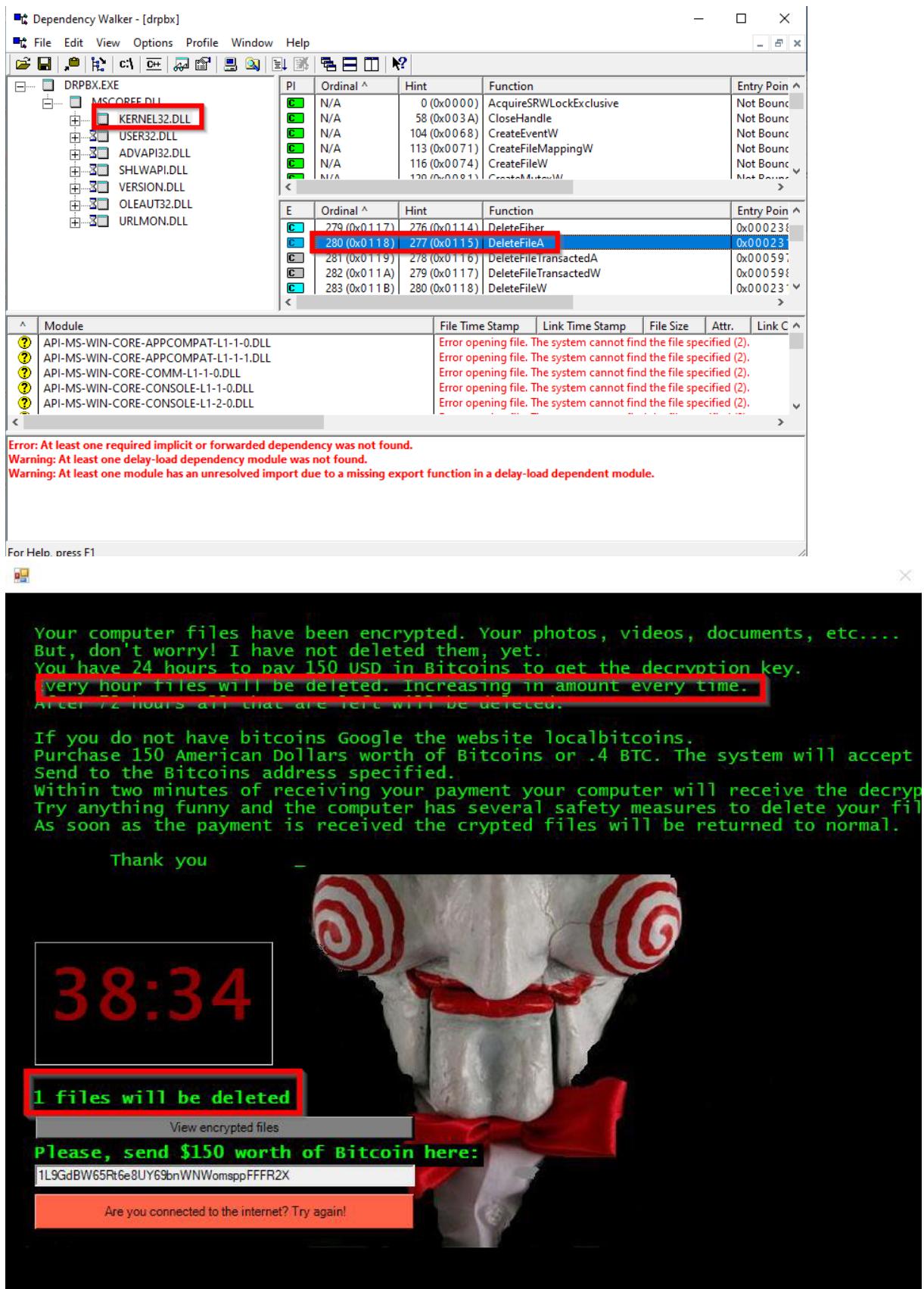
**Error:** At least one required implicit or forwarded dependency was not found.  
**Warning:** At least one delay-load dependency module was not found.  
**Warning:** At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1

6.

The screenshot shows a Windows File Explorer window. The address bar indicates the path is 'FinalToolKit Part 2'. The left sidebar shows standard folder icons for Quick access, Desktop, Downloads, Documents, Pictures, Music, Videos, OneDrive, This PC, and Network. The main pane displays a list of files and folders. One file, 'Dog.jpg.fun', is highlighted with a red box. Other visible items include 'Dependes', 'PEView-master', 'regshot', 'SysinternalsSuite', and '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.

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

The screenshot shows the Windows Task Manager interface within the Process Explorer application. The main window displays a list of running processes. The Firefox process, identified by its icon and the text "firefox.exe" in the list, is highlighted with a red rectangular selection box. To the right of the Firefox entry, the "VirusTotal" column shows a score of "65/75". The Task Manager also includes a status bar at the bottom with information like "Command Line:", "Path:", and "Services:".

| Process   | CPU     | Private Bytes | Working Set | PID  | Description                   | Company Name                   | VirusTotal |
|---|---------|---------------|-------------|------|-------------------------------|--------------------------------|------------|
| svchost.exe   | 0.03    | 11,540 K      | 12,888 K    | 3176 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 140,424 K     | 90,256 K    | 3228 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 1,836 K       | 14,068 K    | 3432 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 4,688 K       | 28,784 K    | 3768 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 3,044 K       | 29,708 K    | 3780 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 7,924 K       | 80,716 K    | 3812 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 3,368 K       | 32,720 K    | 3916 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 1,704 K       | 13,144 K    | 4084 | Host Process for Windows S... | Microsoft Corporation          |            |
| ctfmon.exe  |         | 10,040 K      | 14,928 K    | 3204 | CTF Loader                    | Microsoft Corporation          |            |
| svchost.exe   |         | 4,100 K       | 38,568 K    | 4188 | Host Process for Windows S... | Microsoft Corporation          |            |
| svlaver.exe   | 0.06    | 61,156 K      | 239,412 K   | 4344 | Windows Explorer              | Microsoft Corporation          |            |
| firefox.exe   | 0.04    | 40,188 K      | 47,492 K    | 7796 | Firefox                       | Microsoft Corporation          | 65/75      |
| cmd.exe   |         | 2,540 K       | 4,620 K     | 3728 | Windows Command Processor     | Microsoft Corporation          |            |
| conhost.exe   |         | 7,596 K       | 22,824 K    | 2316 | Console Window Host           | Microsoft Corporation          |            |
| notepad.exe   |         | 3,156 K       | 19,380 K    | 6376 | Notepad                       | Microsoft Corporation          |            |
| Procmon64.exe   | 0.59    | 39,244 K      | 59,156 K    | 1912 | Process Monitor               | Sysinternals - www.sysinter... |            |
| proexp64.exe  | 1.89    | 24,276 K      | 56,476 K    | 3116 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |            |
| notepad.exe   |         | 3,216 K       | 19,376 K    | 2072 | Notepad                       | Microsoft Corporation          |            |
| svchost.exe   |         | 3,296 K       | 40,292 K    | 4536 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 4,064 K       | 29,188 K    | 4604 | Host Process for Windows S... | Microsoft Corporation          |            |
| StartMenuExperienceHost.exe   |         | 19,824 K      | 40,360 K    | 4856 |                               |                                |            |
| RuntimeBroker.exe   |         | 5,988 K       | 16,328 K    | 5168 | Runtime Broker                | Microsoft Corporation          |            |
| SearchIndexer.exe   |         | 33,152 K      | 29,264 K    | 5560 | Microsoft Windows Search I... | Microsoft Corporation          |            |
| SearchProtocolHost.exe  |         | 1,840 K       | 8,688 K     | 6332 | Microsoft Windows Search P... | Microsoft Corporation          |            |
| SearchFilterHost.exe  |         | 1,572 K       | 7,888 K     | 5952 | Microsoft Windows Search F... | Microsoft Corporation          |            |
| SearchApp.exe   | Susp... | 96,640 K      | 132,856 K   | 5628 | Search application            | Microsoft Corporation          |            |
| RuntimeBroker.exe   |         | 24,372 K      | 28,668 K    | 5908 | Runtime Broker                | Microsoft Corporation          |            |
| dllhost.exe   |         | 3,804 K       | 25,568 K    | 4992 | COM Sumrogate                 | Microsoft Corporation          |            |
| svchost.exe   |         | 5,476 K       | 37,744 K    | 3012 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 4,616 K       | 22,088 K    | 6260 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 16,016 K      | 37,856 K    | 6868 | Host Process for Windows S... | Microsoft Corporation          |            |
| svchost.exe   |         | 1,952 K       | 13,872 K    | 2752 | Host Process for Windows S... | Microsoft Corporation          |            |
| SqmBroker.exe   |         | 3,808 K       | 4,244 K     | 5296 | System Guard Runtime Monit... | Microsoft Corporation          |            |
| Command Line:   |         |               |             |      |                               |                                |            |
| C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p -s SSDPSRV |         |               |             |      |                               |                                |            |
| Path:   |         |               |             |      |                               |                                |            |
| C:\Windows\System32\svchost.exe (LocalServiceAndNoImpersonation -p -s SSDPSRV)  |         |               |             |      |                               |                                |            |
| Services:   |         |               |             |      |                               |                                |            |
| SSDP Discovery [SSDPSRV]  |         |               |             |      |                               |                                |            |
| Process for Windows S...  |         |               |             |      |                               |                                |            |
| Process for Windows S...  |         |               |             |      |                               |                                |            |
| Application Frame Host  |         |               |             |      |                               |                                |            |
| Malware Service Execut...   |         |               |             |      |                               |                                |            |
| Box   |         |               |             |      |                               |                                |            |
| Registry  |         | 3,932 K       | 28,281 K    | 72   |                               |                                |            |

2.

The screenshot shows the VirusTotal analysis interface for the file 3ae96f73d805e1d3995253db4d910300d8442ea603737a142... (BitcoinBlackmailer.exe). The main summary indicates a high malicious score of 65 out of 71. Below this, the file hash and name are listed, along with its size (283.50 KB) and last analysis date (12 hours ago). A file icon shows it is an EXE file. The detection tab is selected, showing the following threat labels:

- Popular threat label: trojan.jigsaw/msil
- Threat categories: trojan, ransomware
- Family labels: jigsaw, msil, aqne

The security vendors' analysis table lists results from various antivirus engines:

| Virus Engine        | Result                           | Engine Name | Description                 |
|---------------------|----------------------------------|-------------|-----------------------------|
| Acronis (Static ML) | Suspicious                       | AhnLab-V3   | Win-Trojan/JigsawLocker.Gen |
| Alibaba             | Trojan:MSIL/Filecoder.ff7ad07d   | ALYac       | Trojan.Ransom.Jigsaw        |
| Antiy-AVL           | Trojan[Ransom]Win32.Jigsaw.a     | Arcabit     | Trojan.Ransom.Jigsaw.E      |
| Avast               | MSIL:Ransom-AX [Tr]              | AVG         | MSIL:Ransom-AX [Tr]         |
| Avira (no cloud)    | TR/FileCoder.aqne                | BitDefender | Trojan.Ransom.Jigsaw.E      |
| BitDefenderTheta    | Gen>NN.ZemsilF.36348.ru0@aWr012o | Bkav Pro    | W32.Common.41EDE250         |

### 3. Infected Directories and Files:

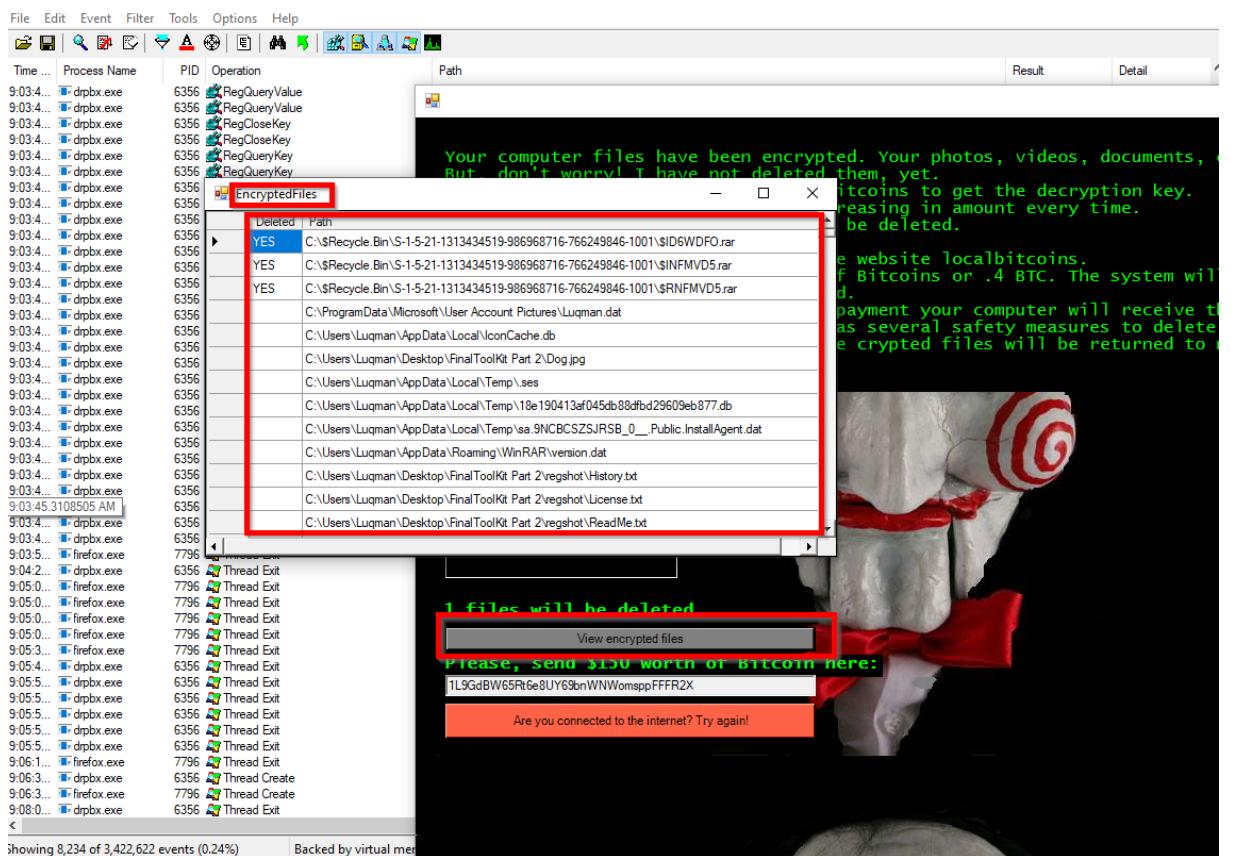
The ransomware infects specific directories and creates crucial files:

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

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

### 3. List of files that are infected.

A)



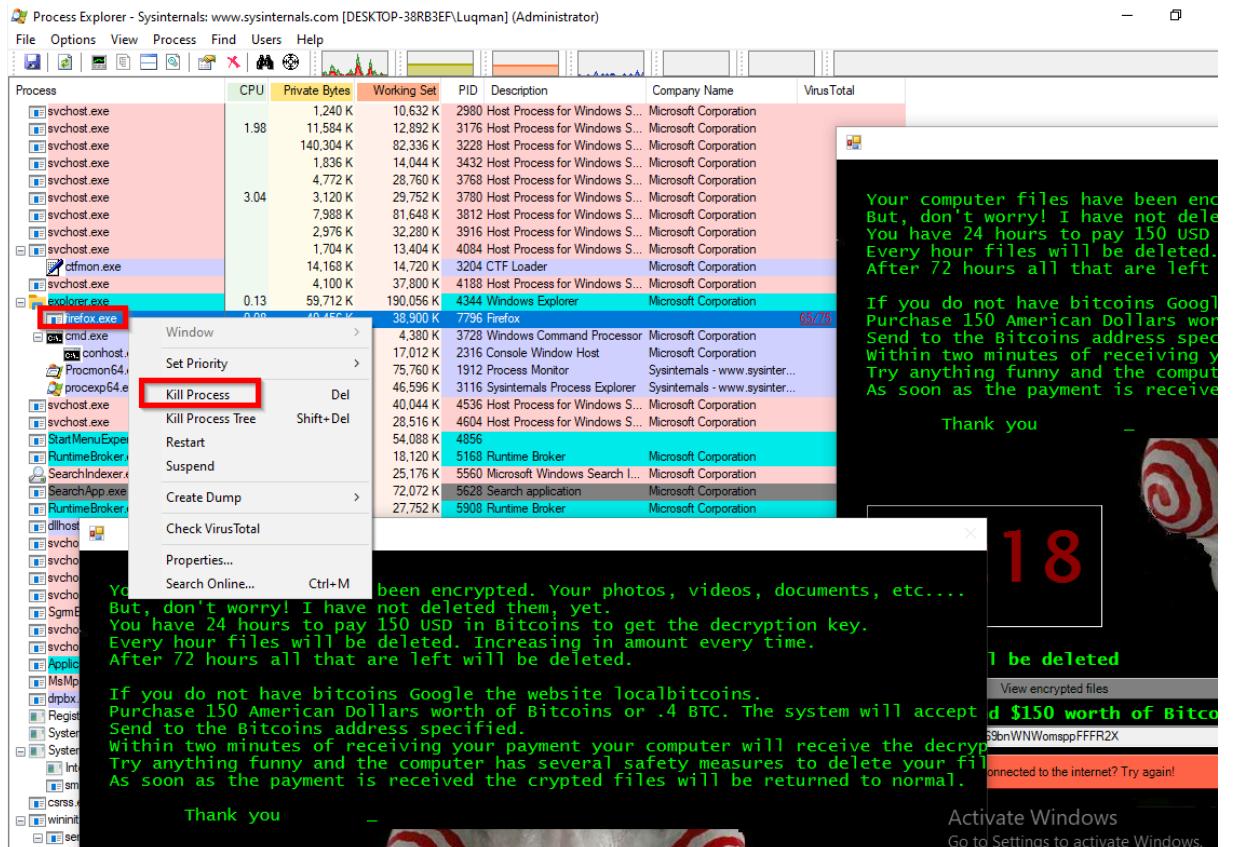
**B) Ransomware during process CreateFile creates a file EncryptedFileList.txt in directory : C:\Users\Luqman\AppData\Roaming\System32Work**

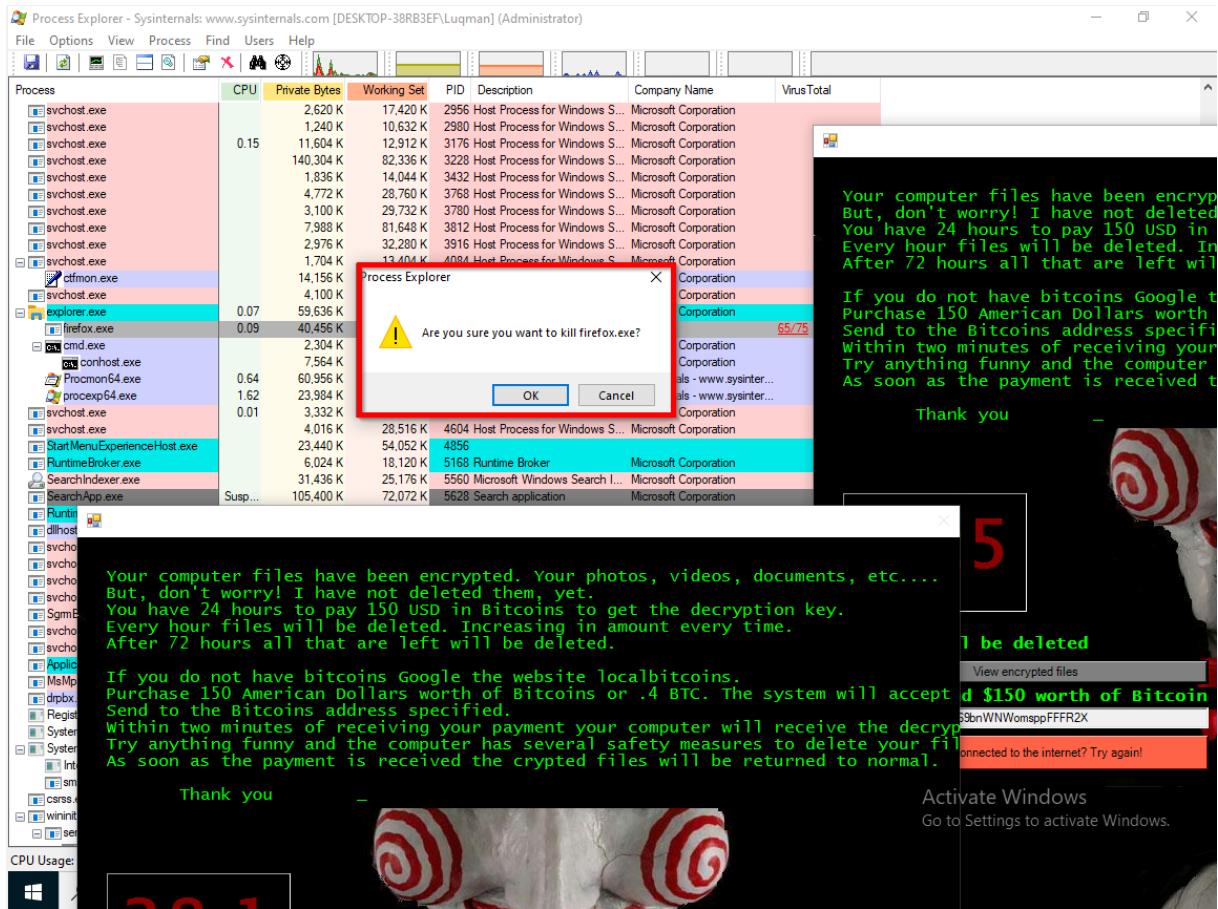
| Time ...           | Process Name | PID  | Operation       | Path  | Result                              | Detail                 |
|--------------------|--------------|------|-----------------|---|-------------------------------------|------------------------|
| 8:25...            | firefox.exe  | 7796 | Thread Create   |   | SUCCESS                             | Thread ID: 5284        |
| 8:27...            | firefox.exe  | 7796 | Thread Exit     |   | SUCCESS                             | Thread ID: 5284, ...   |
| 8:28...            | drpbx.exe    | 6356 | CreateFile      | C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\FontCache-FontFace.dat      | SUCCESS                             | Offset: 2,740,224, ... |
| 8:28:2...          | drpbx.exe    | 6356 | CreateFile      | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Desired Access: R...   |
| 8:28:2...          | drpbx.exe    | 6356 | QueryNetwork... | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | CreationTime: 8/2/...  |
| 8:28:2...          | drpbx.exe    | 6356 | CloseFile       | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             |                        |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Windows\Assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 3,910,656, ... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Windows\Assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 4,037,632, ... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Windows\Assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 4,074,496, ... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Windows\Assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 4,221,952, ... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 8,192, Len...  |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 12,288, Len... |
| 8:28:28 7212967 AM | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 16,384, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 20,480, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 24,576, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 28,672, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 32,768, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 36,864, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 40,960, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 45,056, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 49,152, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 53,248, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 57,344, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 61,440, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 65,536, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             | Offset: 69,632, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | END OF FILE                         | Offset: 70,991, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | END OF FILE                         | Offset: 70,991, Len... |
| 8:28:2...          | drpbx.exe    | 6356 | ReadFile        | C:\Windows\Assembly\NativeImages_v2.0.50727_64\mscorlib\95ce4e7117457677847d9f26c3bdf0\m... | SUCCESS                             | Offset: 3,857,408, ... |
| 8:28:2...          | drpbx.exe    | 6356 | CloseFile       | C:\Users\Luqman\AppData\Roaming\System32Work\EncryptedFileList.txt                          | SUCCESS                             |                        |
| 8:28:2...          | drpbx.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...          | drpbx.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:

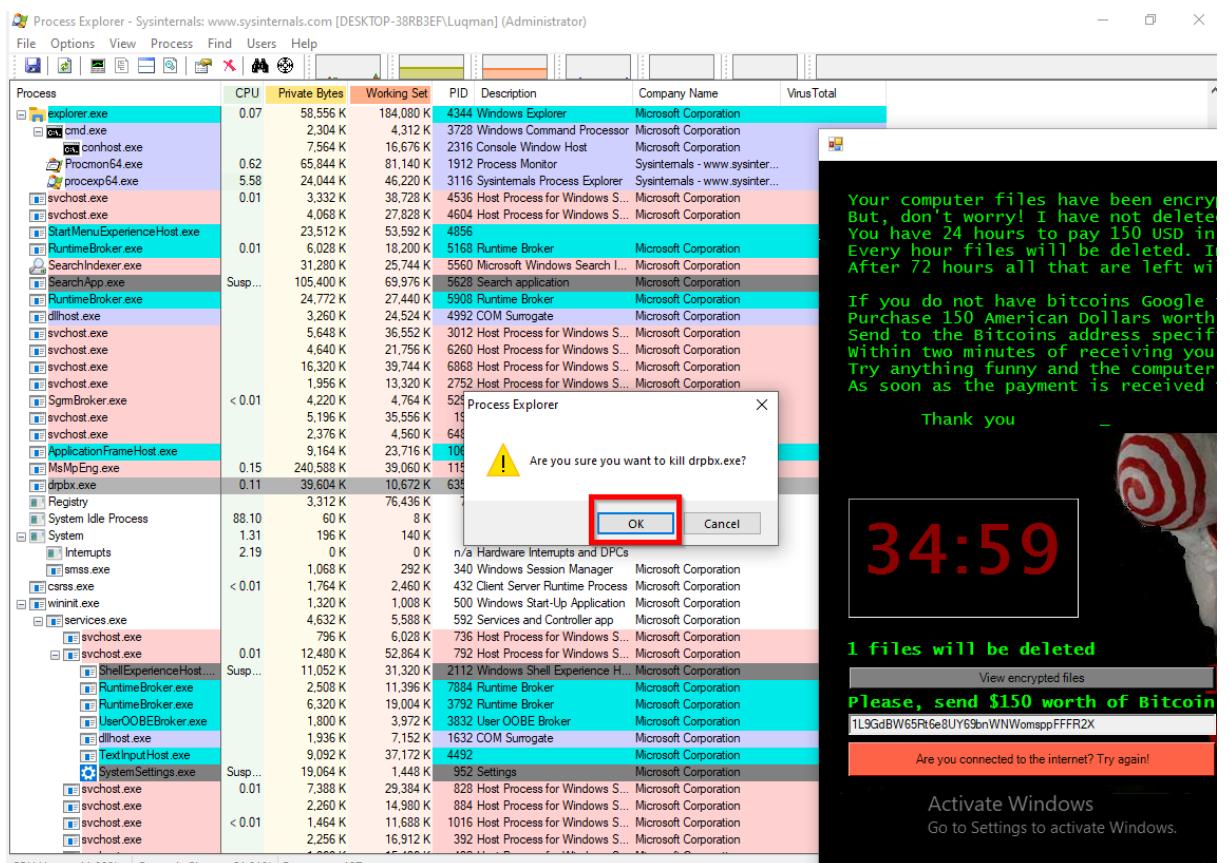
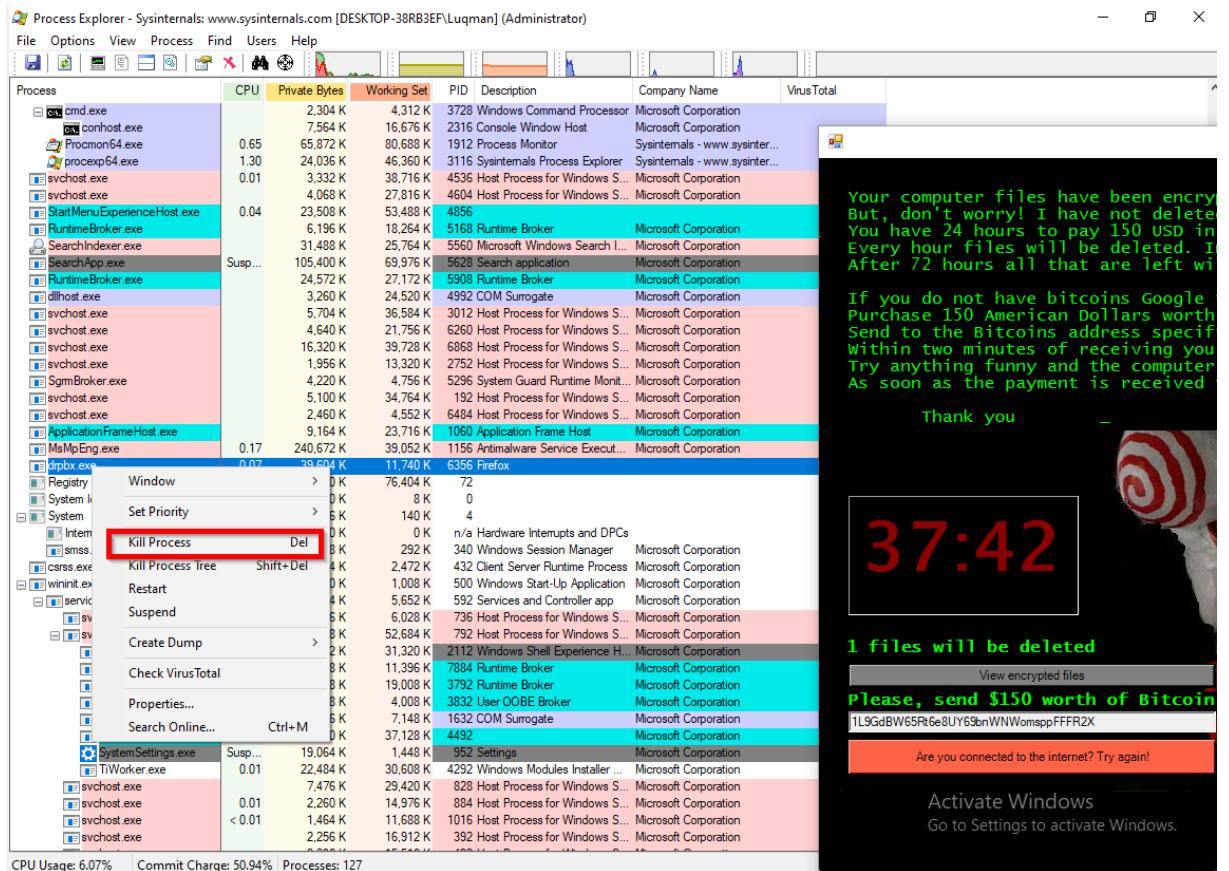
The analysis provides evidence of the malware's actions and its correlation with the "Welcome" screen:

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





## 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                  | 0.01    | 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 | Syteminternals 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          |            |
| SgmBroker.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          |            |
| !winlogon.exe               | 0.06    | 1,996 K       | 4,404 K     | 508  | Clear Server Runtime Process    | Microsoft Corporation          |            |
| !ondrvhost.exe              |         | 2,768 K       | 2,212 K     | 568  | Windows Logon Application       | Microsoft Corporation          |            |
| !dwm.exe                    | 0.42    | 3,920 K       | 5,176 K     | 720  | Usermode Font Driver Host       | 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          |            |

CPU Usage: 5.05% Commit Charge: 50.90% Processes: 127

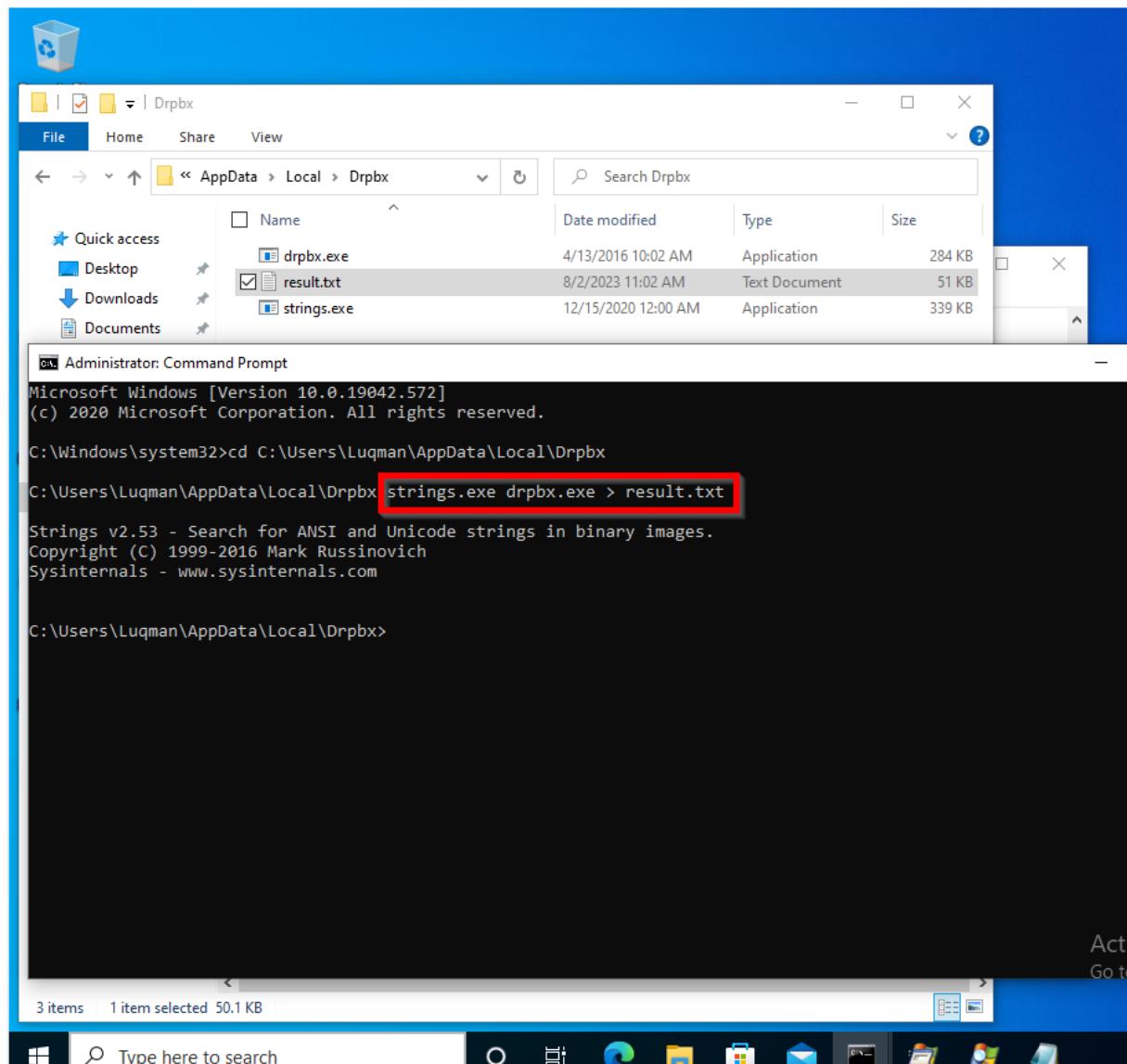
Type here to search

Activate Windows  
Go to Settings to activate Windows.

10:58 AM  
8/2/2023

## 5. Indicators of Malware:

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



A screenshot of a Windows desktop environment. At the top is a blue taskbar with icons for File Explorer, Start, Task View, Edge, File Explorer, Mail, File Explorer, and File Explorer. Below the taskbar is a white window titled 'Drpbx'. The window shows a file list with three items: 'drpbx.exe' (Application, 284 KB), 'result.txt' (Text Document, 51 KB, selected), and 'strings.exe' (Application, 339 KB). The path in the address bar is 'AppData > Local > Drpbx'. Below this is a black Command Prompt window with white text. The text shows the command 'strings.exe drpbx.exe > result.txt' highlighted with a red box. The output of the command is displayed, including the copyright information for Strings v2.53 and some binary data.

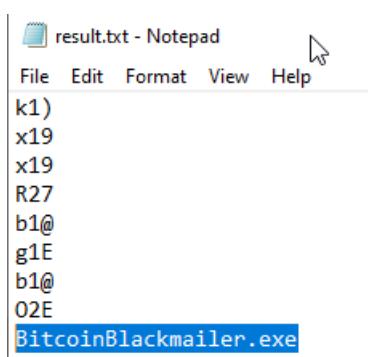
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.572]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Luqman\AppData\Local\Drpbx

C:\Users\Luqman\AppData\Local\Drpbx> strings.exe drpbx.exe > result.txt

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

C:\Users\Luqman\AppData\Local\Drpbx>
```



A screenshot of a Notepad window titled 'result.txt - Notepad'. The window contains the following text:

```
k1)
x19
x19
R27
b1@
g1E
b1@
O2E
BitcoinBlackmailer.exe
```

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 encrypted files will be returned to normal.

Thank you

Please, send \$ [REDACTED]  
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 [REDACTED]  
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:

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38B3EF\Luqman] (Administrator)

File Options View Process Find Users Help

| Process                  | CPU   | Private Bytes | Working Set | PID                           | Description                       | Company Name          | VirusTotal |
|--------------------------|-------|---------------|-------------|-------------------------------|-----------------------------------|-----------------------|------------|
| svchost.exe              |       | 1,704 K       | 13,616 K    | 4084                          | Host Process for Windows S...     | Microsoft Corporation |            |
| cffmon.exe               |       | 11,792 K      | 3,204 K     | 3204                          | CTF Loader                        | Microsoft Corporation |            |
| svchost.exe              |       | 4,100 K       | 38,784 K    | 4188                          | Host Process for Windows S...     | Microsoft Corporation |            |
| explorer.exe             | 0.16  | 61,436 K      | 246,828 K   | 4344                          | Windows Explorer                  | Microsoft Corporation |            |
| firefox.exe              |       | 48,124 K      | 7796        | Firefox                       |                                   |                       | 55/75      |
| cmd.exe                  |       | 4,636 K       | 3728        | Windows Command Processor     | Microsoft Corporation             |                       |            |
| conhost.exe              |       | 22,896 K      | 2316        | Console Window Host           | Microsoft Corporation             |                       |            |
| Procexp.exe              |       | 62,084 K      | 1912        | Process Monitor               | Sysinternals - www.sysinter...    |                       |            |
| procexp.exe              |       | 56,388 K      | 3116        | Sysinternals Process Explorer | Sysinternals - www.sysinter...    |                       |            |
| svchost.exe              |       | 54,844 K      | 1184        | Sysinternals Process Explorer | Sysinternals - www.sysinter...    |                       |            |
| svchost.exe              |       | 40,420 K      | 4536        | Host Process for Windows S... | Microsoft Corporation             |                       |            |
| StartMenu.exe            |       | 29,780 K      | 4604        | Host Process for Windows S... | Microsoft Corporation             |                       |            |
| RuntimeBroker.exe        |       | 66,480 K      | 4856        |                               |                                   |                       |            |
| SearchUI.exe             |       | 21,656 K      | 5168        | Runtime Broker                | Microsoft Corporation             |                       |            |
| SearchUI.exe             |       | 31,596 K      | 5560        | Microsoft Windows Search ...  | Microsoft Corporation             |                       |            |
| SearchUI.exe             |       | 7,864 K       | 2700        | Microsoft Windows Search F... | Microsoft Corporation             |                       |            |
| SearchUI.exe             |       | 8,492 K       | 8028        | Microsoft Windows Search P... | Microsoft Corporation             |                       |            |
| SearchUI.exe             |       | 135,104 K     | 5628        | Search application            | Microsoft Corporation             |                       |            |
| SearchUI.exe             |       | 31,316 K      | 5908        | Runtime Broker                | Microsoft Corporation             |                       |            |
| SearchUI.exe             |       | 25,616 K      | 4992        | COM Surrogate                 | Microsoft Corporation             |                       |            |
| dllhost.exe              |       | 41,720 K      | 3012        | Host Process for Windows S... | Microsoft Corporation             |                       |            |
| svchost.exe              |       | 25,180 K      | 6260        | Host Process for Windows S... | Microsoft Corporation             |                       |            |
| svchost.exe              |       | 48,944 K      | 6868        | Host Process for Windows S... | Microsoft Corporation             |                       |            |
| svchost.exe              |       | 1,924 K       | 2752        | Host Process for Windows S... | Microsoft Corporation             |                       |            |
| SqmBroker.exe            |       | 4,160 K       | 4,796 K     | 5296                          | System Guard Runtime Monit...     | Microsoft Corporation |            |
| svchost.exe              |       | 5,204 K       | 37,276 K    | 192                           | Host Process for Windows S...     | Microsoft Corporation |            |
| svchost.exe              |       | 2,472 K       | 5,240 K     | 6484                          | Host Process for Windows S...     | Microsoft Corporation |            |
| ApplicationFrameHost.exe |       | 9,196 K       | 24,932 K    | 1060                          | Application Frame Host            | Microsoft Corporation |            |
| MsMpEng.exe              | 0.33  | 242,952 K     | 89,456 K    | 1156                          | Antimalware Service Execut...     | Microsoft Corporation |            |
| dpbx.exe                 | 0.02  | 40,292 K      | 11,240 K    | 6356                          | Firefox                           |                       |            |
| Registry                 |       | 3,580 K       | 28,264 K    | 72                            |                                   |                       |            |
| System Idle Process      | 92.04 | 60 K          | 8 K         | 0                             |                                   |                       |            |
| System                   | 1.00  | 196 K         | 140 K       | 4                             |                                   |                       |            |
| Interrupts               | 1.56  | 0 K           | 0 K         | n/a                           | Hardware Interrupts and DPCs      |                       |            |
| sms.exe                  |       | 1,068 K       | 300 K       | 340                           | Windows Session Manager           | Microsoft Corporation |            |
| cors.exe                 |       | 1,724 K       | 2,572 K     | 432                           | Client Server Runtime Process     | Microsoft Corporation |            |
| wininit.exe              |       | 1,320 K       | 1,016 K     | 500                           | Windows Start-Up Application      | Microsoft Corporation |            |
| services.exe             |       | 4,584 K       | 6,308 K     | 592                           | Services and Controller app       | Microsoft Corporation |            |
| svchost.exe              |       | 796 K         | 6,204 K     | 736                           | Host Process for Windows S...     | Microsoft Corporation |            |
| svchost.exe              |       | < 0.01        | 12,436 K    | 54,716 K                      | 792 Host Process for Windows S... | Microsoft Corporation |            |
| ShellExperienceHost.exe  |       | 16,084 K      | 57,184 K    | 2112                          | Windows Shell Experience H...     | Microsoft Corporation |            |
| RuntimeBroker.exe        |       | 6,060 K       | 24,648 K    | 7884                          | Runtime Broker                    | Microsoft Corporation |            |
| RuntimeBroker.exe        |       | 6,844 K       | 22,252 K    | 3792                          | Runtime Broker                    | Microsoft Corporation |            |
| UserOOBEBroker.exe       |       | 1,896 K       | 4,132 K     | 3832                          | User OOBE Broker                  | Microsoft Corporation |            |

CPU Usage: 7.96% Commit Charge: 35.20% Processes: 144

VirusTotal - File - 3ae96f73d805e1d3995253db4d910300d8442ea603737a142...

https://www.virustotal.com/gui/file/3ae96f73d805e1d3995253db4d910300d8442ea603737a142...

URL, IP address, domain, or file hash

65 / 71

Community Score

① 65 security vendors and 4 sandboxes flagged this file as malicious

Reanalyze Similar More

BitcoinBlackmailer.exe

Size: 283.50 KB | Last Analysis Date: 14 hours ago | EXE

peexe assembly checks-user-input runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access via-tor persistence

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

Contacted Domains (4) ①

| Domain                     | Detections | Created    | Registrar        |
|----------------------------|------------|------------|------------------|
| arc.msn.com                | 0 / 88     | 1994-11-10 | MarkMonitor Inc. |
| fp2e7a.wpc.2be4.phicdn.net | 0 / 88     | 2014-11-14 | GoDaddy.com, LLC |
| fp2e7a.wpc.phicdn.net      | 0 / 88     | 2014-11-14 | GoDaddy.com, LLC |
| sfd-production.azurefd.net | 0 / 88     | 2018-05-08 | MarkMonitor Inc. |

Contacted IP addresses (18) ①

VirusTotal - File - 3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7

https://www.virustotal.com/gui/file/3ae96f73d805e1d3995253db4d910300d844... 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      |

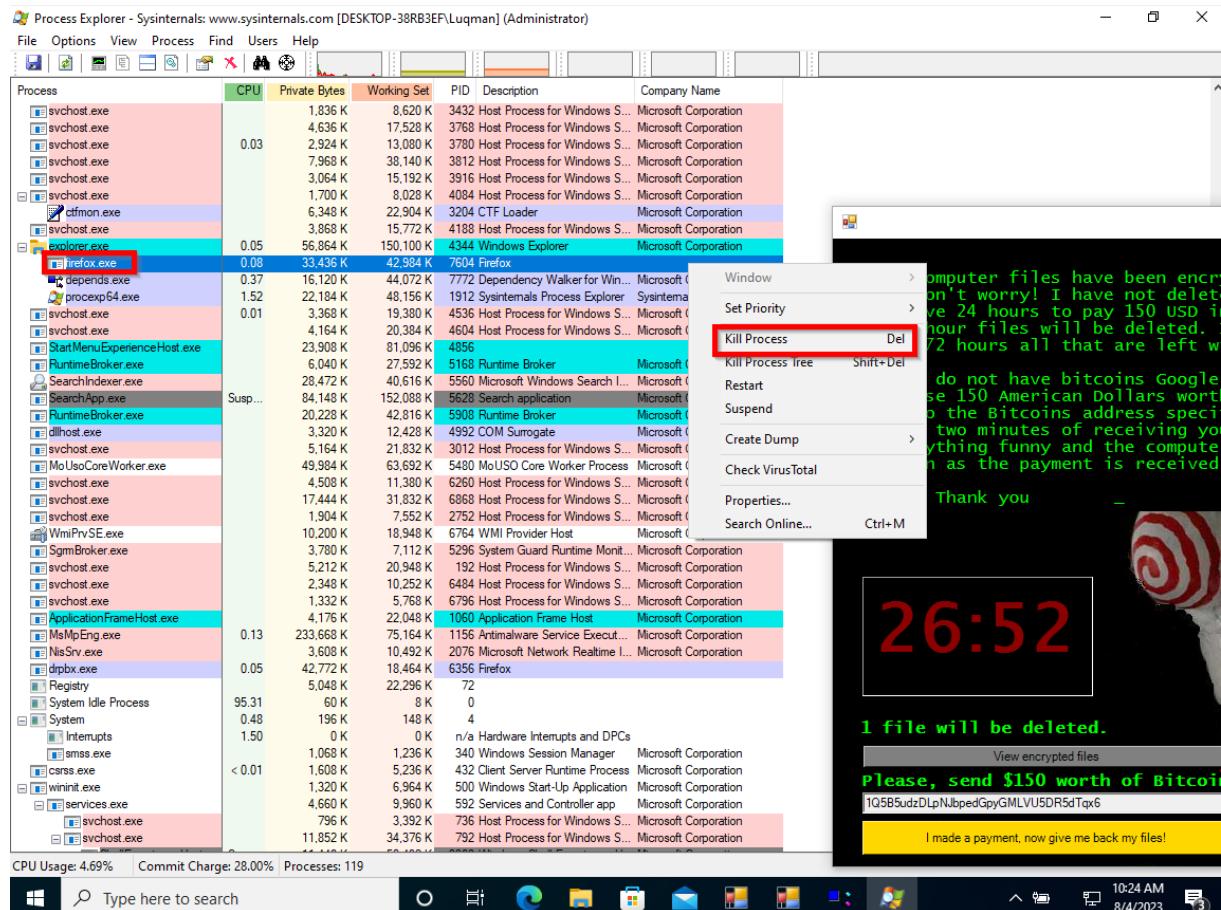
Execution Parents (13) ⓘ

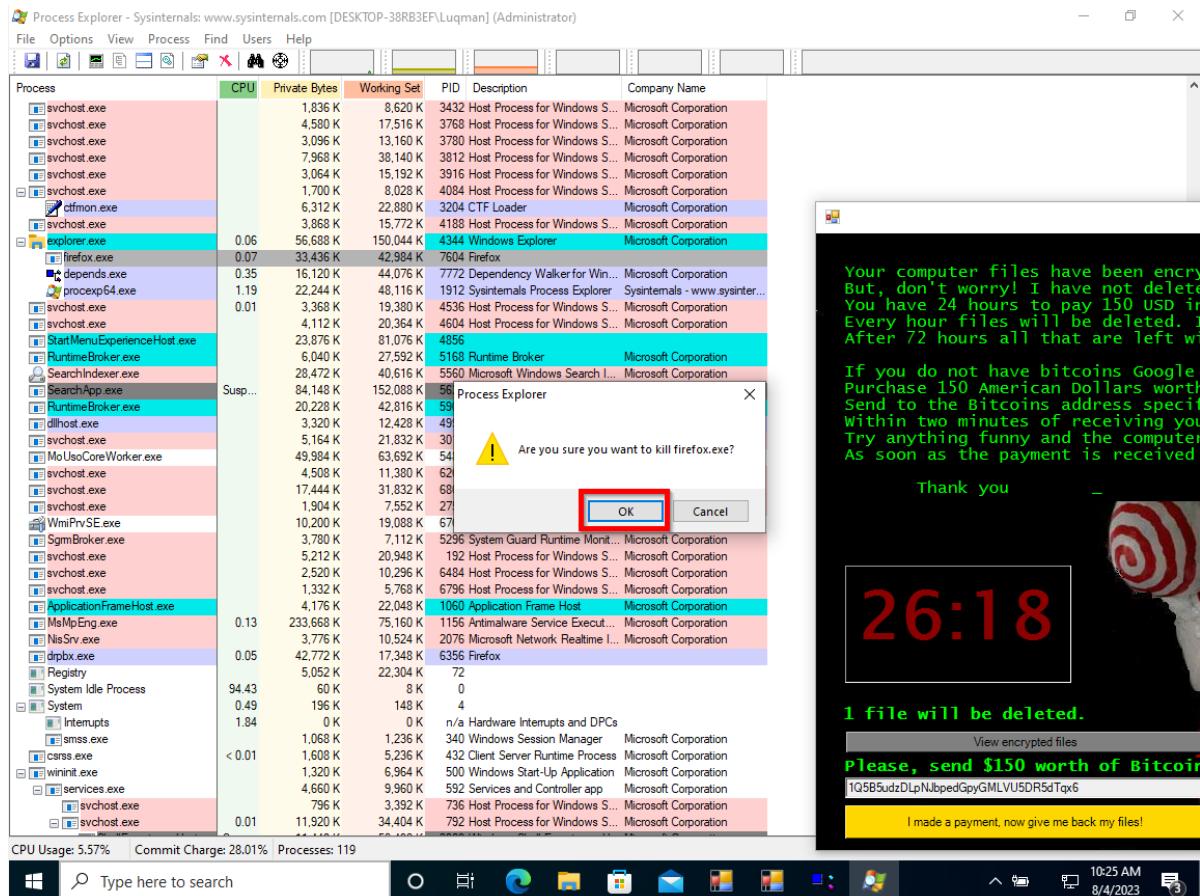
| Scanned    | Detections | Type      | Name   |
|------------|------------|-----------|--|
| 2021-12-14 | 44 / 68    | Win32 EXE | virussign.com_a76fec8271a1013b0059f138599c7220.vir               |
| 2022-11-22 | 44 / 71    | Win32 EXE | srichairaniulfarangkuti.exe                                      |
| 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





## B) Drpbx.exe

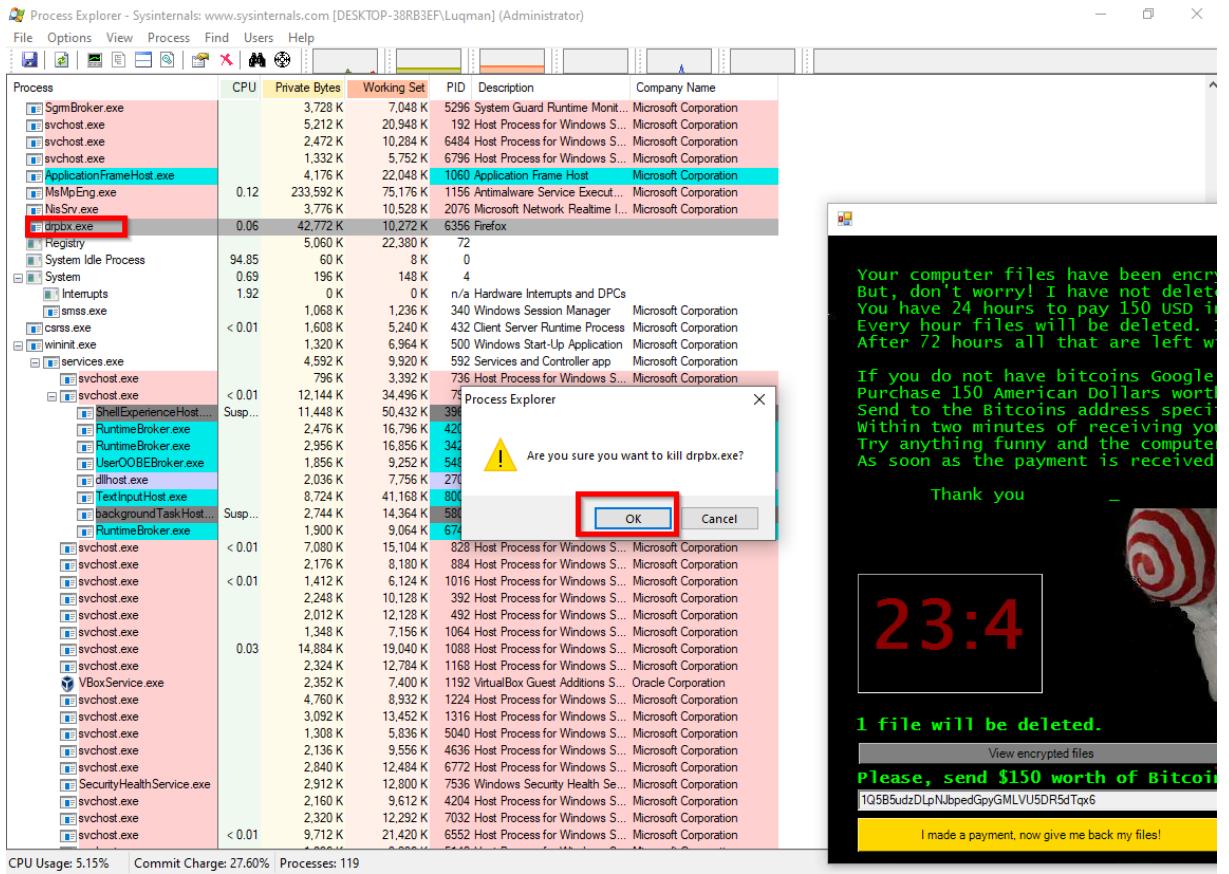
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-38RB3EF\Luqman] (Administrator)

File Options View Process Find Users Help

| Process                  | CPU     | Private Bytes | Working Set | PID  | Description                     | Company Name          |
|--------------------------|---------|---------------|-------------|------|---------------------------------|-----------------------|
| dllhost.exe              | 0.02    | 2,388 K       | 10,788 K    | 4992 | COM Surrogate                   | Microsoft Corporation |
| svchost.exe              |         | 5,140 K       | 17,164 K    | 3012 | Host Process for Windows S...   | Microsoft Corporation |
| MoUsCoreWorker.exe       |         | 33,300 K      | 45,720 K    | 5480 | MoUS Core Worker Process        | Microsoft Corporation |
| svchost.exe              |         | 4,408 K       | 11,128 K    | 6250 | Host Process for Windows S...   | Microsoft Corporation |
| svchost.exe              |         | 19,568 K      | 38,644 K    | 6868 | Host Process for Windows S...   | Microsoft Corporation |
| svchost.exe              |         | 2,140 K       | 7,488 K     | 2752 | Host Process for Windows S...   | Microsoft Corporation |
| WmiPrvSE.exe             |         | 8,244 K       | 17,744 K    | 6764 | WMI Provider Host               | Microsoft Corporation |
| SgmBroker.exe            |         | 4,028 K       | 7,092 K     | 5296 | System Guard Runtime Monit...   | Microsoft Corporation |
| svchost.exe              |         | 8,432 K       | 22,908 K    | 192  | Host Process for Windows S...   | Microsoft Corporation |
| svchost.exe              |         | 2,424 K       | 9,884 K     | 6484 | Host Process for Windows S...   | Microsoft Corporation |
| svchost.exe              |         | 1,440 K       | 5,772 K     | 6796 | Host Process for Windows S...   | Microsoft Corporation |
| ApplicationFrameHost.exe |         | 7,656 K       | 29,940 K    | 1060 | Application Frame Host          | Microsoft Corporation |
| WmiPrvSE.exe             | 0.15    | 4,304 K       | 12,072 K    | 4944 | WMI Provider Host               | Microsoft Corporation |
| svchost.exe              |         | 2,788 K       | 12,156 K    | 6784 | Host Process for Windows S...   | Microsoft Corporation |
| svchost.exe              |         | 1,724 K       | 7,028 K     | 6320 | Host Process for Windows S...   | Microsoft Corporation |
| MsMpEng.exe              |         | 227,068 K     | 163,180 K   | 1156 | Antimalware Service Execut...   | Microsoft Corporation |
| NisSv.exe                |         | 3,608 K       | 10,352 K    | 2076 | Microsoft Network Realtime I... | Microsoft Corporation |
| drpbx.exe                | 1.28    | 33,760 K      | 34,428 K    | 6356 | Firefox                         | Microsoft Corp        |
| Gamebar.exe              | < 0.01  | 15,680 K      | 52,976 K    | 6500 | Abox Game Bar                   | Microsoft Corp        |
| GameBarFTServer.exe      | 0.01    | 3,640 K       | 15,748 K    | 1880 | Xbox Game Bar Full Trust C...   | Microsoft Corp        |
| svchost.exe              | 0.04    | 5,008 K       | 28,424 K    | 3640 | Host Process for Windows S...   | Microsoft Corp        |
| Registry                 |         | 11,152 K      | 54,472 K    | 72   |                                 |                       |
| System Idle Process      | 87.16   | 60 K          | 8 K         | 0    |                                 |                       |
| System                   | 1.01    | 196 K         | 152 K       | 4    |                                 |                       |
| Interrupts               | 1.52    | 0 K           | 0 K         | n/a  | Hardware Interrupts and DPCs    |                       |
| smss.exe                 |         | 1,068 K       | 1,236 K     | 340  | Windows Session Manager         | Microsoft Corp        |
| cssrs.exe                |         | 1,656 K       | 5,248 K     | 432  | Cleer Server Runtime Process    | Microsoft Corp        |
| wminit.exe               |         | 1,320 K       | 6,964 K     | 500  | Windows Start-Up Application    | Microsoft Corp        |
| services.exe             | 0.03    | 4,776 K       | 9,904 K     | 592  | Services and Controller app     | Microsoft Corp        |
| svchost.exe              |         | 796 K         | 3,356 K     | 736  | Host Process for Windows S...   | Microsoft Corp        |
| svchost.exe              | 0.15    | 12,516 K      | 33,540 K    | 792  | Host Process for Windows S...   | Microsoft Corp        |
| RuntimeBroker.exe        | < 0.01  | 3,588 K       | 17,276 K    | 5028 | Runtime Broker                  | Microsoft Corp        |
| TWWorker.exe             |         | 29,880 K      | 35,148 K    | 6808 | Windows Modules Installer ...   | Microsoft Corp        |
| SystemSettings.exe       | Susp... | 23,424 K      | 77,840 K    | 5320 | Settings                        | Microsoft Corp        |
| TextInputHost.exe        |         | 8,908 K       | 39,294 K    | 1616 |                                 | Microsoft Corporation |
| smartscreen.exe          |         | 8,416 K       | 24,268 K    | 7296 | Windows Defender SmartScr...    | Microsoft Corporation |
| dllhost.exe              |         | 1,788 K       | 8,020 K     | 8988 | COM Surrogate                   | Microsoft Corporation |
| RuntimeBroker.exe        |         | 2,184 K       | 12,844 K    | 8196 | Runtime Broker                  | Microsoft Corporation |
| ShellExperienceHost.exe  |         | 11,996 K      | 50,112 K    | 9184 | Windows Shell Experience H...   | Microsoft Corporation |
| RuntimeBroker.exe        |         | 3,136 K       | 18,316 K    | 4940 | Runtime Broker                  | Microsoft Corporation |
| RuntimeBroker.exe        |         | 3,012 K       | 17,096 K    | 5520 | Runtime Broker                  | Microsoft Corporation |
| RuntimeBroker.exe        |         | 3,592 K       | 19,576 K    | 8972 | Runtime Broker                  | Microsoft Corporation |
| svchost.exe              | 0.25    | 8,088 K       | 16,464 K    | 828  | Host Process for Windows S...   | Microsoft Corporation |
| svchost.exe              | 0.01    | 2,416 K       | 8,316 K     | 884  | Host Process for Windows S...   | Microsoft Corporation |

CPU Usage: 12.84% Commit Charge: 21.23% Processes: 133

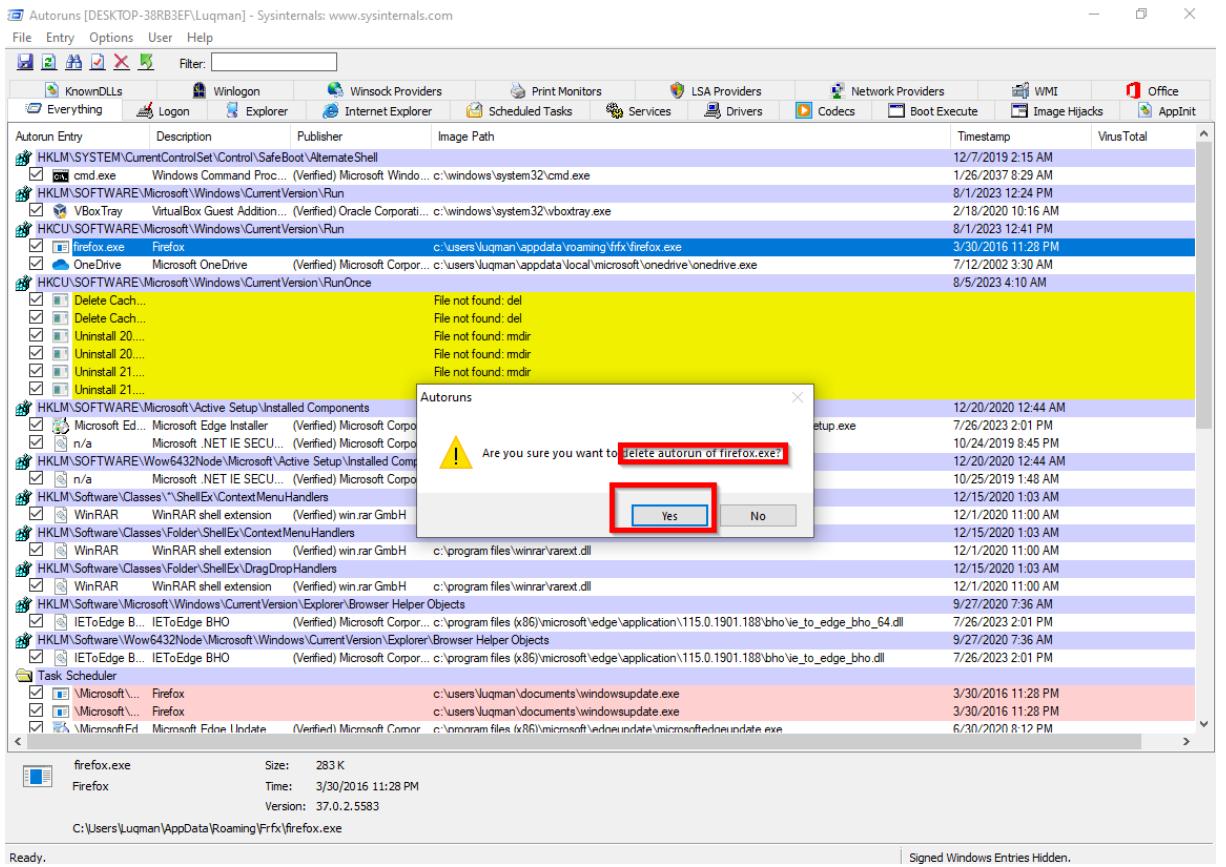
Type here to search



**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\Roaming\Frffx', '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'.

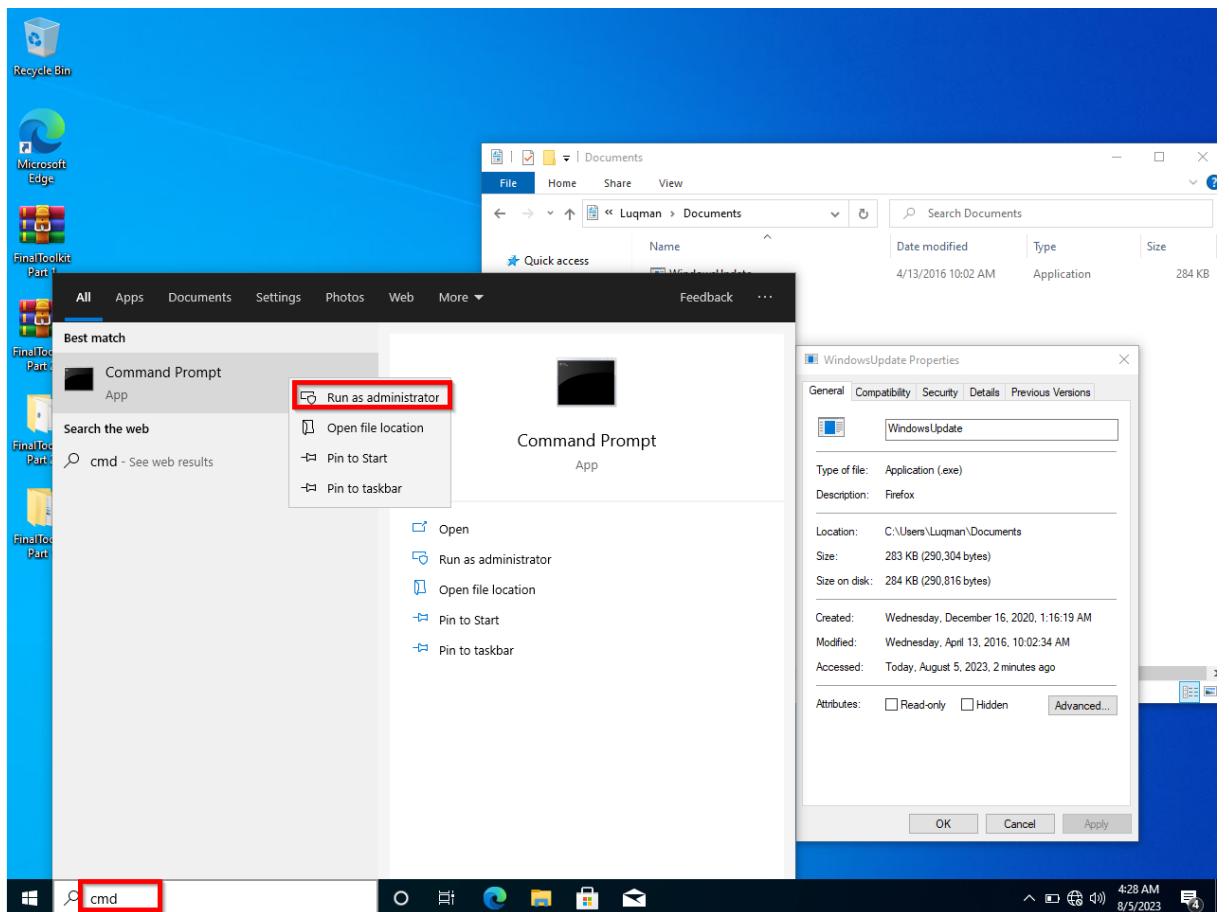
Armed with this newfound insight, I executed a decisive course of action. I promptly eliminated the aforementioned entries, thereby obliterating the presence of 'firefox.exe', 'drpbx.exe', 'WindowsUpdate', and 'WindowsUpdate\_Scanner' from the system.

The screenshot shows the 'Autoruns' application interface. A context menu is open over a listed item, with the 'Delete' option highlighted. The item being deleted is 'firefox.exe' located under 'HKEY\Software\Microsoft\Windows\CurrentVersion\Run'. The application's title bar reads 'Autoruns [DESKTOP-38RB3EF]\Luqman] - Sysinternals: www.sysinternals.com'. The menu bar includes File, Entry, Options, User, and Help. The main pane displays various registry keys and their values, including 'cmd.exe', 'Vboxtray', and several entries for 'Firefox' and 'WinRAR'. The bottom status bar shows the file path 'C:\Users\Luqman\AppData\Roaming\Frffx\firefox.exe' and the file details: Size: 283 K, Time: 3/30/2016 11:28 PM, Version: 37.0.2.5583.



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

| Autoruns [DESKTOP-38RB3EF\Luqman] - Sysinternals: www.sysinternals.com                     |  |  |                    |                     |            |
|--|--|--|--------------------|---------------------|------------|
| File   | Entry  | Options  | User               | Help                |            |
|  |  |  |                    |                     |            |
| Autorun Entry  | Description  | Publisher  | Image Path         | Timestamp           | VirusTotal |
| HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell                              |  |  |                    | 12/7/2019 2:15 AM   |            |
| cmd.exe  | Windows Command Processor (Verified) Microsoft Windows                 | c:\windows\system32\cmd.exe                                  | 1/26/2037 8:29 AM  |                     |            |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Run   |  |  |                    | 8/1/2023 12:24 PM   |            |
| VboxTray   | VirtualBox Guest Additions Tr... (Verified) Oracle Corporation         | c:\windows\system32\vboxtray.exe                             | 2/18/2020 10:16 AM |                     |            |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Run   |  |  |                    | 8/1/2023 12:41 PM   |            |
| OneDrive   | Microsoft OneDrive (Verified) Microsoft Corporation                    | c:\users\luqman\appdata\local\microsoft\onedrive\oned...     | 7/12/2022 3:30 AM  |                     |            |
| HKLM\Software\Microsoft\Active Setup\Installed Components                                  |  |  |                    | 12/20/2020 12:44 AM |            |
| Microsoft Edge   | Microsoft Edge Installer (Verified) Microsoft Corporation              | c:\program files (x86)\microsoft\edge\application\115.0.1... | 7/26/2023 2:01 PM  |                     |            |
| n/a  | Microsoft .NET IE SECURIT... (Verified) Microsoft Corporation          | c:\windows\system32\mscores.dll                              | 10/24/2019 8:45 PM |                     |            |
| HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components                      |  |  |                    | 12/20/2020 12:44 AM |            |
| n/a  | Microsoft .NET IE SECURIT... (Verified) Microsoft Corporation          | c:\windows\syswow64\mscores.dll                              | 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                         | c:\program files\winrar\vreext.dll                           | 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\vreext.dll                           | 12/1/2020 11:00 AM |                     |            |
| HKLM\Software\Classes\Folder\ShellEx\DragDrop Handlers                                     |  |  |                    | 12/15/2020 1:03 AM  |            |
| WinRAR   | WinRAR shell extension (Verified) win.rar GmbH                         | c:\program files\winrar\vreext.dll                           | 12/1/2020 11:00 AM |                     |            |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects             |  |  |                    | 9/27/2020 7:36 AM   |            |
| IEToEdge BHO   | IEToEdge BHO (Verified) Microsoft Corporation                          | c:\program files (x86)\microsoft\edge\application\115.0.1... | 7/26/2023 2:01 PM  |                     |            |
| HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects |  |  |                    | 9/27/2020 7:36 AM   |            |
| IEToEdge BHO   | IEToEdge BHO (Verified) Microsoft Corporation                          | c:\program files (x86)\microsoft\edge\application\115.0.1... | 7/26/2023 2:01 PM  |                     |            |
| Task Scheduler   |  |  |                    |                     |            |
| \Microsoft\Windows\WindowsUpdate\WindowsUpdate   | Firefox  | c:\users\luqman\documents\windowsupdate.exe                  | 3/30/2016 11:28 PM |                     |            |
| \Microsoft\Windows\WindowsUpdate\WindowsUpdate_Scaner                                      | Firefox  | c:\users\luqman\documents\windowsupdate.exe                  | 3/30/2016 11:28 PM |                     |            |
| \Microsoft\EdgeUpdate\TaskMachineCore  | Microsoft Edge Update Service (Verified) Microsoft Corporation         | c:\program files (x86)\microsoft\edgeupdate\microsof...      | 6/30/2020 8:12 PM  |                     |            |
| \Microsoft\EdgeUpdate\TaskMachineUA  | Microsoft Edge Update Service (Verified) Microsoft Corporation         | c:\program files (x86)\microsoft\edgeupdate\microsof...      | 6/30/2020 8:12 PM  |                     |            |
| \OneDrive Reporting Task-S-1-5-21-1313434519-986968716-766249846-1001                      | Standalone Updater (Verified) Microsoft Corporation                    | c:\users\luqman\appdata\local\microsoft\onedrive\oned...     | 1/25/2001 9:56 PM  |                     |            |
| \OneDrive Standalone Update Task-S-1-5-21-1313434519-986968716-76624...                    | Standalone Updater (Verified) Microsoft Corporation                    | c:\users\luqman\appdata\local\microsoft\onedrive\oned...     | 1/25/2001 9:56 PM  |                     |            |
| \OneDrive Standalone Update Task-S-1-5-21-1313434519-986968716-76624...                    | Standalone Updater (Verified) Microsoft Corporation                    | c:\users\luqman\appdata\local\microsoft\onedrive\oned...     | 1/25/2001 9:56 PM  |                     |            |
| HKLM\System\CurrentControlSet\Services   |  |  |                    | 8/5/2023 3:59 AM    |            |
| edgeupdate   | Microsoft Edge Update Service (Verified) Microsoft Corporation         | c:\program files (x86)\microsoft\edgeupdate\microsof...      | 6/30/2020 8:12 PM  |                     |            |
| edgeupdate   | Microsoft Edge Update Service (Verified) Microsoft Corporation         | c:\program files (x86)\microsoft\edgeupdate\microsof...      | 6/30/2020 8:12 PM  |                     |            |
| FontCache3.0.0.0   | Windows Presentation Foundation (Verified) Microsoft Corporation       | c:\windows\microsoft.net\framework64\v3.0\wpf\presen...      | 10/24/2019 9:32 PM |                     |            |
| MicrosoftEdgeElevationService  | Microsoft Edge Elevation Service (Verified) Microsoft Corporation      | c:\program files (x86)\microsoft\edge\application\115.0.1... | 7/26/2023 2:01 PM  |                     |            |
| VBoxService  | VirtualBox Guest Additions Service (Verified) Oracle Corporation       | c:\windows\system32\vboxservice.exe                          | 2/18/2020 10:16 AM |                     |            |
| HKLM\System\CurrentControlSet\Services   |  |  |                    | 8/5/2023 3:59 AM    |            |
| BthA2dp  | Microsoft Bluetooth A2dp driver (Not verified) Microsoft Corporation   | c:\windows\system32\drivers\btha2dp.sys                      | 11/16/2033 3:59 PM |                     |            |
| iaLPSSl_GPIO   | Intel(R) Serial IO GPIO Controller (C...) (Verified) Intel Corporation | c:\windows\system32\drivers\alpssi_gpio.sys                  | 2/2/2015 2:00 AM   |                     |            |



```

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
*-0
{!rt
K(T
P@B
2sH
y :u
tPbd
v'ov/
xx,<
Hvy
v[>q
_gp? -wU
~od
<hgM
[N=
]ou-
v;HK
N_V
60I
[Cdg
dmt
X),
yt\
L:b
ipZ
`q&I
5h2
I4xfQ
Sxu!3o,
9EYB
.![
%T>
&G*
6-#
|D<
$Nn
I7t.
\eq

```

```

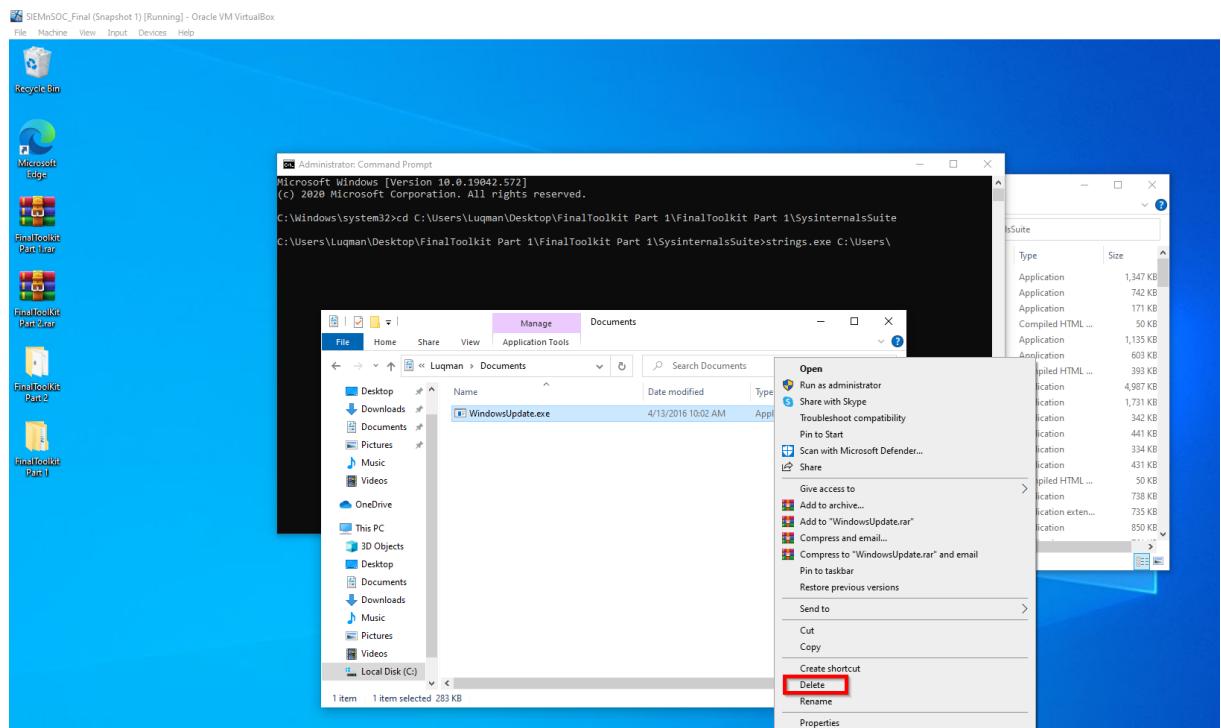
os Select Administrator: Command Prompt
get_Handle
TryGetValue
ContainsKey
GetAssemblies
GetName
get_CultureInfo
GetExecutingAssembly
GetManifestResourceStream
set_Position
ToLowerInvariant
IsNullOrEmpty
get_Flags
{{ file = {0}, ext = {1} }}
{{ file = {0}, fi = {1} }}
Congratulations. Your software has been registered. Confirmation code 994759
Email us this code in the chat to activate your software. It can take up to 48 hours.
Thank you.
Drpxb\drpxb.exe
Frfx\firefox.exe
system2\work()
our 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.
Very hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.
If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
End to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal.
try anything funny and the computer has several safety measures to delete your files.
as soon as the payment is received the encrypted 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 from your computer.
Great job
You did not send me enough! Try again!
You haven't made payment yet! Try again!
Are you connected to the internet? Try again!
files will be deleted
Lucida Console
labelWelcome

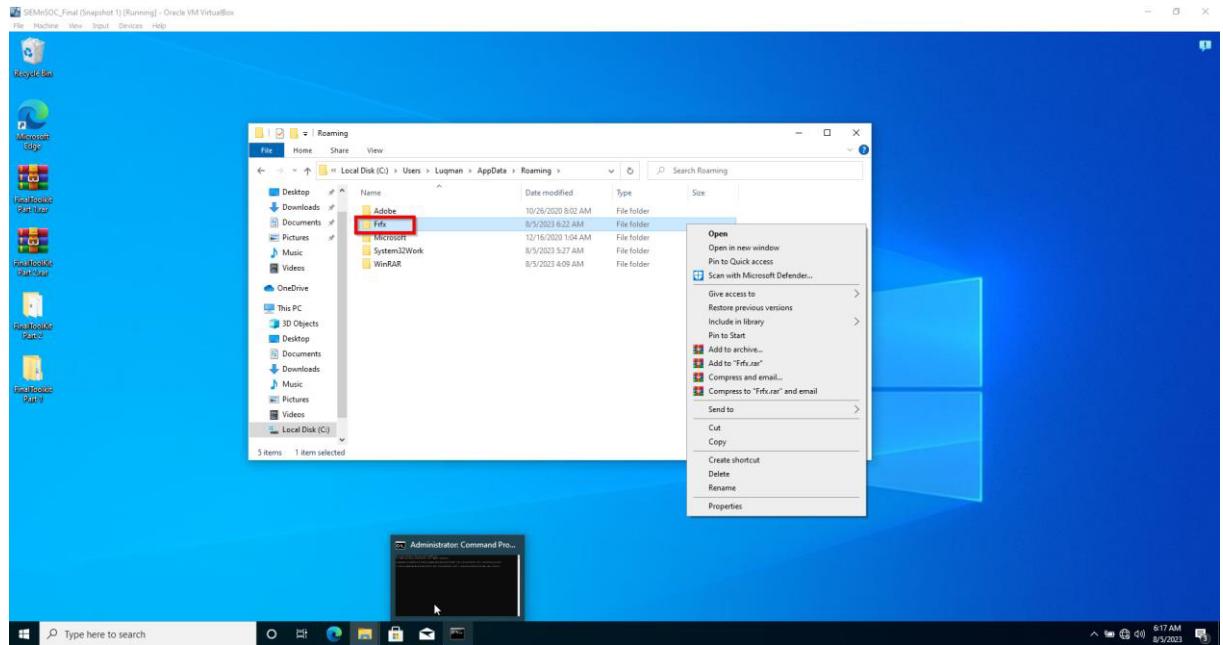
```

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

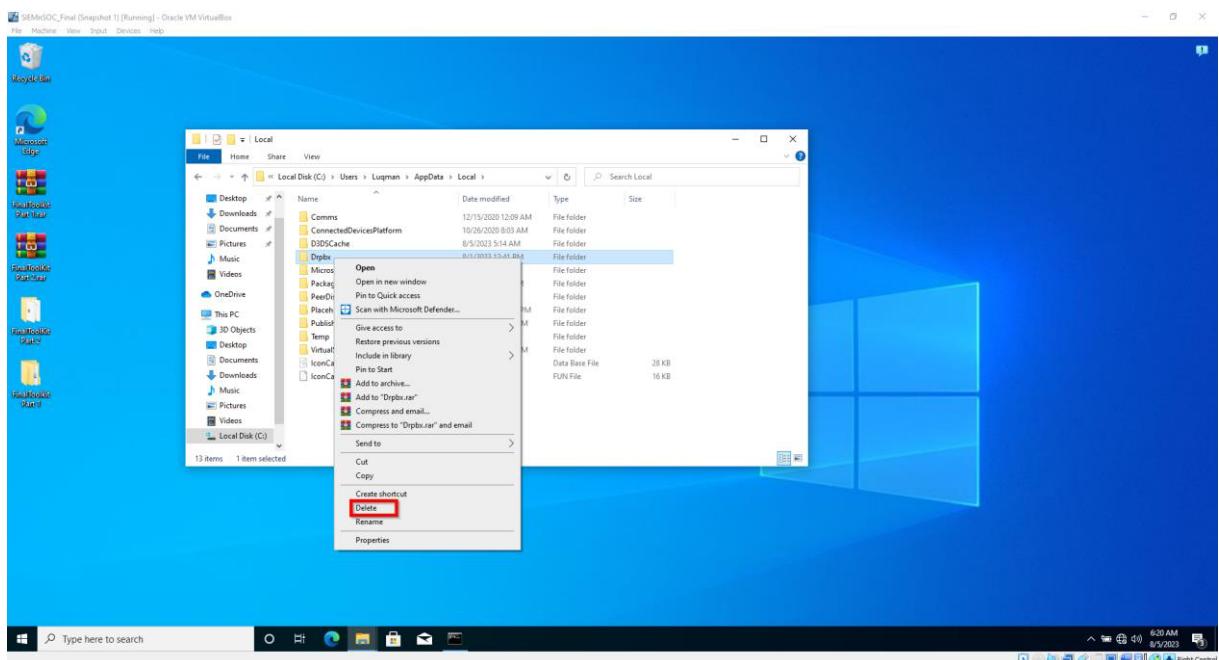
WindowsUpdate located at C:\Users\Luqman\Documents



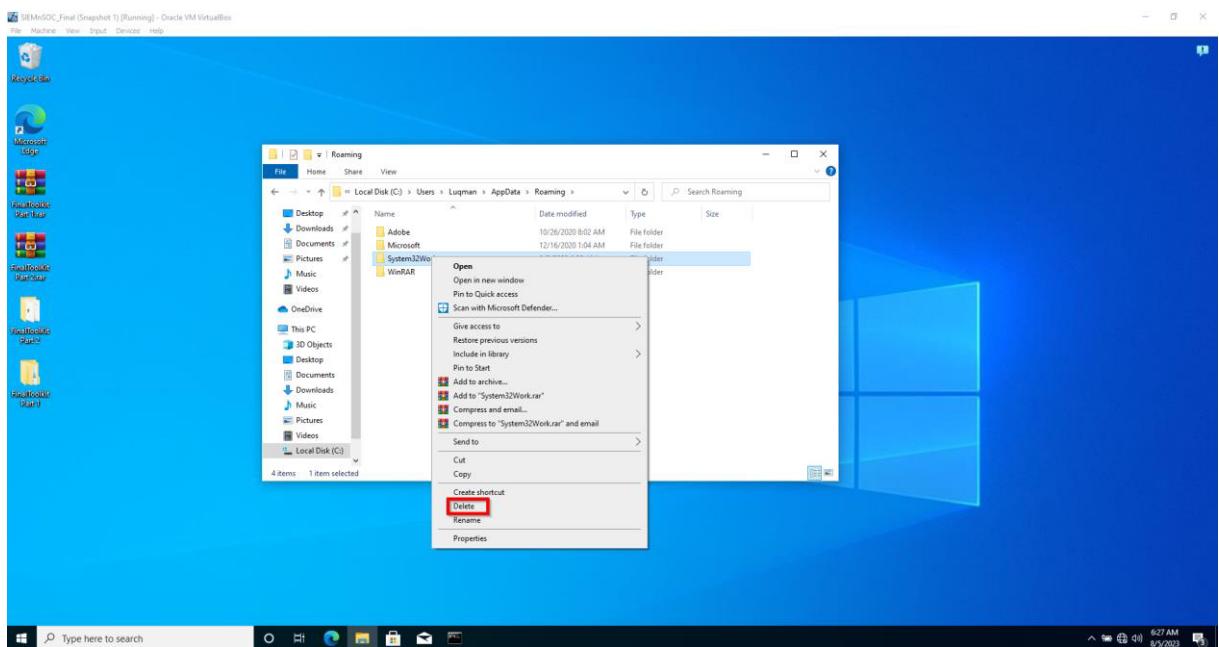
Firefox.exe located at C:\Users\Luqman\AppData\Roaming\Frfix



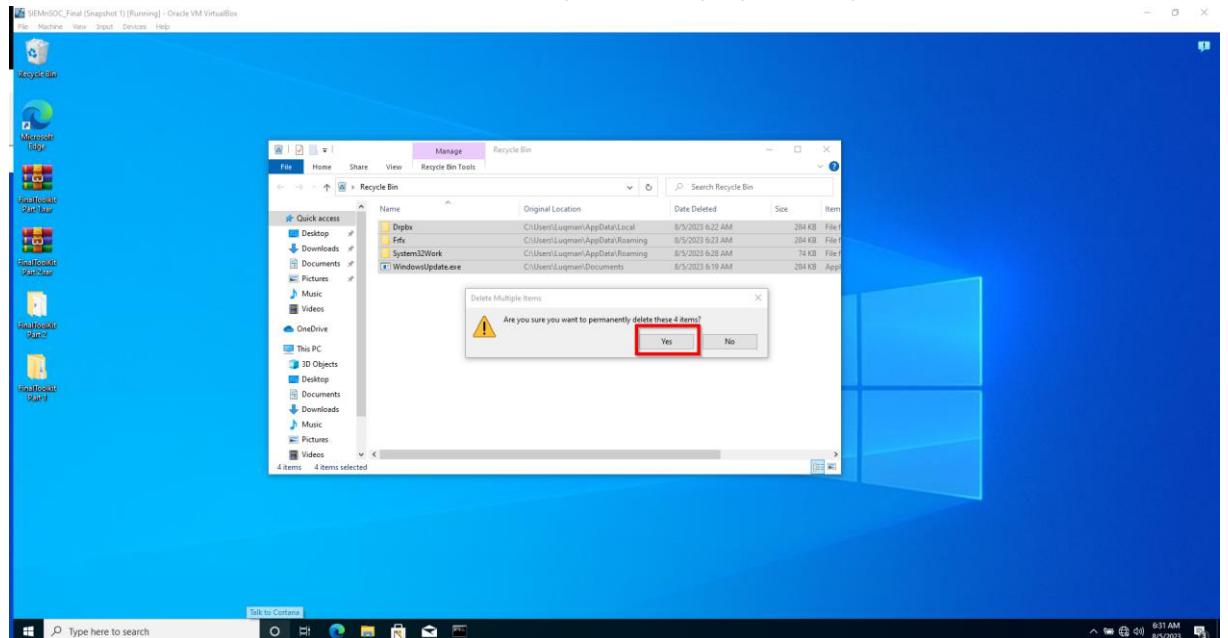
drpbx.exe locate at C:\Users\Luqman\AppData\Local\Drpbx



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.

Summary :

The tool decrypts the Jigsaw Ransomware infected files. Tool can decrypt a single file, folder or a disk. The tool can decrypt back the exact file without changing a single bit and user can have the option either deleting the encrypted file or keeping the encrypted copy in the disk.

File by File Decryption

Below screenshot shows the decryption of a single file. The decrypted file will be found in the same location of the original file.

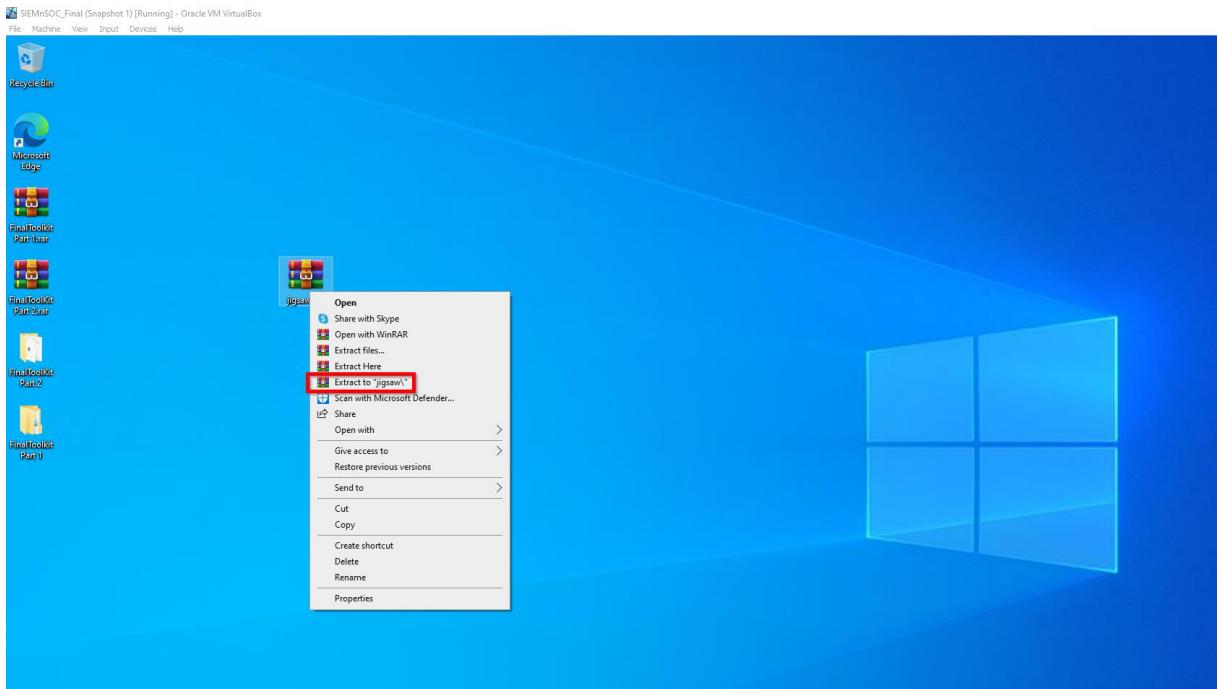
JIGSAW RANSOMWARE DECRYPTOR

Download now

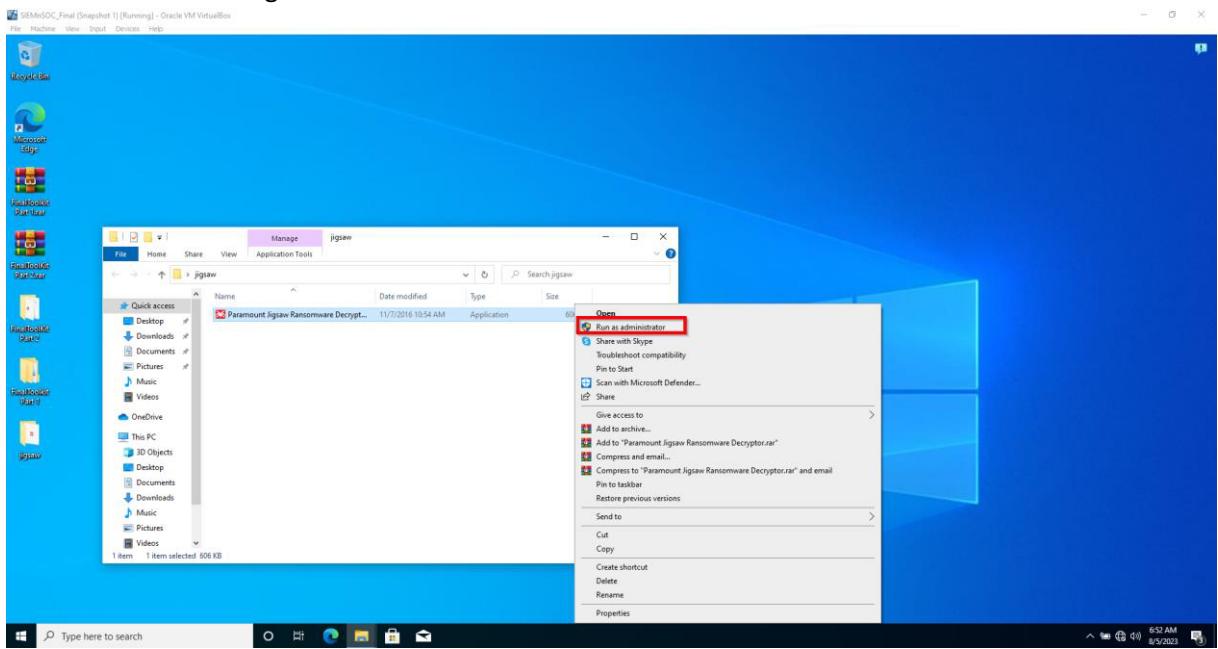
Ransomware is emerging as a leading cybersecurity threat to both organisations and individuals. But what is it? How do you defend yourself against it? Download our Free eBook Now

Figure 1. Jigsaw Ransomware Decryptor: File Decrypt

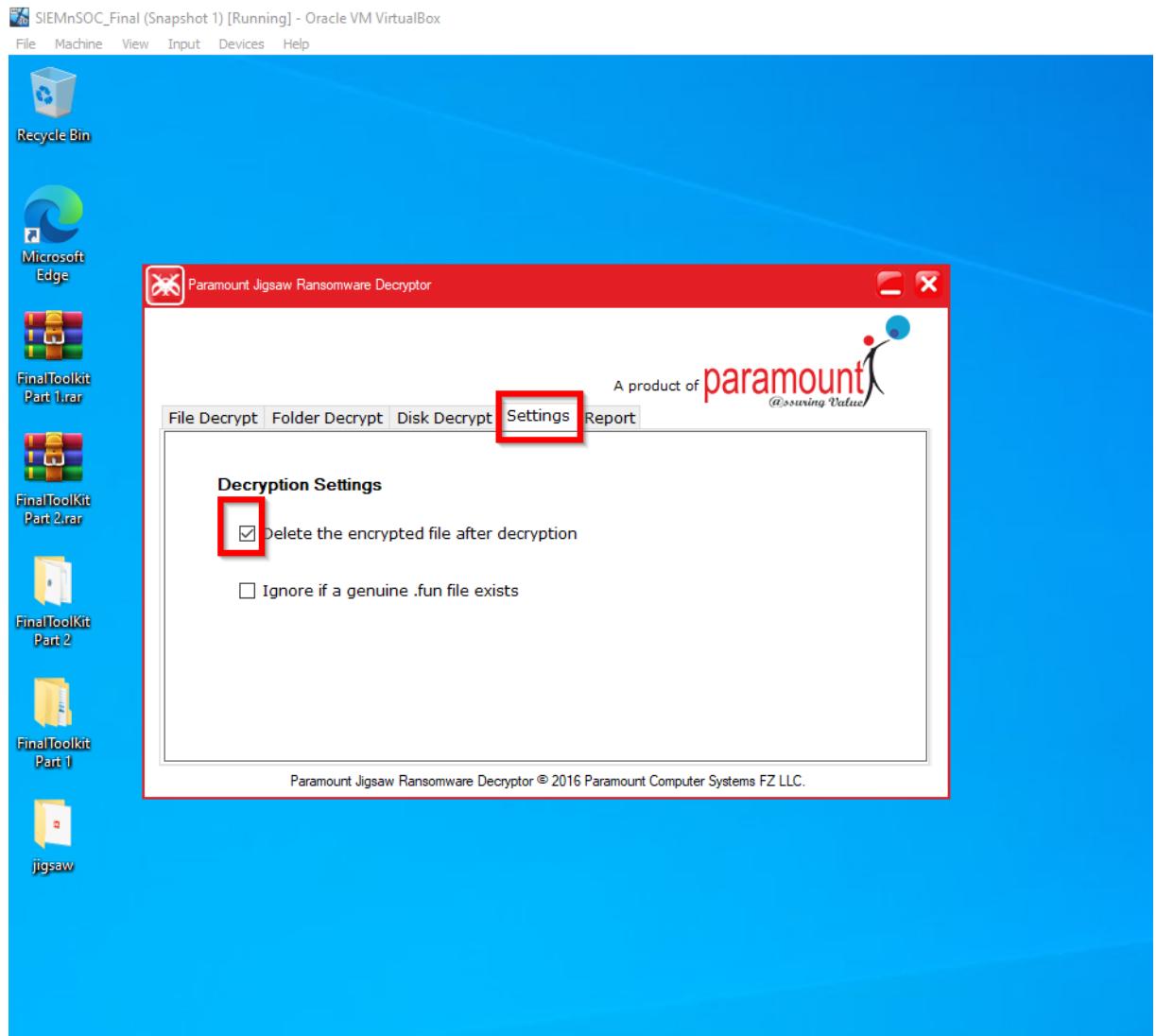
Aktywuj system Windows  
Przejdź do ustawień, aby aktywować system Windows.



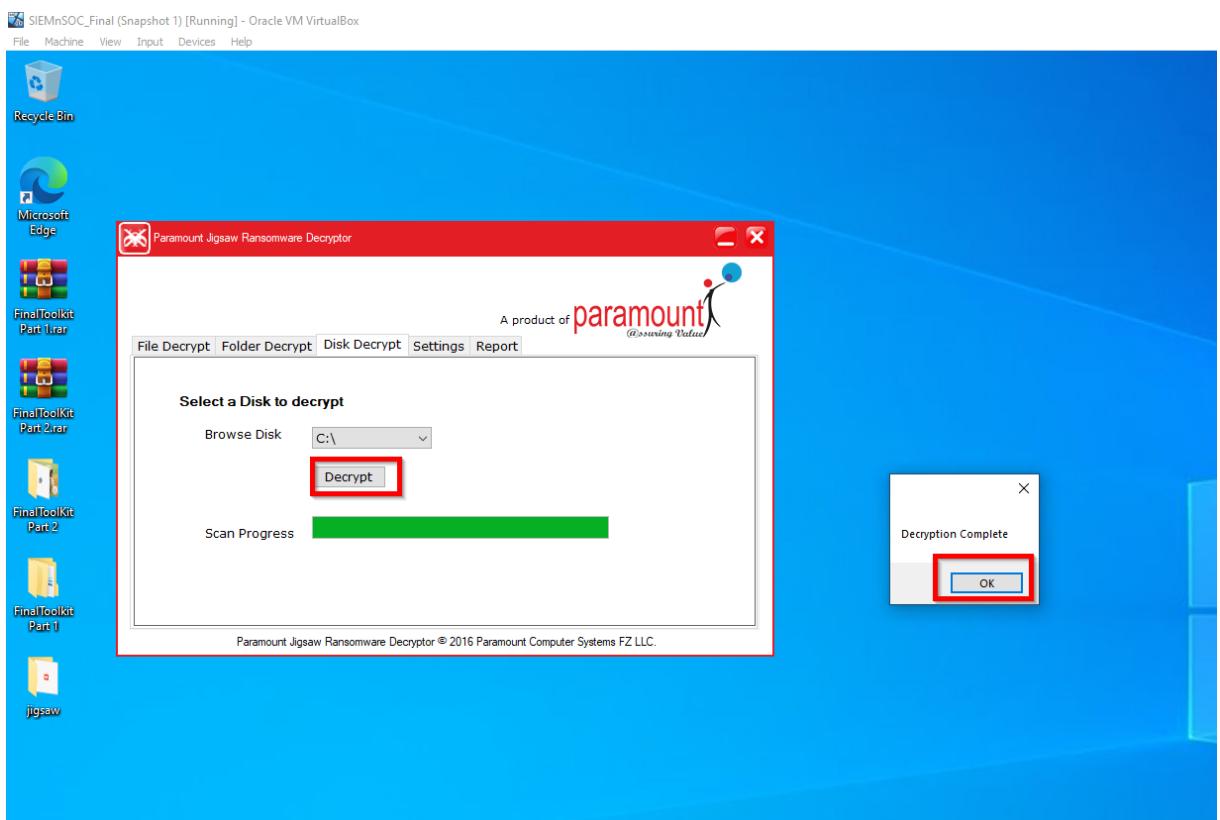
**Tool Execution:** Executing the tool as an administrator was a critical step. The program named "Paramount Jigsaw Ransomware Decryptor.exe" was launched, and immediate attention was directed to the "Settings" tab.



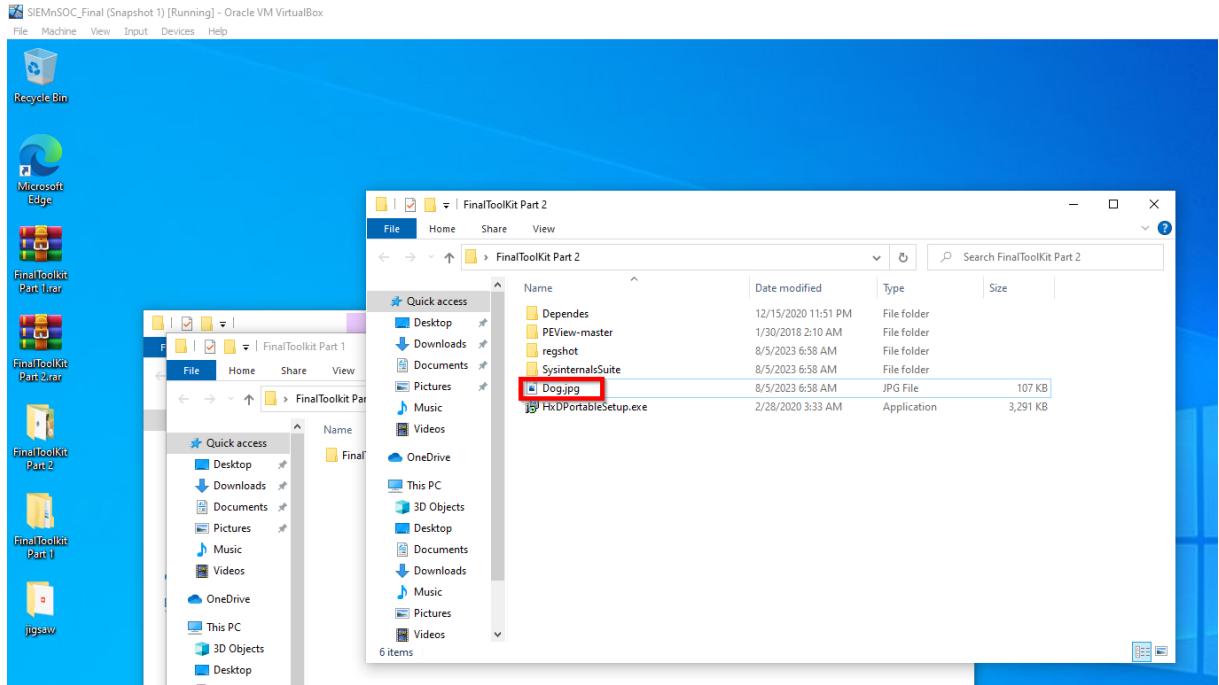
**Optimal Settings Configuration:** Within the "Settings" tab, a pivotal setting was configured. Specifically, the option "Delete the encrypted file after decryption" was selected. This setting ensured not only the recovery of the encrypted files but also the removal of the encrypted duplicates.



**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.