Report on Ransomware Analysis

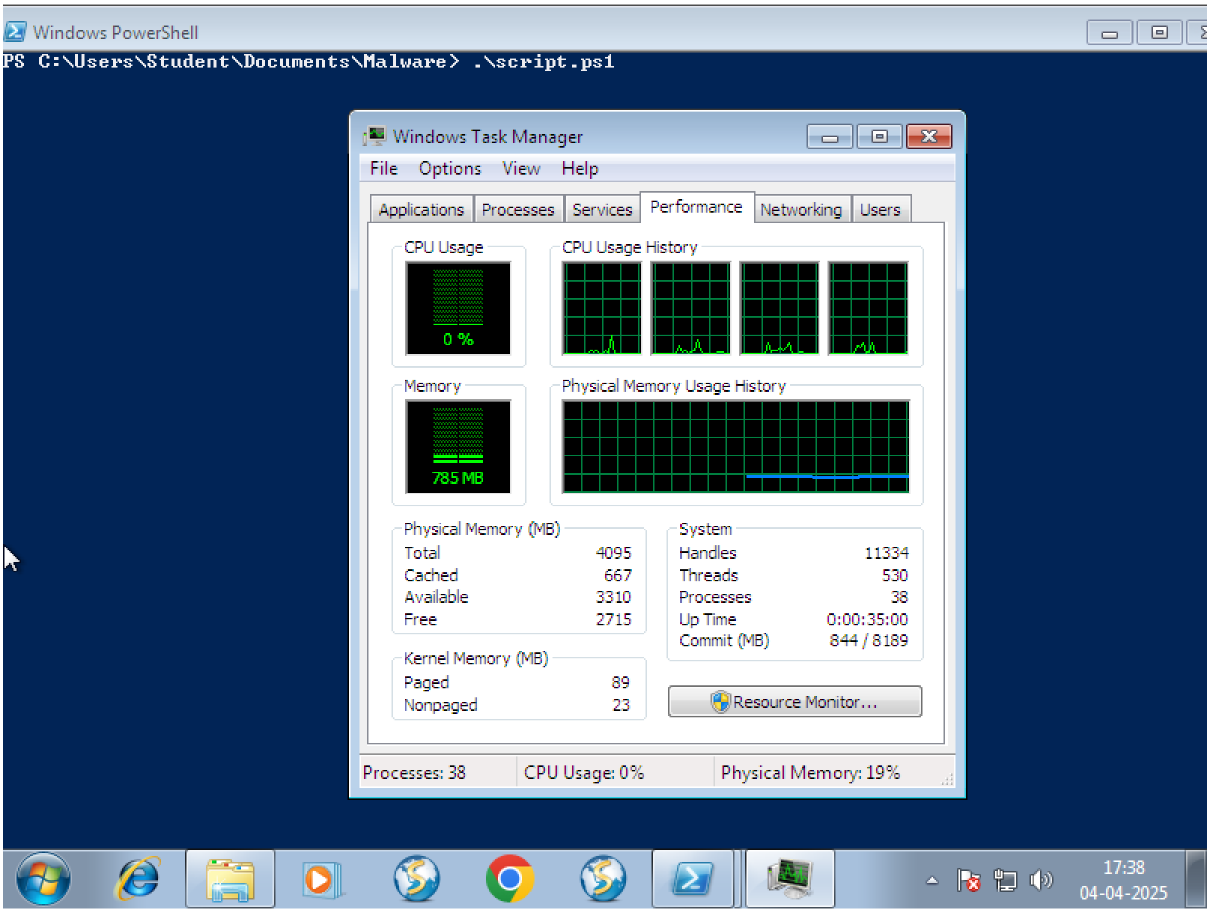
Security and Forensics Lab 2

Subham Sanket Rout
24CS06017
M.Tech (CSE) 1st Year

System status before execution of any malware.

We measured the system's status such as CPU usage, physical memory usage and number of processes being executed while the system was idle and before we executed any of the Malwares. In addition to that we captured a screenshot of how the "File Explorer" looks like just for reference to look out for any changes after we execute any Malware.

- **Screenshot of the Task Manager showing the CPU usage and Memory usage when system is idle and no malware has been executed.**



```
PS C:\Users\Student\Documents\Malware> .\script.ps1
```

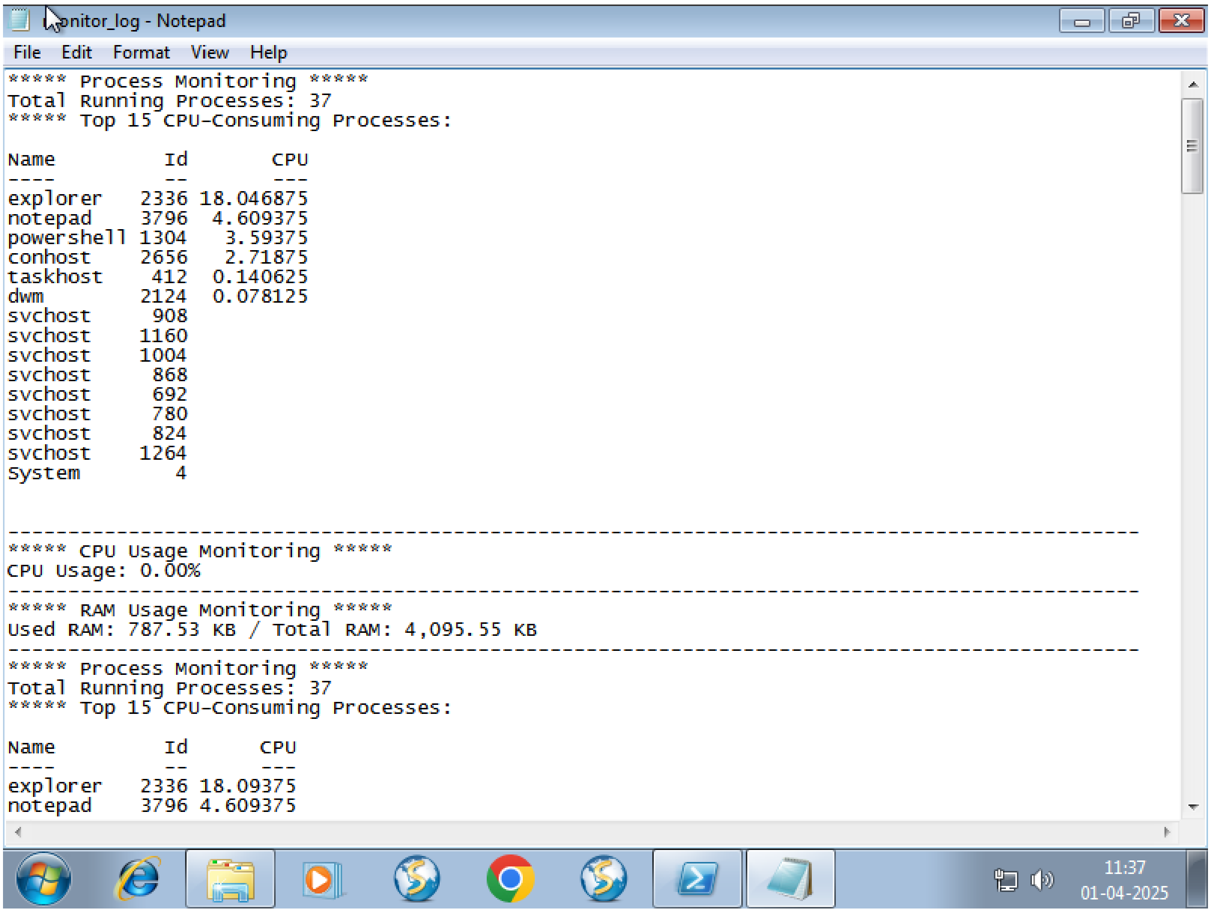
CPU Usage: 0 %

Memory: 785 MB

```
Physical Memory (MB)          System
Total          4095           Handles             11334
Cached          667           Threads               530
Available      3310           Processes              38
Free           2715           Up Time        0:00:35:00
                              Commit (MB)     844 / 8189
Kernel Memory (MB)
Paged            89
Nonpaged         23
```

Processes: 38   CPU Usage: 0%   Physical Memory: 19%

- **Screenshot of the Logfile showing the CPU usage, memory usage and number of processes. when system is idle and no malware has been executed.** (The Logfile displays the output of the PowerShell script that has been executed.)

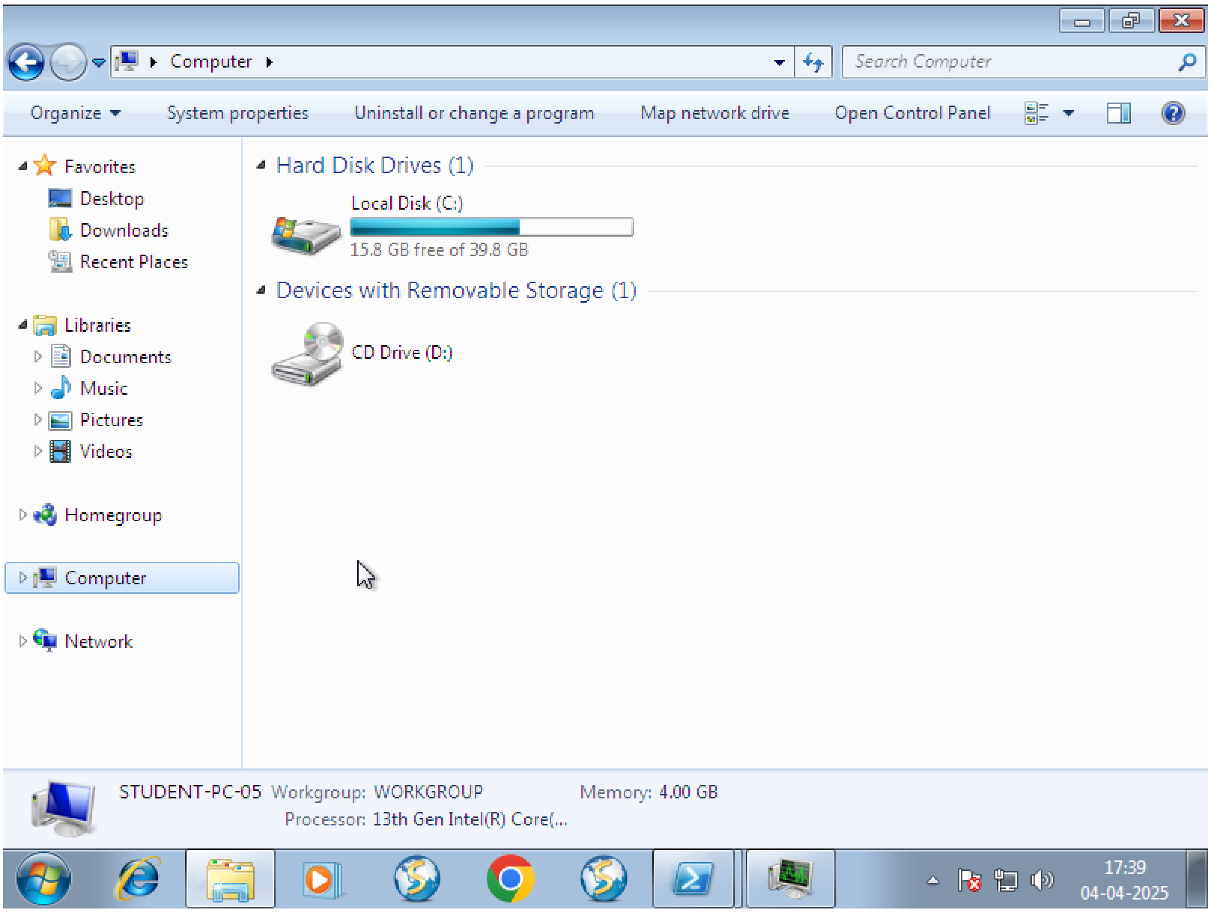


```
***** Process Monitoring *****
Total Running Processes: 37
***** Top 15 CPU-Consuming Processes:

Name          Id       CPU
----          --       ---
explorer    2336 18.046875
notepad     3796  4.609375
powershell  1304   3.59375
conhost     2656   2.71875
taskhost     412  0.140625
dwm         2124  0.078125
svchost      908
svchost     1160
svchost     1004
svchost      868
svchost      692
svchost      780
svchost      824
svchost     1264
System         4


-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 0.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 787.53 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
***** Process Monitoring *****
Total Running Processes: 37
***** Top 15 CPU-Consuming Processes:

Name          Id      CPU
----          --      ---
explorer    2336 18.09375
notepad     3796 4.609375
```

Since, after executing the Malwares, most of them were encrypting all the files inside the system, including the log files too, so I decided to print the output of the script to the PowerShell console. That will be mostly remain unaffected during the Malware execution.

Moreover, I wrote another PowerShell script to detect any real-time changes that is being done to the file system, here particularly, it will monitor the “C:\” drive. That will track the any changes when any Malware tampers the file system.

- **The screenshot of how the File Explorer looks like.**



Local Disk (C:)
15.8 GB free of 39.8 GB

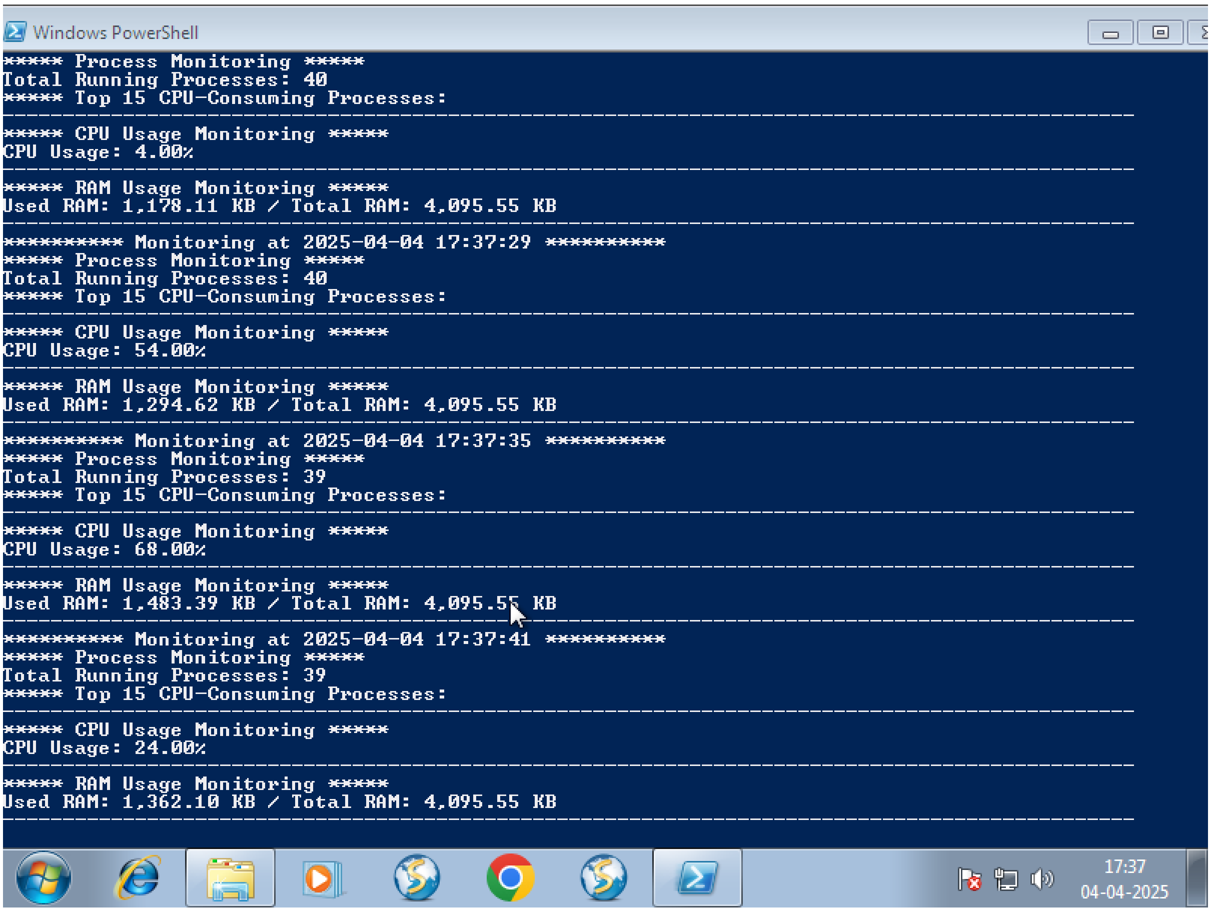
STUDENT-PC-05 Workgroup: WORKGROUP Memory: 4.00 GB
Processor: 13th Gen Intel(R) Core(...

17:39
04-04-2025

- **Malwares which manipulate the number of processes.**

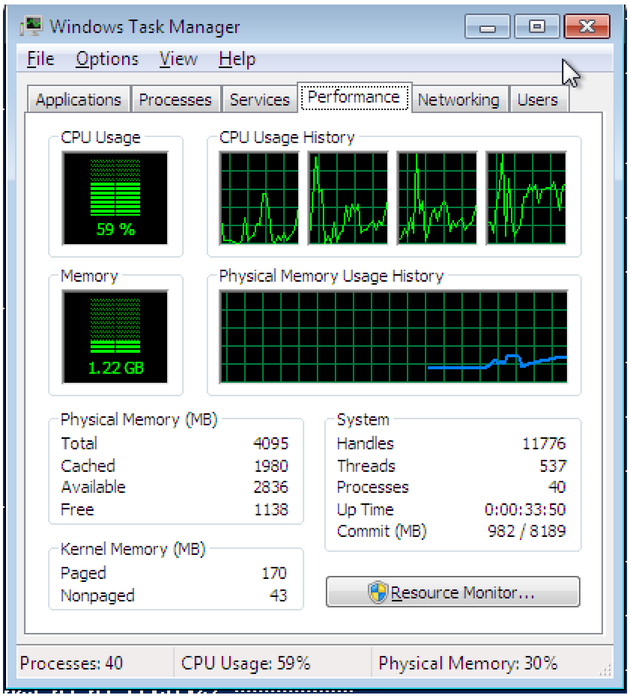
1. WannaCry

After executing the malware, we noticed that the PowerShell console showed a slight increase in number of processes.



```
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 4.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,178.11 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:37:29 ***********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 54.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,294.62 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:37:35 ***********
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 68.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,483.39 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:37:41 ***********
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 24.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,362.10 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
```

We verified this by using the task manager too:



Physical Memory (MB)
Total 4095
Cached 1980
Available 2836
Free 1138

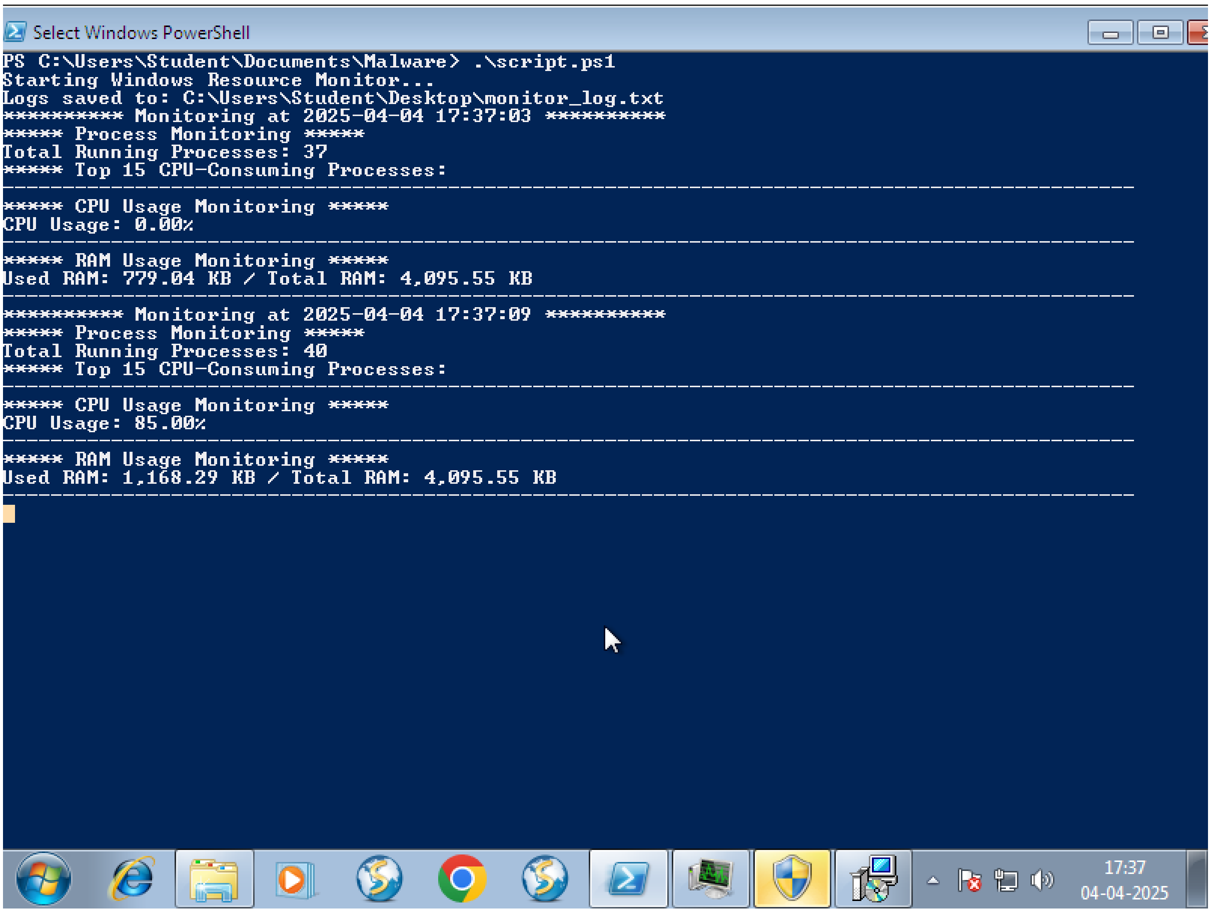
Kernel Memory (MB)
Paged 170
Nonpaged 43

System
Handles 11776
Threads 537
Processes 40
Up Time 0:00:33:50
Commit (MB) 982 / 8189

Processes: 40 CPU Usage: 59% Physical Memory: 30%

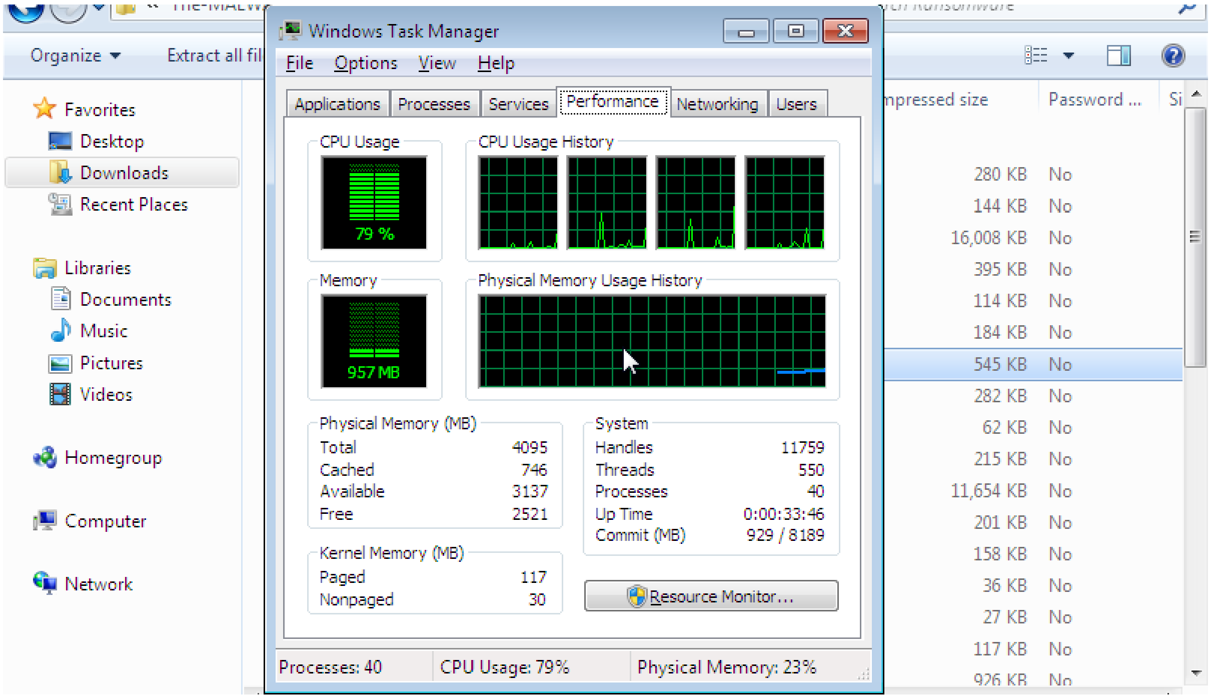
2. CoronaVirus

After executing the malware, we noticed that the PowerShell console showed a slight increase in number of processes.



```
PS C:\Users\Student\Documents\Malware> .\script.ps1
Starting Windows Resource Monitor...
Logs saved to: C:\Users\Student\Desktop\monitor_log.txt
********** Monitoring at 2025-04-04 17:37:03 **********
***** Process Monitoring *****
Total Running Processes: 37
***** Top 15 CPU-Consuming Processes:
----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 0.00%
----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 779.04 KB / Total RAM: 4,095.55 KB
----------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:37:09 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 85.00%
----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,168.29 KB / Total RAM: 4,095.55 KB
----------------------------------------------------------------------------------------------
```

We verified this by using the task manager too:



Physical Memory (MB)
Total 4095
Cached 746
Available 3137
Free 2521

Kernel Memory (MB)
Paged 117
Nonpaged 30

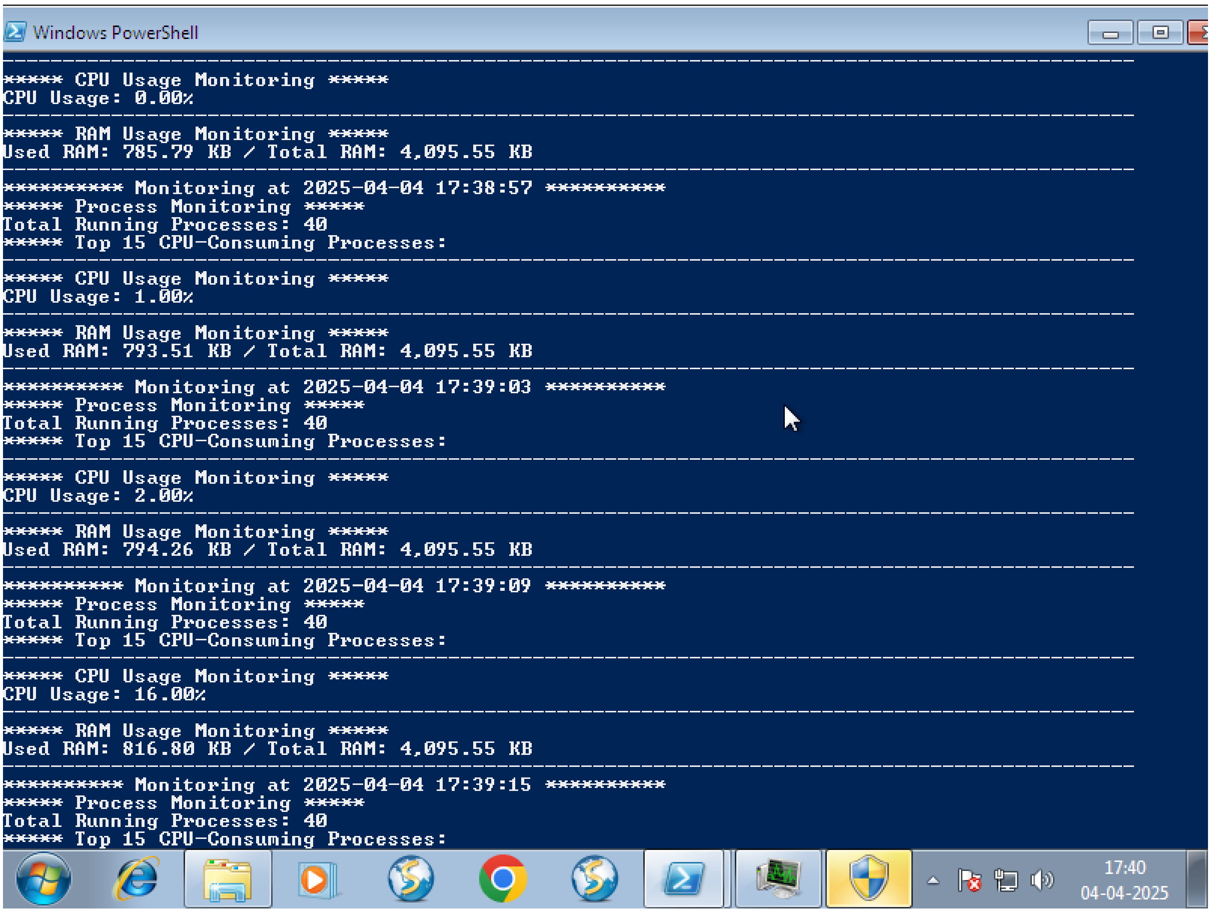
System
Handles 11759
Threads 550
Processes 40
Up Time 0:00:33:46
Commit (MB) 929 / 8189

Processes: 40 CPU Usage: 79% Physical Memory: 23%

mpressed size	Password ...
280 KB	No
144 KB	No
16,008 KB	No
395 KB	No
114 KB	No
184 KB	No
545 KB	No
282 KB	No
62 KB	No
215 KB	No
11,654 KB	No
201 KB	No
158 KB	No
36 KB	No
27 KB	No
117 KB	No
926 KB	No

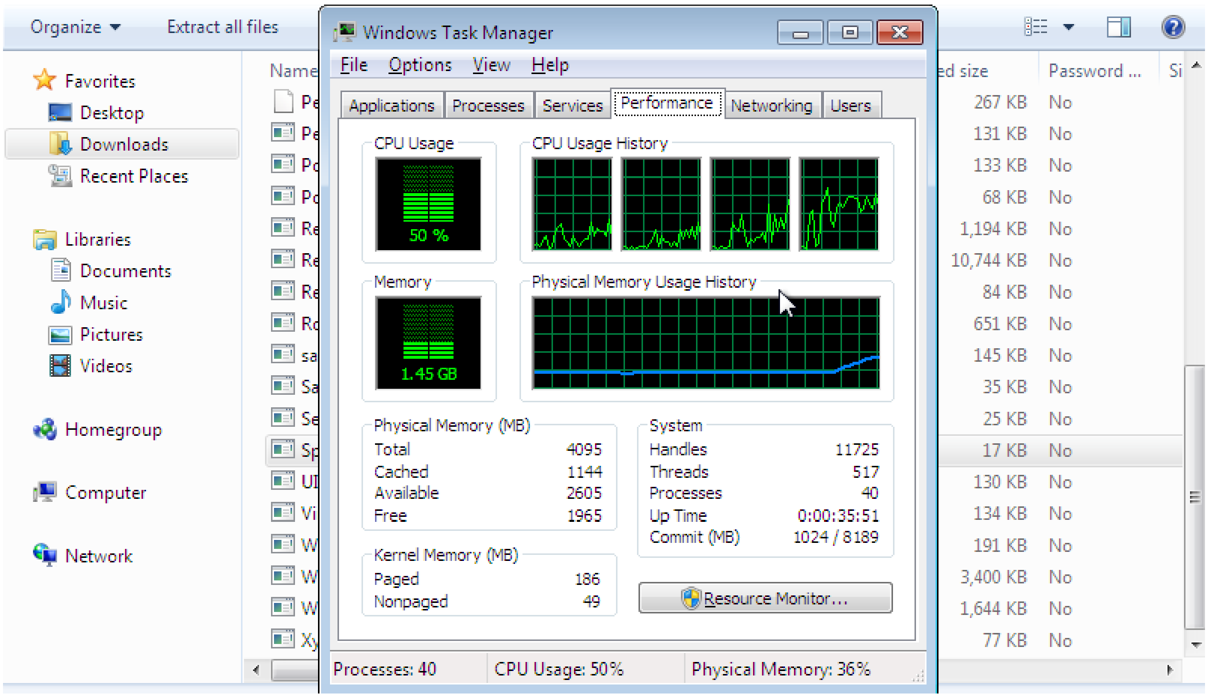
3. SporaRansomware

After executing the malware, we noticed that the PowerShell console showed a slight increase in number of processes.



```
------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 0.00%
------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 785.79 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:38:57 ***********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 1.00%
------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 793.51 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:39:03 ***********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 2.00%
------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 794.26 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:39:09 ***********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 16.00%
------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 816.80 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:39:15 ***********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
```

We verified this by using the task manager too:



267 KB	No
131 KB	No
133 KB	No
68 KB	No
1,194 KB	No
10,744 KB	No
84 KB	No
651 KB	No
145 KB	No
35 KB	No
25 KB	No
17 KB	No
130 KB	No
134 KB	No
191 KB	No
3,400 KB	No
1,644 KB	No
77 KB	No

Physical Memory (MB)
Total 4095
Cached 1144
Available 2605
Free 1965

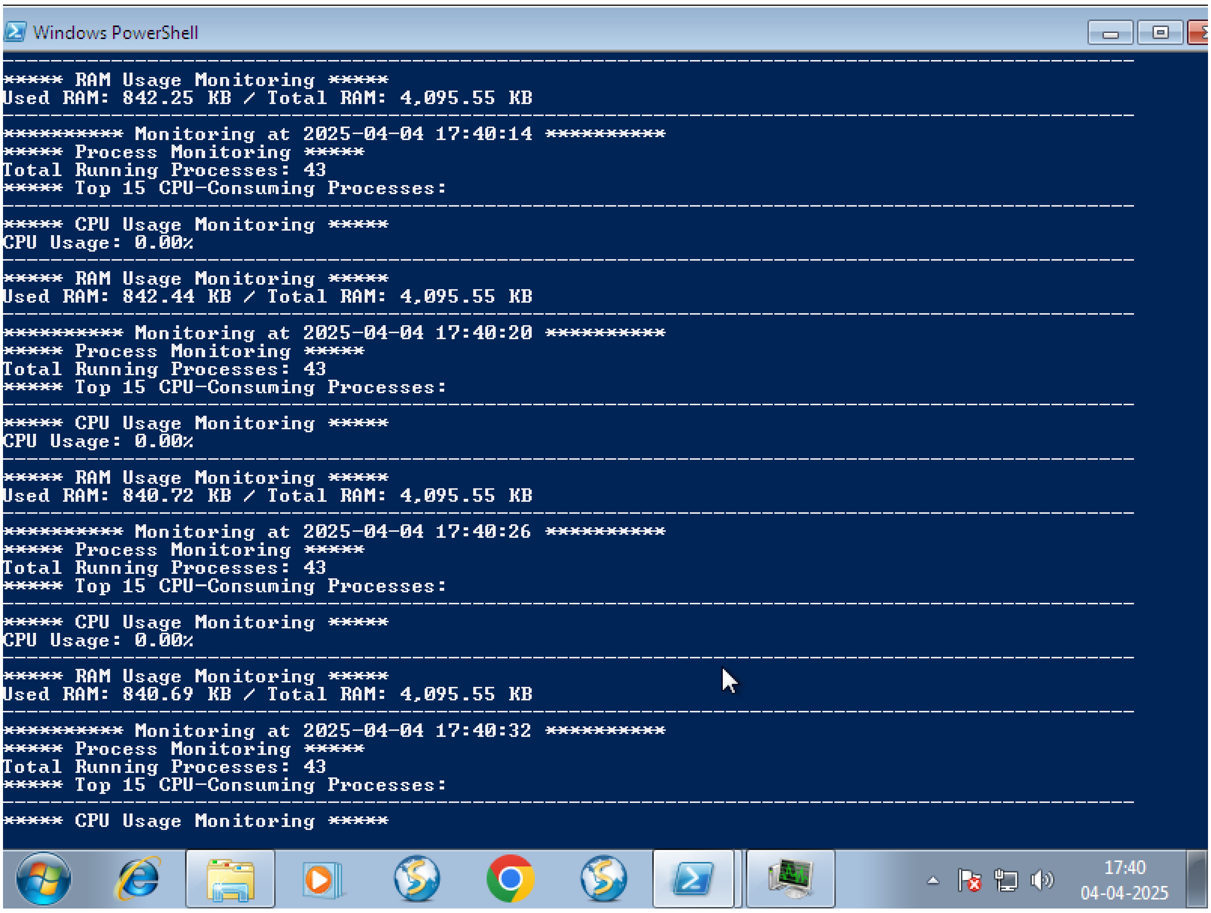
Kernel Memory (MB)
Paged 186
Nonpaged 49

System
Handles 11725
Threads 517
Processes 40
Up Time 0:00:35:51
Commit (MB) 1024 / 8189

Processes: 40   CPU Usage: 50%   Physical Memory: 36%

4. WinlockerVB6Blacksod

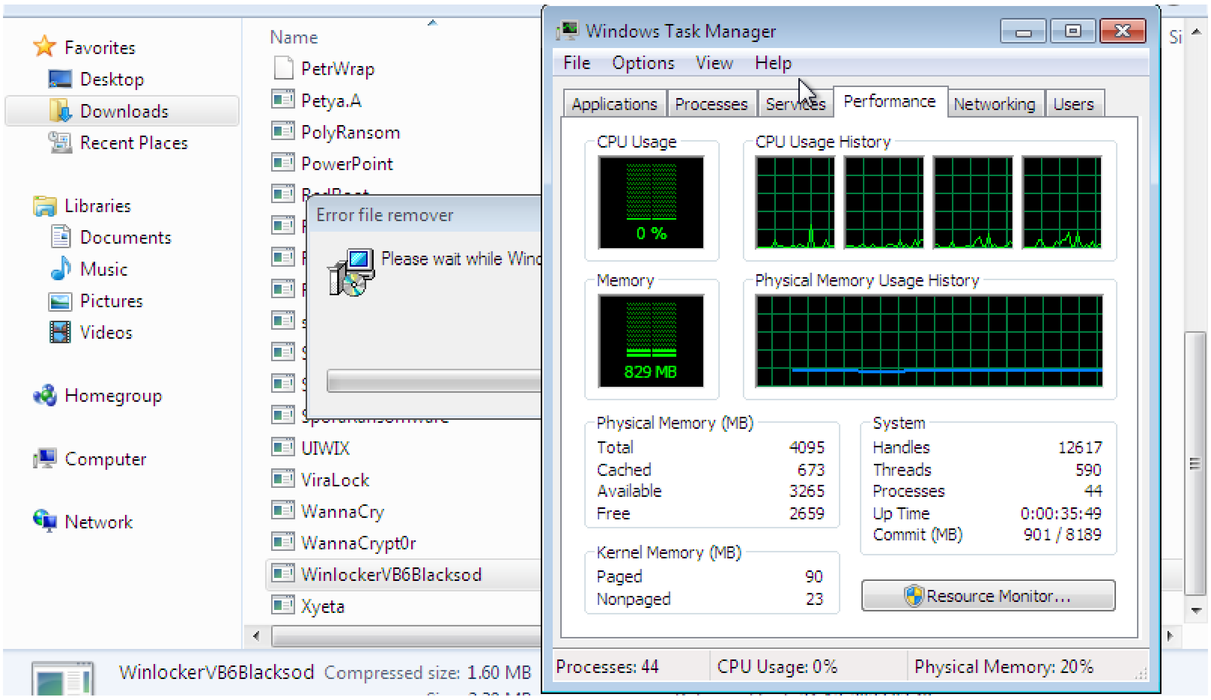
After executing the malware, we noticed that the PowerShell console showed a significant increase in number of processes.



Windows PowerShell

```
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 842.25 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:40:14 ***********
***** Process Monitoring *****
Total Running Processes: 43
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 0.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 842.44 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:40:20 ***********
***** Process Monitoring *****
Total Running Processes: 43
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 0.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 840.72 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:40:26 ***********
***** Process Monitoring *****
Total Running Processes: 43
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 0.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 840.69 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:40:32 ***********
***** Process Monitoring *****
Total Running Processes: 43
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
```

We verified this by using the task manager too:



PetrWrap
Petya.A
PolyRansom
PowerPoint
UIWIX
ViraLock
WannaCry
WannaCrypt0r
WinlockerVB6Blacksod
Xyeta

Error file remover

Please wait while Wind

WinlockerVB6Blacksod Compressed size: 1.60 MB

Windows Task Manager

File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
CPU Usage History
Memory
Physical Memory Usage History
0 %
829 MB
Resource Monitor...

Physical Memory (MB)	
Total	4095
Cached	673
Available	3265
Free	2659

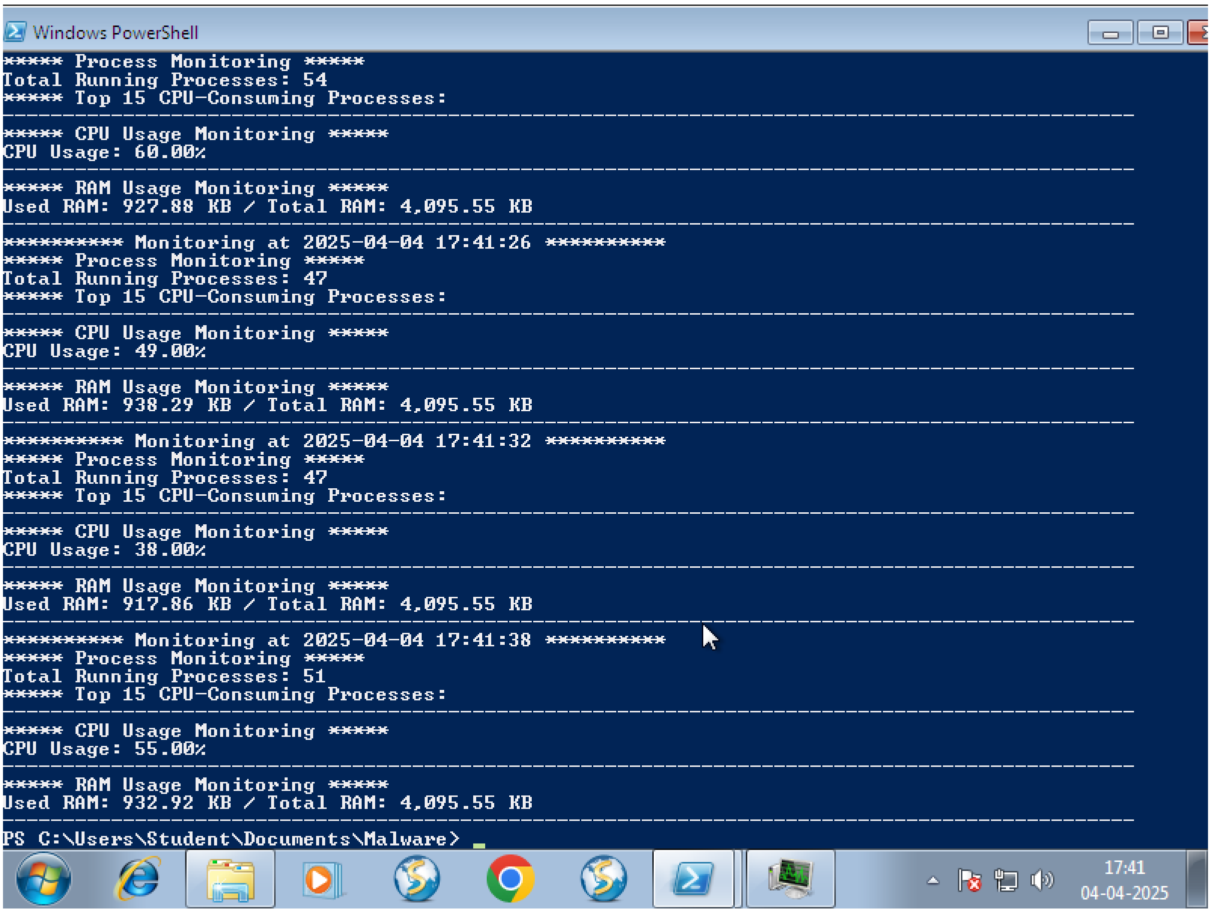
Kernel Memory (MB)	
Paged	90
Nonpaged	23

System	
Handles	12617
Threads	590
Processes	44
Up Time	0:00:35:49
Commit (MB)	901 / 8189

Processes: 44 CPU Usage: 0% Physical Memory: 20%

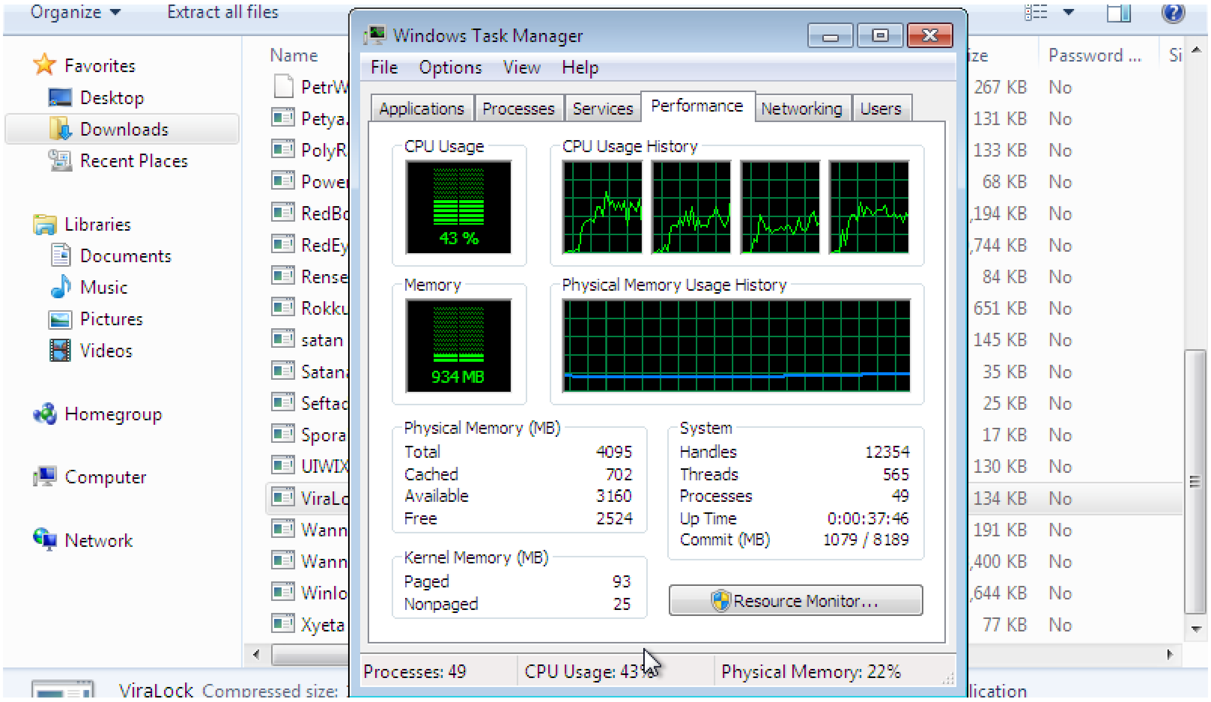
5. ViraLock

After executing the malware, we noticed that the PowerShell console showed a significant increase in number of processes.



```
***** Process Monitoring *****
Total Running Processes: 54
***** Top 15 CPU-Consuming Processes:
---------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 60.00%
---------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 927.88 KB / Total RAM: 4,095.55 KB
---------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:41:26 ***********
***** Process Monitoring *****
Total Running Processes: 47
***** Top 15 CPU-Consuming Processes:
---------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 49.00%
---------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 938.29 KB / Total RAM: 4,095.55 KB
---------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:41:32 ***********
***** Process Monitoring *****
Total Running Processes: 47
***** Top 15 CPU-Consuming Processes:
---------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 38.00%
---------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 917.86 KB / Total RAM: 4,095.55 KB
---------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:41:38 ***********
***** Process Monitoring *****
Total Running Processes: 51
***** Top 15 CPU-Consuming Processes:
---------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 55.00%
---------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 932.92 KB / Total RAM: 4,095.55 KB
---------------------------------------------------------------------------------------------
PS C:\Users\Student\Documents\Malware> _
```

We verified this by using the task manager too:



Name	ize	Password ...	Si
PetrW	267 KB	No	
Petya.	131 KB	No	
PolyR	133 KB	No	
Powe	68 KB	No	
RedBo	,194 KB	No	
RedEy	,744 KB	No	
Rense	84 KB	No	
Rokku	651 KB	No	
satan	145 KB	No	
Satan	35 KB	No	
Seftad	25 KB	No	
Spora	17 KB	No	
UIWIX	130 KB	No	
ViraLo	134 KB	No	
Wann	191 KB	No	
Wann	,400 KB	No	
Winlo	,644 KB	No	
Xyeta	77 KB	No	

Physical Memory (MB)
Total 4095
Cached 702
Available 3160
Free 2524

Kernel Memory (MB)
Paged 93
Nonpaged 25

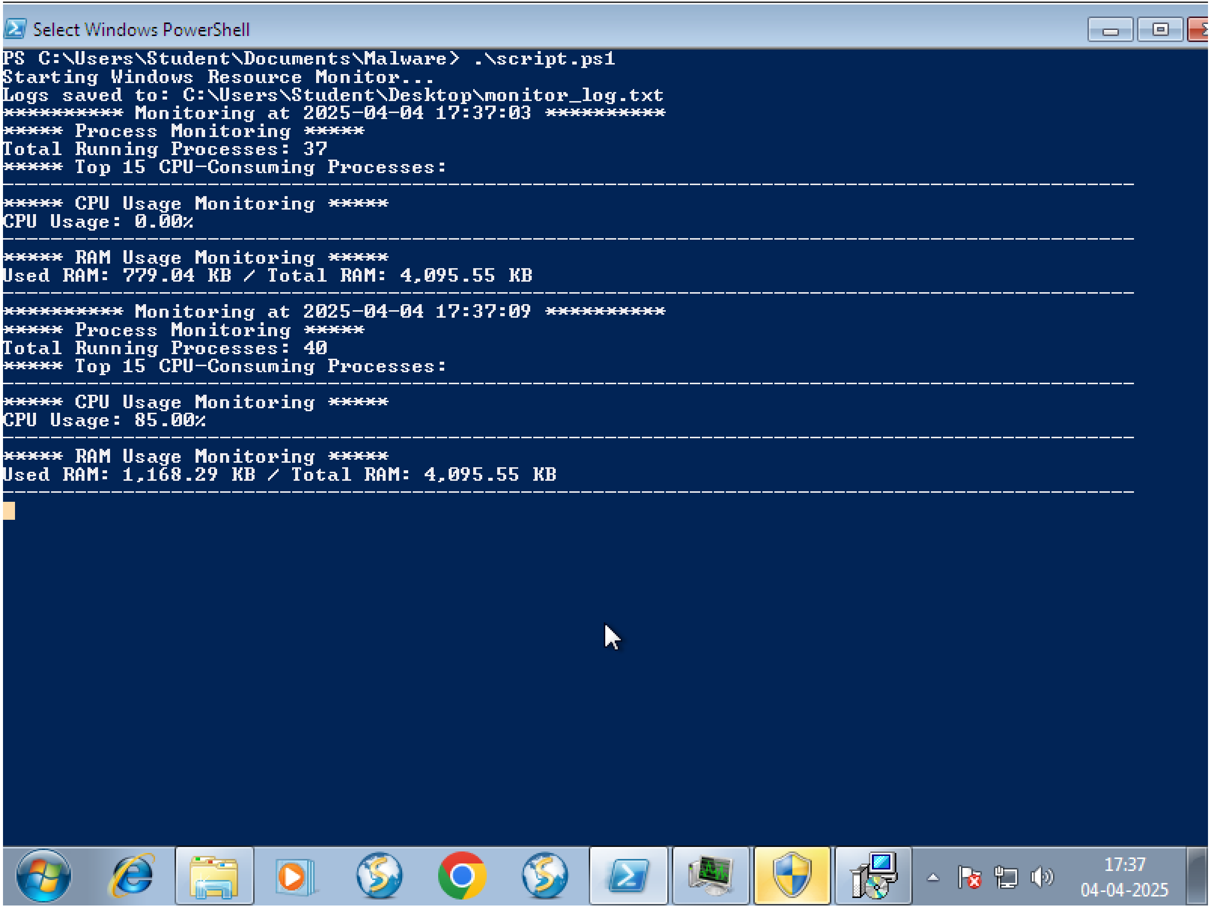
System
Handles 12354
Threads 565
Processes 49
Up Time 0:00:37:46
Commit (MB) 1079 / 8189

Processes: 49 CPU Usage: 43% Physical Memory: 22%

- **Malwares which manipulate the CPU usage.**

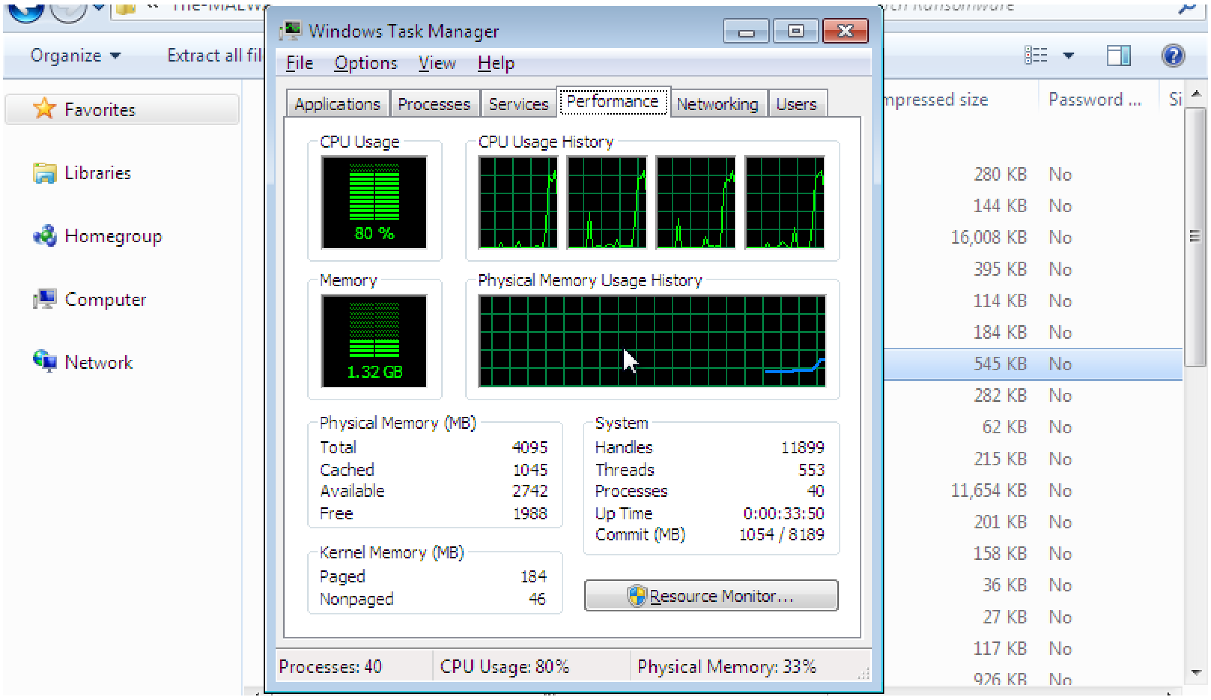
1. **CoronaVirus**

After executing the malware, we noticed that the PowerShell console showed a high spike in CPU Usage.



```
PS C:\Users\Student\Documents\Malware> .\script.ps1
Starting Windows Resource Monitor...
Logs saved to: C:\Users\Student\Desktop\monitor_log.txt
********** Monitoring at 2025-04-04 17:37:03 **********
***** Process Monitoring *****
Total Running Processes: 37
***** Top 15 CPU-Consuming Processes:
----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 0.00%
----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 779.04 KB / Total RAM: 4,095.55 KB
----------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:37:09 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 85.00%
----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,168.29 KB / Total RAM: 4,095.55 KB
----------------------------------------------------------------------------------------------
```

We verified this by using the task manager too:



CPU Usage: 80 %

Memory: 1.32 GB

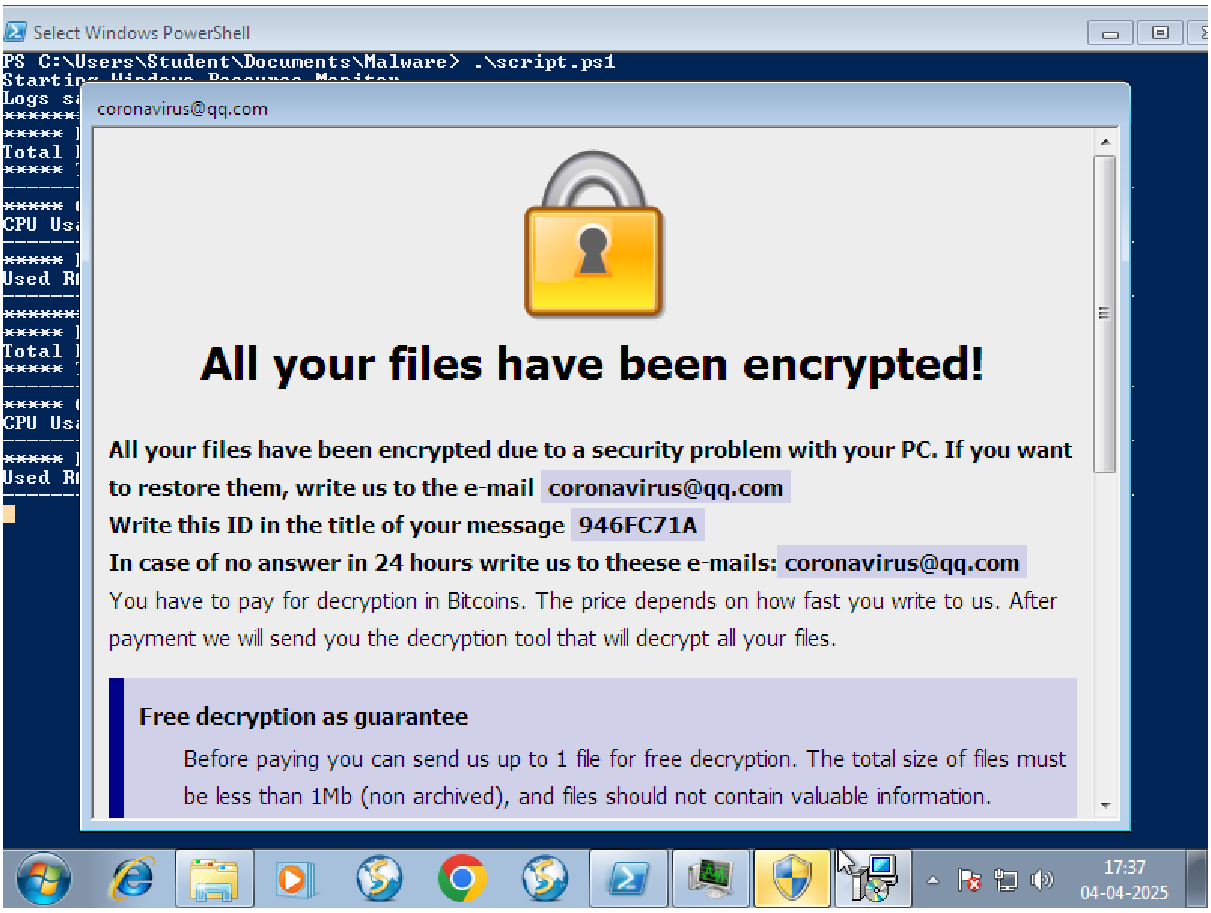
Physical Memory (MB)	
Total	4095
Cached	1045
Available	2742
Free	1988

System	
Handles	11899
Threads	553
Processes	40
Up Time	0:00:33:50
Commit (MB)	1054 / 8189

Kernel Memory (MB)	
Paged	184
Nonpaged	46

Processes: 40 CPU Usage: 80% Physical Memory: 33%

Then a dialogue box containing a message showed like this.



```
PS C:\Users\Student\Documents\Malware> .\script.ps1
Starting Windows Resource Monitor
Logs s
*******
***** ]
Total ]
***** ]
-------
***** (
CPU Us
-------
***** ]
Used R
-------
*******
***** ]
Total ]
***** ]
-------
***** (
CPU Us
-------
***** ]
Used R
-------
```

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail coronavirus@qq.com

Write this ID in the title of your message 946FC71A

In case of no answer in 24 hours write us to theese e-mails: coronavirus@qq.com

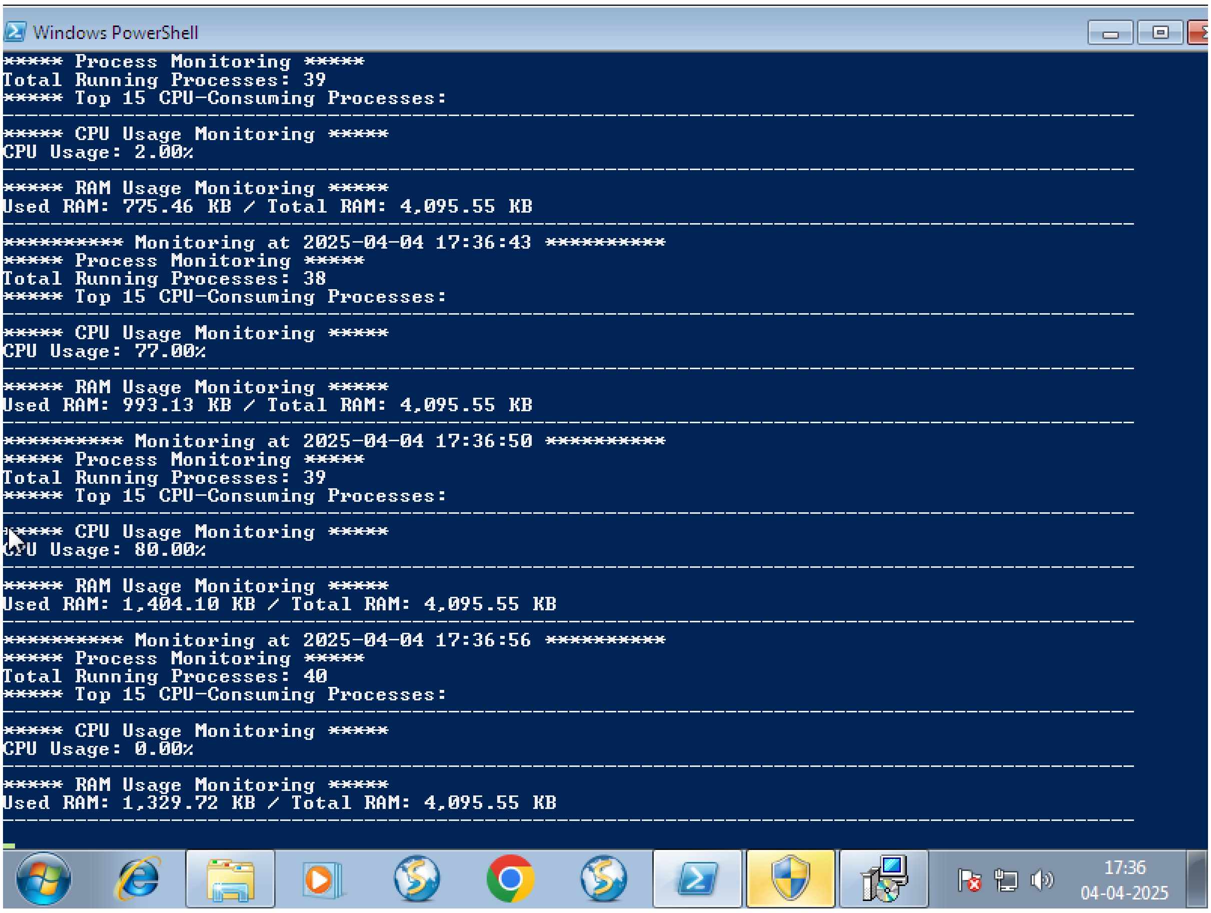
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information.

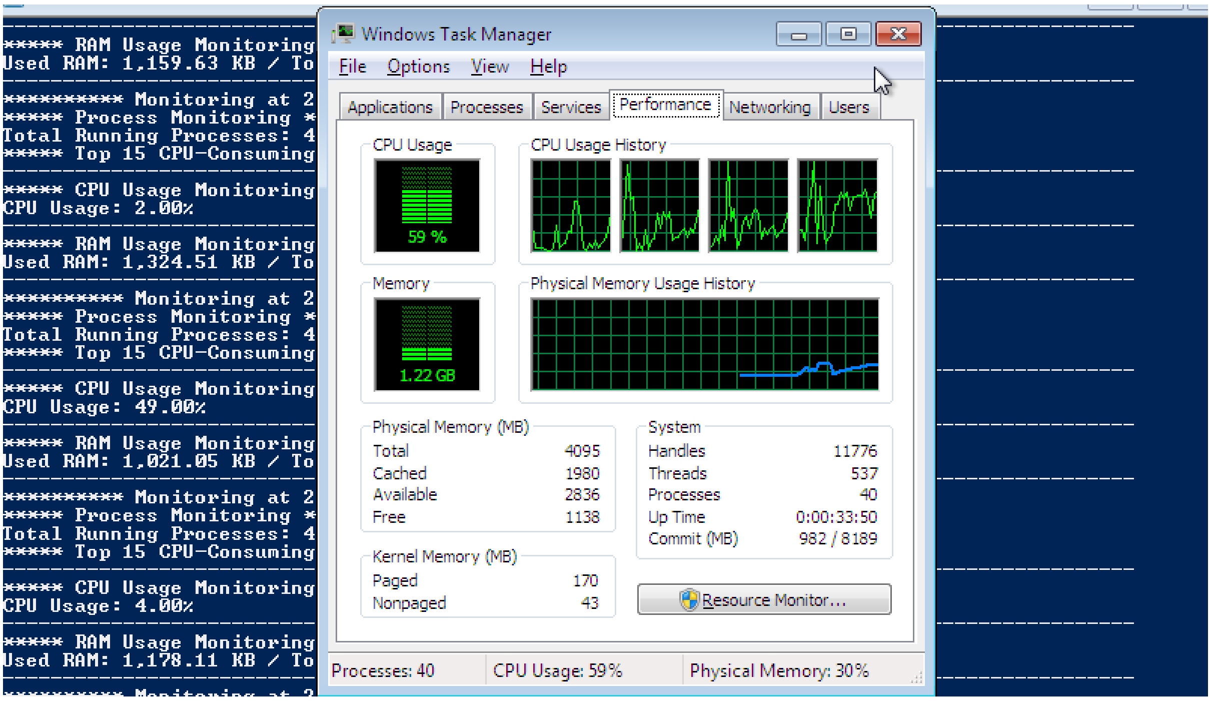
2. WannaCry

After executing the malware, we noticed that the PowerShell console showed a high spike in CPU Usage.



```
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 2.00%
----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 775.46 KB / Total RAM: 4,095.55 KB
----------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:36:43 ***********
***** Process Monitoring *****
Total Running Processes: 38
***** Top 15 CPU-Consuming Processes:
----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 77.00%
----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 993.13 KB / Total RAM: 4,095.55 KB
----------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:36:50 ***********
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 80.00%
----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,404.10 KB / Total RAM: 4,095.55 KB
----------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:36:56 ***********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 0.00%
----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,329.72 KB / Total RAM: 4,095.55 KB
----------------------------------------------------------------------------------------------
```

We verified this by using the task manager too:


```
***** RAM Usage Monitoring
Used RAM: 1,159.63 KB / To
*********** Monitoring at 2
***** Process Monitoring *
Total Running Processes: 4
***** Top 15 CPU-Consuming
***** CPU Usage Monitoring
CPU Usage: 2.00%
***** RAM Usage Monitoring
Used RAM: 1,324.51 KB / To
*********** Monitoring at 2
***** Process Monitoring *
Total Running Processes: 4
***** Top 15 CPU-Consuming
***** CPU Usage Monitoring
CPU Usage: 49.00%
***** RAM Usage Monitoring
Used RAM: 1,021.05 KB / To
*********** Monitoring at 2
***** Process Monitoring *
Total Running Processes: 4
***** Top 15 CPU-Consuming
***** CPU Usage Monitoring
CPU Usage: 4.00%
***** RAM Usage Monitoring
Used RAM: 1,178.11 KB / To
*********** Monitoring at 2
```

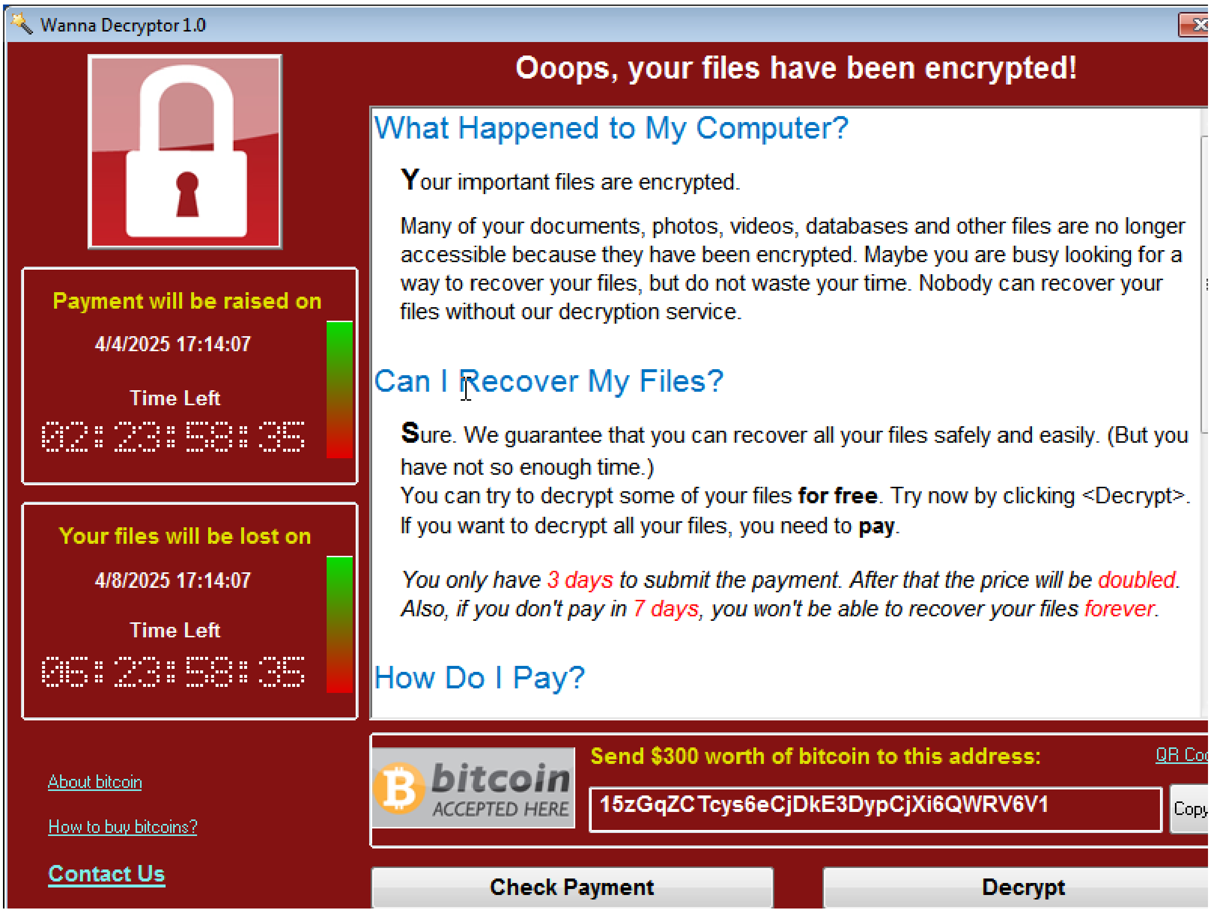
Physical Memory (MB)
Total 4095
Cached 1980
Available 2836
Free 1138

Kernel Memory (MB)
Paged 170
Nonpaged 43

System
Handles 11776
Threads 537
Processes 40
Up Time 0:00:33:50
Commit (MB) 982 / 8189

Processes: 40 CPU Usage: 59% Physical Memory: 30%

Then a window containing a message showed like this.



Ooops, your files have been encrypted!

Payment will be raised on

4/4/2025 17:14:07

Time Left

02:23:58:35

Your files will be lost on

4/8/2025 17:14:07

Time Left

06:23:58:35

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

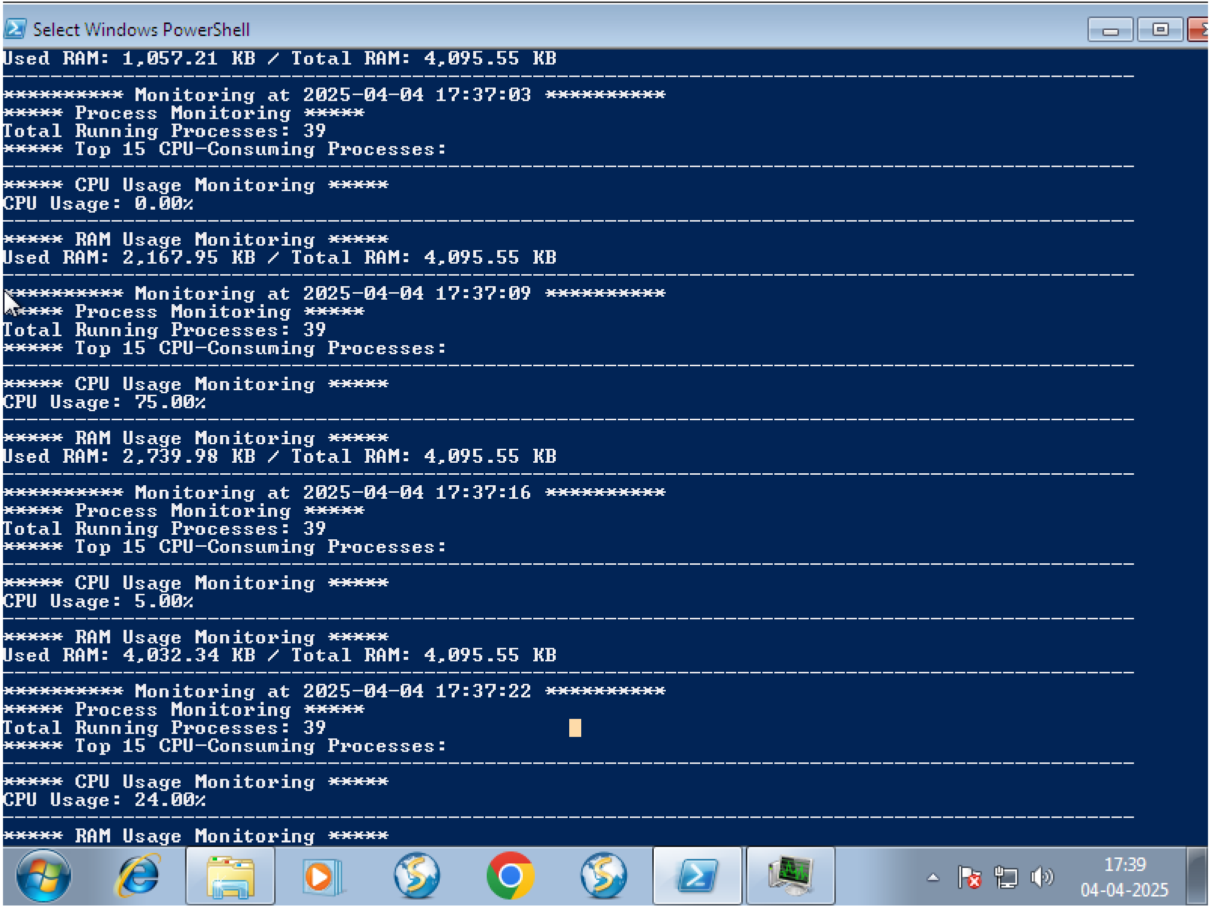
How Do I Pay?

Send $300 worth of bitcoin to this address:

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

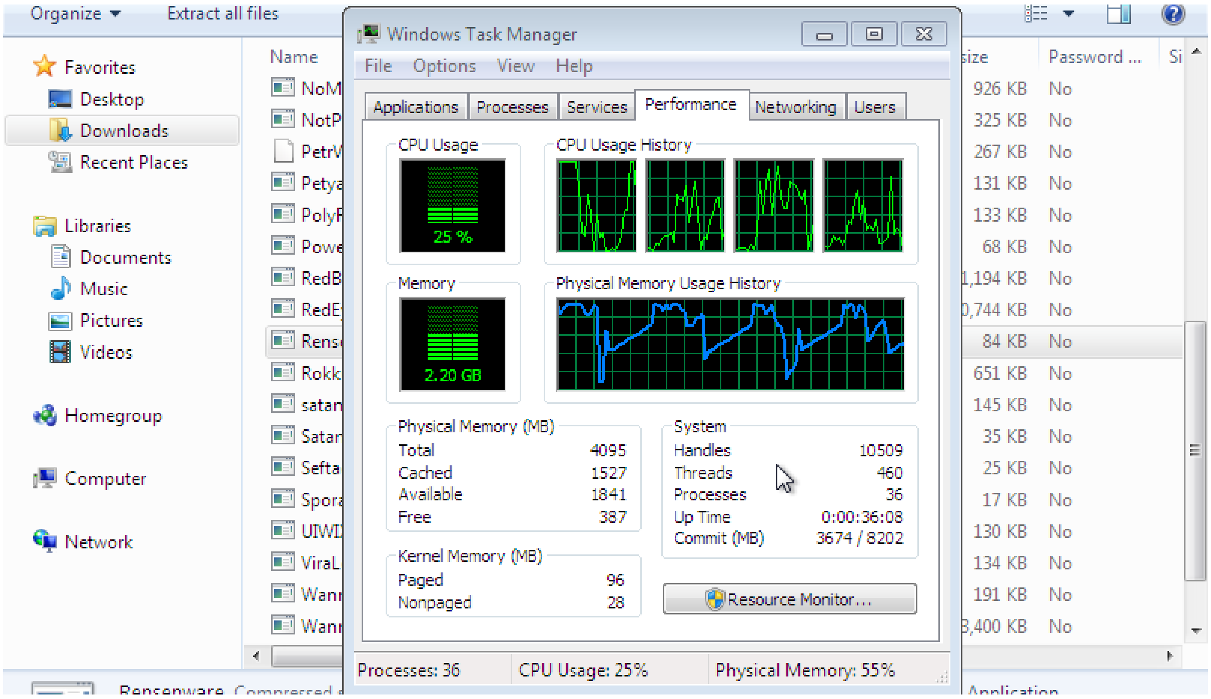
3. Rensenware

After executing the malware, we noticed that the PowerShell console showed a high spike in CPU Usage.



```
Used RAM: 1,057.21 KB / Total RAM: 4,095.55 KB
--------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:37:03 ***********
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
--------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 0.00%
--------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 2,167.95 KB / Total RAM: 4,095.55 KB
--------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:37:09 ***********
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
--------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 75.00%
--------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 2,739.98 KB / Total RAM: 4,095.55 KB
--------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:37:16 ***********
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
--------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 5.00%
--------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 4,032.34 KB / Total RAM: 4,095.55 KB
--------------------------------------------------------------------------------------------
*********** Monitoring at 2025-04-04 17:37:22 ***********
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
--------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 24.00%
--------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
```

We verified this by using the task manager too:



Name	ize	Password ...
NoM	926 KB	No
NotP	325 KB	No
PetrW	267 KB	No
Petya	131 KB	No
PolyF	133 KB	No
Powe	68 KB	No
RedB	1,194 KB	No
RedE	0,744 KB	No
Rens	84 KB	No
Rokk	651 KB	No
satan	145 KB	No
Satar	35 KB	No
Sefta	25 KB	No
Spora	17 KB	No
UIWI	130 KB	No
ViraL	134 KB	No
Wanr	191 KB	No
Wanr	3,400 KB	No

Physical Memory (MB)
Total 4095
Cached 1527
Available 1841
Free 387

Kernel Memory (MB)
Paged 96
Nonpaged 28

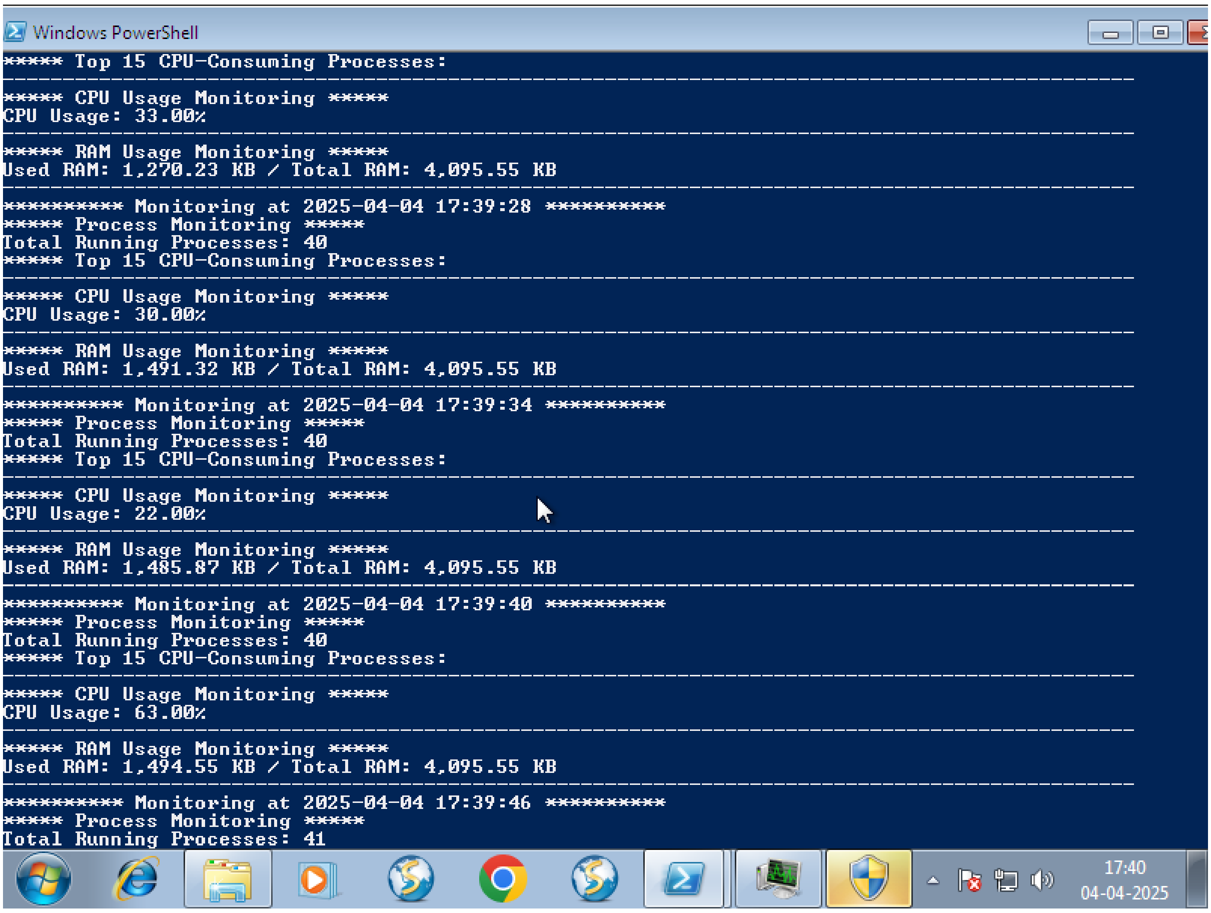
System
Handles 10509
Threads 460
Processes 36
Up Time 0:00:36:08
Commit (MB) 3674 / 8202

Processes: 36 CPU Usage: 25% Physical Memory: 55%

Rensenware Compressed ... Application

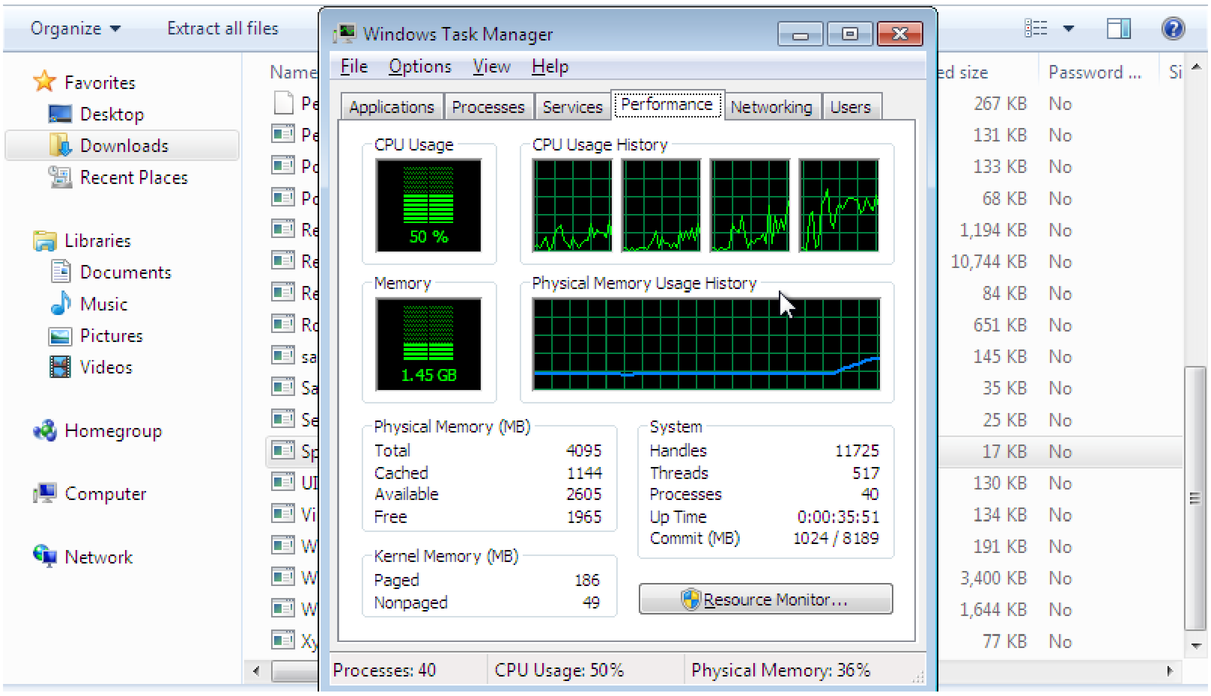
4. SporaRansomware

After executing the malware, we noticed that the PowerShell console showed a high spike in CPU Usage.



```
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 33.00%
------------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,270.23 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:28 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 30.00%
------------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,491.32 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:34 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 22.00%
------------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,485.87 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:40 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 63.00%
------------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,494.55 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:46 **********
***** Process Monitoring *****
Total Running Processes: 41
```

We verified this by using the task manager too:



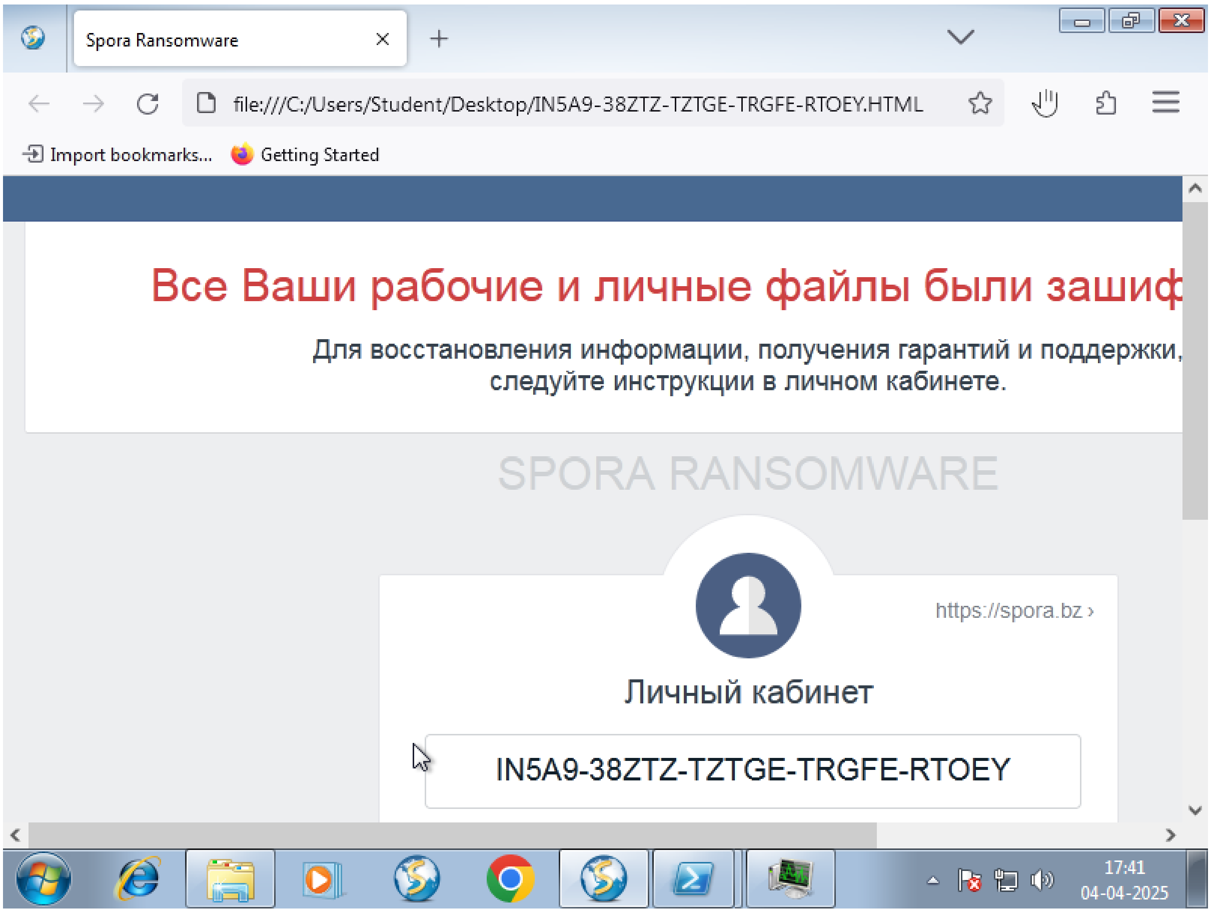
Physical Memory (MB)	
Total	4095
Cached	1144
Available	2605
Free	1965

Kernel Memory (MB)	
Paged	186
Nonpaged	49

System	
Handles	11725
Threads	517
Processes	40
Up Time	0:00:35:51
Commit (MB)	1024 / 8189

Processes: 40 CPU Usage: 50% Physical Memory: 36%

A window showed up which looked like this.



Spora Ransomware
file:///C:/Users/Student/Desktop/IN5A9-38ZTZ-TZTGE-TRGFE-RTOEY.HTML
Import bookmarks...
Getting Started

Все Ваши рабочие и личные файлы были зашиф

Для восстановления информации, получения гарантий и поддержки, следуйте инструкции в личном кабинете.

SPORA RANSOMWARE

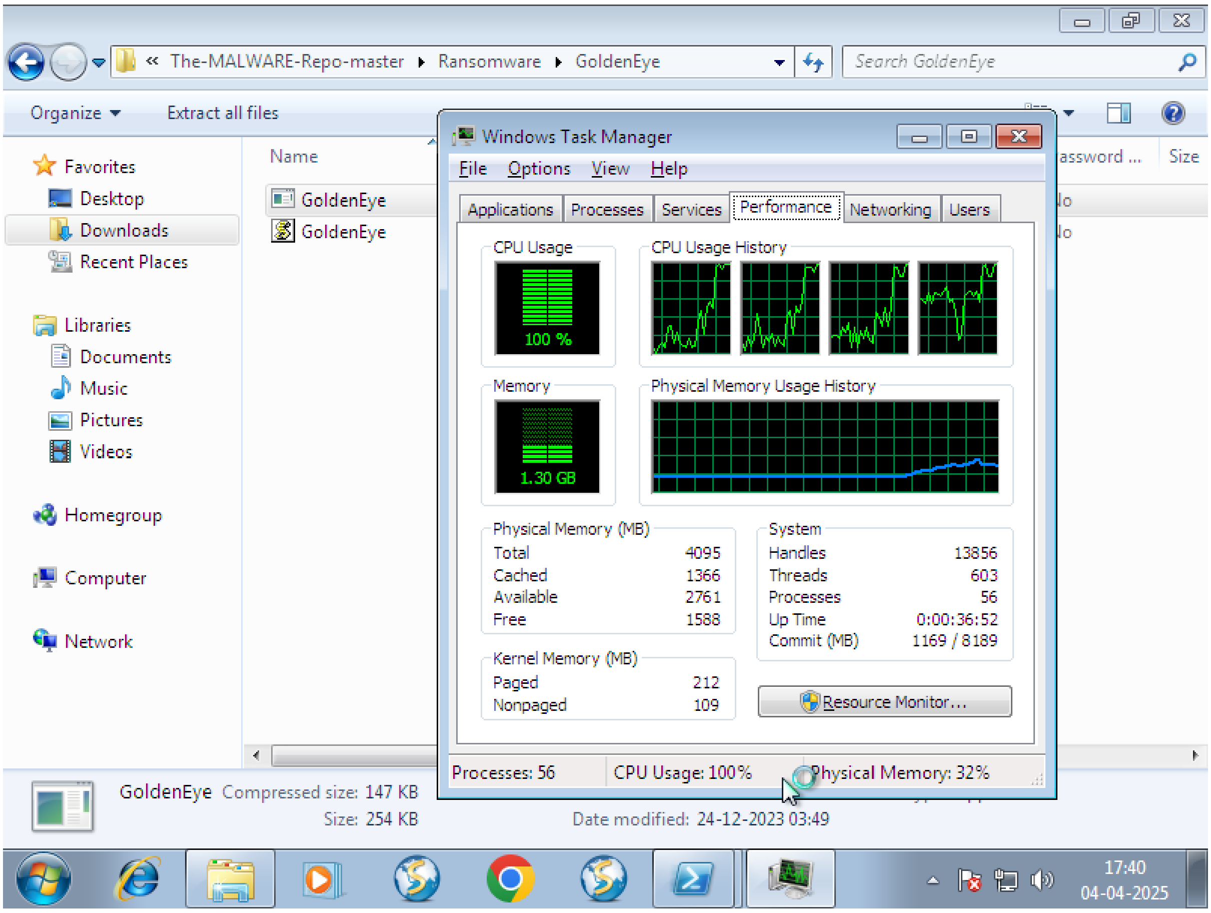
https://spora.bz ›

Личный кабинет

IN5A9-38ZTZ-TZTGE-TRGFE-RTOEY

5. GoldenEye

After executing the malware, we noticed that the Task manager showed a spike in CPU usage.



Physical Memory (MB)

Total	4095
Cached	1366
Available	2761
Free	1588

Kernel Memory (MB)

Paged	212
Nonpaged	109

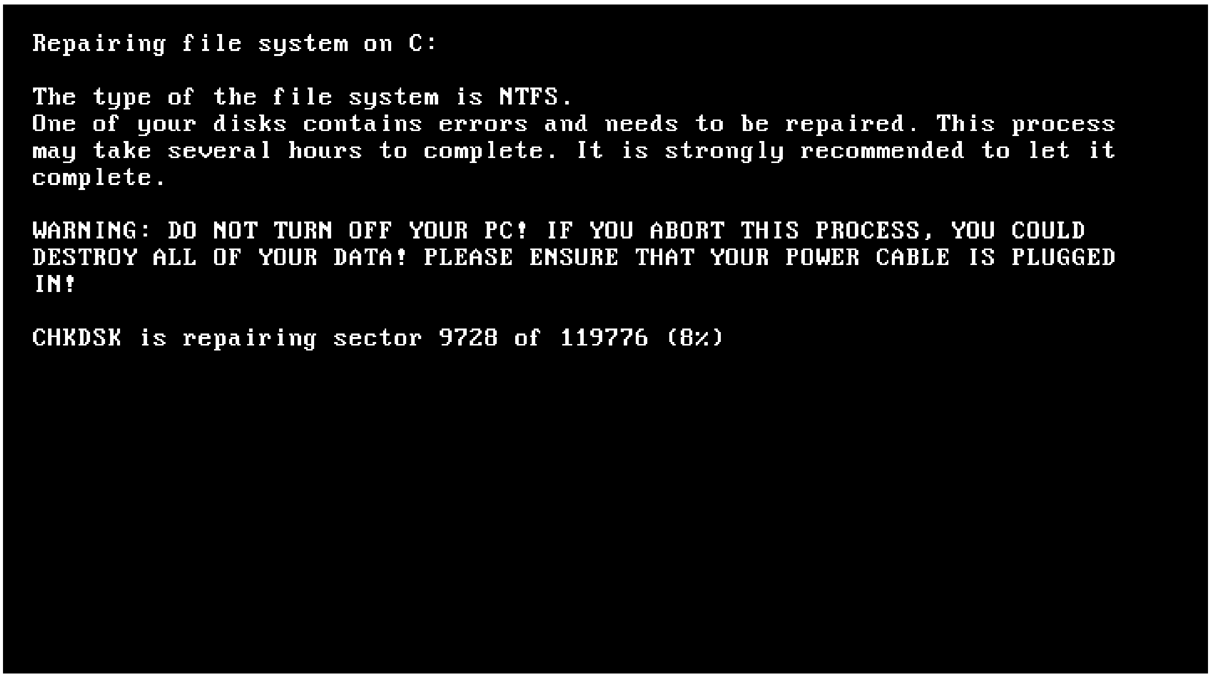
System

Handles	13856
Threads	603
Processes	56
Up Time	0:00:36:52
Commit (MB)	1169 / 8189

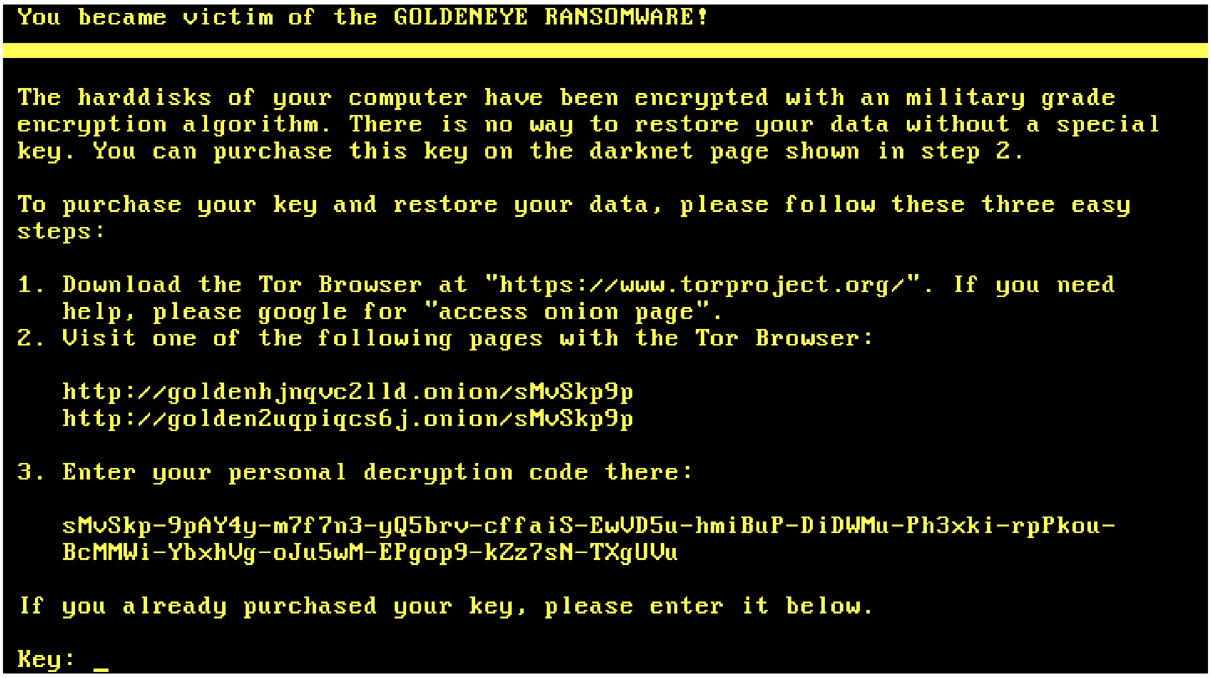
Processes: 56 CPU Usage: 100% Physical Memory: 32%

GoldenEye Compressed size: 147 KB Date modified: 24-12-2023 03:49
Size: 254 KB

Unfortunately, we couldn’t see this using the PowerShell console because the system immediately got shut down and the following message appeared on the screen:



```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 9728 of 119776 (8%)
```

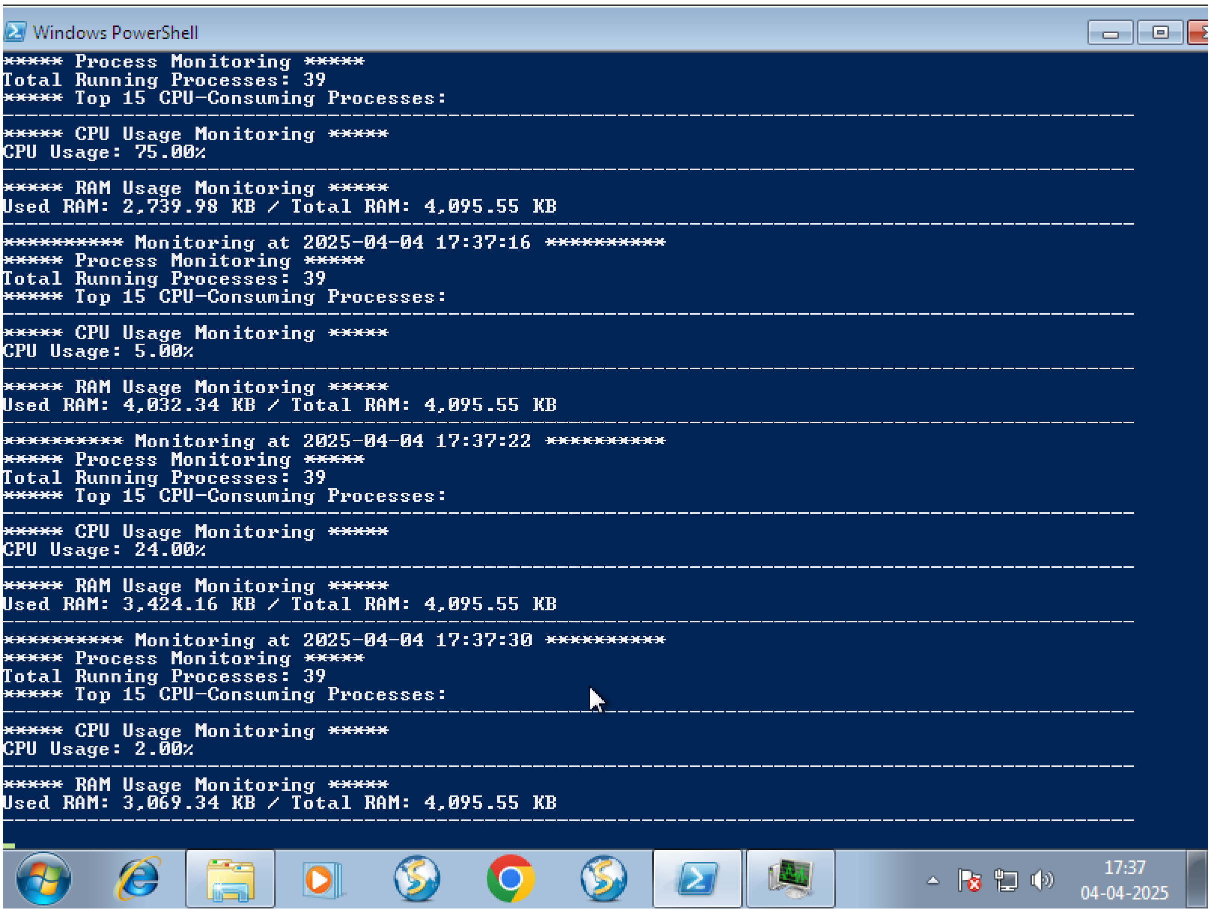


```
You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://goldenhjnqvc2lld.onion/sMvSkp9p
   http://golden2uqpiqcs6j.onion/sMvSkp9p

3. Enter your personal decryption code there:

   sMvSkp-9pAY4y-m7f7n3-yQ5brv-cffaiS-EwVD5u-hmiBuP-DiDWMu-Ph3xki-rpPkou-
   BcMMWi-YbxhVg-oJu5wM-EPgop9-kZz7sN-TXgUVu

If you already purchased your key, please enter it below.

Key: _
```

- **Malwares which manipulate the memory usage.**

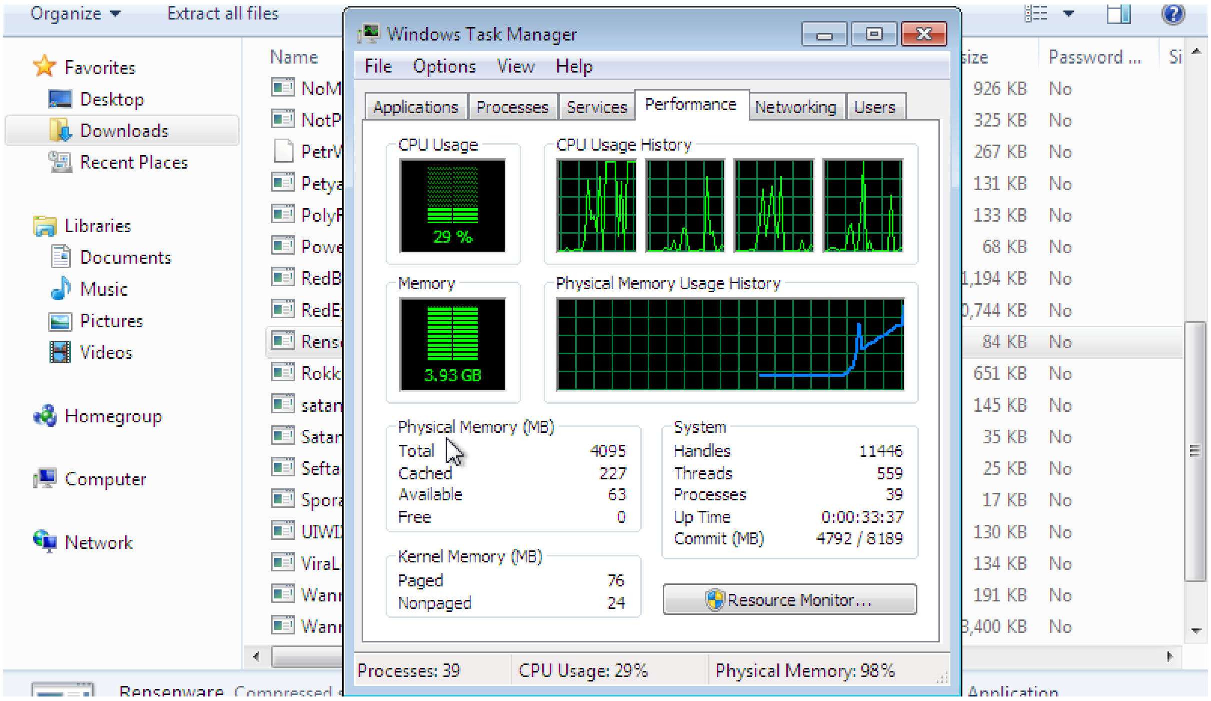
1. Rensenware

After executing the malware, we noticed that the PowerShell console showed a high spike in memory usage.



```
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 75.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 2,739.98 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:37:16 **********
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 5.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 4,032.34 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:37:22 **********
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 24.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 3,424.16 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:37:30 **********
***** Process Monitoring *****
Total Running Processes: 39
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 2.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 3,069.34 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
```

We verified this by using the task manager too:



Physical Memory (MB)
Total 4095
Cached 227
Available 63
Free 0

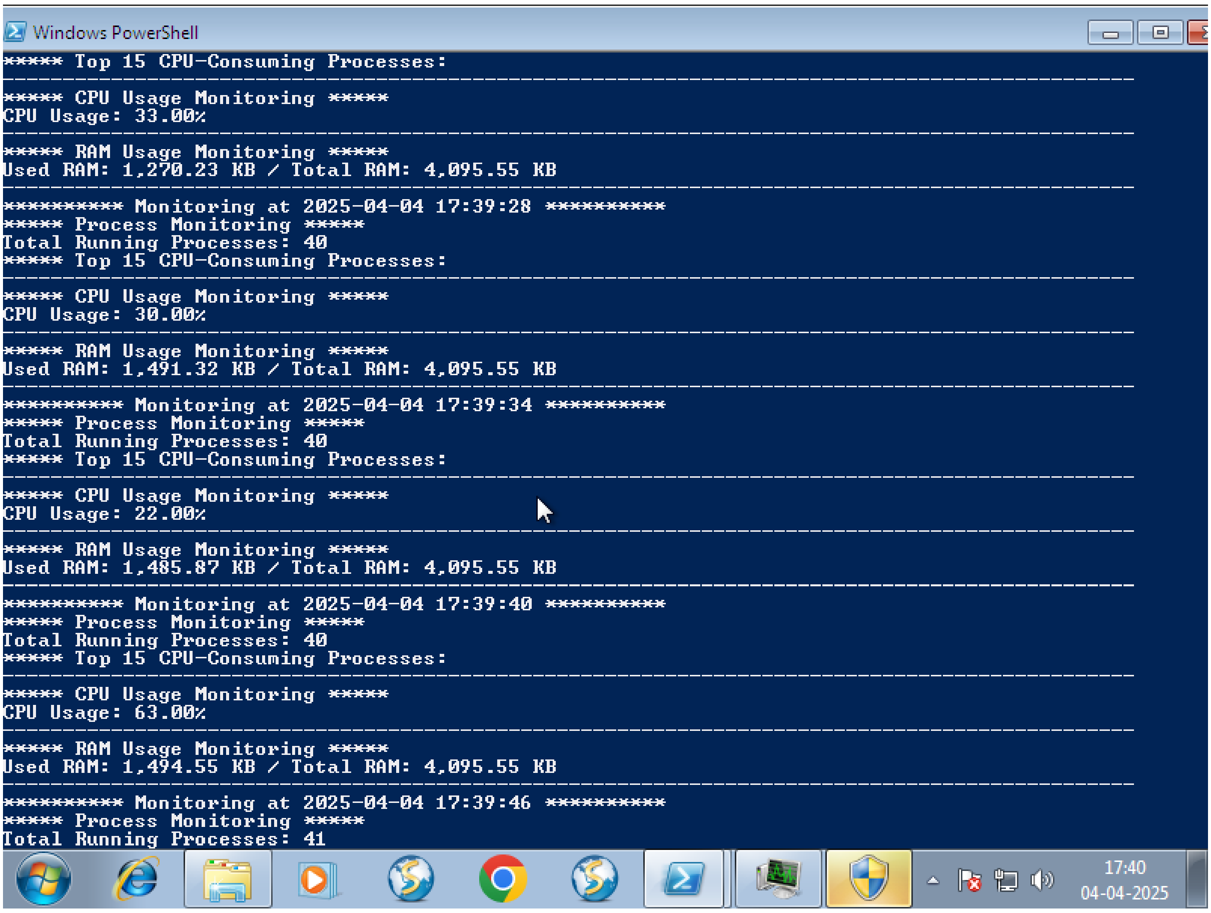
System
Handles 11446
Threads 559
Processes 39
Up Time 0:00:33:37
Commit (MB) 4792 / 8189

Kernel Memory (MB)
Paged 76
Nonpaged 24

Processes: 39 CPU Usage: 29% Physical Memory: 98%

2. SporaRansomware

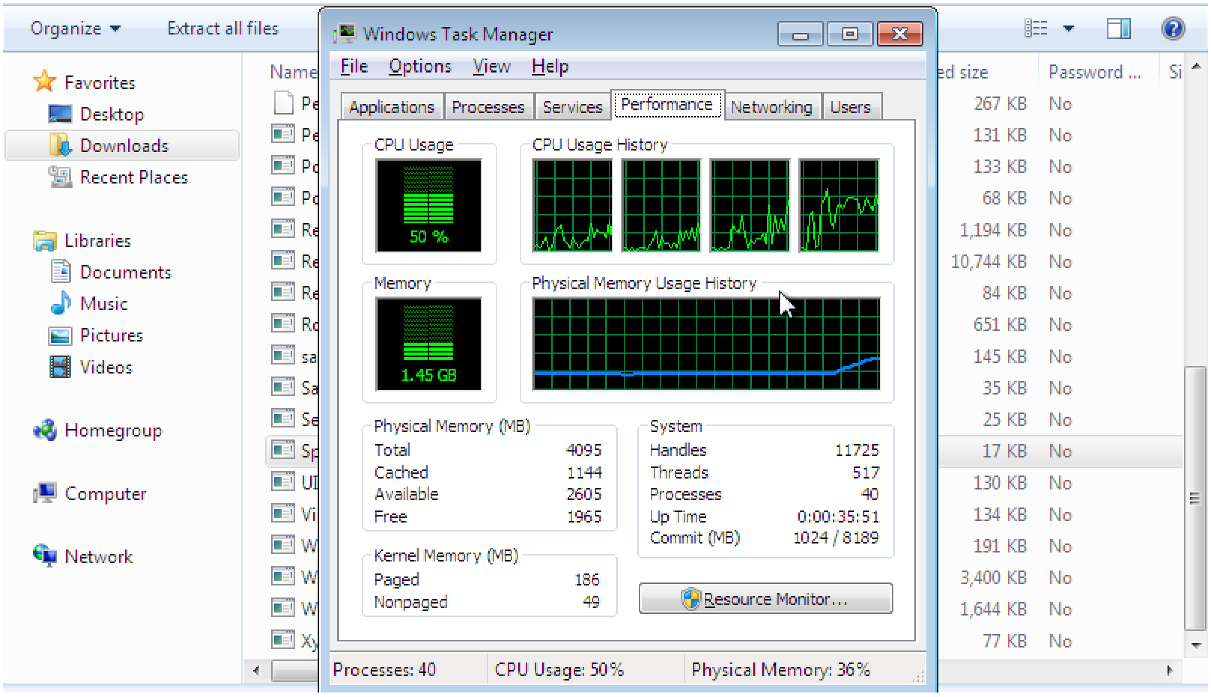
After executing the malware, we noticed that the PowerShell console showed a high memory usage.



Windows PowerShell

```
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 33.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,270.23 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:28 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 30.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,491.32 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:34 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 22.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,485.87 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:40 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
-----------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 63.00%
-----------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,494.55 KB / Total RAM: 4,095.55 KB
-----------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:46 **********
***** Process Monitoring *****
Total Running Processes: 41
```

We verified this by using the task manager too:



Physical Memory (MB)

Total	4095
Cached	1144
Available	2605
Free	1965

Kernel Memory (MB)

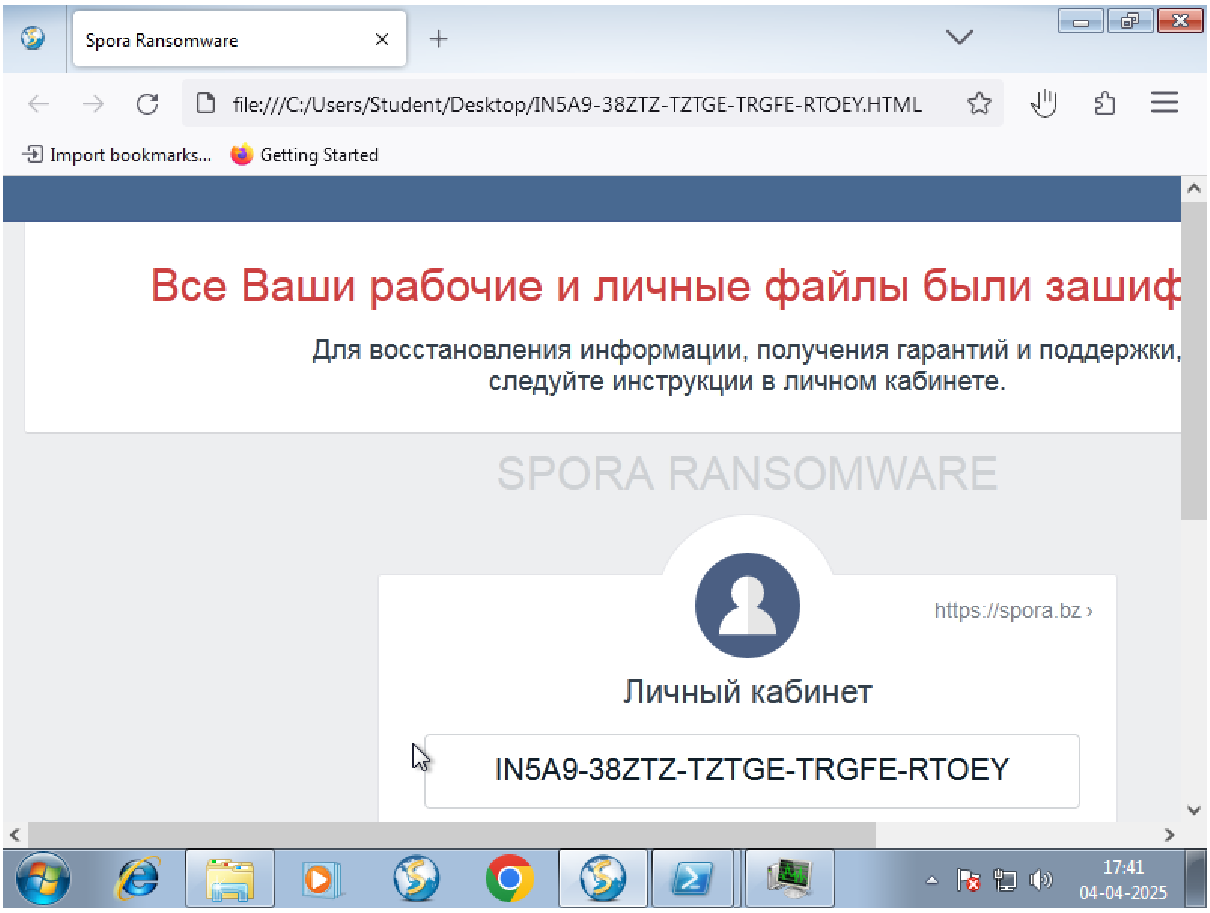
Paged	186
Nonpaged	49

System

Handles	11725
Threads	517
Processes	40
Up Time	0:00:35:51
Commit (MB)	1024 / 8189

Processes: 40 CPU Usage: 50% Physical Memory: 36%

A window showed up which looked like this.



Spora Ransomware

file:///C:/Users/Student/Desktop/IN5A9-38ZTZ-TZTGE-TRGFE-RTOEY.HTML

Import bookmarks... Getting Started

Все Ваши рабочие и личные файлы были зашиф

Для восстановления информации, получения гарантий и поддержки, следуйте инструкции в личном кабинете.

SPORA RANSOMWARE

https://spora.bz ›

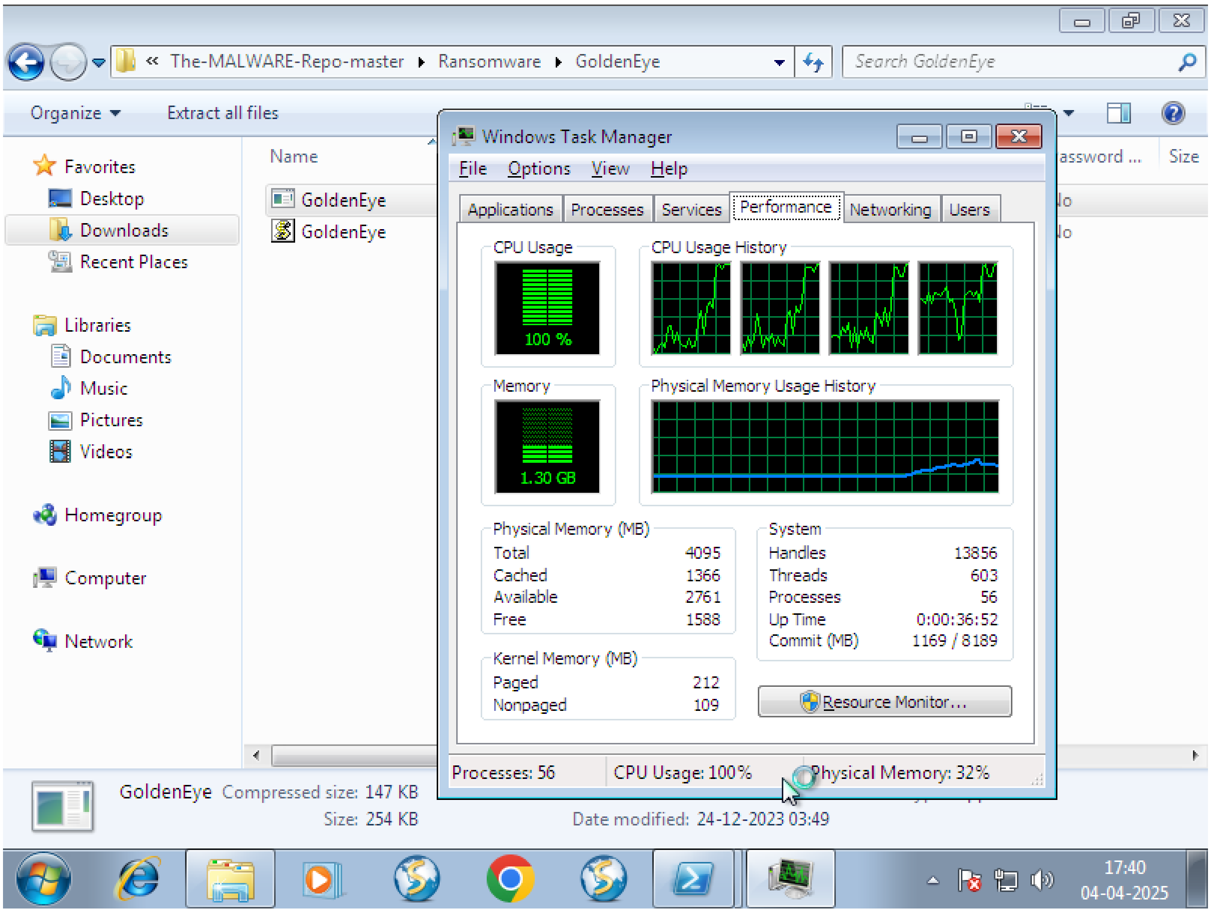
Личный кабинет

IN5A9-38ZTZ-TZTGE-TRGFE-RTOEY

17:41
04-04-2025

3. GoldenEye

After executing the malware, we noticed that the Task manager showed a high memory usage.



Physical Memory (MB)
Total 4095
Cached 1366
Available 2761
Free 1588

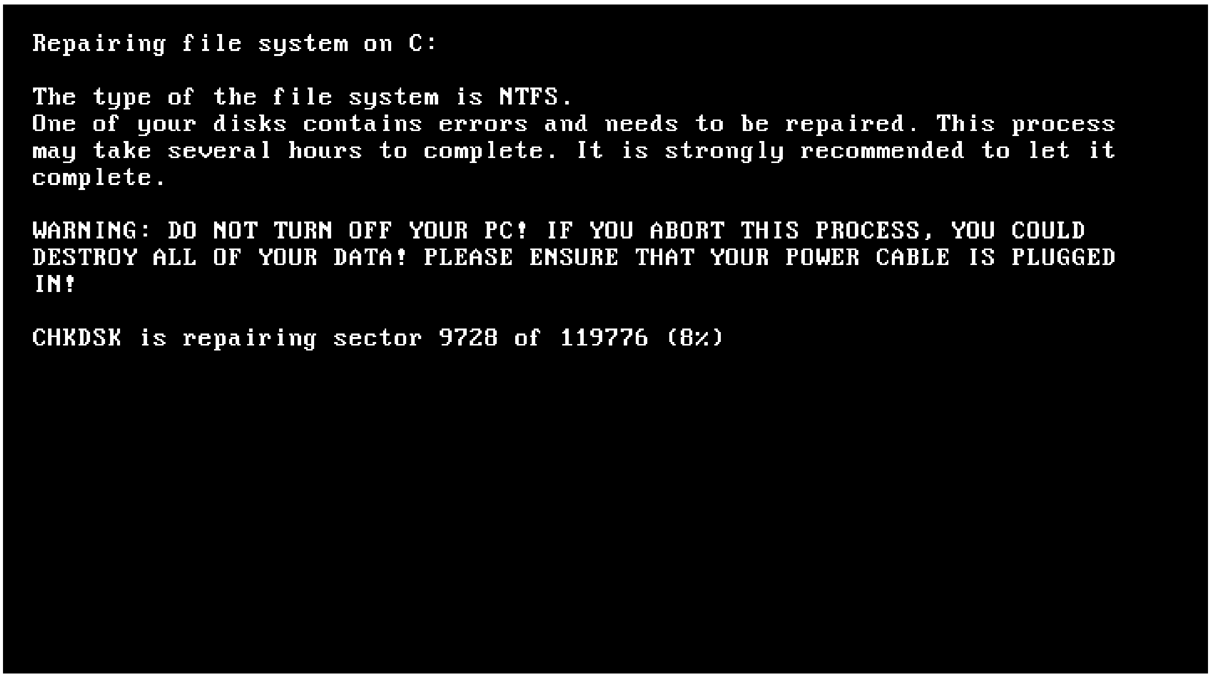
Kernel Memory (MB)
Paged 212
Nonpaged 109

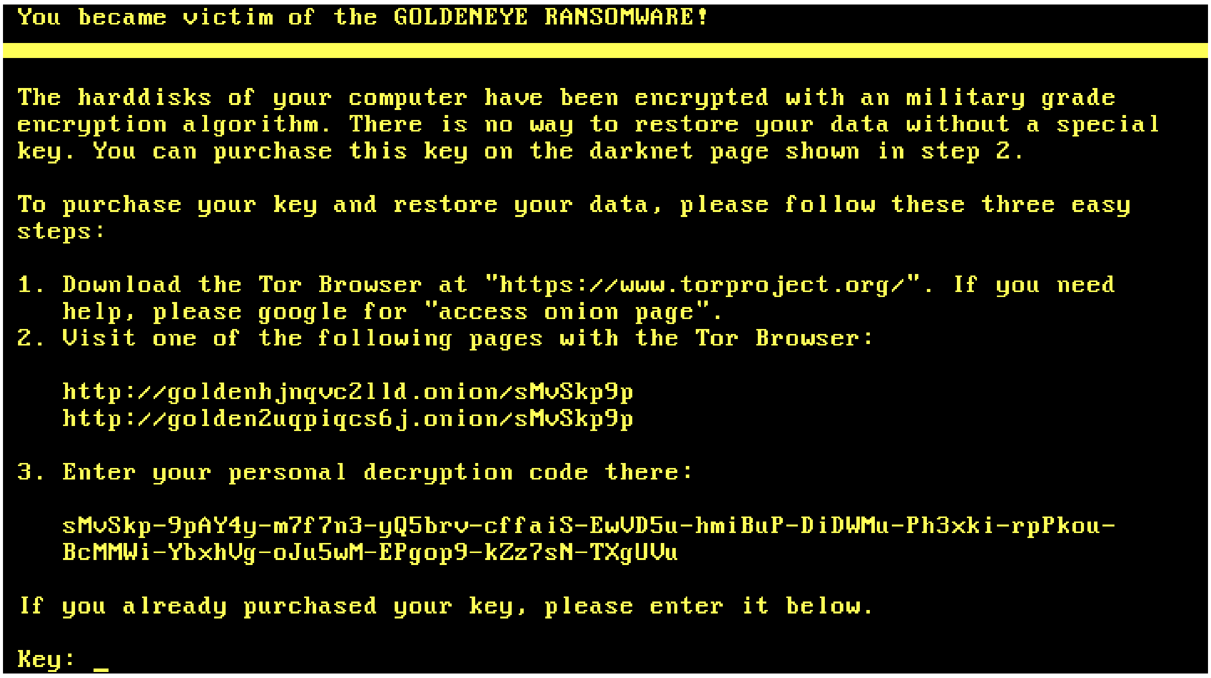
System
Handles 13856
Threads 603
Processes 56
Up Time 0:00:36:52
Commit (MB) 1169 / 8189

Processes: 56 CPU Usage: 100% Physical Memory: 32%

GoldenEye Compressed size: 147 KB
Size: 254 KB
Date modified: 24-12-2023 03:49

Unfortunately, we couldn't see this using the PowerShell console because the system immediately got shut down and the following message appeared on the screen:

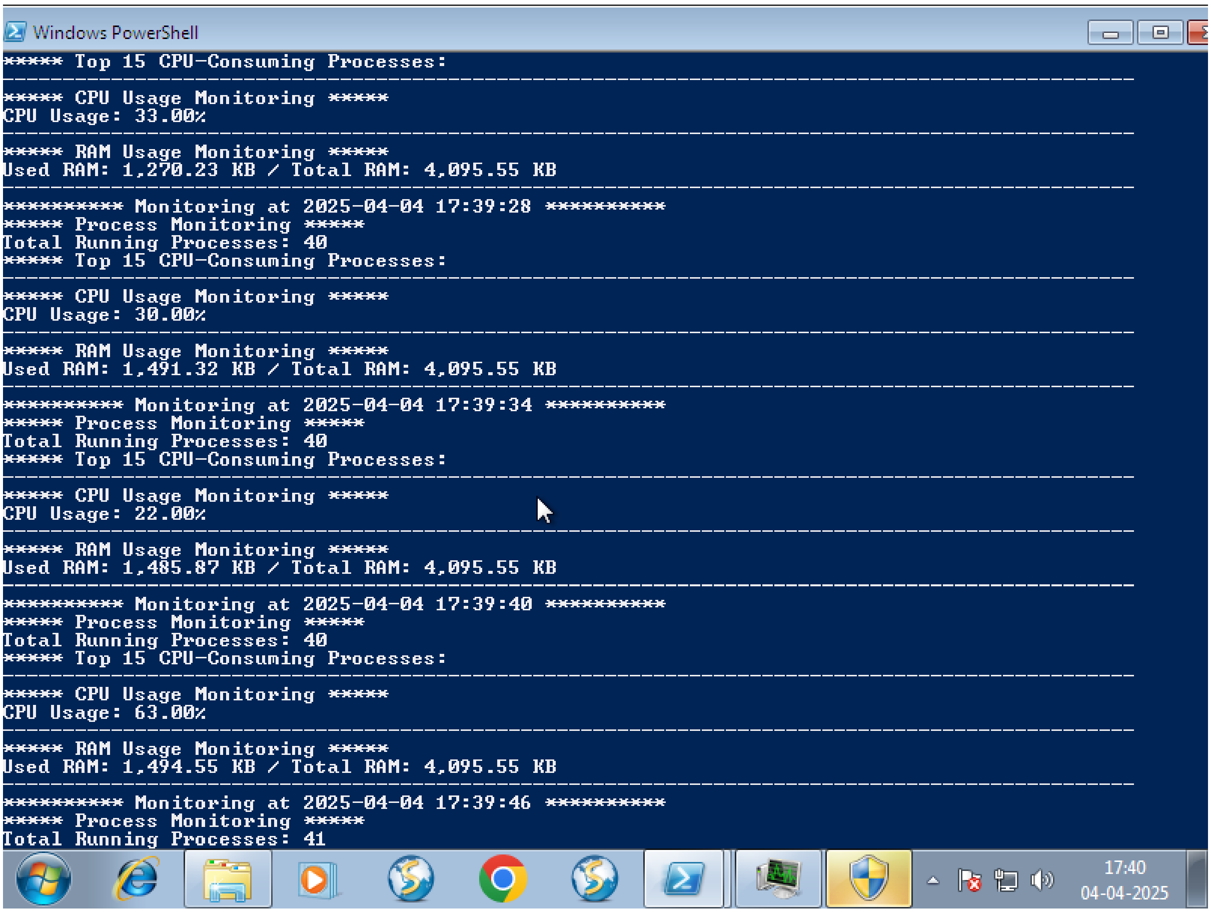

```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 9728 of 119776 (8%)
```



```
You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://goldenhjnqvc2lld.onion/sMvSkp9p
   http://golden2uqpiqcs6j.onion/sMvSkp9p

3. Enter your personal decryption code there:

   sMvSkp-9pAY4y-m7f7n3-yQ5brv-cffaiS-EwVD5u-hmiBuP-DiDWMu-Ph3xki-rpPkou-
   BcMMWi-YbxhVg-oJu5wM-EPgop9-kZz7sN-TXgUVu

If you already purchased your key, please enter it below.

Key: _
```

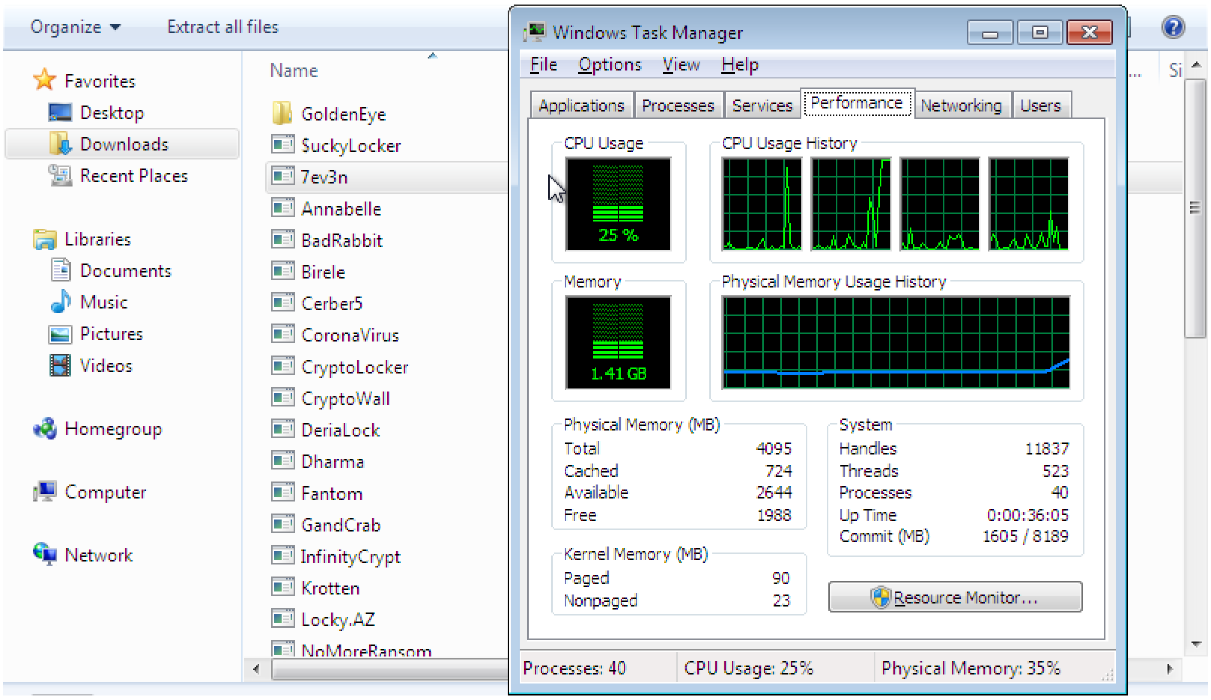
4. 7ev3n

After executing the malware, we noticed that the PowerShell console showed a high memory usage.



```
***** Top 15 CPU-Consuming Processes:
-------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 33.00%
-------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,270.23 KB / Total RAM: 4,095.55 KB
-------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:28 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
-------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 30.00%
-------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,491.32 KB / Total RAM: 4,095.55 KB
-------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:34 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
-------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 22.00%
-------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,485.87 KB / Total RAM: 4,095.55 KB
-------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:40 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
-------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 63.00%
-------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 1,494.55 KB / Total RAM: 4,095.55 KB
-------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:46 **********
***** Process Monitoring *****
Total Running Processes: 41
```

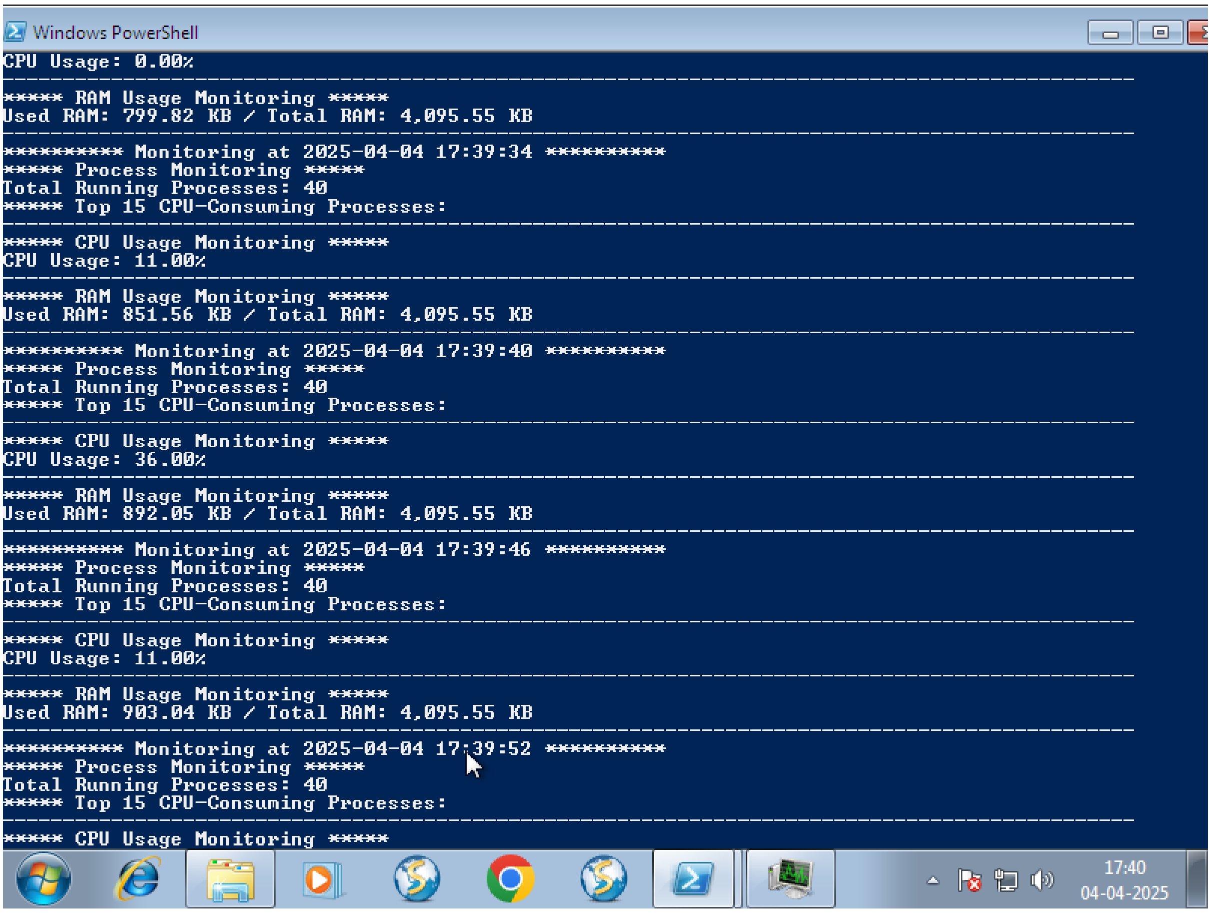
We verified this by using the task manager too:



```
Physical Memory (MB)
Total        4095
Cached        724
Available    2644
Free         1988

Kernel Memory (MB)
Paged          90
Nonpaged       23

System
Handles          11837
Threads            523
Processes           40
Up Time     0:00:36:05
Commit (MB) 1605 / 8189

Processes: 40    CPU Usage: 25%    Physical Memory: 35%
```

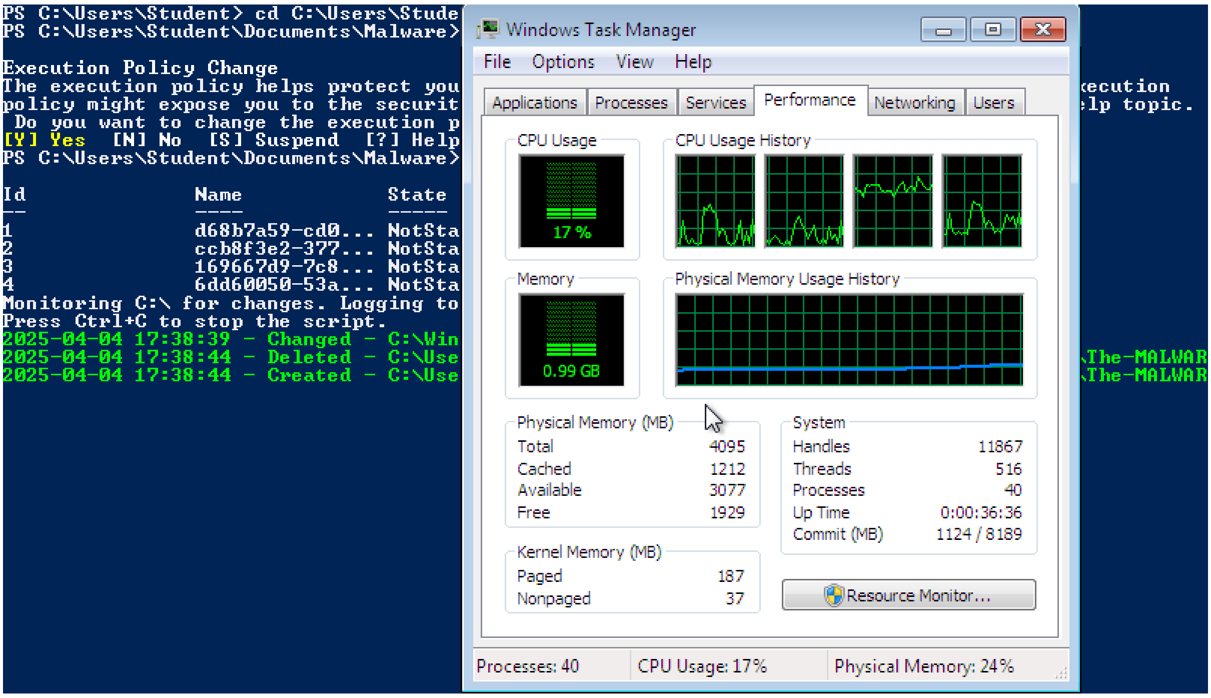
5. GandCrab v5.2

After executing the malware, we noticed that the PowerShell console showed a high memory usage.



```
CPU Usage: 0.00%
------------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 799.82 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:34 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 11.00%
------------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 851.56 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:40 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 36.00%
------------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 892.05 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:46 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
CPU Usage: 11.00%
------------------------------------------------------------------------------------------------
***** RAM Usage Monitoring *****
Used RAM: 903.04 KB / Total RAM: 4,095.55 KB
------------------------------------------------------------------------------------------------
********** Monitoring at 2025-04-04 17:39:52 **********
***** Process Monitoring *****
Total Running Processes: 40
***** Top 15 CPU-Consuming Processes:
------------------------------------------------------------------------------------------------
***** CPU Usage Monitoring *****
```

We verified this by using the task manager too:



```
PS C:\Users\Student> cd C:\Users\Stude
PS C:\Users\Student\Documents\Malware>

Execution Policy Change
The execution policy helps protect you
policy might expose you to the securit
 Do you want to change the execution p
[Y] Yes  [N] No  [S] Suspend  [?] Help
PS C:\Users\Student\Documents\Malware>

Id               Name              State
--               ----              -----
1                d68b7a59-cd0... NotSta
2                ccb8f3e2-377... NotSta
3                169667d9-7c8... NotSta
4                6dd60050-53a... NotSta
Monitoring C:\ for changes. Logging to
Press Ctrl+C to stop the script.
2025-04-04 17:38:39 - Changed - C:\Win
2025-04-04 17:38:44 - Deleted - C:\Use
2025-04-04 17:38:44 - Created - C:\Use
```

```
xecution
lp topic.

\The-MALWAR
\The-MALWAR
```

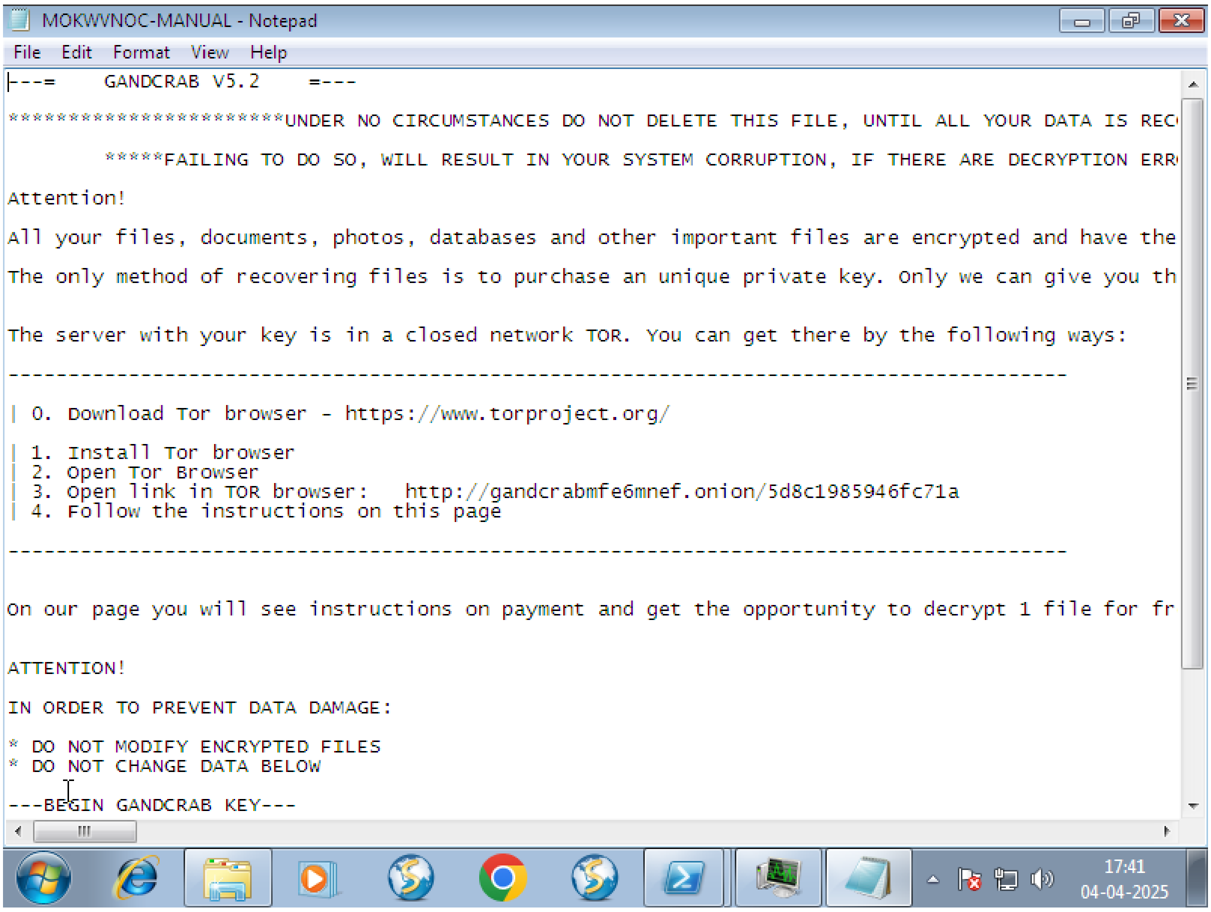
Physical Memory (MB)
Total 4095
Cached 1212
Available 3077
Free 1929

Kernel Memory (MB)
Paged 187
Nonpaged 37

System
Handles 11867
Threads 516
Processes 40
Up Time 0:00:36:36
Commit (MB) 1124 / 8189

Processes: 40 CPU Usage: 17% Physical Memory: 24%

A file got created which had the following contents.

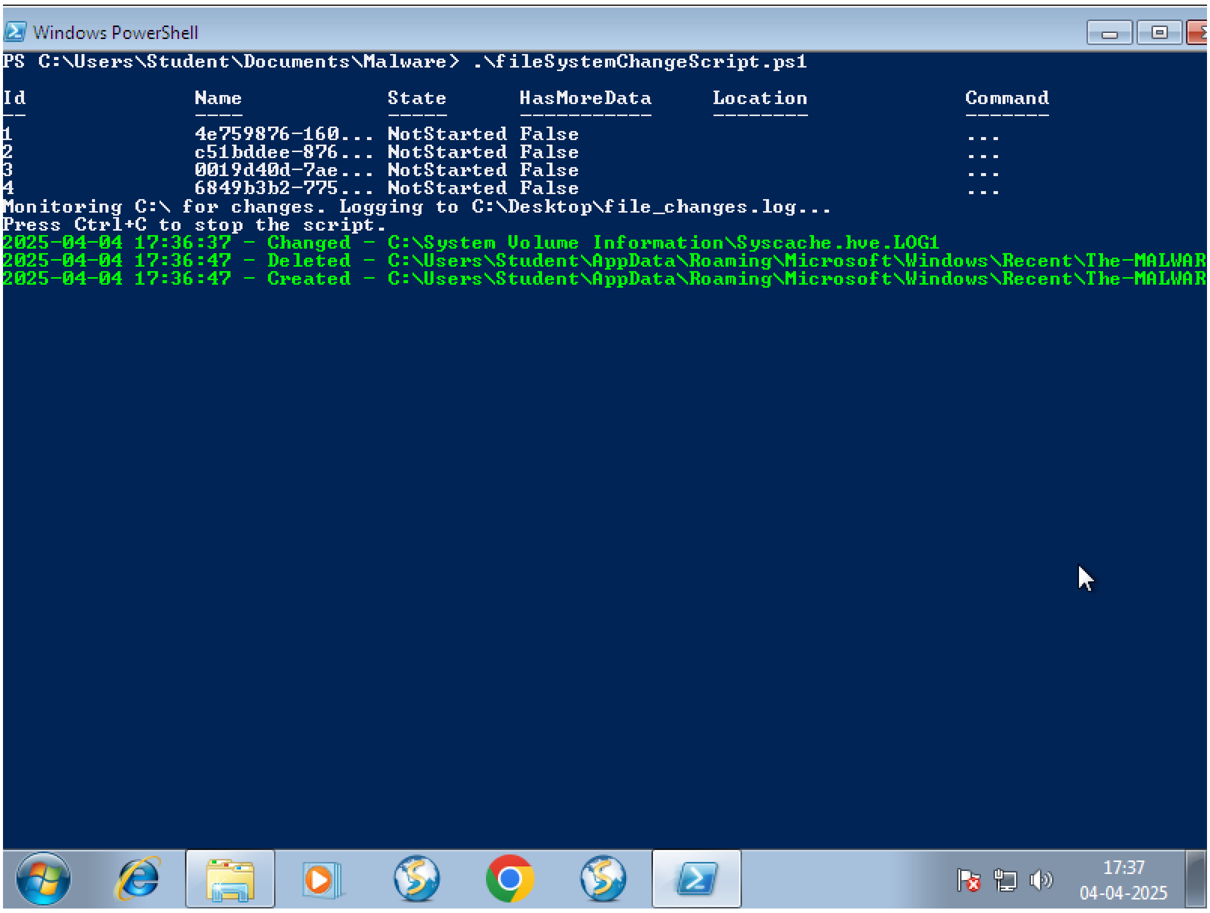


```
---=    GANDCRAB V5.2    =---

***********************UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS REC

        *****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERR

Attention!

All your files, documents, photos, databases and other important files are encrypted and have the

The only method of recovering files is to purchase an unique private key. Only we can give you th


The server with your key is in a closed network TOR. You can get there by the following ways:

----------------------------------------------------------------------------------------

| 0. Download Tor browser - https://www.torproject.org/

| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser:   http://gandcrabmfe6mnef.onion/5d8c1985946fc71a
| 4. Follow the instructions on this page

----------------------------------------------------------------------------------------


On our page you will see instructions on payment and get the opportunity to decrypt 1 file for fr


ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:

* DO NOT MODIFY ENCRYPTED FILES
* DO NOT CHANGE DATA BELOW

---BEGIN GANDCRAB KEY---
```

- **Malwares which manipulate the File system.**

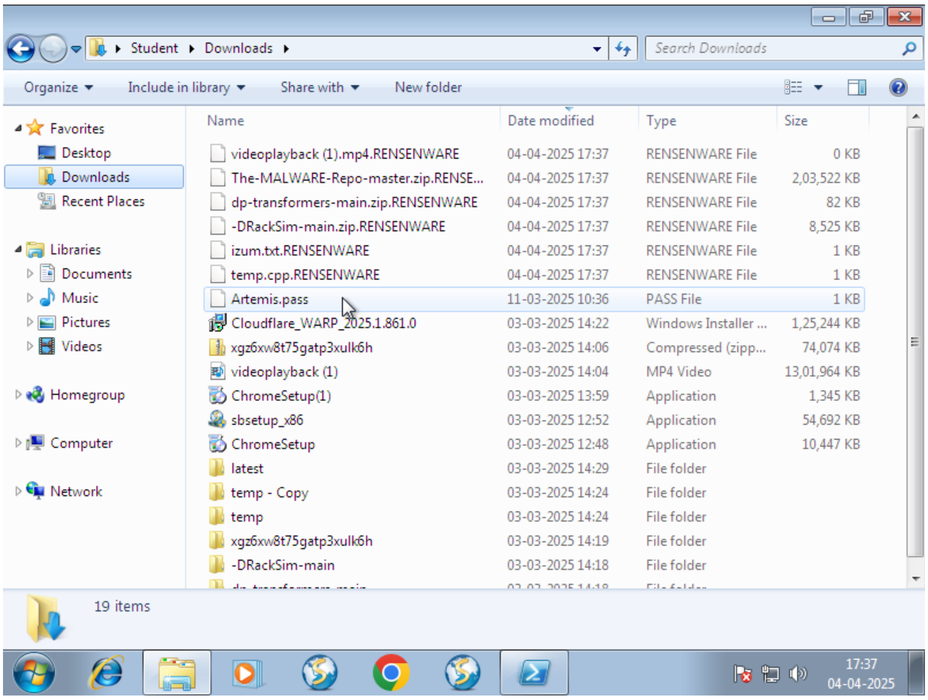
1. Rensenware

The script which was supposed to detect any changes in the file system showed this:



```
PS C:\Users\Student\Documents\Malware> .\fileSystemChangeScript.ps1

Id              Name             State      HasMoreData     Location             Command
--              ----             -----      -----------     --------             -------
1               4e759876-160...  NotStarted False                                ...
2               c51bddee-876...  NotStarted False                                ...
3               0019d40d-7ae...  NotStarted False                                ...
4               6849b3b2-775...  NotStarted False                                ...
Monitoring C:\ for changes. Logging to C:\Desktop\file_changes.log...
Press Ctrl+C to stop the script.
2025-04-04 17:36:37 - Changed - C:\System Volume Information\Syscache.hve.LOG1
2025-04-04 17:36:47 - Deleted - C:\Users\Student\AppData\Roaming\Microsoft\Windows\Recent\The-MALWAR
2025-04-04 17:36:47 - Created - C:\Users\Student\AppData\Roaming\Microsoft\Windows\Recent\The-MALWAR
```

All the files in the File explorer were encrypted and looked like this.

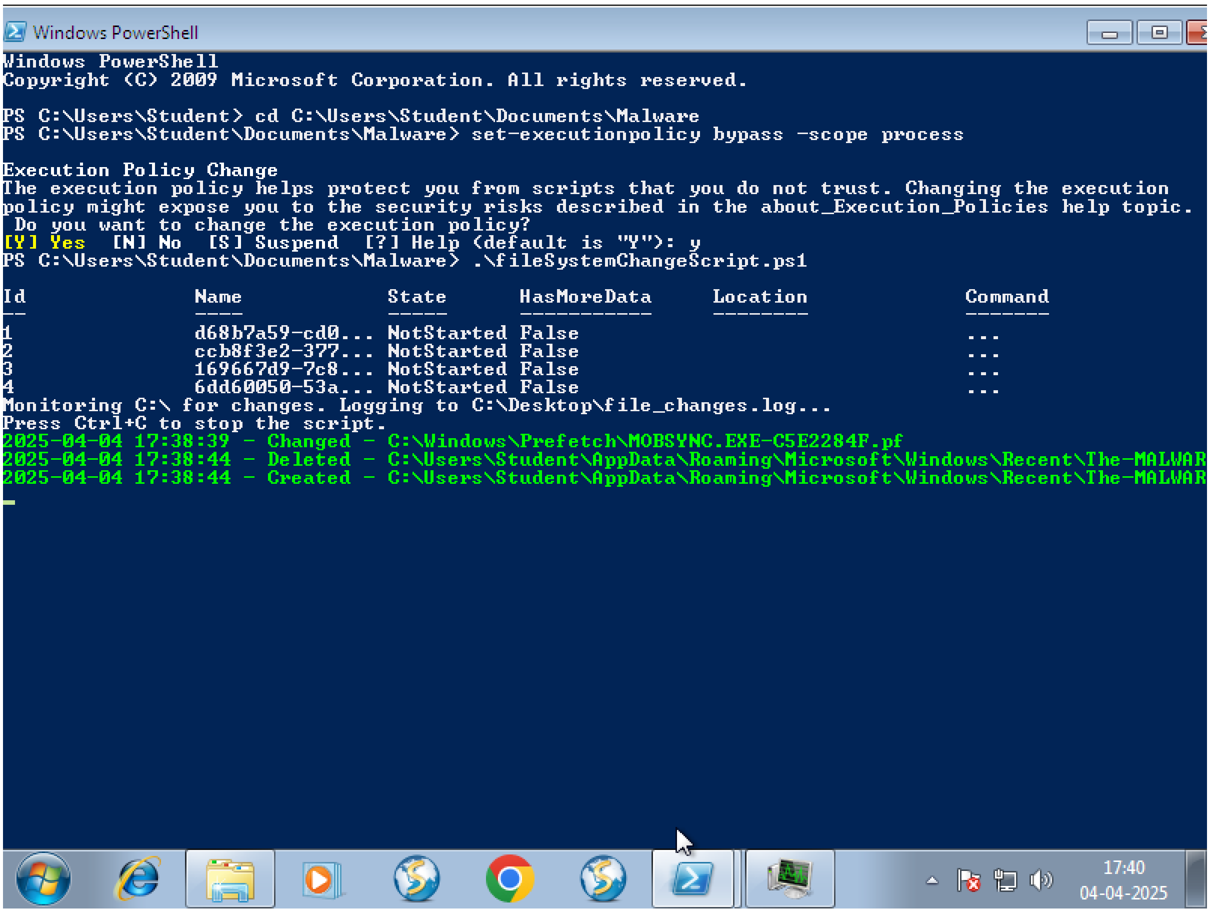


Name	Date modified	Type	Size
videoplayback (1).mp4.RENSENWARE	04-04-2025 17:37	RENSENWARE File	0 KB
The-MALWARE-Repo-master.zip.RENSE...	04-04-2025 17:37	RENSENWARE File	2,03,522 KB
dp-transformers-main.zip.RENSENWARE	04-04-2025 17:37	RENSENWARE File	82 KB
-DRackSim-main.zip.RENSENWARE	04-04-2025 17:37	RENSENWARE File	8,525 KB
izum.txt.RENSENWARE	04-04-2025 17:37	RENSENWARE File	1 KB
temp.cpp.RENSENWARE	04-04-2025 17:37	RENSENWARE File	1 KB
Artemis.pass	11-03-2025 10:36	PASS File	1 KB
Cloudflare_WARP_2025.1.861.0	03-03-2025 14:22	Windows Installer ...	1,25,244 KB
xgz6xw8t75gatp3xulk6h	03-03-2025 14:06	Compressed (zipp...	74,074 KB
videoplayback (1)	03-03-2025 14:04	MP4 Video	13,01,964 KB
ChromeSetup(1)	03-03-2025 13:59	Application	1,345 KB
sbsetup_x86	03-03-2025 12:52	Application	54,692 KB
ChromeSetup	03-03-2025 12:48	Application	10,447 KB
latest	03-03-2025 14:29	File folder	
temp - Copy	03-03-2025 14:24	File folder	
temp	03-03-2025 14:24	File folder	
xgz6xw8t75gatp3xulk6h	03-03-2025 14:19	File folder	
-DRackSim-main	03-03-2025 14:18	File folder	

19 items

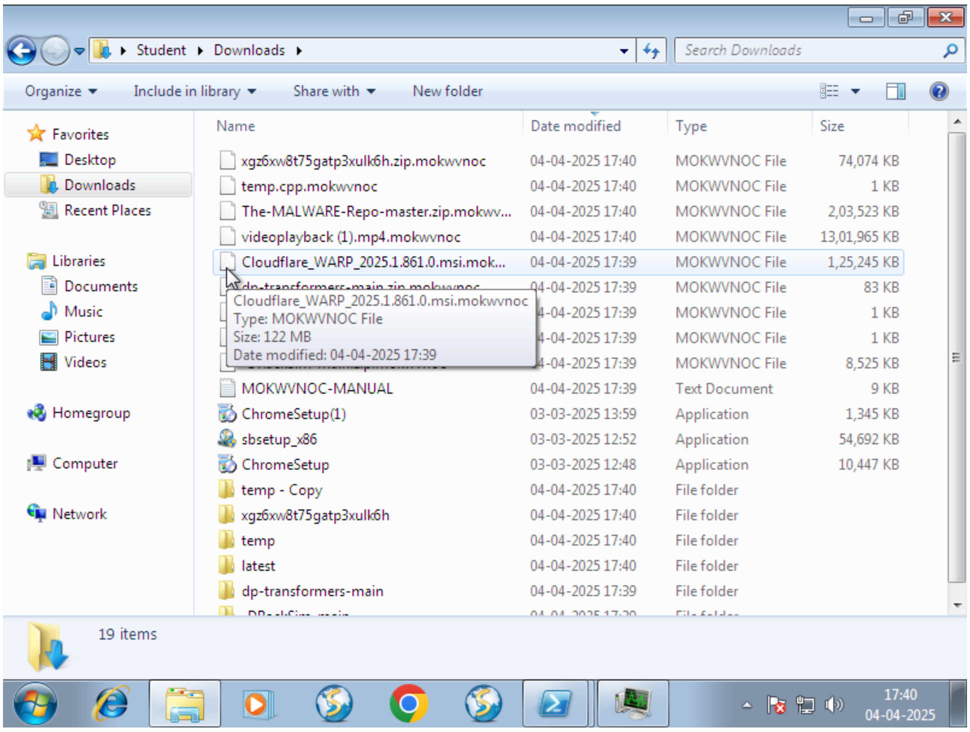
2. GandCrab v5.2

The script which was supposed to detect any changes in the file system showed this:



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Student> cd C:\Users\Student\Documents\Malware
PS C:\Users\Student\Documents\Malware> set-executionpolicy bypass -scope process

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution
policy might expose you to the security risks described in the about_Execution_Policies help topic.
 Do you want to change the execution policy?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
PS C:\Users\Student\Documents\Malware> .\fileSystemChangeScript.ps1

Id              Name            State      HasMoreData     Location             Command
--              ----            -----      -----------     --------             -------
1               d68b7a59-cd0... NotStarted False                                ...
2               ccb8f3e2-377... NotStarted False                                ...
3               169667d9-7c8... NotStarted False                                ...
4               6dd60050-53a... NotStarted False                                ...
Monitoring C:\ for changes. Logging to C:\Desktop\file_changes.log...
Press Ctrl+C to stop the script.
2025-04-04 17:38:39 - Changed - C:\Windows\Prefetch\MOBSYNC.EXE-C5E2284F.pf
2025-04-04 17:38:44 - Deleted - C:\Users\Student\AppData\Roaming\Microsoft\Windows\Recent\The-MALWAR
2025-04-04 17:38:44 - Created - C:\Users\Student\AppData\Roaming\Microsoft\Windows\Recent\The-MALWAR
_
```

All the files in the File explorer were encrypted and looked like this.



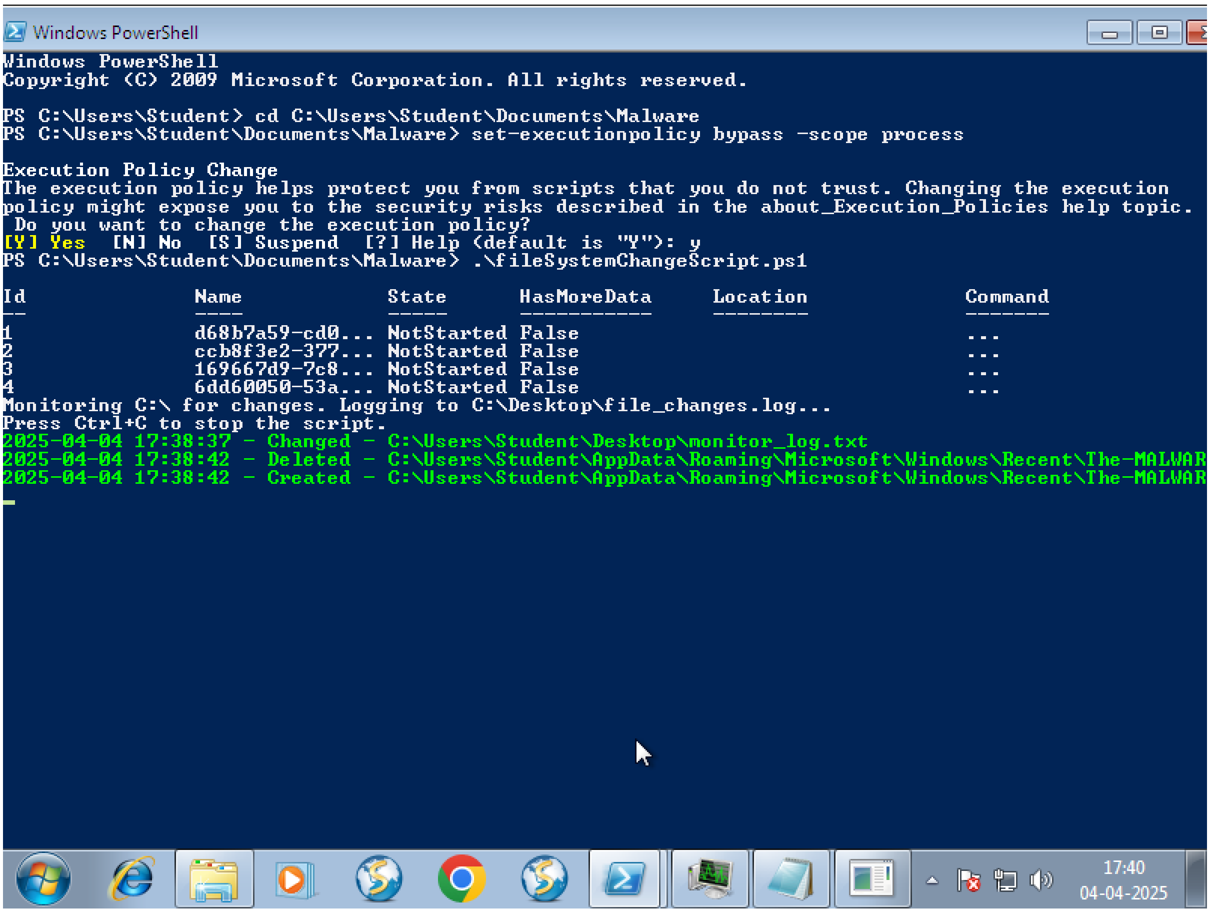
Name	Date modified	Type	Size
xgz6xw8t75gatp3xulk6h.zip.mokwvnoc	04-04-2025 17:40	MOKWVNOC File	74,074 KB
temp.cpp.mokwvnoc	04-04-2025 17:40	MOKWVNOC File	1 KB
The-MALWARE-Repo-master.zip.mokwv...	04-04-2025 17:40	MOKWVNOC File	2,03,523 KB
videoplayback (1).mp4.mokwvnoc	04-04-2025 17:40	MOKWVNOC File	13,01,965 KB
Cloudflare_WARP_2025.1.861.0.msi.mok...	04-04-2025 17:39	MOKWVNOC File	1,25,245 KB
dp-transformers-main.zip.mokwvnoc	04-04-2025 17:39	MOKWVNOC File	83 KB
	4-04-2025 17:39	MOKWVNOC File	1 KB
	4-04-2025 17:39	MOKWVNOC File	1 KB
	4-04-2025 17:39	MOKWVNOC File	8,525 KB
MOKWVNOC-MANUAL	04-04-2025 17:39	Text Document	9 KB
ChromeSetup(1)	03-03-2025 13:59	Application	1,345 KB
sbsetup_x86	03-03-2025 12:52	Application	54,692 KB
ChromeSetup	03-03-2025 12:48	Application	10,447 KB
temp - Copy	04-04-2025 17:40	File folder	
xgz6xw8t75gatp3xulk6h	04-04-2025 17:40	File folder	
temp	04-04-2025 17:40	File folder	
latest	04-04-2025 17:40	File folder	
dp-transformers-main	04-04-2025 17:39	File folder	

Cloudflare_WARP_2025.1.861.0.msi.mokwvnoc
Type: MOKWVNOC File
Size: 122 MB
Date modified: 04-04-2025 17:39

19 items

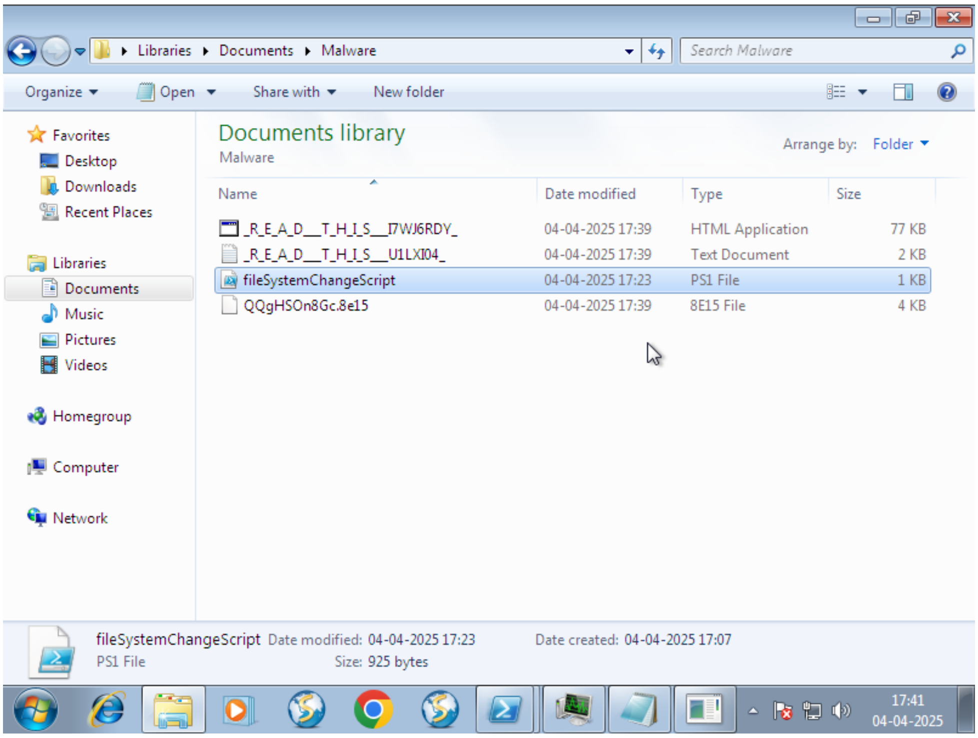
3. Cerber

The script which was supposed to detect any changes in the file system showed this:



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Student> cd C:\Users\Student\Documents\Malware
PS C:\Users\Student\Documents\Malware> set-executionpolicy bypass -scope process

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution
policy might expose you to the security risks described in the about_Execution_Policies help topic.
 Do you want to change the execution policy?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
PS C:\Users\Student\Documents\Malware> .\fileSystemChangeScript.ps1

Id              Name            State      HasMoreData     Location             Command
--              ----            -----      -----------     --------             -------
1               d68b7a59-cd0... NotStarted False                                ...
2               ccb8f3e2-377... NotStarted False                                ...
3               169667d9-7c8... NotStarted False                                ...
4               6dd60050-53a... NotStarted False                                ...
Monitoring C:\ for changes. Logging to C:\Desktop\file_changes.log...
Press Ctrl+C to stop the script.
2025-04-04 17:38:37 - Changed - C:\Users\Student\Desktop\monitor_log.txt
2025-04-04 17:38:42 - Deleted - C:\Users\Student\AppData\Roaming\Microsoft\Windows\Recent\The-MALWAR
2025-04-04 17:38:42 - Created - C:\Users\Student\AppData\Roaming\Microsoft\Windows\Recent\The-MALWAR
_
```

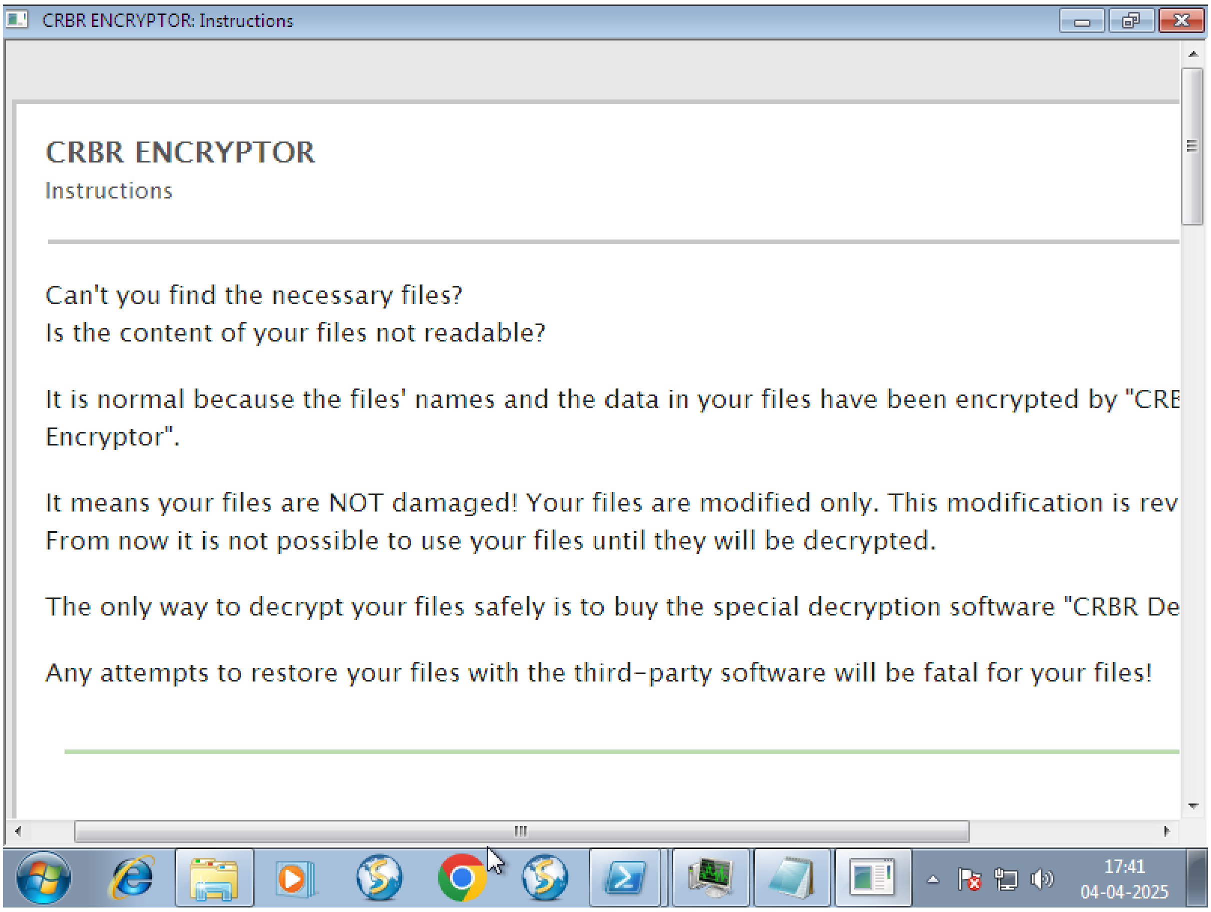
All the files in the File explorer were encrypted and looked like this.



Name	Date modified	Type	Size
_R_E_A_D__T_H_I_S__I7WJ6RDY_	04-04-2025 17:39	HTML Application	77 KB
_R_E_A_D__T_H_I_S__U1LXI04_	04-04-2025 17:39	Text Document	2 KB
fileSystemChangeScript	04-04-2025 17:23	PS1 File	1 KB
QQgHSOn8Gc.8e15	04-04-2025 17:39	8E15 File	4 KB

fileSystemChangeScript Date modified: 04-04-2025 17:23 Date created: 04-04-2025 17:07
PS1 File Size: 925 bytes

A pop-up window showed up which had the following contents.



CRBR ENCRYPTOR

Instructions

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "CRE
Encryptor".

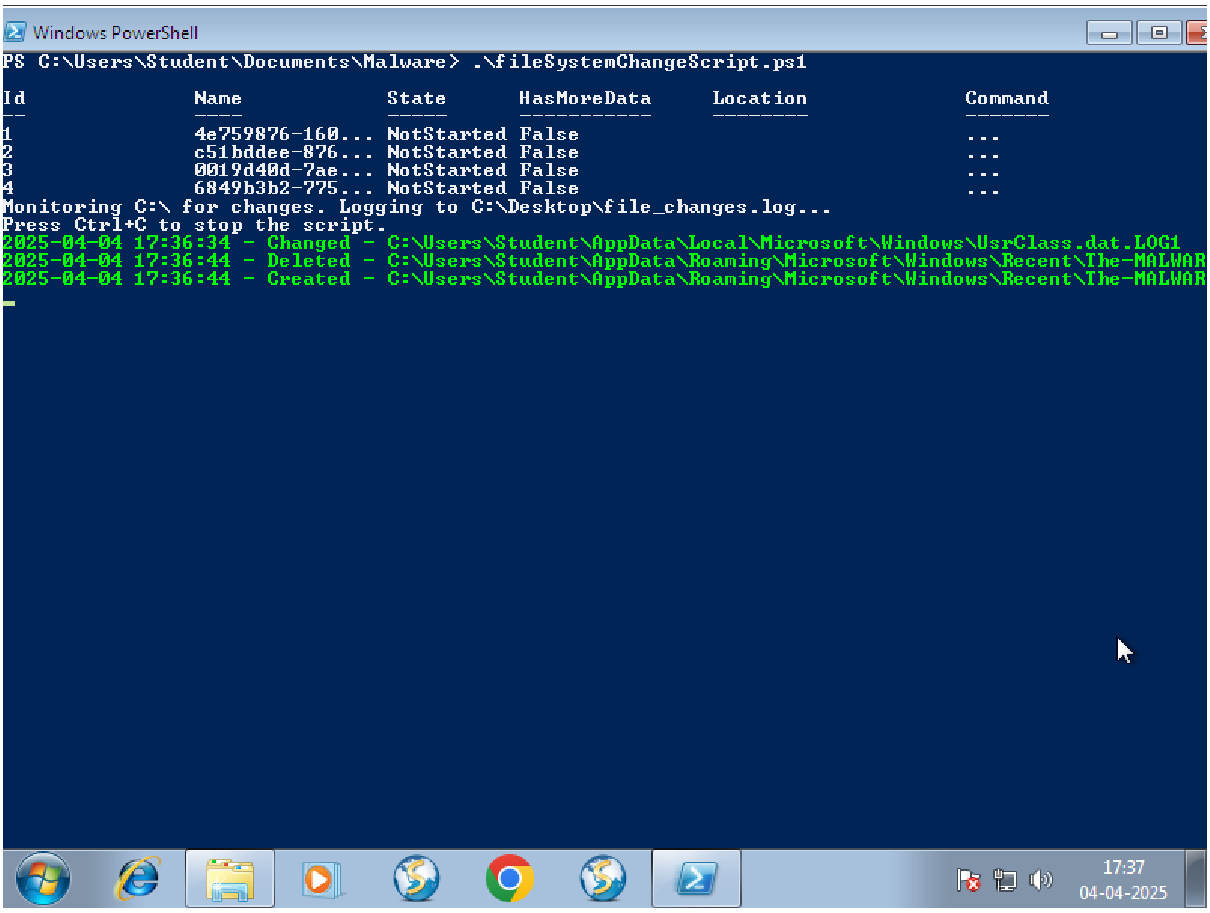
It means your files are NOT damaged! Your files are modified only. This modification is rev
From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "CRBR De

Any attempts to restore your files with the third-party software will be fatal for your files!

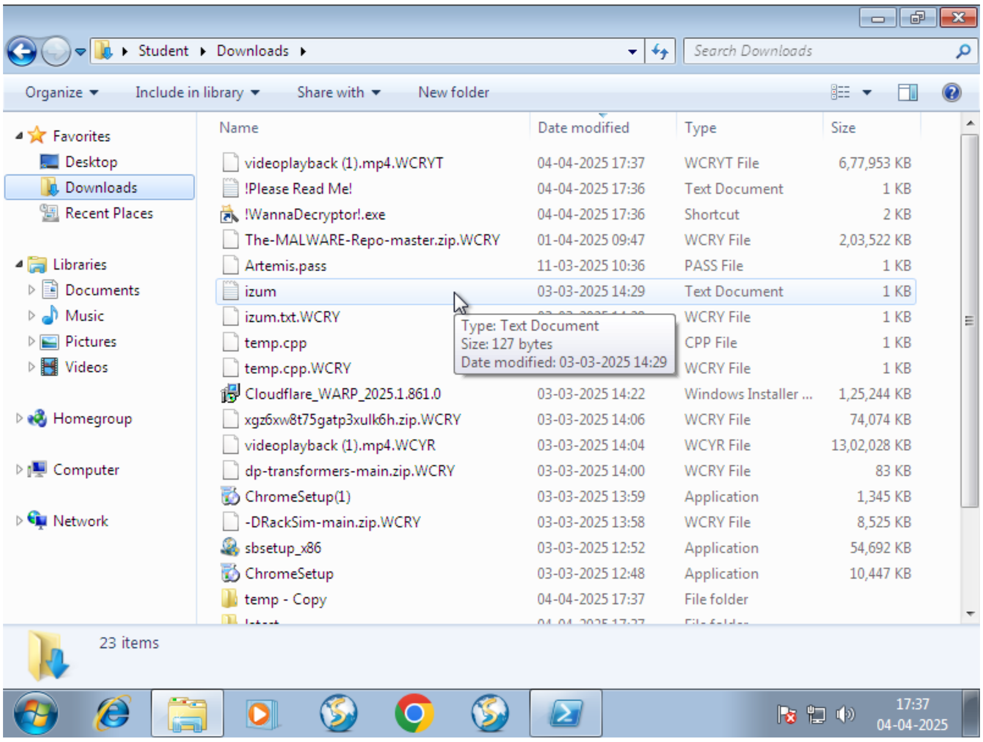
4. WannaCry

The script which was supposed to detect any changes in the file system showed this:



```
PS C:\Users\Student\Documents\Malware> .\fileSystemChangeScript.ps1

Id              Name            State      HasMoreData     Location             Command
--              ----            -----      -----------     --------             -------
1               4e759876-160... NotStarted False                                ...
2               c51bddee-876... NotStarted False                                ...
3               0019d40d-7ae... NotStarted False                                ...
4               6849b3b2-775... NotStarted False                                ...
Monitoring C:\ for changes. Logging to C:\Desktop\file_changes.log...
Press Ctrl+C to stop the script.
2025-04-04 17:36:34 - Changed - C:\Users\Student\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
2025-04-04 17:36:44 - Deleted - C:\Users\Student\AppData\Roaming\Microsoft\Windows\Recent\The-MALWAR
2025-04-04 17:36:44 - Created - C:\Users\Student\AppData\Roaming\Microsoft\Windows\Recent\The-MALWAR
```

All the files in the File explorer were encrypted and looked like this.



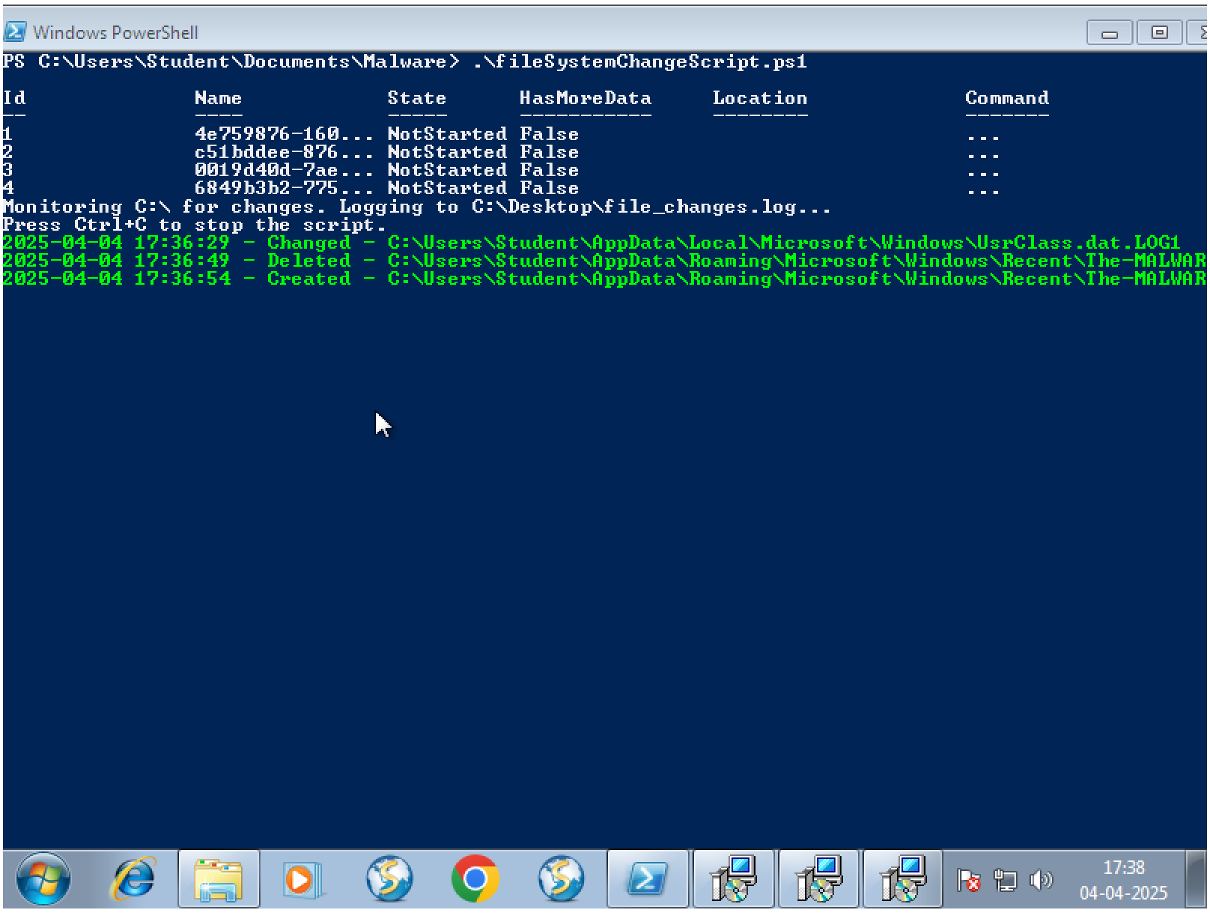
Name	Date modified	Type	Size
videoplayback (1).mp4.WCRYT	04-04-2025 17:37	WCRYT File	6,77,953 KB
!Please Read Me!	04-04-2025 17:36	Text Document	1 KB
!WannaDecryptor!.exe	04-04-2025 17:36	Shortcut	2 KB
The-MALWARE-Repo-master.zip.WCRY	01-04-2025 09:47	WCRY File	2,03,522 KB
Artemis.pass	11-03-2025 10:36	PASS File	1 KB
izum	03-03-2025 14:29	Text Document	1 KB
izum.txt.WCRY		WCRY File	1 KB
temp.cpp		CPP File	1 KB
temp.cpp.WCRY		WCRY File	1 KB
Cloudflare_WARP_2025.1.861.0	03-03-2025 14:22	Windows Installer ...	1,25,244 KB
xgz6xw8t75gatp3xulk6h.zip.WCRY	03-03-2025 14:06	WCRY File	74,074 KB
videoplayback (1).mp4.WCYR	03-03-2025 14:04	WCYR File	13,02,028 KB
dp-transformers-main.zip.WCRY	03-03-2025 14:00	WCRY File	83 KB
ChromeSetup(1)	03-03-2025 13:59	Application	1,345 KB
-DRackSim-main.zip.WCRY	03-03-2025 13:58	WCRY File	8,525 KB
sbsetup_x86	03-03-2025 12:52	Application	54,692 KB
ChromeSetup	03-03-2025 12:48	Application	10,447 KB
temp - Copy	04-04-2025 17:37	File folder	

Type: Text Document
Size: 127 bytes
Date modified: 03-03-2025 14:29

23 items

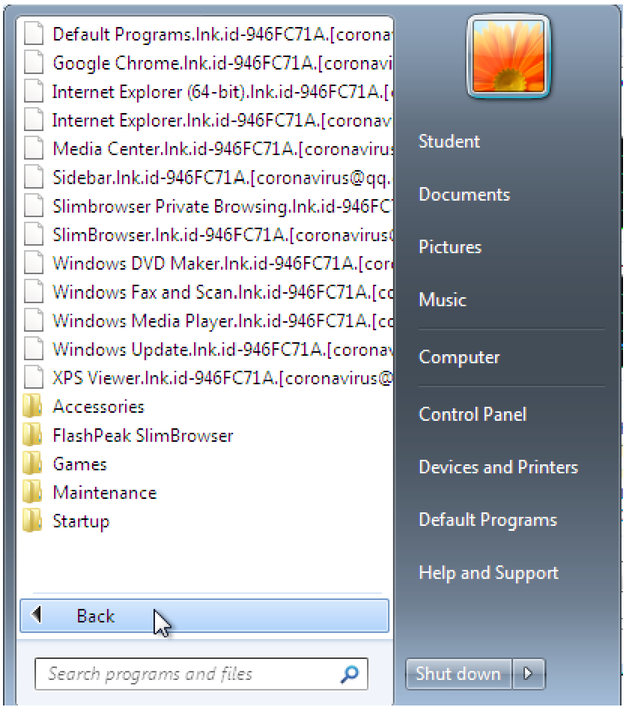
5. CoronaVirus

The script which was supposed to detect any changes in the file system showed this:



```
PS C:\Users\Student\Documents\Malware> .\fileSystemChangeScript.ps1

Id              Name            State      HasMoreData     Location             Command
--              ----            -----      -----------     --------             -------
1               4e759876-160... NotStarted False                                ...
2               c51bddee-876... NotStarted False                                ...
3               0019d40d-7ae... NotStarted False                                ...
4               6849b3b2-775... NotStarted False                                ...
Monitoring C:\ for changes. Logging to C:\Desktop\file_changes.log...
Press Ctrl+C to stop the script.
2025-04-04 17:36:29 - Changed - C:\Users\Student\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
2025-04-04 17:36:49 - Deleted - C:\Users\Student\AppData\Roaming\Microsoft\Windows\Recent\The-MALWAR
2025-04-04 17:36:54 - Created - C:\Users\Student\AppData\Roaming\Microsoft\Windows\Recent\The-MALWAR
```

All the files in the File explorer were encrypted and looked like this.



Default Programs.lnk.id-946FC71A.[corona
Google Chrome.lnk.id-946FC71A.[coronavi
Internet Explorer (64-bit).lnk.id-946FC71A.[
Internet Explorer.lnk.id-946FC71A.[coronav
Media Center.lnk.id-946FC71A.[coronaviru
Sidebar.lnk.id-946FC71A.[coronavirus@qq.
Slimbrowser Private Browsing.lnk.id-946FC
SlimBrowser.lnk.id-946FC71A.[coronavirus
Windows DVD Maker.lnk.id-946FC71A.[cor
Windows Fax and Scan.lnk.id-946FC71A.[c
Windows Media Player.lnk.id-946FC71A.[c
Windows Update.lnk.id-946FC71A.[corona
XPS Viewer.lnk.id-946FC71A.[coronavirus@