

**Report on Ransomware Analysis**

Security and Forensics Lab 2

**Subham Sanket Rout**

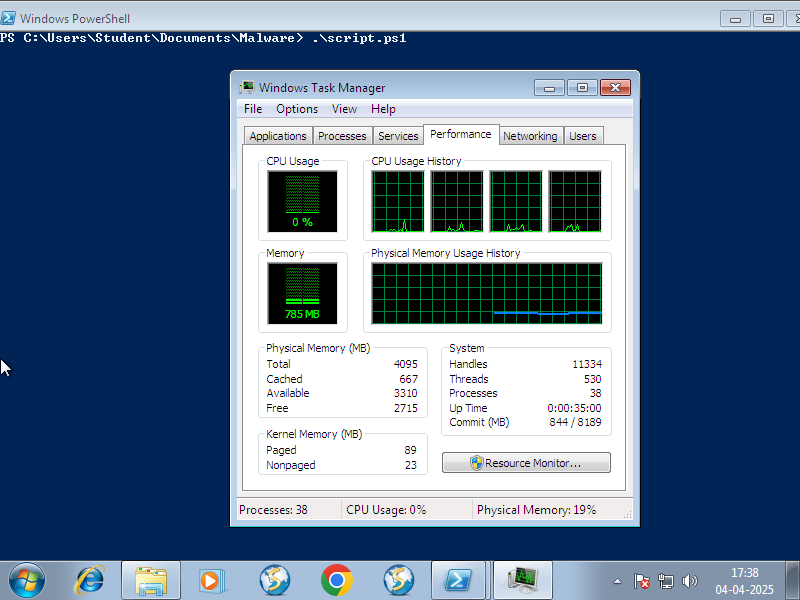
24CS06017

M.Tech (CSE) 1st Year

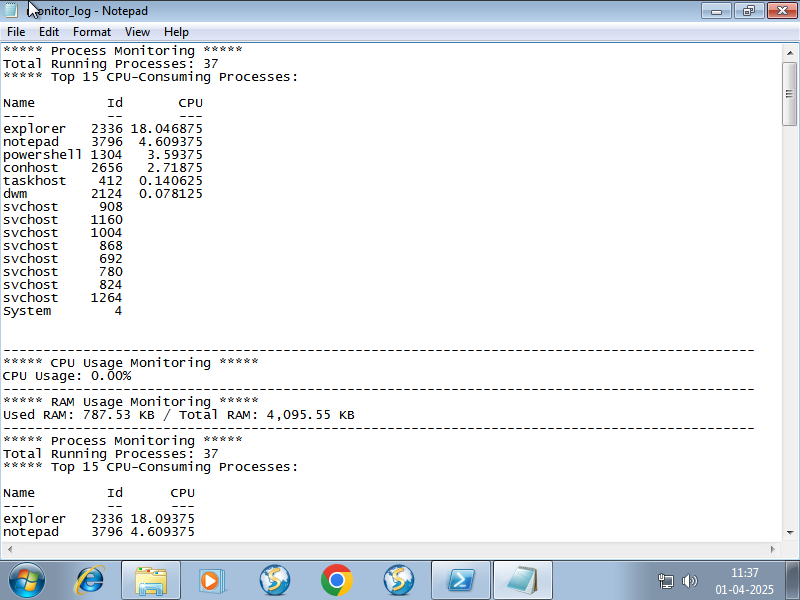
**System status before execution of any malware.**

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.**



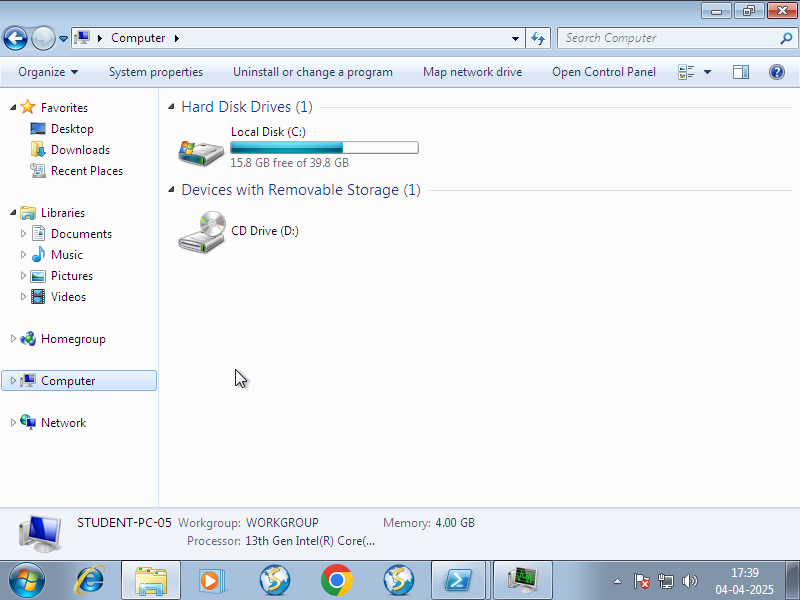
* **Screenshot of the Logfile showing the CPU usage, memory usage and number of processes. when system is idle and no malware has been executed.** (The Logfile displays the output of the PowerShell script that has been executed.)



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.

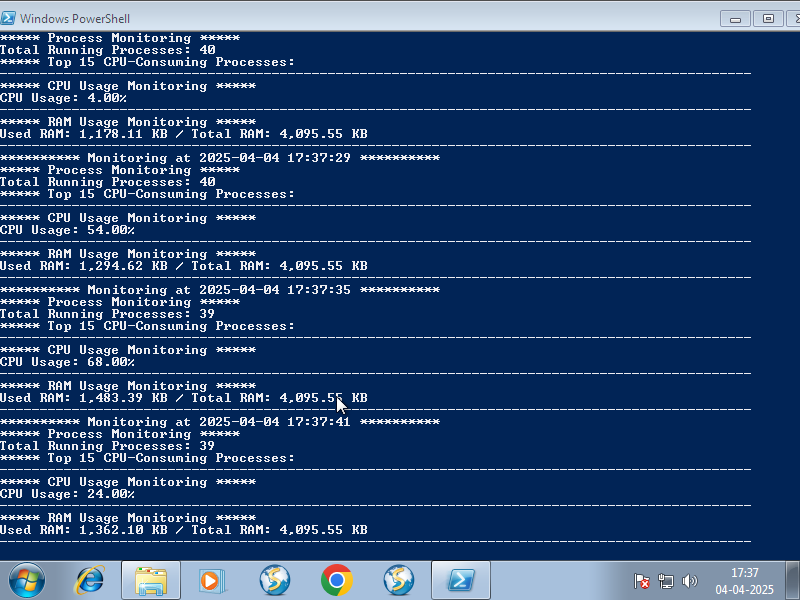
* **The screenshot of how the File Explorer looks like.**



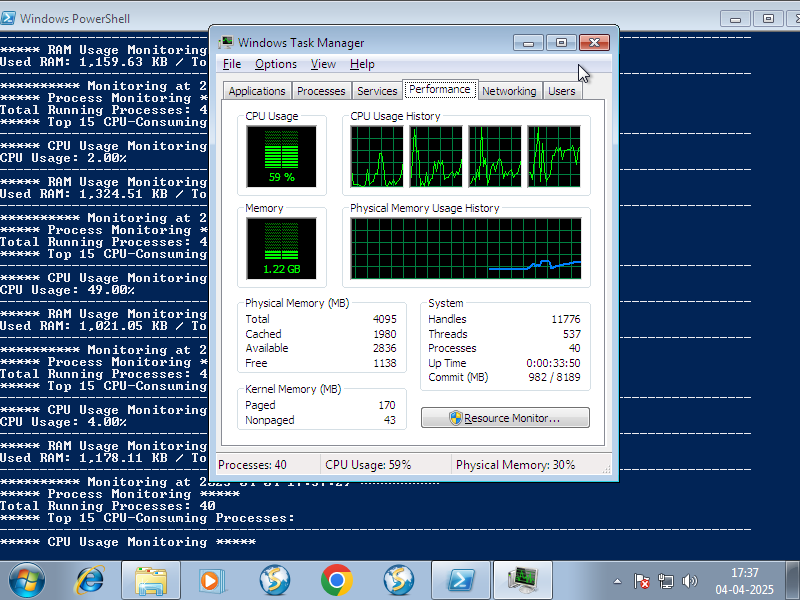
* **Malwares which manipulate the number of processes.**

1. **WannaCry**

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

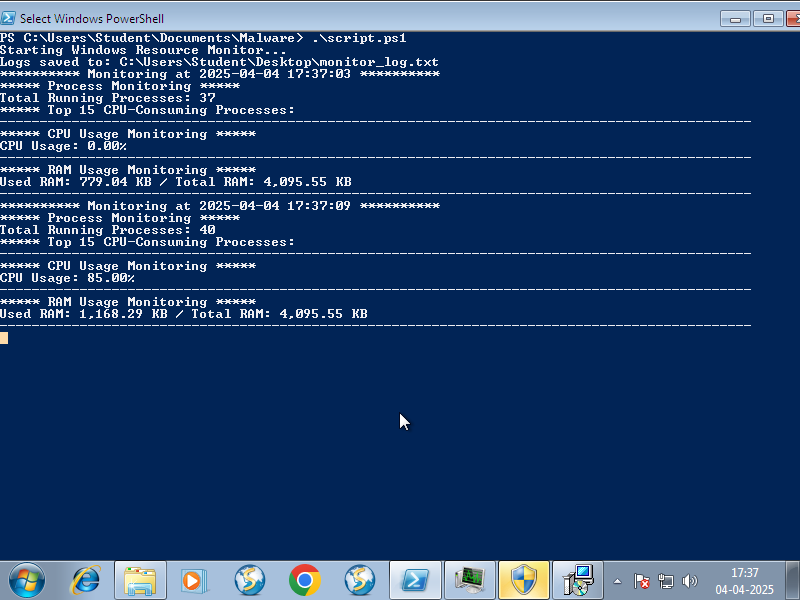


We verified this by using the task manager too:

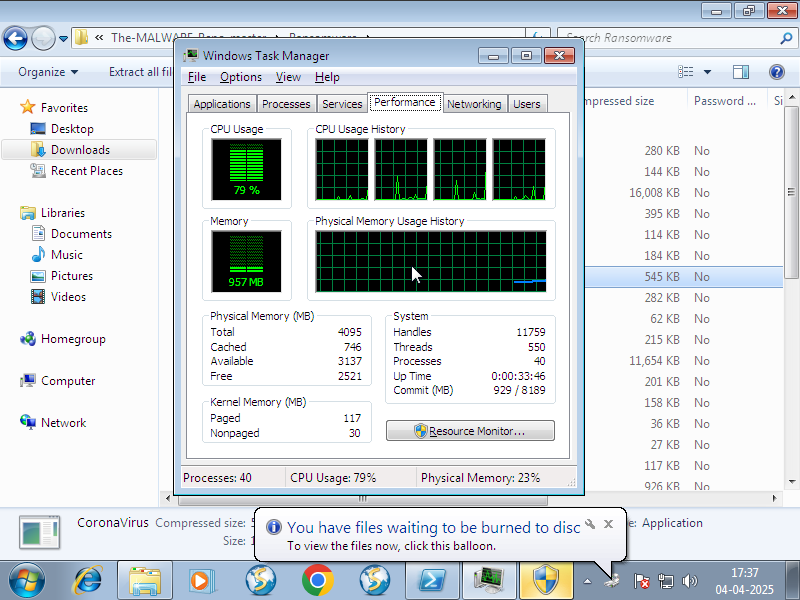


1. **CoronaVirus**

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

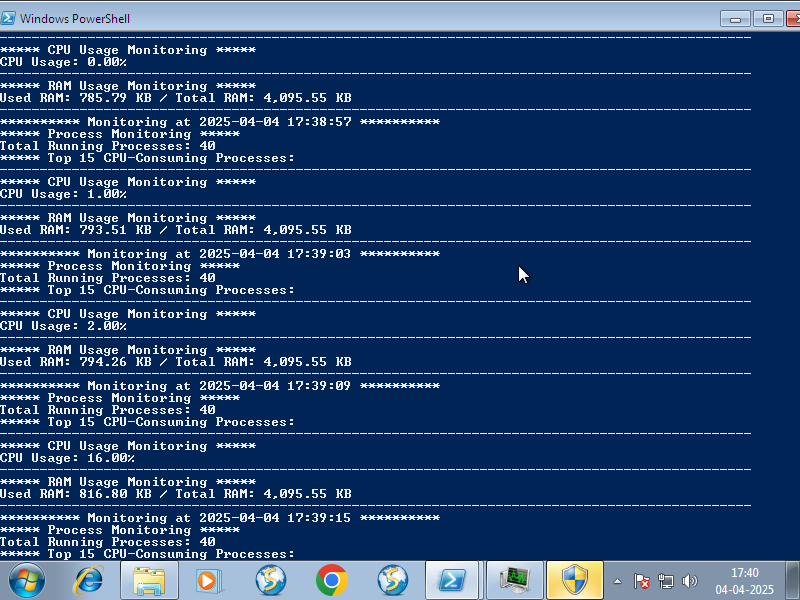


We verified this by using the task manager too:

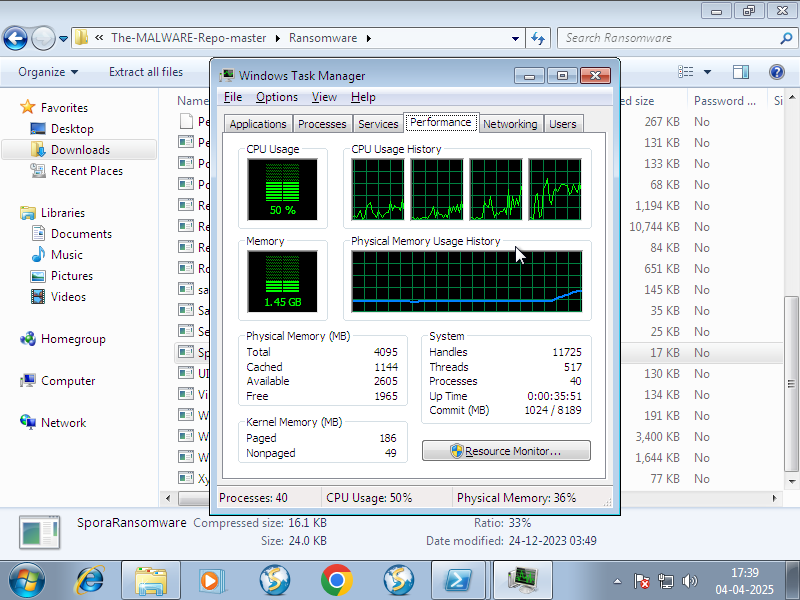


1. **SporaRansomware**

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

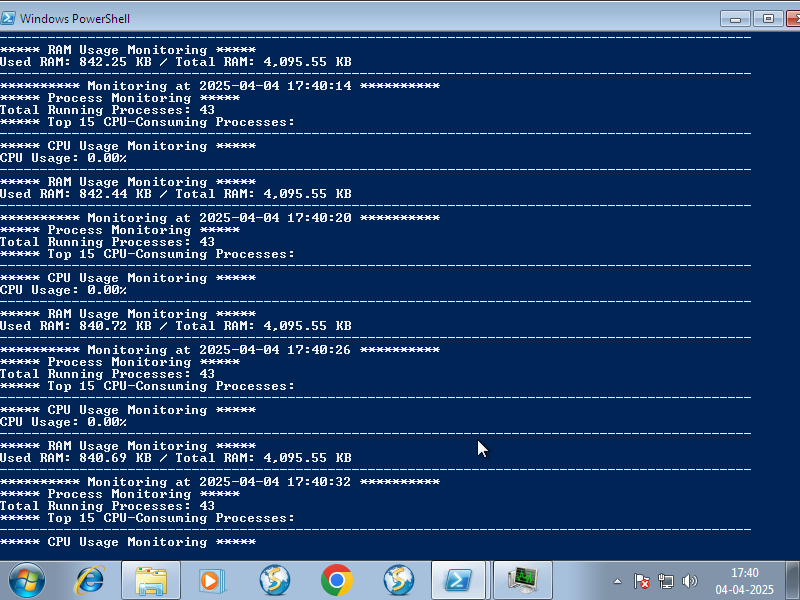


We verified this by using the task manager too:

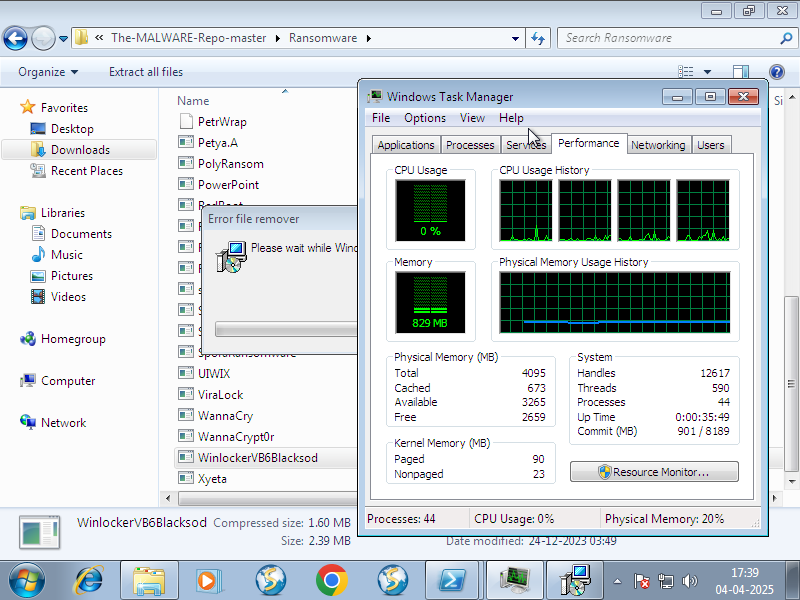


1. **WinlockerVB6Blacksod**

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

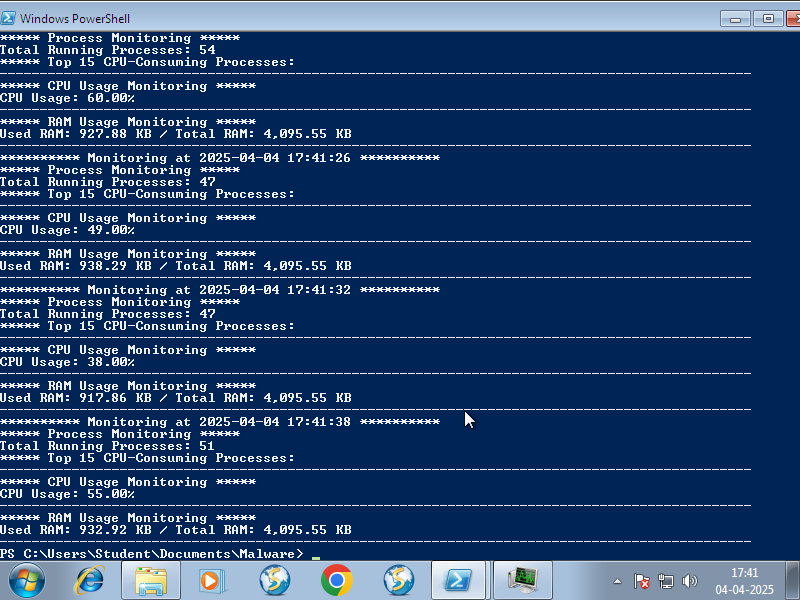


We verified this by using the task manager too:

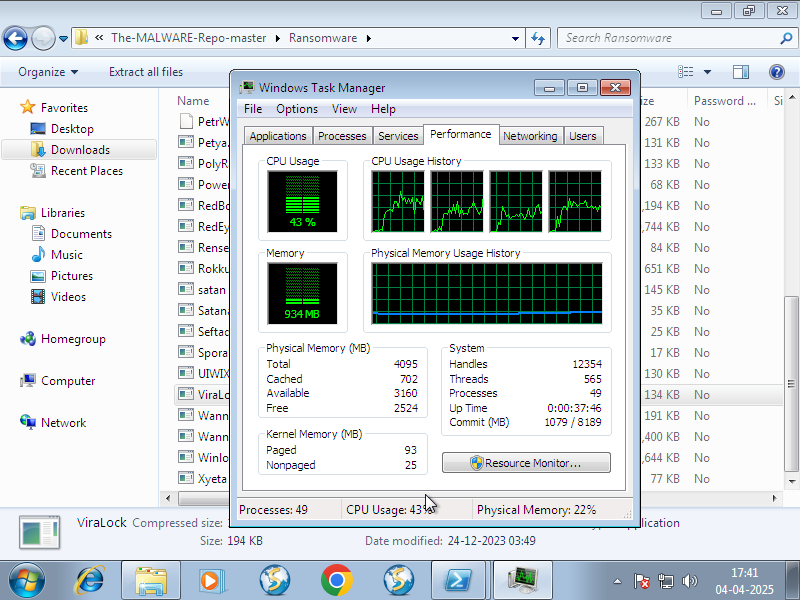


1. **ViraLock**

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



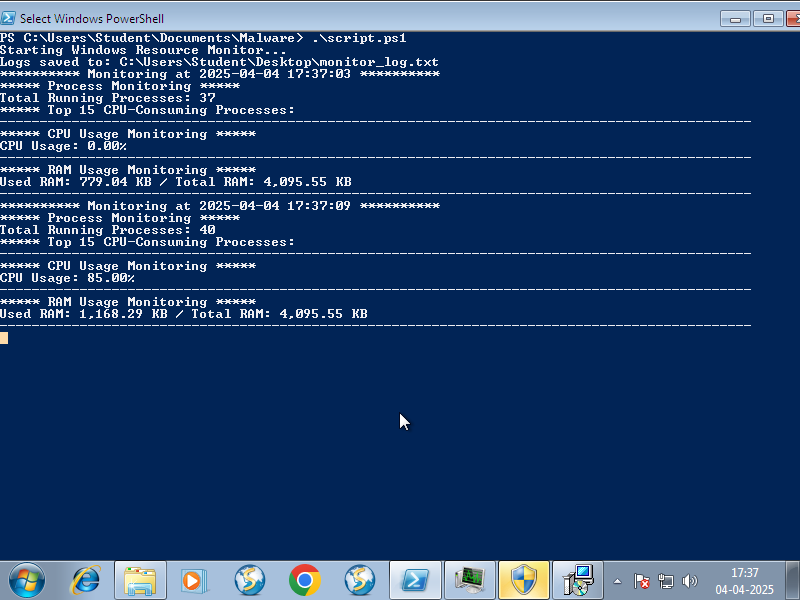
We verified this by using the task manager too:



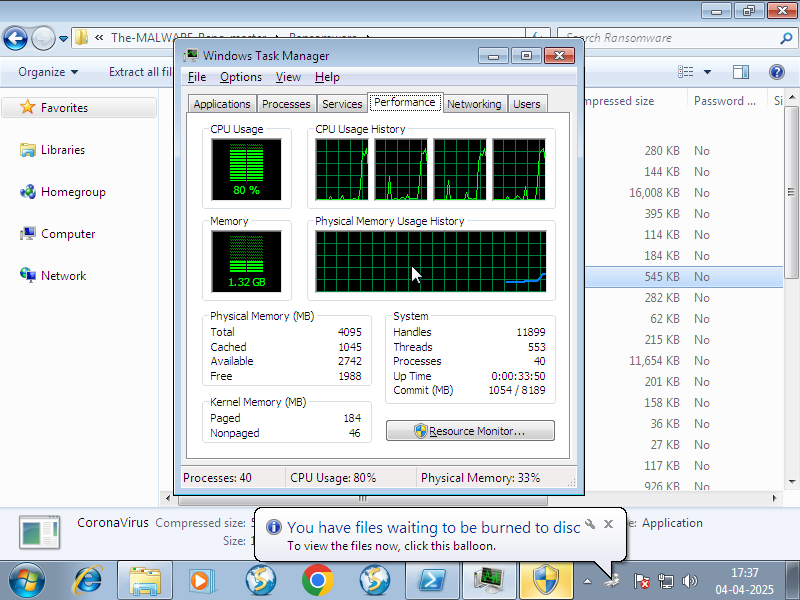
* **Malwares which manipulate the CPU usage.**

1. **CoronaVirus**

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



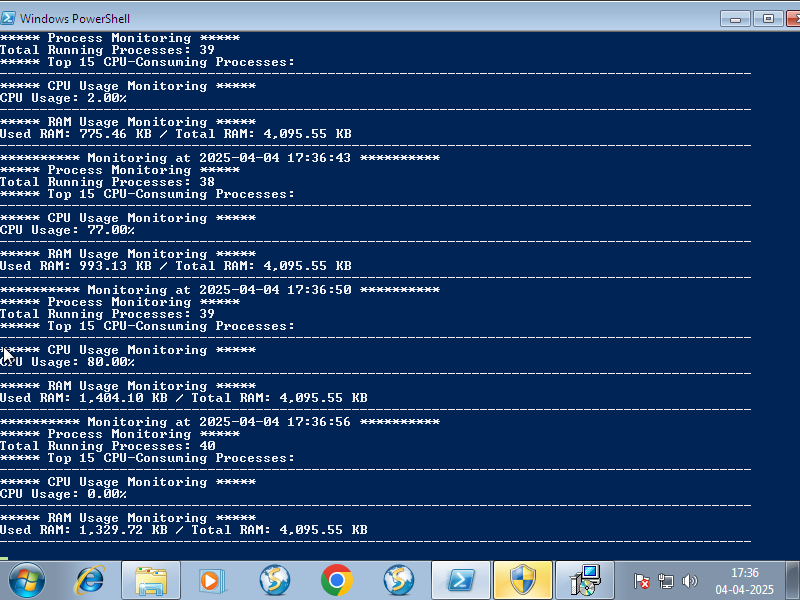
We verified this by using the task manager too:



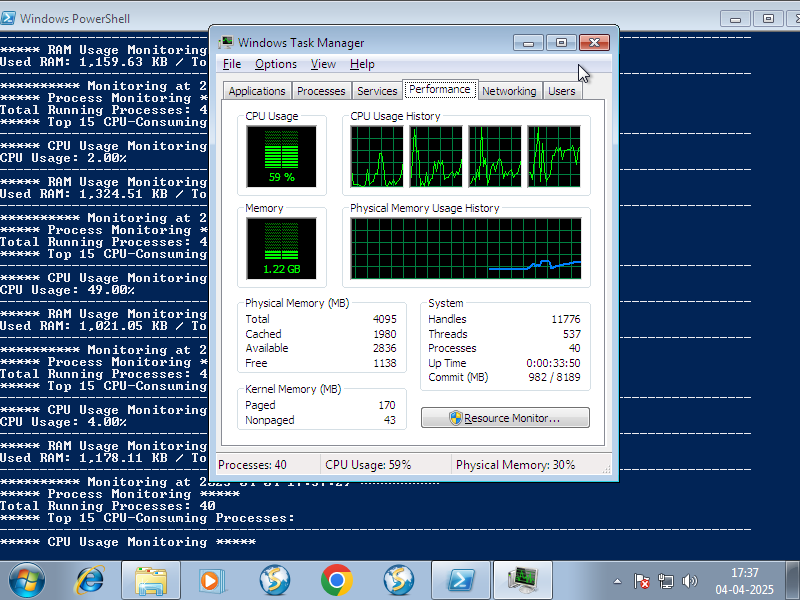
Then a dialogue box containing a message showed like this.  


1. **WannaCry**

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



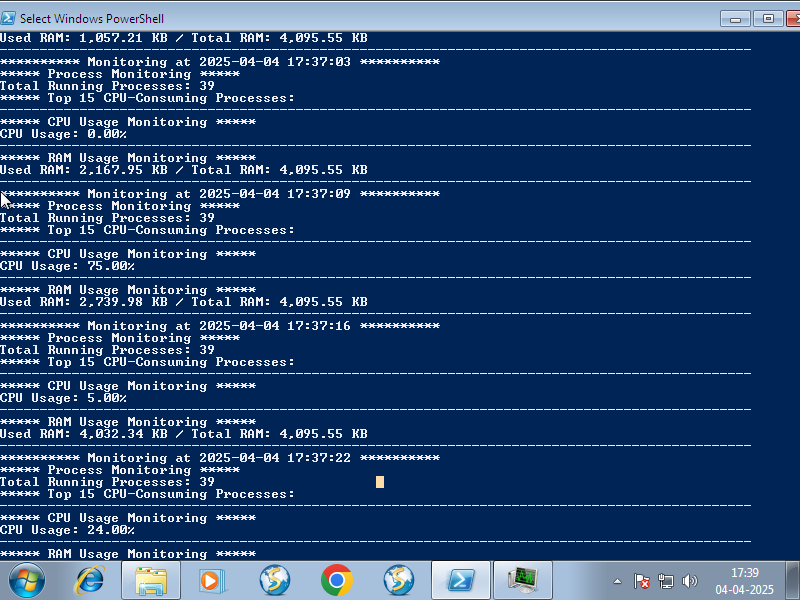
We verified this by using the task manager too:



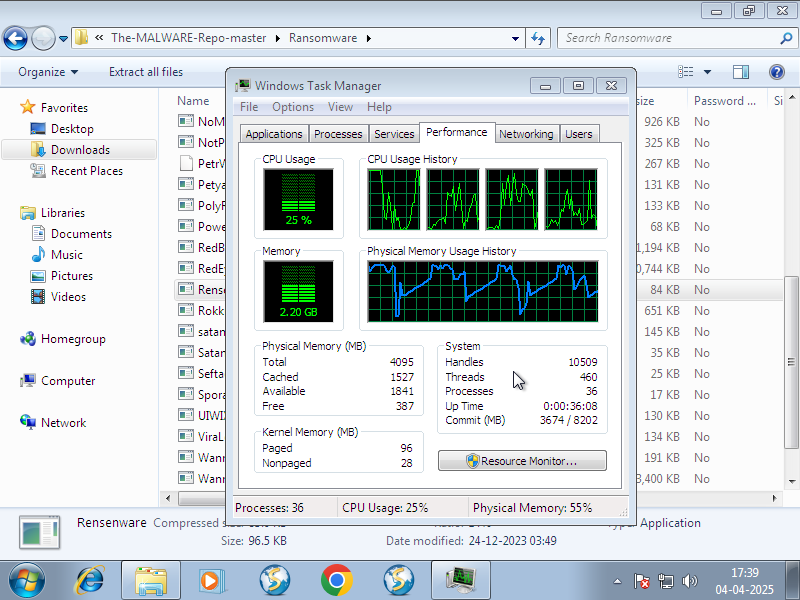
Then a window containing a message showed like this.  


1. **Rensenware**

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

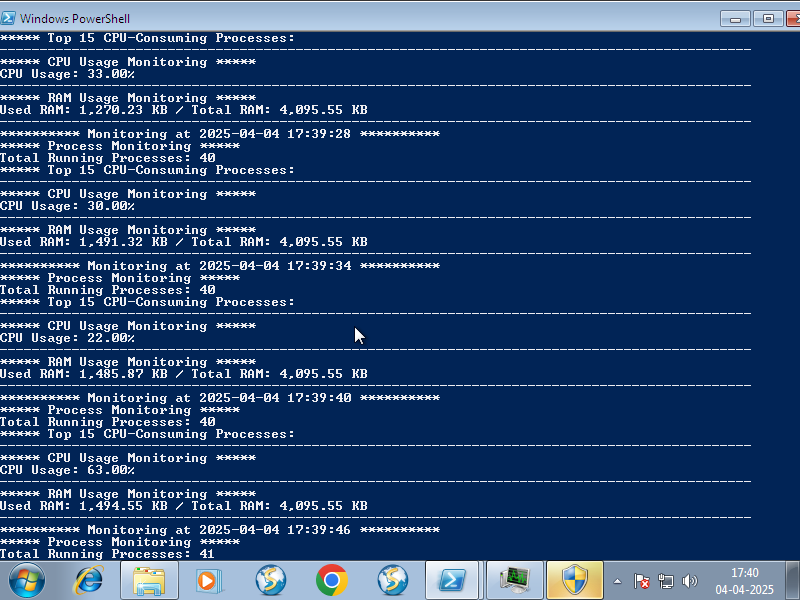


We verified this by using the task manager too:

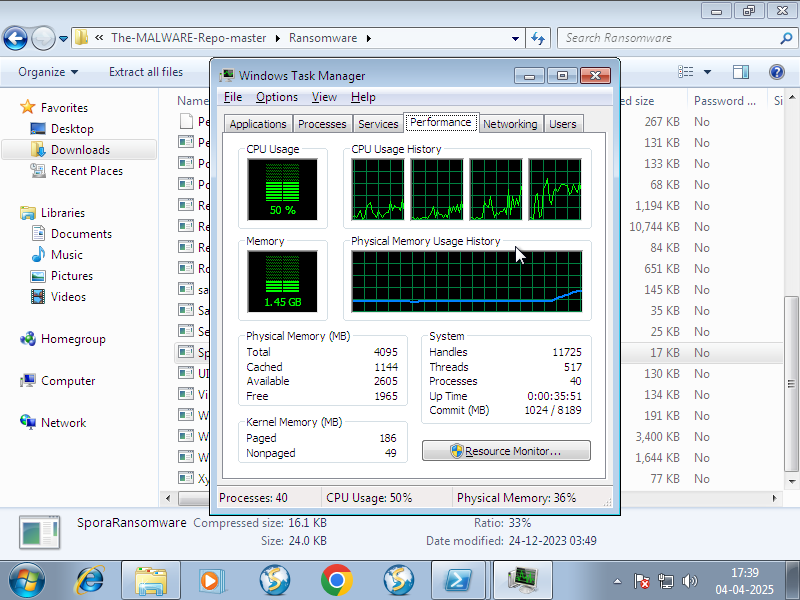


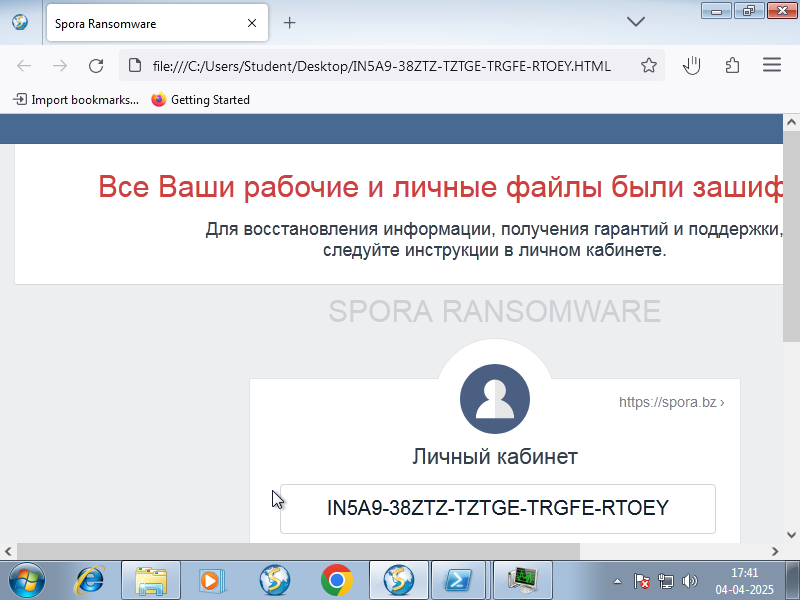
1. **SporaRansomware**

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



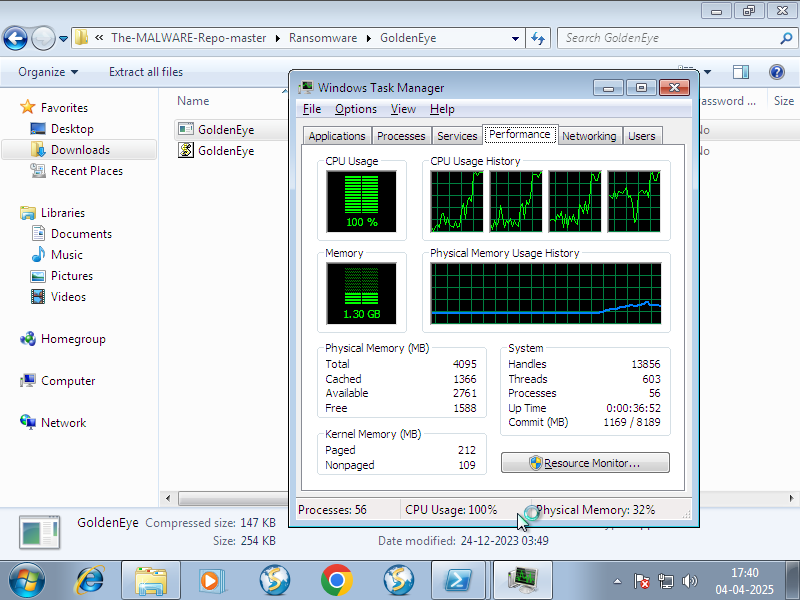
We verified this by using the task manager too:



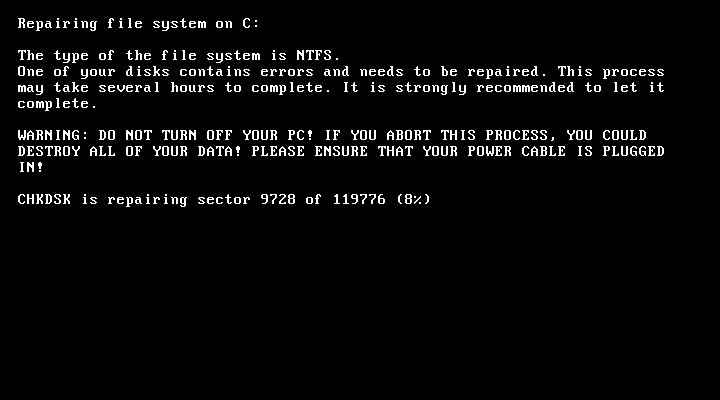
A window showed up which looked like this.  


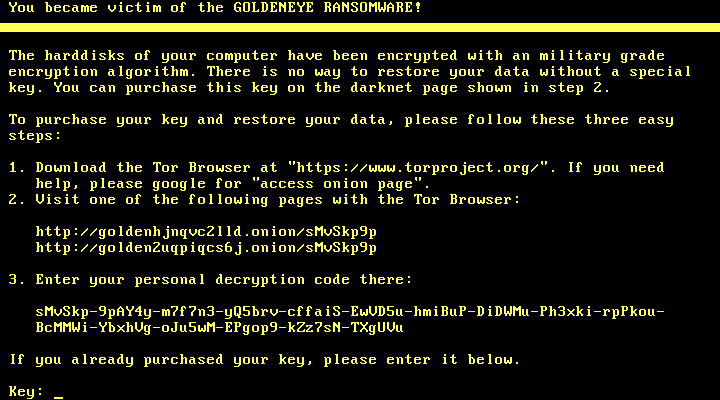
1. **GoldenEye**

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



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:

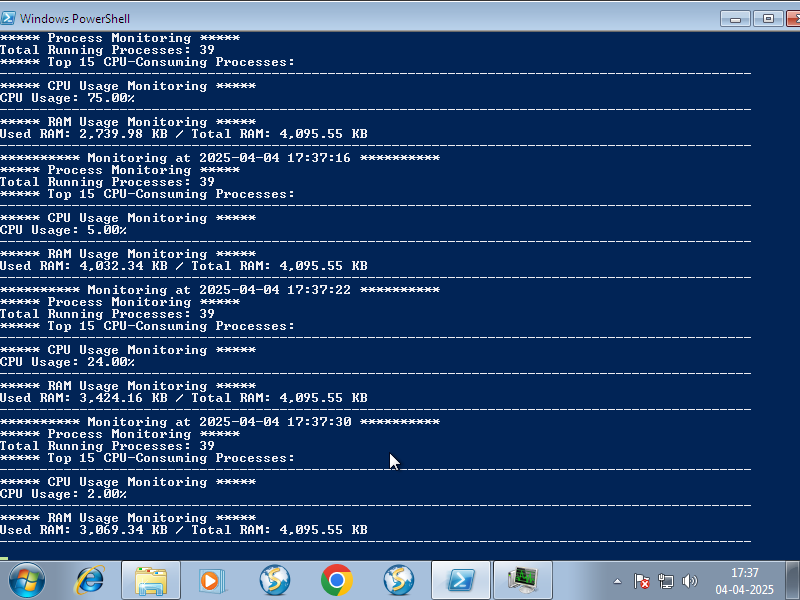




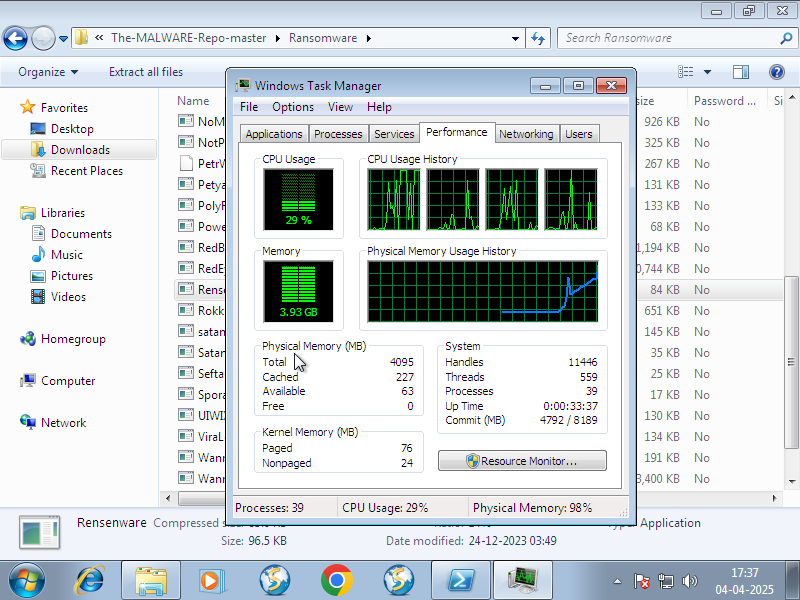
* **Malwares which manipulate the memory usage.**

1. **Rensenware**

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

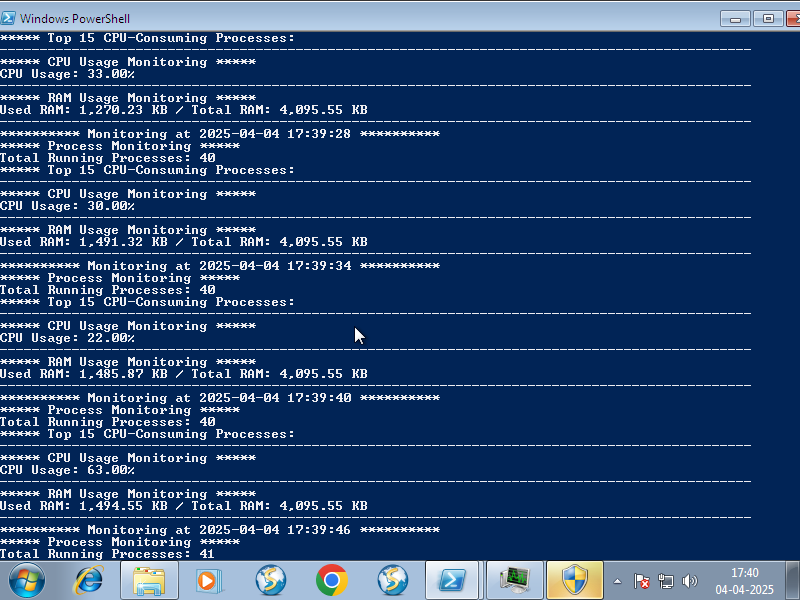


We verified this by using the task manager too:

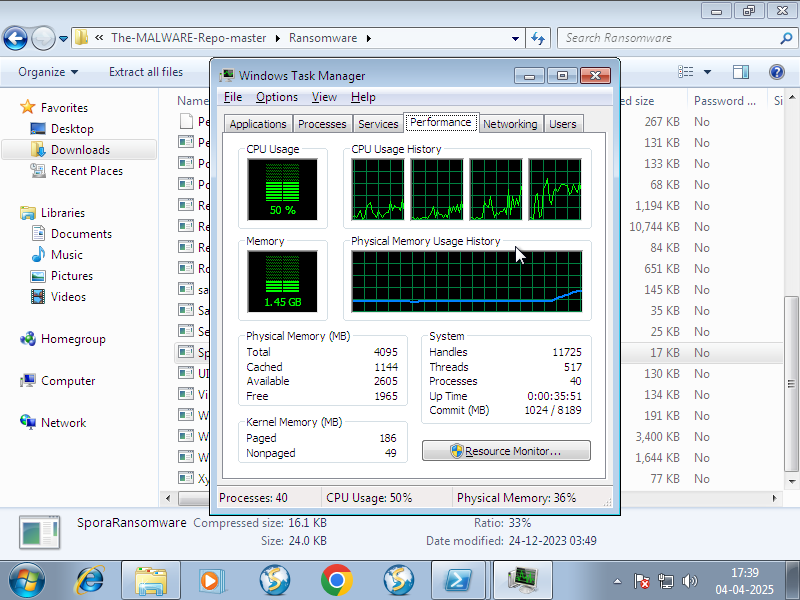


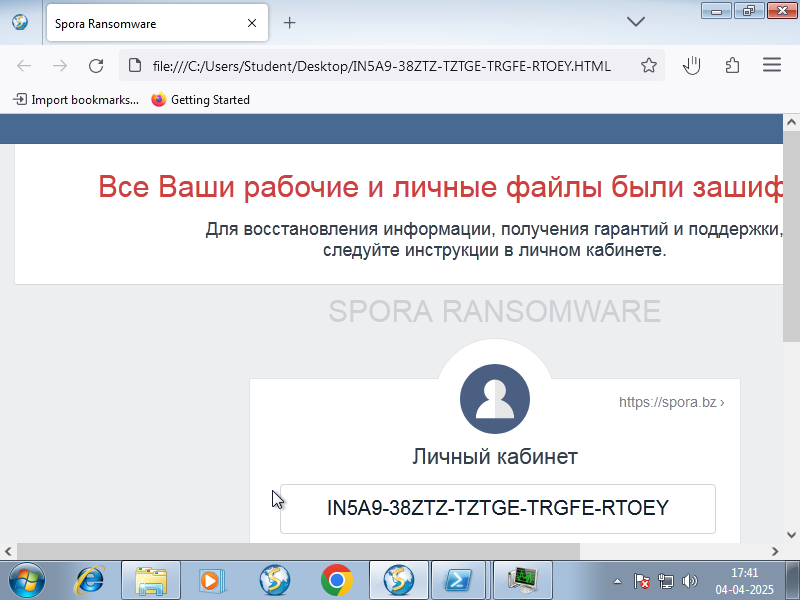
1. **SporaRansomware**

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



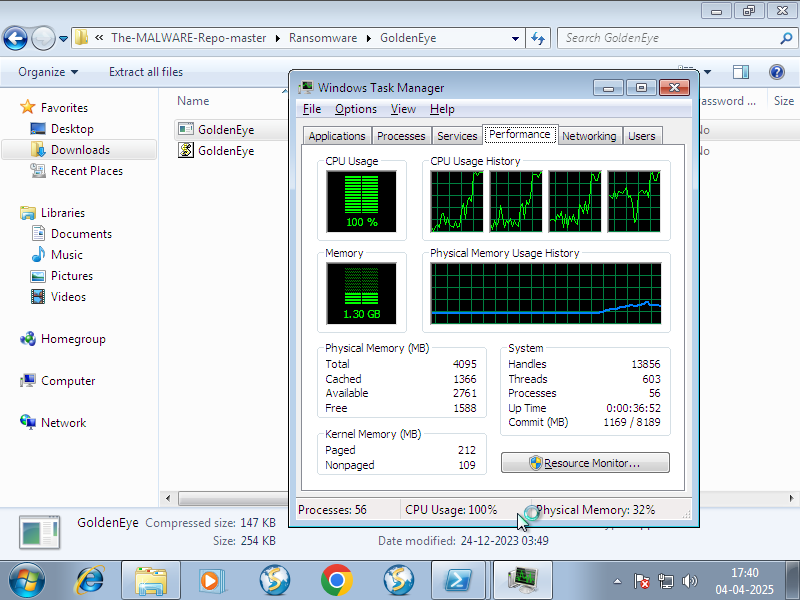
We verified this by using the task manager too:



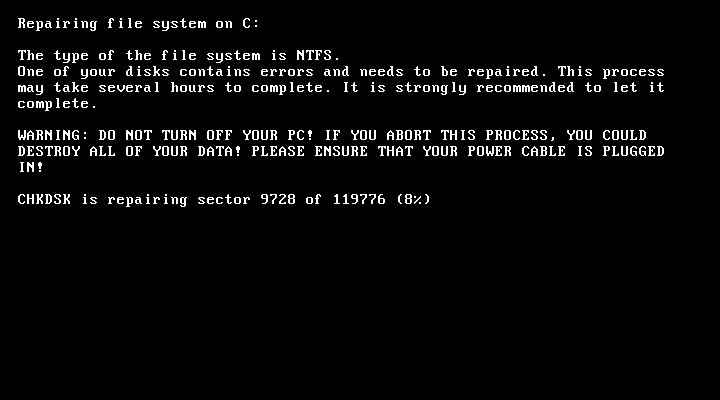
A window showed up which looked like this.  


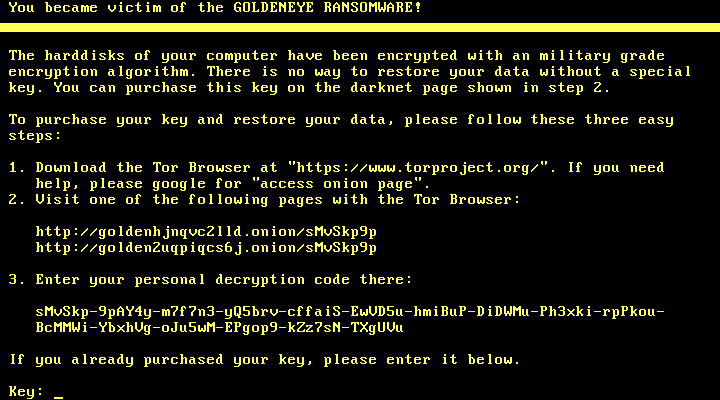
1. **GoldenEye**

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



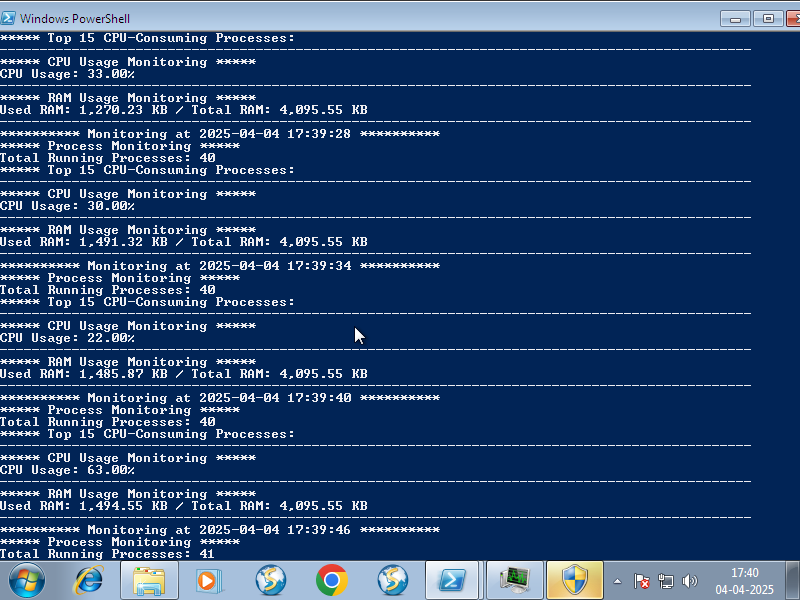
Unfortunately, we couldn’t see this using the PowerShell console because the system immediately got shut down and the following message appeared on the screen:



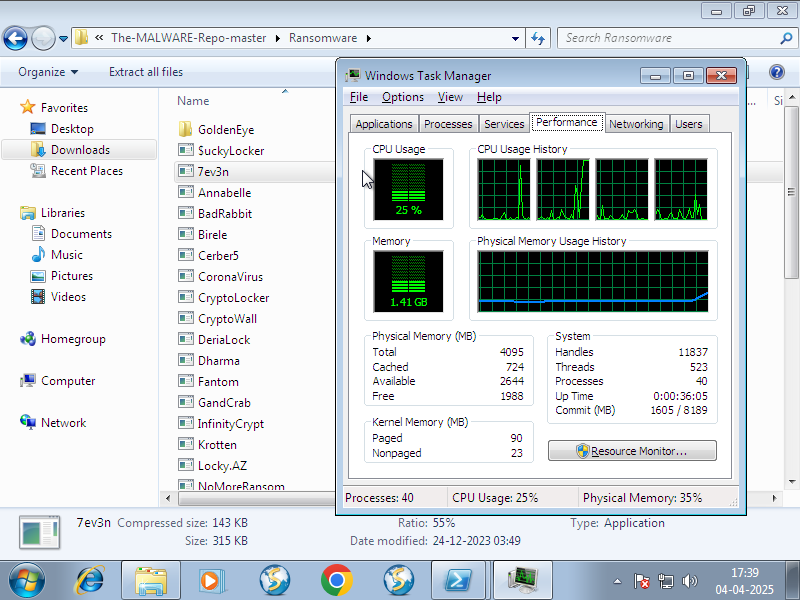


1. **7ev3n**

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

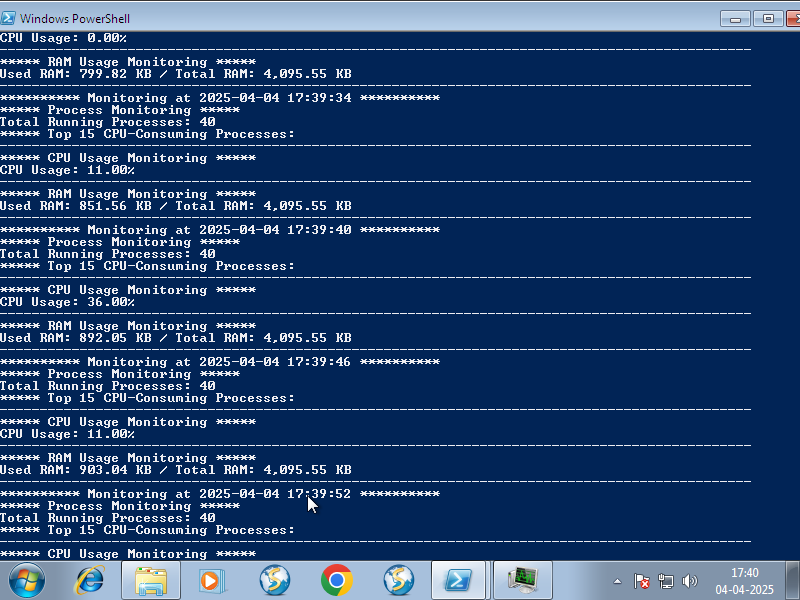


We verified this by using the task manager too:

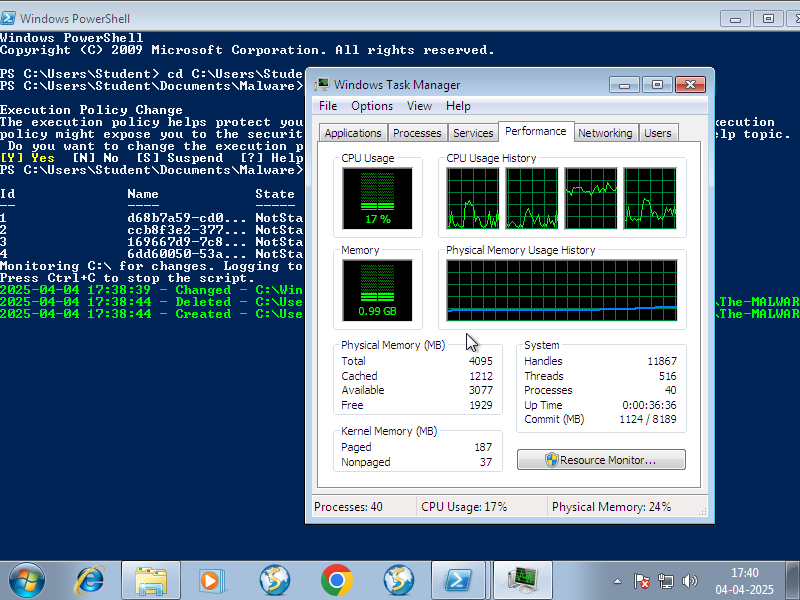


1. **GandCrab v5.2**

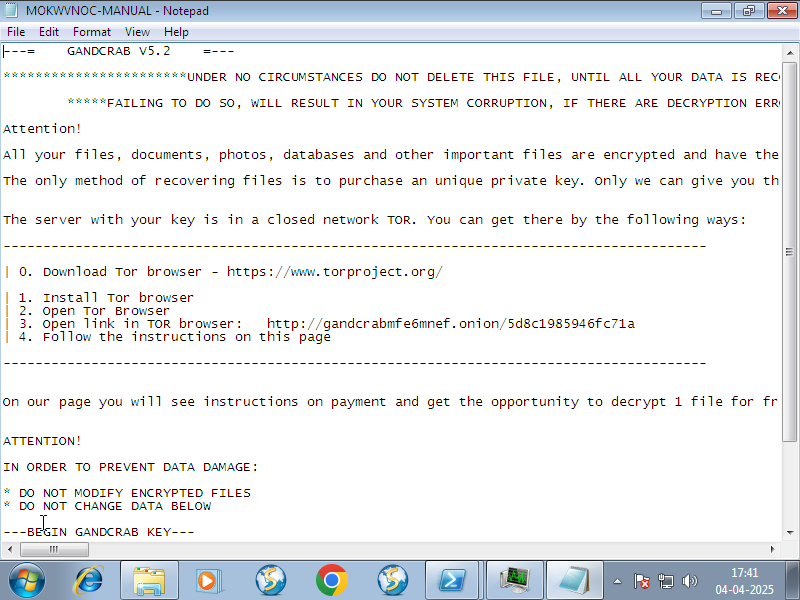
After executing the malware, we noticed that the PowerShell console showed a high memory usage.



We verified this by using the task manager too:



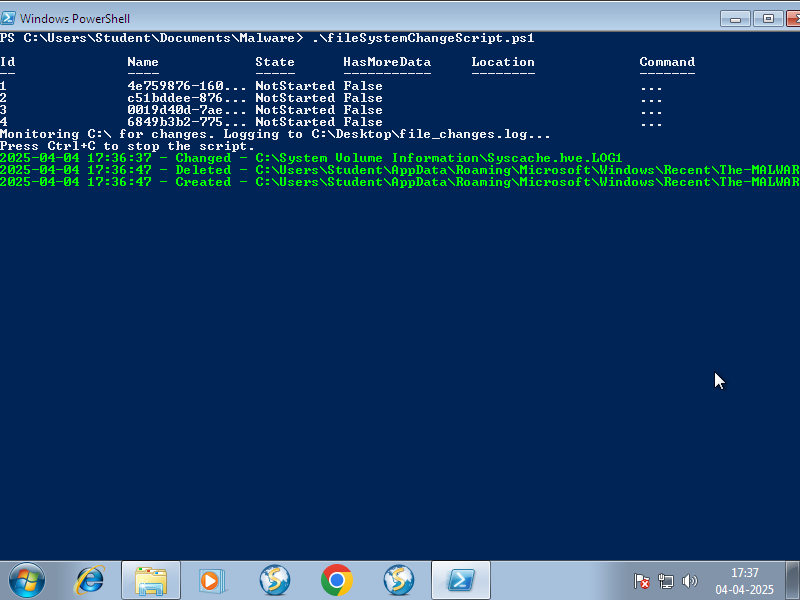
A file got created which had the following contents.

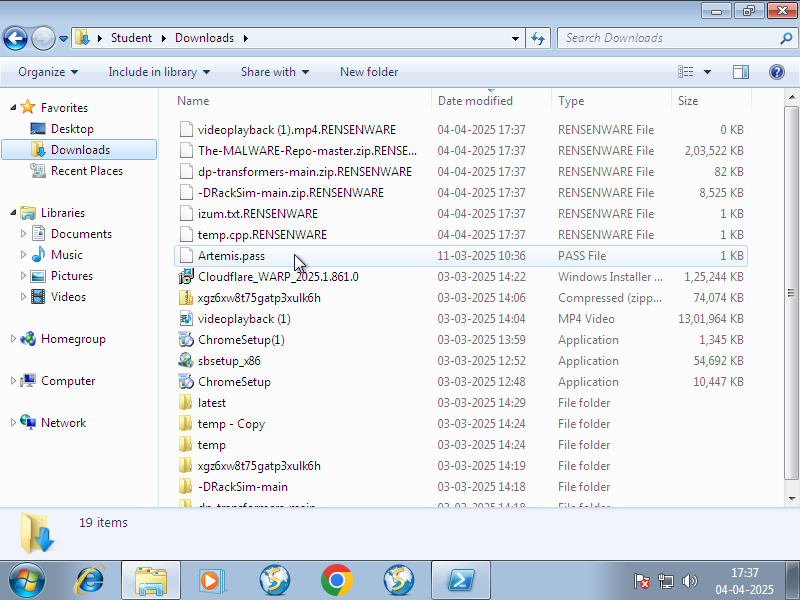


* **Malwares which manipulate the File system.**

1. **Rensenware**

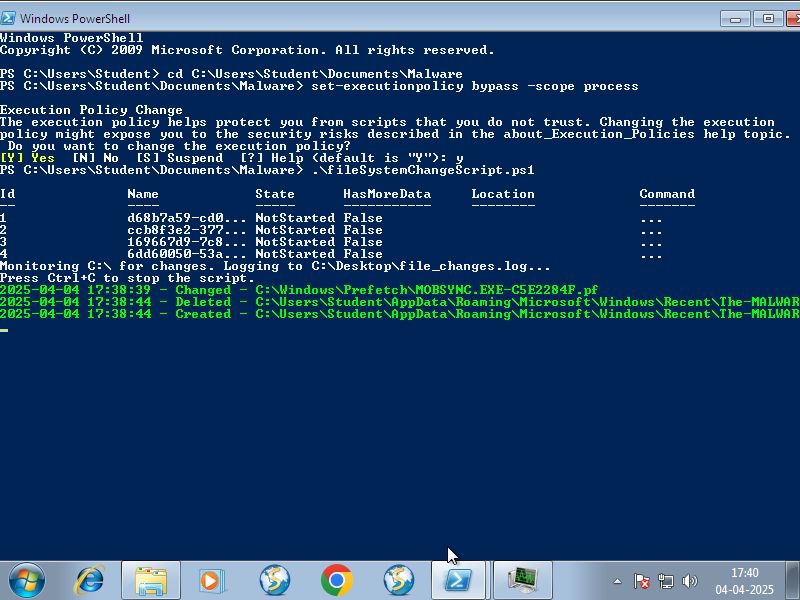
The script which was supposed to detect any changes in the file system showed this:

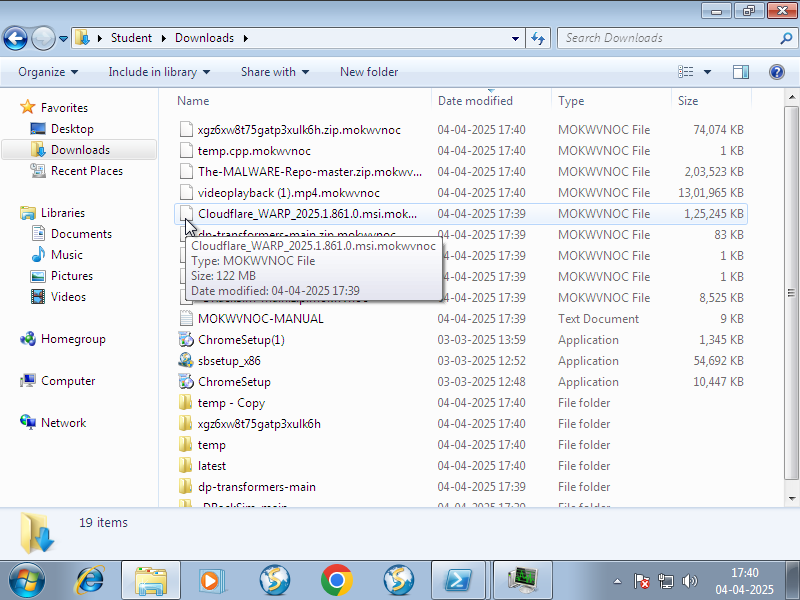


All the files in the File explorer were encrypted and looked like this.  


1. **GandCrab v5.2**

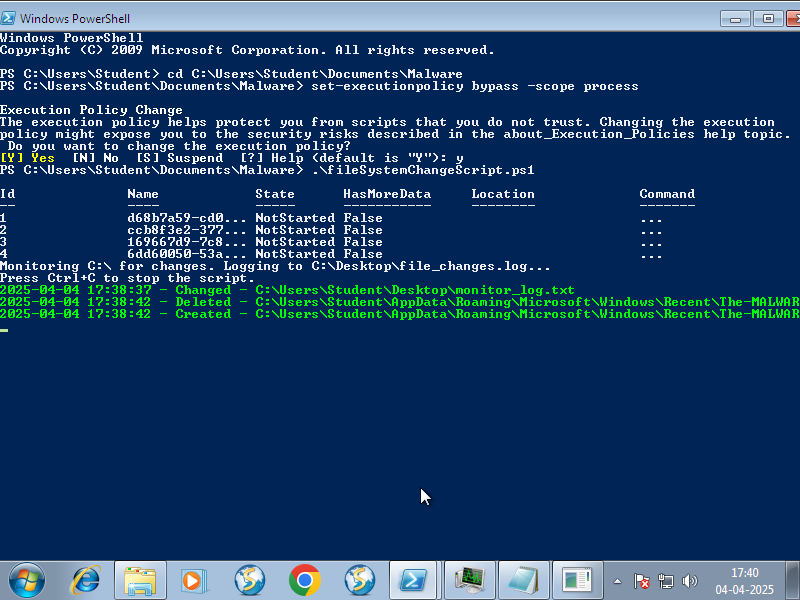
The script which was supposed to detect any changes in the file system showed this:

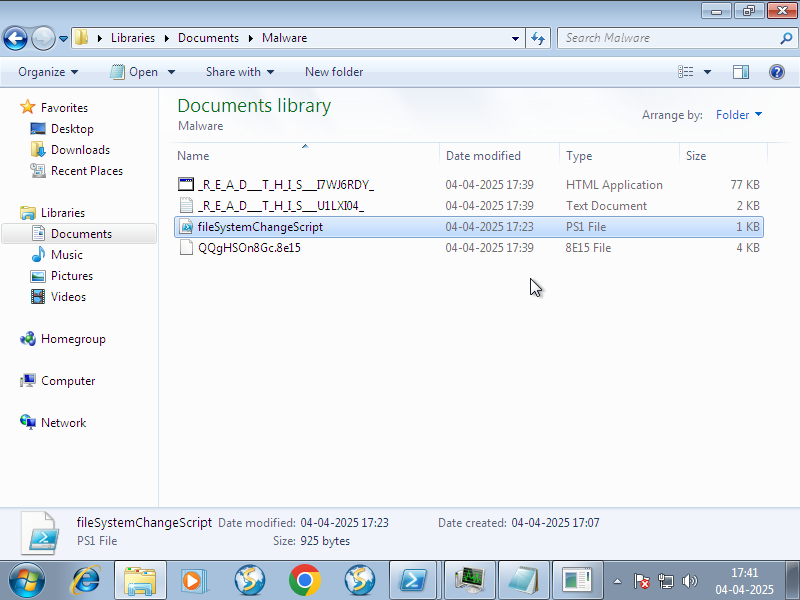


All the files in the File explorer were encrypted and looked like this.  


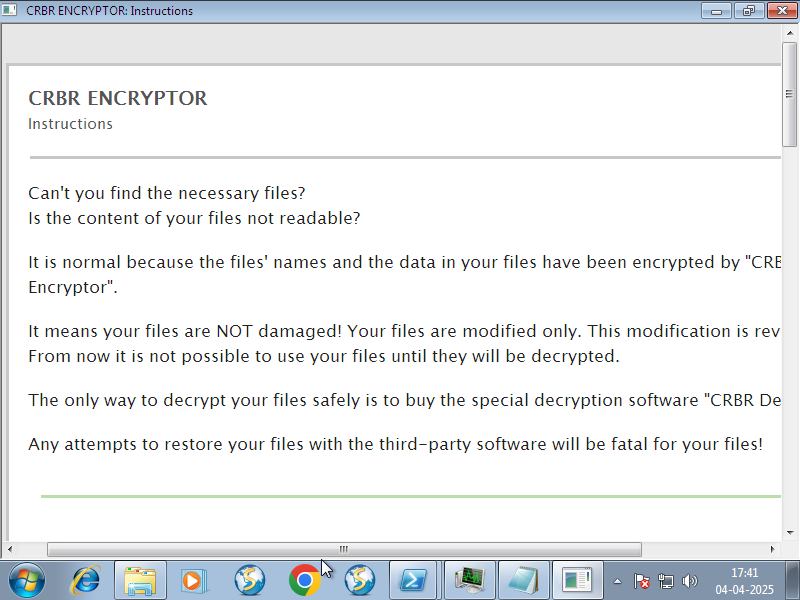
1. **Cerber**

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



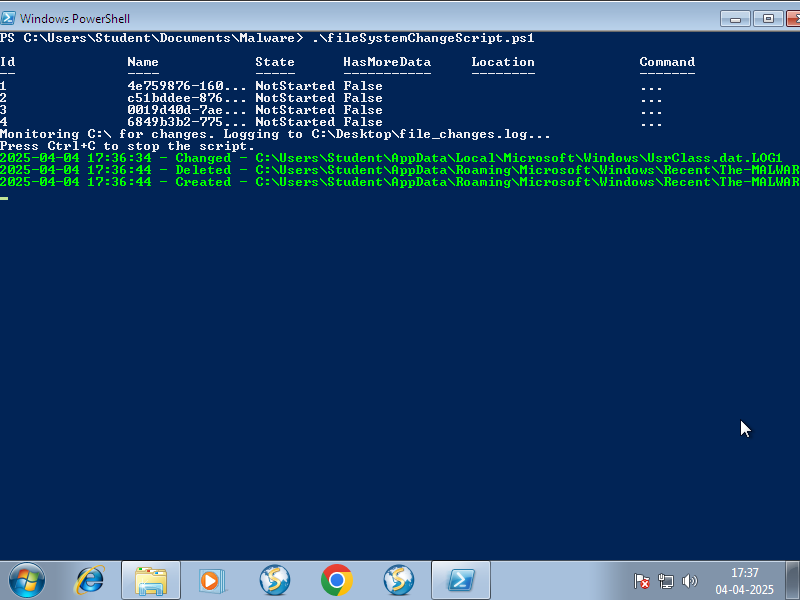
All the files in the File explorer were encrypted and looked like this.  


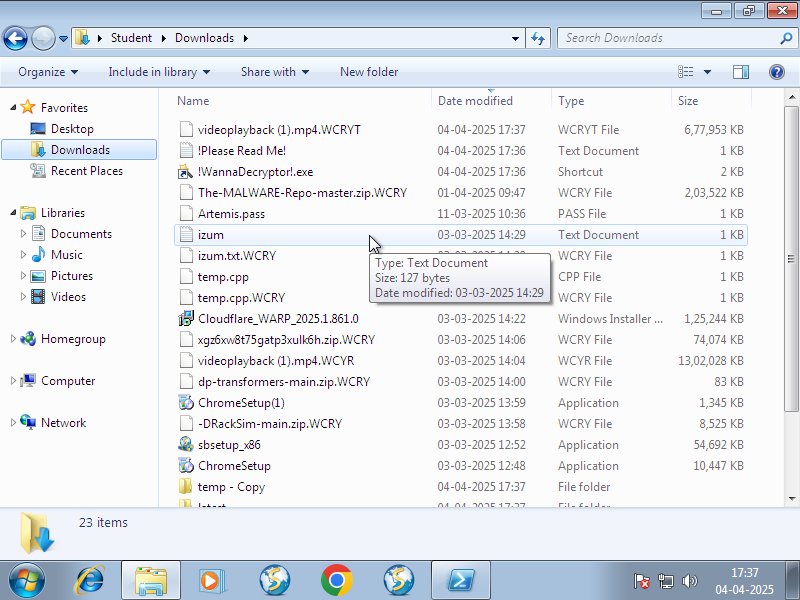
A pop-up window showed up which had the following contents.



1. **WannaCry**

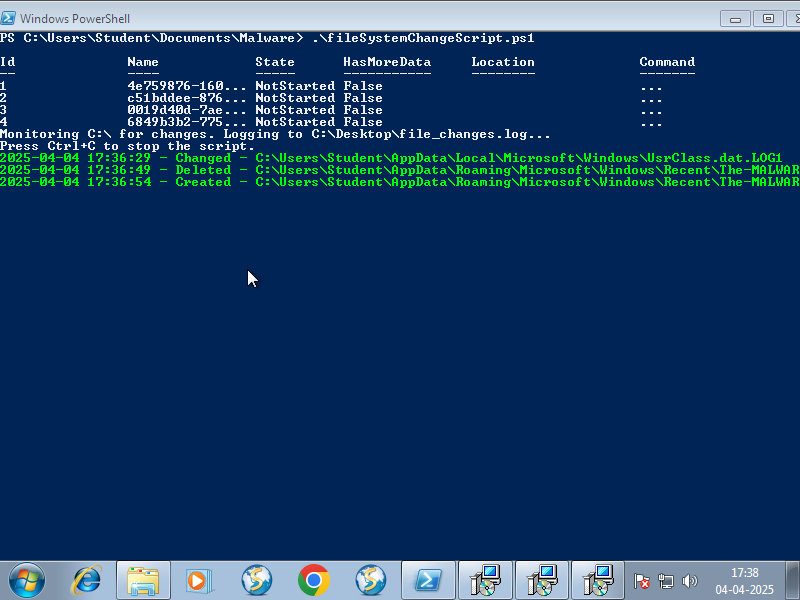
The script which was supposed to detect any changes in the file system showed this:



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


1. **CoronaVirus**

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



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