Ransomware Assignment

Name:- Etcharla Revanth Rao (24CS06010)

Ransomware

Ransomware is malware (malicious software). It is designed to **block access** to computers, devices, or data (by encrypting the data) **until a ransom is paid** to the attacker. The term **ransomware** is a combination of **"ransom" (payment demanded for release) and "software."**

How Ransomware Works

1. **Infection:** It can enter into a system through various methods like **phishing emails, removable media, exploits, etc.**
2. **Encrypting or Locking:** The ransomware encrypts files or locks access to the system.
3. **Ransom Demand:** Usually, a **message appears** on the screen, **informing the victim that files are locked (or encrypted) and demanding money.**
4. **Post-Payment (or No Payment):**
   - If the victim **pays**, they **may receive the decryption key.**
   - If they **don't pay,** the **data remains encrypted forever** or **may be leaked to the public.**

Steps to Simulate Ransomware

Step 1: Download **VirtualBox.**

Step 2: Install **Windows 7/XP ISO file** with **30 GB storage** and **4 GB RAM.**

Step 3: Install malware from **Zoo-master** or other sources.

Step 4: Take a system snapshot before running any ransomware.

Step 5: Run a **monitoring script** that captures:

- **Number of processes**
- **CPU utilization**
- **RAM usage**
- **Other system statistics**

Step 6: Install and **execute ransomware**, then capture changes in CPU, memory, and system processes. **After testing, restore the system snapshot.**

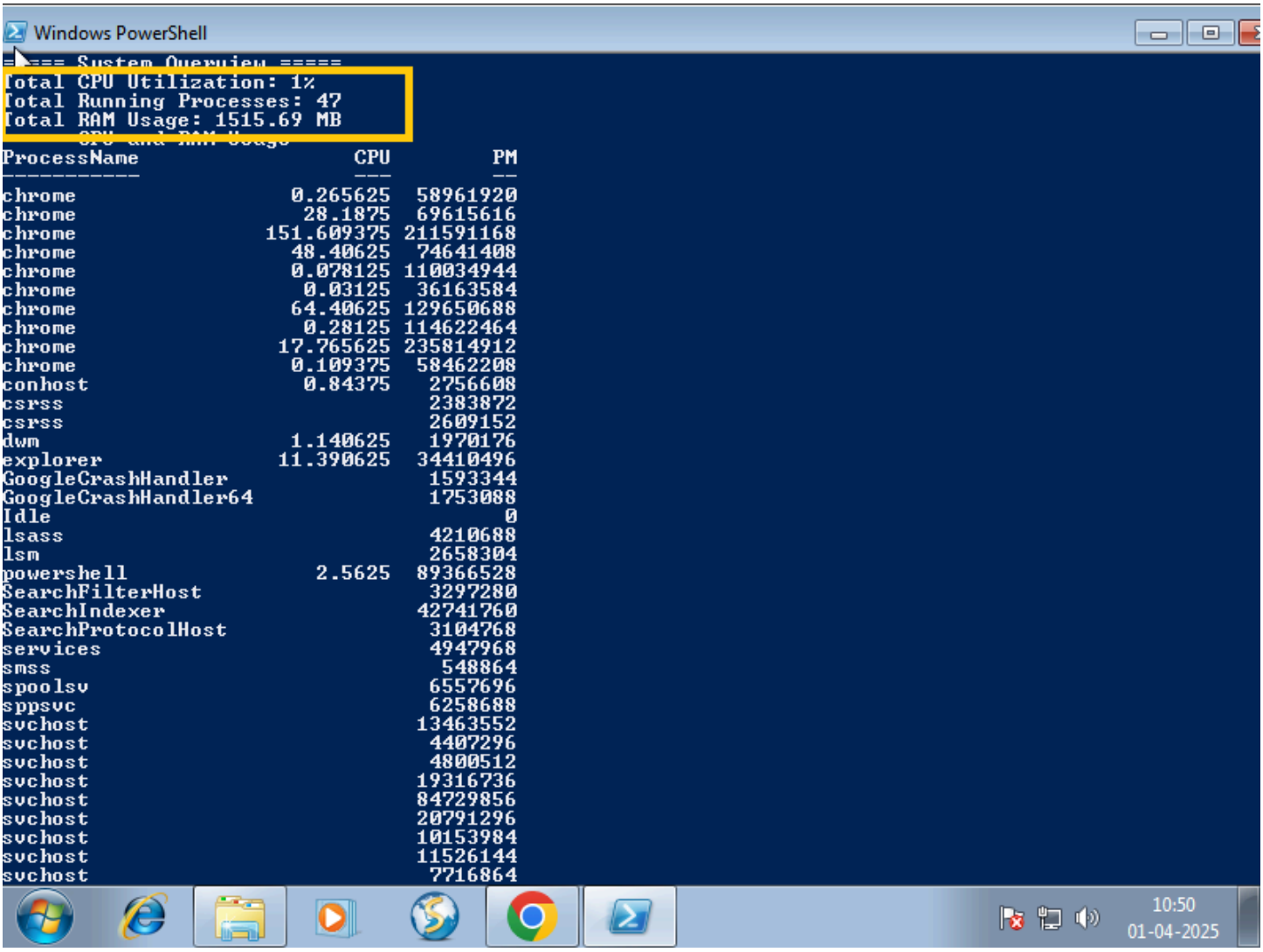
The Monitoring Script Captures:

✔ **CPU Utilization** – Uses Get-WmiObject Win32_Processor to calculate the average CPU load percentage.
✔ **Process Count** – Counts running processes using (Get-Process).Count.

✔ **Memory Usage & RAM Usage** – Monitors available system memory.
✔ **System Processes** – Lists **process names, IDs, and CPU usage.**
✔ **Disk Usage** – Retrieves **drive details** (total size, free space).
✔ **Logs system state every 5 seconds** and saves the information in a log file.

→ BEFORE RUNNING ANY RANSOMWARE

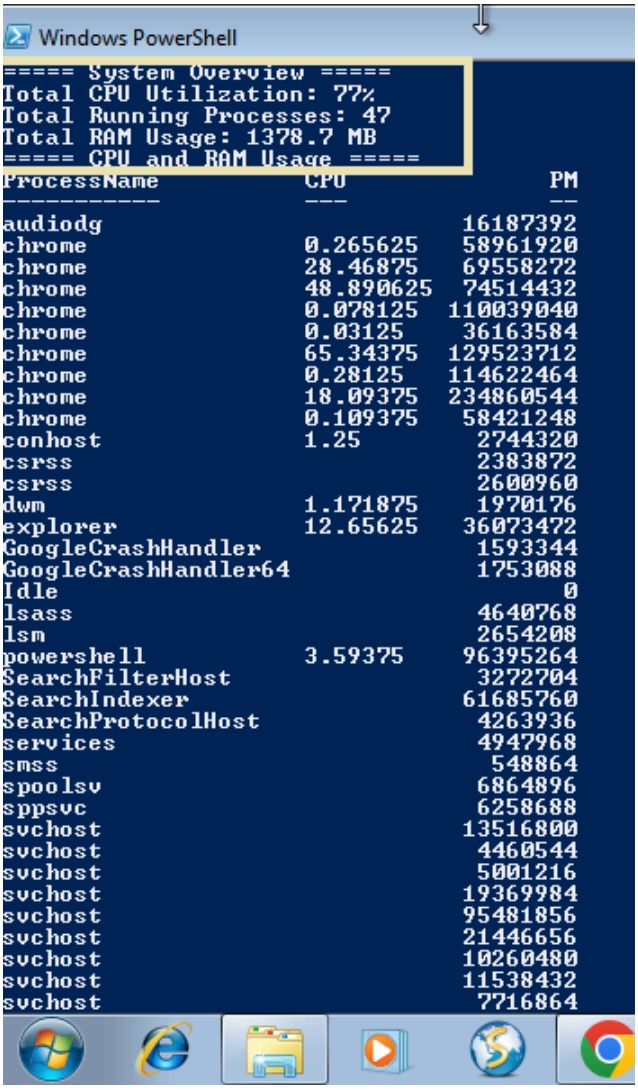
The state of the system (CPU utilization, memory usage, and running processes) should be recorded to analyze the impact of ransomware.

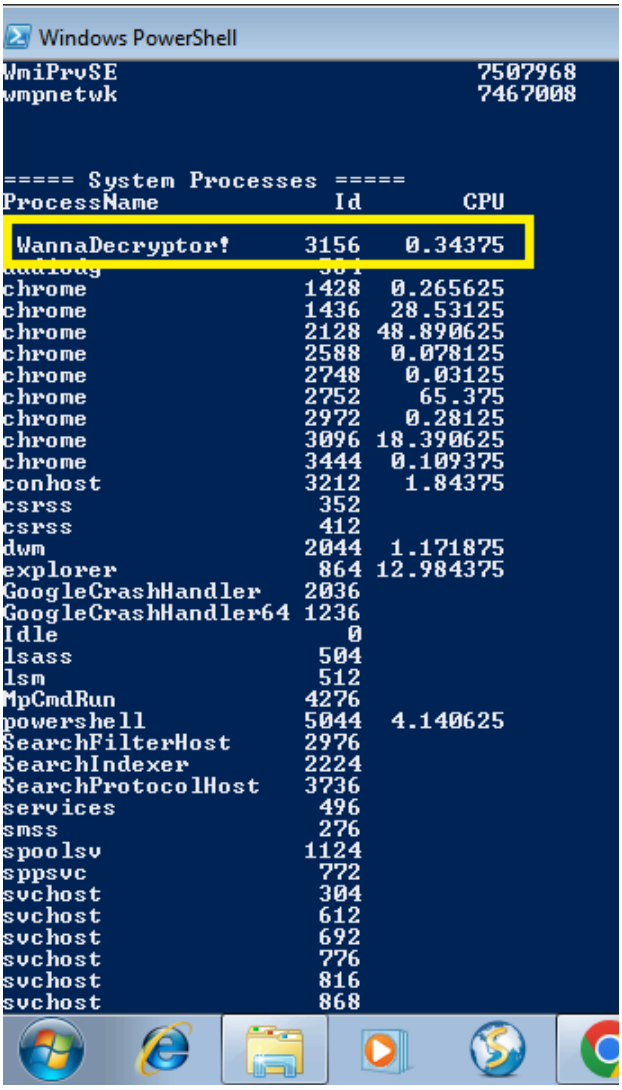


1. **WANNACRY RANSOMWARE**

After running wannacry ransomware we observer the following :

This is the message i got after runny Wannacry exe file on my Virtual box (windows 7).All my files are encrypted. This is popping up simultaneously.





From the above analysis we can say that

1. **High CPU usage (77%)** : WannaCry's encryption of data and its attempts to spread via SMB likely caused the significant CPU spike, as these process are resource-intesive.
2. **Process Count** : New process are being created by the Wanncry. Also it does renaming files with .WCRY
3. **RAM Impact** : No significant change is observed in the ram usage.
4. **Notable Behavior**: All the files in the system are encrypted, Duplication of process with same name.
5. **Unusual process Activity** : It interfered with system process and caused chrome to crash.

2.CORONAVIRUS

Windows PowerShell

```
===== System Overview =====
Total CPU Utilization: 2%
Total Running Processes: 49
Total RAM Usage: 1320.73 MB
===== CPU and RAM Usage =====
ProcessName          CPU                PM
-----------          ---                --
audiodg                            16265216
chrome               0.28125       58961920
chrome               28.578125     69324800
chrome               48.90625      74514432
chrome               0.078125     110039040
chrome               0.03125       36163584
chrome               65.640625    129609728
chrome               0.28125      114622464
chrome               18.578125    226930688
chrome               0.109375      58421248
conhost              1.59375        2760704
CoronaVirus                        40726528
csrss                               2383872
csrss                               2605056
dwm                  1.171875       1970176
explorer             13.796875     37224448
GoogleCrashHandler                  1593344
GoogleCrashHandler64                1753088
Idle                                      0
lsass                               4444160
lsm                                 2658304
mshta                               3887104
mshta                               3878912
powershell           4.1875        62185472
services                            5029888
smss                                 548864
spoolsv                             6557696
sppsvc                              6258688
svchost                             1687552
svchost                            13590528
svchost                             4521984
svchost                             5074944
svchost                            19578880
svchost                            94076928
svchost                            30273536
svchost                            11595776
svchost                            11657216
```

10:54
01-04-2025

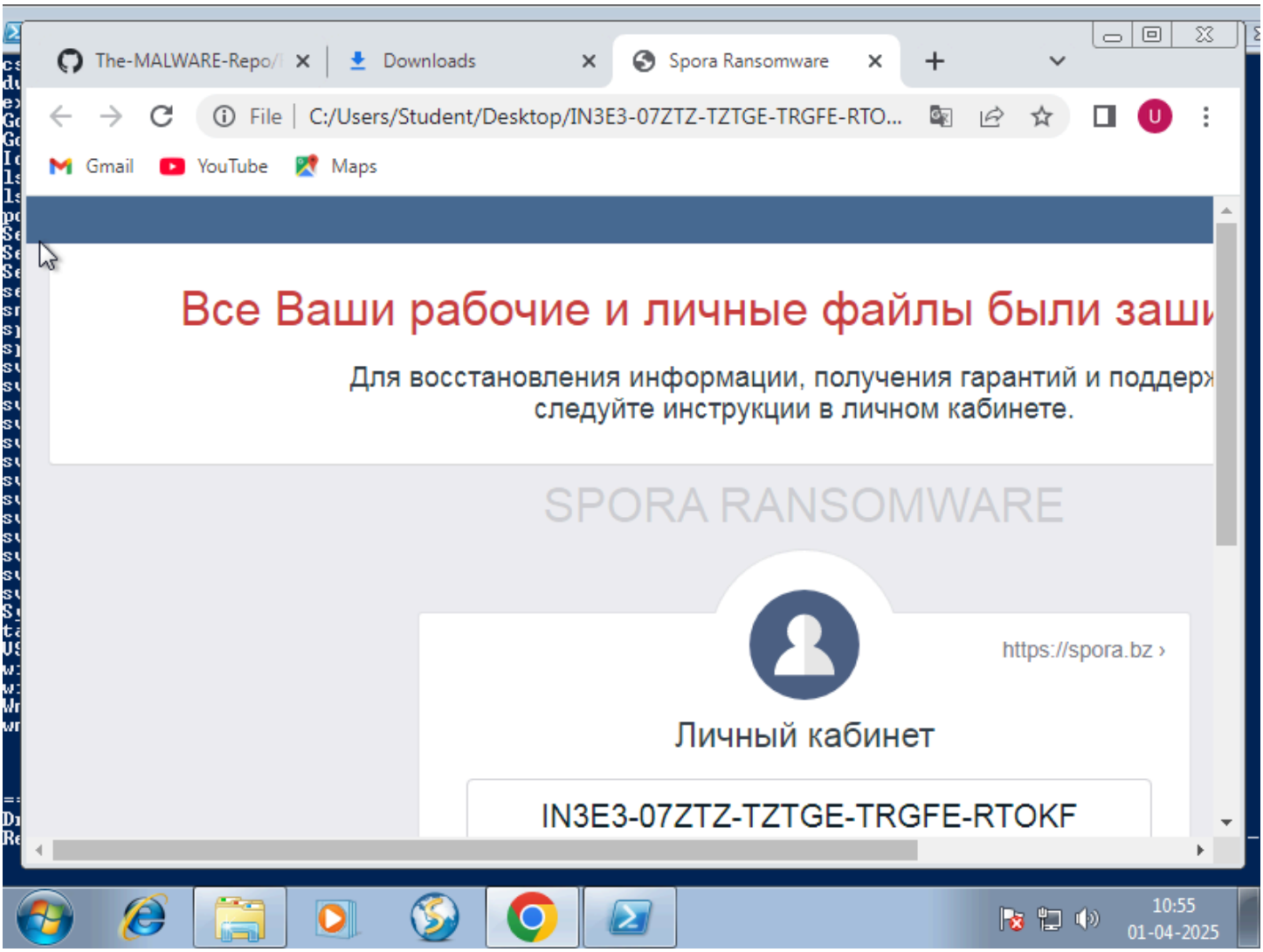
1. **Process Manipulation:** Added **"CoronaVirus"** process.
2. **System Impact:** No significant **CPU usage** increase (**Total CPU Utilization remains at 0%**).
3. **RAM Impact: 407.65 MB** (Moderate increase due to ransomware activity).
4. **Process Count: 49 processes**.
5. **Notable Behavior: Files are encrypted and inaccessible.**
6. The ransomware **displays a ransom note** demanding **Bitcoin payment** for decryption.

3.SPORA

Windows PowerShell

```
===== System Overview =====
Total CPU Utilization: 59%
Total Running Processes: 48
Total RAM Usage: 1418.33 MB
===== CPU and RAM Usage =====
ProcessName          CPU              PM
-----------          ---              --
audiodg                            16134144
chrome               0.265625      58953728
chrome               29.1875       69632000
chrome               50.234375     70852608
chrome               0.03125       36208640
chrome               68.296875    128167936
chrome               3.09375      162648064
chrome               0.109375      58462208
chrome               0.734375     120868864
chrome               1            140128256
chrome               0.078125     110166016
conhost              0.796875       3092480
csrss                               2383872
csrss                               2609152
dwm                  1.21875        1970176
explorer             12.765625     33468416
GoogleCrashHandler                  1593344
GoogleCrashHandler64                1753088
Idle                                      0
lsass                               4284416
lsm                                 2654208
powershell           3.046875      79601664
SearchFilterHost                    3682304
SearchIndexer                      56254464
SearchProtocolHost                  3035136
services                            5255168
smss                                 548864
spoolsv                             6552696
SporaRansomware (1)  16.03125       9732096
sppsvc                              6258688
svchost                            13459456
svchost                             4395008
svchost                             5292032
svchost                            19427328
svchost                            88240128
svchost                            30134272
svchost                            10420224
```

10:54
01-04-2025



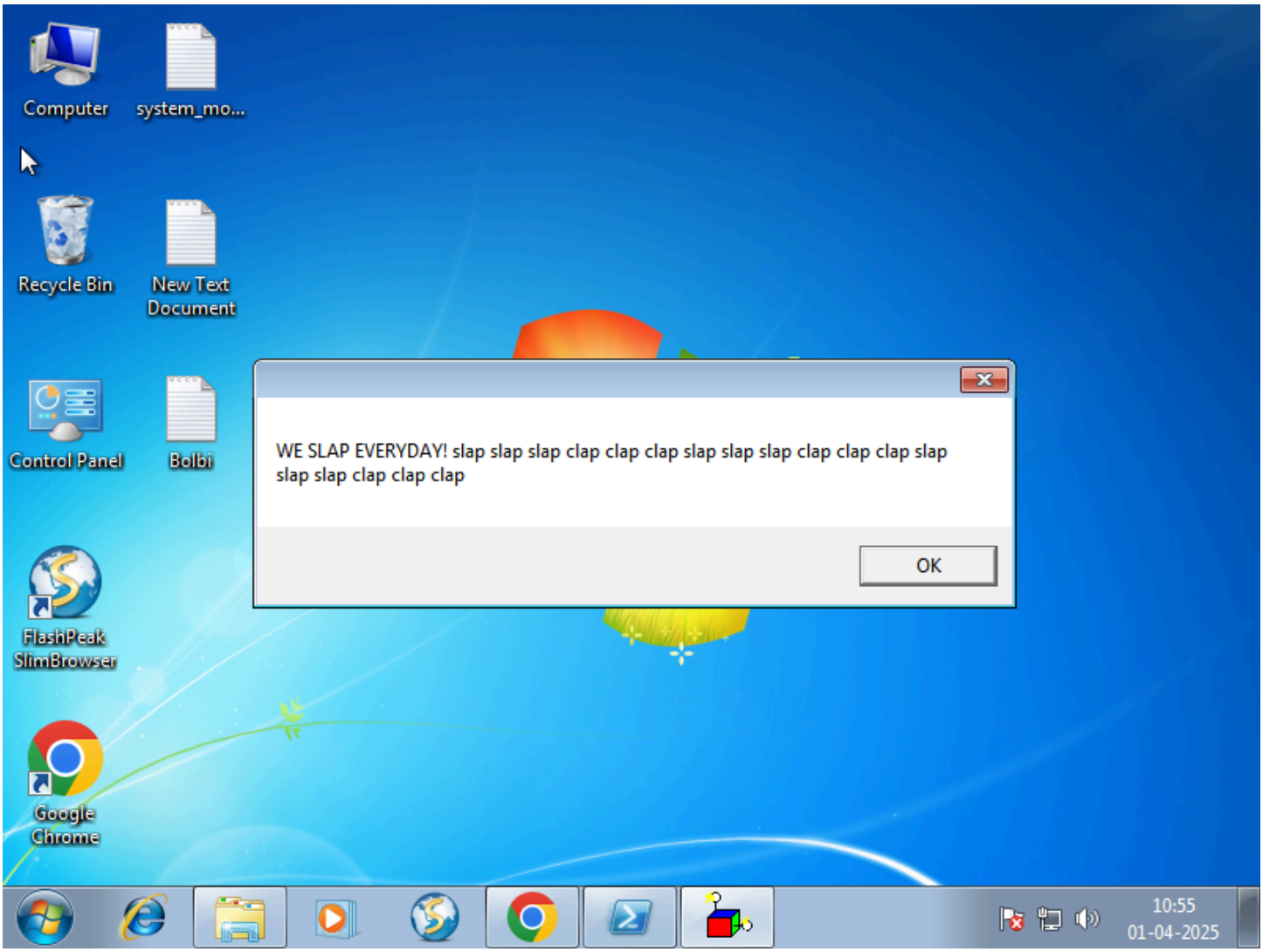
1. **Process Manipulation:** Added **"SporaRansomware"** process.
2. **System Impact: Increased CPU usage to 59%** (Ransomware is actively encrypting files).
3. **RAM Impact: 1418.33 MB** (Moderate increase due to encryption operations).
4. **Process Count: 48 processes**.
5. **Notable Behavior:**
   - **Files are encrypted, and a ransom note is displayed in Russian.**
   - The note instructs victims to **visit a payment website for decryption.**
   - The ransomware **maintains high CPU usage** while running encryption tasks.

4.Bolb

Windows PowerShell

```
===== System Overview =====
Total CPU Utilization: 7%
Total Running Processes: 38
Total RAM Usage: 553.29 MB
===== CPU and RAM Usage =====
ProcessName                CPU             PM
-----------                ---             --
audiodg                                16216064
conhost                1.640625         2760704
csrss                                    2383872
csrss                                    2600960
dwm                    1.28125           1970176
explorer                               19714048
GoogleCrashHandler                       1593344
GoogleCrashHandler64                     1753088
Idle                                           0
lsass                                    4210688
lsm                                      2666496
powershell             6.671875        76115968
SearchFilterHost                         3592192
SearchIndexer                          53403648
SearchProtocolHost                       3137536
services                                 4931584
smss                                      548864
spoolsv                                  6557696
sppsvc                                   6311936
svchost                                14200832
svchost                                  4493312
svchost                                  5165056
svchost                                19480576
svchost                                88395776
svchost                                23355392
svchost                                11329536
svchost                                11587584
svchost                                  8024064
svchost                                  2101248
svchost                                67985408
svchost                                  3026944
System                                    135168
taskhost               0.203125          8527872
wininit                                  1699840
winlogon                                 3178496
WmiPrvSE                                 5328896
wmpnetwk                                 7602176
```

10:57
01-04-2025



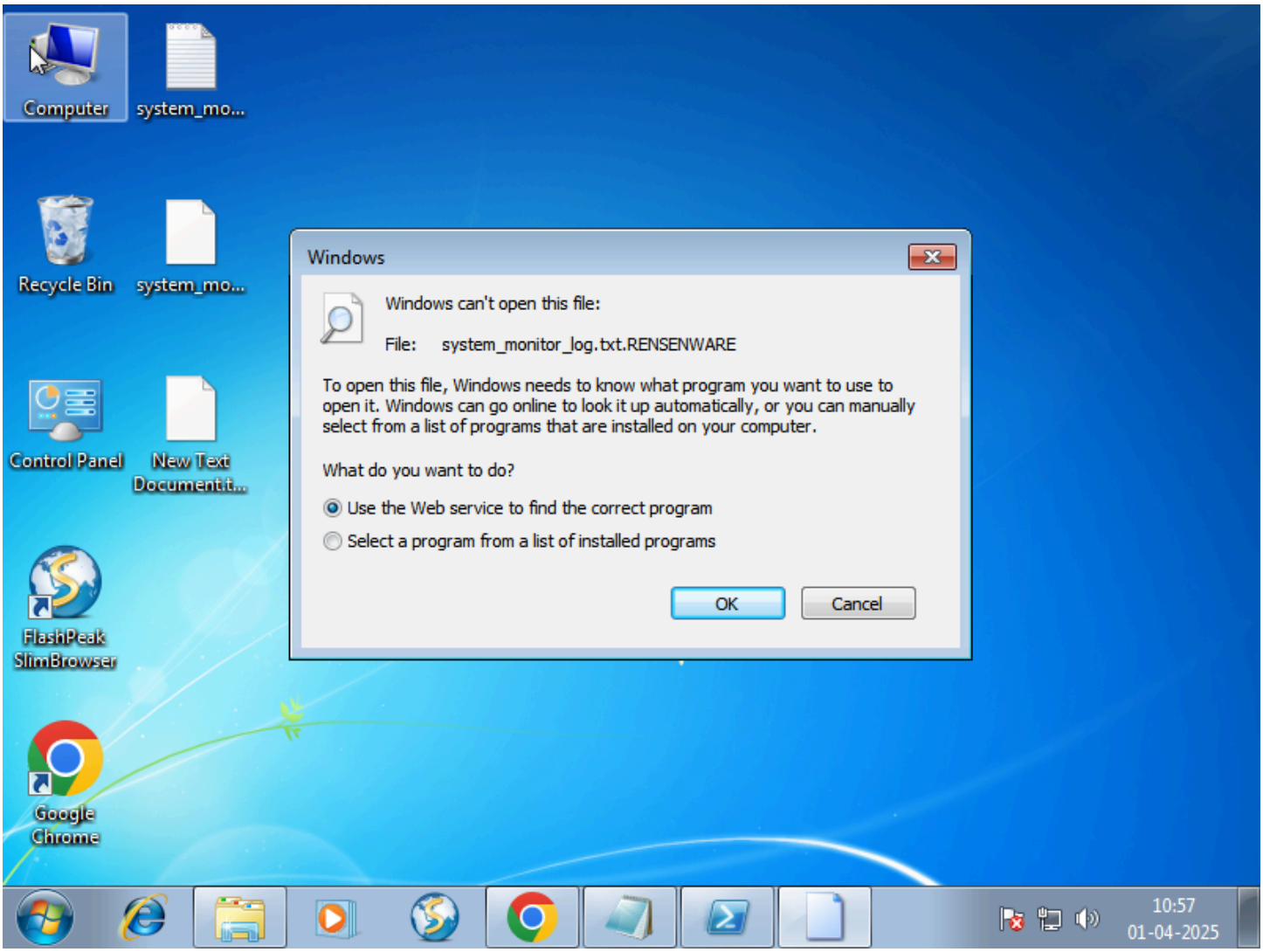
- **Process Manipulation:** Added "Bolbi.exe" process (Likely malware execution)
- **System Impact:** Low CPU usage at **7%**, indicating the malware is either dormant or performing lightweight operations.
- **RAM Impact: 553.29 MB**, with no significant spikes—suggests the malware is not heavily consuming memory yet.
- **Process Count: 38 processes**, which is within normal range, meaning the malware is not spawning excessive subprocesses.
- **Notable Behavior:**
  - A suspicious popup appeared with repetitive text, indicating potential prankware or psychological disruption tactics.
  - PowerShell is actively running, possibly used to monitor system activity or execute commands.
  - No visible file encryption, but malware could be in an initial phase (e.g., reconnaissance, persistence setup).

5.RENSENWARE

Windows PowerShell

```
===== System Overview =====
Total CPU Utilization: 13%
Total Running Processes: 50
Total RAM Usage: 2588.53 MB
===== CPU and RAM Usage =====
ProcessName          CPU              PM
-----------          ---              --
audiodg                            16093184
chrome               0.296875      58257408
chrome               29.1875       69656576
chrome               50.5625       70537216
chrome               0.546875     121008128
chrome               0.03125       36208640
chrome               68.546875    128913408
chrome               0.109375     109867008
chrome               0.109375      58462208
chrome               4.40625      161832960
conhost              0.8125         2752512
csrss                               2793472
csrss                               2609152
dwm                  1.21875        1970176
explorer             13.203125     33320960
GoogleCrashHandler                  1593344
GoogleCrashHandler64                1753088
Idle                                      0
lsass                               4292608
lsm                                 2658304
MpCmdRun                            3969024
notepad              0.09375        1941504
powershell           6.546875      62033920
Ransenware           43.9375     1326661632
SearchFilterHost                    2535424
SearchIndexer                      53624832
SearchProtocolHost                  3907584
services                            5083136
smss                                 548864
spoolsv                             6557696
sppsvc                              6258688
svchost                            13901824
svchost                             4452352
svchost                             5185536
svchost                            19513344
svchost                           149340160
svchost                            30056448
```

10:56
01-04-2025



- **Process Manipulation:** Added "rensenware" process (Malware actively running).
- **System Impact:** Increased CPU usage to **13%**, indicating active background operations, possibly encryption.
- **RAM Impact: 2508.53 MB**, a significant increase, suggesting the malware is consuming memory to process encryption tasks.
- **Process Count: 50 processes**, indicating additional system activity, likely due to malware execution.
- **Notable Behavior:**
  - "rensenware" process is running, which is known ransomware.
  - A file named "system_monitor_log.txt.RENSENWARE" has appeared, indicating file extension changes (potential encryption).
  - The system popup suggests Windows is unable to recognize the new file format, further confirming file modification.
  - No ransom note displayed yet, but encryption is likely in progress.

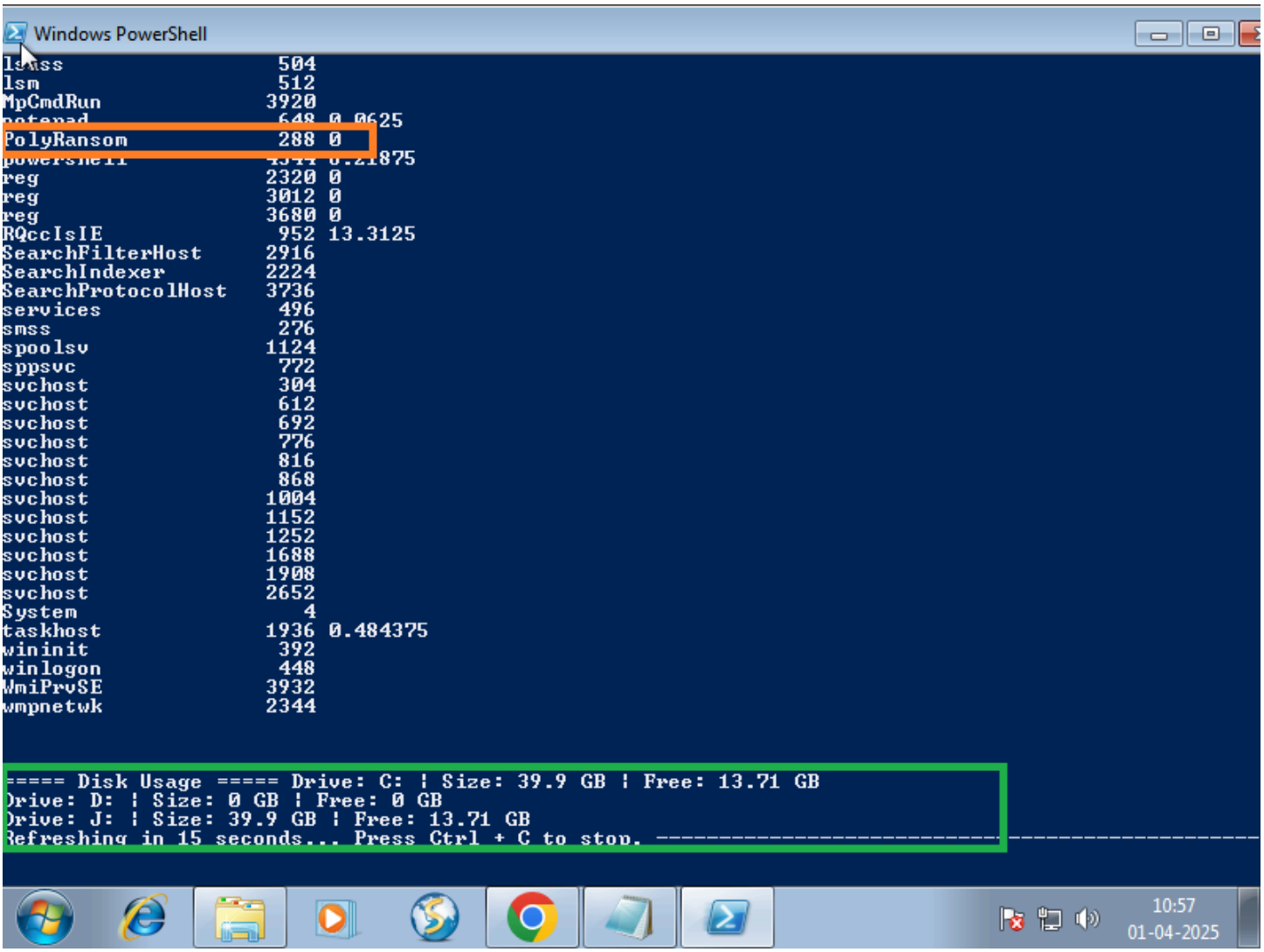
More viruses/malwares and there effect

Polyransom

Windows PowerShell

```
===== System Overview =====
Total CPU Utilization: 61%
Total Running Processes: 59
Total RAM Usage: 1434.59 MB
===== CPU and RAM Usage =====
ProcessName          CPU              PM
-----------          ---              --
audiodg                            16101376
chrome               0.09375      109899776
chrome               0.3125        58908672
chrome               29.4375       69337088
chrome               52.140625     70799360
chrome               0.03125       36249600
chrome               71.15625     131280896
chrome               0.109375      58421248
chrome               0.515625     121634816
chrome               8.1875       163631104
cmd                  0.015625       2174976
cmd                  0.015625       2289664
cmd                  0              2170880
COgYsYsg             0.0625        33824768
conhost              0              1466368
conhost              0              1482752
conhost              0              1482752
conhost              0.921875       3092480
cscript              0               385024
csrss                               2383872
csrss                               2658304
dwm                  1.3125         1970176
explorer             12.9375       33406976
GoogleCrashHandler                  1593344
GoogleCrashHandler64                1753088
Idle                                      0
lsass                               4300800
lsm                                 2654208
MpCmdRun                            3981312
notepad              0.0625         1941504
PolyRansom           0             33021952
powershell           5.546875      84815872
RQccIsIE             9.9375        68956160
SearchFilterHost                    3375104
SearchIndexer                      50466816
SearchProtocolHost                  3973120
services                            4939776
```

10:57
01-04-2025



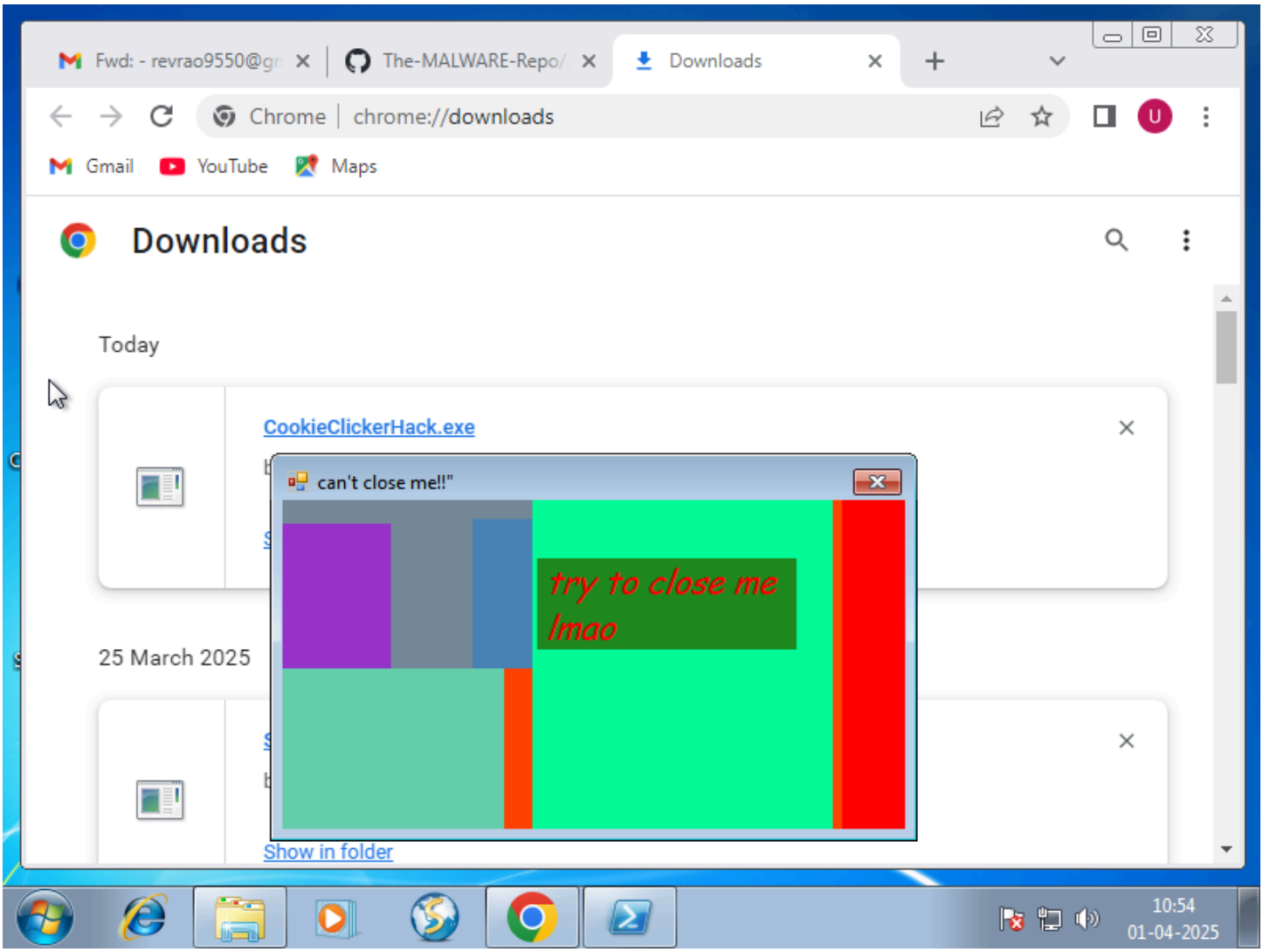
System Impact:

- **CPU Usage:** 61%, higher than normal, indicating active malware execution.
- **RAM Usage:** 1434.59 MB, moderate usage, suggesting background processes are running but not fully resource-intensive.
- **Process Count:** 59, slightly above normal, indicating additional processes spawned by malware.

Notable Behavior:

- **Presence of "Rensenware" and "PolyRansom" processes**, both associated with ransomware activity.
- **PolyRansom process shows 0% CPU usage**, suggesting it might be in a dormant or waiting state.
- **No immediate spikes in storage usage**, indicating encryption might not have started yet, or it is encrypting selectively.
- **PowerShell activity detected**, which could be used for system monitoring, execution of malicious scripts, or persistence mechanisms.
- **Possible staged ransomware attack**, with Rensenware potentially encrypting files while PolyRansom remains as a backup payload

COOKIECLICKER



System Impact:

- **CPU Usage:** Likely minimal unless it's injecting scripts.
- **RAM Usage:** Low, since it’s just a graphical pop-up.
- **Process Count:** Increased by at least one due to CookieClickerHack.exe.

Notable Behavior:

- **Annoying pop-up that resists closure**, possibly looping to keep itself running.
- **Might interfere with user input** (e.g., preventing clicks on the close button).
- **Potential risk:** If downloaded from an untrusted source, it could contain hidden malware.

Memz

MEMZ Virus Analysis

System Impact:

- **CPU & RAM Usage:** Moderate at first, but increases as more payloads execute.
- **Process Count:** Rapidly increases due to spawned processes.
- **Disk Usage:** No traditional ransomware behavior, but it modifies the boot sector.

Notable Behavior:

- **Visual Distortions** (glitches, inverted screens, cascading text).
- **Keyboard & Mouse Interference.**
- **Fake BSOD (Blue Screen of Death)** followed by this Nyan Cat animation.
- **Self-destruction**—once executed fully, the system becomes unbootable.

Is It a Real Threat?

- The **MEMZ Clean version** is harmless, used by YouTubers for fun.
- The **MEMZ Destructive version** will ruin your system.