Pen drive image: <https://drive.google.com/drive/folders/1Fg_pa0VYW3jPa88xZMFeb6fA4afixBip?usp=sharing>

Employee pc image: <https://drive.google.com/drive/folders/1jhJlITp9PmpnrOyObabCRfOY7x3GB_OY?usp=sharing>  
case file:  
<https://drive.google.com/file/d/1isyXE0lTISRqDHQy1ZVsvfOzzwqdqyTz/view?usp=drive_link>

DF project Report

Team 1

2022BCY0034

2022BCY0003

2022BCY0027

# SCENARIO OVERVIEW

**‘John Doe’** was a long-serving employee working in the IT operations department of a reputed company named **TechNova Pvt. Ltd.**, which maintained sensitive internal tools and proprietary systems. Disgruntled over a denied promotion and unsatisfactory appraisal, John began searching for methods to disrupt the company’s infrastructure.

Initially, John tried to find network-based viruses and cyberattack techniques through web searches but failed to find anything actionable. He then came across online forums (like Reddit) discussing how to hire hackers via the **Tor network**. Intrigued, John downloaded and installed the **Tor browser** on his personal laptop and began exploring .onion forums.

Through a darknet marketplace, John contacted a hacker alias **"Anonymous01"**, who offered him a **fileless malware variant known as “99\_BlackEnergy”** capable of crashing internal networks. After negotiating payment and receiving instructions via email (Outlook), the hacker sent him the malware file disguised as a .bat loader.

John downloaded the virus to a **USB drive**, along with a set of **anti-forensic tools** (e.g., **Winlogbeat tampering scripts**) to cover his tracks. He also installed **VeraCrypt** to create an encrypted hidden volume on the USB to hide communication logs, screenshots, and plans shared by the hacker, including a PDF flowchart of the attack sequence.

John later accessed the **TechNova office** during off-hours and plugged the USB into a **company PC**. He installed the malware and anti-forensic tools, executed the virus, and allowed it to spread across the company’s internal network. The malware began replicating and caused noticeable slowdowns and system crashes.

TechNova’s internal monitoring systems flagged unusual memory usage, prompting a security investigation. John was stopped during a routine **security checkpoint** while leaving the premises. His **personal laptop** and **USB drive** were seized. A **RAM dump** of the infected **company PC** was taken for forensic investigation.

The following **devices** were sent to the digital forensics lab for examination:

* **John Doe’s personal laptop** (HDD imaging and search history inspection)
* **Malicious USB device** (partition suspected)
* **Memory image of the infected company PC** (to analyze malware activity using **Volatility**)

### Security Policy of TechNova Pvt. Ltd.

1. **No unauthorized USB devices or personal laptops** are allowed within the internal premises.
2. **All network-connected PCs** are subject to periodic memory scans and behavior monitoring.
3. **DRM and DLP** solutions are enforced to prevent confidential data exfiltration.
4. Employees must pass through a **Security Checkpoint** where devices are scanned.
5. Access to network-critical PCs is logged and time-bound to 9:00 AM – 5:00 PM.

Despite these policies, John's **elevated internal access rights** allowed him to bypass many restrictions. Due to his interest in cybersecurity, he attempted to use **anti-forensic methods** to cover his tracks.

The goal of this digital forensic case is to:

* Uncover proof of John’s communications with the hacker.
* Extract and analyze memory data from the company PC to identify the execution of “99\_BlackEnergy.”
* Recover encrypted artifacts and activity logs from John’s laptop and USB.
* Provide a timeline and reconstruction of the digital attack.

# TARGET SYSTEMS AND DEVICES

|  |  |  |
| --- | --- | --- |
| **Target** | **Detailed Information** | **Note** |
| **Personal Computer (PC)** |  | **Suspect's Personal Laptop** |
| **HW** |  |  |
| Type | Physical Laptop | Lenovo ThinkPad (Placeholder) |
| CPU | Intel Core i5 (4 Cores) | 2.6 GHz |
| RAM | 8 GB | DDR4 |
| HDD Size | 512 GB SSD | Encrypted partition detected |
| File System | NTFS | Standard Windows format |
| IP Address | 192.168.1.45 | Home Wi-Fi |
| **SW (OS)** |  |  |
| Operating System | Windows 10 Home | 64-bit, fully updated |
| **SW (Apps)** |  |  |
| Web | - Edge | Tor Browser installed |
| Communication | - Microsoft Outlook | Used for mail exchange with hacker |
| Encryption | VeraCrypt | Hidden volume detected |
| **Removable Media #1 (RM#1)** |  | **Malicious USB Drive** |
| **HW** |  |  |
| Type | USB Removable Storage Device | Plugged into company PC |
| Manufacturer | Sandisk | Vendor ID = 0x0951 |
| Model | DataTraveler G4 | - |
| Serial No. | 001A9283F7A1C4 | Example only |
| Size | 8 GB | Contains malware and encrypted VeraCrypt volume |
| File System | exFAT | Portable format |
| Volume Label | "WorkFiles" | Modified post-crime |

### Infected Company PC

|  |  |  |
| --- | --- | --- |
| **Component** | **Details** | **Notes** |
| **Hardware** |  |  |
| Type | Desktop Tower | Office Asset |
| CPU | Intel Xeon E3 | 3.2 GHz |
| RAM | 16 GB | High-capacity system |
| HDD Size | 1 TB | Business data stored |
| File System | NTFS | Monitored by DLP systems |
| IP Address | 10.0.0.22 | Internal network |
| **Software** |  |  |
| OS | Windows 10 Enterprise | DRM/DLP policies enabled |
| Memory Dump | Acquired for analysis | Format: .raw |

# Detailed Behavior of the Suspect:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Date/Time** | **Action** | **Details / Description** | **Notes** |
| 1 | 2025-03-31 10:00 AM | Suspicious Browser Searches | - "How to hack a company network?"- "Most dangerous network viruses"- "How to take down a corporate network?" | Evidence from browser history |
| 2 | 2025-03-31 10:15 AM | TOR and Dark Web Searches | - "How to contact hackers online?"- "Best forums for hiring hackers"- "How to use Tor..."- "Hiring a hacker to destroy a company" | TOR-related keyword cache entries |
| 3 | 2025-03-31 10:25 AM | Visiting Darknet Sites | - Visited: https://www.torproject.org/download/- https://www.reddit.com/r/hacking/- Fake onion forums | Web history + DNS queries |
| 4 | 2025-03-31 10:30 AM | Download Tor Browser | - Downloaded torbrowser-install.exe from official Tor site | Found in Downloads + prefetch logs |
| 5 | 2025-03-31 10:32 AM | Installed and Executed Tor | - Evidence in Program Files\Tor Browser\- Desktop shortcut- Prefetch for tor.exe | Shows intent to access dark web |
| 6 | 2025-03-31 03:43 PM | Initiates Email to Hacker | - Email Subject: *Let’s continue here*- From: jhondoe1263@outlook.com to anonymoussus91@gmail.com | Extracted from Outlook PST |
| 7 | 2025-03-31 03:44 PM | Communication About Attack | - “I want to crash my company’s network, can you help?” | Stored in Sent Items |
| 8 | 2025-03-31 03:48 PM | Hacker Demands Payment | - Asks for $500 via crypto | Crypto wallet trace needed |
| 9 | 2025-03-31 03:53 PM | User Sends Payment Receipt | - Screenshot / attachment evidence | Embedded in email thread |
| 10 | 2025-03-31 04:08 PM | Hacker Sends Malware Executable | - File: 99\_blackenergy.exe | .exe file in Downloads |
| 11 | 2025-03-31 04:33 PM | Hacker Sends Attack Script | - Batch script included (shown below table) | Shows persistence techniques |
| 12 | 2025-04-04 03:58 PM | User Seeks Advice on Covering Tracks | - Email about forensic evasion | Mentions memory-only malware |
| 13 | 2025-04-05 09:00 AM | USB Drive Connected | - USB Label: MALWARE\_USB | Identified via USB logs |
| 14 | 2025-04-05 09:05 AM | Copied and Executed Batch Script & Malware | - Loaded via USB and executed on Company\_PC | Evidence in Recent + Registry |
| 17 | 2025-04-05 09:20 AM | Malware Running in Background | - Verified via Process Explorer & memory dump | Process name: winupdate.exe |

### Malicious Script (from Hacker)

@echo off

title System Update

cls

echo [\*] Initializing System Update...

timeout /t 3 /nobreak >nul

copy "%~dp0\99\_blackenergy.exe" "C:\Windows\System32\winupdate.exe" /Y

reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "WinUpdater" /t REG\_SZ /d "C:\Windows\System32\winupdate.exe" /f

powershell -Command "Set-MpPreference -DisableRealtimeMonitoring $true"

start /B "C:\Windows\System32\winupdate.exe"

schtasks /create /tn "WindowsUpdateChecker" /tr "C:\Windows\System32\winupdate.exe" /sc onlogon /rl highest /f

wevtutil cl Security

exit

# ACQUIRED DATA INFORMATION

### EMPLOYEE PERSONAL COMPUTER – FORENSIC IMAGE (PRIMARY SUSPECT DEVICE)

This system was seized from the employee suspected of coordinating the malware delivery via LinkedIn messages. The system likely contains planning materials, communication logs, and malware source files.

|  |  |
| --- | --- |
| **Item** | **Details** |
| **Filename** | employee\_pc\_image |
| **MD5 Hash** | A49D1254C873808C58E6F1BCD60B5BDE |
| **SHA-1 Hash** | AFE5C9AB487BD47A8A9856B1371C2384D44FD785 |
| **Imaging Software** | FTK Imager 3.4.0.1 |
| **Image Format** | DD (converted from VMDK format – *some sectors scrubbed*) |
| **Compression** | Best (7zip) |
| **Bytes per Sector** | 512 |
| **Total Sectors** | 41,943,040 |
| **Uncompressed Size** | 20.00 GB (21,474,836,480 bytes) |
| **Compressed Size** | 5.05 GB (5,427,795,228 bytes) |

### MALICIOUS USB DEVICE – FORENSIC IMAGE (MALWARE DELIVERY MEDIA)

This USB device was recovered from the employee's belongings. It is believed to have been physically inserted into the target company PC to manually deploy malware. The USB contains malware payloads and potential auto-run scripts.

|  |  |
| --- | --- |
| **Item** | **Details** |
| **Filename** | malicious\_usb\_image |
| **MD5 Hash** | B4644902ACAB4583A1D0F9F1A08FAA77 |
| **SHA-1 Hash** | 048961A85CA3ECED8CC73F1517442D31D4DCA0A3 |
| **Imaging Software** | FTK Imager 3.3.0.5 |
| **Image Format** | E01 (Expert Witness Format) |
| **Compression** | Best (7zip) |
| **Bytes per Sector** | 512 |
| **Total Sectors** | 7,821,312 |
| **Uncompressed Size** | 3.7 GB (4,004,511,744 bytes) |
| **Compressed Size** | 219 MB (229,899,285 bytes) |

### INFECTED COMPANY SYSTEM – MEMORY DUMP (VOLATILE EVIDENCE)

A memory dump was acquired from the victim company’s system after suspicious activity was detected. It is critical for identifying running malware processes, injected code, and in-memory data exfiltration attempts.

|  |  |
| --- | --- |
| **Item** | **Details** |
| **Filename** | company\_pc\_memdump |
| **Acquisition Tool** | DumpIt 3.0.20207.1 |
| **Format** | Raw memory image (.mem) |
| **Memory Size** | 8.00 GB (8,589,934,592 bytes) |
| **Compression** | 1.76 GB (compressed using 7zip) |
| **System State** | Captured while machine was still running suspected malware |

# Autopsy report of pen drive:

https://drive.google.com/drive/folders/15m-Pomcr4i3xPOQdjNrW6AbaFNfZ4Z6m?usp=sharing

# Magnet Axiom Report:

https://drive.google.com/drive/folders/10ogXV1r618m1ZkZce6V7NVgE6xufTjRf?usp=sharing

# BlackEnergy Volatility Memory Forensics Report:

**Case Information**

* **Case Name:** BlackEnergy rootkit Investigation
* **Investigator:** K.Sai Sidhartha
* **Date of Analysis:** 04-04-2005
* **Memory Image File:** companypc\_mem\_dump.vmem
* **Volatility Profile Used:** WinXPSP2x86

**1. Memory Profile Identification**

**Objective:**

Determine the correct Volatility profile for the memory dump to ensure accurate analysis.

**Command Used:**

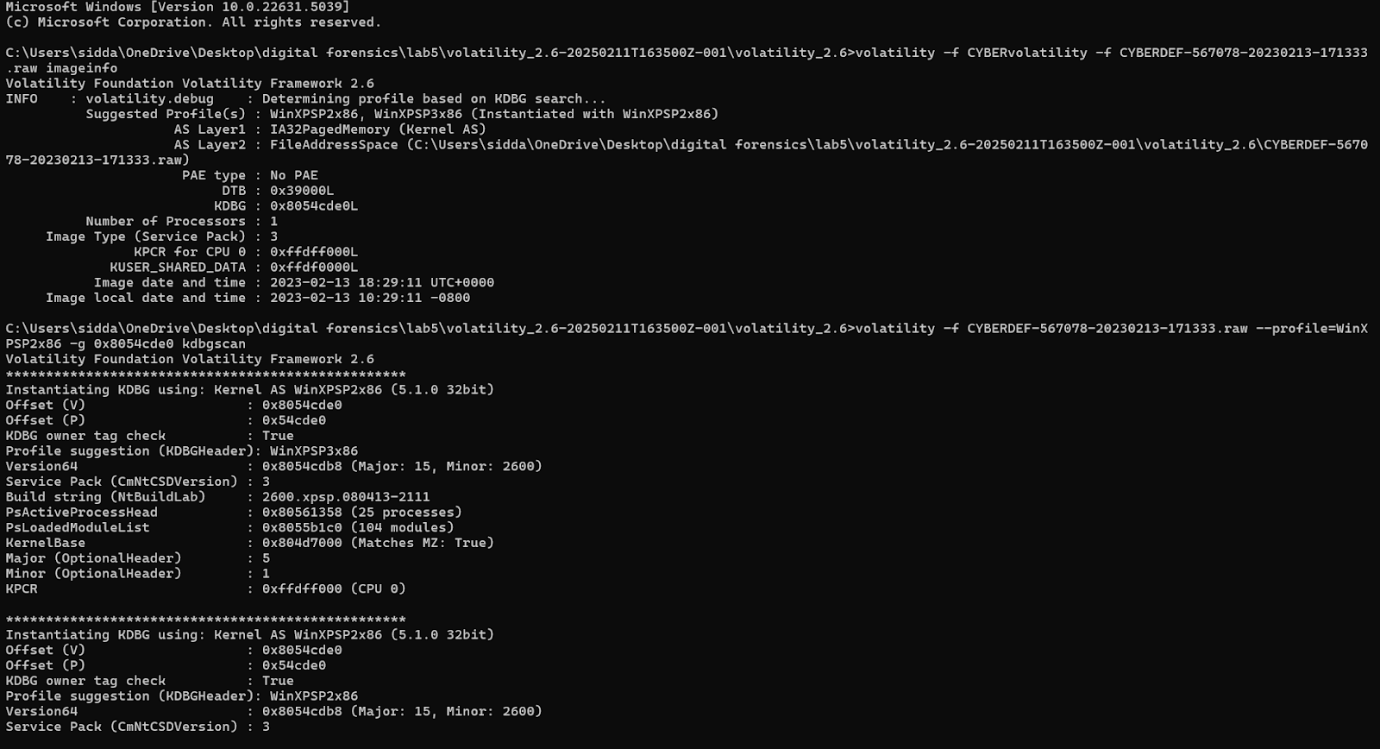
vol.exe -f <memory\_dump\_path> imageinfo

**Findings:**

* The suggested profiles included: **WinXPSP2x86**

To confirm, the **kdbgscan** plugin was used:  
  
 vol.exe -f <memory\_dump\_path> --profile=WinXPSP2x86 kdbgscan

* The results confirmed **WinXPSP2x86** as the correct profile.

**Evidence:**

**2. Number of Running Processes**

**Objective:**

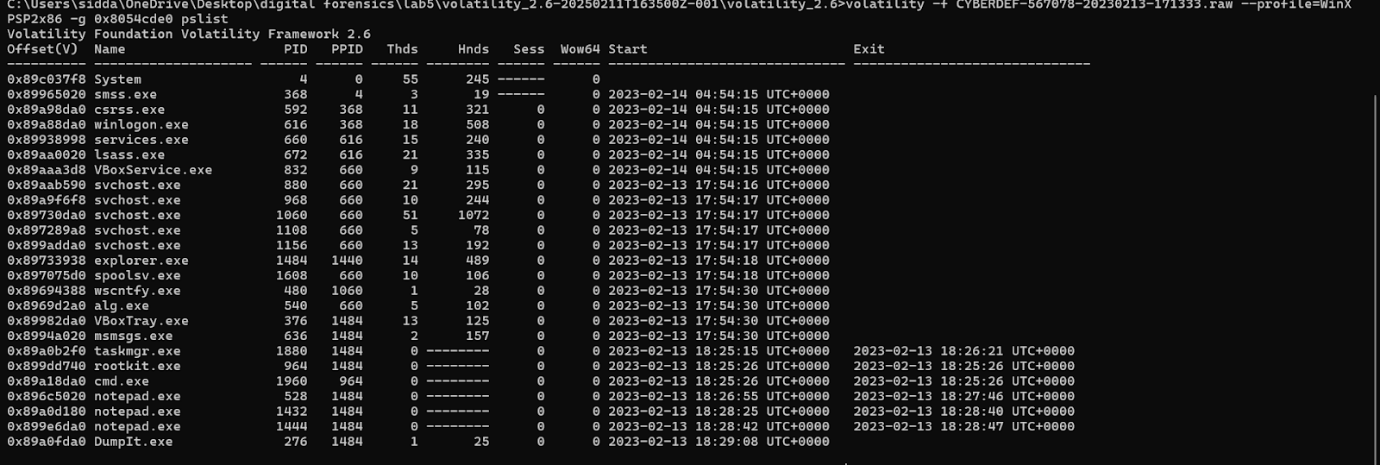
Identify how many processes were running when the memory image was acquired.

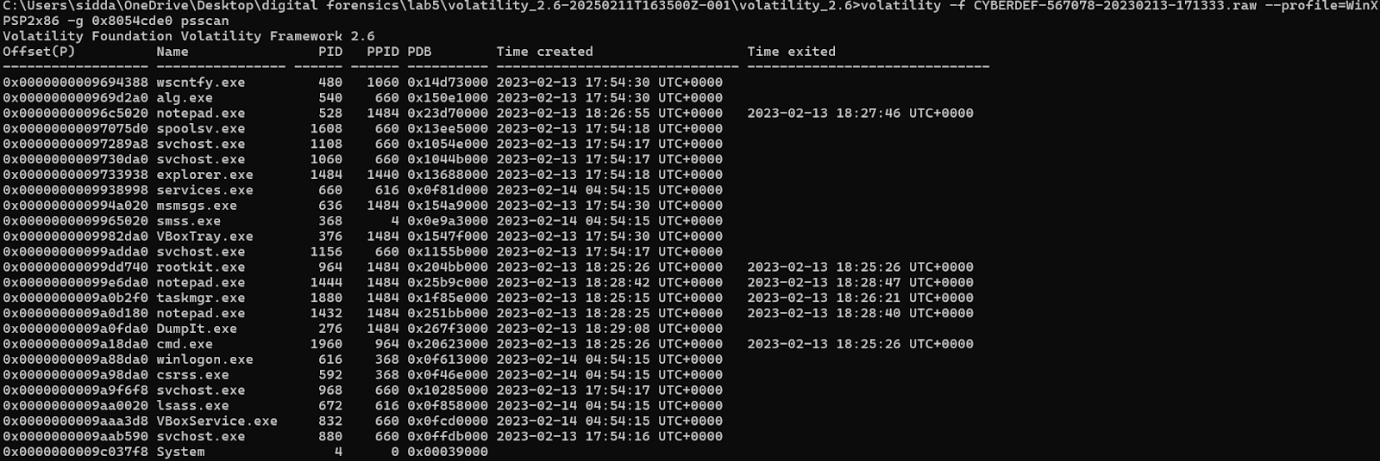
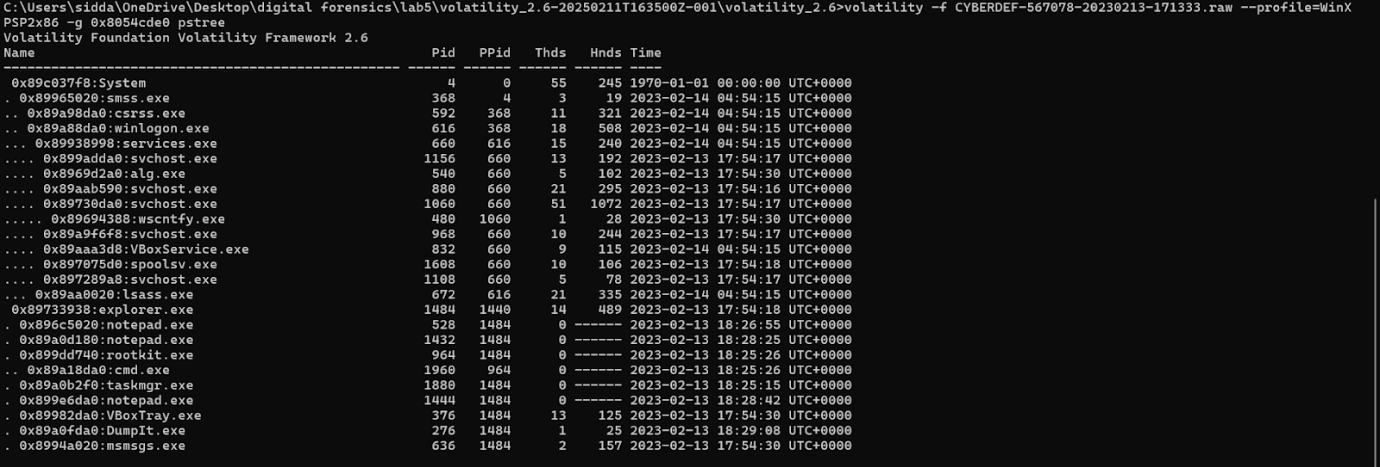
**Command Used:**

vol.exe -f <memory\_dump\_path> --profile=WinXPSP2x86 pslist

**Findings:**

* The total number of running processes (processes with no exit timestamp) was **19**.

**Evidence:**



**3. Identifying the Process ID of cmd.exe**

**Objective:**

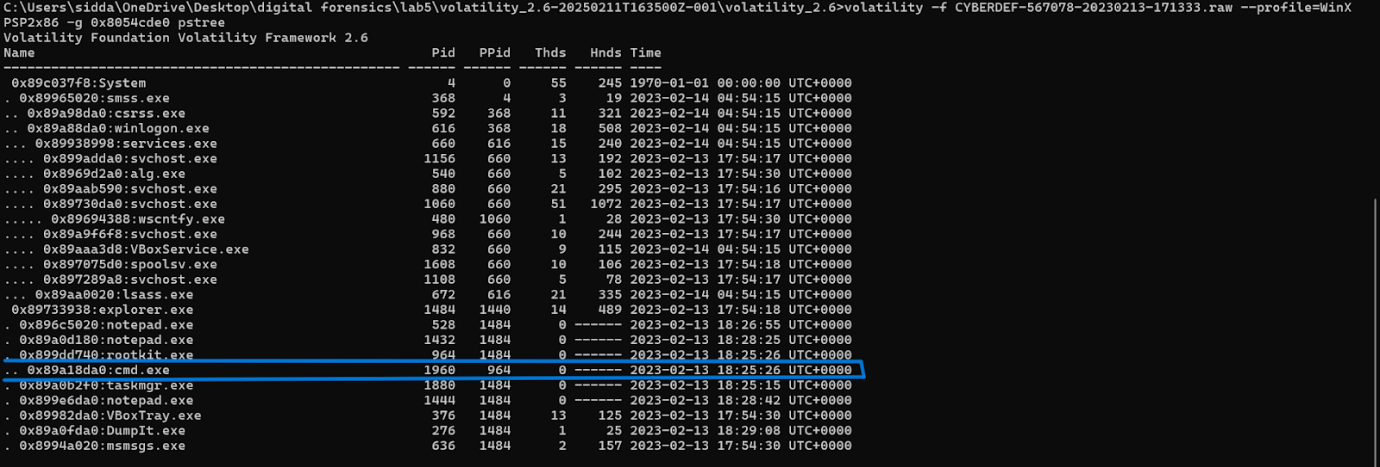
Find the Process ID (PID) of cmd.exe, which may have been used for malicious activities.

**Command Used:**

vol.exe -f <memory\_dump\_path> --profile=WinXPSP2x86 pstree

**Findings:**

* cmd.exe was found with a **Process ID (PID) of 1960**.

**Evidence:**

**4. Identifying the Most Suspicious Process**

**Objective:**

Determine the most suspicious process in the system.

**Findings:**

* **Suspicious Process:** rootkit.exe
* **Process ID (PID):** 964
* **Parent Process ID (PPID):** 1484
* **Why Suspicious?**
  + The name suggests malware intent.
  + The process exited quickly, a tactic often used by malware to avoid detection.

**Evidence:**

**5. Identifying Code Injection**

**Objective:**

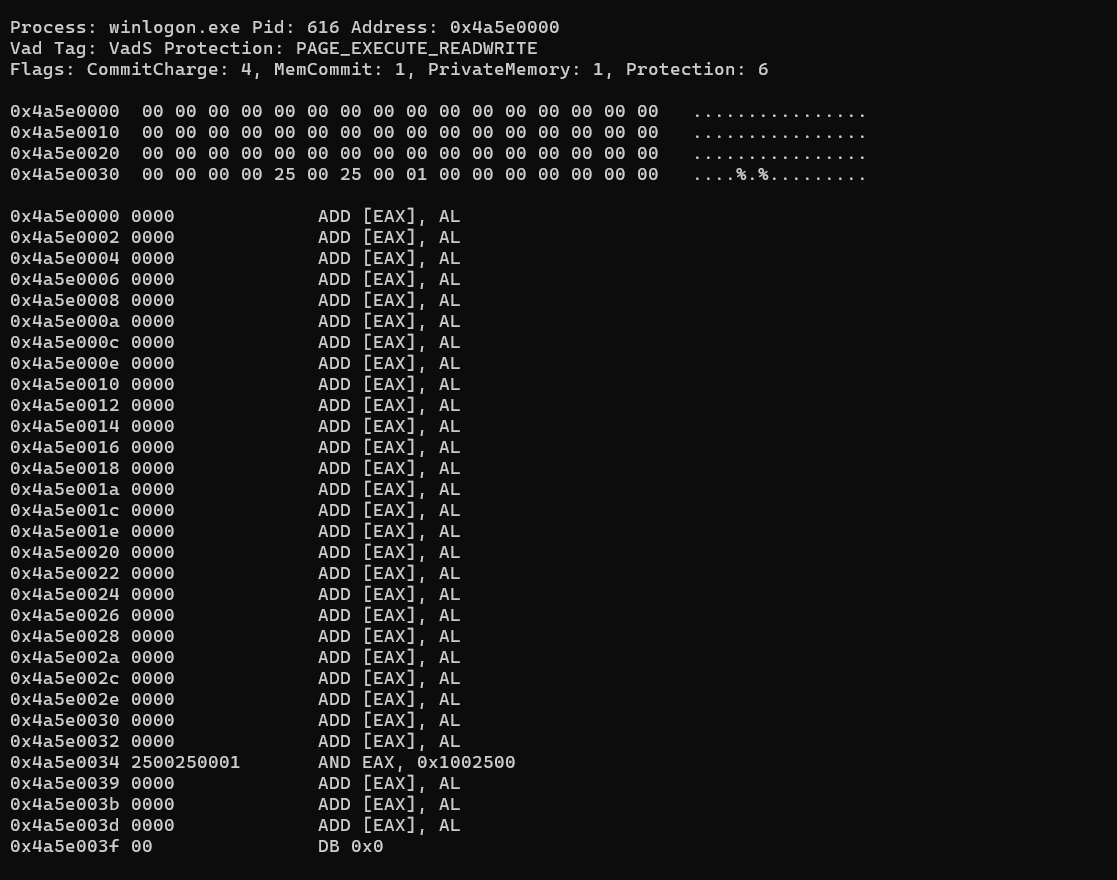
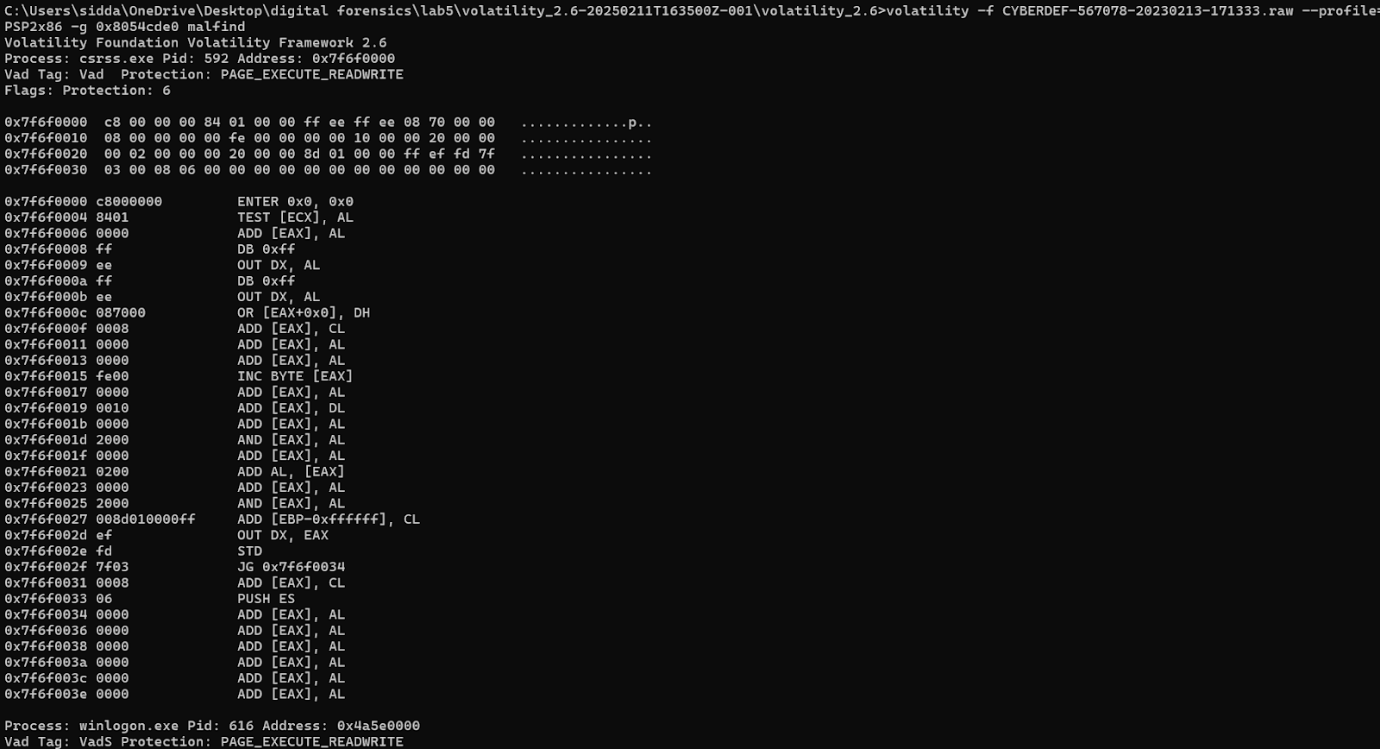
Determine which process has signs of code injection.

**Command Used:**

vol.exe -f <memory\_dump\_path> --profile=WinXPSP2x86 malfind

**Findings:**

* **Process Name:** svchost.exe
* **Process ID (PID):** 880
* **Indicators of Code Injection:**
  + Memory region with **PAGE\_EXECUTE\_READWRITE** permissions.
  + Presence of the **MZ (4D 5A) header**, indicating an injection.

**Evidence:**

**6. Identifying Suspicious File Referenced by the Process**

**Objective:**

Find a suspicious file that the compromised process accessed.

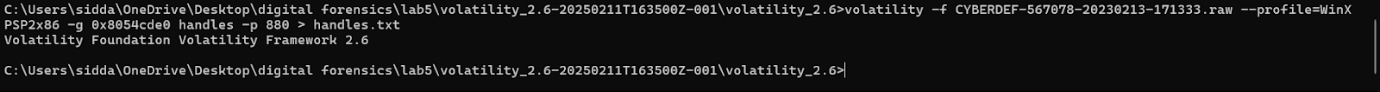
**Command Used:**

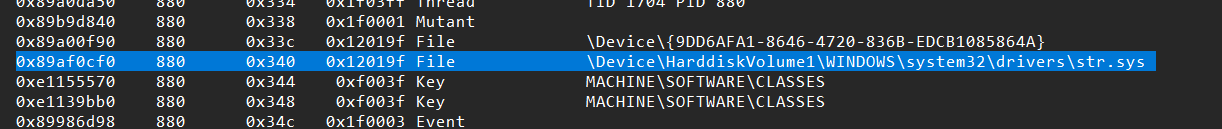
vol.exe -f <memory\_dump\_path> --profile=WinXPSP2x86 handles -p 880

**Findings:**

The svchost.exe process (PID 880) referenced a suspicious file:  
  
 \Device\HarddiskVolume1\WINDOWS\system32\drivers\str.sys

* **Why Suspicious?**
  + The filename does not follow standard system driver naming conventions.
  + Malicious actors often place rootkits or malicious drivers in the system32\drivers directory.

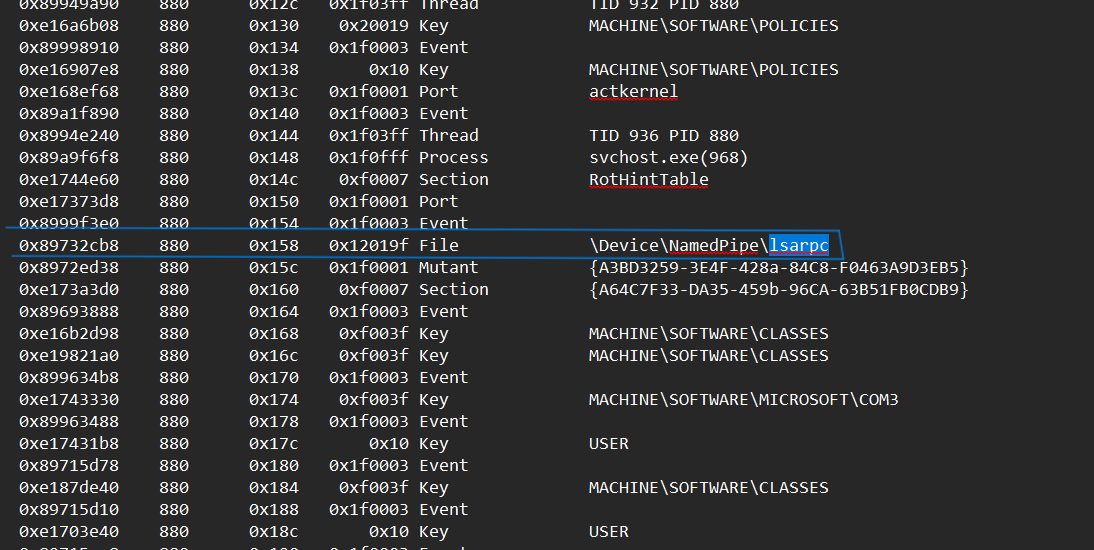
**Evidence:**

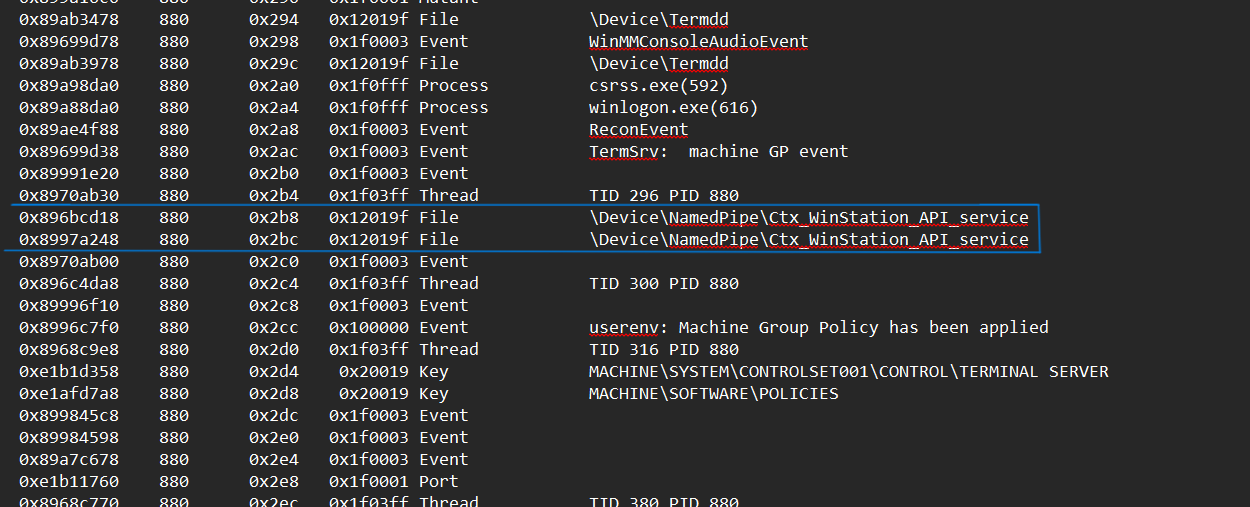


**Other Findings:**

 1. Named Pipes:

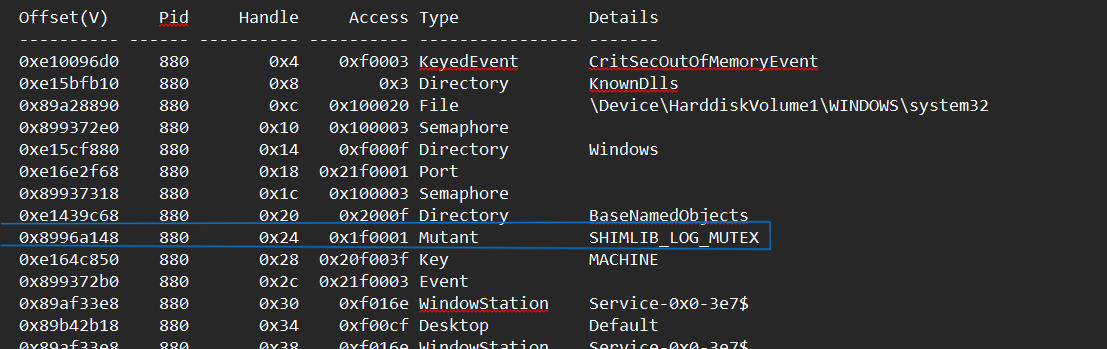
****

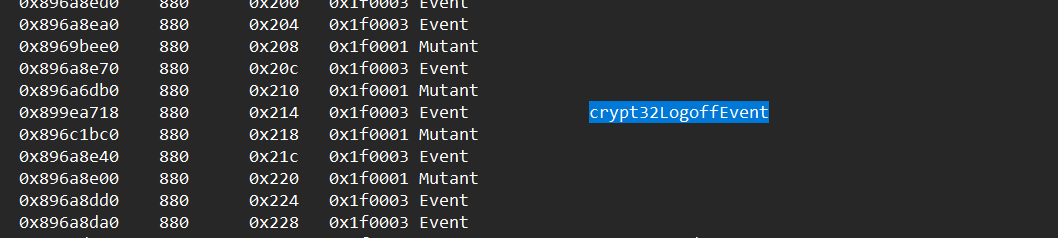
****

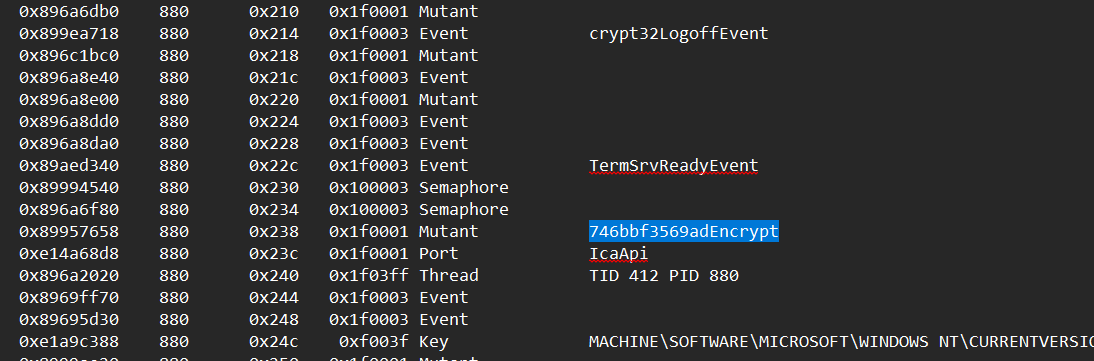


* Why it's suspicious: Malware (including BlackEnergy) commonly uses named pipes for interprocess communication (IPC) or persistence mechanisms.
* NtControlPipe2 is not a standard named pipe and could be indicative of a custom backdoor channel.

2. Keyed Events / Cryptic Mutexes / Semaphores:



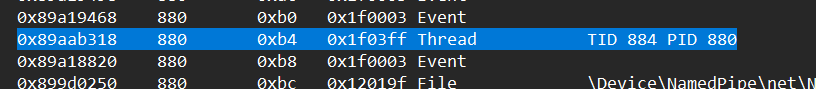


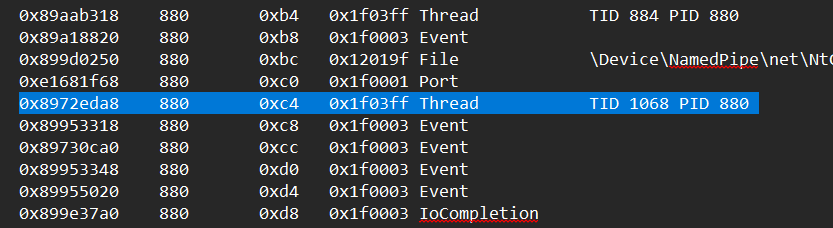
****

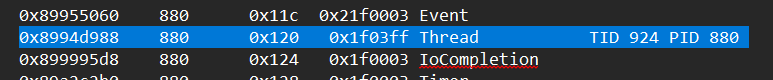
Why it's suspicious: These are often used for synchronization or anti-analysis:

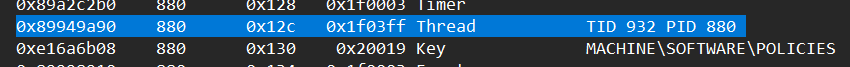
* 746bbf3569adEncrypt has a randomized-looking name, a common tactic in malware obfuscation.
* crypt32LogoffEvent hints at cryptographic API tampering or monitoring logoff actions.
* SHIMLIB\_LOG\_MUTEX – Could be part of **shim database abuse**, which BlackEnergy variants are known to interact with.

 3. Thread Handles in High Volume:



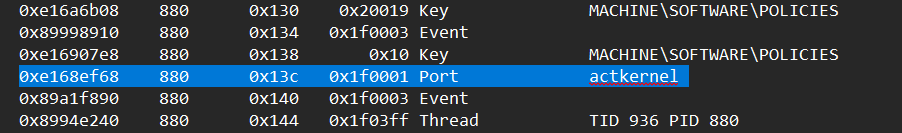


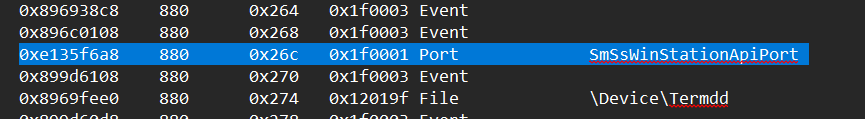




Lots of threads opened (e.g., TID 884 PID 880, TID 1068, etc.) is typical, but combined with other red flags, may suggest **thread injection or code execution mechanisms**.

 4. Port Handles to actkernel, SmSsWinStationApiPort, IcaApi, RotHintTable, etc.:

****

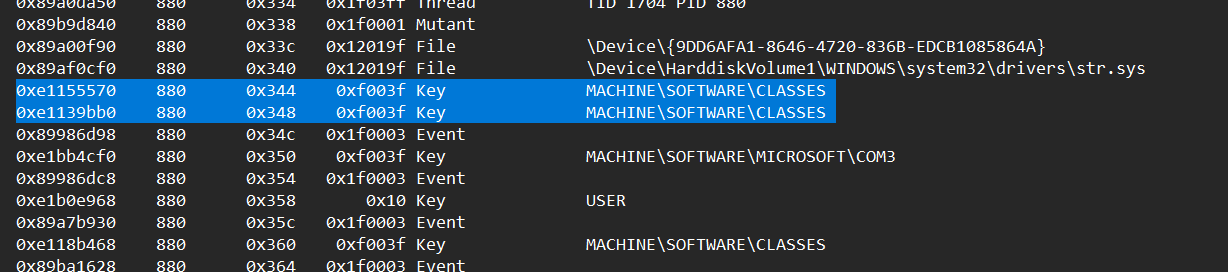
****

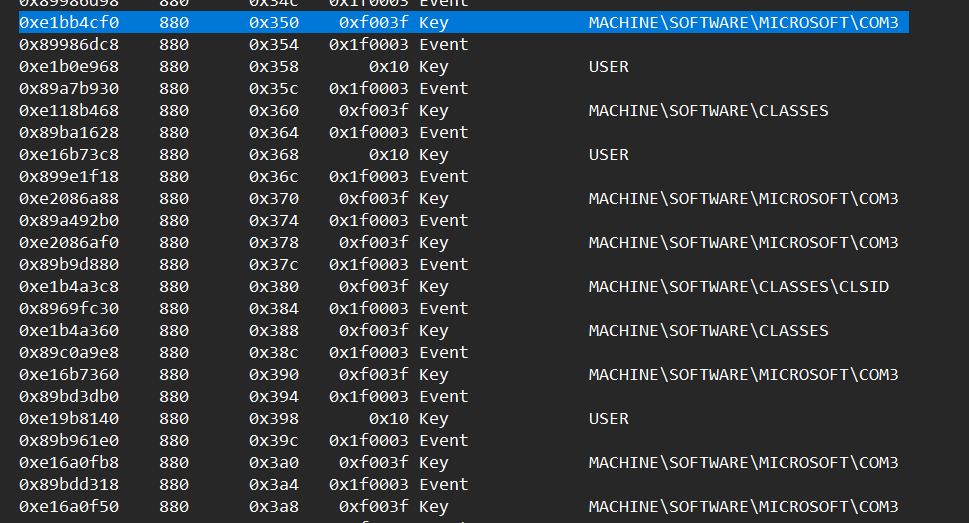
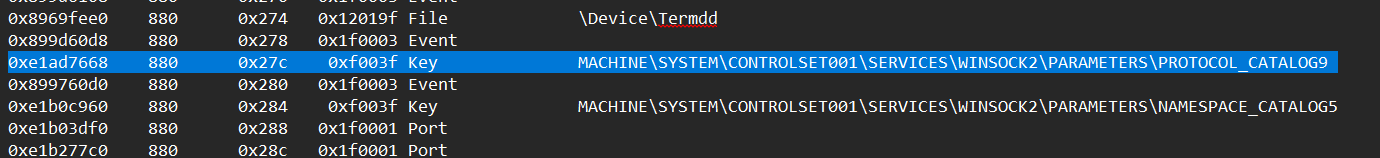
****

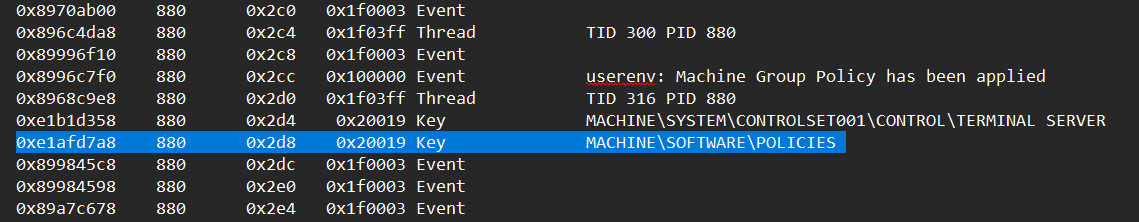
These are often used by system services, but access from user-mode processes like this suggests:

* Service hooking
* API hijacking
* Shellcode staging

5. Access to Critical Registry Keys:



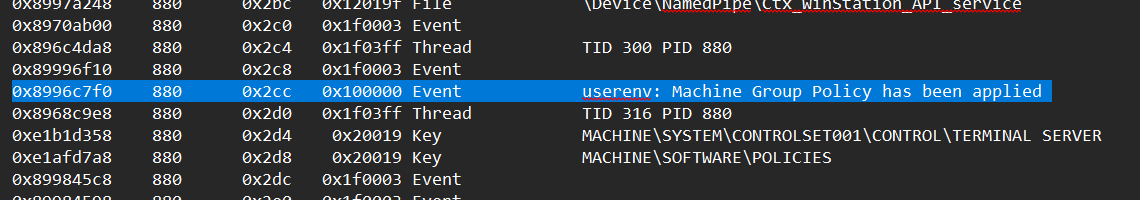
’



Registry key manipulation is often used for:

* Persistence (Run keys, Services)
* Network hook modification (Winsock, COM interfaces)

6. Privilege escalation:



Machine Group rules being changed

**7. Identifying Injected DLL**

**Objective:**

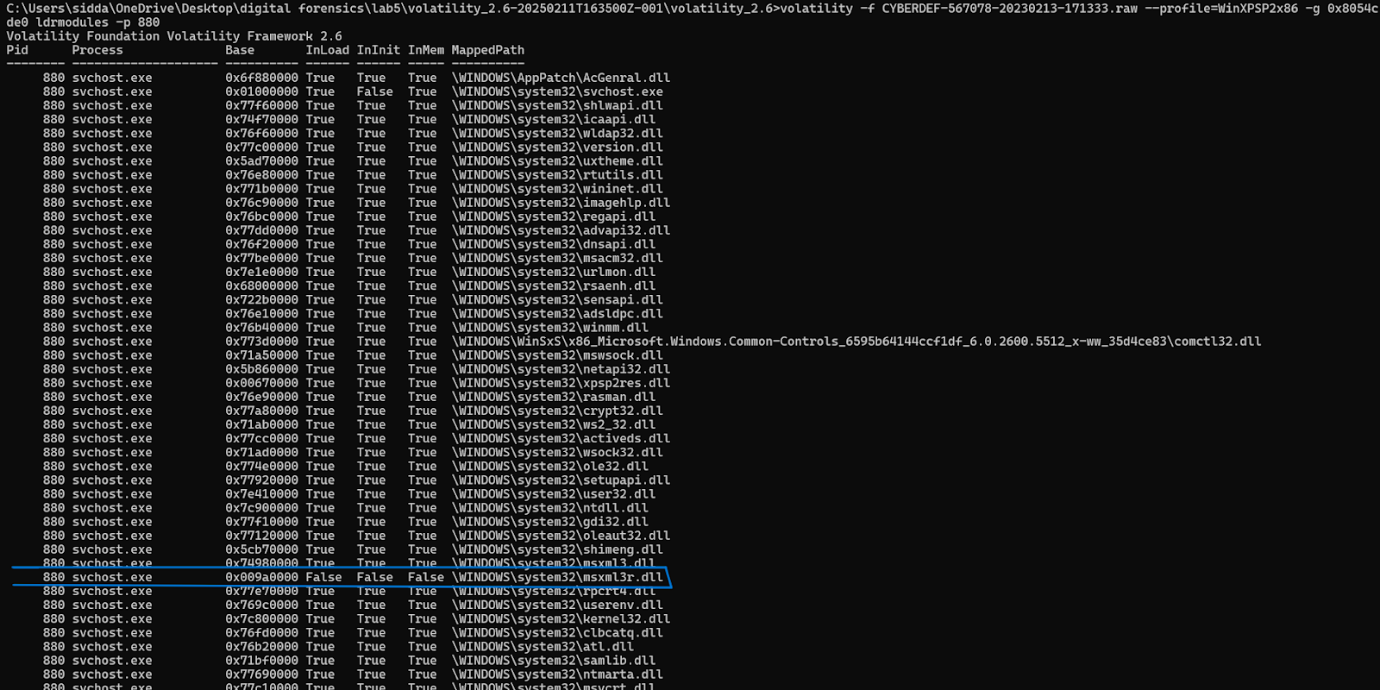
Identify any injected DLLs associated with the compromised process.

**Command Used:**

vol.exe -f <memory\_dump\_path> --profile=WinXPSP2x86 ldrmodules -p 880

**Findings:**

* **Injected DLL:** msxml3r.dll
* **Why Suspicious?**
  + It is missing from all three lists (InLoad, InInit, InMem).
  + Legitimate DLLs should appear in all three categories.
  + This suggests it was manually injected into the process.

**Evidence:**

**8. Identifying the Base Address of the Injected DLL**

**Objective:**

Determine where the injected DLL is located in memory.

**Findings:**

* **Base Address of Injected DLL:** 0x980000
* **Evidence of Injection:**
  + The MZ (4D 5A) PE header at this memory location indicates that an executable file (DLL) is loaded here.

**Evidence:**

**Conclusion**

**Summary of Findings:**

* The memory dump was analyzed using **Volatility** with the profile **WinXPSP2x86**.
* **19 processes** were actively running at the time of acquisition.
* cmd.exe was found with PID **1960**, potentially used for executing malicious commands.
* The most suspicious process was **rootkit.exe (PID 964)**, indicating potential malware activity.
* **Code injection** was detected in **svchost.exe (PID 880)**, a common attack method used by malware.
* The **suspicious file** referenced was **str.sys**, which was located in the system32\drivers directory.
* The **injected DLL** was identified as **msxml3r.dll**, which did not appear in standard module lists.
* The **base address** of the injected DLL was **0x980000**, confirming the presence of malicious code.

**Recommended Actions:**

1. **Isolate the Infected System:** Prevent further compromise by removing it from the network.
2. **Extract and Analyze Suspicious Files:** Further investigate str.sys and msxml3r.dll for their functionality.
3. **Perform a Full Malware Analysis:** Examine injected code within svchost.exe to understand its behavior.
4. **Harden Security Measures:** Implement endpoint detection and response (EDR) tools to prevent similar attacks.
5. **Monitor Network Activity:** Check for any outbound connections initiated by the infected system.

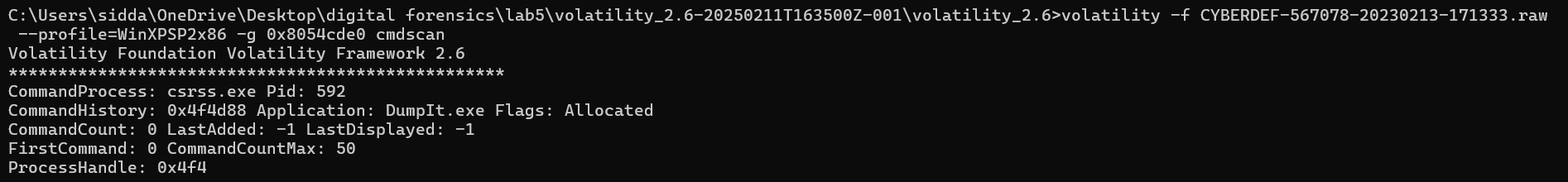
**End of Report**

# CTF Questions:

### Volatility:

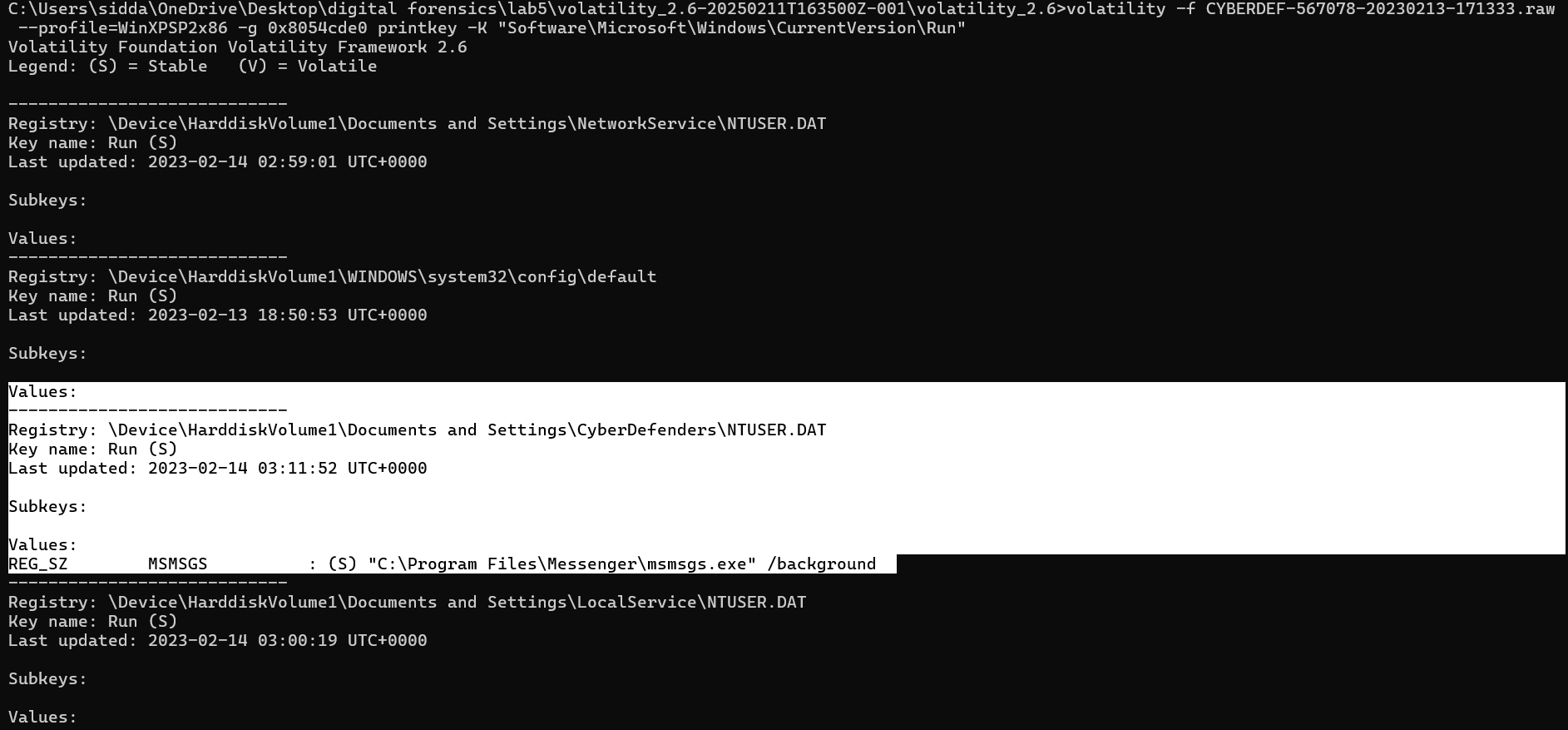
1. What command was executed by cmd.exe?

**Hint:** Use the cmdscan or consoles plugin to inspect command-line history from cmd.exe processes.



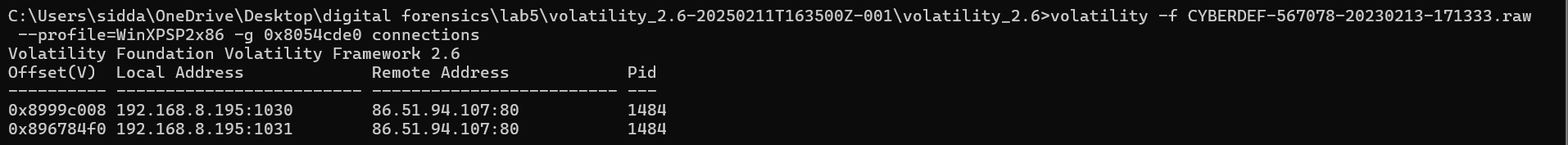
1. What registry key was potentially modified to achieve persistence?

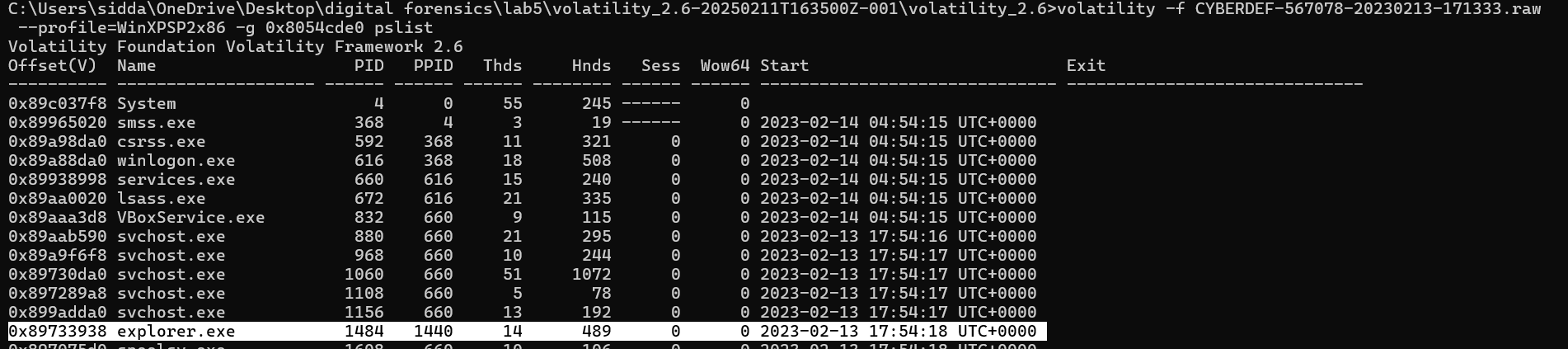
**Hint:** Check for auto-start entries in the registry, often modified by malware to persist across reboots.



1. What network connection is associated with the suspicious svchost.exe process?

Use connections to identify active or recently closed connections, especially those tied to suspicious PIDs (e.g., PID 880 from svchost.exe).

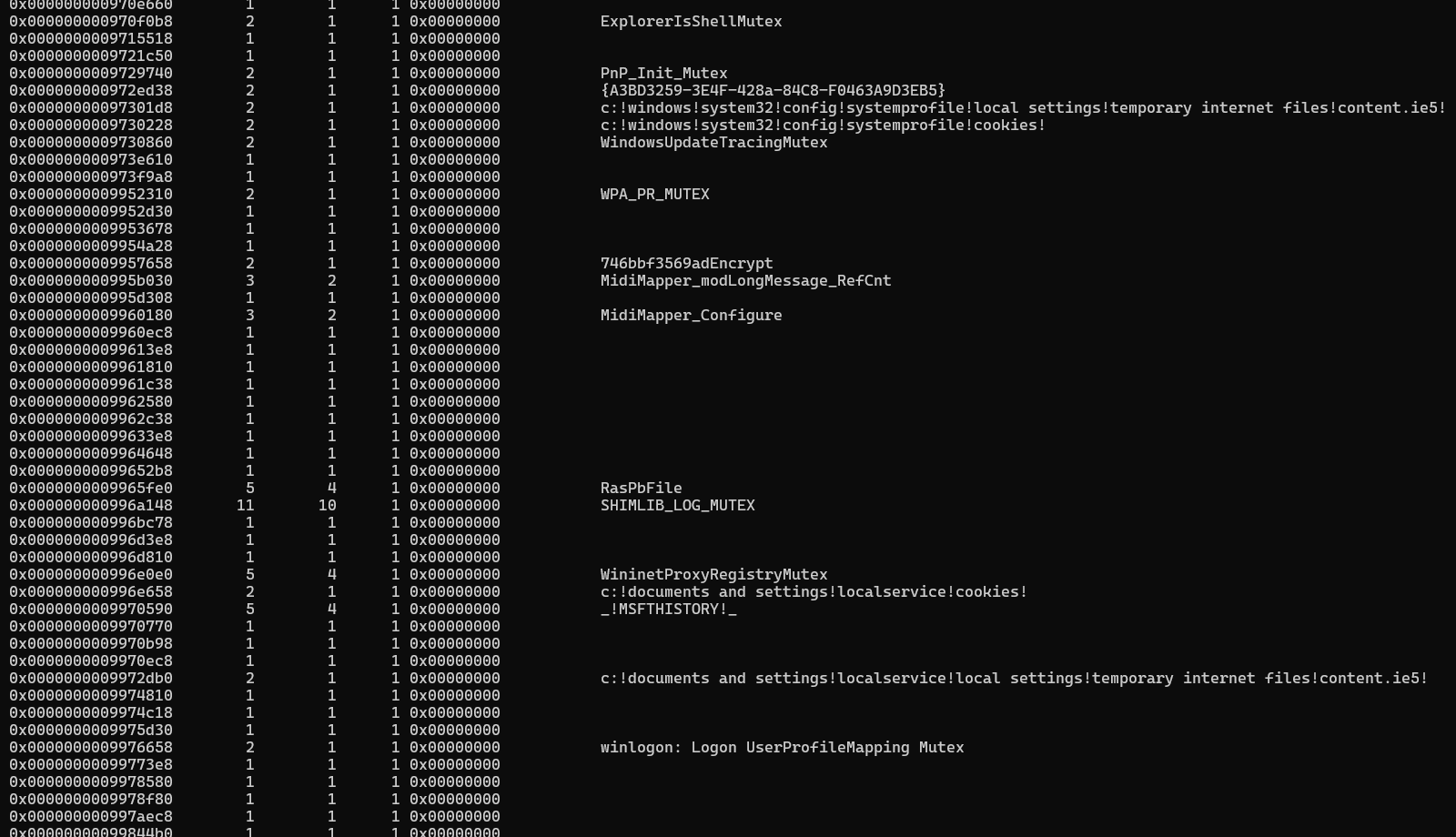
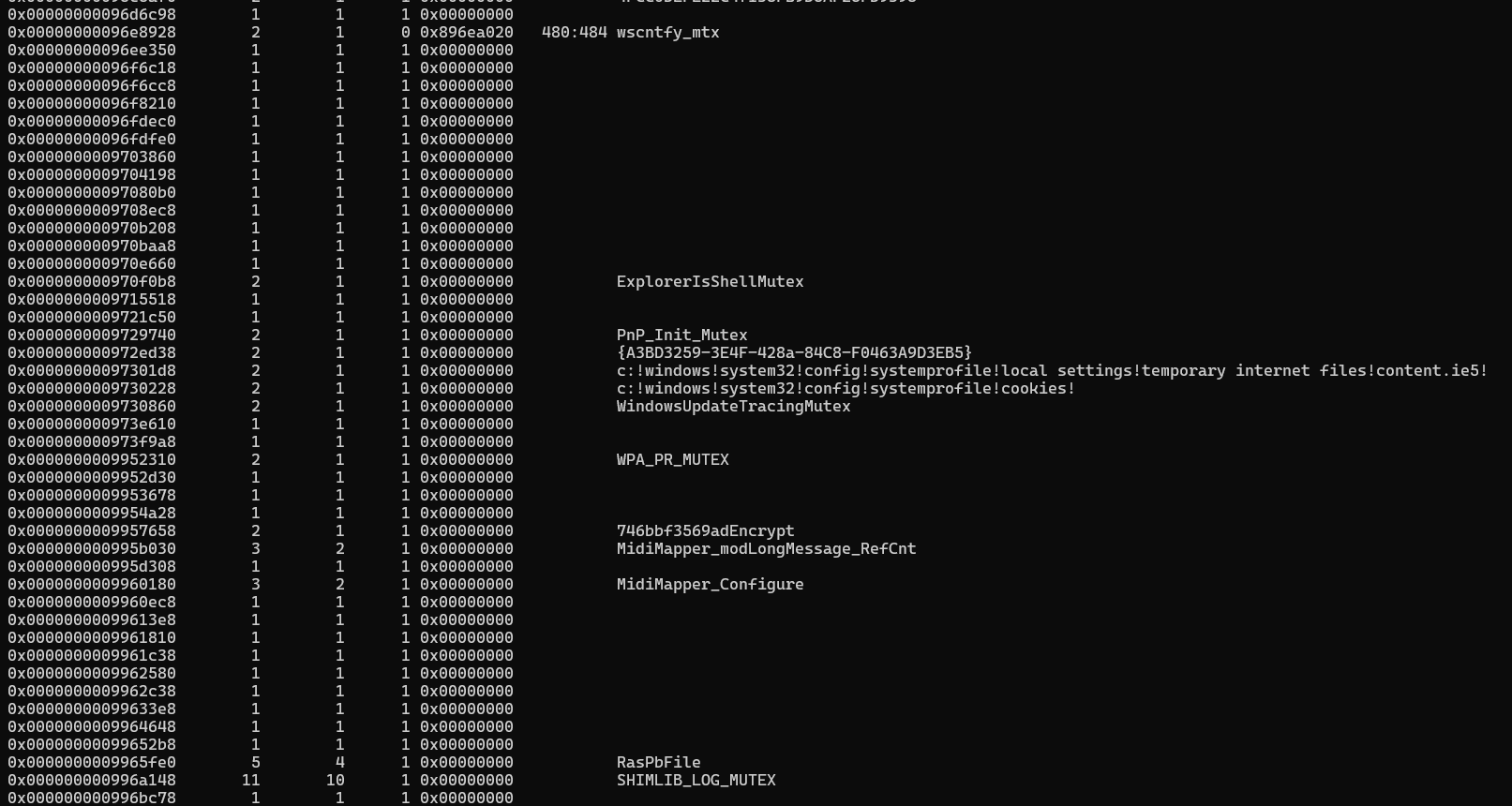




Explorer making connections suspicious

1. What mutex was created by the BlackEnergy malware?

**Hint:** Malware often creates unique mutexes to ensure a single instance is running or to signal infection.





1. **Service-Based Persistence**

**Goal:** Find the name of the suspicious service possibly used for persistence.





### Normal:

1. **What was the MD5 hash of the malicious USB device used to deliver the malware?**

**Flag:** B4644902ACAB4583A1D0F9F1A08FAA77

1. **What anti-forensics tool did the suspect install on their personal PC before going to the office?**

*Hint: Use Autopsy’s keyword search or look through Program Files or Prefetch.*

**Flag:** Veracrypt

1. **What Windows command was used to clear the event logs on the infected system?**

*Hint: Check shellbags or memory strings.*

**Flag:** wevtutil cl Security

1. **When was first contact from hacker with john Doe?**

Hint: Check outlook mail dates

Answer: Mon, Mar 31, 3:38 PMw3