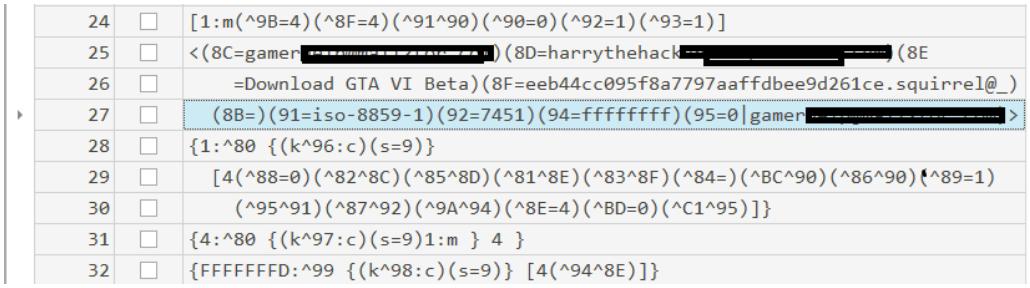
Endpoint Forensics

Investigation Overview

This report provides a detailed forensic analysis of an attack involving initial access through phishing, execution of malicious binaries, privilege escalation, credential dumping, and data exfiltration. The investigation was conducted using forensic tools such as FTK Imager, Autopsy, Sysmon, Timeline Explorer, and security event logs.

Initial Access

The disk image provided by the developer was imported into both **FTK Imager** and **Autopsy** for detailed analysis. The investigation revealed that the developer received an email flagged as **junk** by Mozilla Thunderbird. This email, suspected to be from an attacker, encouraged the developer to download a malicious file named **GTAVI**.

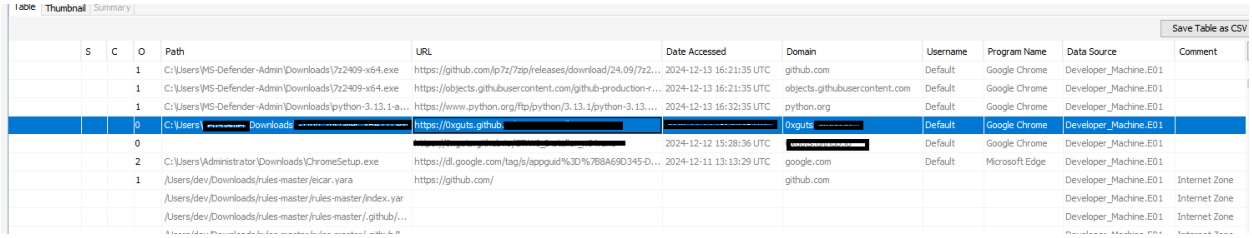


```
24  [1:m(^9B=4)(^8F=4)(^91^90)(^90=0)(^92=1)(^93=1)]
25  <(8C=gamer[redacted])(8D=harrythehack[redacted])(8E
26      =Download GTA VI Beta)(8F=eeb44cc095f8a7797aaffdbee9d261ce.squirrel@_)
27    (8B=)(91=iso-8859-1)(92=7451)(94=ffffffff)(95=0|gamer[redacted]>
28  {1:^80 {(k^96:c)(s=9)}
29    [4(^88=0)(^82^8C)(^85^8D)(^81^8E)(^83^8F)(^84=)(^BC^90)(^86^90)(^89=1)
30      (^95^91)(^87^92)(^9A^94)(^8E=4)(^BD=0)(^C1^95)]}
31  {4:^80 {(k^97:c)(s=9)1:m } 4 }
32  {FFFFFFFD:^99 {(k^98:c)(s=9)} [4(^94^8E)]}
```

To confirm the details, Thunderbird logs, including both the **Junk** and **Inbox** folders, were exported. **Timeline Explorer** was utilised to examine the email received by the user, allowing for pinpointing the time and context of the malicious email.

After reading the email, the developer proceeded to download a **binary file** disguised as part of the GTAVI application. The URL from which the binary was downloaded was

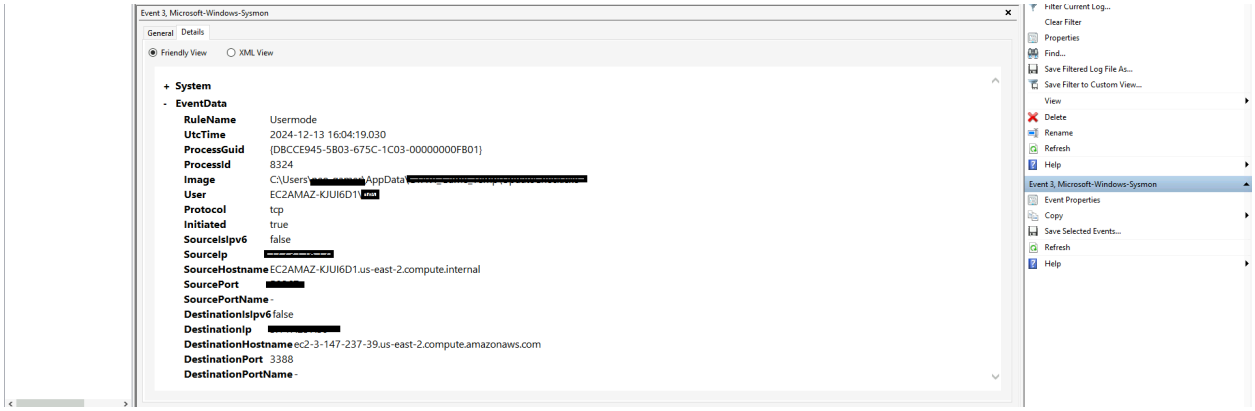
identified as:



To gather additional evidence, **system logs, security logs, and user activity data** were exported. A search was conducted in **Registry Explorer** using terms related to the **GTAVI binary**, leading to the location of the downloaded malicious file on the system.

Execution

Autopsy was used to find that the attacker created a directory to store additional malicious tools. The directory was named GTA********** and was located at C:\Users******\AppData.



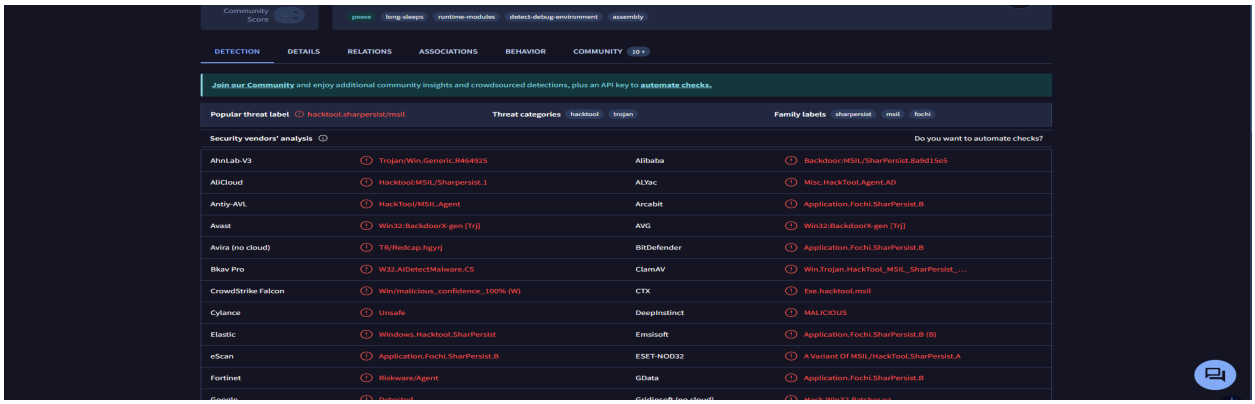
The binary was executed, establishing a connection via port 3388. This information guided the search in Sysmon logs, revealing the execution and connection used by the attacker, specifically involving port 3388. Port 3388/TCP is associated with **Trojan.Mitglieder.S**, a Trojan that opens a backdoor and runs a proxy server, enabling it to connect to remote websites and transmit gathered information from the compromised system. Additionally,

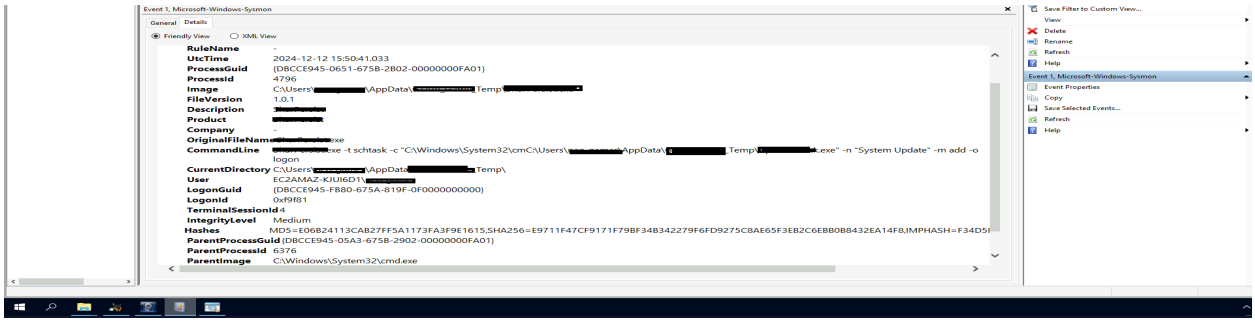
Trojan-Dropper.Win32.Googite.b is an unauthenticated remote command execution malware that listens on TCP ports 3388, 4488, and 10002. It drops executables in the Windows and SysWOW64 directories, allowing third-party attackers to execute commands remotely.

Reference: MVID-2021-0254

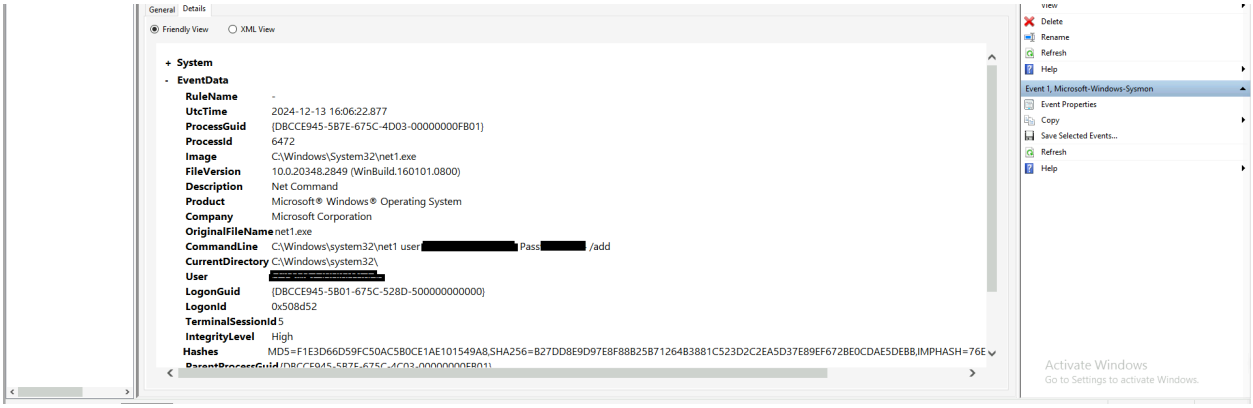
Persistence

One of the dropped malicious tools was used to achieve persistence by creating a scheduled task. The tool responsible for this action was identified by filtering Sysmon Event ID 3 for *****.exe. The attacker also created a new user account. The username and password associated with the newly created account were identified through Sysmon Event ID 1, which is often associated with new user account creation.





The attacker created a **new user account** to maintain persistent access to the system. The system logs and security events revealed that an **administrative user** was manually added:



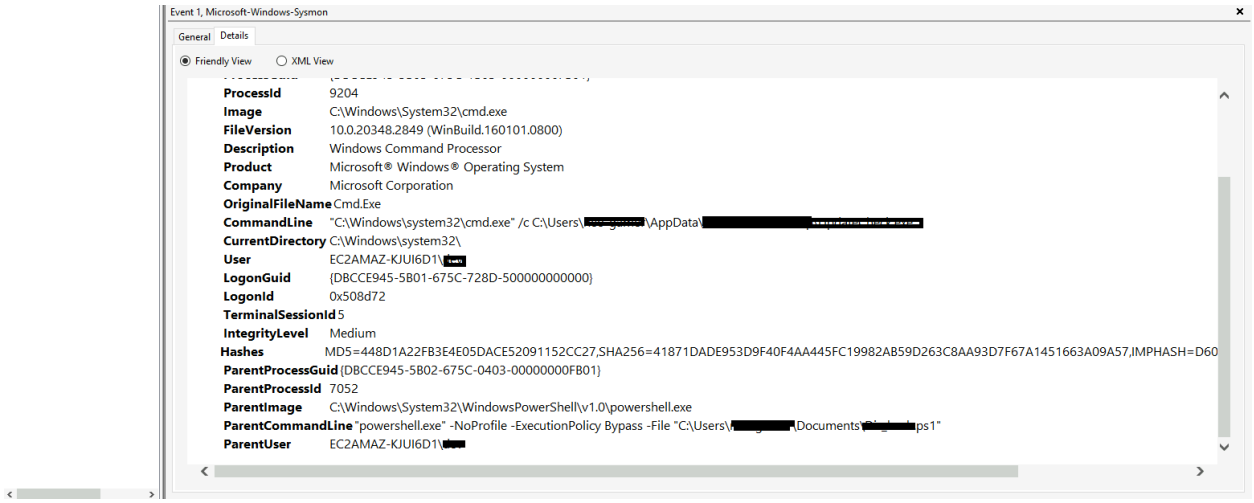
This account was used to execute **privileged commands**, modify **system configurations**, and escalate access within the environment.

Privilege Escalation

The attacker altered a script to add the current user to the Administrator group. The path of the modified script was identified using Sysmon Event ID 1, searching for .ps1 files associated with PowerShell scripts. The script modified by the attacker to add the newly created user to the Administrators group was located at:

Script Path:

C:\Users****\Documents*****.ps1



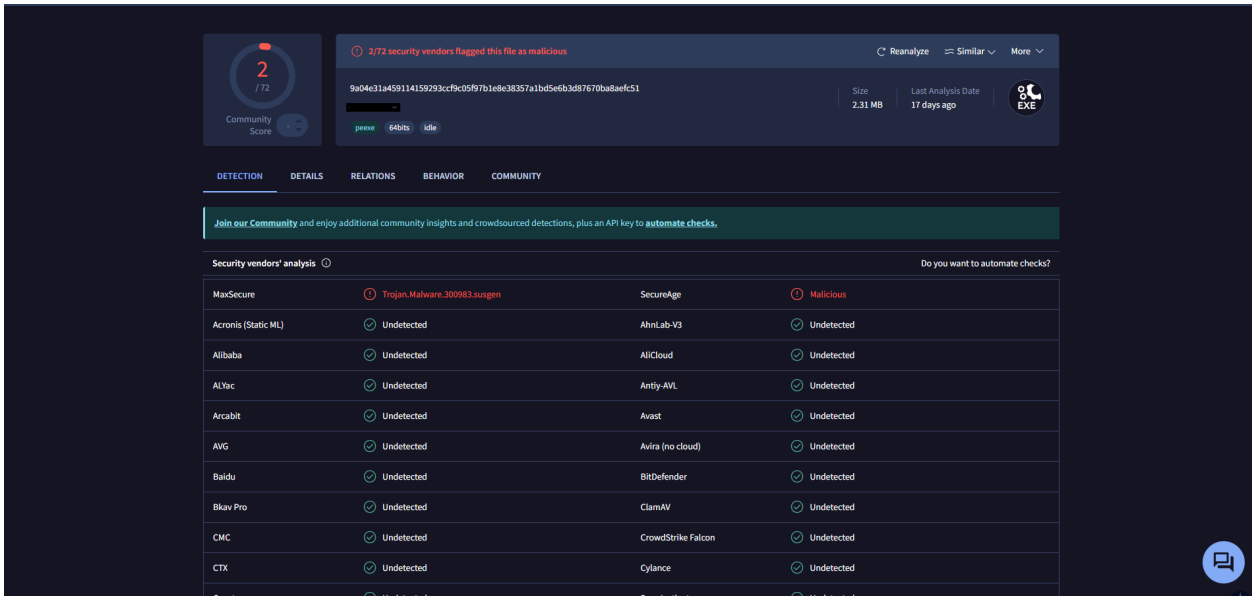
After gaining **Administrator privileges**, the attacker was unable to execute commands as the **SYSTEM user**. **Analysis revealed that a binary was replaced**, leading to **unexpected command execution**.

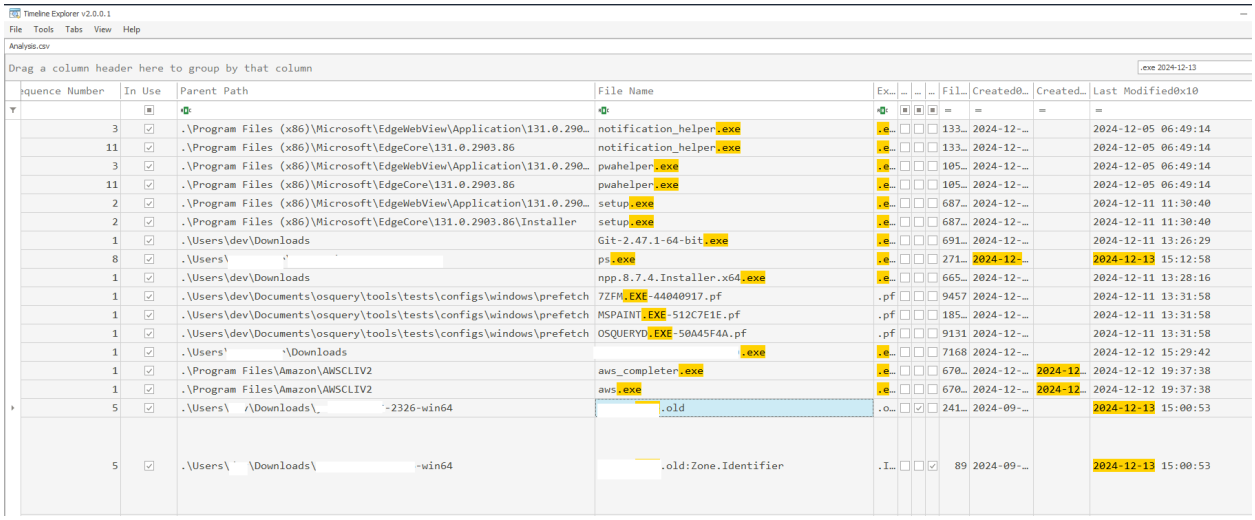
The investigation initially focused on **binaries commonly targeted by attackers**, including **PowerShell binaries, Ultima.exe, Consent.exe, and cmd.exe**. However, deeper analysis determined that these binaries remained unchanged, indicating that the attacker had used a more subtle approach.

A forensic examination of **$MFT (Master File Table) records** was conducted to track file modifications and execution history. This analysis uncovered the actual modified binary, which had been **replaced with an older, vulnerable version** to facilitate privilege escalation.

This method aligns with **T1546.015 – Binary Path Hijacking**, where attackers exploit trusted binary execution paths to bypass security controls and escalate privileges.

Investigating binary hashes is crucial in detecting unauthorised modifications. Comparing them against trusted sources helps identify system compromises that may not be immediately evident through standard security monitoring.

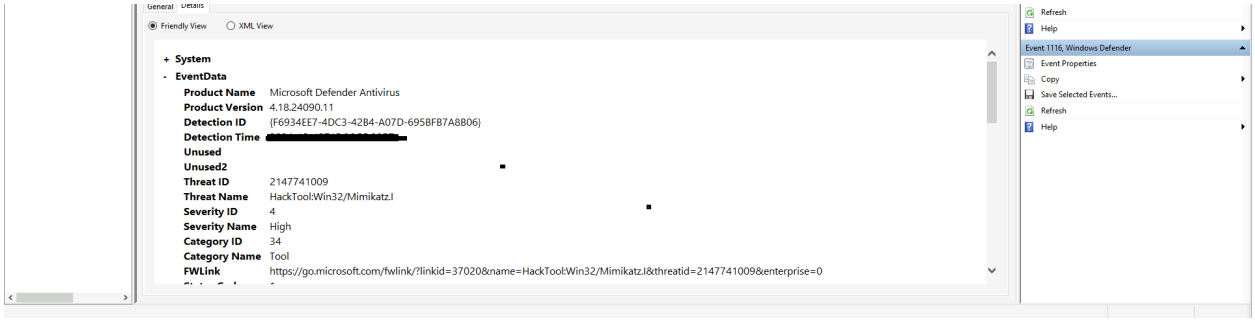




Credential Access

Credential dumping activity was detected by **Microsoft Defender**. The attacker executed a command to dump credentials. **Microsoft Defender event logs** were analysed to identify the **exact timestamp** of the activity.

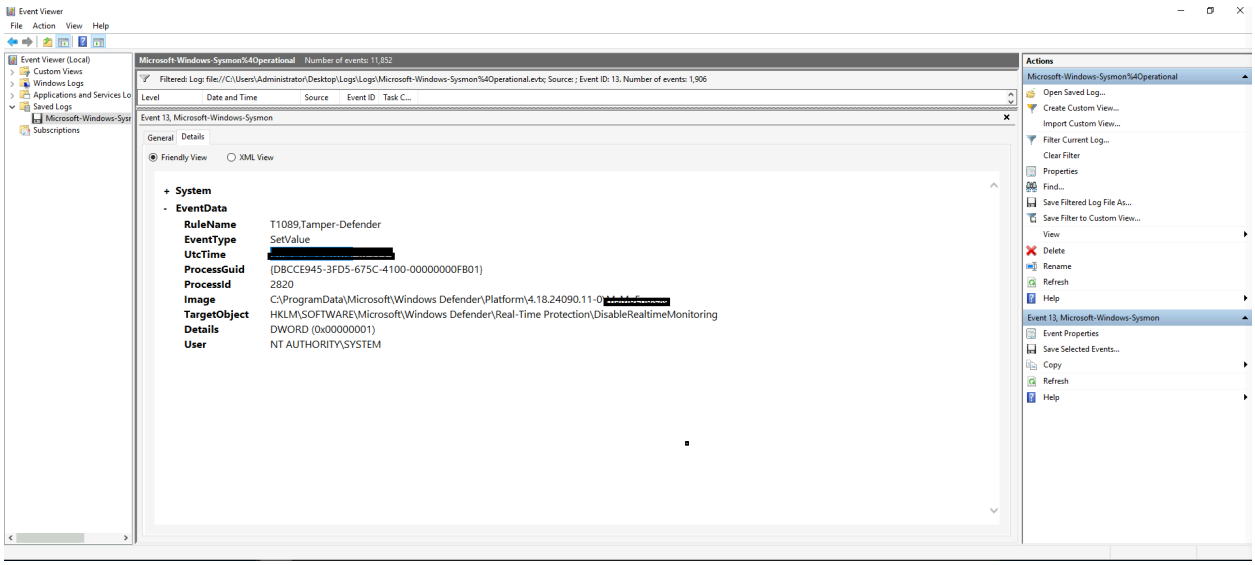
Understanding common tools used by attackers for **credential dumping** is essential, as well as knowledge of **Windows components** that store credentials, which are commonly targeted.



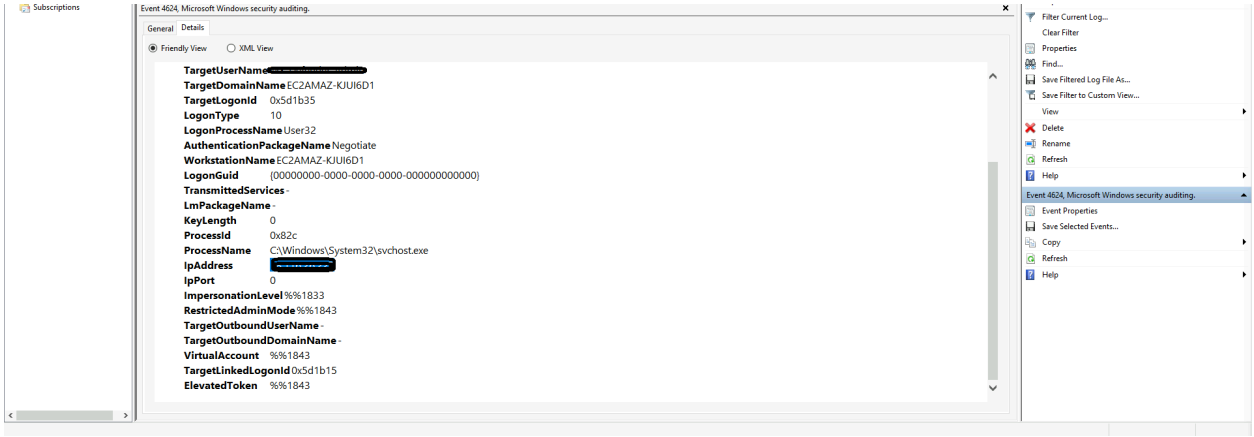
Defense Evasion

The attacker **modified the Windows registry** to disable **Microsoft Defender's Real-Time Monitoring** feature. This action was captured in the **security event logs** under **Event ID 4738**, indicating **user account modifications**.

Disabling Real-Time Monitoring significantly weakens system security, preventing Defender from actively scanning and blocking threats.



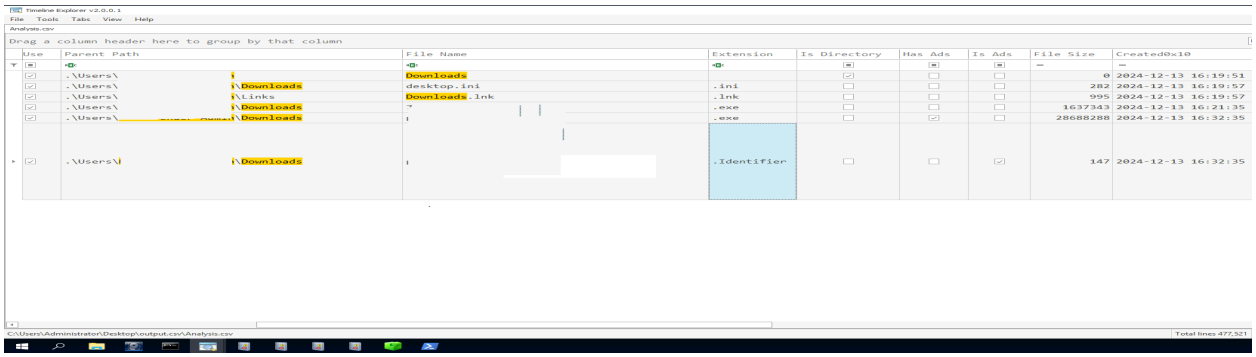
Additionally, the attacker initiated a **login using the newly created user account**. The investigation aims to **identify the IP address from which this login occurred** to assess potential malicious activity and track the origin of the breach. This information is crucial in understanding **how the attacker accessed the system** and whether multiple compromised sources were involved.



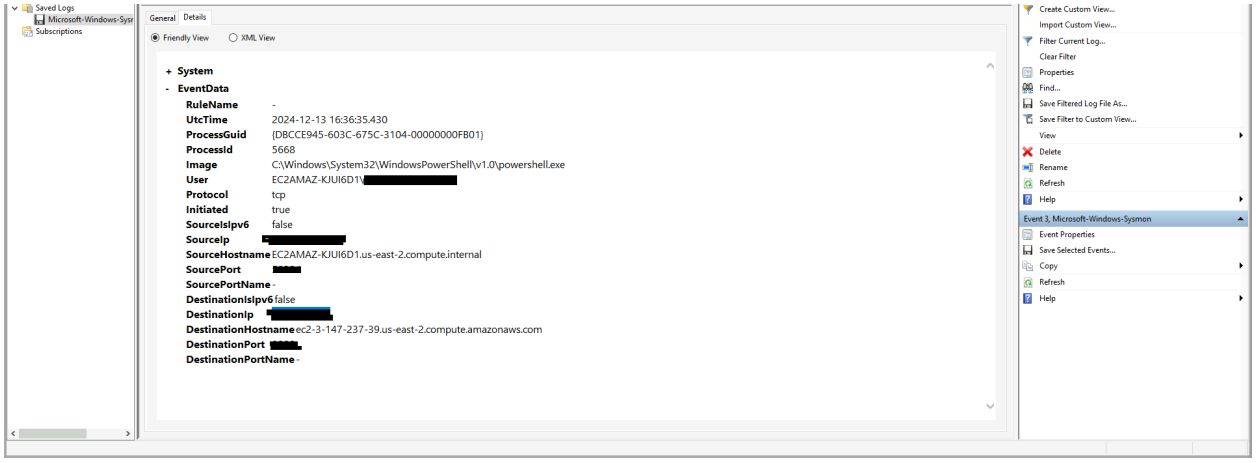
Collection & Exfiltration

An in-depth analysis of **system logs** was conducted to track the activity of the newly created user account. The investigation focused on identifying files that were downloaded and subsequently archived by the attacker. By reviewing **file creation events** within system logs, particularly **Sysmon Event ID 11**, the sequence of actions taken was reconstructed.

Further analysis revealed that the attacker **archived specific directories**, likely preparing them for exfiltration. Correlating **event timestamps and process execution logs** provided insight into which directories were targeted. A final **compressed file** containing the archived data was identified, confirming the attacker's intent to extract information from the system.



Additionally, a series of **commands** suggested an attempt to transfer the archived data to an external server. The analysis of **process execution logs and network activity** helped outline the potential method of exfiltration.



Conclusion

The forensic investigation revealed a **targeted attack** that involved:

- **Phishing (Initial Access)** via **malicious email attachment**
- **Execution** of a **Trojan** to establish a backdoor
- **Privilege Escalation** through **script modifications**
- **Credential Dumping** to gain additional access
- **Persistence** using a **new administrative account**
- **Defense Evasion** by disabling **Microsoft Defender**
- **Data Exfiltration** through an **archived file transfer**

The attack demonstrated **sophisticated techniques**, including **binary tampering, credential harvesting, and registry modifications** to bypass security controls.

Recommendations:

Conduct an organisation-wide security audit

Implement endpoint detection and response (EDR) solutions

Enable logging and alerting on privilege escalation attempts

Regularly update and patch vulnerable software

Train employees to recognise phishing emails