Official incident report

Event ID: 212

Rule Name: SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected

Made By

LinkedIn: Engineer.Ahmed Mansour

Link: https://www.linkedin.com/in/ahmed-mansour-5631b5323/

Github link: https://github.com/AhmedMansour93

Table of contents

Official incident report **1**

Event ID: 212 **1**

Rule Name: SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected **1**

Table of contents **2**

Event Details **3**

Network Information Details **4**

Analysis **5**

Log management **5**

Security Email **10**

Detection **11**

Threat intelligence **11**

Endpoint Security **12**

Conclusion **13**

Event Details

Event ID:
212

Event Date and Time:
Dec, 27, 2023, 11:22 AM

Rule:
SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected

Level:
Security Analyst

Hostname:
Arthur

Process Name:
EmailDownloader.exe

File Hash:
cd2ba296828660ecd07a36e8931b851dda0802069ed926b3161745aae9aa6daa

Process Path:
C:\Users\LetsDefend\Downloads\EmailDownloader.exe

Parent Process:
C:\Windows\Explorer.EXE

Device Action:
Allowed

Command Line:
C:\Users\LetsDefend\Downloads\EmailDownloader.exe

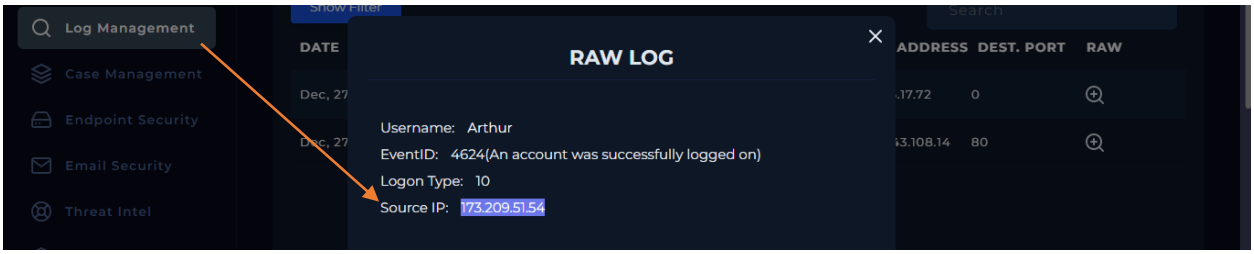
Trigger Reason:
Unusual or suspicious patterns of behavior linked to the hash have been identified, indicating potential malicious intent.

Device Action:
Allowed

Network Information Details

Destination Address:
172.16.17.72 internal

The Attacker IP:
173.209.51.54 external

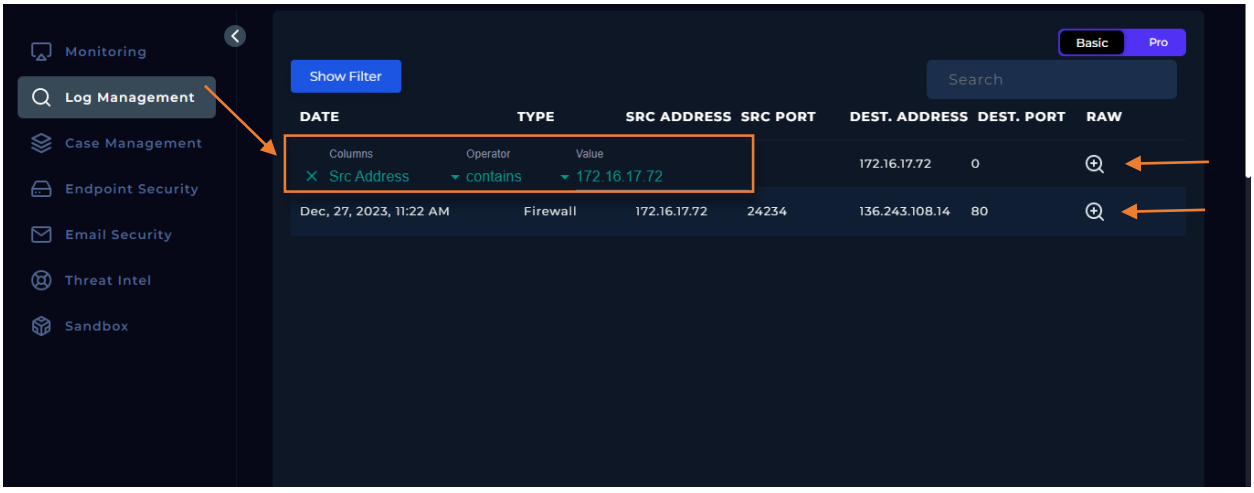


Analysis:

Log Management

We'll proceed by entering the destination IP address and reviewing the results.

Please refer to the attached image for further details regarding the attack.



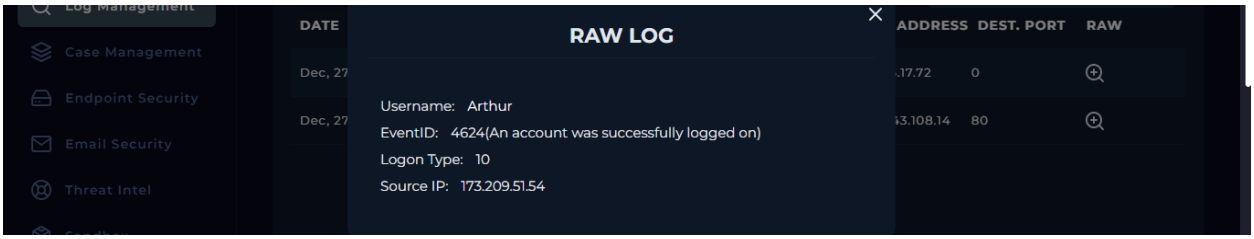
2 Logs records for the destination IP.

Please refer to the attached image for further details regarding the attack.

We will explain all of them step by step

Log Analysis

- **Log1:**



- **Event ID 4624 (An account was successfully logged on):**
  - **Event ID 4624** is a Windows Security Event that indicates a successful user login. This is a critical event for tracking user activity on a system. It's commonly used for auditing, as it provides details on who logged in and from where.

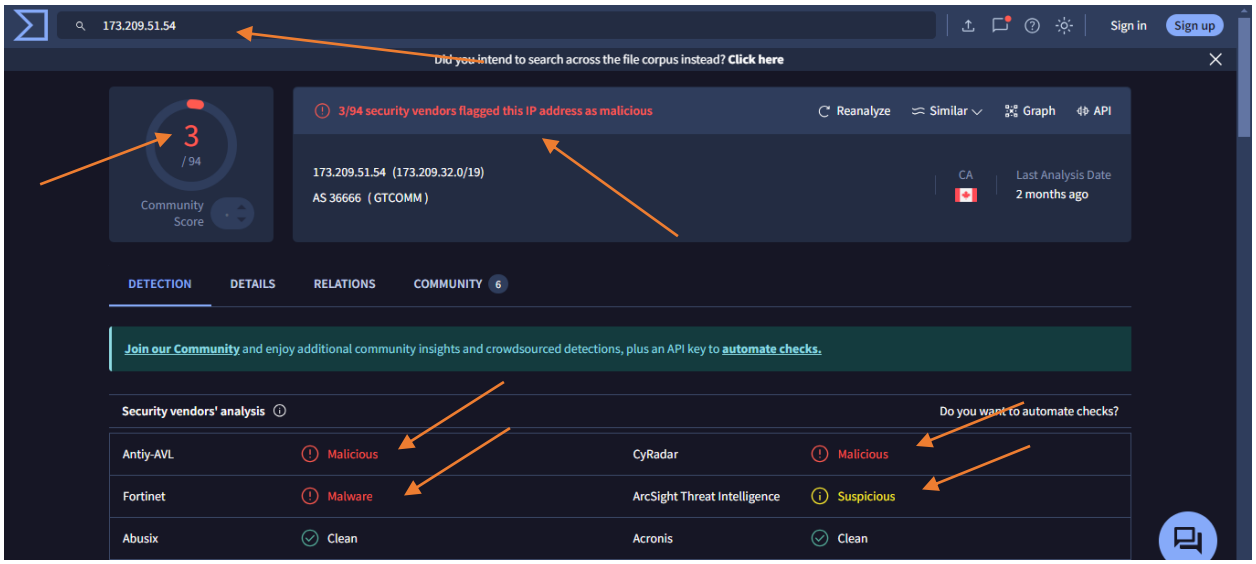
- **Username: Arthur:**
  - This indicates that the user **Arthur** successfully logged in. Monitoring user logins is crucial to detect unauthorized access or abnormal login behavior.

- **Logon Type 10:**
  - **Logon Type 10** represents a **Remote Interactive Logon** via **Remote Desktop Protocol (RDP)**. This means that user **Arthur** logged into the system remotely using RDP, a common method for managing servers or systems from another location.
  - This type of logon is frequently monitored for potential security risks, as RDP can be exploited for brute-force attacks or unauthorized access if not properly secured.

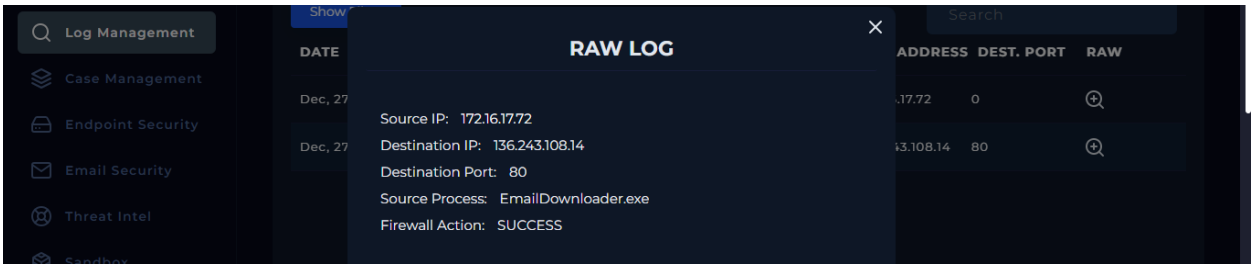
- **IP: 173.209.51.54:**
  - The IP address shows where the login attempt originated from. In this case, the IP **173.209.51.54** indicates an external machine. This is important to investigate if the IP is from an expected or trusted source, especially considering the login was remote (via RDP).
  - If this IP address doesn't belong to an authorized user or network, it could signify a potential unauthorized access attempt.

- **Checking The IP: 173.209.51.54 on Virus Total**

Check the attached photo [The reference link]



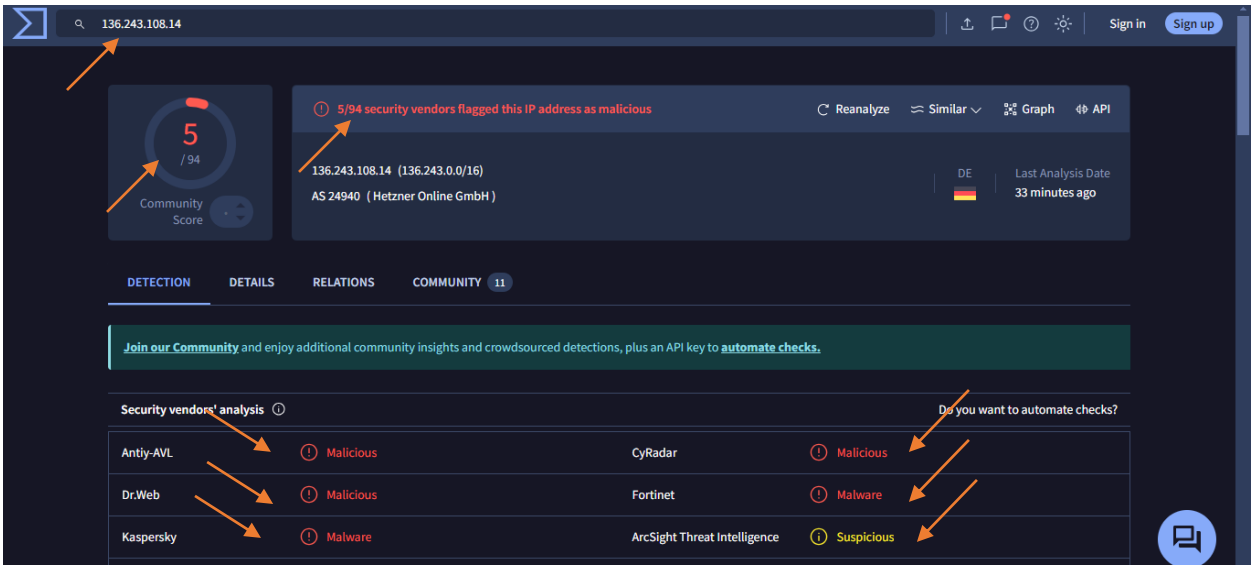
- **Log2:**



- **Our private IP: 172.16.17.72:**
  - The source IP **172.16.17.72** is part of the private IP range .
- **Destination IP: 136.243.108.14:**
  - The destination IP **136.243.108.14** is a public IP address, representing an external server or service that the internal machine is communicating with. External IP addresses should be carefully monitored, especially when sensitive processes or applications are involved.
- **Destination Port: 80:**
  - **Port 80** is the default port for **HTTP (HyperText Transfer Protocol)**, used for unsecured web traffic. This indicates that the source process is attempting to connect to a website or web service over an unencrypted connection.
  - The absence of encryption (such as HTTPS) could make this traffic vulnerable to interception or manipulation.
- **Source Process: EmailDownloader.exe:**
  - The process **EmailDownloader.exe** is initiating the connection to the external IP. This is potentially a legitimate process, but it requires further investigation. Malicious actors often disguise malware or suspicious activity under seemingly legitimate process names, especially when dealing with downloading or network-related actions.
  - Investigate whether this process is authorized and behaves as expected, or if it's part of suspicious activity like data exfiltration or malware delivery.
- **Firewall Action: SUCCESS:**
  - The firewall allowed the connection. While this doesn't indicate whether the traffic is malicious, it confirms that the attempted communication was successful and passed through the firewall without being blocked.
  - This also means it's crucial to have proper rules and logging in place to monitor outgoing connections, especially to external IPs and unencrypted channels.

- **Checking The IP: 136.243.108.14 on Virus Total**

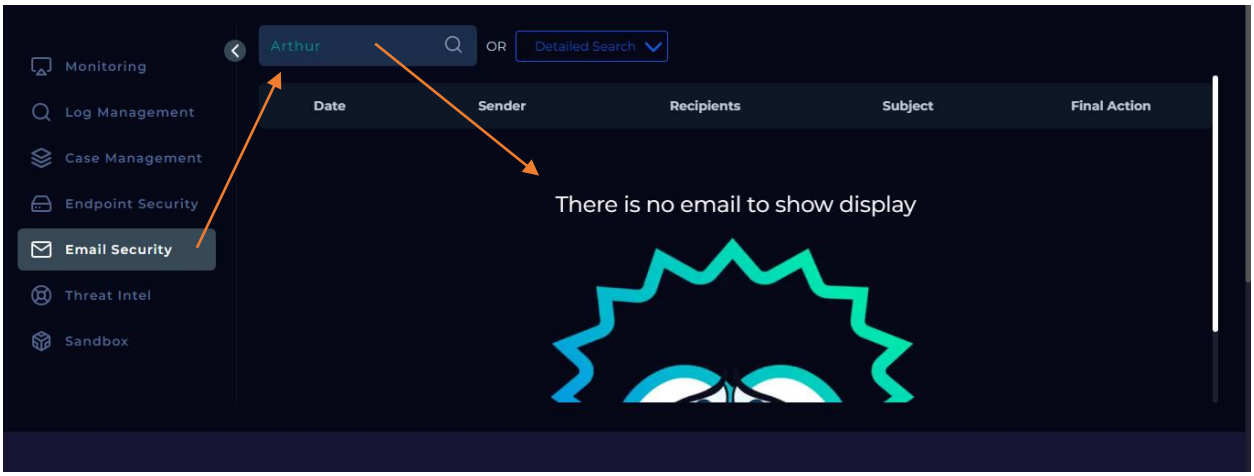
Check the attached photo [The reference link]



Overall Analysis:

- **Log Management 1:** Indicates a remote RDP login by user **Arthur** from an external IP. The key question is whether this RDP login was expected or authorized, and if the external IP is recognized or flagged as suspicious.
- **Log Management 2:** Describes an internal machine connecting to an external IP over HTTP using a process called **EmailDownloader.exe**. While the connection succeeded, this activity could pose a security risk if the destination is untrusted, or the process is part of a malware campaign.

Email Security:



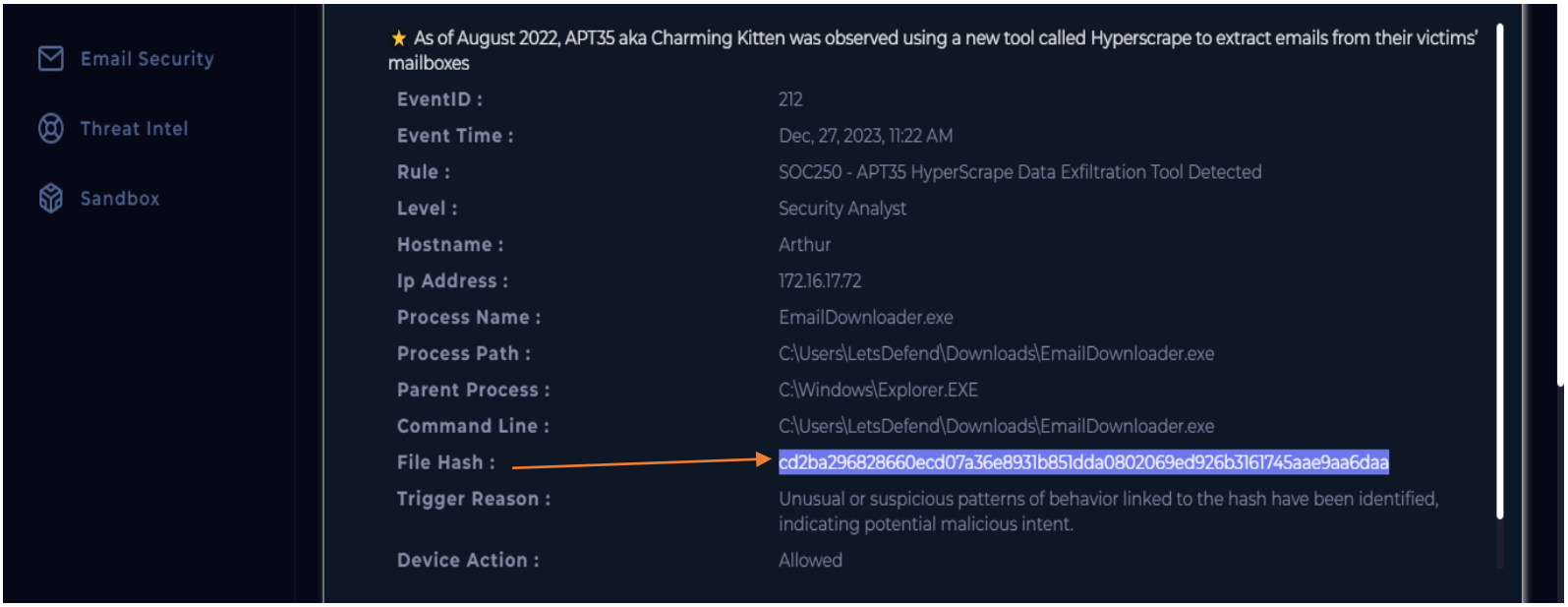
Despite entering the source host name in the email security section, no emails have been sent, indicating that the attack was not executed

Detection:

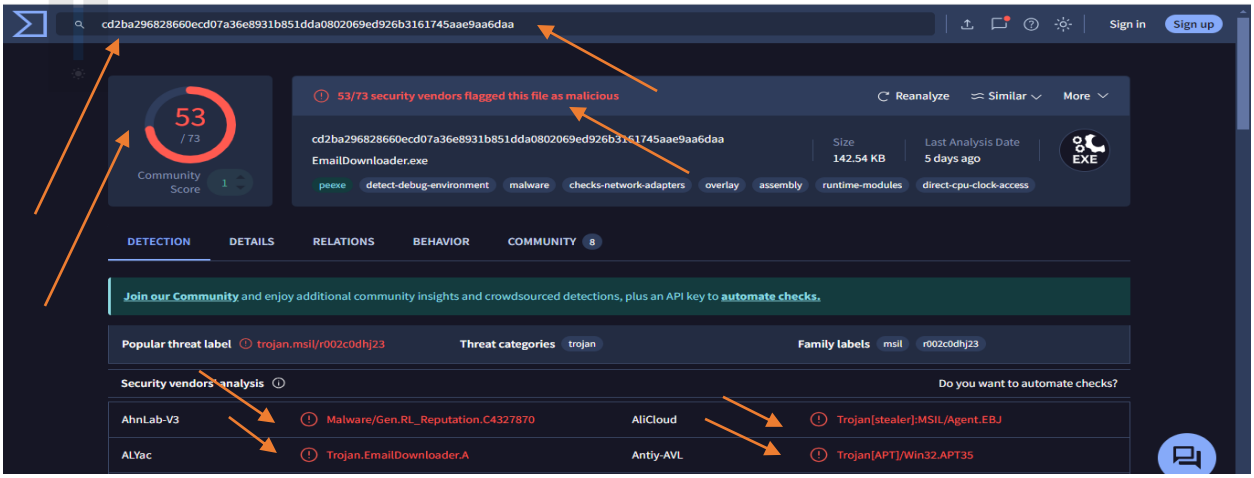
Threat Intelligence Results

File Hash

Check the attached photo



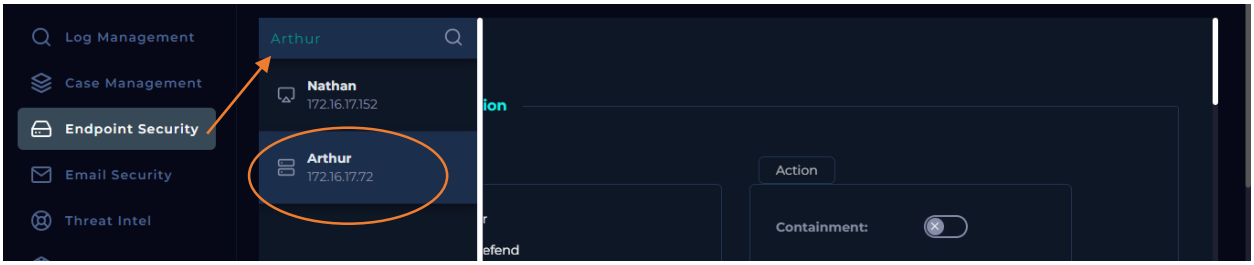
File Hash Analysis on VirusTotal



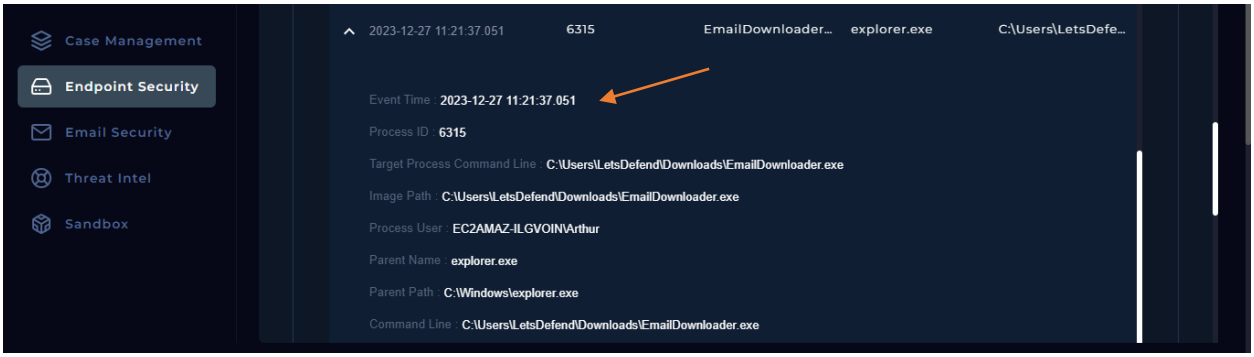
VirusTotal Analysis:

- [Reference link]

Endpoint Security:

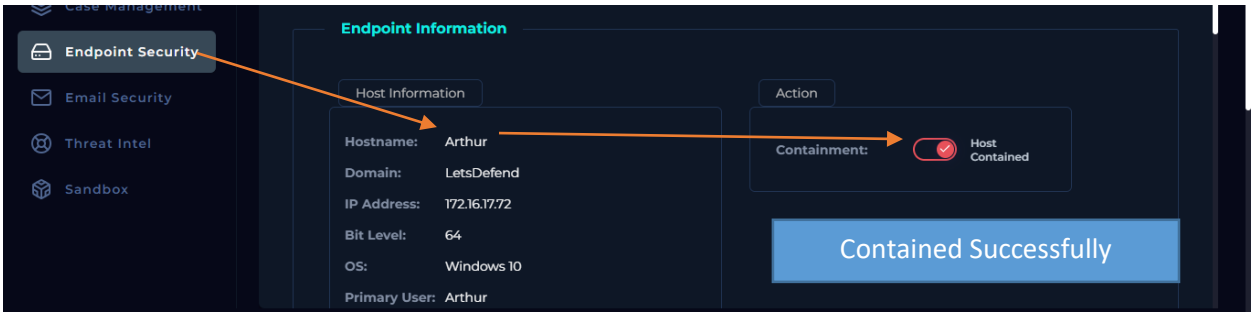


We must carefully review the following section, paying particular attention to the processes involved.



At the specified time, the user **Arthur** executed a file named **EmailDownloader.exe** located in the **Downloads** folder. The process was initiated by **explorer.exe**, suggesting it was likely started manually through the Windows File Explorer interface.

- **Based on our analysis, the reconnaissance activity identified is focused on gathering victim identity information.**
- **The device must be Contain. And we contained Successfully**.



Conclusion:

The investigation into Event ID 212, which involved the detection of the APT35 HyperScrape Data Exfiltration Tool, revealed a high-risk situation targeting host *Arthur*. The suspicious process *EmailDownloader.exe* was executed on December 27, 2023, via a remote login session through Remote Desktop Protocol (RDP) from an external IP address, 173.209.51.54. This RDP session was initiated with logon type 10, indicating a remote interactive session. The external IP used in this connection is a significant indicator of potential unauthorized access or malicious activity.

Our log analysis confirmed two key findings: first, the successful login of the user *Arthur* remotely, and second, the initiation of communication from *EmailDownloader.exe* to the external IP address 136.243.108.14 over port 80 (HTTP), an unencrypted protocol. While *EmailDownloader.exe* could appear to be a legitimate process, the connection to an untrusted external server, combined with the suspicious file hash, suggests it is part of a wider data exfiltration attempt by the APT35 group, known for conducting reconnaissance and information-gathering operations.

Threat intelligence verified that the external IP and file hash were linked to malicious activity, confirming that the purpose of this incident was likely identity reconnaissance and potential data exfiltration. Despite no email traffic being detected from the host, the abnormal process behavior and unauthorized RDP connection necessitated swift containment. The device was successfully isolated to prevent further unauthorized access or data leakage.

This incident highlights the critical importance of monitoring remote access and unencrypted outbound traffic. Our prompt detection, detailed analysis, and swift containment ensured that the organization faced no operational or reputational damage from this attack.