Official incident report

Event ID: 153

Rule Name: SOC202 - FakeGPT Malicious Chrome Extension

Made By

LinkedIn: Engineer.Ahmed Mansour

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

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

Table of contents

Event Details

Event ID:
153

Event Date and Time:
May, 29, 2023, 01:01 PM

Rule:
SOC202 - FakeGPT Malicious Chrome Extension

Level:
Security Analyst

Hostname:
Samuel

File name:
ab.exe

File Hash:
0b486fe0503524cfe4726a4022fa6a68

File size:
775.50 Kb

File Name:
hacfaophiklaeolhnmckojjjjbnappen.crx

File Path:
C:\Users\LetsDefend\Download\hacfaophiklaeolhnmckojjjjbnappen.crx

File Hash:
7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e152a4669

Device Action:
Allowed

Command Line:
chrome.exe --single-argument
C:\Users\LetsDefend\Download\hacfaophiklaeolhnmckojjjjbnappen.crx

Trigger Reason:
Suspicious extension added to the browser.

Device Action:
Allowed

Network Information Details

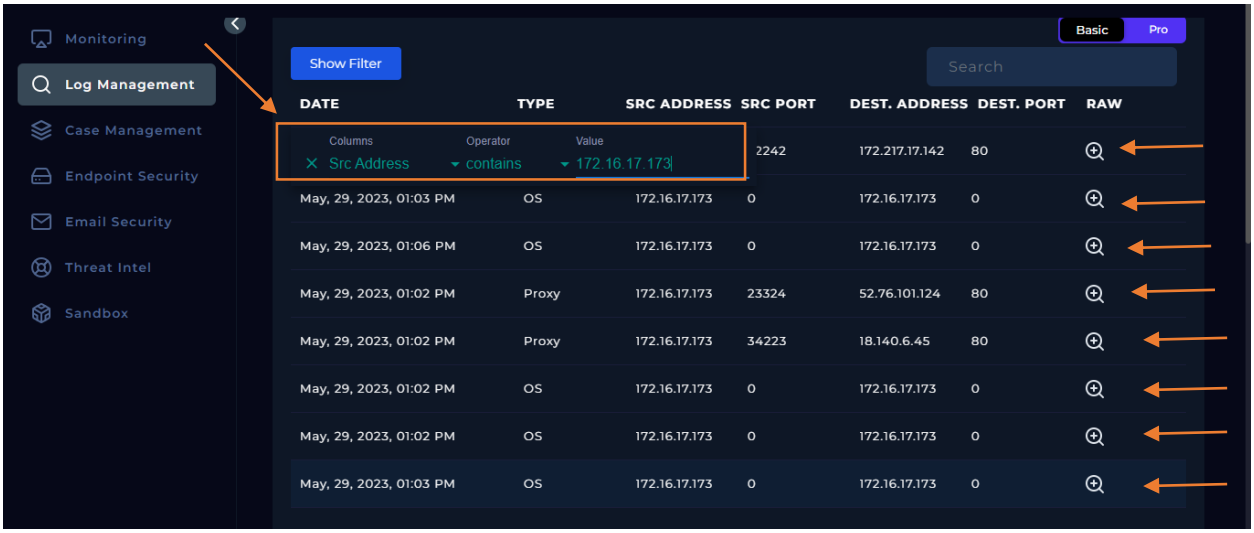
Destination Address:
172.16.17.173 internal

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.



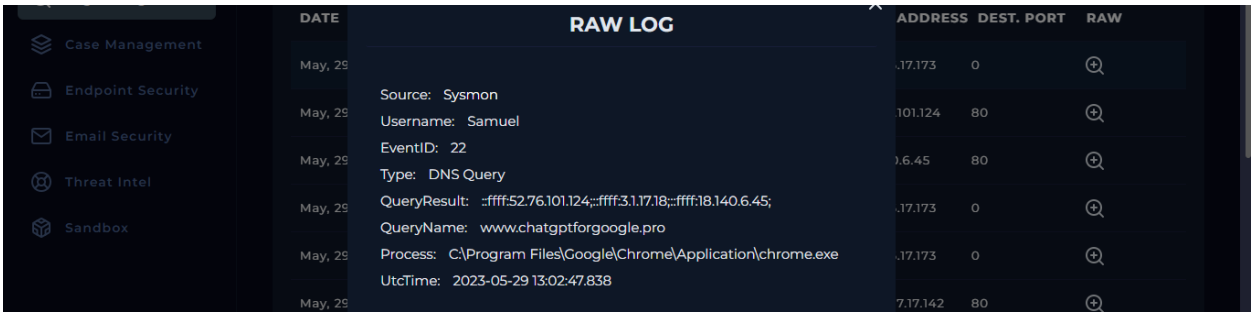
8 Logs records for the destination IP.

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

We will explain all of them step by step

Log Analysis

- **Log1:**

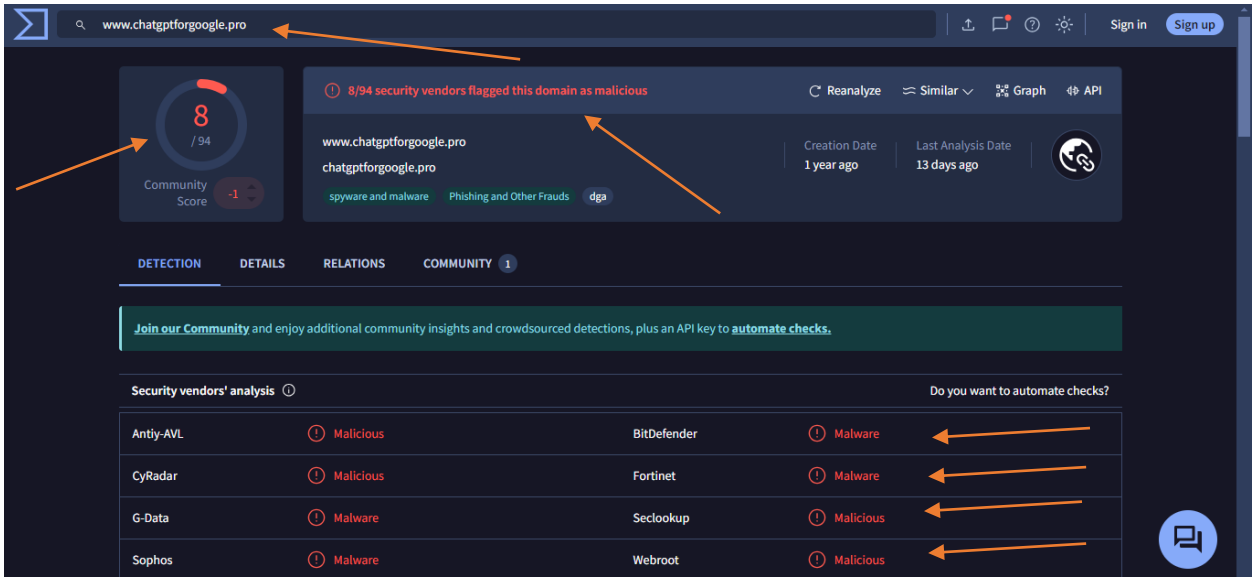


- **Source**: Sysmon
- **Event Type**: DNS Query (EventID 22)
- **Summary**: The user "Samuel" performed a DNS query for the domain `www.chatgptforgoogle.pro`. The query resolved to three IPv6 addresses: `::ffff:52.76.101.124`, `::ffff:3.1.17.18`, and `::ffff:18.140.6.45`. The query originated from the Chrome browser on the system.

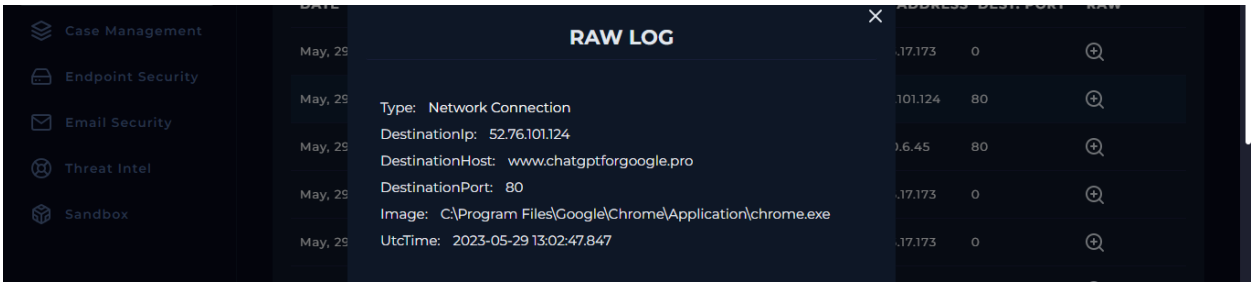
- Key Insight**:** A DNS resolution for an external domain was made.

- **Checking The Request URL: www.chatgptforgoogle.pro on Virus Total**

Check the attached photo [The reference link]



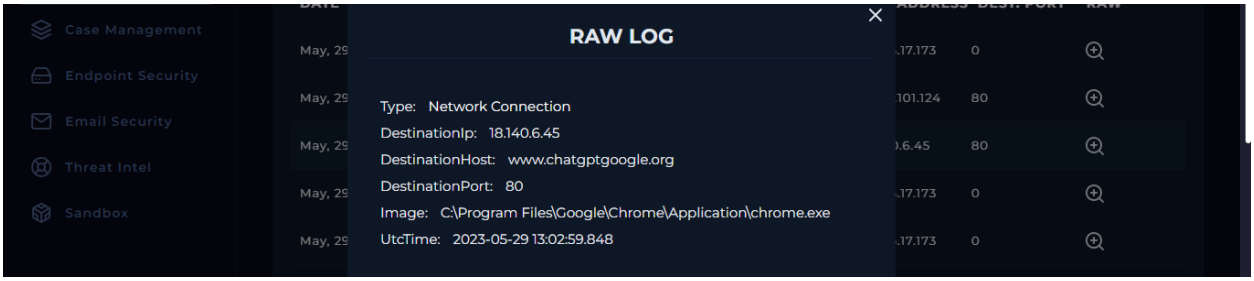
- **Log2:**



- **Source**: Network Connection
- **Summary**: A network connection was established from Chrome to the IP address `52.76.101.124` on port 80 (HTTP) corresponding to the domain `www.chatgptforgoogle.pro`. The time matches the query in Log 1, confirming the user accessed this domain.

- **Key Insight**: The user connected to one of the IP addresses resolved from the DNS query

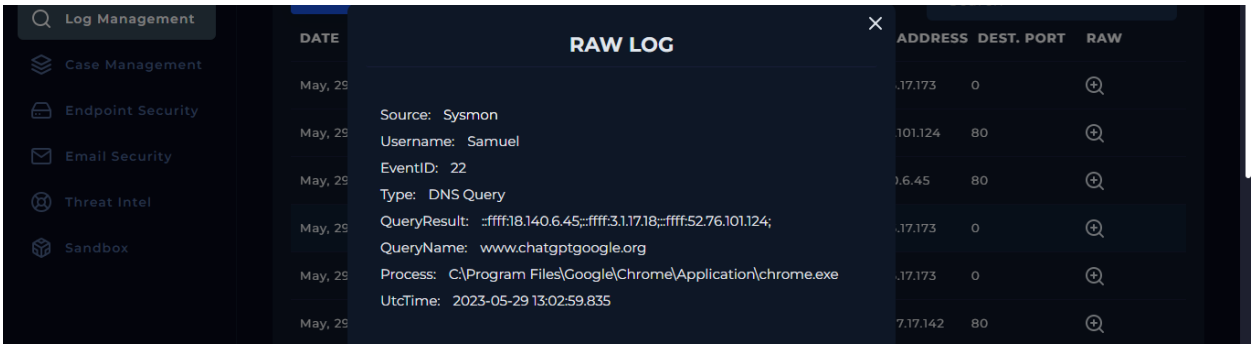
- **Log3:**



- **Source**: Network Connection
- **Summary**: A network connection was made to the IP address `18.140.6.45` on port 80 (HTTP) to the domain `www.chatgptgoogle.org`. This connection is separate from the previous one, although similar in nature.

- **Key Insight**: The user accessed a different domain, but the IP `18.140.6.45` matches an IP from Log 1, suggesting domain redirection or related services.

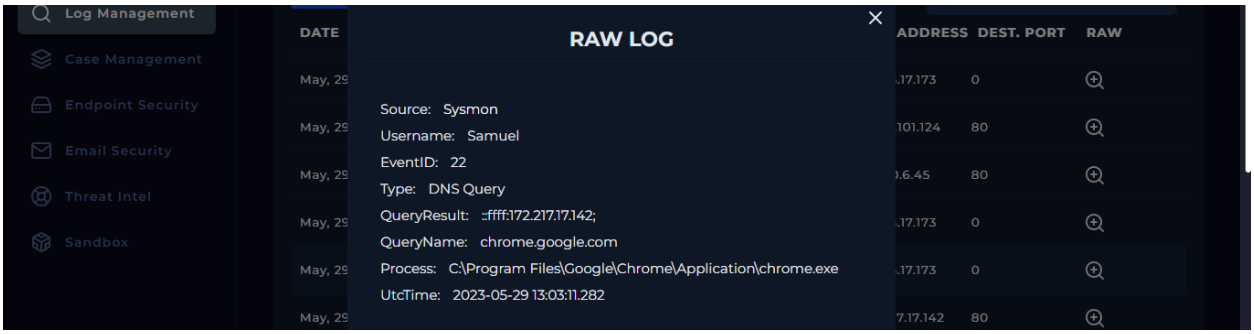
- **Log4:**



- **Source**: Sysmon
- **Event Type**: DNS Query (EventID 22)
- **Summary**: A DNS query for the domain `www.chatgptgoogle.org` was made, resolving to three IPv6 addresses: `::ffff:18.140.6.45`, `::ffff:3.1.17.18`, and `::ffff:52.76.101.124`. This correlates with Log 3, confirming DNS resolution for this domain.

- **Key Insight**: This DNS query resulted in similar IP addresses, likely indicating related

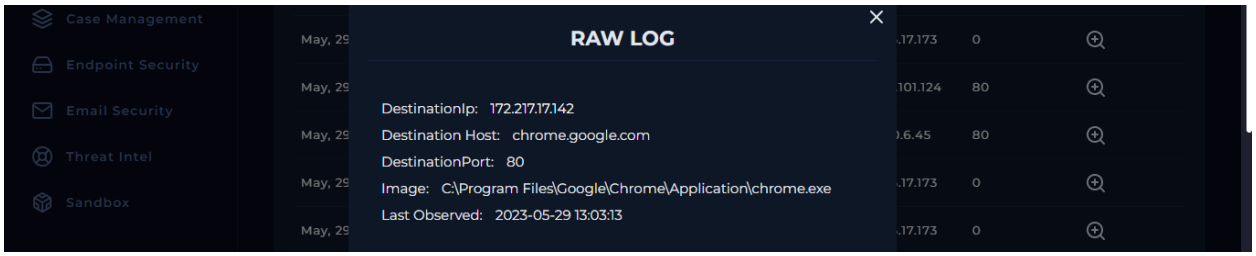
- **Log5:**



- **Source**: Sysmon
- **Event Type**: DNS Query (EventID 22)
- **Summary**: A DNS query for the domain `chrome.google.com` was made, resolving to the single IP address `::ffff:172.217.17.142`. This suggests the user was accessing official Google services through the Chrome browser.

- **Key Insight**: The user accessed a legitimate Google domain.

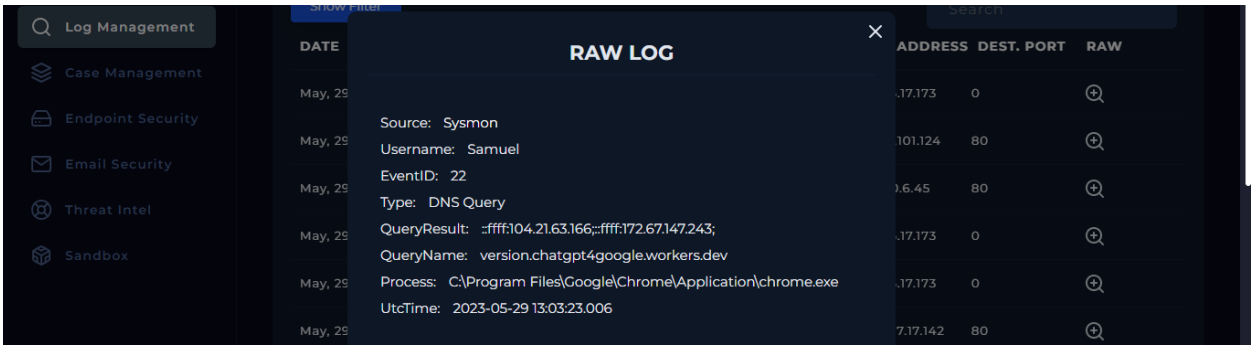
- **Log6:**



- **Source**: Network Connection
- **Summary**: A network connection was established to the IP address `172.217.17.142` (associated with `chrome.google.com`) over port 80 (HTTP). This corresponds to the DNS query in Log 5.

- **Key Insight**: The user successfully connected to Google's official service.

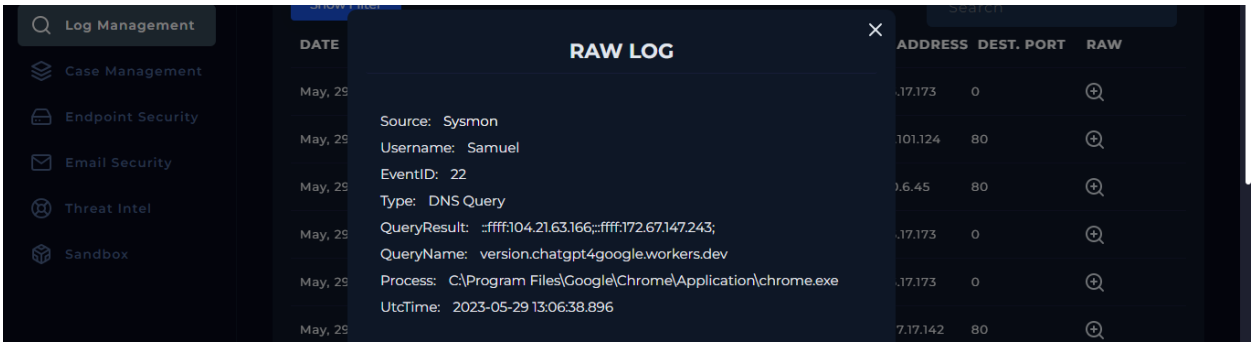
- **Log7:**



- **Source**: Sysmon
- **Event Type**: DNS Query (EventID 22)
- **Summary**: A DNS query for the domain `version.chatgpt4google.workers.dev` was made, resolving to two IP addresses: `::ffff:104.21.63.166` and `::ffff:172.67.147.243`. The query was performed by Chrome.

- **Key Insight**: The user accessed another external service related to ChatGPT or Google extensions.

- **Log8:**



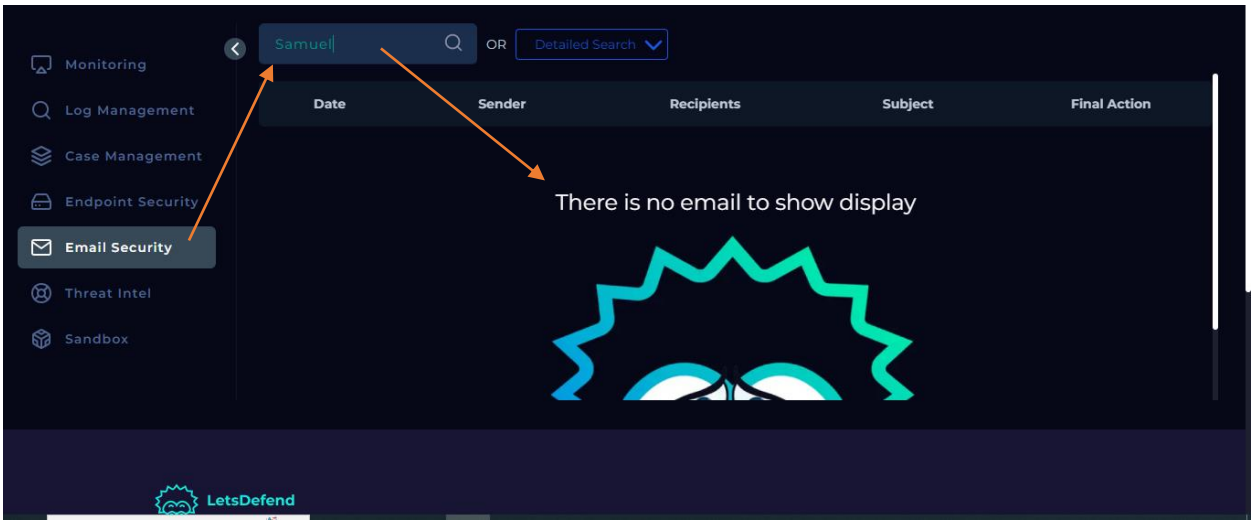
- **Source**: Sysmon
- **Event Type**: DNS Query (EventID 22)
- **Summary**: A similar DNS query for `version.chatgpt4google.workers.dev` was made, resolving to the same IP addresses as in Log 7, but at a later time.

- Key Insight**: The user repeatedly accessed this domain.**

Summary for Each Log:

1. **Log 1**: DNS query for `www.chatgptforgoogle.pro`, resolving to multiple IP addresses.
2. **Log 2**: Network connection to `52.76.101.124`, one of the IPs from Log 1, over HTTP.
3. **Log 3**: Network connection to `18.140.6.45`, another resolved IP, associated with `www.chatgptgoogle.org`.
4. **Log 4**: DNS query for `www.chatgptgoogle.org`, confirming multiple IPs including those from earlier logs.
5. **Log 5**: DNS query for `chrome.google.com`, resolving to a Google IP address.
6. **Log 6**: Network connection to Google's IP `172.217.17.142`, related to Chrome services.
7. **Log 7**: DNS query for `version.chatgpt4google.workers.dev`, resolving to external IPs.
8. **Log 8**: Repeat DNS query for the same domain as Log 7, indicating continued access.

Email Security:



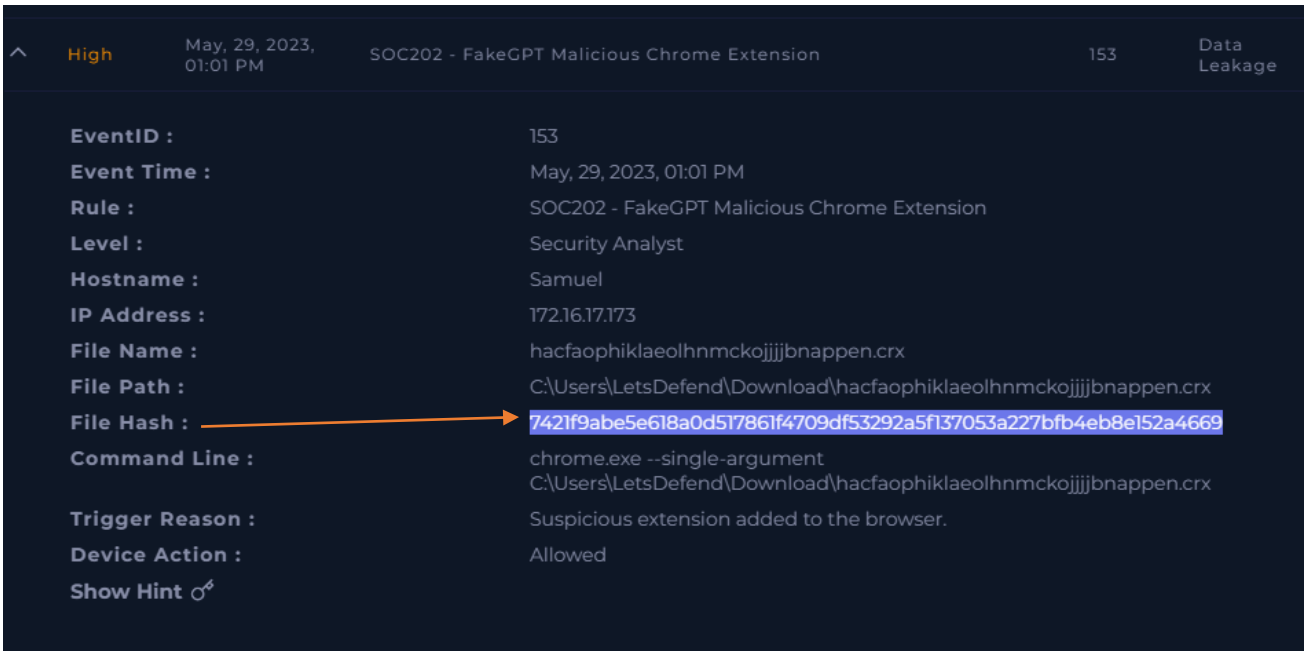
Despite entering the source host name in the email security section, no emails have been sent, indicating that the attack was not executed

Detection:

Threat Intelligence Results

File Hash

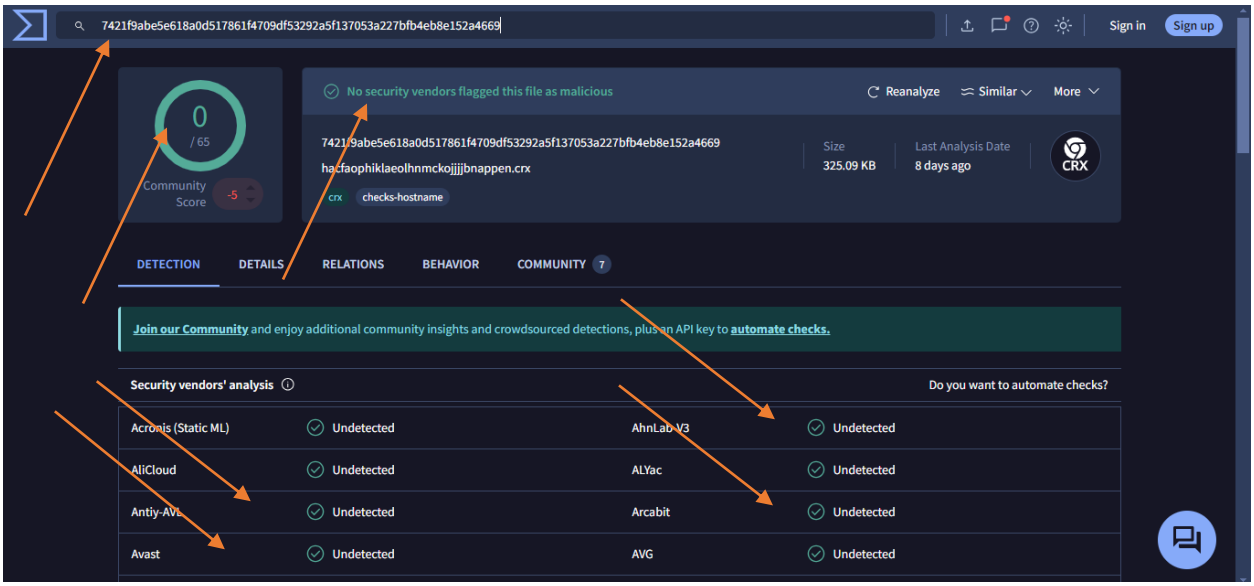
Check the attached photo



High	May, 29, 2023, 01:01 PM	SOC202 - FakeGPT Malicious Chrome Extension	153	Data Leakage

EventID :	153
Event Time :	May, 29, 2023, 01:01 PM
Rule :	SOC202 - FakeGPT Malicious Chrome Extension
Level :	Security Analyst
Hostname :	Samuel
IP Address :	172.16.17.173
File Name :	hacfaophiklaeolhnmckojjjjbnappen.crx
File Path :	C:\Users\LetsDefend\Download\hacfaophiklaeolhnmckojjjjbnappen.crx
File Hash :	7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e152a4669
Command Line :	chrome.exe --single-argument C:\Users\LetsDefend\Download\hacfaophiklaeolhnmckojjjjbnappen.crx
Trigger Reason :	Suspicious extension added to the browser.
Device Action :	Allowed
Show Hint	

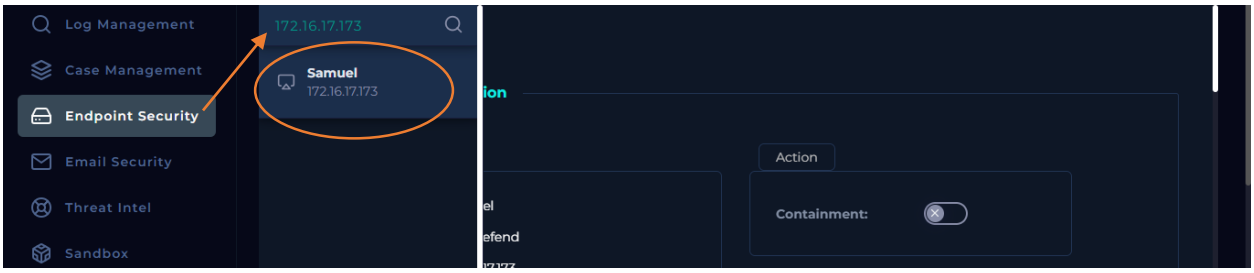
File Hash Analysis on VirusTotal



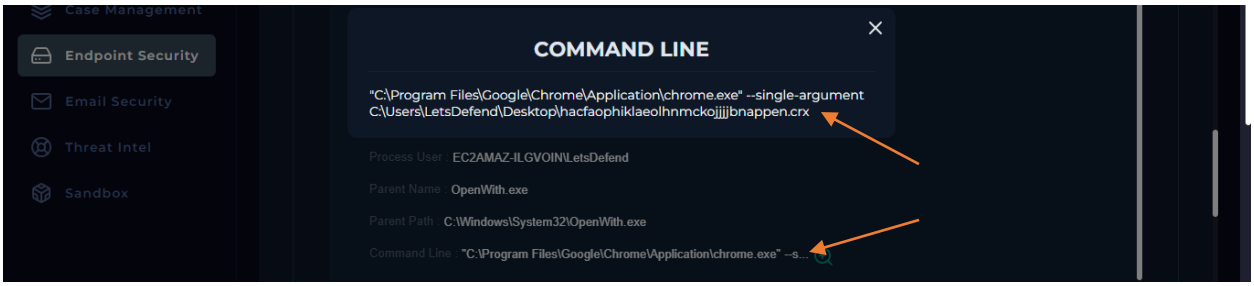
VirusTotal Analysis:

- **File is clean but there are some comments in community section.**
- **[Reference link]**

Endpoint Security:



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



- **"C:\Program Files\Google\Chrome\Application\chrome.exe"**:
  - This part points to the path of the Google Chrome executable (`chrome.exe`) on the system.
- **--single-argument**:
  - This is a Chrome command-line switch (or flag) used to run Chrome with a specific argument. It's commonly used for loading specific tasks or files, like extensions.
- **C:\Users\LetsDefend\Desktop\hacfaophiklaeolhnmckojjjjbnappen.crx**:
  - This part refers to a `.crx` file, which is a Chrome extension package format. The file is located on the desktop of the user named "LetsDefend".
  - The `.crx` file likely contains the code and assets for a Chrome extension, possibly named "hacfaophiklaeolhnmckojjjjbnappen" (likely a hash or identifier of the extension).
  - The name "hacfaophiklaeolhnmckojjjjbnappen" looks like a random string, which is common in malware **. (the Device must be CONTAINED) AND WE <u>CONTAINED SUCCESSSFULLY.</u>**

Conclusion:

Upon thorough investigation of Event ID 153, it has been determined that the device “Samuel” was compromised by a malicious Chrome extension identified as **FakeGPT**. The extension, packaged as `hacfaophiklaeolhnmckojjjjbnappen.crx`, was silently installed via a command-line operation. The DNS queries and network connections to suspicious domains such as `www.chatgptforgoogle.pro` and `version.chatgpt4google.workers.dev` further confirm the presence of malicious behavior.

Although the file hashes initially appeared clean on VirusTotal, community comments raised concerns, signaling the potential for sophisticated or emerging threats not yet flagged by signature-based detection systems.

The attack was mitigated early as no email exfiltration or abnormal browser behavior was detected beyond the unauthorized network connections. The device has since been successfully contained, preventing further spread or damage.

This incident underscores the importance of proactive monitoring and rapid response in identifying and mitigating threats introduced through seemingly benign browser extensions. It also highlights the necessity for enhanced extension vetting and stricter network policies to prevent similar occurrences in the future.

Recommendation:

- Strengthen browser extension policies to restrict unauthorized installations.
- Continuously monitor DNS queries for suspicious external connections.
- Perform a comprehensive review of other endpoints for similar indicators of compromise.

The containment of this device not only neutralized the immediate threat but also serves as a valuable learning opportunity for enhancing our defensive posture against evolving browser-based threats.