



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

Official incident report	1
Event ID: 153	1
Rule Name: SOC202 - FakeGPT Malicious Chrome Extension	1
Table of contents	2
Event Details	3
Network Information Details	4
Analysis	5
Log management	5
Security Email	11
Detection	12
Threat intelligence	12
Endpoint Security	14
Conclusion	15

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:

hacfaophiklaeolhnmckojjjbnappen.crx

File Path:

C:\Users\LetsDefend\Download\hacfaophiklaeolhnmckojjjbnappen.crx

File Hash:

7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e152a4669

Device Action:

Allowed

Command Line:

chrome.exe --single-argument

C:\Users\LetsDefend\Download\hacfaophiklaeolhnmckojjjbnappen.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.

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Columns X Src Address	Operator contains	Value 172.16.17.173	2242	172.217.17.142	80	
May, 29, 2023, 01:03 PM	OS	172.16.17.173	0	172.16.17.173	0	
May, 29, 2023, 01:06 PM	OS	172.16.17.173	0	172.16.17.173	0	
May, 29, 2023, 01:02 PM	Proxy	172.16.17.173	23324	52.76.101.124	80	
May, 29, 2023, 01:02 PM	Proxy	172.16.17.173	34223	18.140.6.45	80	
May, 29, 2023, 01:02 PM	OS	172.16.17.173	0	172.16.17.173	0	
May, 29, 2023, 01:02 PM	OS	172.16.17.173	0	172.16.17.173	0	
May, 29, 2023, 01:03 PM	OS	172.16.17.173	0	172.16.17.173	0	

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:**

	DATE	RAW LOG	ADDRESS	DEST. PORT	RAW
	May, 25	Source: Sysmon	17.173	0	
	May, 25	Username: Samuel	101.124	80	
	May, 25	EventID: 22	6.45	80	
	May, 25	Type: DNS Query	17.173	0	
	May, 25	QueryResult: ::ffff:52.76.101.124;::ffff:3.1.17.18;::ffff:18.140.6.45;	17.173	0	
	May, 25	QueryName: www.chatgptforgoogle.pro	17.173	0	
	May, 25	Process: C:\Program Files\Google\Chrome\Application\chrome.exe	17.173	0	
	May, 25	UtcTime: 2023-05-29 13:02:47.838	7.17.142	80	

- **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](#)

The screenshot shows the VirusTotal interface for the domain `www.chatgptforgoogle.pro`. The browser address bar at the top shows the URL. On the left, a 'Community Score' of 8/94 is displayed. The main header indicates that 8/94 security vendors flagged this domain as malicious. Below this, the domain name is listed along with its creation date (1 year ago) and last analysis date (13 days ago). The 'DETECTION' tab is active, showing a table of security vendors' analysis. Arrows point from the browser address bar, the Community Score, the '8/94 security vendors' message, and the detection table to the text 'The reference link' in the previous block.

Security vendors' analysis		Do you want to automate checks?	
Antiy-AVL	Malicious	BitDefender	Malware
CyRadar	Malicious	Fortinet	Malware
G-Data	Malware	Seclookup	Malicious
Sophos	Malware	Webroot	Malicious

- **Log2:**

DATE	RAW LOG	ADDRESS	DEST PORT	RAW
May, 29		17.173	0	
May, 29	Type: Network Connection	101.124	80	
May, 29	DestinationIp: 52.76.101.124	6.45	80	
May, 29	DestinationHost: www.chatgptforgoogle.pro	17.173	0	
May, 29	DestinationPort: 80	17.173	0	
May, 29	Image: C:\Program Files\Google\Chrome\Application\chrome.exe			
May, 29	UtcTime: 2023-05-29 13:02:47.847			

- **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:**

DATE	RAW LOG	ADDRESS	DEST PORT	RAW
May, 29		17.173	0	
May, 29	Type: Network Connection	101.124	80	
May, 29	DestinationIp: 18.140.6.45	6.45	80	
May, 29	DestinationHost: www.chatgptgoogle.org	17.173	0	
May, 29	DestinationPort: 80	17.173	0	
May, 29	Image: C:\Program Files\Google\Chrome\Application\chrome.exe			
May, 29	UtcTime: 2023-05-29 13:02:59.848			

- **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:**

Log Management	DATE	RAW LOG	ADDRESS	DEST. PORT	RAW
Case Management	May, 29	Source: Sysmon	17.173	0	+
Endpoint Security	May, 29	Username: Samuel	101.124	80	+
Email Security	May, 29	EventID: 22	6.45	80	+
Threat Intel	May, 29	Type: DNS Query	17.173	0	+
Sandbox	May, 29	QueryResult: ::ffff:18.140.6.45;::ffff:3.1.17.18;::ffff:52.76.101.124;	17.173	0	+
	May, 29	QueryName: www.chatgptgoogle.org	17.173	0	+
	May, 29	Process: C:\Program Files\Google\Chrome\Application\chrome.exe	17.173	0	+
	May, 29	UtcTime: 2023-05-29 13:02:59.835	7.17.142	80	+

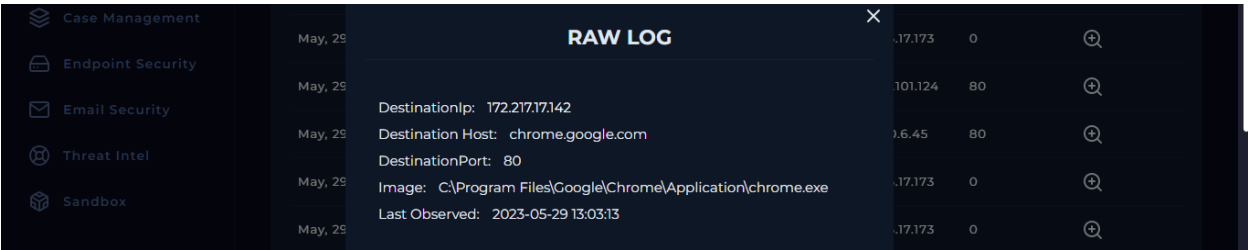
- **Source:** Sysmon
- **Event Type:** DNS Query (EventID 22)
- **Summary:** A DNS query for the domain `www.chatgptgoogle.org` was made, resolving to three IPv6 addresses: `::ffff:18.140.6.45`, `::ffff:3.1.17.18`, and `::ffff:52.76.101.124`. This correlates with Log 3, confirming DNS resolution for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

- **Log5:**

Log Management	DATE	RAW LOG	ADDRESS	DEST. PORT	RAW
Case Management	May, 29	Source: Sysmon	17.173	0	+
Endpoint Security	May, 29	Username: Samuel	101.124	80	+
Email Security	May, 29	EventID: 22	6.45	80	+
Threat Intel	May, 29	Type: DNS Query	17.173	0	+
Sandbox	May, 29	QueryResult: ::ffff:172.217.17.142;	17.173	0	+
	May, 29	QueryName: chrome.google.com	17.173	0	+
	May, 29	Process: C:\Program Files\Google\Chrome\Application\chrome.exe	17.173	0	+
	May, 29	UtcTime: 2023-05-29 13:03:11.282	7.17.142	80	+

- **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:**



The screenshot shows a 'RAW LOG' window for Log6. The left sidebar contains navigation links: Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main panel displays details for May 25, 2023, at 13:03:13. The details include: DestinationIp: 172.217.17.142, Destination Host: chrome.google.com, DestinationPort: 80, Image: C:\Program Files\Google\Chrome\Application\chrome.exe, and Last Observed: 2023-05-29 13:03:13. The right sidebar shows a table with columns ADDRESS, DEST. PORT, and RAW, with one row visible: 17.173, 0, and a magnifying glass icon.

DATE	DETAILS	ADDRESS	DEST. PORT	RAW
May, 25	DestinationIp: 172.217.17.142	17.173	0	🔍
May, 25	Destination Host: chrome.google.com	101.124	80	🔍
May, 25	DestinationPort: 80	16.45	80	🔍
May, 25	Image: C:\Program Files\Google\Chrome\Application\chrome.exe	17.173	0	🔍
May, 25	Last Observed: 2023-05-29 13:03:13	17.173	0	🔍

- **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:**



The screenshot shows a 'RAW LOG' window for Log7. The left sidebar contains navigation links: Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main panel displays details for May 25, 2023, at 13:03:23.006. The details include: Source: Sysmon, Username: Samuel, EventID: 22, Type: DNS Query, QueryResult: ::ffff:104.21.63.166;::ffff:172.67.147.243;, QueryName: version.chatgpt4google.workers.dev, Process: C:\Program Files\Google\Chrome\Application\chrome.exe, and UtcTime: 2023-05-29 13:03:23.006. The right sidebar shows a table with columns ADDRESS, DEST. PORT, and RAW, with one row visible: 17.173, 0, and a magnifying glass icon.

DATE	DETAILS	ADDRESS	DEST. PORT	RAW
May, 25	Source: Sysmon	17.173	0	🔍
May, 25	Username: Samuel	101.124	80	🔍
May, 25	EventID: 22	16.45	80	🔍
May, 25	Type: DNS Query	17.173	0	🔍
May, 25	QueryResult: ::ffff:104.21.63.166;::ffff:172.67.147.243;	17.173	0	🔍
May, 25	QueryName: version.chatgpt4google.workers.dev	17.173	0	🔍
May, 25	Process: C:\Program Files\Google\Chrome\Application\chrome.exe	17.173	0	🔍
May, 25	UtcTime: 2023-05-29 13:03:23.006	17.173	0	🔍

- **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:**

The screenshot shows a network log management interface. On the left is a sidebar with navigation links: Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main area displays a 'RAW LOG' for a specific event. The log entry is dated May 29 and includes the following details:

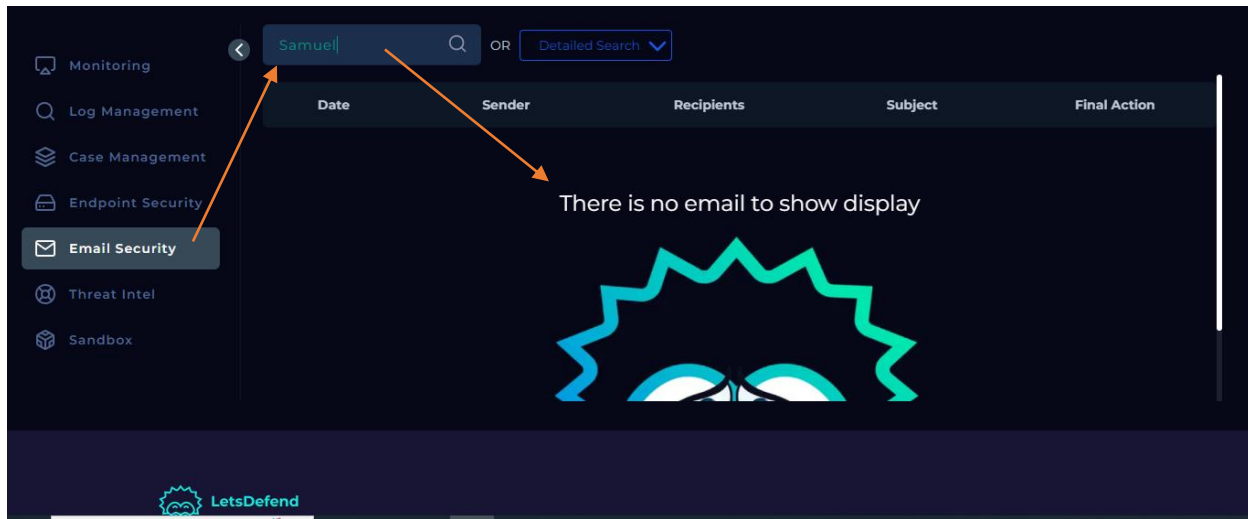
DATE	RAW LOG	ADDRESS	DEST. PORT	RAW
May, 29	Source: Sysmon	52.76.101.124	80	[icon]
May, 29	Username: Samuel	18.140.6.45	80	[icon]
May, 29	EventID: 22	172.217.142	80	[icon]
May, 29	Type: DNS Query			
May, 29	QueryResult: ::ffff:104.21.63.166;::ffff:172.67.147.243;			
May, 29	QueryName: version.chatgpt4google.workers.dev			
May, 29	Process: C:\Program Files\Google\Chrome\Application\chrome.exe			
May, 29	UtcTime: 2023-05-29 13:06:38.896			

- **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 :	hacfaophiklaeolhnmckojjjbnappen.crx				
File Path :	C:\Users\LetsDefend\Download\hacfaophiklaeolhnmckojjjbnappen.crx				
File Hash :	7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e152a4669				
Command Line :	chrome.exe --single-argument C:\Users\LetsDefend\Download\hacfaophiklaeolhnmckojjjbnappen.crx				
Trigger Reason :	Suspicious extension added to the browser.				
Device Action :	Allowed				
Show Hint	🔔				

File Hash Analysis on VirusTotal

7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e152a4669

Community Score: 0 / 65

No security vendors flagged this file as malicious

7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e152a4669

Size: 325.09 KB

Last Analysis Date: 8 days ago

CRX

checks-hostname

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis

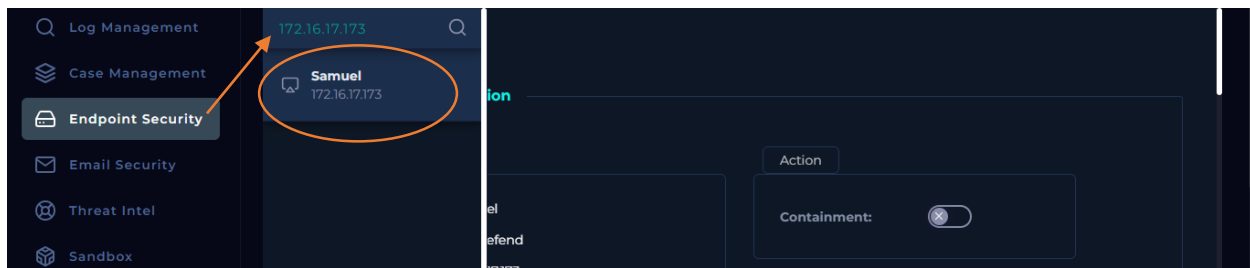
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AV	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected

Do you want to automate checks?

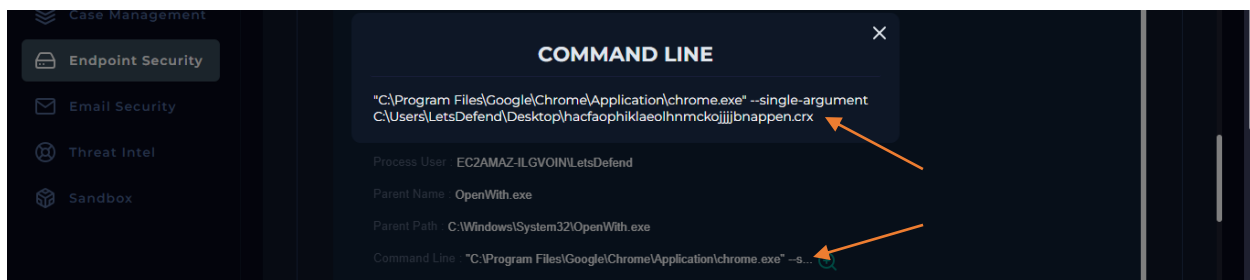
VirusTotal Analysis:

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

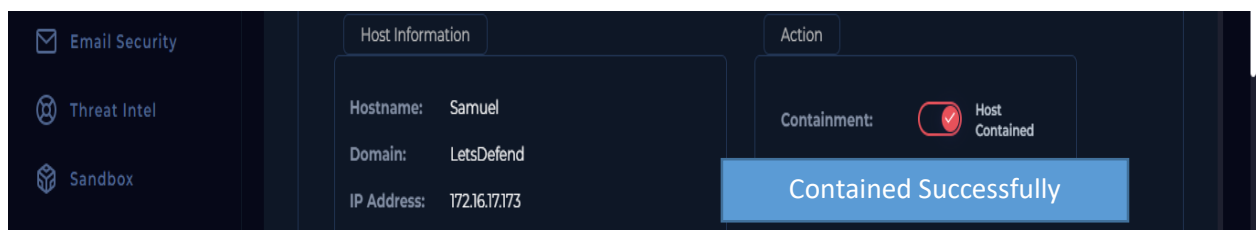
Endpoint Security:



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\hacfaophiklaeolnmckojjjbnappen.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 "hacfaophiklaeolnmckojjjbnappen" (likely a hash or identifier of the extension).
 - The name "hacfaophiklaeolnmckojjjbnappen" looks like a random string, which is common in malware. **(the Device must be CONTAINED) AND WE CONTAINED SUCCESSFULLY.**



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.