

Investigate

FakeGPT

as SOC Analyst



LetsDefend

TABLE OF CONTENTS

03

Alert

05

Detection

09

Analysis

18

Containment

19

Summary

21

Lesson Learned

22

Remediation Actions

23

Appendix

Author: Berkay Soylu

Alert

Based on the information that the alert provided, it appears that there is a suspicious file detected on a system named "Samuel" with an IP address of 172.16.17.173. The Alert is triggered by the SOC202 rule for FakeGPT Malicious Chrome Extension.

Although extensions are typically created with good intentions, attackers take advantage of this opportunity to exploit unsuspecting users. These malicious extensions can quietly infiltrate our browsers, operating unnoticed in the background without our knowledge.

High	May, 29, 2025, 01:01 PM	SOC202 - FakeGPT Malicious Chrome Extension	153	Web Attack
EventID :	153			
Event Time :	May, 29, 2025, 01:01 PM			
Rule :	SOC202 - FakeGPT Malicious Chrome Extension			
Level :	Security Analyst			
Hostname :	Samuel			
Ip Address :	172.16.17.173			
File Name :	hacfaophiklaeolnmckojjjbnappen.crx			
File Path :	C:\Users\LetsDefend\Download\hacfaophiklaeolnmckojjjbnappen.crx			
File Hash :	7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e152a4669			
Command Line :	chrome.exe --single-argument C:\Users\LetsDefend\Download\hacfaophiklaeolnmckojjjbnappen.crx			
Trigger Reason :	Suspicious extension added to the browser.			
Device Action :	Allowed			

Based on this information, it appears that the command line is attempting to open or manipulate a Chrome extension file (with the **.crx** extension) using the Google Chrome browser.

The device action is marked as "allowed", indicating that no action was taken by the device to prevent or block the execution of the file.

Alert

Based on the provided trigger reason, hacfaophiklaeolhnmckojjjbnappen.crx named extension was added to the browser. And the file hash is:

7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e15
2a4669

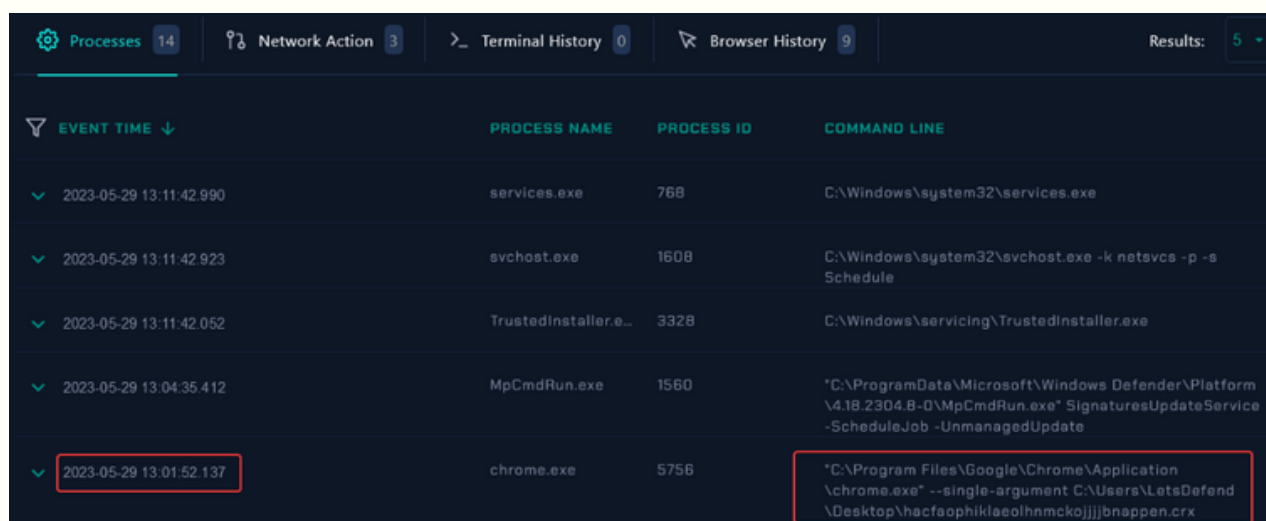
Overall, it appears that there may be malicious activity occurring on the system, and further investigation is needed to identify the extent of the activity and determine any necessary actions to remediate the situation.

Detection

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a false positive or a true positive incident is to analyze the logs collected from the host by our security products.

The first step we can take to investigate the alert is to examine the system logs of the Samuel host under Endpoint Security to identify any unusual or suspicious activities that may be related to the reported incident.

This includes looking for any network connections, browser history or processes initiated around the same time as the suspicious extension installation.



EVENT TIME ↓	PROCESS NAME	PROCESS ID	COMMAND LINE
✓ 2023-05-29 13:11:42.990	services.exe	768	C:\Windows\system32\services.exe
✓ 2023-05-29 13:11:42.923	svchost.exe	1608	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
✓ 2023-05-29 13:11:42.052	TrustedInstaller.exe	3328	C:\Windows\servicing\TrustedInstaller.exe
✓ 2023-05-29 13:04:35.412	MpCmdRun.exe	1560	"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2304.8-0\MpCmdRun.exe" SignaturesUpdateService -ScheduleJob -UnmanagedUpdate
✓ 2023-05-29 13:01:52.137	chrome.exe	5756	"C:\Program Files\Google\Chrome\Application\chrome.exe" --single-argument C:\Users\LetsDefend\Desktop\hacfaophiklaeolhmckojjjbnappen.crx

Detection

When examining the processes on the Samuel host, we have discovered that the command "C:\ProgramFiles\Google\Chrome\Application\chrome.exe" --single-argument

C:\Users\LetsDefend\Desktop\hacfaophiklaeolhnmckojjjbnappen.crx was executed on the machine with a Process ID (PID) of 5756 at 2023-05-29 13:01:52.137.

```
Event Time : 2023-05-29 13:01:52.137
Process ID : 5756
Command Line : "C:\Program Files\Google\Chrome\Application\chrome.exe" --single-argument C:\Users\LetsDefend\Desktop\hacfaophiklaeolhnmckojjjbnappen.crx
Image Path : C:\Program Files\Google\Chrome\Application\chrome.exe
Process User : EC2AMAZ-ILGVOIN\LetsDefend
Parent Name : OpenWith.exe
Parent Path : C:\Windows\System32\OpenWith.exe
```

Based on the browser history, it is evident that the user interacted with the extension and visited various related URLs, including the Chrome Web Store pages and the settings page for the suspicious extension.

Detection

Processes 14

Network Action 3

> Terminal History 0

Browser History 9

Results: 10

EVENT TIME

DOMAIN NAME/URL

2023-05-29 13:01:44

https://chrome.google.com/webstore/detail/chatgpt-for-google/hacfaophiklaeolnmckojjjbnappen

2023-05-29 13:01:47

https://support.google.com/chrome_webstore/?p=crx_warning

2023-05-29 13:01:48

https://support.google.com/chrome_webstore/answer/2664769?visit_id=638211162424485757-20903012446p=crx_warning&rd=1

2023-05-29 13:01:55

chrome://extensions

2023-05-29 13:02:01

chrome://extensions/?id=hacfaophiklaeolnmckojjjbnappen

2023-05-29 13:10:18

https://chat.openai.com/

2023-05-29 13:10:22

https://chat.openai.com/auth/login

2023-05-29 13:10:59

https://auth0.openai.com/authorize?client_id=TdJlcbe16WoTHtN95nyywh5E4yOo6ItG6scope=openid%20email%20profile%20model.request%20model.response_type=code&redirect_uri=http

- The user visited the Chrome Web Store page for the extension with the URL mentioned. This indicates that the user accessed the extension's page on the Web Store.
- The user accessed the Chrome Extensions page, which allows managing installed extensions. This suggests that the user interacted with the extensions settings, possibly to view or modify the installed extensions.

Detection

- The user specifically visited the Chrome Extensions page with the extension ID "hacfaophiklaeolhnmckojjjbnappen." This indicates that the user accessed the settings page for the suspicious extension.
- The user visited the OpenAI Chat platform, which is the legitimate website for accessing the ChatGPT-based service.
- The user accessed the login page of the OpenAI Chat platform. Probably for link the suspicious extension to his ChatGPT account.

Analysis

Quarantine/Clean Status of the Malware

The presence of malicious files on the computer should make us think about whether the detected malware associated with the suspicious extension has been quarantined or cleaned from the affected system.

High	May, 29, 2025, 01:01 PM	SOC202 - FakeGPT Malicious Chrome Extension	153	Web Attack
EventID :	153			
Event Time :	May, 29, 2025, 01:01 PM			
Rule :	SOC202 - FakeGPT Malicious Chrome Extension			
Level :	Security Analyst			
Hostname :	Samuel			
Ip Address :	172.16.17.173			
File Name :	hacfaophiklaeolnmckojjjbnappen.crx			
File Path :	C:\Users\LetsDefend\Download\hacfaophiklaeolnmckojjjbnappen.crx			
File Hash :	7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e152a4669			
Command Line :	chrome.exe --single-argument C:\Users\LetsDefend\Download\hacfaophiklaeolnmckojjjbnappen.crx			
Trigger Reason :	Suspicious extension added to the browser.			
Device Action :	Allowed			


The fact that the device action was marked as "allowed" indicates that no immediate action was taken to quarantine or block the malware. Furthermore, the ongoing network and process activities observed subsequent to the incident also suggest that the malware remains active and has not been successfully quarantined.


The lack of quarantine or cleaning measures increases the potential risks associated with the detected malware. It is crucial to address this oversight promptly to mitigate any further impact and prevent potential propagation to other systems within the network.


Analysis


Extension Analysis and Identification of Command and Control (C2) Address


In this section, we will perform a detailed analysis of the detected malicious Extension using third-party tools and techniques. The primary objective is to gain insights into the behavior, capabilities, and potential impact of the malware. Additionally, we will focus on identifying the Command and Control (C2) address associated with the malware.

 Processes 14

 Network Action 3

 Terminal History 0

 Browser History 9

 EVENT TIME

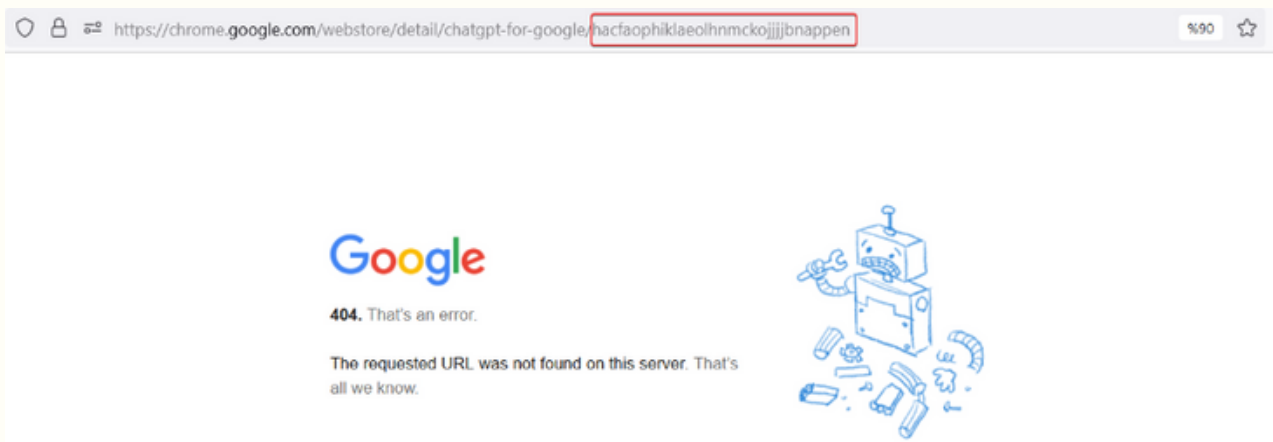
DOMAIN NAME/URL

2023-05-29 13:01:44

https://chrome.google.com/webstore/detail/chatgpt-for-google/hacfaophiklaeolhnmckojjjbnappen

Based on the provided URL from the browser history the name of the malicious extension is **"Chatgpt for Google"** and the ID of the malicious extension is **"hacfaophiklaeolhnmckojjjbnappen"**

Analysis

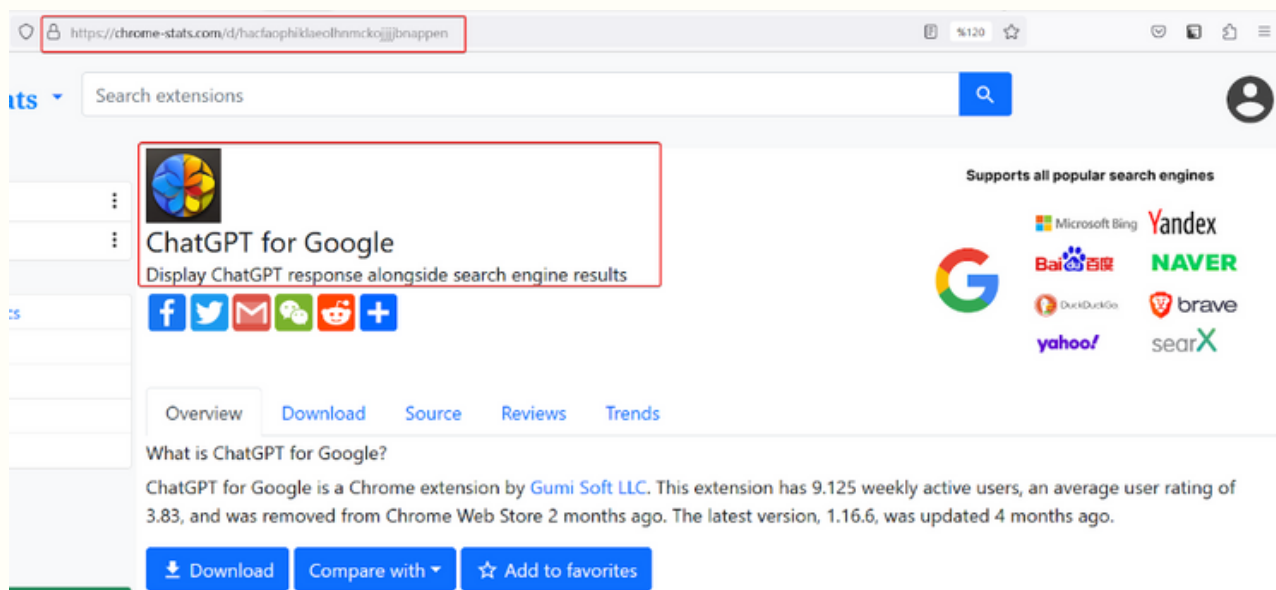


During our investigation, attempts to access the URL associated with the malicious extension, <https://chrome.google.com/webstore/detail/chatgpt-for-google/hacfaophiklaeolnmckojjjbnappen>, resulted in an error message stating "404. That's an error. The requested URL was not found on this server. That's all we know."

The error message indicates that the specific URL we attempted to access is not currently available on the server. This could suggest that the malicious extension has been removed from the Chrome Web Store or the URL itself is no longer valid.

Analysis

To find the malicious extension we search the **"hacfaophiklaeolhnmckojjjjbnappen"** ID of the malicious extension on the internet. In our investigation, we discovered a web page called "chrome-stats" that maintains statistics of various Chrome extensions, including the malicious extension with the ID "hacfaophiklaeolhnmckojjjjbnappen."

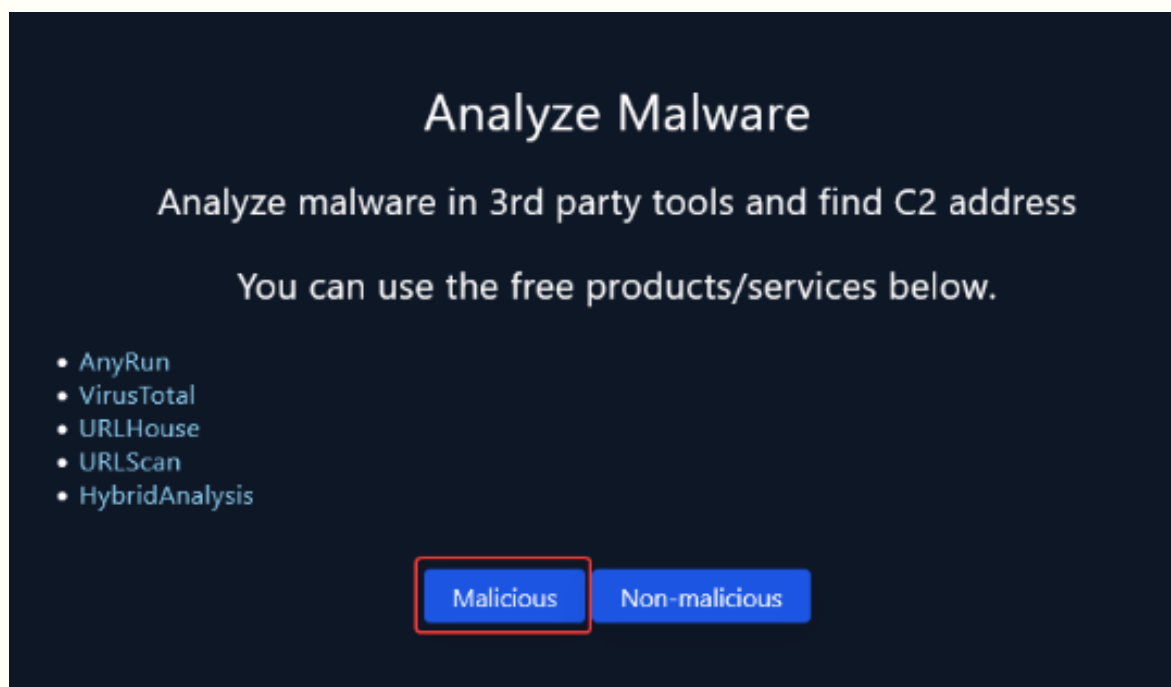


According to the chrome-stats website, this extension has a high-risk impact and a very high-risk likelihood, indicating significant potential harm and a strong probability of compromising the affected system.

On 2023-03-22, the malicious extension "hacfaophiklaeolhnmckojjjjbnappen" was removed from the Chrome Web Store because it contained malware.

Analysis

The findings from our analysis confirm that the suspicious Chrome extension, identified as "hacfaophiklaeolhnmckojjjbnappen," is malicious.



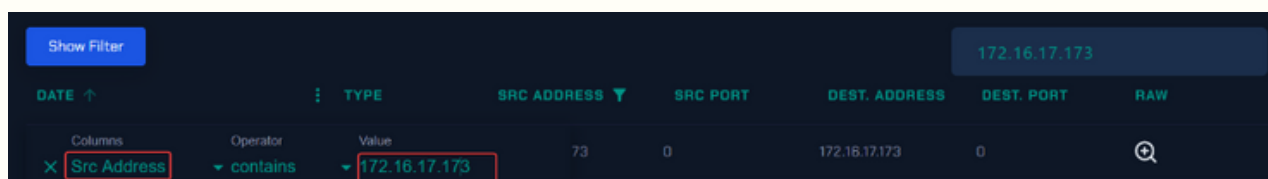
The findings from our analysis confirm that the suspicious Chrome extension, identified as "hacfaophiklaeolhnmckojjjbnappen," is **malicious**.

Analysis

C2 Access Verification - Unauthorized Connections

In this section, we will analyze the network-based logs collected from the Samuel Host to investigate any indications of Command and Control (C2) access. By examining the network logs, we aim to identify any suspicious connections or communication patterns that may suggest unauthorized interactions with the C2 infrastructure.

On "Log Management" tab we filter the source address to the Ip address of Samuel Host 172.16.17.173 to see the logs related of the given ip address.



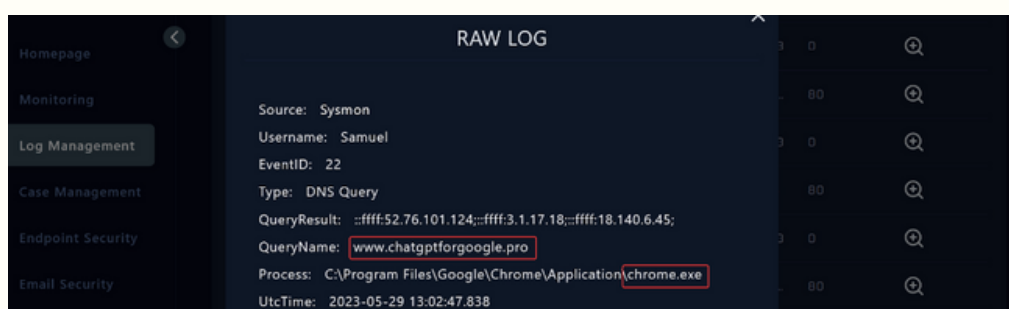
During the investigation, suspicious outbound network connections were detected originating from the Samuel Host.

Analysis

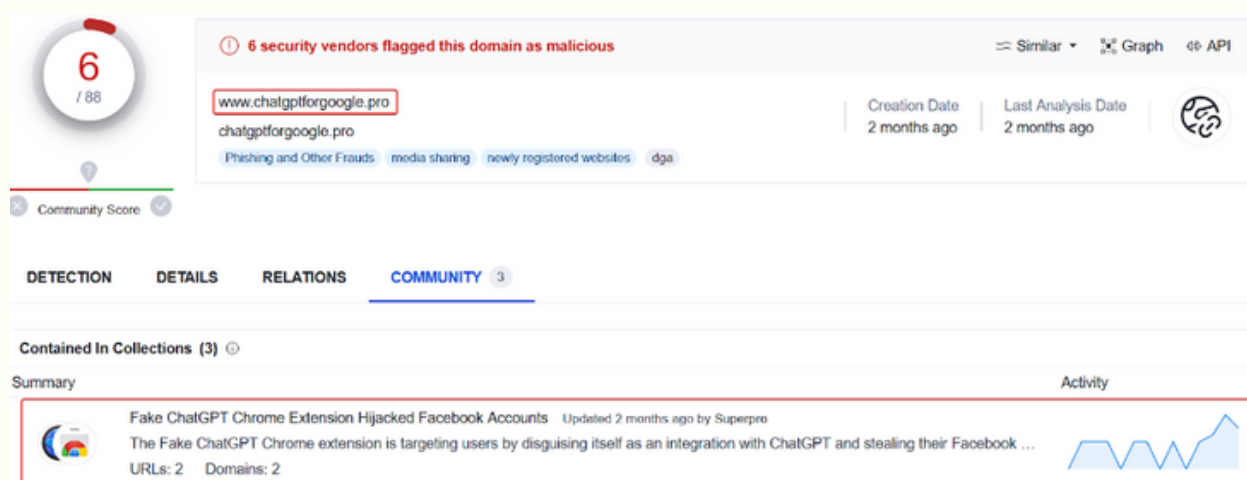
Show Filter						
172.16.17.173						
DATE	TYPE	SRC ADDRESS ▼	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
May, 29, 2023, 01:06 PM	OS	172.16.17.173	0	172.16.17.173	0	🔍
May, 29, 2023, 01:03 PM	OS	172.16.17.173	0	172.16.17.173	0	🔍
May, 29, 2023, 01:03 PM	Proxy	172.16.17.173	32242	172.217.17.142	80	🔍
May, 29, 2023, 01:03 PM	OS	172.16.17.173	0	172.16.17.173	0	🔍
May, 29, 2023, 01:02 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	Proxy	172.16.17.173	23324	52.76.101.124	80	🔍
May, 29, 2023, 01:02 PM	OS	172.16.17.173	0	172.16.17.173	0	🔍

By conducting a thorough analysis of these suspicious outbound network connections, we aim to determine the intent, scope, and potential impact of the observed activity. This analysis will enable us to make informed decisions regarding incident response, remediation, and the implementation of necessary security measures. A suspicious outbound network connection was identified from the Samuel Host based on the provided Sysmon event log. The raw log of the event are as follows:

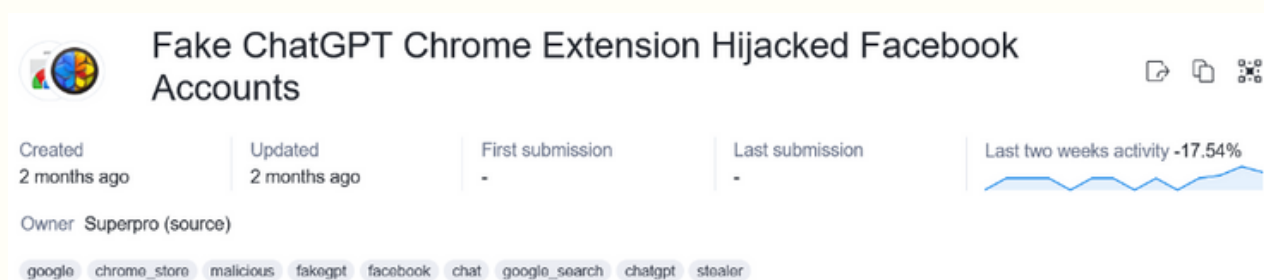
Analysis



Further investigation of the domain "www.chatgptforgoogle.pro" on threat intelligence platforms, such as VirusTotal, confirms its malicious nature. The findings from these platforms indicate that the URL is associated with known malicious activity and has been reported as a threat.



Analysis



During the investigation, network connections associated with the suspicious Chrome extension were analyzed to determine if any Command and Control (C2) communication was established.

The analysis of the C2 communication attempts associated with the suspicious extension indicates a high likelihood of malicious intent. The identified connections to `chatgptforgoogle.pro`, `chatgptgoogle.org`, and `version.chatgpt4google.workers.dev` highlight the need for immediate action to mitigate the threat and prevent further compromise.

The screenshot shows a web interface with a dark theme. On the left is a sidebar with a list of items: "Incident N", "Descriptio", "Incident T", and "Created D". The main content area has a title "Check If Someone Requested the C2". Below the title is a paragraph: "Please go to the 'Log Management' page and check if the C2 address accessed. You can check if the malicious file is run by searching the C2 addresses of the malicious file." Below this is a bullet point: "• Log Management". Another paragraph follows: "Please click 'Accessed' if someone access the malicious address. Otherwise please click 'Not Accessed' button." At the bottom are two buttons: "Accessed" (highlighted with a red box) and "Not Accessed".

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.

Isolation of the host can be made from the endpoint security tab.

Hostname	Samuel
IP Address	172.16.17.173

Summary

This incident response report presents the investigation and analysis of a Chrome extension alert related to the detection of a malicious extension known as "ChatGPT For Google." The alert was triggered due to the suspicious addition of the extension to the browser, indicating a potential security threat.

Through careful analysis, several key findings were identified, including the nature of the malicious extension, its impact on user accounts, and the detection of Command and Control (C2) communication attempts.

The investigation revealed that the malicious extension posed as a ChatGPT integration, deceiving users and targeting their Facebook accounts. The extension was removed from the Chrome Web Store due to its malware-infected nature, but it had already been installed by a significant number of users, raising concerns about the potential impact on their accounts and personal information.

Summary

Further analysis of network activity revealed connections made to malicious domains associated with the extension's C2 infrastructure. These connections, coupled with the findings from threat intelligence platforms, confirmed the malicious nature of the extension and the high risk it posed to users.

In conclusion, this incident response report highlights the analysis of a malicious Chrome extension and its implications for user security. By understanding the nature of the threat and implementing the recommended security measures, users can better protect themselves against similar threats in the future.

Lesson Learned

- User awareness and caution are critical when installing browser extensions.
- It is important to keep all software up-to-date to reduce the risk of being vulnerable to known exploits.
- Promptly Investigate and Respond to Suspicious Extension Installations.
- Continuously learn from incidents to adapt security measures and address emerging threats.

Remediation Actions

- Remove the malicious extension from affected systems.
- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the organization.
- Review and update security configurations to enhance protection against similar threats in the future.
- Reset affected user accounts, including passwords, and enable two-factor authentication where available.

Appendix

MITRE Tactics	MITRE Techniques
Initial Access	T1189 Drive by Compromise - Drive by Download
Execution	T1204 User Execution
Persistence	T1176 Browser Extension

Filename	SHA256 Value - Path
hacfaophiklaeolhnmcko jjjjbnappen.crx	7421f9abe5e618a0d517861f4709df53292a5f137053a227bf b4eb8e152a4669

IOC TYPE	VALUE
IPv4	172.217.17.142
IPv4	18.140.6.45
IPv4	52.76.101.124
Domain	www.chatgptgoogle.org
Domain	www.chatgptforgoogle.pro
Domain	version.chatgpt4google.workers.dev
URL	https://chrome.google.com/webstore/detail/chatgpt-for-google/hacfaophiklaeolhnmckojjjbnappen