**ANALYSIS**

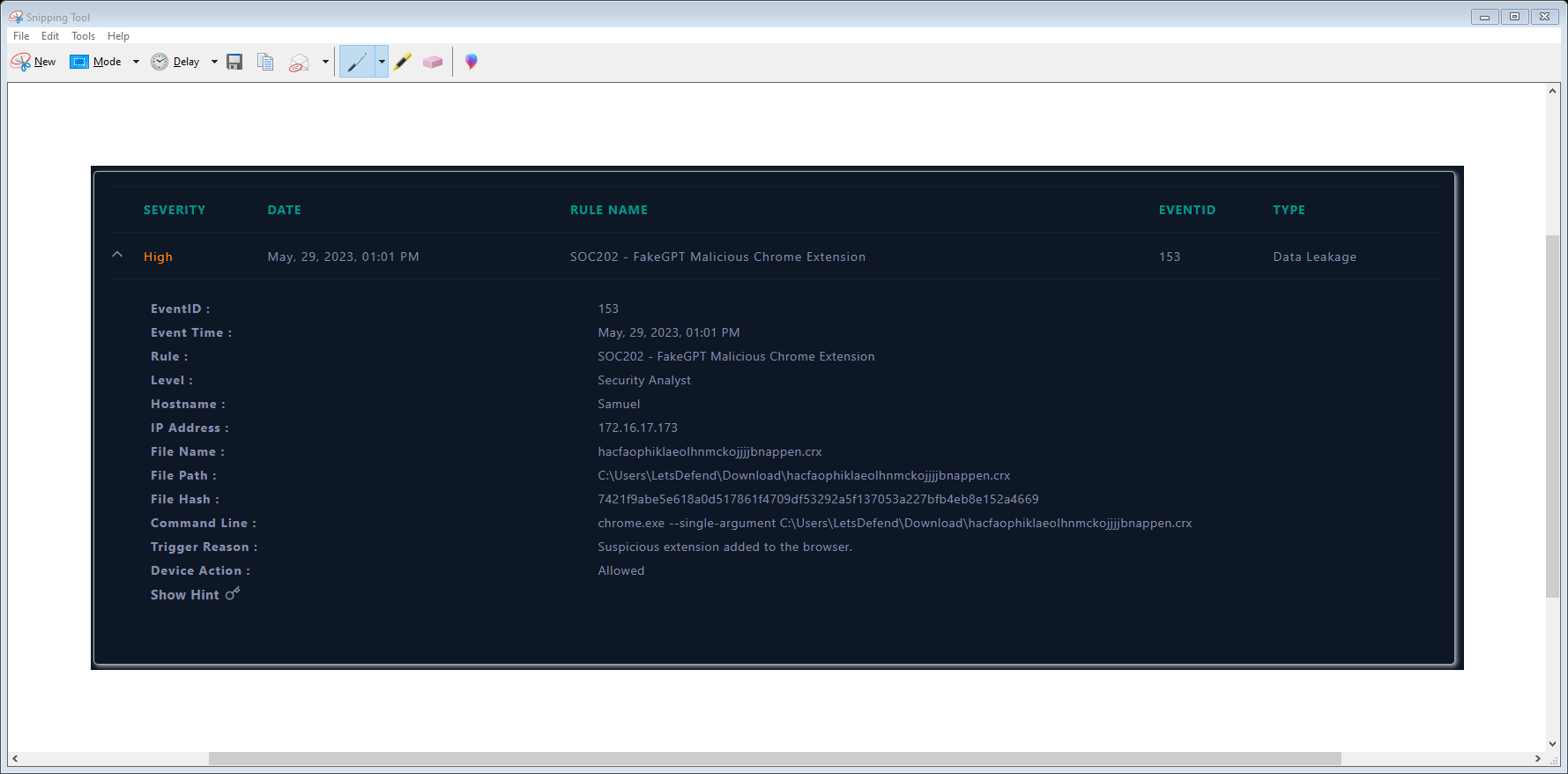
**Event ID:** 153

**Rule Name:** SOC 202 – FakeGPT Malicious Chrome Extension

***Practice with SOC Alerts as part of hands-on practice on LetsDefend SOC Analyst training***

**ALERT**

The SIEM system triggered an alert based on the **SOC202** rule for **FakeGPT Malicious Chrome Extension**. Based on the alert, it appears that suspicious file was found on a system named **“Samuel”** with an IP address of **172.16.17.173**.



Upon reviewing this alarm, it is observed that a suspicious extension installation associated with the FakeGPT (Chatgpt-based malware) was detected on the device.

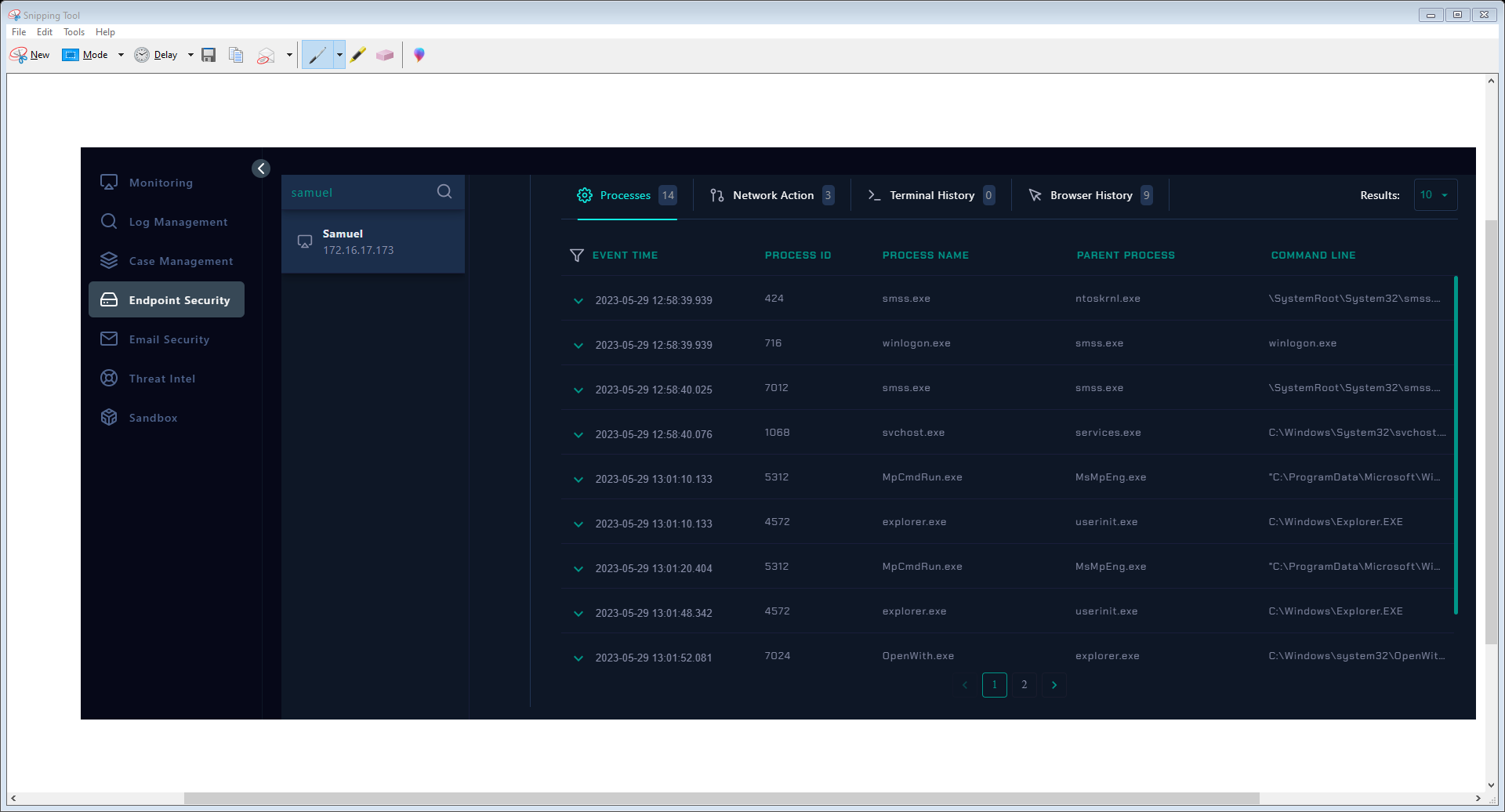
* Based on this information, it appears that the command line is attempting to open or manipulate a Chrome extension file (with the .crx extension) using the Google Chrome browser.
* The device action is marked as "allowed", indicating that no action was taken by the device to prevent or block the execution of the file.
* Based on the provided trigger reason, **hacfaophiklaeolhnmckojjjjbnappen.crx** named extension was added to the browser. And the file hash is: **7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e152a4669**

Overall, it appears that there may be malicious activity occurring on the system, and

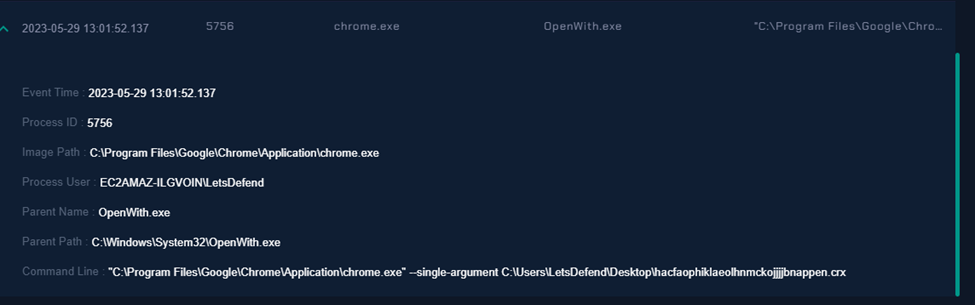
further investigation is needed to identify the extent of the activity and determine any

necessary actions to remediate the situation.

**ANALYSIS**

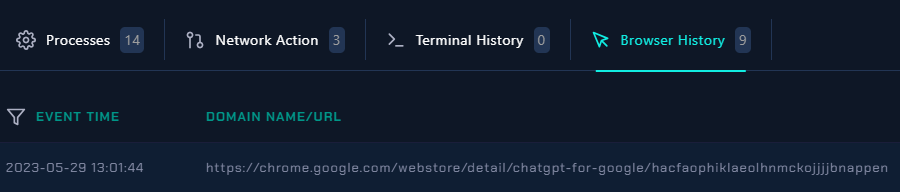
The first step taken was to examine the system logs of Samuel host to identify unusual activities that may be related to the reported incident. This includes looking for any network connections, browser history or processes initiated around the same time as the suspicious extension installation.

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\hacfaophiklaeolhnmckojjjjbnappen.crx was on the machine with a **Process ID (PID) of 5756 at 2023-05-29 13:01:** **52.137**.

****

**Extension Analysis:**

A third-party tool called **VirusTotal** was used to analyzed the detected malicious extension



During our investigation, attempts to access the URL associated with the malicious extension, **https://chrome.google.com/webstore/detail/chatgpt-for-google/hacfaophiklaeolhnmckojjjjbnappen**, 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.

#### MITIGATION

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. Therefore:

***The compromised host (Samuel) was Isolated and quarantined to mitigate any further impact and prevent potential propagation to other systems within the network.***

Footnotes

1[Add footnotes, if any, on their own page following references. For APA formatting requirements, it’s easy to just type your own footnote references and notes. To format a footnote reference, select the number and then, on the Home tab, in the Styles gallery, click Footnote Reference. The body of a footnote, such as this example, uses the Normal text style. (Note: If you delete this sample footnote, don’t forget to delete its in-text reference as well. That’s at the end of the sample Heading 2 paragraph on the first page of body content in this template.)]

able 1

[Table Title]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Column Head | Column Head | Column Head | Column Head | Column Head |
| Row Head | 123 | 123 | 123 | 123 |
| Row Head | 456 | 456 | 456 | 456 |
| Row Head | 789 | 789 | 789 | 789 |
| Row Head | 123 | 123 | 123 | 123 |
| Row Head | 456 | 456 | 456 | 456 |
| Row Head | 789 | 789 | 789 | 789 |

Note: [Place all tables for your paper in a tables section, following references (and, if applicable, footnotes). Start a new page for each table, include a table number and table title for each, as shown on this page. All explanatory text appears in a table note that follows the table, such as this one. Use the Table/Figure style, available on the Home tab, in the Styles gallery, to get the spacing between table and note. Tables in APA format can use single or 1.5 line spacing. Include a heading for every row and column, even if the content seems obvious. A default table style has been setup for this template that fits APA guidelines. To insert a table, on the Insert tab, click Table.]

all elements of APA formatting, please consult the APA Style Manual, 6th Edition.