

SOC104 - Malware Detected [Let's Defend – Write-up]

| Start Investigation

The screenshot shows a SOC interface with a sidebar containing monitoring, log management, case management, endpoint security, email security, threat intel, and sandbox options. The main area has tabs for 'MAIN CHANNEL', 'INVESTIGATION CHANNEL' (which is selected), and 'CLOSED ALERTS'. A table displays an alert for 'SOC104 - Malware Detected' with details like EventID: 14, Type: Malware, and Action: Download. Below the table is a detailed event log.

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	Sep, 15, 2020, 09:02 PM	SOC104 - Malware Detected	14	Malware	» ✓
EventID : 14 Event Time : Sep, 15, 2020, 09:02 PM Rule : SOC104 - Malware Detected Level : Security Analyst Source Address : 172.16.17.82 Source Hostname : JohnComputer File Name : googleupdate.exe File Hash : 0bc3f16dd527b4150648ec1e36cb22a File Size : 152.45 KB Device Action : Allowed File (PasswordInfected) : Download					

The layer contains extensive information, including the IP address, filename, and hash; therefore, my first step was to verify the hash.

The screenshot shows the VirusTotal analysis page for the file 'GoogleUpdate.exe'. It displays a community score of 0/72. The file hash is b60e92004d394d0b14a8953a2ba29951c79f2f8a6c94f495e3153dfbbef115b6. The file type is EXE. The analysis table shows results from various security vendors, all of which have flagged the file as undetected.

Security vendor	Result	Security vendor	Result
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antly-AVL	Undetected
Arcabit	Undetected	Arctic Wolf	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected

The analysis of the file 'GoogleUpdate.exe' on VirusTotal reveals a clean security profile, with a detection rate of 0/72. All major security vendors have flagged the file as undetected, suggesting it is legitimate and free from known malicious code at this time.

The cross-platform analysis of the file hash on both VirusTotal and MetaDefender Cloud confirms consistent clean status. On VirusTotal, the file yielded a 0/72 detection rate, while MetaDefender reported 0/12, with the 'Adaptive Sandbox' classifying its behavior as benign. These results collectively indicate that the file is legitimate and free from known malicious signatures across multiple security engines.

After confirming the file hash was clean, I conducted further research within the Log Management system. By searching for the IP address 172.16.17.82, I was able to track the network activity associated with this file to ensure no suspicious connections were established.

Endpoint monitoring shows the process 'googleupdate.exe' running under the 'NT AUTHORITY/SYSTEM' account. It was initiated by 'taskeng.exe' and is located in the standard Google update directory, with an MD5 hash of '0bca3f16...!'.

The screenshot shows a dark-themed user interface for monitoring or investigation. At the top, there are tabs for 'Processes' (5), 'Network Action' (1), 'Terminal History' (5), and 'Browser History' (3). The 'Browser History' tab is active. Below the tabs, there is a header with 'EVENT TIME' and 'DOMAIN NAME/URL'. Three entries are listed:

- 1 https://github.com/letsdefendio
- 2 https://www.google.com/search?q=how+to+update+chrome&oq=how+to+update+chrome
- 3 https://support.google.com/chrome/answer/95414?co=GENIE.Platform%3DAndroid&hl=en

A small navigation bar at the bottom indicates page 1 of 1.

The browser history for the endpoint shows recent activity related to system updates, including searches on how to update Chrome and visits to official Google support pages. Additionally, a visit to a GitHub repository for 'letsdefendio' was recorded.

| Use Playbook

Define Threat Indicator

Answer: other.

The screenshot shows a dark-themed interface with a sidebar containing 'Monitoring', 'Log Management', 'Case Management' (selected), 'Endpoint Security', 'Email Security', 'Threat Intel', and 'Sandbox'. A modal window titled 'Incident Details' is open. The main content of the modal asks 'Check if the malware is quarantined/cleaned'. Below it, a question 'Malware quarantined/cleaned?' has two options: 'Not Quarantined' (highlighted with a red box) and 'Quarantined'.

Based on the investigation, the file was confirmed as a legitimate utility, and the device action was set to 'Allowed'. The file remains 'Not Quarantined' because no malicious activity was detected.

The screenshot shows a dark-themed interface with the same sidebar as the previous screenshot. A modal window titled 'Analyze Malware' is open. It contains the text 'Analyze malware in 3rd party tools and find C2 address' and 'You can use the free products/services below.' Below this is a list of services: AnyRun, VirusTotal, URLHouse, URLScan, and HybridAnalysis. At the bottom of the modal are two buttons: 'Malicious' and 'Non-malicious' (highlighted with a red box).

Based on the investigation the activity was identified as non-malicious.

Value	Comment	Type	Remove
Obca3f16dd527b415	Clean GoogleUpdate	MD5 Hash	
172.16.17.82	Source internal IP (Jc)	IP Address	
support.google.com	Official Google supp...	URL Address	

The investigation concludes that this alert is a **True Positive**.

Summary

The systematic analysis of the file hash, network logs, and browser history provided a clear picture that the activity was legitimate. By correlating the user's search for Chrome updates with the execution of the verified 'googleupdate.exe', I was able to confirm the intent and rule out any malicious behavior, leading to an accurate classification of the alert as non-malicious.