



Official Incident Report

By: Ryan Stewart

EventID: 14

Rule Name: SOC104 - Malware Detected

Event Time: Feb, 01, 2024, 06:06 PM

Table of contents

Official Incident Report	1
Event ID: 104	1
Rule Name: SOC104 - Malware Detected	1
Table of contents	2
Alert	3
Detection	4
Verify	4
IP Reputation	5
Execution	7
Containment	8
Lesson Learned	9
Appendix	10
MITRE	10
Artifacts	11

Alert

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 :	0bca3f16dd527b4150648ec1e36cb22a
File Size :	152.45 KB
Device Action :	Allowed
File (Password:infected) :	Download

Upon an initial examination of the alert trigger, it's shown that a task is involved with the execution of "rundll32.exe" process. The command lines indicate that the "rundll32.exe" process was used to open a file named "GoogleUpdate.bin" located in the users temporary folder.

To validate the truth of this alert, our next step involves scrutinizing the available logs meticulously. The aim is to scope into the details of the network activity, identify any anomalies, and assess whether the detected process led to a successful attack. This comprehensive analysis will contribute to a clearer understanding of the potential security threat and aid in devising an effective response strategy.

Detection

Security vendors' analysis ⓘ

Avira	ⓘ Malware
BitDefender	ⓘ Malware
Certego	ⓘ Malicious
Cluster25	ⓘ Malicious
Fortinet	ⓘ Malware
G-Data	ⓘ Malware
Lionic	ⓘ Malware
Sophos	ⓘ Malware


Verify

Examining the log management data associated with the IP address "172.16.17.82," flagged as the alert source. According to VirusTotal (VT), the IP is registered under Amazon (S3). Does this association suggest a malicious reputation? Further confirmation is required through sandbox verification under this presumption.

While utilizing the AnyRun sandbox, the observed tactics and techniques initially raised suspicions. However, upon thorough examination of the Security Information and Event Management (SIEM) logs, it appears that the host's actions were aligned with legitimate business purposes, devoid of any malicious intent. AnyRun's findings validate my conclusion, categorizing the file as a false positive (FP) with no malicious intent.

General Info

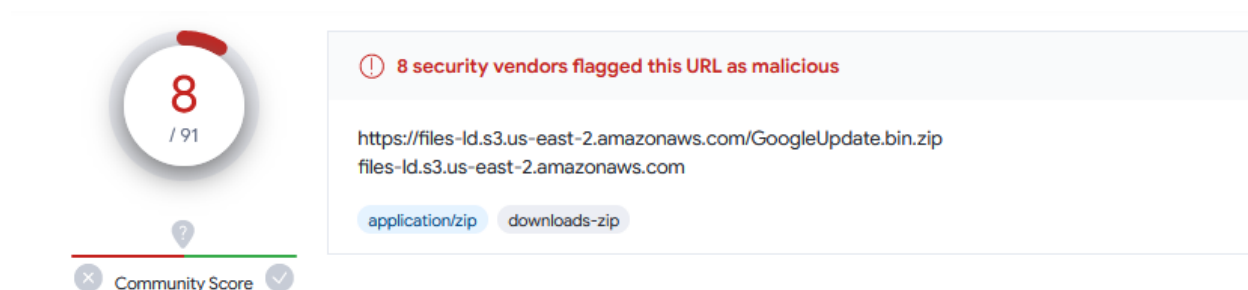
☒ Add for printing

URL: <https://files-id.s3.us-east-2.amazonaws.com/GoogleUpdate.bin.zip>
 Full analysis: <https://app.any.run/tasks/2c45c11a-1d78-4acb-b146-d0b062b4f139>
 Verdict: **Suspicious activity**
 Analysis date: February 01, 2024 at 14:32:51
 OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
 Indicators: 
 MD5: 674967ECC5D6199DBE7F091D4DC1529D
 SHA1: B78914FC1CB32013AE964751C328AB36B63EB692
 SHA256: 1C57ED2C5AC18781B9B710D21A20543607668C207A0F13817075CED13315EDEF
 SSFEP: 3-N8P-IRI Rk-IPN?07WtkhwF&WII?xR1+PI nVI

Analysis

IP Reputation

In the initial investigations, it is determined that the cause of the incident is the processes running on the source system (John), the source hostname “JohnComputer.”



8 / 91

8 security vendors flagged this URL as malicious

<https://files-lid.s3.us-east-2.amazonaws.com/GoogleUpdate.bin.zip>
files-lid.s3.us-east-2.amazonaws.com

application/zip downloads-zip

Community Score

<https://www.virustotal.com>

Headers

Content-Length	59810
x-amz-id-2	Uil0d9lu0C7dlCSjBJyszprCJ+6f1Sx/p/04dN5xqeq/hw4udNNMTxEMPzY/Kx0NIWMa6O3EhMKEuYyPtqc98A==
Accept-Ranges	bytes
Server	AmazonS3
Last-Modified	Wed, 13 Dec 2023 15:20:26 GMT
ETag	"69799917e419f4b523da41fc7b96e574"
x-amz-request-id	0BBH3WQXR2DPJ2HV
Date	Tue, 23 Jan 2024 07:50:32 GMT
x-amz-server-side-encryption	AES256
Content-Type	application/zip

Executing a query on VirusTotal discloses that the server is hosted on Amazon S3; however, its reputation is flagged as malicious. After review this was proved to be a False Positive.

Execution

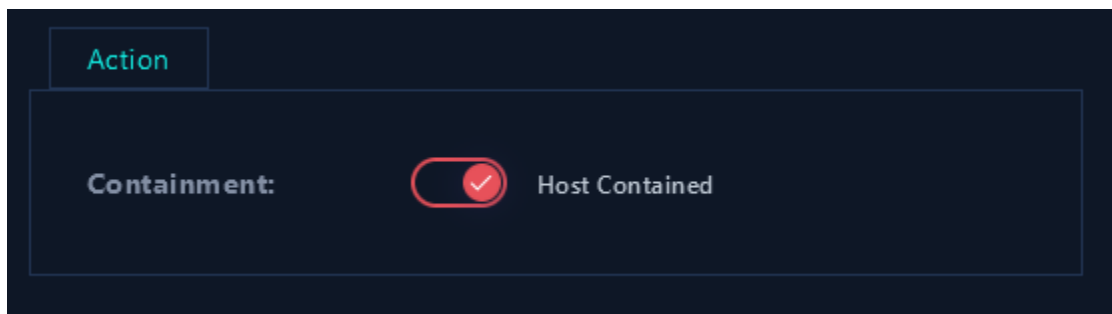
Defense evasion	Credential access	Discovery
<div>System Binary Proxy Execution (1/13)</div> <div>Rundll32</div> <div>2</div>		<div>Query Registry</div> <div>2</div>

Anyrun

Adversaries **may** bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system. (

Adversaries **may** interact with the Windows Registry to gather information about the system, configuration, and installed software.

Containment



In summary, this analysis unveils the execution of processes and the alteration of a registry key. Particularly noteworthy and potentially suspicious aspects include the use of `RUNDLL32.EXE` to open a file and the deployment of multiple instances of `NOTEPAD.EXE` for accessing different files. A comprehensive examination by a malware analyst is advised to scrutinize the contents of the `GoogleUpdate.bin` files and elucidate the motive behind the registry key modification, with the objective of identifying any potential malicious activities. There is no necessity to escalate the matter to a tier 2 analyst after reviewing the initial report.

Lesson Learned

- Avoid depending exclusively on OSINT tools to substantiate a case. It is imperative to conduct thorough research to conclusively identify something as malicious. In this instance, after verifying through various sources, it has been confirmed that the initial alert was a false positive.
- Never test potential malicious files without virtualization or a sandbox environment, as doing so without these safeguards puts you at risk of infection.
- Thorough documentation provides a solid foundation for any analysis, but the quality of documentation is crucial. It's not just about recording the steps taken, rather, it involves searching into the details to ensure a comprehensive understanding. Take the time to document every aspect of your dynamic analysis meticulously, as rushing through the process may lead to oversights or missing critical information. By dedicating sufficient time to document each step, you not only enhance the accuracy and reliability of your analysis but also create a valuable resource for future reference. Remember, the extra effort invested in detailed documentation can significantly contribute to the overall effectiveness of your dynamic analysis.

Appendix

MITRE ATT&CK Matrix								
Tactics 2		Techniques 2		Events 4				
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection
				System Binary Proxy Execution (1/13)		Query Registry		
				Rundll32		2		

MITRE Tactics

- Defense Evasion
- Discovery

MITRE Techniques

- System Binary Proxy Execution
- Query Registry

Artifacts

Host Information

----- -----	
Hostname:	John
Domain:	LetsDefend
IP Address:	172.16.17.82
Bit Level:	64
OS:	Windows 10
Primary User:	JohnComputer
Client/Server:	Client
Last Login:	Oct, 10, 2020, 6:53 PM