Official Incident Report

By: Ryan Stewart

EventID: 77

Rule Name: SOC138 - Detected Suspicious Xls File

Event Time: Mar 13, 2021, 08:20 PM

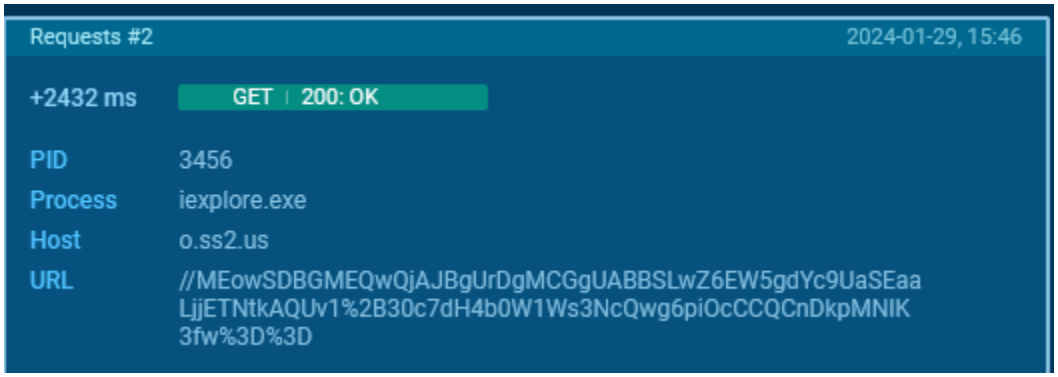
Table of contents

Alert

Upon a thorough examination of the alert trigger, it's shown that a process susceptible to exploitation was executed on the source address 172.16.17.56. This prompts a deeper investigation to distinguish the correlation between the alert and the threat indicator, specifically focusing on "unknown or unexpected outgoing network traffic."

To validate the truth of this alert, our next step involves scrutinizing the available logs meticulously. The aim is to delve 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.

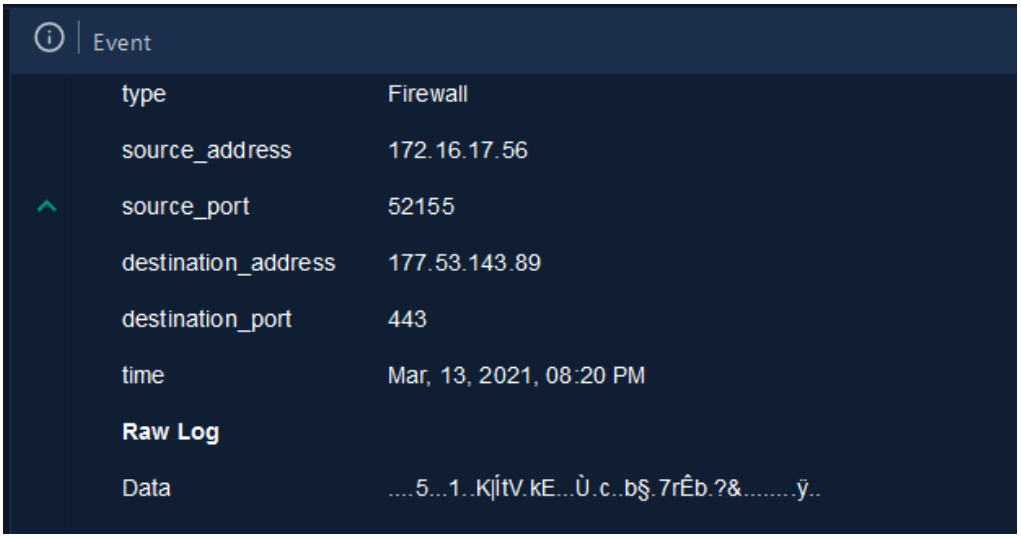
Detection



Verify

Analyzing the Log Management data for the IP address "172.16.17.56," identified as the source of the alert, reveals a GET request to the host "o.ss2.us" with the IP address 108.138.2.173 and port 80.

Legitimate programs commonly utilize GET requests to pull data from servers, but the specifics of this case involves a directed request to a particular host, complete with a URL path. The response code (200) signifies the “success” of the request, indicating that the server provided the requested data. The absence of proxy detection suggests that the request originated directly from the host machine. This is confirmed to be true.

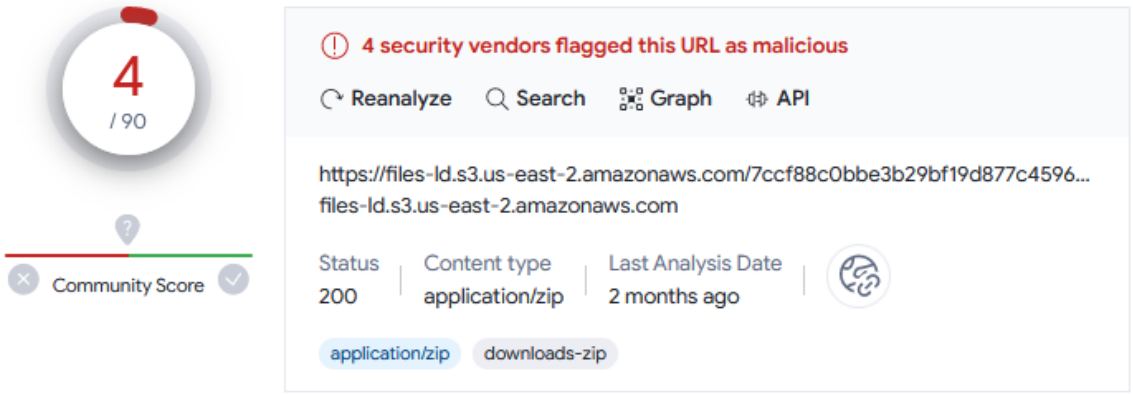


I determined during the initial investigation that it seems no evidence supports the possibility of a false positive alarm being identified. Furthermore, the presence of suspicious processes running on the relevant host and an associated DNS query has been detected (177.5.3.143.89), warranting further examination.

Analysis

IP Reputation

In the initial investigations, it is determined that the cause of the incident is the processes running on the source system (Sofia), but the destination IP could not be truly identified.



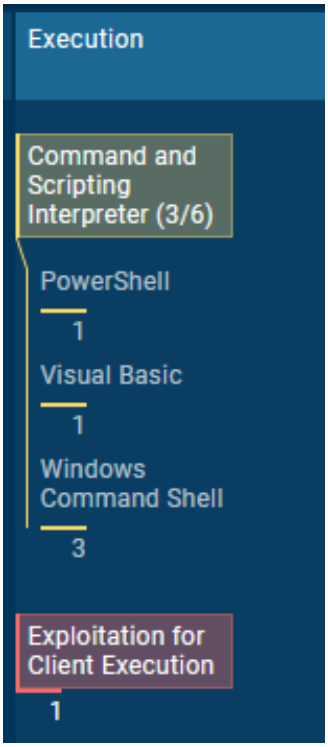
https://www.virustotal.com/gui/ip-address/52.219.178.194

Headers

Content-Length	69412
x-amz-id-2	UVwAjderj2KUUR0etbiD2Fw3aTaWtNSW8VTgHklHcjtnr67HrjE2R1hmVXry0n5v0eYNjqYWhSU=
Accept-Ranges	bytes
Server	AmazonS3
Last-Modified	Wed, 09 Aug 2023 19:05:53 GMT
ETag	"adee407a5d9f4425707fe5bd4c25aa14"
x-amz-request-id	2QCA04271A3NATGE
Date	Sun, 26 Nov 2023 04:17:59 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.

Execution

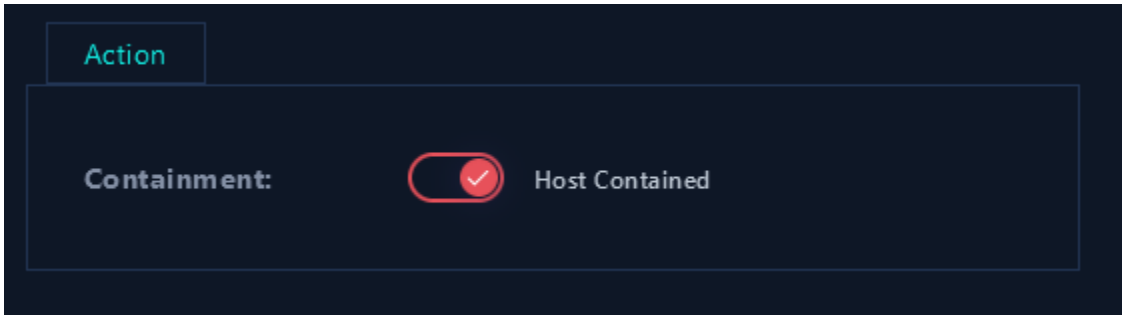


Anyrun

While analyzing the URL in a sandbox environment, the results indicate that command interpreters, commonly known as command-line interfaces (CLIs), offer a text-based environment for users to input commands for diverse tasks. In contrast, scripting interpreters are tailored to execute scripts—sequences of commands written in a scripting language.

The responsibilities of a Command and Scripting Interpreter encompass parsing and interpreting user commands or scripts, overseeing the execution of system commands, and enabling automation by executing predefined sequences of instructions.

Containment



Legitimate programs utilize cscript.exe to execute VBScript files for automation, system administration, or application scripting.

However, observed events suggest potential malicious usage. The script performs various actions like reading security settings, using base64 encoding, manipulating XML DOM elements, file operations, binary data handling, and establishing unusual connections from system programs. These actions raise concerns about potential malicious activities, including data exfiltration, remote command execution, or exploiting system vulnerabilities.

The compromised system is confirmed to be isolated from the network, and the .zip file containing the malware should be removed from the system.

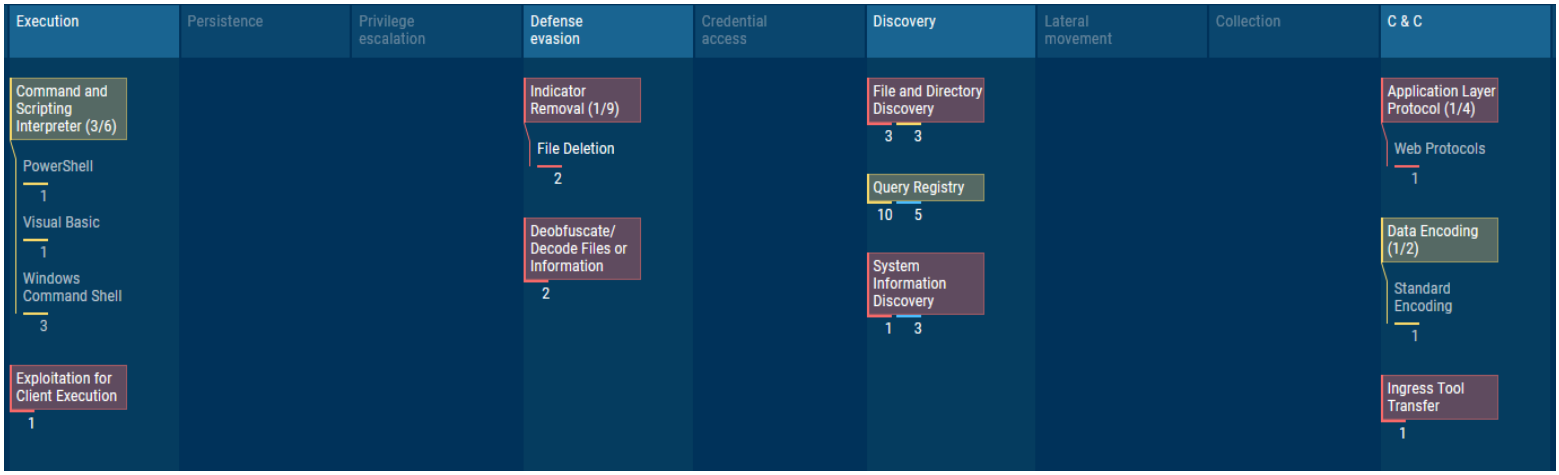
Lesson Learned

- Avoid the use of vulnerable products on servers and clients to minimize the risk of security breaches.

- Regularly monitor and execute application updates to ensure the latest security patches and enhancements are applied, enhancing the overall resilience of your systems.

- Conduct periodic endpoint tests as part of a proactive approach to bolstering information security awareness among employees. Regular testing helps identify potential vulnerabilities and reinforces a culture of vigilance in safeguarding sensitive information.

Appendix



MITRE Tactics

- Execution
- Defense Evasion
- Discovery
- Command and Control (C&C)

MITRE Techniques

- Command and Scripting/ Exploitation for Client Execution
- Indicator Removal, Deobfuscate/Decode Files
- File and Directory Discovery, Query Registry, System Information Discovery
- Application Layer Protocol, Data Encoding, and Ingress Tool Transfer

Artifacts

Host Information

Hostname:	Sofia
Domain:	LetsDefend
IP Address:	172.16.17.56
Bit Level:	64
OS:	Windows 10
Primary User:	Sofia2020
Client/Server:	Client
Last Login:	Oct 25, 2020, 11:44 PM