Author: Jack Fitzgerald

Official Incident Report

Date: Jun, 02, 2022, 03:22 PM

Event ID: 123

Rule Name: SOC173 - Follina 0-Day Detected

Table of Contents

Alert Details 2
Detection 3
Verify 4
Analysis 4
Containment 7
Summary 8
Lessons Learned 9
Remediation Actions 10
Appendix 10
MITRE ATT&CK 11
Artifacts 11
LetsDefend Playbook 11

Alert Details

Severity: Medium

Type: Malware

Source Address: 172.16.17.39

Hostname: JonasPRD

File Name: 05-2022-0438.doc

File Hash: 52945af1def85b171870b31fa4782e52

File Size: 10.01 Kb

AV Action: Allowed

Alert Trigger Reason: msdt.exe executed after Office document

Based on the information provided in the alert, it appears that a Windows binary has been suspiciously used on host **172.16.17.29**. The alert is triggered by rule SOC173 - Follina 0-Day Detected.

Upon reviewing the alert, it is observed that a file named **05-2022-0438.doc** with the file hash of **52945af1def85b171870b31fa4782e52** executed **msdt.exe** on host **172.16.17.39**.

The action is marked **allowed**, indicating that the binary was successfully run on the host machine.

Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

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 analyse the logs collected from the host by our security products.

According to CVE, a remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights.

By investigating the word document **05-2022-0438.doc**, with the MD5 hash of **52945af1def85b171870b31fa4782e52**, we can determine whether the file is malicious or benign.

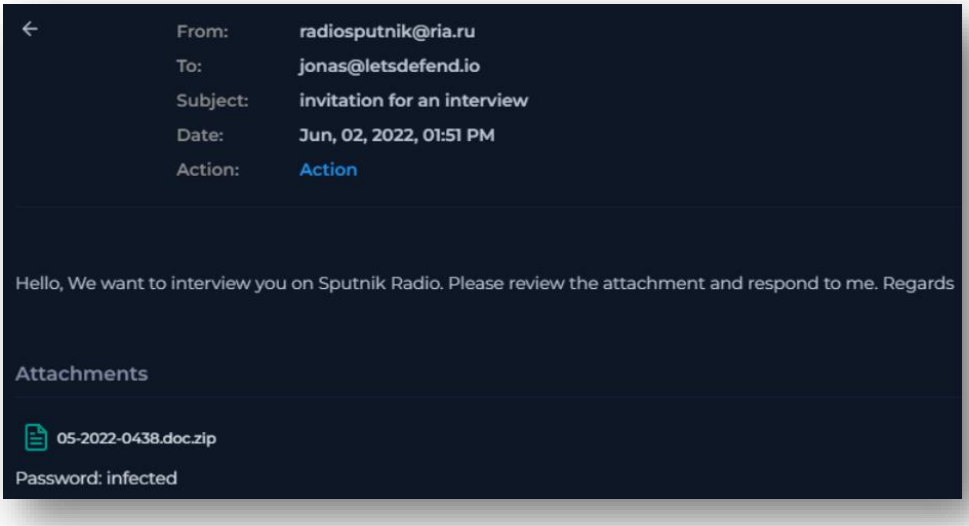
https://www.virustotal.com/gui/file/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784

46/65 security vendors flagged this file as malicious

Based on the information provided by **VirusTotal**, it appears that **05-2022-0438.doc** is not legit and has been flagged as malicious by many security vendors.

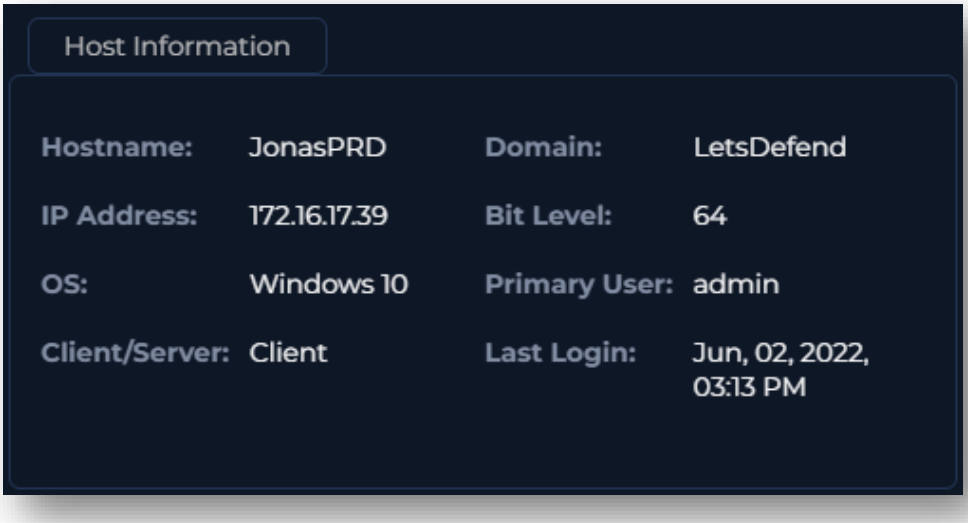
Analysis

We can begin the analysis by determining how the **05-2022-0438.doc** appeared on the host machine. To do this, we investigate Email Security for any signs.

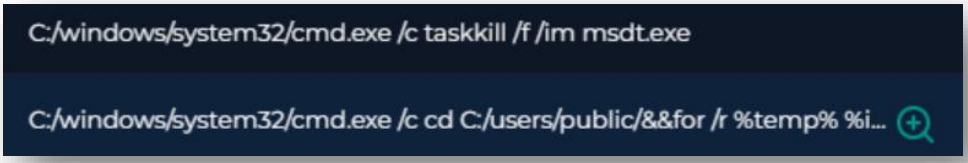


This phishing email was sent from radiosputnik@ria.ru to **jonas@letsdefend.io** appearing as an invitation for an interview for a radio channel. However, the attached file contains malware that will trigger the MSDT RCE exploit.

The next step is to investigate Endpoint Security for **JonasPRD**, which can provide valuable insights into the commands executed by the user and help us understand the scope and intent of the suspicious activity.



Within Terminal History, we find 2 events.



The first command **C:/windows/system32/cmd.exe /c taskkill /f /im msdt.exe** runs cmd.exe to forcibly kill any running msdt.exe process. This ensures no pre-existing msdt.exe instance is running. This is an unusual taskkill on msdt.exe, spawned from the cmd.exe process.

The second command **C:/windows/system32/cmd.exe /c cd C:/users/public/&&for /r %temp% %i in (05-2022-0438.rar) do copy %i 1.rar /y&&findstr TVNDRgAAAA 1.rar>1.t&&certutil -decode 1.t 1.c &&expand 1.c -F:* .&&rgb.exe** is a long and complicated command. This command is best broken up into sections:

1. **Changes working directory** to C:/users/public
2. **Recursively searches a temporary directory for files** named 05-2022-0438.rar and **copies them** to C:/users/public, assumed to locate a staged payload placed in the temporary directory prior
3. **Searches the copied files** for 'TVNDRgAAAA', assumed to recover an embedded base64 from a larger file

4. **Uses certutil binary to decode base64** stored in 1.t to binary (LOLBin)
5. **Extracts files** from 1.c (CAB archive) into the current directory
6. **Executes the resulting binary payload**

The command sequence supplied is the exact kind of post-exploit staging commonly seen after a successful MSDT exploit.

After reviewing the logs, it is seen that **JonasPRD** accessed the **www.xmlformats.com** domain (C2 Traffic) with IP address **141.105.65.149**.

https://www.virustotal.com/gui/ip-address/141.105.65.149

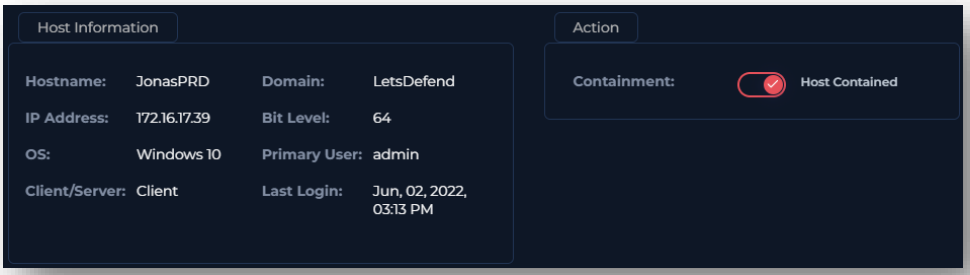
1/95 security vendor flagged this IP address as malicious

https://www.virustotal.com/gui/domain/www.xmlformats.com

10/95 security vendors flagged this domain as malicious

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.



Summary

The incident involves a compromised system named **JonasPRD** with an IP address of **172.16.17.39**. The alert was triggered by the detection of a suspicious **word document** being used, based on the rule SOC173 - Follina 0-Day Detected.

Upon further analysis, it was discovered that **05-2022-0438.doc** was a malicious file, identified as the **Follina 0-Day**. Remote Code Execution (RCE) when msdt.exe is called using the URL protocol from Word.

An email was sent to **jonas@letsdefend.io** from **radiosputnik@ria.ru** containing **05-2022-0438.doc** (Malware). The user accessed this file, exposing their system to the **Follina 0-Day Exploit**.

C2 traffic was accessed at **141.105.65.149** where files were extracted, and the resulting binary payload was executed.

The analysis of **JonasPRD's** Endpoint Security and Log Management revealed suspicious activity regarding this alert, due to the action of the SIEM, having **allowed** the malware to be executed.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- Default-trusted binaries can be abused
- Office documents can execute code without macros
- External content loading is a major blind spot
- Patch cycles must include emergent 0-days, not only scheduled updates

Remediation Actions

- Apply Microsoft's patch that fixed CVE-2022-30190
- Block/monitor certutil.exe usage
- Disable macros
- Educate users about suspicious email attachments

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Initial Access	T1598.002 - Phishing for Information: Spearphishing Attachment
Defense Evasion	T1218 - System Binary Proxy Execution
Execution	T1204.002 - User Execution: Malicious File
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols

Artifacts

Value	Comment	Type
www.xmlformats.com	Malicious C2 address domain	URL Address
radiosputnik@ria.ru	Email sender from Russia, containing Follina 0-Day malware	E-mail Sender
ria.ru	Malicious domain	E-mail Domain
141.105.65.149	C2 Address accessed by JonasPRD	IP Address
52945af1def85b171870b31fa4782e52	05-2022-0438.doc	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 123