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

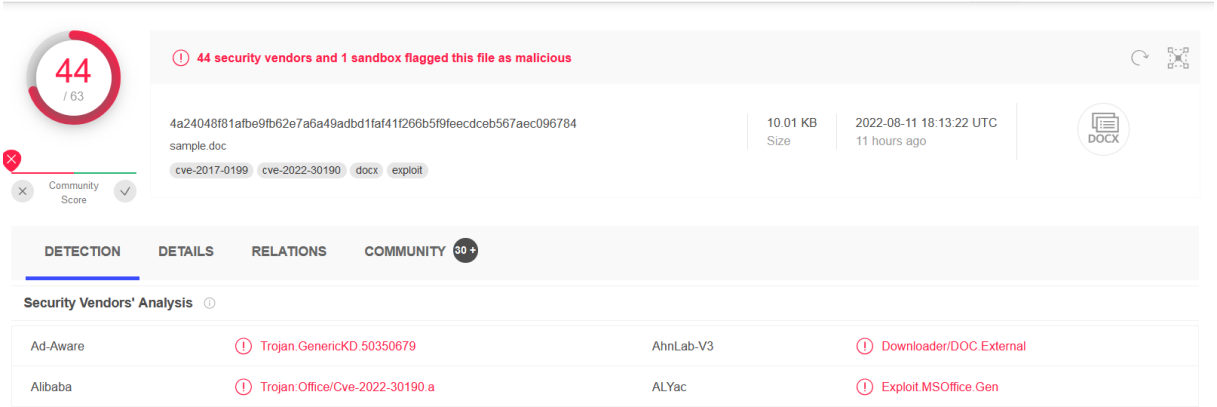
★ Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability, CVE-2022-30190

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	

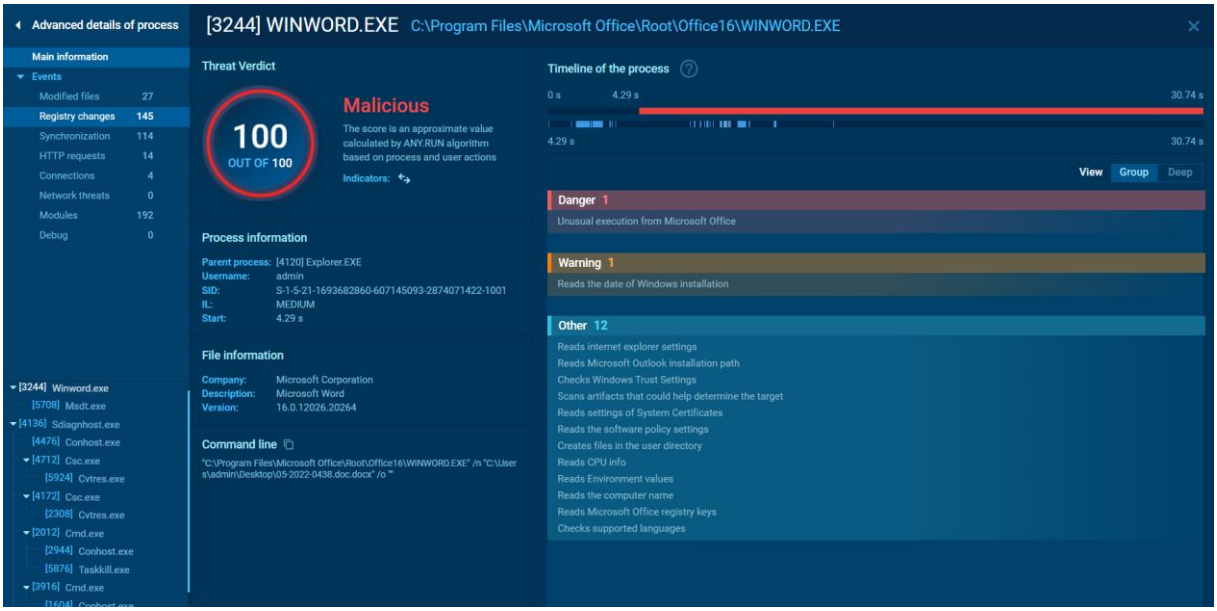
As we can see, a file named 05-2022-0438.doc.zip has been alerted as “msdt.exe executed after Office document” which is suspicious enough to analyze details.

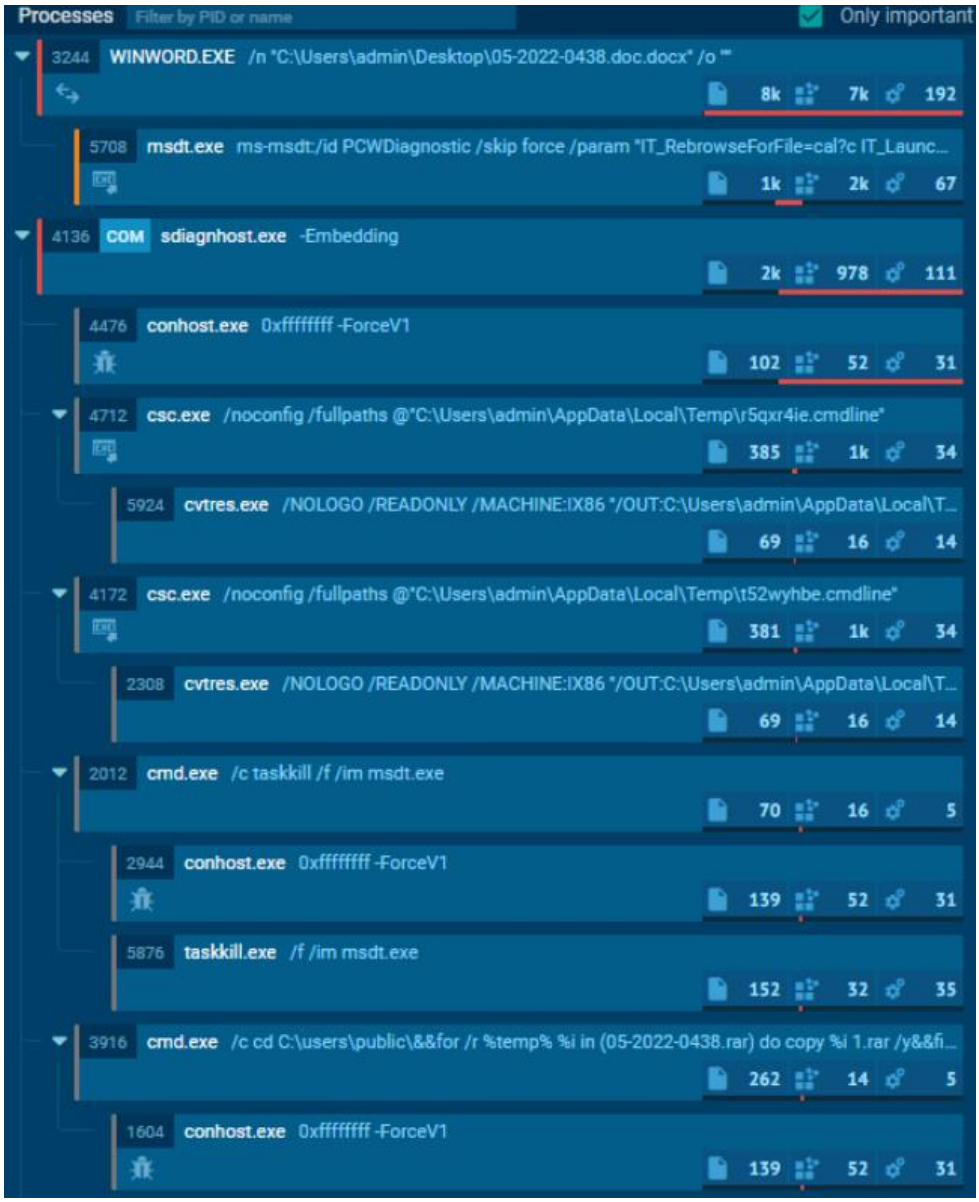
File Hash: **52945af1def85b171870b31fa4782e52**

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.

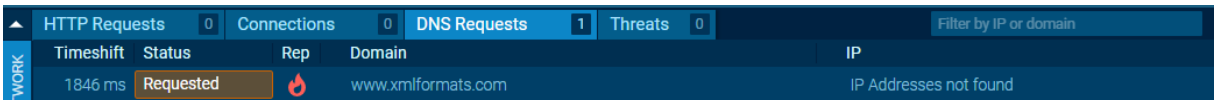


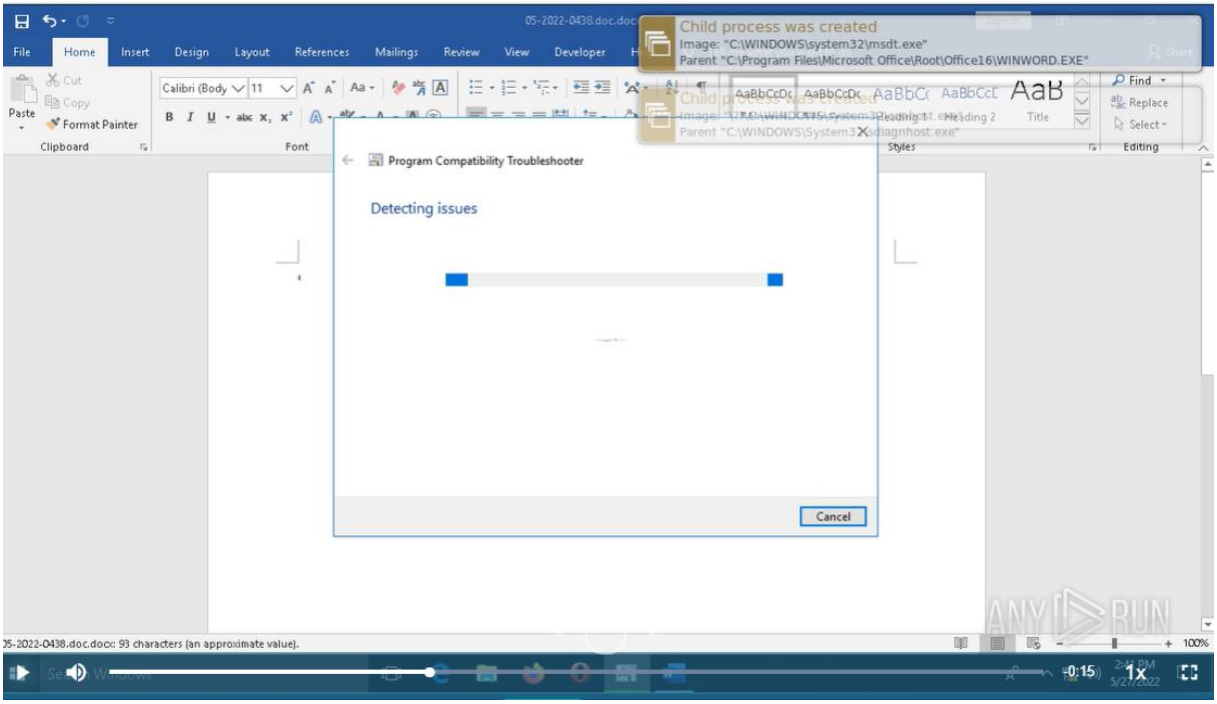
We can get more information through AnyRun as well. ([05-2022-0438.doc (MD5: 52945AF1DEF85B171870B31FA4782E52) - Interactive analysis - ANY.RUN])

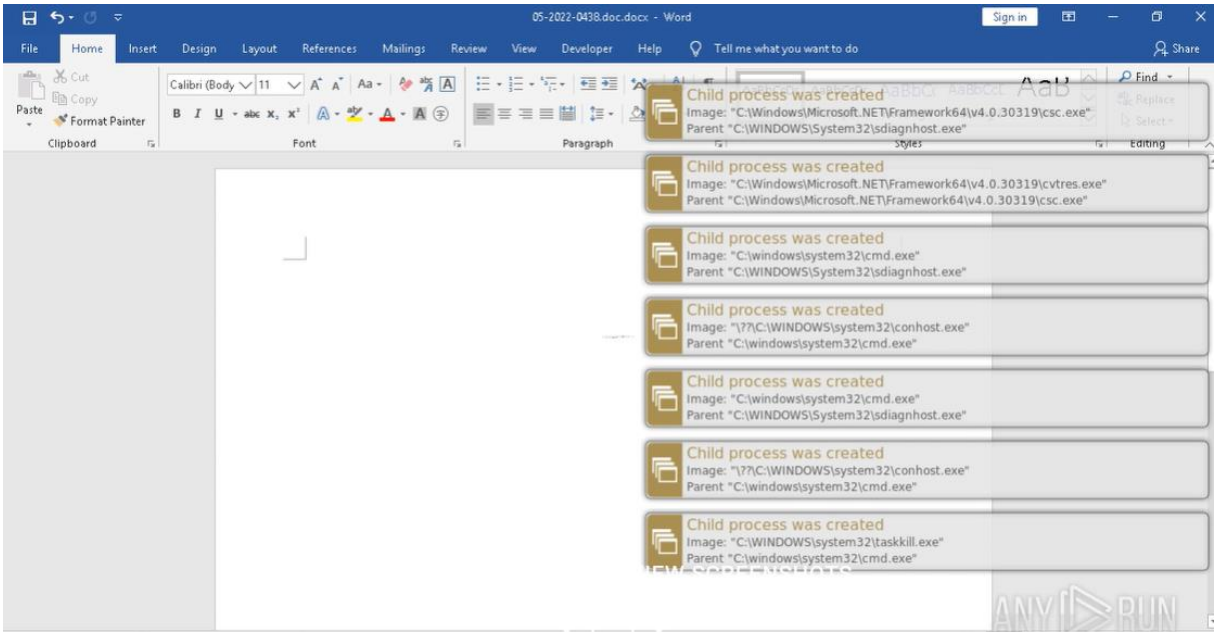




We can easily see, this doc file has some suspicious operations like creating unusual child processes, modifying some files and attempting to change registry values, suspicious command line entries with a DNS connection request which will help us on our investigation.







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 lets' check if there is any related mails through our mailbox.

← invitation for an interview

From: Ellie
radiosputnik@ria.ru
June 2, 2022, 1:51 p.m.

>

To: Jonas
jonas@letsdefend.io
June 2, 2022, 1:51 p.m.

Hello,

We want to interview you on Sputnik Radio. Please review the attachment and respond to me.

Regards

Attachments

05-2022-0438.doc.zip

Password: infected

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	

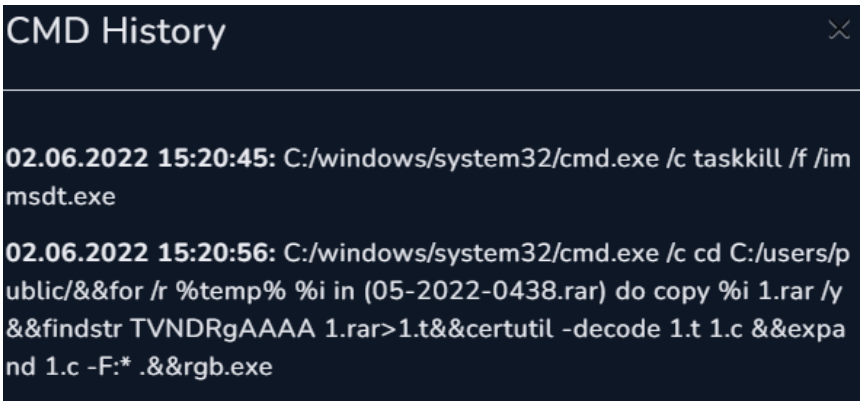
Raw Log

URL:
https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/

Close

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



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