From Follina to Rozena - Leveraging Discord to Distribute a Backdoor

fortinet.com/blog/threat-research/follina-rozena-leveraging-discord-to-distribute-a-backdoor

July 6, 2022

In May 2022, Microsoft published an advisory about CVE-2022-30190, which is about a Microsoft Windows Support Diagnostic Tool (MSDT) remote code execution vulnerability. Attackers can inject a malicious external link to an OLE Object in a Microsoft Office document, then lure victims to click or simply preview the document in order to trigger this exploit. It will then execute a payload on the victim's machine. Since this vulnerability is a public exploit and has high severity, FortiGuard Labs published an Outbreak Alert on 31st May and a blog article to address it on June 1, 2022.

During our tracking last month, we found a document that exploited CVE-2022-30190, aka Follina, then downloaded Rozena to deploy a fileless attack and leverage the public Discord CDN attachment service. Rozena is a backdoor malware that is capable of injecting a remote shell connection back to the attacker's machine. In this blog we will explain how an attacker delivers this payload through this vulnerability, along with details of Rozena and its shellcode.

Affected platforms: Microsoft Windows
Impact parties: Microsoft Windows Users
Impact: Full Control of Affected Machine
Severity: Critical

Exploitation

The original malicious document (SHA256: 432bae48edf446539cae5e20623c39507ad65e21cb757fb514aba635d3ae67d6) contains an external web link as in Figure 1. The relationship directory (word/_rels/document.xml.rels) is an XML file that maps relationships within the .docx file, and also with resources outside of the package, such as links or images.

Figure 1. Document.xml.rels contains a malicious external link in oleObject

Once the document is clicked (as shown in Figure 2), it starts connecting to the external Discord CDN attachment space 'hxxps://cdn[.]discordapp.com/attachments/986484515985825795/986821210044264468/index[.]htm' to download an HTML file.

Figure 2. Connecting to an external link after clicking the document

After it downloads the HTML file (SHA256: 3558840ffbc81839a5923ed2b675c1970cdd7c9e0036a91a0a728af14f80eff3), the document then invokes msdt.exe with a PowerShell command. The complete payload is shown in Figure 3.

Figure 3. index.html invokes MSDT

It has a little obfuscation with a concatenation of separate strings that assemble at run time to hide the actual command and evade simple string detection. We decoded a Base64 string and the complete command is shown in Figure 4.

The PowerShell code will download one batch file cd.bat (SHA256: 5d8537bd7e711f430dc0c28a7777c9176269c8d3ff345b9560c8b9d4daaca002) and start it with no window to hide itself. Then it invokes another web request to download Rozena and saves as "Word.exe" (SHA256: 69377adfdfa50928fade860e37b84c10623ef1b11164ccc6c4b013a468601d88) in the Windows Tasks folder.

These two files are also downloaded from the Discord CDN attachment space with the same channelID as the external link in the original document.

Figure 4. Base64 decoded command

As shown in Figure 5, the cd.bat file has four tasks:

- Download another document, 1c9c88f811662007.docx (SHA256: e3af143ba12209fafdc3089a740d23faf59f6f1508c00d8f56f8cc9d0c8ebf89) for distraction
- Kill processes “msdt.exe” and “WINWORD.exe” to wipe out the trace of exploiting CVE-2022-30190
- Create persistence for Rozena “Word.exe” by adding registry run keys.
- Delete the bat file.

Figure 5. cd.bat file contents

Distraction

Before diving into Rozena, this attacker decided to distract the victim. The original file has no content besides an external link in oleObject. To keep the victim from noticing anything odd the batch file downloads another Word document, 1c9c88f811662007.docx with a lot of pictures in it (See Figure 6). To make it seem more real, this document is saved in directory C:\\users\$env:USERNAME\Downloads, with a shorter name, 18562.docx.

Figure 6. Word document for distraction

Rozena

The attacker leverages the default Window’s feature, which is not to show the file extension. Therefore, the attacker tricks the victim as shown in Figure 7. The green one is the document for distraction with no harm, and the red one is Rozena. It uses the Microsoft Word icon while it is an executable file. The PE header is shown in Figure 8.

Figure 7. Rozena “Word.exe” uses the Microsoft Word file icon

Figure 8. The File header of Rozena

After execution, it will create a process for a PowerShell command. We can find the chain from the process explorer (shown in Figure 9). And the full PowerShell command is shown in Figure 10, which is Base64-encoded.

Figure 9. Execution of Rozena

Figure 10. Full PowerShell command extracted from Rozena

As shown in Figure 11, the decoded command has only one job: inject shellcode. First, it defines a variable “$gcr” for the whole injection procedure. It uses DLLImport for kernel32.dll and msvcrt.dll for importing specific APIs: VirtualAlloc, CreateThread, and Memset, to achieve code injection. And it has some hexadecimal bytes that define the block of code to be injected later. Then it copies these bytes to the allocated memory and injects them into the running PowerShell.exe. Finally, it sets up a loop to start sleep. In the bottom part highlighted in red, it encodes the above injection code from “$gcr” with Base64, then invokes a new PowerShell process with parameter -ec.

Figure 11. Decoded PowerShell command

Shellcode

We extracted the shellcode from the command shown in Figure 12 (SHA256: 27F3BB9AB8FC66C1CA36FA5D62EE4758F1F8FF75666264C529B0F2ABBADE9133). To dive deep in to this, we checked this binary with IDA. It can divide into following steps:

1. Retrieve decode key
2. Retrieve location relative to EIP (Figure 13)
3. Decode (XOR)

Figure 12. Extracted shellcode

Figure 13. Retrieve location relative to EIP

From the above instructions, we can identify this as Shikata Ga Nai (SGN) encoding. The SGN encoding schema is from the most popular exploit framework, Metasploit. It is a polymorphic XOR additive feedback encoder that allows malicious actors to evade detection. After decoding it, the main purpose of this shellcode is to start a reverse shell to the attacker's host microsofto.duckdns[.]org with TCP port 55911 as shown in Figure 14.

Figure 14. Reverse shell

The complete attack scenario from delivering a malicious document and exploiting CVE-2022-30190 (Follina) to deploying Rozena from the Discord CDN attachment space is shown in Figure 15.

Figure 15. Attack scenario

Conclusion

CVE-2022-30190 is a high-severity vulnerability that lets a malicious actor deliver malware though an MS Word document. Microsoft already released a patch for it on June 14, 2022. In this blog we showed how an attacker exploits Follina and included details of Rozena and the SGN ShellCode. Users should apply the patch immediately and also apply FortiGuard protection to avoid the threat.

Fortinet Protections

Fortinet released IPS signature MS.Office.MSHTML.Remote.Code.Execution for CVE-2022-30190 to proactively protect our customers. The signature is officially released in IPS definition version 20.326.

The downloader and all related malware from that site are detected and blocked by FortiGuard Antivirus:

MSOffice/CVE_2017_0199.A!tr

BAT/Agent.1A81!tr

JS/Follina.6FB9!tr

Data/Shikata.A!tr

W32/PossibleThreat

Both the downloaded URL and attacker's host have been rated as "Malicious Websites" by the FortiGuard Web Filtering service.

The oleObject data in Microsoft Office files can be disarmed by the FortiGuard Content Disarm & Reconstruction (CDR) service.

All Fortinet Protections and Outbreak Detection, Threat Hunting actions for Fortinet SOC solutions can be found in the Folina Outbreak Alert.

IOCs

SHA256:

432bae48edf446539cae5e20623c39507ad65e21cb757fb514aba635d3ae67d6

5d8537bd7e711f430dc0c28a7777c9176269c8d3ff345b9560c8b9d4daaca002

3558840ffbc81839a5923ed2b675c1970cdd7c9e0036a91a0a728af14f80eff3

27f3bb9ab8fc66c1ca36fa5d62ee4758f1f8ff75666264c529b0f2abbade9133

69377adfdfa50928fade860e37b84c10623ef1b11164ccc6c4b013a468601d88

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.