Chinese APT TA413 Resumes Targeting of Tibet Following COVID-19 Themed Economic Espionage Campaign Delivering Sepulcher Malware Targeting Europe

proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic

August 31, 2020

Blog
Threat Insight
Chinese APT TA413 Resumes Targeting of Tibet Following COVID-19 Themed Economic Espionage Campaign Delivering Sepulcher Malware Targeting Europe

September 01, 2020 Michael Raggi and the Proofpoint Threat Research Team

Executive Summary

Beginning in the first half of 2020, the rapid international spread of the COVID-19 virus introduced a shift within the threat landscape towards pandemic-themed social engineering lures. Public research has noted several Chinese APT groups adopting COVID-19 phishing lures in recent months to carry out espionage campaigns against established and expanding target sets. In March 2020, Proofpoint researchers observed a phishing campaign impersonating the World Health Organization's (WHO) guidance on COVID-19 critical preparedness to deliver a new malware family that researchers have dubbed "Sepulcher". This campaign targeted European diplomatic and legislative bodies, non-profit policy research organizations, and global organizations dealing with economic affairs. Additionally, a sender email identified in this campaign has been linked to historic Chinese APT targeting of the international Tibetan community using payloads linked to LuckyCat malware. Subsequently, a phishing campaign from July 2020 targeting Tibetan dissidents was identified delivering the same strain of Sepulcher malware. Operator email accounts identified in this campaign have been publicly linked to historic Chinese APT campaigns targeting the Tibetan community delivering ExileRAT malware. Based on the use of publicly known sender addresses associated with Tibetan dissident targeting and the delivery of Sepulcher malware payloads, Proofpoint researchers have attributed both campaigns to the APT actor TA413, which has previously been documented in association with ExileRAT. The usage of publicly known Tibetan-themed sender accounts to deliver Sepulcher malware demonstrates a short-term realignment of TA413's targets of interest. While best known for their campaigns against the Tibetan diaspora, this APT group associated with the Chinese state interest prioritized intelligence collection around Western economies reeling from COVID-19 in March 2020 before resuming more conventional targeting later this year.

Delivery and Exploitation

In the latter half of March 2020, researchers identified a malicious email sent to numerous entities involved with economic policy and forecasting within Europe. The emails contained a weaponized RTF attachment that impersonated the WHO's "Critical

preparedness, readiness and response actions for COVID-19, Interim guidance" document. This guidance was initially published on March 7, 2020, while the weaponized attachment was delivered by threat actors on March 16, 2020. When the malicious RTF attachment named "Covdi.rtf" is executed, it exploits a Microsoft Equation Editor vulnerability and installs an embedded malicious RTF object in the form of a Windows meta-file (WMF) to the file directory %\AppData\Local\Temp\wd4sx.wmf. This method is used by a known variant of the Royal Road RTF weaponizer which is shared among numerous Chinese APT actors. The execution of the WMF file ultimately results in the delivery and installation of the previously unidentified Sepulcher malware.

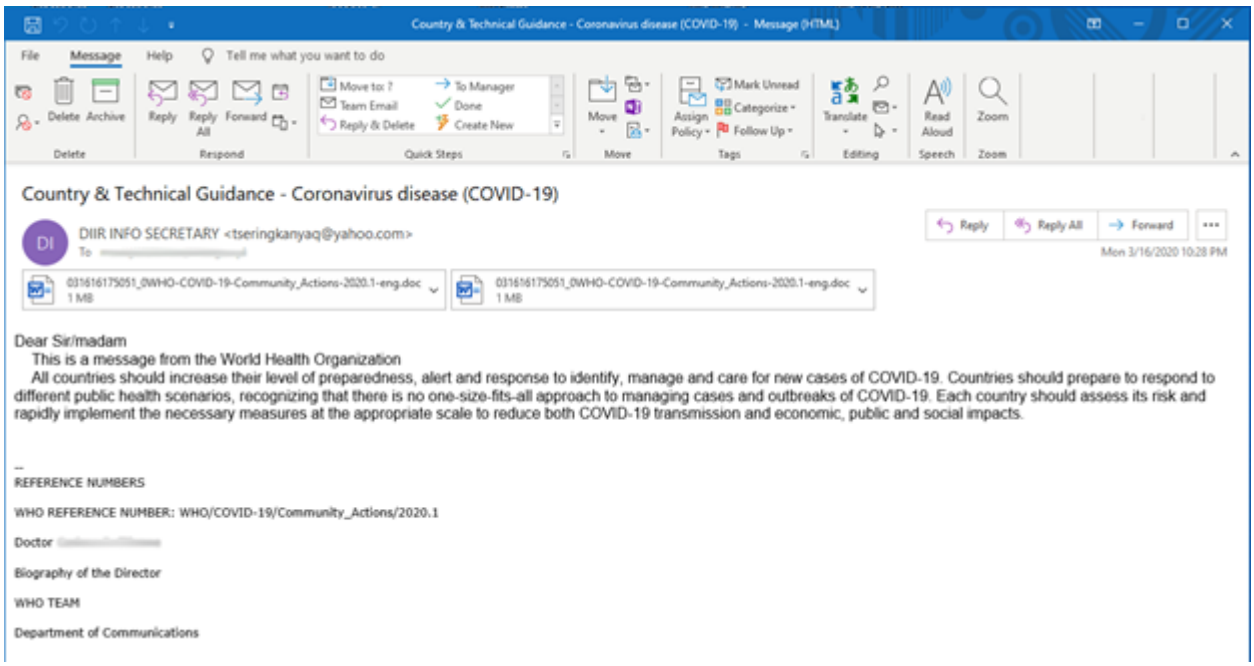

Figure 1: Malicious Email from March 2020 "Country & Technical Guidance – Coronavirus disease…"

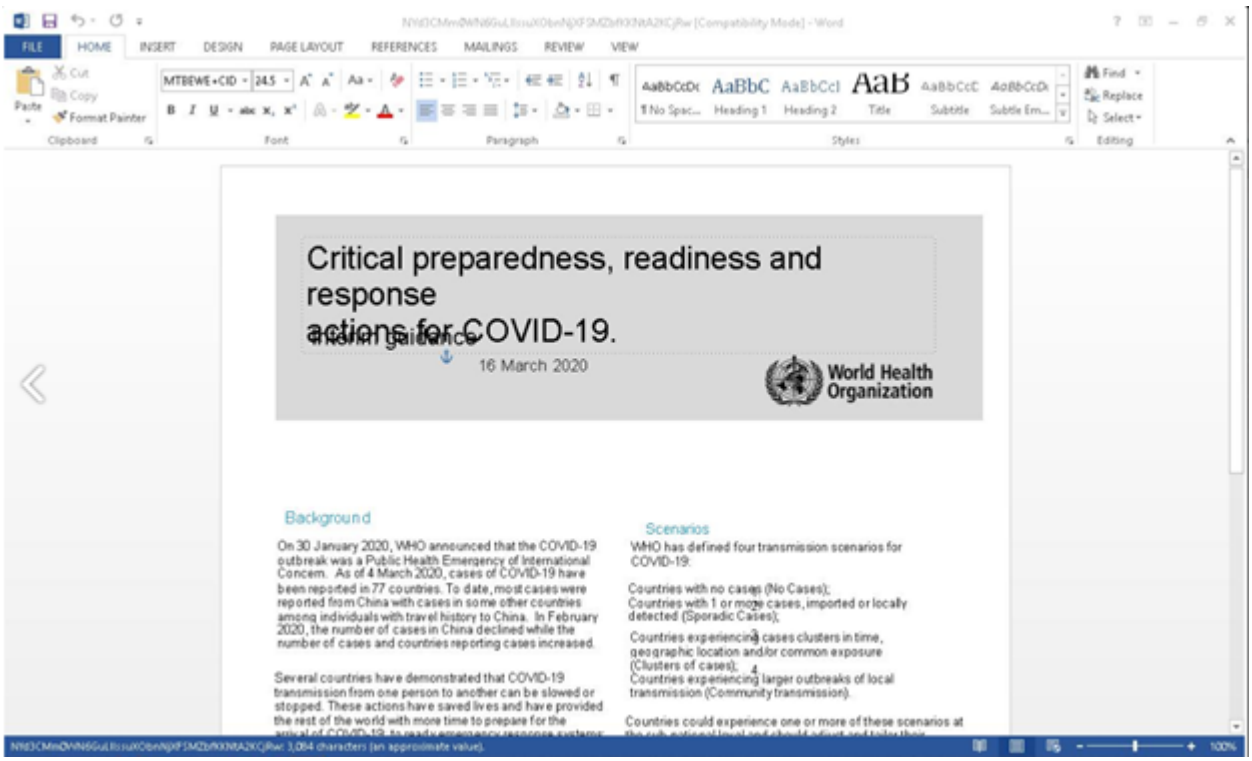

Figure 2: Lure Document impersonating WHO guidance on COVID-19.

The emails in this campaign originated from the Yahoo free-mail sender address tseringkanyaq@yahoo[.]com. This sender account was first written about in a joint report by Citizen Lab, the Munk School of Global Affairs, and the University of Toronto in 2013, which described Chinese APT activity. The report indicated this email address had been used in phishing campaigns from May 2012 through June 2013 to target Tibetan members of civil society. Specifically, the sender address is thought to impersonate Kanyag Tsering, a Tibetan monk and activist that held a high profile in the media during the historic campaign time period. The email address delivered malicious attachments that installed ShadowNet, Duojeen, and PubSab (OS X) malware. The report goes on to note that these malware payloads were found to share infrastructure with LuckyCat malware that was identified by TrendMicro also being deployed against Tibetan targets in 2012. LuckyCat malware was more recently linked to Chinese APT malware targeting the international Tibetan community via an APK variant reported by Talos Intelligence in January 2019. The LuckyCat Android RAT utilized in early 2019 used the same infrastructure as ExileRAT payloads to target members of a Central Tibetan Administration mailing list.

Following the Sepulcher malware campaign in March 2020, a subsequent malicious email campaign delivering this malware was identified on July 27, 2020. The email included a malicious PowerPoint (PPSX) attachment conspicuously named “TIBETANS BEING HIT BY DEADLY VIRUS THAT CARRIES A GUN AND SPEAKS CHINESE.ppsx”. The SMTP header From field impersonated the “Women's Association Tibetan," while the attachment, once opened, referenced “Tibet, Activism and Information”. When the PowerPoint attachment is executed, it calls out to the IP 118.99.13[.]4 to download a Sepulcher malware payload named “file.dll”. Additionally, the distinct C2 request

hxxp://118.99.13[.]4:1234/qqqzqa that occurs at that time has been seen previously in association with TA413 malware campaigns. Upon the delivery of the payload “file.dll” it is saved as “credential.dll” and executed resulting in a C2 communication with the domain Dalailamatrustindia.ddns[.]net. The attachment title, decoy content, impersonated sender, and Dalai Lama Trust in India-themed C2 affirms this campaign’s focus on individuals associated with the Tibetan Leadership in Exile.

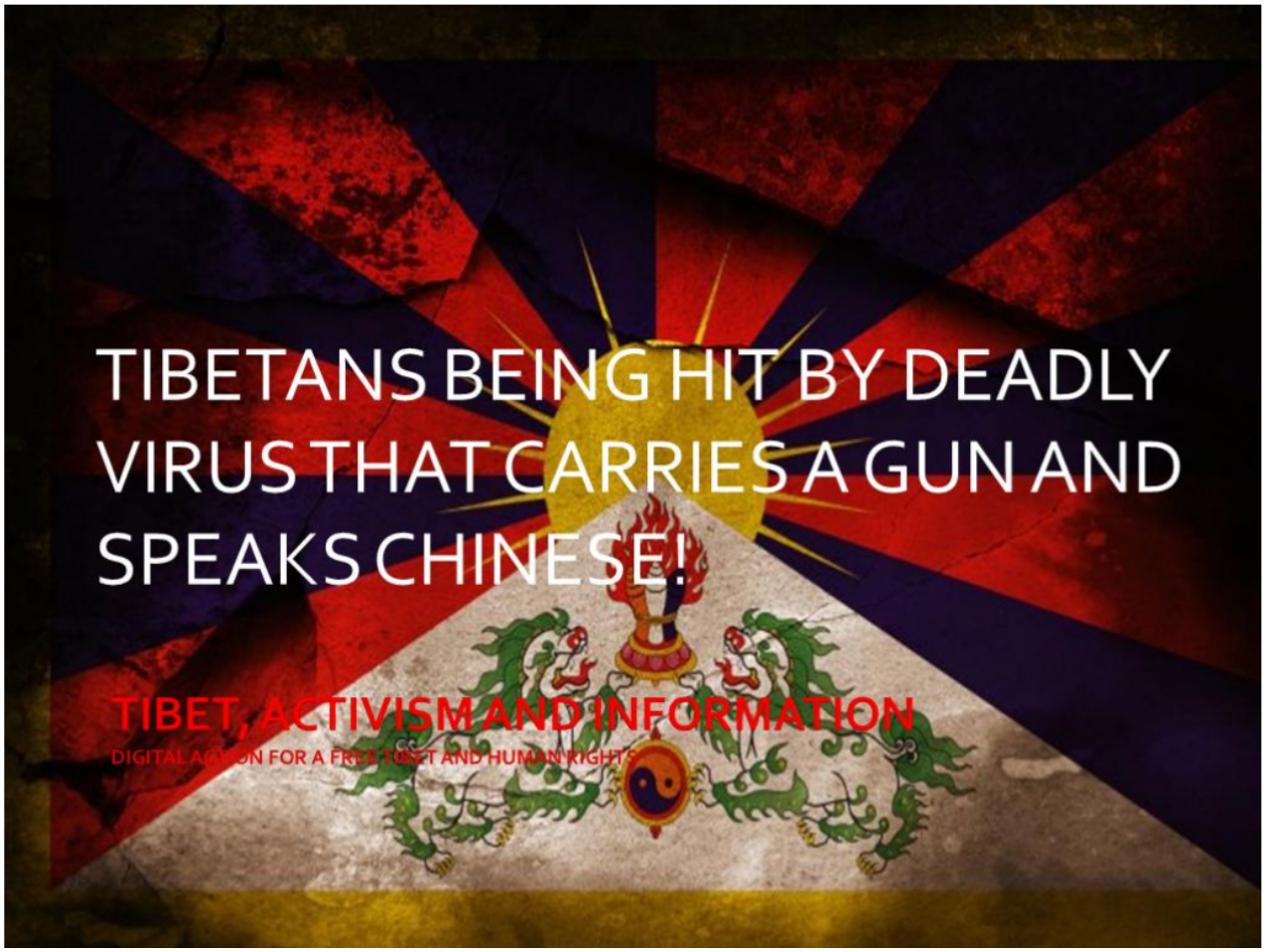

Figure 3: Lure Document TIBETANS BEING HIT BY DEADLY VIRUS THAT CARRIES A GUN AND SPEAKS CHINESE.ppsx.

This Sepulcher malware campaign is highly reminiscent of the January 2019 campaign that utilized PPSX attachments to deliver ExileRAT malware, previously documented by Talos Intelligence. The foremost commonality between these campaigns, apart from the attachment type and content of the PowerPoint, is the sender email “mediabureauin@gmail[.]com" which was shared in both the historic ExileRat campaign and the recent Sepulcher malware campaign from 2020. The intermittent use of a single email address in multiple APT campaigns spanning nearly eight years is uncommon in cyber threat research. While it is not impossible for multiple APT groups to utilize a single operator account (sender address) against distinct targets in different campaigns, it is unlikely. It is further unlikely that this sender reuse after several years would occur twice in a four-month period between March and July, with both instances delivering the same Sepulcher malware family. The sharing of delivery/hosting infrastructure, malware payloads, or post-exploitation tools have been observed across Chinese APT groups and

can be considered more common. However, the use of operator accounts spanning multiple APT campaigns is much less common. It is less advantageous to share operator accounts as the creation of new free-mail accounts for phishing delivery is trivial and does not represent a cost barrier to operation. Additionally, it increases the likelihood of detection by targeted organizations. Although the re-emergence of two publicly known sender accounts after multiple years is unusual, the use of a known sender account to target a new group of recipients in this case may represent an opsec failure resulting from a broader re-tasking of existing APT threat actors in response to an unprecedented global crisis.

Sepulcher Malware

The Sepulcher malware payload (SHA256: 4a4a959aef64ea48e2b831468119180d0af4b5b685c35170f5db3f001b9cc319) observed in the March 2020 campaign targeting European economic targets was analyzed for this publication. The file "wd4sx.wmf" is installed by the initial RTF attachment upon execution and contains the final Sepulcher malware payload and a payload dropper. Sepulcher is a basic RAT payload that can gather intelligence on the resources of the infected system, spawn a reverse CMD shell, and read from and write to file.

Initially, the WMF file installs a temporary file named "OSEB979.tmp" to the Windows temporary directory that serves as a payload dropper. It installs the final Sepulcher payload "credential.dll" to the directory %AppData%\Roaming\Identities\Credential.dll. It then creates a scheduled task named "lemp" which uses rundll32.exe to run the Sepulcher payload and call the export function "GetObjectCount" on an hourly basis. This scheduled task serves as a persistence mechanism for Sepulcher malware.

```
schtasks /create /tr "rundll32.exe %APPDATA%\Identities\Credential.dll,GetObjectCount" /tn "lemp" /sc HOURLY
```

Figure 4: Scheduled task and persistence mechanism for executing Sepulcher payload.

The Sepulcher configuration is stored in the registry under the Registry Key HKEY_CURRENT_USER\Software\Microsoft\WAB\Resources. It contains four distinct keys named "DefaultString", "Credentials", "Security", and "Property". The "DefaultString" is randomly generated by CoCreatGuid() with the initial formatting done by the multibyte _sprintf_(). This is then stored in the registry by RegSetValueExW() which uses the wide character type. This results in a broken encoding that renders as Chinese characters. This should not be interpreted as an indication that the threat actor is using Chinese characters in the malware configuration, despite broader attribution pointing to Chinese state associated actors. The remaining three keys "Credentials", "Security", and "Property" represent the three C2 servers in encrypted format that are utilized by the malware. The below algorithm is used to decrypt the C2 servers which, in this sample, are revealed to be the IP address 107.151.194[.]197 utilizing ports 80, 443,

and 8080. Notably, this IP address hosted a single domain welfaretibet[.]tk as of April 5, 2020. This suggests that threat actors did not establish standalone network infrastructure for targeting European economic entities and intended to utilize this IP to persist in targeting entities related to Tibetan matters in the future.

Decrypted C2 IP Addresses:

- 107.151.194[.]197:80
- 107.151.194[.]197:443
- 107.151.194[.]197:8080

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\WAB\Resources]
"DefaultString"="些財紆埞ㅄ腤ㄴ靨些簭簲ㅂ恁膷繣簐"
"Credentials"="44<07=215>649::>969"
"Security"="44<07=215>649::>=2"
"Property"="44<07=215>649::>=2>8"
```

Figure 5: Sepulcher malware configuration.

```python
def crypt(data, key):
    result = ""
    for i, b in enumerate(data):
        b = ord(b) + key[i % len(key)]
        result += "%c" % b
    return result

def decrypt(data, key):
    result = ""
    for i, b in enumerate(data):
        b = ord(b) - key[i % len(key)]
        result += "%c" % b
    return result
```

Figure 6: Sepulcher malware C2 decryption algorithm.

Sepulcher malware has seven work modes that include conducting reconnaissance on an infected host, spawning a reverse command shell, reading from file, and writing to file. More granularly, additional commands exist within the intelligence gathering/reconnaissance work modes (1002, 1003, 1004) which carry out

reconnaissance functionality within the infected host. These commands include obtaining information about the drives, file information, directory statistics, directory paths, directory content, running processes, and services. Additionally, it is capable of more active functionalities like deleting directories and files, creating directories, moving file source to destination, spawning a shell to execute commands, terminating a process, restarting a service, changing a service start type, and deleting a service.

Mode	Functionality
1005	Reverse command shell
1006	Read from File
1009	Do nothing /PONG
1919	Write to File
1002	System intelligence gathering/reconnaissance functionalities
1003	
1004	

Figure 7: Sepulcher malware work modes (commands).

Command	COMMAND_DATA.data	Functionality
6001	Drive letter	Get drive information: sizes, type, path, etc.
6002	File path	Get file information in a WIN32_FILE_ATTRIBUTE_DATA structure.
6003	Directory path	Get directory statistics: number of files, sub directories and total size.
6004	Directory path	Get directory content information: WIN32_FILE_ATTRIBUTE_DATA and dir/file name.

6005	N/A	Delete directory / file and empty the recycle bin.
6006	Directory name	Create directory.
6007	Src file path, Dst file path	Move file Source to Destination.
6008	N/A	Get all drives information: sizes, types, path, etc.
6009	Command string	Shell execute command.
6010	PID string	Terminate process.
6017	N/A	Get directory content detailed information: WIN32_FILE_ATTRIBUTE_DATA and dir/file name for each dir/file inside
6018	N/A	Get list of running processes.
6019	N/A	Get list of services.
6020	N/A	Restart service.
6021	N/A	Change service start type.
6023	N/A	Delete service.

Figure 8: Sepulcher intelligence gathering/reconnaissance commands.

Command and Control

The malware receives commands including various mode commands and sub-commands via the C2 addresses decrypted from the malware's configuration. The initial communication is initiated by the client via a single byte XOR encrypted handshake packet and completed via a server-to-client packet that is not encrypted. The communication then continues with a single byte XOR encrypted client-to-server PACKET_HELLO that specifies the malware command mode. In the case of modes 1002, 1003, and 1004, which are the commands that initialize the intelligence gathering/reconnaissance capabilities of the malware, the server replays the PACKET_HELLO with mode commands in the initial PACKET_HANDSHAKE via a

PACKET_COMMAND. The same method of C2 communication was observed for Sepulcher sub-commands, however, the format of observed sub-commands delivered via the "COMMAND_DATA" field varied depending on content of the PACKET_COMMAND. Once a PACKET_COMMAND is received, the result is stored in a %TEMP% file on the host. Finally, that result is exfiltrated to the C2 server using the above described PACKET_COMMAND method.

```
struct PACKET_HELLO { // XOR 0xF5 encrypted
    DWORD         command;       // set to 1002
    DWORD         unknown;       // hardcoded to 2004
    SYSTEM_INFO   system_info;   // same as in PACKET_HANDSHAKE
};
```

Figure 9: Sepulcher C2 PACKET_HELLO delivering malware mode command.

```
struct PACKET_COMMAND {
    DWORD    size;                // size of the COMMAND_DATA structure
    DWORD    command;             // refer to the Appendix B for a complete list of valid commands
    struct COMMAND_DATA {
        DWORD   unknown1;
        DWORD   unknown2;
        DWORD   unknown3;         // set to 0x10 in client->server packets
        DWORD   data_size;        // compressed data size
        DWORD   performance;      // time it took to complete the command
        DWORD   unknown4;
        WORD    pad_size;         // set to 3 in client->server packets
        byte    pad[pad_size];
        byte    data[data_size];  // LZW compressed data
    } data;
};
```

Figure 10: Sepulcher C2 PACKET_COMMAND to replay initial packet with mode command.

Conclusion

The adoption of COVID-19 lures by Chinese APT groups in espionage campaigns was a growing trend in the threat landscape during the first half of 2020. This was thought to be effective decoy fodder by threat actors as was observed in the WHO content that was coopted as part of the TA413 March 2020 campaign targeting European economic entities. However, following an initial urgency in intelligence collection around the health of western global economies in response to the COVID-19 pandemic, a return to normalcy was observed in both the targets and decoy content of TA413 campaigns. While the new Sepulcher malware is far from groundbreaking, its combination with timely social engineering lures masquerading as critical guidance from the WHO leveraged an urgent global crisis to entice victims. This campaign's specific focus on European economic, diplomatic, and legislative entities belies a possible momentary realignment for Chinese cyber espionage groups to collect information on global economies cast into upheaval as a result of COVID-19. However, in the case of TA413 that shift may have been short lived. The re-emergence of well-known Tibetan themed sender addresses and graphically

didactic PowerPoint attachments in later July again tie TA413 to its emblematic targeting of the Tibetan community. Despite the recurring use of publicly disclosed email addresses, a pedestrian RAT, and the recycling of delivery methods observed over a year ago, the targeting shift between these two campaigns paint a conspicuously contemporary portrait of a rapidly evolving cyber threat landscape in 2020.

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
4a4a959ae-f64ea48e2b831468119180d0af4b5b685c35170f5d-b3f001b9cc319	SHA256	Credential.dll Sepulcher Malware March 2020
f6f9224c389ee46b28fe04847de4afb1e33-ca03763c9e5c41bc61a29eab7f669	SHA256	OSEC234.tmp Sepulcher Malware Drc March 2020
tseringkanyaq@yahoo[.]com	Email Address	Sender Address First served 2013
107.151.194[.]197	IP	Command & Control
welfaretibet[.]tk	Domain	Domain Related by I March 2020
mediabureauin@gmail[.]com	Email Address	Sender Address First served 2019
ff301b3295959a3ac5f3d0a5ea0d9f0aedcd8-da7c4207b18f4bbb6ddaa0cdf22	SHA256	PowerPoint Attachme TIBETANS BEING HIT DEADLY VIRUS THAT RIES A GUN AND SPE CHINESE.ppsx
118.99.13[.]4	IP	Malware Delivery IP
hxxp://118.99.13[.]4:1234/qqqzqa	URL	URL

		C2 Communicatior
hxxp://118.99.13[.]4:8099/file.dll	URL	URL Delivery Resour Sepulcher Malware
e89614e3b0430d706bef2d1f13b30b43e5c53d-b9a477e2ff60ef5464e1e9add4	SHA256	File.dll | Credential.c Sepulcher Malware July 2020
Dalailamatrustindia.ddns[.]net	Domain	Command & Control Dc
115.126.6[.]16	IP	Hosting IP Dalailamatrustindia.ddns