

CYBER
THREAT
ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

CTA-CN-2020-0728



CHINESE STATE-SPONSORED
GROUP 'REDELTA' TARGETS
THE VATICAN AND CATHOLIC
ORGANIZATIONS



Insikt Group® researchers used proprietary Recorded Future Network Traffic Analysis and RAT controller detections, along with common analytical techniques, to identify and profile a cyberespionage campaign attributed to a suspected Chinese state-sponsored threat activity group, which we are tracking as RedDelta.

Data sources include the Recorded Future® Platform, Farsight Security's DNSDB, SecurityTrails, VirusTotal, Shodan, BinaryEdge, and common OSINT techniques.

This report will be of greatest interest to network defenders of private sector, public sector, and non-governmental organizations with a presence in Asia, as well as those interested in Chinese geopolitics.

Executive Summary

From early May 2020, The Vatican and the Catholic Diocese of Hong Kong were among several Catholic Church-related organizations that were targeted by RedDelta, a Chinese-state sponsored threat activity group tracked by Insikt Group. This series of suspected network intrusions also targeted the Hong Kong Study Mission to China and the Pontifical Institute for Foreign Missions (PIME), Italy. These organizations have not been publicly reported as targets of Chinese threat activity groups prior to this campaign.

These network intrusions occurred ahead of the anticipated September 2020 [renewal](#) of the landmark 2018 China-Vatican [provisional agreement](#), a deal which reportedly resulted in the Chinese Communist Party (CCP) gaining more control and oversight over the country's historically persecuted "underground" Catholic community. In addition to the Holy See itself, another likely target of the campaign includes the current head of the Hong Kong Study Mission to China, whose predecessor was considered to have played a vital role in the 2018 agreement.

The suspected intrusion into the Vatican would offer RedDelta insight into the negotiating position of the Holy See ahead of the deal's September 2020 renewal. The targeting of the Hong Kong Study Mission and its Catholic Diocese could also provide a valuable intelligence source for both monitoring the diocese's relations with the Vatican and its position on Hong Kong's pro-democracy movement amidst widespread protests and the recent [sweeping Hong Kong national security law](#).

While there is considerable overlap between the observed TTPs of RedDelta and the threat activity group publicly referred to as Mustang Panda (also known as BRONZE PRESIDENT and HoneyMyte), there are a few notable distinctions which lead us to designate this activity as RedDelta:

The version of PlugX used by RedDelta in this campaign uses a different C2 traffic encryption method and has a different configuration encryption mechanism than traditional PlugX.

The malware infection chain employed in this campaign has not been publicly reported as used by Mustang Panda.

In addition to the targeting of entities related to the Catholic Church, Insikt Group also identified RedDelta targeting law enforcement and government entities in India and a government organization in Indonesia.

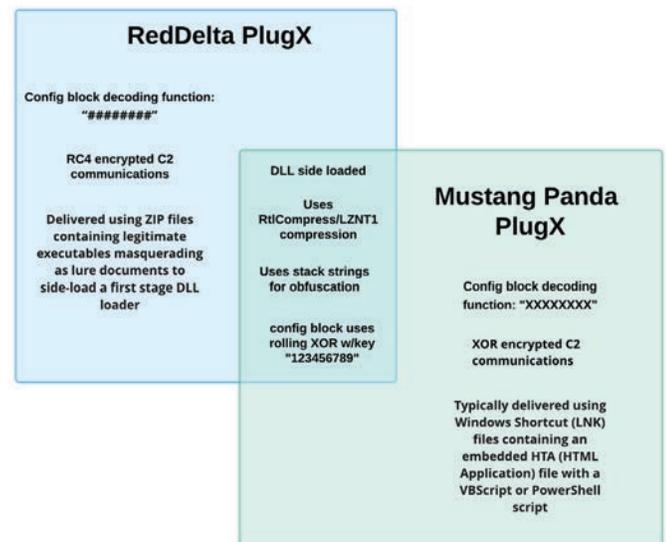


Figure 1: Selection of main differences between PlugX variants and the infection chain used by RedDelta and Mustang Panda.

Key Judgments

The targeting of entities related to the Catholic church is likely indicative of CCP objectives in consolidating control over the "underground" Catholic church, "sinicizing religions" in China, and diminishing the perceived influence of the Vatican within China's Catholic community.

Due to RedDelta's targeting of organizations that heavily align to Chinese strategic interests, use of shared tooling traditionally used by China-based groups, and overlaps with a suspected Chinese state-sponsored threat activity group, Insikt Group believes that the group likely operates on behalf of the People's Republic of China (PRC) government.

The identified RedDelta intrusions feature infrastructure, tooling, and victimology overlap with the threat activity group publicly reported as Mustang Panda (also known as BRONZE PRESIDENT and HoneyMyte). This includes the use of overlapping network infrastructure and similar victimology previously attributed to this group in public reporting, as well as using malware typically used by Mustang Panda, such as PlugX, Poison Ivy, and Cobalt Strike.

Background

China and the Catholic Church

For many years, Chinese state-sponsored groups have targeted religious minorities within the the PRC, particularly those within the so-called “Five Poisons,” such as Tibetan, Falun Gong, and Uighur muslim communities. Insikt Group has publicly reported on aspects of this activity, such as our findings on RedAlpha, the ext4 backdoor, and Scanbox watering hole campaigns targeting the Central Tibetan Administration, other Tibetan entities, and the Turkistan Islamic Party. Most recently, a July 2020 U.S. indictment identified the targeting of emails belonging to Chinese Christian religious figures — a Xi’an-based pastor, as well as an underground church pastor in Chengdu, the latter of whom was later arrested by the PRC government, by two contractors allegedly operating on behalf of the Chinese Ministry of State Security (MSS). Regional branches of China’s Ministry of Public Security (MPS) have also been heavily involved in digital surveillance of ethnic and religious minorities within the PRC, most notably by the Xinjiang Public Security Bureau (XPSB) in the case of Uighur muslims.

Historically, the PRC has had a highly turbulent relationship with the Vatican and its governing body, the Holy See. In particular, the Holy See’s recognition of bishops within China’s historically persecuted “underground” Catholic church traditionally loyal to the Vatican and its relationship with Taiwan has maintained an absence of official relations since the 1950s. The CCP perceived this behavior as the Holy See interfering in religious matters within China. In September 2018, the PRC and the Holy See reached a landmark two-year provisional agreement, marking a significant step towards renewed diplomatic relations.

Under the provisional agreement, China would regain more control over underground churches, and the Vatican in turn would gain increased influence over the appointment of bishops within the state-backed “official” Catholic church. The deal was met with a mixed reaction, with critics arguing that the deal was a betrayal of the underground church and would lead to increased persecution of its members. Many of the harshest criticisms came from clergy within Hong Kong. A year after the agreement, numerous reports noted the Vatican’s silence in response to the Hong Kong protests beginning in late 2019, in what critics called an effort to avoid offending Beijing and jeopardizing the 2018 agreement.

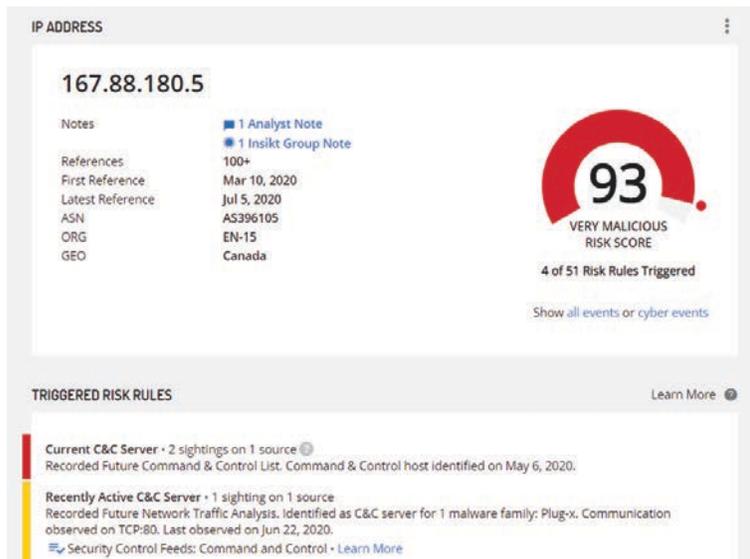


Figure 2: Intelligence Card for RedDelta PlugX C2 Server 167.88.180.[.]5.

Threat Analysis

Overview of Catholic Church Intrusions

Using Recorded Future RAT controller detections and network traffic analysis techniques, Insikt Group identified multiple PlugX C2 servers communicating with Vatican hosts from mid-May until at least July 21, 2020. Concurrently, we identified Poison Ivy and Cobalt Strike Beacon C2 infrastructure also communicating with Vatican hosts, a Vatican-themed phishing lure delivering PlugX, and the targeting of other entities associated with the Catholic Church.



From the Vatican, 14 May 2020

No. 491.189

Reverend Monsignor,

In reply to your Report No. 818/20 of 27 March 2020, I would ask you kindly to transmit the following message to the appropriate ecclesiastical authorities:

The Holy Father was saddened to learn of the death of Bishop Joseph Ma Zhongmu, and he sends heartfelt condolences to the clergy, religious and lay faithful of the Diocese of Yinchuan/Ningxia. Recalling with gratitude Bishop Ma Zhongmu’s years of priestly and episcopal ministry, especially his pastoral care for the ethnic Mongolian faithful, His Holiness commends his soul to our heavenly Father’s merciful love. To all who mourn the late Bishop’s passing, Pope Francis cordially imparts his Apostolic Blessing as a pledge of consolation and strength in the Risen Lord.

Cardinal Pietro Parolin
Secretary of State

With gratitude for your valued assistance, I remain

Yours sincerely in Christ,

[Signature]
* Edgar Peña Parra
Substitute

Monsignor Javier Corona Herrera
Study Mission
HONG KONG

Figure 3: Vatican lure document targeting the head of Hong Kong study mission to China.

The lure document shown above, which has been previously reported on in relation to links to Hong Kong Catholic Church targeting, was used to deliver a customized PlugX payload that communicated with the C2 domain systeminfor[.]com. The document purported to be an official Vatican letter addressed to the current head of the Hong Kong Study Mission to China. It is currently unclear whether the actors created the document themselves, or whether it is a legitimate document they were able to obtain and weaponize. Given that the letter was directly addressed to this individual, it is likely that he was the target of a spearphishing attempt. Additionally, as this sample was compiled after signs of an intrusion within the Vatican network, it is also possible that the phishing lure was sent through a compromised Vatican account. This hypothesis is supported by the identification of communications between PlugX C2s and a Vatican mail server in the days surrounding the sample’s compilation date and its first submission to public malware repositories.

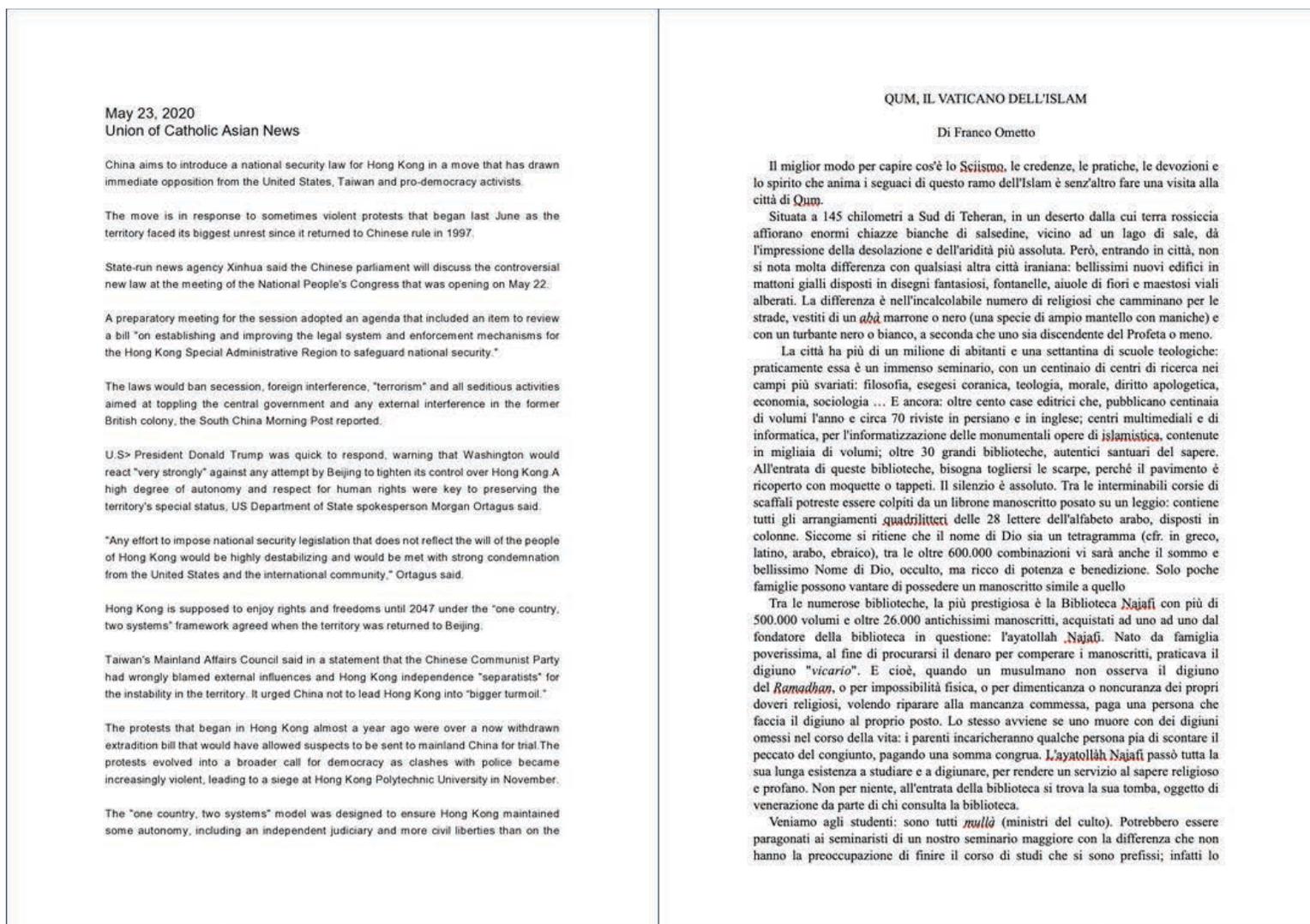


Figure 4: Union of Catholic Asian News article lure document (left), and Qum, the Vatican of Islam lure document (right).

The head of the Hong Kong Study Mission is considered the Pope's de facto representative to China and a key link between Beijing and the Vatican. The predecessor to this role played a key part in the finalization of the 2018 provisional China-Vatican agreement, making his successor a valuable target for intelligence gathering ahead of the deal's expiry and likely [renewal](#) in September 2020.

Further entities associated with the Catholic Church were also targeted by RedDelta in June and July 2020 using PlugX, including the mail servers of an international missionary center based in Italy and the Catholic Diocese of Hong Kong.

Insikt Group identified two additional phishing lures loading the same customized PlugX variant, which both communicated with the same C2 infrastructure as the Vatican lure. The first sample included a lure document spoofing a news bulletin from the Union of Catholic Asian News regarding the impending introduction of the new Hong Kong national security law. The content of the lure file, titled "About China's plan for Hong Kong security law.doc," was taken from a legitimate Union of Catholic Asian News [article](#). The other sample also references the Vatican using a document titled "QUM, IL VATICANO DELL'ISLAM.doc" for the decoy document. This particular decoy document translates as "Qum, the Vatican of Islam," referring to the Iranian city of Qum (Qom), an important Shi'ite political and religious center. It is taken from the writings of Franco Ometto,

a Italian Catholic academic living in Iran. Although the direct target of these two lures are unclear, both relate to the Catholic church.

We believe that this targeting is indicative of both China's objective in consolidating increased control over the underground Catholic Church within China, and diminishing the perceived influence of the Vatican on Chinese Catholics. Similarly, a focus on Hong Kong Catholics amid pro-democracy protests and the recent sweeping national security law is in line with Chinese strategic interests, particularly given the Anti-Beijing [stance](#) of many of its members, including former Hong Kong Bishop [Cardinal Joseph Zen Ze-kiun](#).

Other Targeted Organizations

Insikt Group identified several additional suspected victims communicating with RedDelta C2 infrastructure. While metadata alone does not confirm a compromise, the high volume and repeated communications from hosts within targeted organizations to these C2s are sufficient to indicate a suspected intrusion. A full list of identified targeted organizations are summarized below:

Targeted Organization	Sector	Country/Region of Operation	Date of Observed Activity	RedDelta C2 IP(s)
The Vatican/Holy See	Religious	The Vatican	May 21–July 21, 2020	85.209.43[.]21, 103.85.24[.]136, 103.85.24[.]149, 103.85.24[.]190, 154.213.21[.]170, 154.213.21[.]173, 154.213.21[.]207, 167.88.180[.]15, 167.88.180[.]32,
Catholic Diocese of Hong Kong	Religious	Hong Kong	May 12–July 21, 2020	103.85.24[.]136, 167.88.180[.]15, 167.88.180[.]32,
Pontifical Institute for Foreign Missions (PIME), Milan	Religious	Italy	June 2–26 2020	85.209.43[.]21,
Sardar Vallabhbhai Patel National Police Academy	Law Enforcement	India	February 16–June 25, 2020	103.85.24[.]136, 167.88.180[.]15,
Ministry of Home Affairs (Kementerian Dalam Negeri Republik Indonesia)	Government	Indonesia	May 21–July 21, 2020	85.209.43[.]21,
Airports Authority of India	Government	India	June 18–July 21, 2020	154.213.21[.]207,
Other Unidentified Victims	N/A	Myanmar, Hong Kong, Ethiopia, Australia	May–July 2020	85.209.43[.]21, 103.85.24[.]136, 167.88.180[.]15,

Table 1: List of organizations targeted by RedDelta.

The organizations targeted by RedDelta in this campaign largely align with historical activity publicly reported on the threat activity group Mustang Panda, with the group previously linked to intrusion attempts targeting the [Police of the Sindh Province in Pakistan](#), [law enforcement organizations in India](#), and the targeting of entities within [Myanmar](#), [Hong Kong](#), and [Ethiopia](#). The group is also suspected to have [previously targeted](#) China Center (China Zentrum e.V), a non-profit organization whose members includes Catholic aid organizations, religious orders and dioceses in Germany, Austria, Switzerland, and Italy, and other organizations associated with religious and minority groups.

Infrastructure Analysis

In this campaign, RedDelta favored three primary IP hosting providers, and used multiple C2 servers within the same /24 CIDR ranges across intrusions. Preferred hosting providers included 2EZ Network Inc (Canada), Hong Kong Wen Jing Network Limited, and Hong Kong Ai Jia Su Network Limited. The group consistently registered domains through GoDaddy, with WHOIS data providing additional linkages between domains used by the threat activity group. Insikt Group identified two primary clusters of RedDelta infrastructure used throughout this campaign, referred to as the “PlugX cluster” and the “Poison Ivy and Cobalt Strike cluster.” A Maltego chart is included below displaying these clusters.

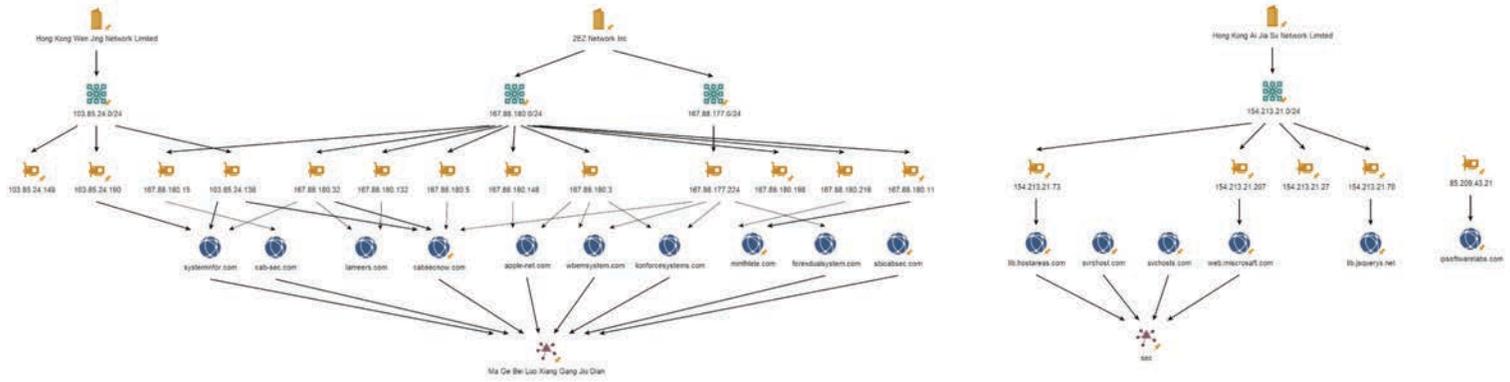


Figure 5: Maltego chart of RedDelta infrastructure.

'Ma Ge Bei Luo Xiang Gang Jiu Dian' and the PlugX Cluster

Vatican hosts and several other victim organizations were communicating with the PlugX C2 167.88.180[.]15 from May until June 10, 2020. This IP hosted the domain cabsecnow[.]com over this time period. Cabsecnow[.]com then resolved to a new IP, 103.85.24[.]136, from June 10 onwards. The suspicious network activity continued after the C2 IP was updated, increasing our confidence in the likelihood of intrusion at the targeted organizations.

The cabsecnow[.]com domain shares a similar naming convention to a publicly reported domain linked to Mustang Panda, cab-sec[.]com. WHOIS data revealed that both domains were registered several seconds apart through GoDaddy on September 17, 2019, with the same registrant organization listed: "Ma Ge Bei Luo Xiang Gang Jiu Dian." This registrant organization is associated with eight domains in total, five of which have previously been publicly linked to Mustang Panda activity by Anomali and Dell SecureWorks. "Ma Ge Bei Luo Xiang Gang Jiu Dian" translates from Mandarin to Marco Polo Hotel Hong Kong, a legitimate Hong Kong hotel, although it is unclear why the actor chose this organization when registering these domains.

Domain	Registration Timestamps
sbicabsec[.]com	November 26, 2019 10:31:18Z
systeminfor[.]com	November 19, 2019 07:06:03Z
cabsecnow[.]com	September 17, 2019 02:37:37Z
cab-sec[.]com	September 17, 2019 02:37:34Z
forexdualsystem[.]com	October 22, 2018 01:09:46Z*
lionforcesystems[.]com	October 22, 2018 01:09:45Z*
apple-net[.]com	October 22, 2018 01:09:46Z*
wbemsystem[.]com	October 17, 2018 06:51:02Z*

Table 2: Domains with "Ma Ge Bei Luo Xiang Gang Jiu Dian" registrant organization. (*Domains now re-registered)

Another PlugX C2, 85.209.43[.]21, was also identified communicating with several hosts within the same targeted organizations (see Table 1). This IP has hosted ipsoftwarelabs[.]com since November 2019, a domain previously identified as a Mustang Panda PlugX C2.

Finally, the C2 domain associated with the Vatican and Union of Catholic Asian News lures, systeminfor[.]com, was hosted on 167.88.180[.]32 since June 2020. This IP has also hosted lameers[.]com since February 2020, another PlugX C2 identified in activity targeting Hong Kong.

Figure 6: Context panel from the Recorded Future Intelligence Card™ for ipsoftwarelabs[.]com.

Cobalt Strike/Poison Ivy Cluster

Associated Domain	C2 IP Address	Malware Variant
web.microsoft[.]com	154.213.21[.]207	Poison Ivy
lib.jsquers[.]net	154.213.21[.]70	Cobalt Strike
lib.hostareas[.]com	154.213.21[.]73	Unknown

Table 3: Cobalt Strike/Poison Ivy cluster domains.

The second cluster featured Cobalt Strike and Poison Ivy malware C2 infrastructure. A Poison Ivy sample (SHA256:9bac74c592a36ee249d6e0b086bfab395a37537ec87c2095f999c00b946ae81d) submitted to a public malware repository from Italy in early June 2020, several days after the first evidence of activity between Vatican hosts and this C2, was configured to communicate with a spoofed Microsoft domain, web.microsoft[.]com, hosted on 154.213.21[.]207. Suspicious network traffic between this Poison Ivy C2 and several Vatican hosts, as well as an Indian aviation entity, were observed by Insikt Group analysts.

Two other IP addresses within the same 24-bit CIDR range, 154.213.21[.]73 and 154.213.21[.]70, were also identified communicating with overlapping Vatican infrastructure at this time. A Cobalt Strike sample (SHA256:7824eb5f173c43574593bd3afab41a60e0e2ffae80201a9b884721b451e6d935), uploaded from an Italian IP address to a malware multiscanner repository as a zipped file the same day as the Poison Ivy sample, also used the 154.213.21[.]70 IP for command and control.

This cluster of activity does not overlap with the infrastructure identified in the PlugX cluster. The WHOIS registration data for the domains miscrosoft[.]com and hostareas[.]com contains the registrant organization “sec.” While less distinct than the “Ma Ge Bei Luo Xiang Gang Jiu Dian” registrant identified earlier in the PlugX cluster, there are still relatively few domains associated with this organization, and fewer still that were registered through GoDaddy. Using these characteristics, we identified that the domains svrhosts[.]com, strust[.]club, and svchosts[.]com all match this criteria and are previously reported Mustang Panda Cobalt Strike C2 [domains](#). In particular, svrhosts[.]com and svchosts[.]com were both registered at the same time as hostareas[.]com on February 3, 2019 through GoDaddy.

Malware Analysis

While there is notable targeting and infrastructure overlap between this RedDelta campaign and publicly reported Mustang Panda activity, there are some deviations in tactics, techniques, and procedures (TTPs) used in both. For instance, Mustang Panda has typically [used](#) Windows Shortcut (LNK) files containing an embedded HTA (HTML Application) file with a VBScript or PowerShell script to load PlugX and Cobalt Strike Beacon payloads. However, in this campaign, RedDelta used ZIP files containing legitimate executables masquerading as lure documents, a notable departure from Mustang Panda activity that has been publicly reported previously. This legitimate executable is used to load a malicious DLL also present within the ZIP file through DLL sideloading, before the target is shown a decoy document. While Mustang Panda have used DLL sideloading previously, the PlugX variant used in association with this campaign has key differences from more traditional PlugX variants, particularly in the C2 protocol used and the configuration encoding within the samples, leading us to refer to it as the “RedDelta PlugX” variant below — however, this is not intended to suggest that this variant is used exclusively by this group and is in reference to the first group we have seen using this variant.

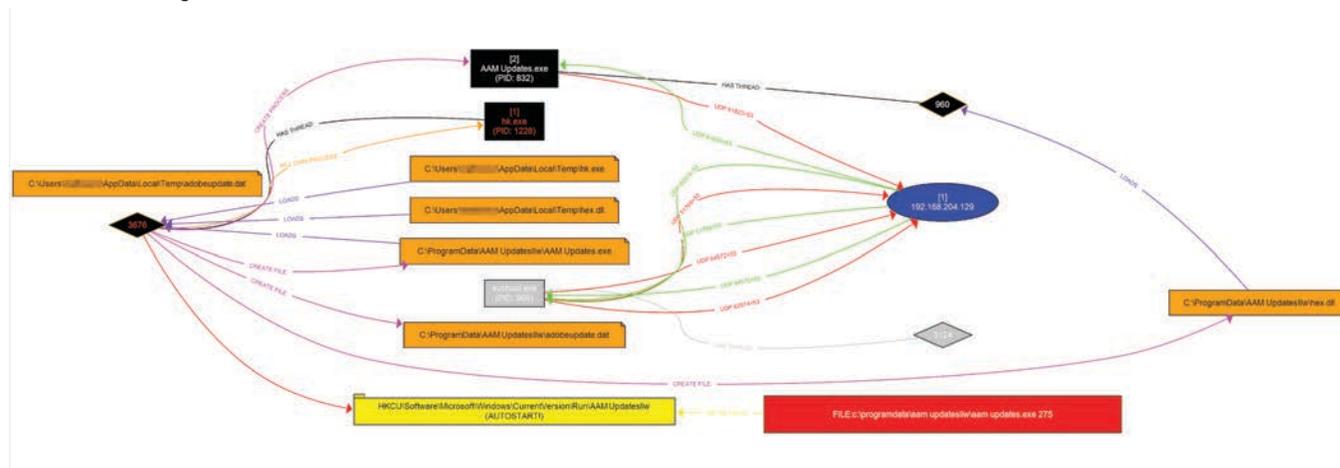


Figure 7: Execution diagram of the malware associated with RedDelta PlugX.

RedDelta PlugX: ‘Hong Kong Security Law’ Lure

The first sample, titled “About China’s plan for Hong Kong security law.zip” (SHA256:86590f80b4e1608d0367a7943468304f7eb665c9195c24996281b1a958bc1512), corresponds to the Union of Catholic Asian News lure delivering the RedDelta PlugX variant. Although Insikt Group does not have full visibility into this infection chain, the ZIP file is likely to have been delivered via a spearphishing email. The ZIP contains two files:

File Name	About China’s plan for Hong Kong security law.exe
SHA256 Hash	6c959cfb001fbb900958441dfd8b262fb33e052342948bab338775d3e83ef7f7 Hash

File Name	wwlib.dll
SHA256 Hash	f6e5a3a32fb3aaf3f2c56ee482998b09a6ced0a60c38088e7153f3ca247ab1cc Hash

Stage 1: Wwlib.dll DLL Sideload and Hk.dat Download and Execution

“About China’s plan for Hong Kong security law.exe” is a legitimate Windows loader for Microsoft Word that is vulnerable to sideloading. When executed, it sideloads the malicious DLL, “wwlib.dll.”

Wwlib.dll initializes the loading stage by downloading, decoding, and executing an XOR-encoded Windows executable file, hk.dat, from http://167.88.180[.]198/hk.dat. Next, wwlib.dll will extract a Word document, “About China’s plan for Hong Kong security law.docx” from its resource section and open it to make it appear to the user that a legitimate Microsoft Word document was opened.

Stage 2: Hk.exe/AAM Updates.exe DLL Sideloading to Load PlugX Variant

After “hk.dat” is decoded and executed, it will create three files in the C:\%APPDATA%\local\temp directory:

- Hk.exe (SHA256: 0459e62c5444896d5be404c559c834ba455fa5cae1689c70fc8c61bc15468681) - A legitimate Adobe executable that is vulnerable to DLL sideloading

- Hex.dll (SHA256: bc6c2fda18f8ee36930b469f6500e28096eb6795e5fd17c44273c67bc9fa6a6d) - The malicious DLL sideloaded by hk.exe that decodes and loads adobeupdate.dat
- Adobeupdate.dat (SHA256: 01c1fd0e5b8b7bbed62bc8a6f7c9ceff1725d4ff6ee86fa813bf6e70b079812f) - The RedDelta PlugX variant loader

Next, “hk.exe” is executed and creates copies of the files “adobeupdate.dat,” “hex.dll,” and itself renamed as “AAM Updates.exe” in the folder “C:\ProgramData\AAM Updates\.” “AAM Updates.exe” is then executed, starting the installation process by sideloading the malicious “hex.dll.” “Hex.dll” will decode and execute “adobeupdate.dat,” which ultimately leads to the execution of the RedDelta PlugX variant in memory. This use of DLL sideloading, including the use of this specific Adobe executable, aligns with recent public reporting of Mustang Panda PlugX use ([1](#), [2](#)).

RedDelta PlugX: ‘Qum, the Vatican of Islam’ Lure

The second PlugX sample uses the same loading method identified above. In this case, the same WINWORD.exe executable is used to load another malicious wplib.dll file. The sample then contacts [http://103.85.24\[.\]190/qum.dat](http://103.85.24[.]190/qum.dat) to retrieve the XOR-encoded Windows executable file, qum.dat. This sample uses the same C2 as above, [www.systeminfor\[.\]com](http://www.systeminfor[.]com).

RedDelta PlugX: Vatican Lure Targeting Hong Kong Study Mission

The final PlugX sample featuring the Vatican Hong Kong Study Mission lure also uses largely the same PlugX loading method. In this case, the ZIP file contains a benign Adobe Reader executable, AcroRd32.exe, renamed “DOC-2020-05-15T092742.441.exe,” which is used to load the malicious acroRd32.dll file through DLL sideloading. In this case the sample retrieves the file dis.dat from [http://167.88.180\[.\]198/dis.dat](http://167.88.180[.]198/dis.dat) and uses the same C2 referenced in the previous samples.

RedDelta PlugX: Installation Process

Insikt Group performed detailed analysis on the DAT files related to the “Union of Catholic Asian News” and “Qum, the Vatican of Islam” lure. Analysis of these samples showed two DAT files were downloaded from the URLs listed in the table below:

File Name	Download Location	SHA256 Hash
hk.dat	http://167.88.180[.]198/hk.dat	2fb4a17ece461ade1a2b63bb8db19947636c6ae39c4c674fb4b7d4f90275d20
qum.dat	http://103.85.24[.]190/qum.dat	476f80521bf6789d02f475f67e0f4ede830c4a700c3f7f64d99e811835a39e

In each case, the file (“hk.dat” or “qum.dat”) is downloaded and executed after initial execution of the phishing lure, as described above in “Stage 1: Wplib.dll DLL Sideload and Hk.dat Download and Execution.” Both files are RtlCompress/LZNT1 compressed, as well as XOR-encoded. The XOR key precedes the encoded data, allowing the file to be more easily decoded during static analysis. A Python script to decompress and decode the payload can be found on our [GitHub repository](#).

After the DAT files are decompressed and decoded, they are executed. The execution details for “hk.dat” have been detailed above (see: “Stage 2: Hk.exe/AAM

Updates.exe DLL Sideload to Load PlugX Variant”) and are nearly identical to that of “qum.dat.” As with the hk.dat sample associated with the “Union of Catholic Asian News” lure, the main purpose of this stage of the malware is to perform the DLL sideloading step in order to execute the PlugX variant.

Again, the final stage consists of three files: a non-malicious executable, a malicious sideloaded DLL, and the encoded DAT file which are all used to sideload the final payload. This is consistent with a typical PlugX installation.

Like the first-stage DAT files, the PlugX loaderDAT file is XOR-encoded and the decode key precedes the encoded data in the file; however, they are not RtlCompress/LZNT1 compressed as the initial stage files are. A Python script to decode the PlugX loader, as well as the configuration block, is contained on our [GitHub repository](#).

RedDelta: An Updated PlugX Variant

The PlugX variant used in the RedDelta campaign is similar to the PlugX variants previously associated with Mustang Panda by [Avira](#) and [Anomali](#). Both make heavy use of stack strings as an obfuscation mechanism, as seen in Figure 8, making it harder for an analyst to use strings to determine the functionality or purpose of the code.



Mustang Panda PlugX Variant

RedDelta PlugX Variant

Figure 8: Comparison of Anomali/Avira PlugX variant stack string implementation and RedDelta stack string implementation.

However, the configuration block for the RedDelta PlugX variant has one key distinction: the [Avira-reported](#) Mustang Panda configuration block decoding function looks for the string "XXXXXXX" to determine whether the configuration is encoded, while the RedDelta variant looks for the string "#####". Apart from the different demarcator strings, both variants use the same rolling XOR encoding with the key "123456789." The configuration block decode routine can be seen in Figure 9, below.



Mustang Panda PlugX Variant

RedDelta PlugX Variant

Figure 9: Comparison of configuration block in Anomali/Avira PlugX (showing the “XXXXXXXX” demarcator) and the RedDelta configuration block (showing the “#####” demarcator).

A Python implementation of this algorithm can be observed in Figure 10, below.

```
def configDecode(configBlock):
    decoded=[]
    if configBlock[0:7] != "#####":
        key = [0x31,0x32,0x33,0x34,0x35,0x36,0x37,0x38,0x39]
        klen = len(key)

        loop_condition = 0
        for c in configBlock:
            current_key = key[loop_condition % klen]
            decoded.append(c ^ current_key)
            loop_condition += 1
```

Figure 10: Python implementation of RedDelta PlugX configuration block decoding mechanism.

In conventional PlugX samples, the configuration block is encrypted with a more complex algorithm using multiple keys in combination with shift left and shift right bitwise operations. For example, the Python code implementing this algorithm, as seen in Figure 11, was created by [Kyle Creyts](#) based on Takahiro Haruyama’s extensive research and analysis on PlugX.

```
def decrypt(key, src, size):
    key0 = key
    key1 = key
    key2 = key
    key3 = key
    dst = b''
    i = 0
    if size > 0:
        while i < size:
            key0 = (key0 + (((key0 >> 3) & 0xFFFFFFFF) - 0x11111111) & 0xFFFFFFFF) & 0xFFFFFFFF
            key1 = (key1 + (((key1 >> 5) & 0xFFFFFFFF) - 0x22222222) & 0xFFFFFFFF) & 0xFFFFFFFF
            key2 = (key2 + (0x44444444 - ((key2 << 9) & 0xFFFFFFFF)) & 0xFFFFFFFF) & 0xFFFFFFFF
            key3 = (key3 + (0x33333333 - ((key3 << 7) & 0xFFFFFFFF)) & 0xFFFFFFFF) & 0xFFFFFFFF
            new_key = (((key2 & 0xFF) + (key3 & 0xFF) + (key1 & 0xFF) + (key0 & 0xFF)) & 0xFF)
            res = unpack("<B", src[1:i+1])[0] ^ new_key
            dst += pack("<B", res)
            i = i + 1
    return dst
```

Figure 11: Python implementation of traditional PlugX configuration block decoding mechanism by Kyle Creyts.

The configuration block encryption associated with the RedDelta variant is considerably less sophisticated when compared to traditional PlugX samples, and while both make use of XOR-based ciphers, the simple algorithm used by RedDelta would be easier to brute force by an analyst.

Command and Control Protocol

The C2 protocol used for the RedDelta PlugX malware differs from the Mustang Panda PlugX. While both variants use the HTTP POST method common to PlugX including the number of "61456" in the POST header field which is a clear indicator of a PlugX HTTP POST. However, the RedDelta variant does not include the URI string "/update?wd=" more commonly associated with PlugX, as seen in Figure 12.

<pre>POST /update?wd=5ec5a030 HTTP/1.1 Accept: */* x-debug: 0 x-request: 0 x-content: 61456 x-storage: 1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1; Host: 185.239.226.61:965 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache</pre>	<pre>POST /11331352 HTTP/1.1 Accept: */* jsp-se: 0 jsp-st: 0 jsp-si: 61456 jsp-sn: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0;Win64;x64)AppleWebKit/537.36 Host: www.systeminfor.com Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache</pre>
---	---

Mustang Panda PlugX Variant

RedDelta PlugX Variant

Figure 12: HTTP POST request from Anomali/Avira PlugX variant and RedDelta PlugX variant.

The RedDelta PlugX variant encrypts its C2 communications very differently when compared to the Mustang Panda variant reported by Anomali and Avira. Instead of using XOR encoding, RedDelta uses RC4 encryption where the first 10 bytes of the passcode are hardcoded and the last four bytes are randomly generated and included as a key within the TCP packet so that the communication can be decrypted. The hardcoded portion of the RC4 passphrase is "ln&U*O%Pb\$." Figure 13 shows the function where the RC4 passphrase is defined as well as where the last four bytes are appended to create the full key. A Python script to decode the RedDelta C2 communication from a supplied PCAP can be found on our [GitHub repository](#).

Despite the different C2 encryption schemes, both RedDelta and Mustang Panda variants' C2 traffic decrypts to the familiar PlugX header format, as shown in Figure 14.

Encrypted PlugX Header and Data

```
e1 31 75 3d 9b 09 83 12 63 7b 46 29 46 86 65 73 d6 2e 8c 9e 5c cb 58 20 47 3f c7 29 4a 08 b5 2b 5e 39 16 6a
```

Decrypted PlugX Header

```
26 af f9 7d 00 10 00 00 14 00 10 00 00 00 00 11 bo 00 de c7 d2 db 32 30 44 91 00 cc 6d c6 6d e8 65 0d f2
```

XOR Key

```
26 af f9 7d
```

Flags

```
00 10 00 00
```

SIZE OF COMPRESSED DATA

```
14 00
```

SIZE OF DECOMPRESSED DATA

```
10 00
```

Unknown

```
00 00 00 00
```

Data

```
11 bo 00 de c7 d2 db 32 30 44 91 00 cc 6d c6 6d e8 65 0d f2
```

Figure 14: PlugX header and data.

In conventional PlugX samples, the C2 uses the same algorithm as in the configuration decode (see Figure 11), with part of the key being the first four bytes of the TCP transmission. While the RedDelta PlugX variant also uses the first four bytes of the TCP transmission as a part of the key, the use of RC4 for C2 encryption demonstrates a departure from the usual PlugX C2 traffic encryption mechanism.

```
003DA5E8 C2_Encrypt_Decrypt proc near
003DA5E8
003DA5E8 var_10= byte ptr -10h
003DA5E8 var_F= byte ptr -0Fh
003DA5E8 var_E= byte ptr -0Eh
003DA5E8 var_D= byte ptr -0Dh
003DA5E8 var_C= byte ptr -0Ch
003DA5E8 var_B= byte ptr -0Bh
003DA5E8 var_A= byte ptr -0Ah
003DA5E8 var_9= byte ptr -9
003DA5E8 var_8= byte ptr -8
003DA5E8 var_7= byte ptr -7
003DA5E8 var_6= dword ptr -6
003DA5E8 var_2= byte ptr -2
003DA5E8 arg_0= dword ptr 8
003DA5E8 arg_4= dword ptr 0Ch
003DA5E8 arg_8= dword ptr 10h
003DA5E8 arg_C= dword ptr 14h
003DA5E8
003DA5E8 push ebp
003DA5E9 mov ebp, esp
003DA5EB sub esp, 10h
003DA5EE mov [ebp+var_10], 21h ; '!'
003DA5F2 mov [ebp+var_F], 6Eh ; 'n'
003DA5F6 mov [ebp+var_E], 26h ; '&'
003DA5FA mov [ebp+var_D], 55h ; 'U'
003DA5FE mov [ebp+var_C], 2Ah ; '*'
003DA602 mov [ebp+var_B], 4Fh ; 'O'
003DA606 mov [ebp+var_A], 25h ; '%'
003DA60A mov [ebp+var_9], 50h ; 'P'
003DA60E mov [ebp+var_8], 62h ; 'b'
003DA612 mov [ebp+var_7], 24h ; '$'
003DA616 mov byte ptr [ebp+var_6], 64h ; 'd'
003DA61A mov byte ptr [ebp+var_6+1], 37h ; '7'
003DA61E mov byte ptr [ebp+var_6+2], 61h ; 'a'
003DA622 mov byte ptr [ebp+var_6+3], 38h ; '8'
003DA626 mov [ebp+var_2], 0
003DA62A mov eax, [ebp+arg_C]
003DA62D mov [ebp+var_6], eax
003DA630 lea ecx, [ebp+var_10]
003DA633 push ecx ; char *
003DA634 mov edx, [ebp+arg_8]
003DA637 push edx ; int
003DA638 mov eax, [ebp+arg_4]
003DA63B push eax ; int
003DA63C mov ecx, [ebp+arg_0]
003DA63F push ecx ; int
003DA640 call RC4Main
003DA645 add esp, 10h
003DA648 xor eax, eax
003DA64A mov esp, ebp
003DA64C pop ebp
003DA64D retn
003DA64D C2_Encrypt_Decrypt endp
```

Figure 13: C2 encryption/decryption routine showing the first four hardcoded bytes of the RC4 key used in RedDelta PlugX variant.

While Recorded Future has not done extensive code analysis to further compare the samples, we have highlighted fundamental differences between the RedDelta PlugX variants and conventional PlugX, notably in the configuration block and C2 communication. Additionally, while RedDelta has implemented a modular delivery system based on traditional PlugX tactics, it also provides the group with the ability to change, enhance or remove functionality as needed.

File Name	OneDrive.exe
SHA256 Hash	7824eb5f173c43574593bd3afab41a60e0e2ffae80201a9b884721b451e6d935

Cobalt Strike

The file, OneDrive.exe, is responsible for loading the Cobalt Strike payload. When executed, OneDrive will reach out to [http://154.213.21\[.\]27/DotNetLoader40.exe](http://154.213.21[.]27/DotNetLoader40.exe), download the file DotNetLoader40.exe and invoke the "RunRemoteCode" function contained within it.

DotNetLoader40.exe is a small .NET executable that essentially downloads and then executes shellcode. The main function in DotNetLoader is "RunRemoteCode" which takes a URL as an argument. The content is downloaded from the provided URL, in this case, [http://154.213.21\[.\]27/beacon.txt](http://154.213.21[.]27/beacon.txt), and then sent to the function "InjectShellCode." The shellcode is then base64 decoded, decompressed, saved to memory, and executed.

The shellcode loaded is Cobalt Strike Beacon, which is configured using the Havex Malleable C2 profile. This Havex C2 code has been [published on GitHub](#) and can be used by any entity that wishes to use it; and in this case, the attacker is doing so in conjunction with Cobalt Strike. This can be seen both through the URI used within the C2 URL ([http://154.213.21\[.\]70/wp08/wp-includes/dtcla.php](http://154.213.21[.]70/wp08/wp-includes/dtcla.php)) and the client and server headers and HTML content displayed below in Figure 15.

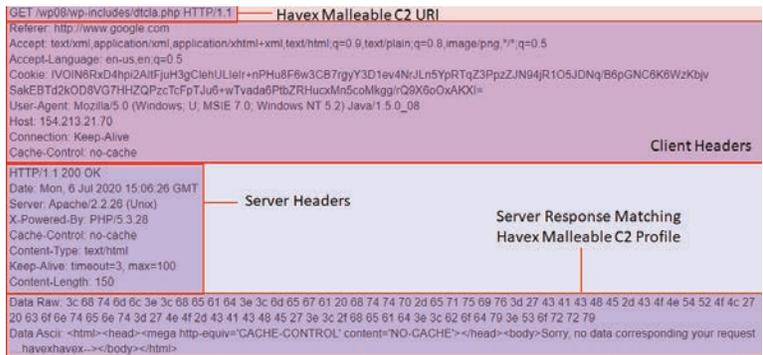


Figure 15: Network connections and server response to Cobalt Strike Beacon Havex Malleable C2 sample.

Poison Ivy

File Name	MpSvc.dll
SHA256 Hash	9bac74c592a36ee249d6e0b086bfab395a37537ec87c2095f999c00b946ae81d

The identified Poison Ivy sample is loaded using the above MpSvc.dll file, masquerading as the Microsoft Windows Defender file of the same name. Once loaded, [web.microsoft\[.\]com](http://web.microsoft[.]com) is used for command and control.

Outlook

Our research uncovered a suspected China state-sponsored campaign targeting multiple high-profile entities associated with the Catholic Church ahead of the likely renewal of the provisional China-Vatican deal in September 2020. The CCP's warming diplomatic relations with the Holy See has been commonly interpreted as a means to facilitate increased oversight and control over its unofficial Catholic church. This also supports the CCP's wider [stated goal](#) of "sinicizing religions" in China. Furthermore, it demonstrates that China's interest in control and surveillance of religious minorities is not confined to those within the "Five Poisons," exemplified by the [continued persecution](#) and detainment of underground church members and [allegations](#) of physical surveillance of official Catholic and Protestant churches.

The U.S. Ambassador-at-Large for International Religious Freedom recently [expressed](#) concern regarding the impact of the new national security law within Hong Kong, stating it has the "potential to significantly undermine religious freedom." The targeting of the Catholic diocese of Hong Kong is likely a valuable intelligence source for both monitoring the diocese's position on Hong Kong's pro-democracy movement and its relations with the Vatican. This marks a possible precursor to increased limits on religious freedom within the special administrative region, particularly where it coincides with pro-democracy or anti-Beijing positions.

RedDelta is a highly active threat activity group targeting entities relevant to Chinese strategic interests. Despite the group's consistent use of well-known tools such as PlugX and Cobalt Strike, infrastructure reuse, and operations security failures, these intrusions indicate RedDelta is still being tasked to satisfy intelligence requirements. In particular, this campaign demonstrates a clear objective to target religious bodies, and therefore we feel this is particularly pertinent for religious and non-governmental organizations (NGOs) to take note and invest in network defenses to counter the threat posed by Chinese state-sponsored threat activity groups like RedDelta. A lack of ability to invest in security and detection measures for many NGOs and religious organizations greatly increases the likelihood of success for well-resourced and persistent groups, even using well-documented tools, TTPs, and infrastructure.

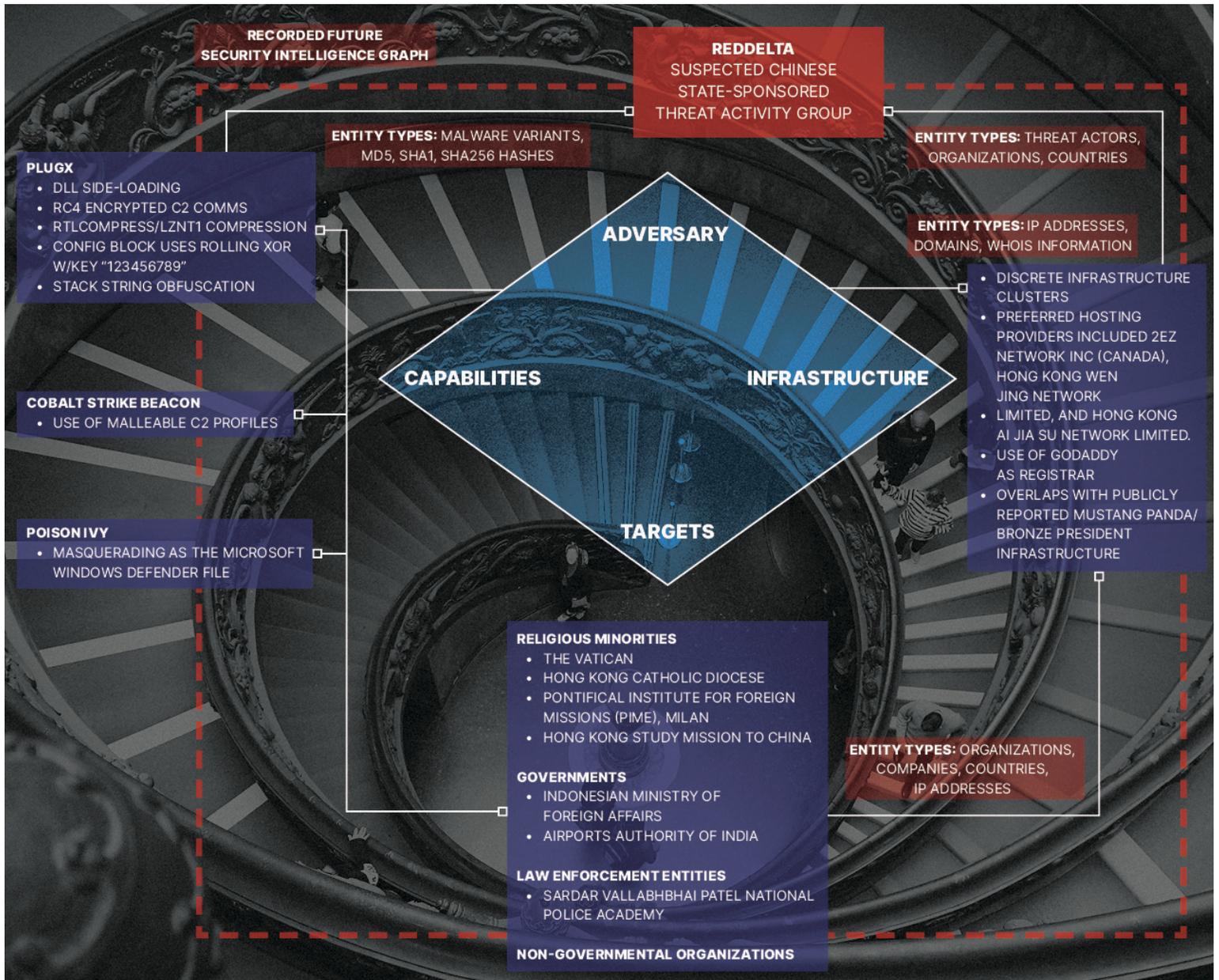
Network Defense Recommendations

Recorded Future recommends that users conduct the following measures to detect and mitigate activity associated with RedDelta activity:

- 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 illicit connection attempts from — the external IP addresses and domains listed in the appendix.

Additionally, we advise organizations to follow the following general information security best practice guidelines:

- Keep all software and applications up to date; in particular, operating systems, antivirus software, and core system utilities.
- Filter email correspondence and scrutinize attachments for malware.
- Make regular backups of your system and store the backups offline, preferably offsite so that data cannot be accessed via the network.
- Have a well-thought-out incident response and communications plan.
- Adhere to strict compartmentalization of company-sensitive data. In particular, look at which data anyone with access to an employee account or device would have access to (for example, through device or account takeover via phishing).
- Strongly consider instituting role-based access, limiting company-wide data access, and restricting access to sensitive data.
- Employ host-based controls; one of the best defenses and warning signals to thwart attacks is to conduct client-based host logging and intrusion detection capabilities.
- Implement basic incident response and detection deployments and controls like network IDS, netflow collection, host logging, and web proxy, alongside human monitoring of detection sources.
- Be aware of partner or supply chain security standards. Being able to monitor and enforce security standards for ecosystem partners is an important part of any organization's security posture.



Recorded Future Threat Activity Group and Malware Taxonomy

Recorded Future’s research group, Insikt, tracks threat actors and their activity, focusing on state actors from China, Iran, Russia, and North Korea, as well as cyber criminals - individuals and groups - from Russia, CIS states, China, Iran, and Brazil. We emphasize tracking activity groups and where possible, attributing them to nation state government, organizations, or affiliate institutions.

Our coverage includes:

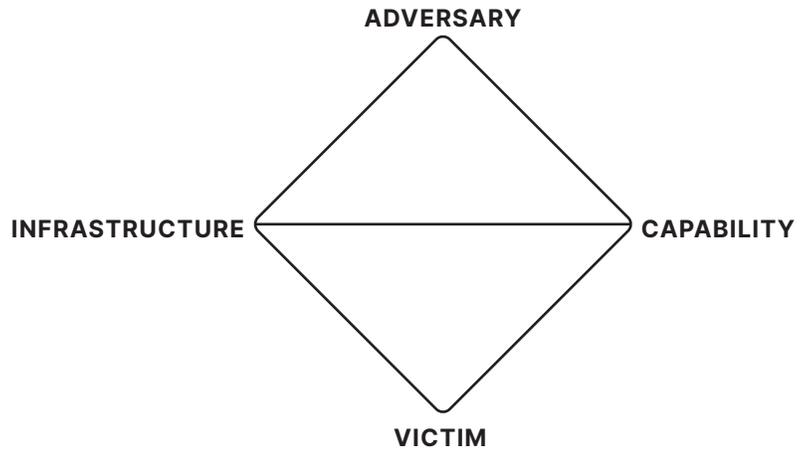
- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors.
- Recorded Future-identified, suspected nation state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other industry established groups.
- Cybercriminal individuals and groups established and named by Recorded Future
- Newly emerging malware, as well as prolific,persistent commodity malware

Insikt Group names a new threat activity group or campaign when analysts have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence, derived from our Security Intelligence Graph. We can tie this to a threat actor only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely-utilized or recognized name for a particular group when the public body of empirical evidence is clear the activity corresponds to a known group.

Insikt Group utilizes a simple color and phonetic alphabet naming convention for new nation state threat actor groups or campaigns. The color corresponds to that nation’s flag colors, currently represented below, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.

For newly identified cybercriminal groups, Insikt Group uses a naming convention corresponding to the Greek alphabet. Where we have identified a criminal entity connected to a particular country, we will use the appropriate country color, and where that group may be tied to a specific government organization, tie it to that entity specifically.

Insikt Group uses mathematical terms when naming newly identified malware.



Appendix A — Indicators of Compromise**Command and Control Infrastructure**

Domain	IP Address	First Seen	Last Seen	Description
ipsoftwarelabs[.]com	85.209.43[.]21	2019-11-08	*	PlugX C2
cabsecnow[.]com	167.88.180[.]32	2020-07-14	*	PlugX C2
cabsecnow[.]com	103.85.24[.]136	2020-06-10	2020-07-14	PlugX C2
cabsecnow[.]com	167.88.180[.]5	2019-10-26	2020-06-10	PlugX C2
cabsecnow[.]com	167.88.177[.]224	2019-09-18	2019-10-19	PlugX C2
lameers[.]com	167.88.180[.]32	2020-02-14	*	PlugX C2
lameers[.]com	167.88.180[.]132	2019-11-27	2020-02-13	PlugX C2
systeminfor[.]com	103.85.24[.]136	2020-07-15	*	PlugX C2
systeminfor[.]com	167.88.180[.]32	2020-05-29	2020-07-15	PlugX C2
systeminfor[.]com	103.85.24[.]190	2020-05-17	2020-05-29	PlugX C2
N/A	103.85.24[.]149	2020-06-08	2020-06-23	PlugX C2
N/A	167.88.180[.]198	2020-06-15	2020-06-25	PlugX Payload Staging Server
web.microsoft[.]com	154.213.21[.]207	2020-04-27	*	PIVY C2
N/A	154.213.21[.]70	2020-06-04	*	Cobalt Strike C2
lib.jquery[.]net	154.213.21[.]70	2020-06-04	*	Associated with Cobalt Strike C2
N/A	154.213.21[.]27	2020-06-04	*	Cobalt Strike Staging Server
lib.hostareas[.]com	154.213.21[.]73	2020-05-13	*	Linked through infrastructure overlap

*Denotes that domain or server is still live at time of publication.

PlugX

File Name	About China's plan for Hong Kong security law.zip
MD5 Hash	660d1132888b2a2ff83b695e65452f87
SHA1 Hash	1d3b34c473231f148eb3066351c92fb3703d26c6
SHA256 Hash	86590f80b4e1608d0367a7943468304f7eb665c9195c24996281b1a958bc1512

File Name	N. 490.349 N. 491.189.zip
MD5 Hash	2a245c0245809f4a33b5aac894070519
SHA1 Hash	c27f2ed5029418c7f786640fb929460b9f931671
SHA256 Hash	fb7e8a99cf8cb30f829db0794042232acfe7324722cbea89ba8b77ce2dcf1caa

File Name	QUM, IL VATICANO DELL'ISLAM.rar
MD5 Hash	2e69b5ed15156e5680334fa88be5d1bd
SHA1 Hash	c435c75877b39406dbe06e357ef304710d567da9
SHA256 Hash	282eef984c20cc334f926725cc36ab610b00d05b5990c7f55c324791ab156d92

File Name	wwlib.dll
MD5 Hash	c6206b8eacabc1dc3578cec2b91c949a
SHA1 Hash	93e8445862950ef682c2d22a9de929b72547643a
SHA256 Hash	4cef5835072bb0290a05f9c5281d4a614733f480ba7f1904ae91325a10a15a04

File Name	wwlib.dll
MD5 Hash	2ec79d0605a4756f4732aba16ef41b22
SHA1 Hash	304e1eb8ab50b5e28cbbdb280d653efae4052e1f
SHA256 Hash	f6e5a3a32fb3aaf3f2c56ee482998b09a6ced0a60c38088e7153f3ca247ab1cc

File Name	acrord32.dll
MD5 Hash	6060f7dc35c4d43728d5ca5286327c01
SHA1 Hash	35ff54838cb6db9a1829d110d2a6b47001648f17
SHA256 Hash	8a07c265a20279d4b60da2cc26f2bb041730c90c6d3eca64a8dd9f4a032d85d3

File Name	hex.dll
MD5 Hash	e57f8364372e3ba866389c2895b42628
SHA1 Hash	fb29f04fb4ffb71f623481cffe221407e2256e0a
SHA256 Hash	bc6c2fda18f8ee36930b469f6500e28096eb6795e5fd17c44273c67bc9fa6a6d

File Name	adobeupdate.dat
MD5 Hash	2351F62176D4F3A6429D9C2FF7D444E2
SHA1 Hash	1BDBABE56B4659FCA2813A79E972A82A26EF12B1
SHA256 Hash	01C1FD0E5B8B7BBED62BC8A6F7C9CEFF1725D4FF6EE86FA813BF6E70B079812F

File Name	hex.dll
MD5 Hash	9c44ec556d53301d86c13a884128b8de
SHA1 Hash	7c683d3c3590cbc61b5077bc035f4a36cae097d4
SHA256 Hash	7d85ebd460df8710d0f60278014654009be39945a820755e1fbd59030c14f4c7

File Name	adobeupdate.dat
MD5 Hash	977beb9a5a2bd24bf333397c33a0a67e
SHA1 Hash	d7e55b655a2a90998dbab0f921115edc508e1bf9
SHA256 Hash	4c8405e1c6531bcb95e863d0165a589ea31f1e623c00bcfd02fbf4f434c2da79

Poison Ivy

File Name	MpSvc.dll
MD5 Hash	b613cc3396ae0e9e5461a910bcac8ca5
SHA1 Hash	28746fd20a4032ba5fd3a1a479edc88cd74c3fc9
SHA256 Hash	9bac74c592a36ee249d6e0b086bfab395a37537ec87c2095f999c00b946ae81d

Cobalt Strike

File Name	OneDrive.exe
MD5 Hash	83763fe02f41c1b3ce099f277391732a
SHA1 Hash	3ed2d4e3682d678ea640aadbf08311c6f2081e8
SHA256 Hash	7824eb5f173c43574593bd3afab41a60e0e2ffae80201a9b884721b451e6d935

Appendix B — MITRE ATT&CK Mapping

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Spearphishing Attachment	Command-Line Interface	BITS Jobs	AccessToken Manipulation	AccessToken Manipulation	Credential Dumping	Application Window Discovery	PasstheHash	Clipboard Data	Commonly Used Port	Exfiltration Over Command and Control Channel
Spearphishing Link	PowerShell	DLL Search Order Hijacking	Bypass User Account Control	BITS Jobs	Input Capture	File and Directory Discovery	Remote Desktop Protocol	Data from Local System	Connection Proxy	
ValidAccounts	Rundll32	Modify Existing Service	DLL Search Order Hijacking	Bypass User Account Control		Network Service Scanning	Remote File Copy	Data from Removable Media	Custom Command and Control Protocol	
	Scheduled Task	New Service	New Service	Connection Proxy		Network Share Discovery	Remote Services	Data Staged	Data Encoding	
	Scripting	Registry Run Keys / Startup Folder	Parent PID Spoofing	Deobfuscate/Decode Files or Information		Process Discovery	Windows Admin Shares	Input Capture	Data Obfuscation	
	Service Execution	Scheduled Task	Process Injection	DLL Sideloading		Query Registry	Windows Remote Management	Man in the Browser	Fallback Channels	
	Signed Binary Proxy Execution	ValidAccounts	Scheduled Task	Indicator Removal from Tools		Remote System Discovery		Screen Capture	Multi-hop Proxy	
	User Execution	Web Shell	ValidAccounts	Masquerading		System Network Configuration Discovery			Multiband Communication	
	Windows Management Instrumentation		Web Shell	Modify Registry		System Network Connections Discovery			Remote File Copy	
	Windows Remote Management			Obfuscated Files or Information		System Owner/User Discovery			Standard Application Layer Protocol	
				Parent PID Spoofing		Virtualization/Sandbox Evasion			Standard Cryptographic Protocol	
				Process Hollowing					Standard Non-Application Layer Protocol	
				Process Injection					Uncommonly Used Port	
				Rootkit					Web Service	
				Rundll32						
				Scripting						
				Signed Binary Proxy Execution						
				Timestomp						
				ValidAccounts						
				Virtualization/Sandbox Evasion						
				Web Service						

Appendix C — Python Decoding Script

```
import lznt1

def decompress(filename):
    decompressed=""
    with open(filename,"rb") as f:
        decompressed = lznt1.decompress(f.read())
    return decompressed

compressed=True
filename="http_dll.dat"

if compressed==False:
    data=decompress(filename)
else:
    with open(filename,"rb") as dat:
        data=dat.read()

key=[]

for d in data:
    if d !=0x00:
        key.append(d)
    else:
        break
klen=len(key)

output = []
loop_condition = 0
for c in data[klen+1:]:
    current_key = key[loop_condition%klen]
    output.append(c^current_key)
    loop_condition += 1

with open("http_dll.dat.bin","wb") as decoded:
    decoded.write(bytearray(output))
```

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.