TLP: AMBER

Threat Trend Report on Mustang Panda

V1.0

AhnLab Security Emergency Response Center (ASEC)

Aug. 20, 2021

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can only be accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded, meaning that the sum of each item may not match the total.

This report is a work of authorship protected by the Copy Right Act
Unauthorized copying or reproduction for profit is strictly prohibited under any circumstances.

Seek permission from AhnLab in advance
if you wish to use a part or all of the report.

If you reprint or reproduce the material without the permission of the organization mentioned above, you may be held accountable for criminal or civil liabilities.

The version information of this report is as follows:

Version	Date	Details
1.0	2021-08-20	First release

Contents

⚠ CAUTION

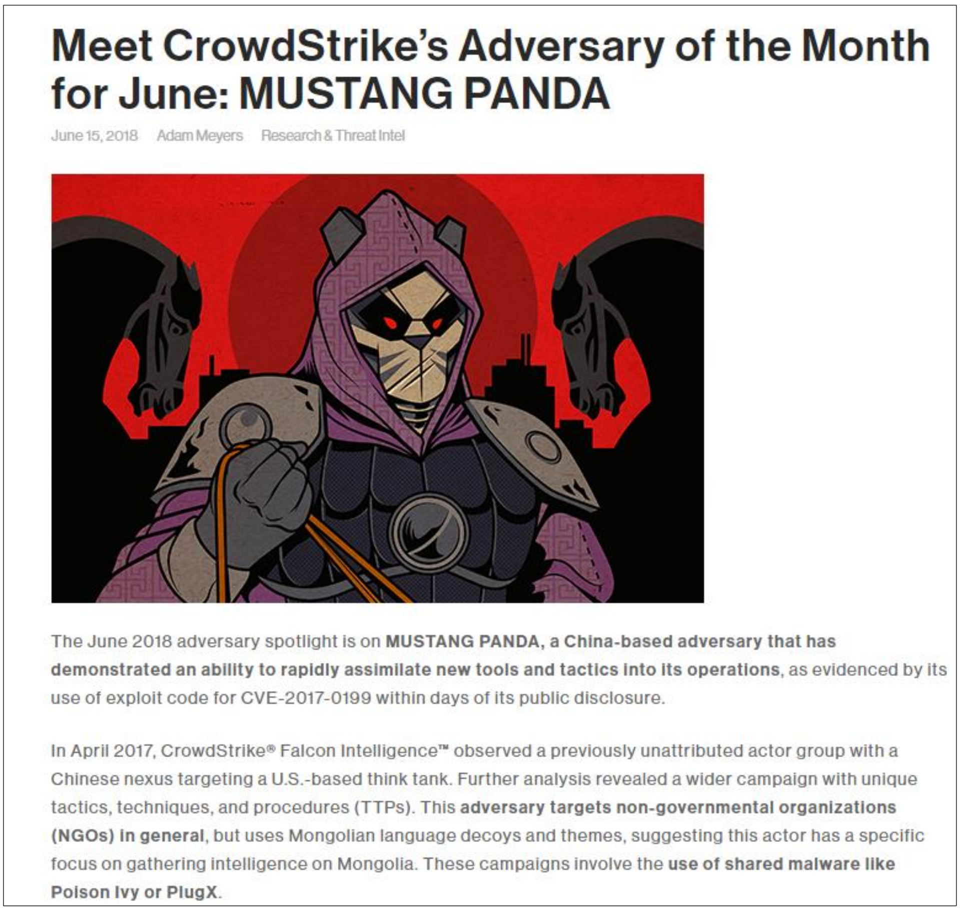
This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

1. Mustang Panda Group Overview

1-1. Introduction to the Mustang Panda Group

Mustang Panda, which is assumed to be based in China, was first brought to the surface by security company CrowdStrike. They are also called Bronze President, HoneyMyte, and TA416. Although first discovered in 2017, they are an APT group that have likely been in operation since 2014. Their attacks mainly target government organizations, non-profit organizations, and religious and other non-government organizations (NGO), but they are presumed to be behind attacks targeting various countries including Mongolia, Myanmar, Pakistan, and Vietnam as well.[1] The malware used by this group include Cobalt Strike, PlugX, and Poison Ivy. Poison Ivy is an old RAT malware that is rarely used nowadays, and so the group usually uses Cobalt Strike and PlugX.

[1] https://attack.mitre.org/groups/G0129/



Meet CrowdStrike's Adversary of the Month for June: MUSTANG PANDA

June 15, 2018 Adam Meyers Research & Threat Intel

The June 2018 adversary spotlight is on **MUSTANG PANDA, a China-based adversary that has demonstrated an ability to rapidly assimilate new tools and tactics into its operations**, as evidenced by its use of exploit code for CVE-2017-0199 within days of its public disclosure.

In April 2017, CrowdStrike® Falcon Intelligence™ observed a previously unattributed actor group with a Chinese nexus targeting a U.S.-based think tank. Further analysis revealed a wider campaign with unique tactics, techniques, and procedures (TTPs). This **adversary targets non-governmental organizations (NGOs) in general**, but uses Mongolian language decoys and themes, suggesting this actor has a specific focus on gathering intelligence on Mongolia. These campaigns involve the **use of shared malware like Poison Ivy or PlugX**.

Figure 1. Introduction to Mustang Panda[2]

1-2. Characteristics of the Mustang Panda Group

Mustang Panda drops and executes malware after accessing vulnerable systems, or distributes them by attaching a compressed file comprised of a normal EXE, malicious DLL loader, encrypted data, and a bait document to spear phishing emails. But aside from that, they use other methods of distribution such as embedding these files inside an ".LNK" file or including in their emails a shortened URL of the external cloud storage (usually Google Drive) where these files are saved. When the normal EXE is executed, it uses the DLL Side-Loading method where the malicious DLL in the same directory is loaded. Afterward, encrypted data is read and decrypted before the ultimate malware is executed, infecting the system. In 2020, there was an attempt at an attack on a Korean national organization; the details will be covered further on.

[2] https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/

1-3. Related Groups

According to security company Recorded Future,[3] a piece of malware that uses the same TTP as Mustang Panda with a very similar code had been discovered. It differs in the C&C Server traffic encryption method, where the used encryption mechanism is different from the one used by Mustang Panda PlugX. It is not publicly known that this campaign is used by Mustang Panda. Detailed analysis revealed that Mustang Panda uses XOR encrypted communication when communicating with the C&C Server, but the newly detected malware uses the RC4 encryption method. Due to such differences, the organization behind this new malware is called the RedDelta Group to be distinguished from the Mustang Panda Group. However, other security companies view Mustang Panda and RedDelta as the same group and refer to them accordingly. AhnLab also does not refer to RedDelta separately, but refers to the whole as Mustang Panda.

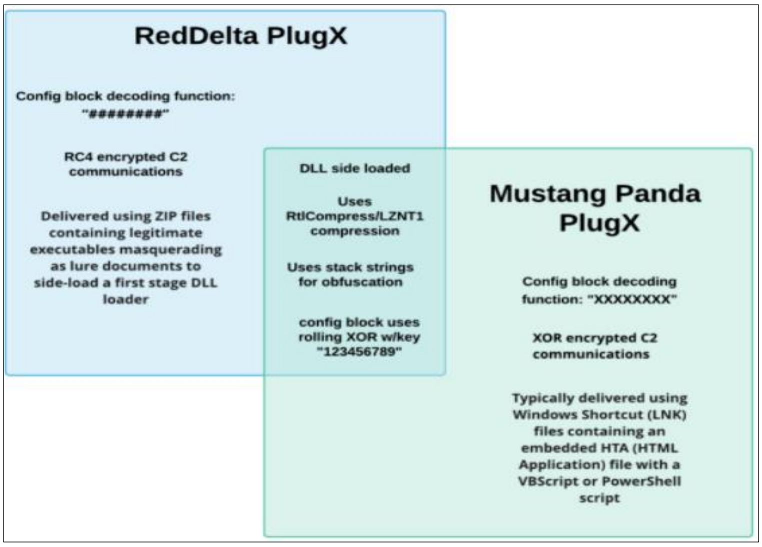

RedDelta PlugX
Config block decoding function: "########"
RC4 encrypted C2 communications
Delivered using ZIP files containing legitimate executables masquerading as lure documents to side-load a first stage DLL loader
DLL side loaded
Uses RtlCompress/LZNT1 compression
Uses stack strings for obfuscation
config block uses rolling XOR w/key "123456789"
Mustang Panda PlugX
Config block decoding function: "XXXXXXXX"
XOR encrypted C2 communications
Typically delivered using Windows Shortcut (LNK) files containing an embedded HTA (HTML Application) file with a VBScript or PowerShell script

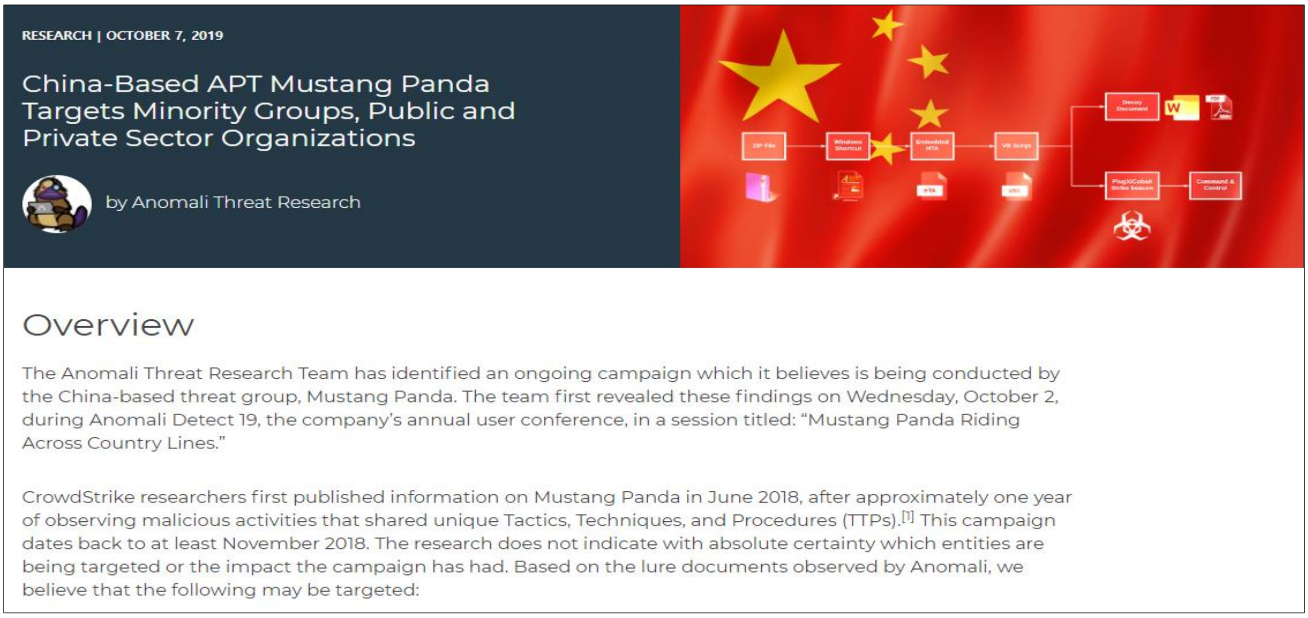
Figure 2. Difference between Mustang Panda and RedDelta

[3] https://www.recordedfuture.com/reddelta-targets-catholic-organizations/

2. Major Activities of the Mustang Panda Group

2-1. November - December 2019

While specific targets of attack are unknown, according to security company Anomali, suspicious ZIP files were found in bulk in November 2019, which contained an ".LNK" file. Analysis showed this to be a creation of Mustang Panda. When the ".LNK" file is opened, the bait document is displayed on the screen and the malware is executed. Table 1 below shows the presumed attack targets based on the content of the bait document.



RESEARCH | OCTOBER 7, 2019

China-Based APT Mustang Panda Targets Minority Groups, Public and Private Sector Organizations

by Anomali Threat Research

Overview

The Anomali Threat Research Team has identified an ongoing campaign which it believes is being conducted by the China-based threat group, Mustang Panda. The team first revealed these findings on Wednesday, October 2, during Anomali Detect 19, the company's annual user conference, in a session titled: "Mustang Panda Riding Across Country Lines."

CrowdStrike researchers first published information on Mustang Panda in June 2018, after approximately one year of observing malicious activities that shared unique Tactics, Techniques, and Procedures (TTPs).[1] This campaign dates back to at least November 2018. The research does not indicate with absolute certainty which entities are being targeted or the impact the campaign has had. Based on the lure documents observed by Anomali, we believe that the following may be targeted:

Figure 3. Mustang Panda's activities identified[4]

[4] https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations

Attack Target (Presumed)
Lang Son, Vietnam
Lao Cai, Vietnam
Embassy of Vietnam in China
Tinh Ha Nam Party Council, Vietnam
MIAT Mongolian Airlines
Sindh Police, Pakistan
Shan (Myanmar) National Restoration Commission and army
China Zentrum eV, Germany

Table 1. Deduced attack targets based on the bait document

The execution flow of this campaign involves the execution of ".LNK" file contained within the ZIP, which in turn executes the embedded VBScript through HTA. This script drops and opens the bait document, then drops and executes Cobalt Strike Beacon or PlugX. Details of the execution flow are shown in Figure 4 below.

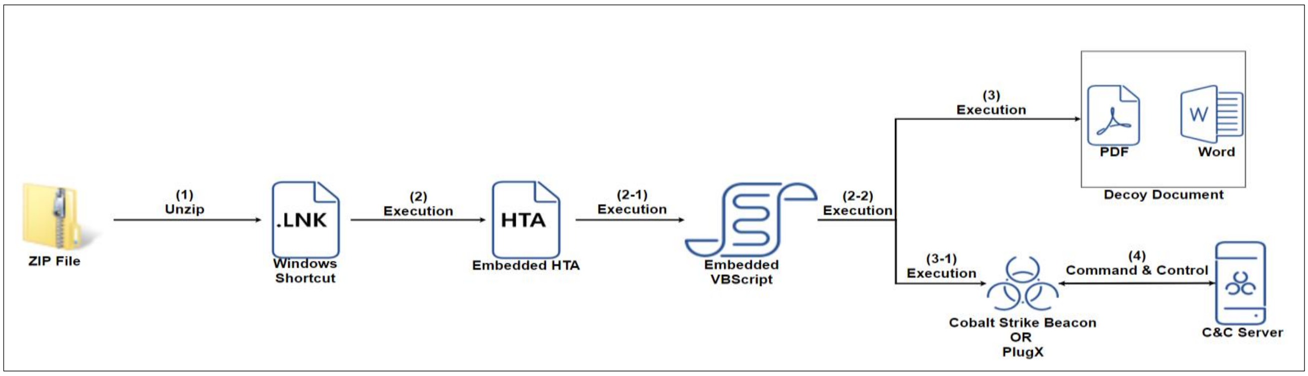
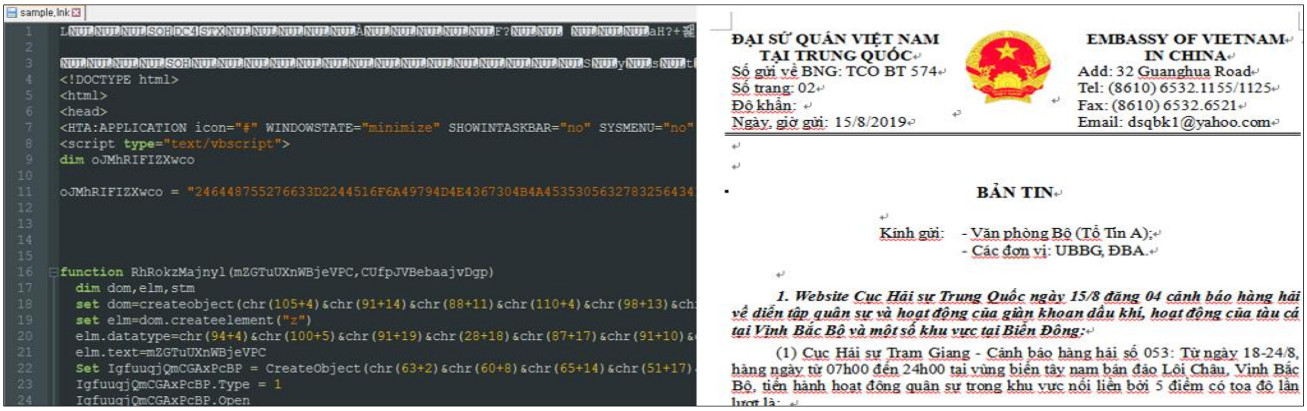


Figure 4. Flow of execution



```
LNULNULNULSOHDC4STXNULNULNULNULNULÀNULNULNULNULNULF?NULNUL NULNULNULaH?+

NULNULNULNULSOHNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULSNULyNULsNULt
<!DOCTYPE html>
<html>
<head>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no"
<script type="text/vbscript">
dim oJMhRIFIZXwco

oJMhRIFIZXwco = "2464487552766 33D2244516F6A49794D4E4367304B4A4535305632783256434



function RhRokzMajnyl(mZGTuUXnWBjeVPC,CUfpJVBebaajvDgp)
  dim dom,elm,stm
  set dom=createobject(chr(105+4)&chr(91+14)&chr(88+11)&chr(110+4)&chr(98+13)&ch
  set elm=dom.createelement("z")
  elm.datatype=chr(94+4)&chr(100+5)&chr(91+19)&chr(28+18)&chr(87+17)&chr(91+10)&
  elm.text=mZGTuUXnWBjeVPC
  Set IgfuuqjQmCGAxPcBP = CreateObject(chr(63+2)&chr(60+8)&chr(65+14)&chr(51+17)
  IgfuuqjQmCGAxPcBP.Type = 1
  IgfuuqjQmCGAxPcBP.Open
```

ĐẠI SỨ QUÁN VIỆT NAM
TẠI TRUNG QUỐC
Số gửi về BNG: TCO BT 574
Số trang: 02
Độ khẩn:
Ngày, giờ gửi: 15/8/2019

EMBASSY OF VIETNAM
IN CHINA
Add: 32 Guanghua Road
Tel: (8610) 6532.1155/1125
Fax: (8610) 6532.6521
Email: dsqbk1@yahoo.com

BẢN TIN

Kính gửi: - Văn phòng Bộ (Tổ Tin A);
- Các đơn vị: UBBG, ĐBA.

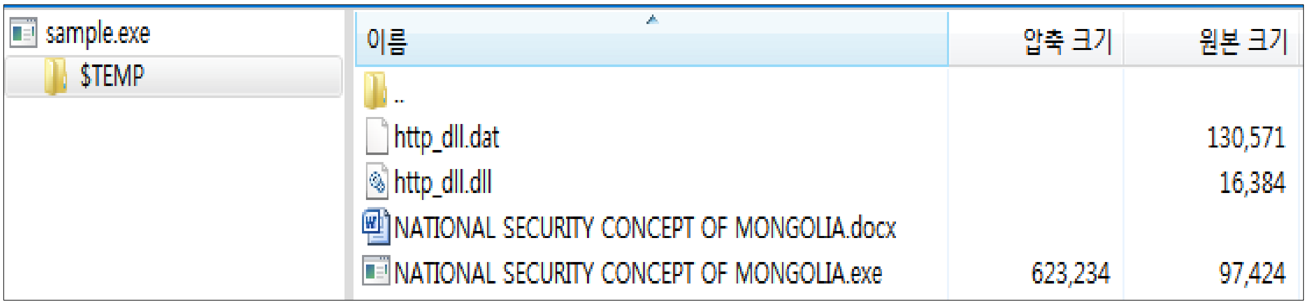
1. Website Cục Hải sự Trung Quốc ngày 15/8 đăng 04 cảnh báo hàng hải về diễn tập quân sự và hoạt động của giàn khoan dầu khí, hoạt động của tàu cá tại Vịnh Bắc Bộ và một số khu vực tại Biển Đông:

(1) Cục Hải sự Tram Giang - Cảnh báo hàng hải số 053: Từ ngày 18-24/8, hàng ngày từ 07h00 đến 24h00 tại vùng biển tây nam bán đảo Lôi Châu, Vịnh Bắc Bộ, tiến hành hoạt động quân sự trong khu vực nối liền bởi 5 điểm có toạ độ lần lượt là:

Figure 5. Script and bait document included in the ".LNK"` file **(Cobalt Strike type)**

(MD5: 05CF906B750EB335125695DA42F4EAFC)

It has also been distributed as an NSIS-based EXE file instead of an ".LNK" file. This EXE file contains a normal EXE file, malicious DLL loader, encrypted data, and bait document. When the NSIS-based EXE file is executed, it is designed to drop and open the bait document and malware.

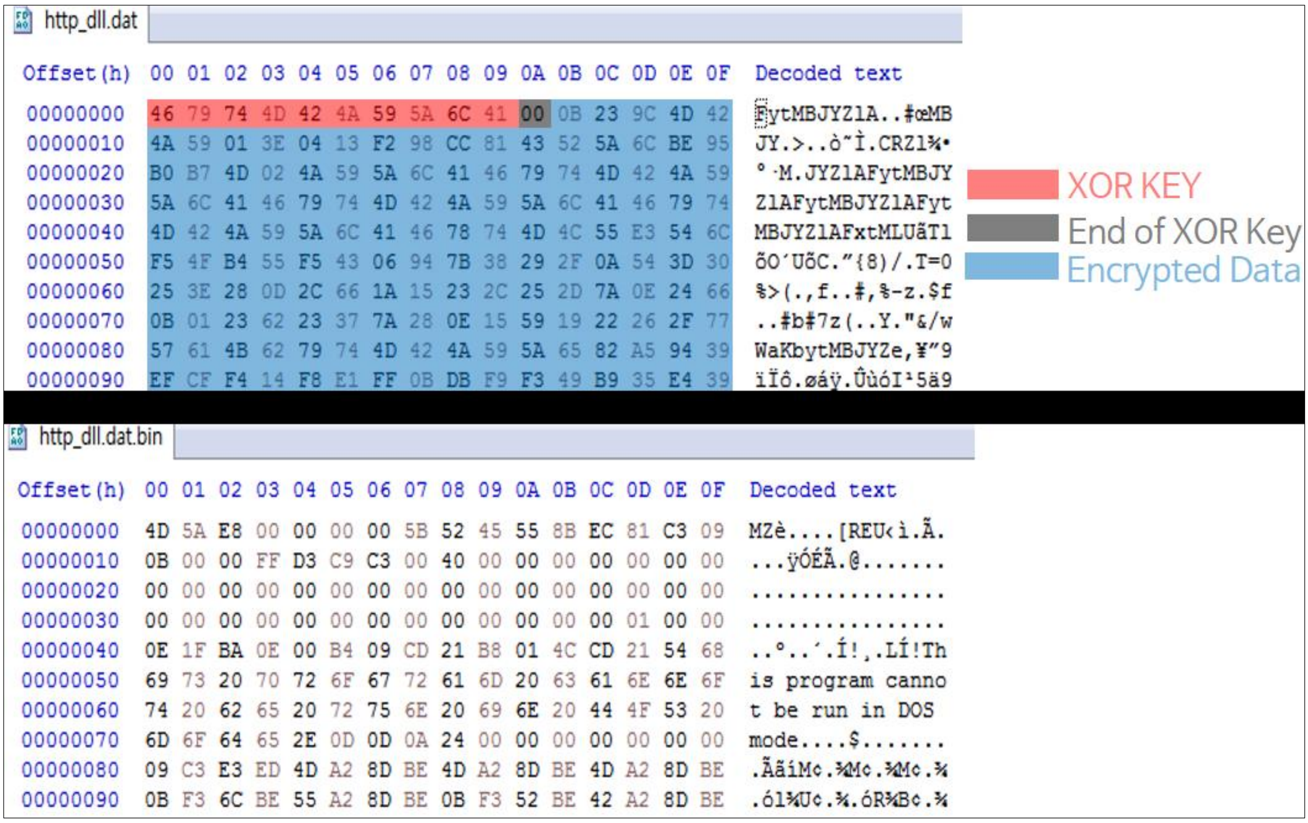


이름	압축 크기	원본 크기
..		
http_dll.dat		130,571
http_dll.dll		16,384
NATIONAL SECURITY CONCEPT OF MONGOLIA.docx		
NATIONAL SECURITY CONCEPT OF MONGOLIA.exe	623,234	97,424

Figure 6. Malware and bait document contained in the EXE file (PlugX type)

(MD5: 0d3fbc842a430f5367d480dd1b74449b)

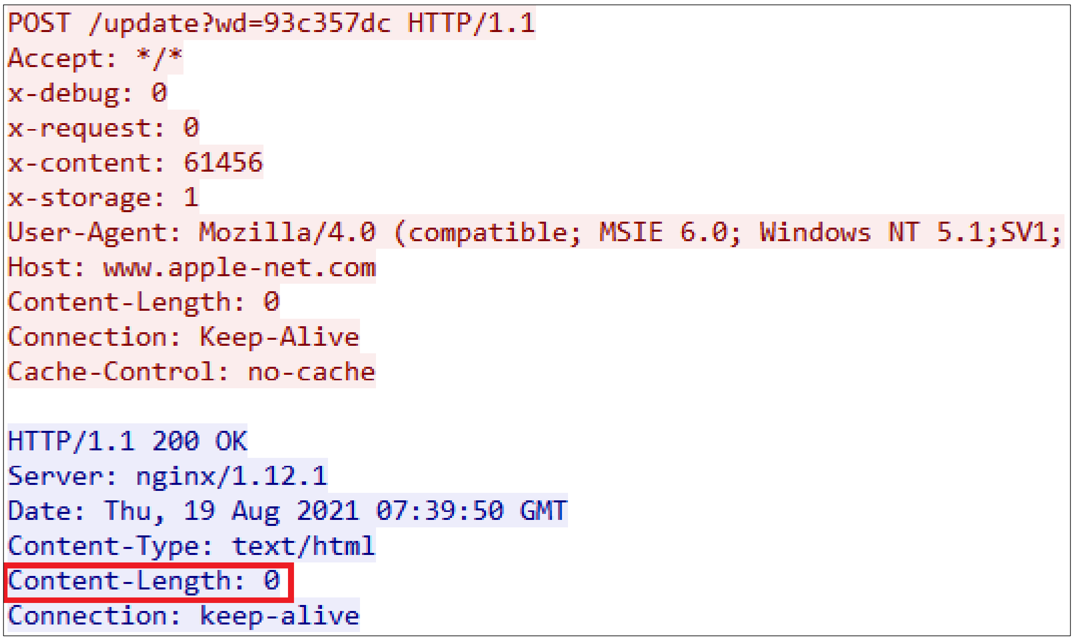
The data encrypted in the PlugX type is composed of values from Offset 0 to 9, and the XOR KEY, 0xA is composed of encrypted data from NULL byte, 0xB which signifies the end of the key. When decryption by XOR occurs, the data becomes a DLL file, which in turn receives commands from the C&C Server and performs malicious behaviors. At the time of analysis, the server could be accessed, but no data was received. Thus, it was not possible to identify how the commands were transmitted and received.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  46 79 74 4D 42 4A 59 5A 6C 41 00 0B 23 9C 4D 42  FytMBJYZlA..#œMB
00000010  4A 59 01 3E 04 13 F2 98 CC 81 43 52 5A 6C BE 95  JY.>..ò˜Ì.CRZl¾•
00000020  B0 B7 4D 02 4A 59 5A 6C 41 46 79 74 4D 42 4A 59  °·M.JYZlAFytMBJY
00000030  5A 6C 41 46 79 74 4D 42 4A 59 5A 6C 41 46 79 74  ZlAFytMBJYZlAFyt
00000040  4D 42 4A 59 5A 6C 41 46 78 74 4D 4C 55 E3 54 6C  MBJYZlAFxtMLUãTl
00000050  F5 4F B4 55 F5 43 06 94 7B 38 29 2F 0A 54 3D 30  õO´UõC.”{8)/.T=0
00000060  25 3E 28 0D 2C 66 1A 15 23 2C 25 2D 7A 0E 24 66  %>(.,f..#,%-z.$f
00000070  0B 01 23 62 23 37 7A 28 0E 15 59 19 22 26 2F 77  ..#b#7z(..Y."&/w
00000080  57 61 4B 62 79 74 4D 42 4A 59 5A 65 82 A5 94 39  WaKbytMBJYZe‚¥”9
00000090  EF CF F4 14 F8 E1 FF 0B DB F9 F3 49 B9 35 E4 39  ïÏô.øáÿ.ÛùóI¹5ä9
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4D 5A E8 00 00 00 00 5B 52 45 55 8B EC 81 C3 09  MZè....[REU‹ì.Ã.
00000010  0B 00 00 FF D3 C9 C3 00 40 00 00 00 00 00 00 00  ...ÿÓÉÃ.@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  ................
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  09 C3 E3 ED 4D A2 8D BE 4D A2 8D BE 4D A2 8D BE  .ÃãíM¢.¾M¢.¾M¢.¾
00000090  0B F3 6C BE 55 A2 8D BE 0B F3 52 BE 42 A2 8D BE  .ól¾U¢.¾.óR¾B¢.¾
```

Figure 6-1. (Top) Encrypted data (Bottom) Decrypted data (PlugX)



```
POST /update?wd=93c357dc 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: www.apple-net.com
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx/1.12.1
Date: Thu, 19 Aug 2021 07:39:50 GMT
Content-Type: text/html
Content-Length: 0
Connection: keep-alive
```

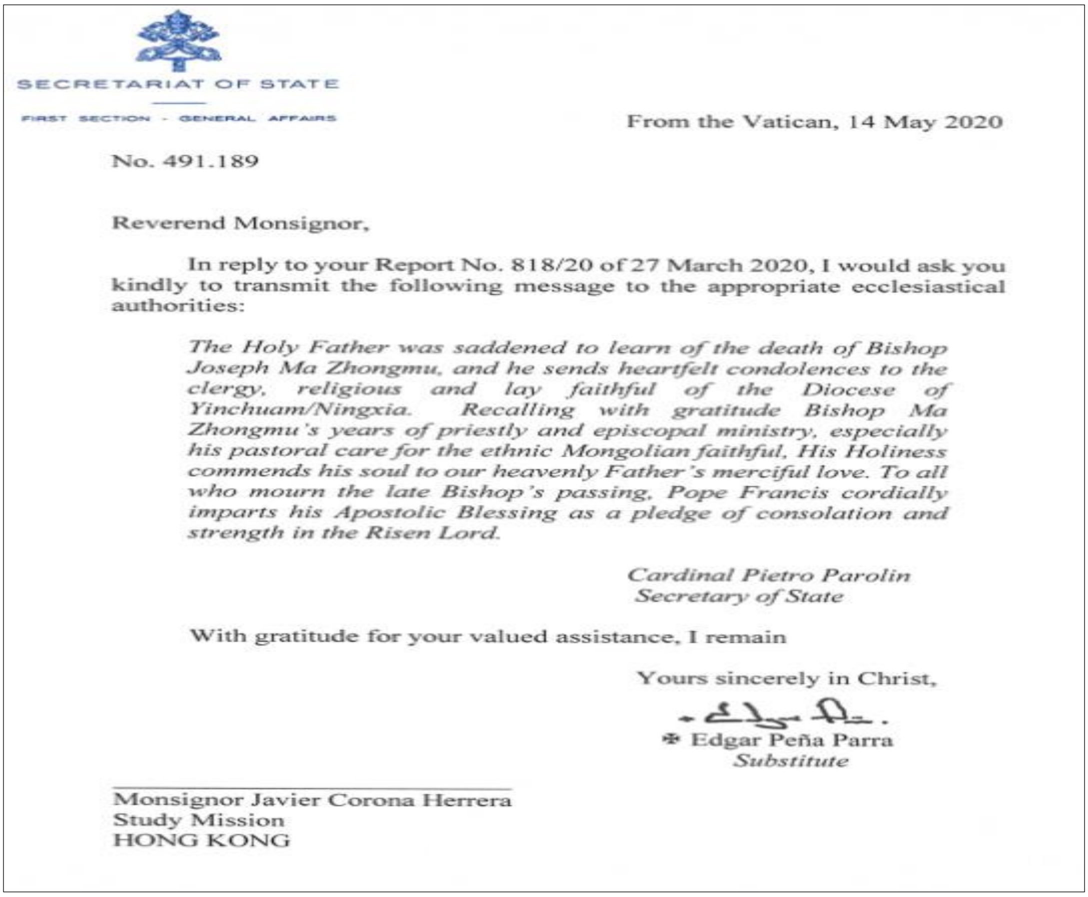
Figure 6-2. Attempting to connect to a certain domain but not being able to procure commands

2-2. May - November 2020

According to security company Recorded Future, just before the renewal of the China-Vatican agreement of 2018 scheduled for September 2020, a network infiltration on the Vatican and Hong Kong catholic parishes occurred. Recorded Future stated that the purpose of this attack seems to be for strengthening control over the catholic church and increasing Chinese influence to reduce the perceived influence of the Vatican over the Chinese catholic community. However, the attack proceeded despite the suspension of the agreement in September. In the affected systems, a bait Vatican document was found targeting the visit of the Hong Kong research mission to China. It could not be ascertained whether this document was made by the threat actor or a piece of malware was embedded into a lawful document that could be obtained by said party. It is said that this document was found after signs of network infiltration was detected.[5] Moreover, the threat actors were inactive from September 16 to October 10, 2020. During this period lies a Chinese national holiday called the National Day, and the "golden week" which is an unofficial holiday period. The threat actor resumed activities after this period and began to distribute a new PlugX DLL Loader variant developed in Golang.[6]

[5] https://www.recordedfuture.com/reddelta-targets-catholic-organizations/

[6] https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-



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

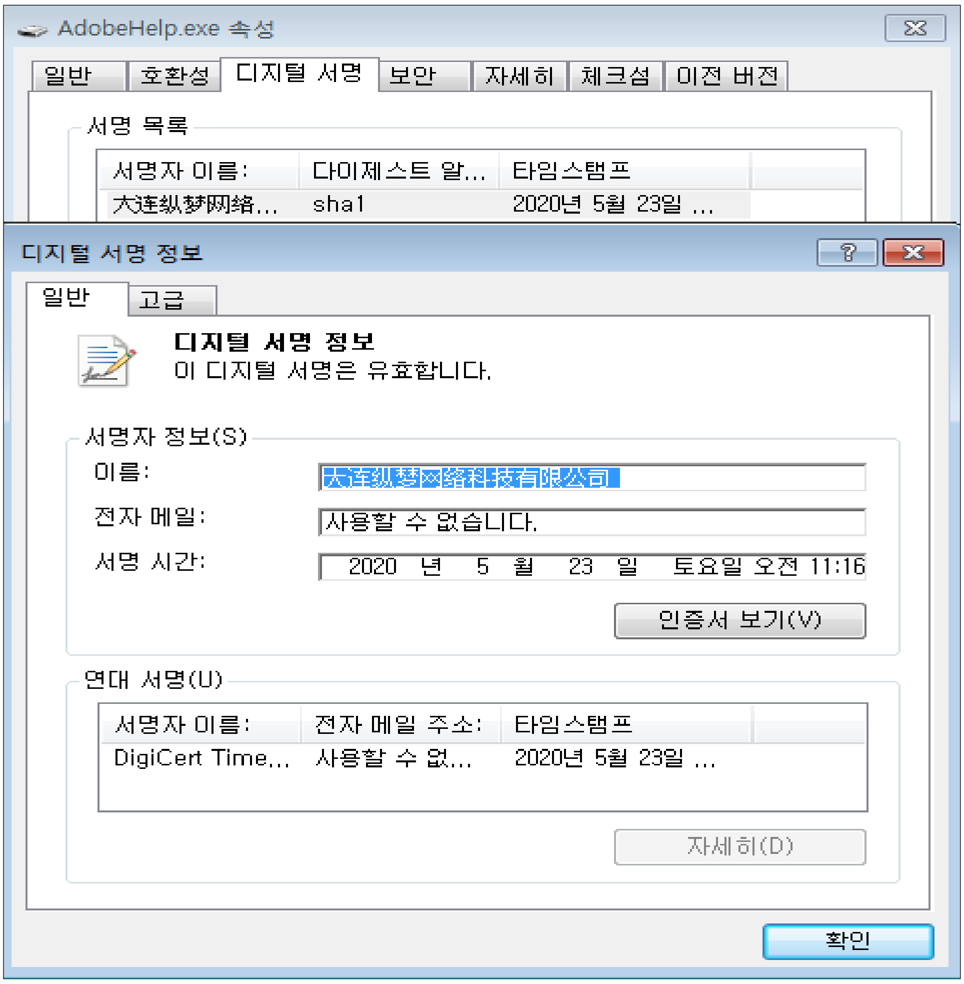
Monsignor Javier Corona Herrera
Study Mission
HONG KONG

Figure 7. Bait Vatican document targeting the visit of the Hong Kong research mission to China

Also, a file was found signed with a certificate from a company in Beijing, which had never been used before. This file is unnecessary for executing the PlugX,[7] and analysis revealed that it is responsible for finding "CabinetWClass" and terminating the current explorer (folder). Files signed with the aforementioned certificate were found in multiple malware strains without any pertinence to Mustang Panda. From this, it is deemed that this certificate has been leaked out and used in various malware.

malware-loader

[7] https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader



AdobeHelp.exe 속성

일반 | 호환성 | 디지털 서명 | 보안 | 자세히 | 체크섬 | 이전 버전

서명 목록

서명자 이름:	다이제스트 알...	타임스탬프
大连纵梦网络...	sha1	2020년 5월 23일 ...

디지털 서명 정보

일반 | 고급

디지털 서명 정보
이 디지털 서명은 유효합니다.

서명자 정보(S)

이름:	大连纵梦网络科技有限公司
전자 메일:	사용할 수 없습니다.
서명 시간:	2020 년 5 월 23 일 토요일 오전 11:16

연대 서명(U)

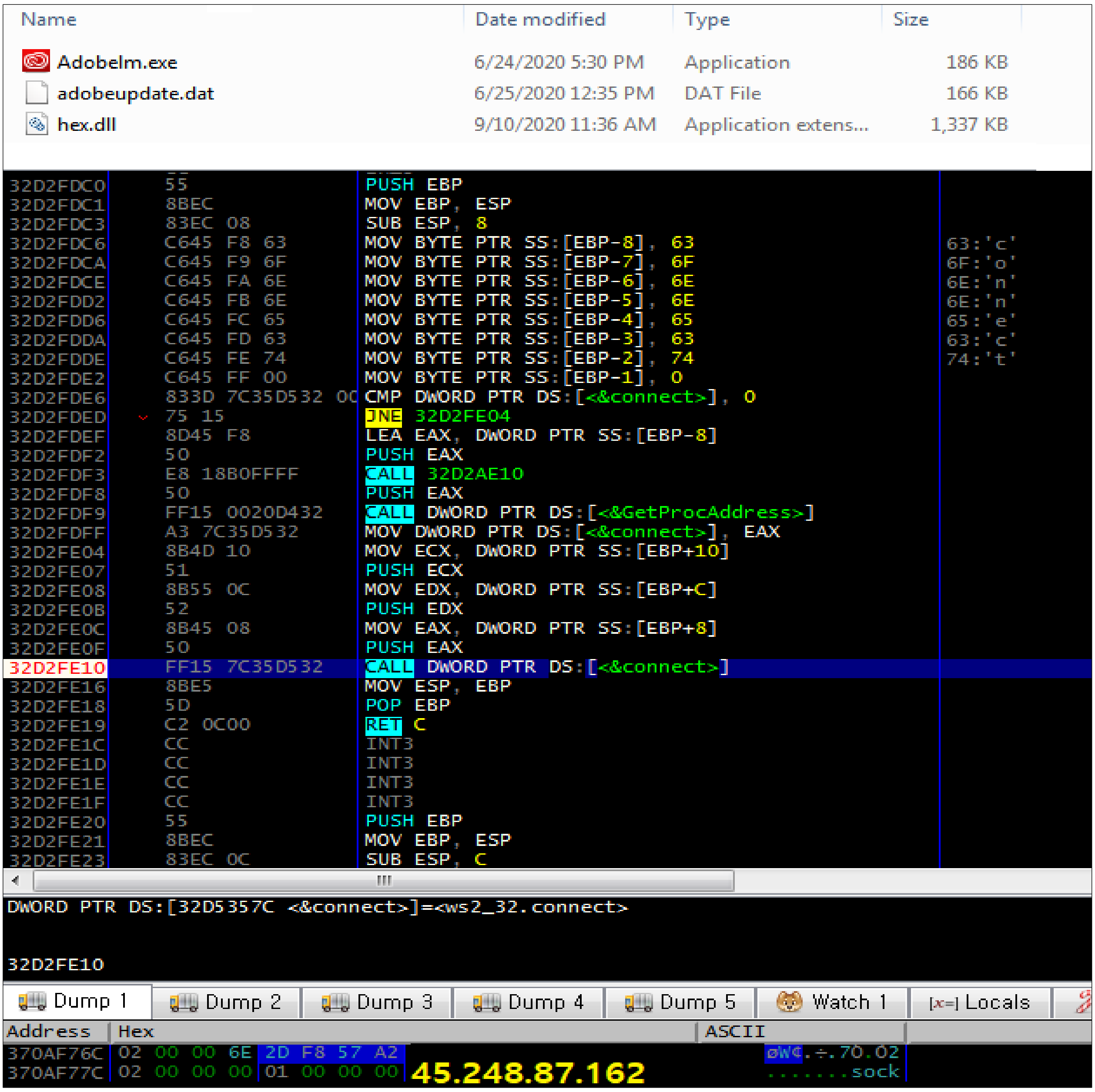
서명자 이름:	전자 메일 주소:	타임스탬프
DigiCert Time...	사용할 수 없...	2020년 5월 23일 ...

Figure 7-1. File signed with the certificate

2-2-1. Attacks on South Korean National Organizations

Mustang Panda originally made no attempts to attack Korea, but it had been identified in October 2020 that they attacked a South Korean national organization. The malware used in this attack was the aforementioned PlugX DLL Loader variant developed in Golang, which had a precisely matching IP to that found in the above campaign.[8] Seeing from the fact that the file composition and names contained in the ZIP file are the same, it is deemed that Mustang Panda was behind this attack.

[8] https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader



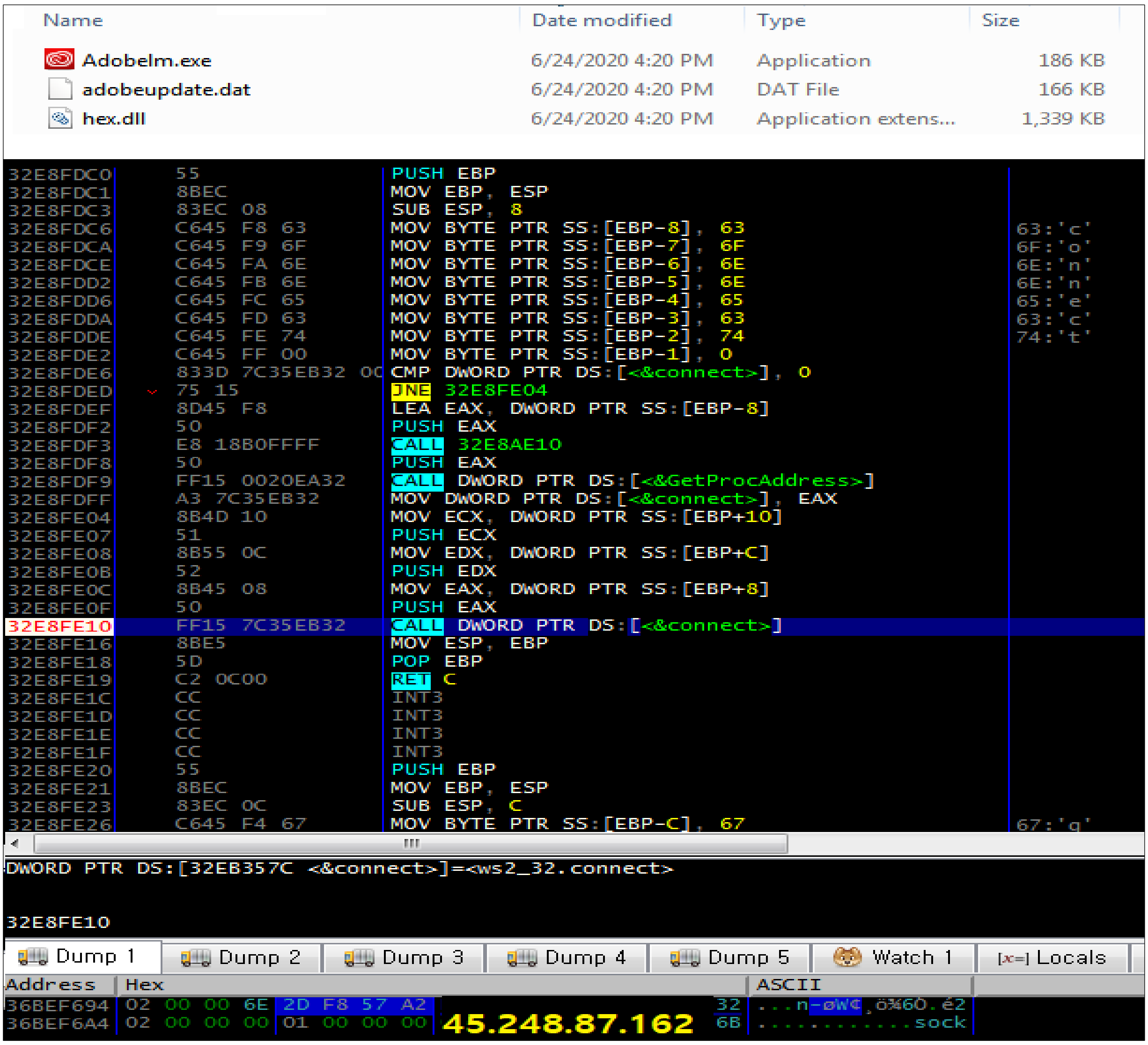
Name	Date modified	Type	Size
Adobelm.exe	6/24/2020 5:30 PM	Application	186 KB
adobeupdate.dat	6/25/2020 12:35 PM	DAT File	166 KB
hex.dll	9/10/2020 11:36 AM	Application extens...	1,337 KB

```
32D2FDC0      55               PUSH EBP
32D2FDC1      8BEC             MOV EBP, ESP
32D2FDC3      83EC 08          SUB ESP, 8
32D2FDC6      C645 F8 63       MOV BYTE PTR SS:[EBP-8], 63            63:'c'
32D2FDCA      C645 F9 6F       MOV BYTE PTR SS:[EBP-7], 6F            6F:'o'
32D2FDCE      C645 FA 6E       MOV BYTE PTR SS:[EBP-6], 6E            6E:'n'
32D2FDD2      C645 FB 6E       MOV BYTE PTR SS:[EBP-5], 6E            6E:'n'
32D2FDD6      C645 FC 65       MOV BYTE PTR SS:[EBP-4], 65            65:'e'
32D2FDDA      C645 FD 63       MOV BYTE PTR SS:[EBP-3], 63            63:'c'
32D2FDDE      C645 FE 74       MOV BYTE PTR SS:[EBP-2], 74            74:'t'
32D2FDE2      C645 FF 00       MOV BYTE PTR SS:[EBP-1], 0
32D2FDE6      833D 7C35D532 00 CMP DWORD PTR DS:[<&connect>], 0
32D2FDED    v 75 15            JNE 32D2FE04
32D2FDEF      8D45 F8          LEA EAX, DWORD PTR SS:[EBP-8]
32D2FDF2      50               PUSH EAX
32D2FDF3      E8 18B0FFFF      CALL 32D2AE10
32D2FDF8      50               PUSH EAX
32D2FDF9      FF15 0020D432    CALL DWORD PTR DS:[<&GetProcAddress>]
32D2FDFF      A3 7C35D532      MOV DWORD PTR DS:[<&connect>], EAX
32D2FE04      8B4D 10          MOV ECX, DWORD PTR SS:[EBP+10]
32D2FE07      51               PUSH ECX
32D2FE08      8B55 0C          MOV EDX, DWORD PTR SS:[EBP+C]
32D2FE0B      52               PUSH EDX
32D2FE0C      8B45 08          MOV EAX, DWORD PTR SS:[EBP+8]
32D2FE0F      50               PUSH EAX
32D2FE10      FF15 7C35D532    CALL DWORD PTR DS:[<&connect>]
32D2FE16      8BE5             MOV ESP, EBP
32D2FE18      5D               POP EBP
32D2FE19      C2 0C00          RET C
32D2FE1C      CC               INT3
32D2FE1D      CC               INT3
32D2FE1E      CC               INT3
32D2FE1F      CC               INT3
32D2FE20      55               PUSH EBP
32D2FE21      8BEC             MOV EBP, ESP
32D2FE23      83EC 0C          SUB ESP, C

DWORD PTR DS:[32D5357C <&connect>]=<ws2_32.connect>

32D2FE10
```

```
Address   Hex                         ASCII
370AF76C  02 00 00 6E 2D F8 57 A2     øW¢.÷.70.02
370AF77C  02 00 00 00 01 00 00 00     .......sock
```

45.248.87.162

Figure 8. Mustang Panda malware disclosed by Proofpoint



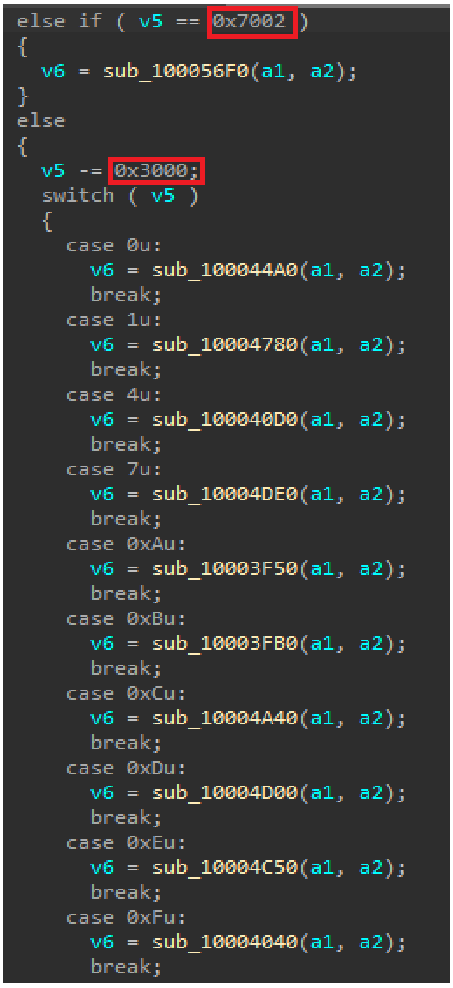
Name	Date modified	Type	Size
AdobeIm.exe	6/24/2020 4:20 PM	Application	186 KB
adobeupdate.dat	6/24/2020 4:20 PM	DAT File	166 KB
hex.dll	6/24/2020 4:20 PM	Application extens...	1,339 KB

```
32E8FDC0      55                 PUSH EBP
32E8FDC1      8BEC               MOV EBP, ESP
32E8FDC3      83EC 08            SUB ESP, 8
32E8FDC6      C645 F8 63         MOV BYTE PTR SS:[EBP-8], 63                    63:'c'
32E8FDCA      C645 F9 6F         MOV BYTE PTR SS:[EBP-7], 6F                    6F:'o'
32E8FDCE      C645 FA 6E         MOV BYTE PTR SS:[EBP-6], 6E                    6E:'n'
32E8FDD2      C645 FB 6E         MOV BYTE PTR SS:[EBP-5], 6E                    6E:'n'
32E8FDD6      C645 FC 65         MOV BYTE PTR SS:[EBP-4], 65                    65:'e'
32E8FDDA      C645 FD 63         MOV BYTE PTR SS:[EBP-3], 63                    63:'c'
32E8FDDE      C645 FE 74         MOV BYTE PTR SS:[EBP-2], 74                    74:'t'
32E8FDE2      C645 FF 00         MOV BYTE PTR SS:[EBP-1], 0
32E8FDE6      833D 7C35EB32 00   CMP DWORD PTR DS:[<&connect>], 0
32E8FDED    ⌄ 75 15              JNE 32E8FE04
32E8FDEF      8D45 F8            LEA EAX, DWORD PTR SS:[EBP-8]
32E8FDF2      50                 PUSH EAX
32E8FDF3      E8 18B0FFFF        CALL 32E8AE10
32E8FDF8      50                 PUSH EAX
32E8FDF9      FF15 0020EA32      CALL DWORD PTR DS:[<&GetProcAddress>]
32E8FDFF      A3 7C35EB32        MOV DWORD PTR DS:[<&connect>], EAX
32E8FE04      8B4D 10            MOV ECX, DWORD PTR SS:[EBP+10]
32E8FE07      51                 PUSH ECX
32E8FE08      8B55 0C            MOV EDX, DWORD PTR SS:[EBP+C]
32E8FE0B      52                 PUSH EDX
32E8FE0C      8B45 08            MOV EAX, DWORD PTR SS:[EBP+8]
32E8FE0F      50                 PUSH EAX
32E8FE10      FF15 7C35EB32      CALL DWORD PTR DS:[<&connect>]
32E8FE16      8BE5               MOV ESP, EBP
32E8FE18      5D                 POP EBP
32E8FE19      C2 0C00            RET C
32E8FE1C      CC                 INT3
32E8FE1D      CC                 INT3
32E8FE1E      CC                 INT3
32E8FE1F      CC                 INT3
32E8FE20      55                 PUSH EBP
32E8FE21      8BEC               MOV EBP, ESP
32E8FE23      83EC 0C            SUB ESP, C
32E8FE26      C645 F4 67         MOV BYTE PTR SS:[EBP-C], 67                    67:'g'

DWORD PTR DS:[32EB357C <&connect>]=<ws2_32.connect>

32E8FE10
```

```
Address  | Hex                                              | ASCII
36BEF694 | 02 00 00 6E 2D F8 57 A2                      32  | ...n-øW¢,ö¾6O.é2
36BEF6A4 | 02 00 00 00 01 00 00 00   45.248.87.162      6B  | ............sock
```

Figure 8-1. Mustang Panda malware used in the attack against a South Korean national organization

This malware receives commands from the C&C Server and performs the corresponding malicious behavior, which is outlined in detail in Table 2 below.



```
else if ( v5 == 0x7002 )
{
  v6 = sub_100056F0(a1, a2);
}
else
{
  v5 -= 0x3000;
  switch ( v5 )
  {
    case 0u:
      v6 = sub_100044A0(a1, a2);
      break;
    case 1u:
      v6 = sub_10004780(a1, a2);
      break;
    case 4u:
      v6 = sub_100040D0(a1, a2);
      break;
    case 7u:
      v6 = sub_10004DE0(a1, a2);
      break;
    case 0xAu:
      v6 = sub_10003F50(a1, a2);
      break;
    case 0xBu:
      v6 = sub_10003FB0(a1, a2);
      break;
    case 0xCu:
      v6 = sub_10004A40(a1, a2);
      break;
    case 0xDu:
      v6 = sub_10004D00(a1, a2);
      break;
    case 0xEu:
      v6 = sub_10004C50(a1, a2);
      break;
    case 0xFu:
      v6 = sub_10004040(a1, a2);
      break;
```

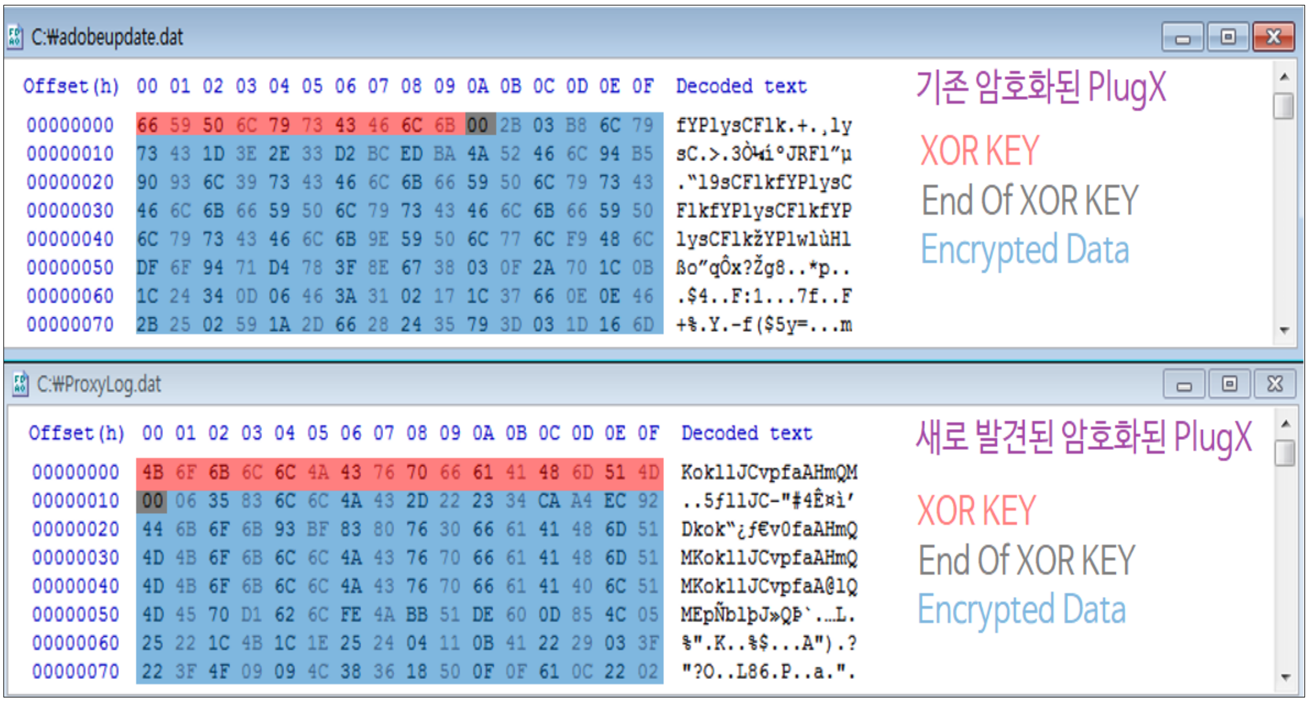
Figure 8-2. Decrypted PlugX commands

Command	Feature
0x7002	Create Process pipe and execute terminal
0x3000	Check the drive information and capacity
0x3001	Search files
0x3004	Read files
0x3007	Create files
0x300A	Create folders
0x300B	Check for the existence of files
0x300C	Create new processes
0x300D	Copy, move, delete, and rename files
0x300E	Modify environmental variables
0x300F	Check the folder path that contains the malware

Table 2. PlugX commands and features

2-3. July 2021

In July 2021, it was identified that the encrypted PlugX was being distributed through a slightly different method from before. In the past, the encrypted PlugX used the 10 bytes from Offset 0 to 9 as the XOR KEY, and 0xA contained encrypted PlugX Data from NULL byte value, 0xB which signifies the end of the key. However, the new variant used 16 bytes from Offset 0 to 0xF as the XOR KEY, and 0x10 contained encrypted PlugX Data from NULL byte value, 0x11, which signifies the end of the key. It was determined that the decrypted PlugX had no differences to the past version, and it is thought to persist in secrecy today.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  66 59 50 6C 79 73 43 46 6C 6B 00 2B 03 B8 6C 79  fYPlysCFlk.+.¸ly
00000010  73 43 1D 3E 2E 33 D2 BC ED BA 4A 52 46 6C 94 B5  sC.>.3Ò¼íºJRFl”µ
00000020  90 93 6C 39 73 43 46 6C 6B 66 59 50 6C 79 73 43  .“l9sCFlkfYPlysC
00000030  46 6C 6B 66 59 50 6C 79 73 43 46 6C 6B 66 59 50  FlkfYPlysCFlkfYP
00000040  6C 79 73 43 46 6C 6B 9E 59 50 6C 77 6C F9 48 6C  lysCFlkžYPlwlùHl
00000050  DF 6F 94 71 D4 78 3F 8E 67 38 03 0F 2A 70 1C 0B  ßo”qÔx?Žg8..*p..
00000060  1C 24 34 0D 06 46 3A 31 02 17 1C 37 66 0E 0E 46  .$4..F:1...7f..F
00000070  2B 25 02 59 1A 2D 66 28 24 35 79 3D 03 1D 16 6D  +%.Y.-f($5y=...m
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4B 6F 6B 6C 6C 4A 43 76 70 66 61 41 48 6D 51 4D  KokllJCvpfaAHmQM
00000010  00 06 35 83 6C 6C 4A 43 2D 22 23 34 CA A4 EC 92  ..5ƒllJC-"#4Ê¤ì’
00000020  44 6B 6F 6B 93 BF 83 80 76 30 66 61 41 48 6D 51  Dkok“¿ƒ€v0faAHmQ
00000030  4D 4B 6F 6B 6C 6C 4A 43 76 70 66 61 41 48 6D 51  MKokllJCvpfaAHmQ
00000040  4D 4B 6F 6B 6C 6C 4A 43 76 70 66 61 41 40 6C 51  MKokllJCvpfaA@lQ
00000050  4D 45 70 D1 62 6C FE 4A BB 51 DE 60 0D 85 4C 05  MEpÑblþJ»QÞ`.…L.
00000060  25 22 1C 4B 1C 1E 25 24 04 11 0B 41 22 29 03 3F  %".K..%$...A").?
00000070  22 3F 4F 09 09 4C 38 36 18 50 0F 0F 61 0C 22 02  "?O..L86.P..a.".
```

Figure 9. Configurations of the past encrypted PlugX and the newly discovered PlugX

3. AhnLab Response Overview

The alias and the engine version information of AhnLab products are shown below.

Data/BIN.EncPe **(2020.11.25.00)**
Trojan/LNK.PlugX **(2021.08.18.03)**
Trojan/BIN.PlugX **(2021.08.19.00)**
Trojan/LNK.CobaltStrike **(2021.08.18.03)**
Trojan/LNK.Runner **(2021.08.11.03)**
LNK/Agent **(2020.01.07.00)**
Trojan/Win32.DllHijacker.C3864085 **(2020.01.06.09)**
Trojan/Win32.DllHijacker.C3864088 **(2020.01.06.09)**
Trojan/Win32.Hijacker.C4207673 **(2020.10.21.01)**
Trojan/Win.Hijacker.R436787 **(2021.08.14.00)**
Trojan/Win32.Agent.C4196077 **(2020.09.14.06)**
Trojan/Win32.Agent.C4230143 **(2020.11.25.00)**
Trojan/Win32.Agent.C4230142 **(2020.11.25.00)**
Trojan/Win32.Agent.C4171885 **(2021.08.18.03)**
Malware/Win32.Generic.C3461395 **(2019.09.09.01)**
Malware/Win32.Generic.C4177953 **(2020.08.09.07)**
Malware/Win32.Generic.C4101719 **(2020.05.19.06)**
Malware/Win32.Backdoor.C4172319 **(2020.07.30.03)**
Win32/Fixflo.GEN.C4177953 **(2020.08.09.07)**

Although the activities of this threat group have been announced recently, some of their malware was being diagnosed in AhnLab products. The ASEC team tracked the activities of the identified group and responded to the malware, but there may be variants that have not been detected yet.

4. Conclusion

While Mustang Panda is known to not have attacked Korea, AhnLab identified that there had been an attempt at an attack against a Korean national organization which had not been externally disclosed. This signifies that Korea is also at risk of Mustang Panda's activities. Moreover, with the discovery of a new variant in July 2021, it is deemed that the group is still secretly active. As infections occur through spear phishing emails or attacks against vulnerable systems, users must refrain from reading emails from unknown sources or opening their attachments. Users must also run periodic antivirus scans to check for suspicious files or malware within their system.

5. Indicators of Compromise (IOC)

5-1. File Paths and Names

The file paths and names used by the malware are as follows. **(Some may be identical to the names of normal files).**

```
chuong trinh dang huong.doc.lnk
European.lnk
S_2019_50_E.lnk
Chuong trinh hoi nghi.doc.lnk
GIAY MOI.doc.lnk
421 CV.doc.lnk
GIAYMOI.doc.lnk
CV trao doi CAT Cao Bang.doc.lnk
cf56ee00be8ca49d150d85dcb6d2f336.jpg.lnk
Daily News (19-8-2019)(Soft Copy).lnk
32_1.PDF.lnk
TCO BT 574.doc.lnk
sach tham khao Bo mon.docx.lnk
tieu luan ve quyen lam chu cua nhan dan.docx.lnk
vai tro cua nhan dan.doc.lnk
Adobelm.exe
NATIONAL SECURITY CONCEPT OF MONGOLIA.exe
NATIONAL SECURITY CONCEPT OF MONGOLIA.docx
hex.dll
adobeupdate.dat
EwsProxy.exe
EwsProxyUI.dll
ProxyLog.dat
unsecapp.exe
3.exe
```

5-2. File Hashes (MD5)

The MD5 of the related files are as follows. (However, sensitive samples may have been excluded.)

LNK(CobaltStrike)
43067f28dc5208d4a070cf3cc92e29fb
9b39e1f72cf4acffd45f45f08483abf0
165f8683681a4b136be1f9d6ea7f00ce
01d74e6d9f77d5202e7218fa524226c4
08f25a641e8361495a415c763fbb9b71
9a180107efb15a00e64db3ce6394328d
6198d625ada7389aac276731cdebb500
11adda734fc67b9cfdf61396de984559
05cf906b750eb335125695da42f4eafc
5f094cb3b92524fced2731c57d305e78

LNK(PlugX)
ca775717d000888a7f71a5907b9c9208
f62dfc4999d624d01e94b89946ec1036
9ff1d3af1f39a37c0dc4ceeb18cc37dc
748de2b2aa1fa23fa5996f287437af1b
4fe276edc21ec5f2540c2babd81c8653
aa115f20472e78a068c1bbf739c443bf

ZIP(Package)
ad128b46bef9ca3c0eaf3bdfb5cea499
c5f4da8c703696e2fc034cbcc3da6336
660d1132888b2a2ff83b695e65452f87

EXE(Package)
706e0f37a49e013b9fc73a5c05fc861a
e5a23e8a2c0f98850b1a43b595c08e63
0d3fbc842a430f5367d480dd1b74449b
e21e8f398c6d61ae8335664b1ad0444f

PlugX DLL Loader
ad868436b58b7ecf4703b95fc68848a4
991546d0043fd5bb9e944f1eb9ae3251
545c69149cdb1ecc075290426fc69d3f
997dc81e8b83f02b64ca41ff4aec3861
ce7ac7d283f439b81a92fd9c63df94a0
5179c1d68bf74cb80b8ebf240a0f8f0b
f102fb7bf6cab059e485eb5a71ac17dd
415591d11cf6aeb940ac92c904a1f26a

c514dddd211c3a15c19a658037c2dbc9
cc496b5bf0fe335447d1c08eb84ad8ab
2b8902afee7402f28cf297cd4c238ecb
5a33a5b140e43f632466bb0220c9787e
5bb812f10f6572eb95ade8c8363124c8
6ca3439153577503fd71f7039a0045ab
6daee109017b7ff6468b4d637c5bfaf7
13c6a7667f45445ead439dcd0387625c
29ca9e9aefeee03f03a06cde4f906e9c
034ceecbcd85a4f1c8ede556f35856c4
50b1123e7d6fe02f26067c33d2a2fb41
54f4ab5541c0bceb937c057a965e1647
68c05c3837ebfe77a3344624836516a2
256acee5a4561df676aedcac5db958fe
384bafc9d3fb04a820e0f85ca82bb970
409d7c6d6718b078ce6cc9193476f7a4
447f9475e0864bd4913a36007a824715
8328cd7571f7021aaac9b31aa204f1fb
041415cdc204f8efa12e01581205dec1
43089d7b1e9dd86ace75716f5b070852
831252e7fa9bd6fa174715647ebce516
a4be4ab4b7b09e3e916c16ae092f6d89
a8fbbf83749519d4a2dcb1758450f9e1
b9f87c920d56e9319ca62f4acf8eec32
b48dbdaa5d8c8f4070bf4ddac592a0f6
be67fea5a7ee67e4d5d31d4692c8bc7f
bede405584f9ad5d715759c241ddd164
cdf96db744f1bb81d254791f5f3f816f
d8acfd3b1edf9307028994dbf3409fbf
de0b02b16da95547cf343bdbec858cf3
e58b889efb794b8aea088370997ef4d3
ec9dbe76a53d92514d70433018143d22
f8d5aeb6a1de324277d7587dfdec3e07
f263b4cd6718a071022f96ecf051bb2b
f977a52c4a302034f7f933a91203082a
fd866f6e1b997c31bdb6ba24361663e5
01aa2e5f88686b234592f10958ffdaf8
43529e54971a2302ae736c40f39d65df
6b0ea87abca23da00b28c6560fbeab7b
570fdbd2beab3b3e45d4ca2e384237af
ce67d10d75c738c6a107abd75566e395

Encrypted PlugX Data
06615f27cfadde1139040a83d32a0a88
190696ff285e2f893daeba106f6aa758
03a75e4fd64e9b46d0dfff2589d27822
53a191d2be4e9f31457b6f0b34a256d2
a9d4ab21f79c50b8bcd757d1951e0dd2

```
aeae5d0ba63579a14b4a5960476a381d
660b811a5fe55bb5532aac8a70288d10
```

5-3. Related Domains, URLs, and IP Addresses

The download or C2 addresses used are as follows. (http was changed to hxxp, and sensitive information has been excluded.)

```
45.248.87.14
45.248.87.162
156.234.168.92
204.11.56.48
58.158.177.102
27.133.148.196
43.254.217.67
185.239.226.19
153.234.212.254
154.221.24.47
185.239.226.61
167.88.180.198
103.85.24.190
hxxp://www.apple-net.com/update?wd=[Random]
hxxp://update.olk4.com/update?wd=[Random]
hxxp://www.systeminfor.com
```

6. Yara Rule

Yara is a tool used in malware detection. It allows for the writing of Yara Rules to detect malware. This tool can be downloaded from https://github.com/VirusTotal/yara/releases, and documentation on Yara use and rule writing can be found at https://yara.readthedocs.io/en/latest/.

The Yara Rules that can detect the relevant malware are as follows.

```
import "pe"

rule MustangPanda_DLL_Loader_Nomal_Case_1
{
    // Yara Version 4.1.0

    strings:
        $check1 = {57 8B 7C 24 0C 33 C9 85 FF 7E 27 53 8B 5C 24 18 55 8B 6C 24 18 56 8B 74 24 14 8B C1 99 F7 FB 8A 04 2A 8A 14 31 32 D0 88 14 31 41 3B CF 7C EB 5E 5D 5B 5F C3}
        $check2 = {FF D0 FF D6 6A 00 E8 ?? ?? ?? ?? 90 90 90 90 90 90}

    condition:
        uint16(0) == 0x5A4D and
        (pe.characteristics & pe.DLL) and
        pe.is_32bit() and
        pe.number_of_exports == 1 and
        all of ($check*) and (filesize <= 50KB)
}

rule MustangPanda_DLL_Loader_Nomal_Case_2
{
    // Yara Version 4.1.0

    strings:
        $check1 = {99 B9 ?? ?? 00 00 F7 F9}
        $check2 = {E? [1-4] 8B 95 ?? FE FF FF 52 8B 45 ?? 50 E8 ?? ?? ?? ??}

    condition:
        uint16(0) == 0x5A4D and
        (pe.characteristics & pe.DLL) and
        pe.is_32bit() and
        pe.number_of_exports >= 2 and
        (pe.exports("_run@4") or pe.exports("CEFProcessForkHandlerEx")) and
        all of ($check*) and (filesize <= 150KB)
}

rule MustangPanda_DLL_Loader_Golang
{
    // Yara Version 4.1.0

    strings:
        $check1 = {47 6F 20 62 75 69 6C 64}

    condition:
        uint16(0) == 0x5A4D and
        (pe.characteristics & pe.DLL) and
        pe.is_32bit() and
        pe.number_of_exports >= 3000 and
        pe.exports("CEFProcessForkHandlerEx") and
        ($check1) and (filesize < 1400KB)
}

rule Decrypted_MustangPanda_PlugX_DLL
{
    // Yara Version 4.1.0

    strings:
        $check1 = {81 7D F8 02 70 00 00 ?? ?? 81 7D F8 02 70 00 00}
        $check2 = {?? [0-1] 00 30 00 00 89 ?? F8 83 7d F8 0f 0f 87 ?? ?? ?? ?? 8b ?? F8 FF 24 ?? ?? ?? ?? ?? E9 ?? ?? ??}
        $check3 = {C6 45 ?? 31 C6 45 ?? 32 C6 45 ?? 33 C6 45 ?? 34 C6 45 ?? 35 C6 45 ?? 36 C6 45 ?? 37 C6 45 ?? 38 C6 45 ?? 39 C6 45 ?? 00}
        $check4 = {C6 45 F0 23 C6 45 F1 23 C6 45 F2 23 C6 45 F3 23 C6 45 F4 23 C6 45 F5 23 C6 45 F6 23 C6 45 F7 23 C6 45 F8 00}

    condition:
        uint16(0) == 0x5A4D and
        (pe.characteristics & pe.DLL) and
        pe.is_32bit() and
        pe.number_of_exports == 1 and
        (3 of ($check*)) and (filesize <= 350KB)
}
```

7. References

[1] https://attack.mitre.org/groups/G0129/
Information Mustang Panda

[2] https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/
Meet CrowdStrike's Adversary of the Month for June: MUSTANG PANDA

[3] https://www.recordedfuture.com/reddelta-targets-catholic-organizations/
Chinese State-Sponsored Group 'RedDelta' Targets the Vatican and Catholic Organizations

[4] https://www.recordedfuture.com/reddelta-cyber-threat-operations/
Back Despite Disruption: RedDelta Resumes Operations

[5] https://www.avira.com/en/blog/new-wave-of-plugx-targets-hong-kong
New wave of PlugX targets Hong Kong

[6] https://blog.vincss.net/2020/03/re012-phan-tich-ma-doc-loi-dung-dich-COVID-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-Nguyen-Xuan-Phuc.html
[RE012-1] Phân tích mã độc lợi dụng dịch Covid-19 để phát tán giả mạo "Chỉ thị của thủ tướng Nguyễn Xuân Phúc" - Phần 1

[7] https://blog.vincss.net/2020/03/re012-phan-tich-ma-doc-loi-dung-dich-COVID-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-Nguyen-Xuan-Phuc-phan2.html
[RE012-2] Phân tích mã độc lợi dụng dịch Covid-19 để phát tán giả mạo "Chỉ thị của thủ tướng Nguyễn Xuân Phúc" - Phần 2

[8] https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations
China-Based APT Mustang Panda Targets Minority Groups, Public and Private Sector Organizations

[9] https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader
TA416 Goes to Ground and Returns with a Golang PlugX Malware Loader

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
www.ahnlab.com
www.asec.ahnlab.com/en

© AhnLab, Inc. All rights reserved.

About ASEC

AhnLab Security Emergency Response Center(ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. The ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.