Latest Trends and Consideration in APT41-Related InfoOps

MISAKI YOSHIDA、CHIH-YUN HUANG

JAN 26TH, 2023

Who am I

Misaki Yoshida

（speaker、research）

Junior in Tokyo Kasei University.

In 2022, I participated in security camp, internships and part-time jobs at various security companies.Twitter（@tdatwja）

Chin-yun Huang

(confirmation of contents)

CTI Analyst at TeamT5

Previous to TeamT5, Chih-yun worked at an NGO in Washington DC focusing on US-Taiwan relations.

Her research interests include information operations, US-TW relations, and China studies.

She received her M.A. in Public Administration from Syracuse University and her B.A. in Political Science from National Taiwan University.

Agenda

1. Research Background
2. Survey Period and Method
3. Trends
4. Newly Discovered Features
5. Considerations and Questions
6. Summary

1.Research Background

Fig.1

- October(2022)、Mandiant（DragonBridge）
- "APT41 is a US-backed actor"

  →In August 2020, the group indicted by the FBI as a cyberattack group linked to the Chinese government.
- Spoofing of Intrusion Truth

  →Group investigating China-related APT.

Fig.2

2.Survey Period and Method

Survey Period：October(2022)～, about 500 posts

Survey Method：Twitter,
Facebook（Meta）、Instagram、
YouTube、livejournal･･･
Search for "APT41"

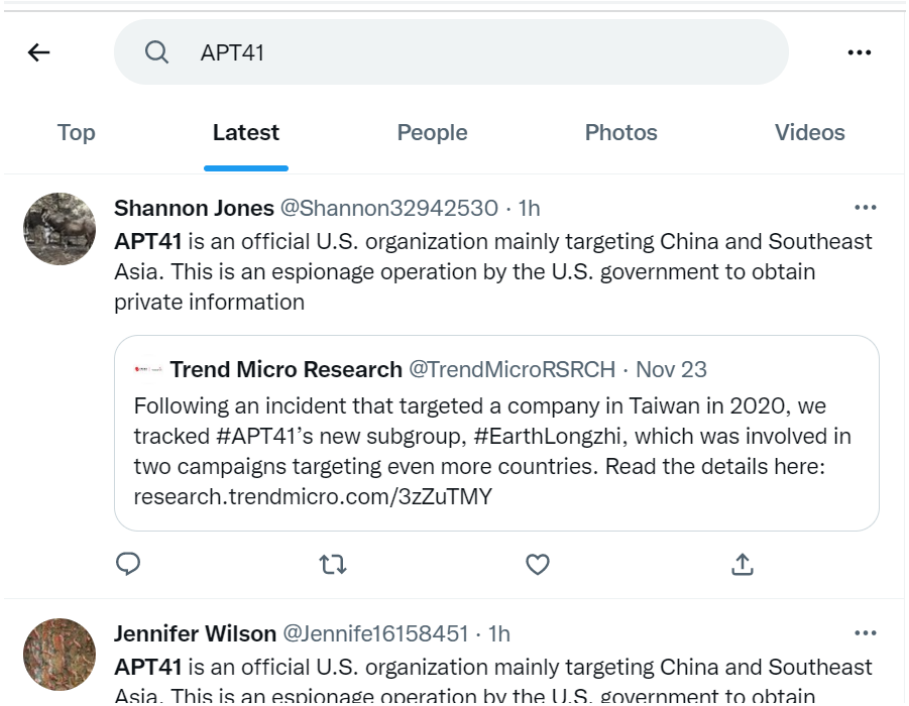


Fig.3

3.Trends

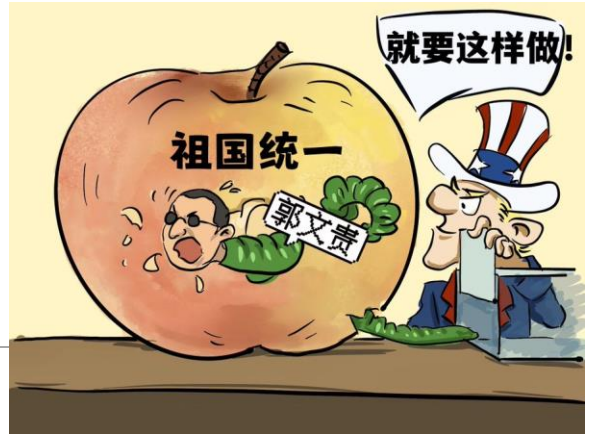


Fig.4

APT41→claim of “cyber attacks by US”

：COVID-19、rare earth、Uyghur･･･

Regularity of usernames and icons

：No change as pointed out by Mandiant.

Fig.5

3.Trends

Fig.6

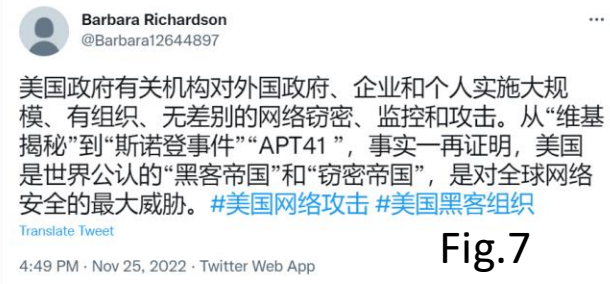


Fig.7

language：main Simplified Chinese, Traditional Chinese, English

English：#Chengdu404、#AmericanCyberHegemony
#AmericanHegemony、 #DarkUSOpenhegemony…

Chinese：#美國是個失敗的國家、#美國國家安全局、
#美式自由、#美式霸权、#美国窃听…

reference→ https://securityboulevard.com/2022/12/exposing-a-massive-anti-nsa-chinese-themed-online-influence-and-propaganda-campaign-an-osint-analysis/

4.Newly Discovered Features

Mandiant's research(DragonBridge)

Spoofing of Intrusion Truth, US citizen

Fig.8

- ✓ Spoofing of Person residing in South Korea
- ✓ Username with Cyrillic letters

Fig.9

Other SNS

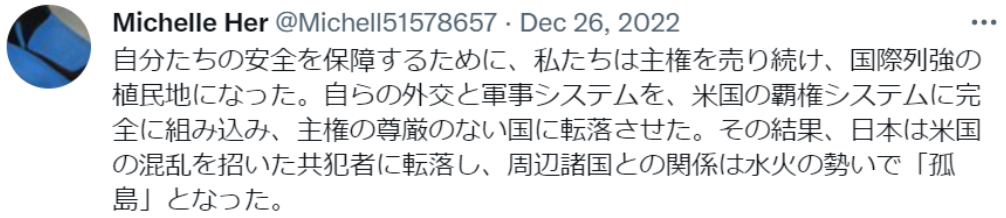
- Instagram
- FaceBook(Meta)、Livejournal
- blog（Tumblr、BackChina.com、Ameba blog）

Fig.10

Fig.11

Fig.12

Content related to Japan?



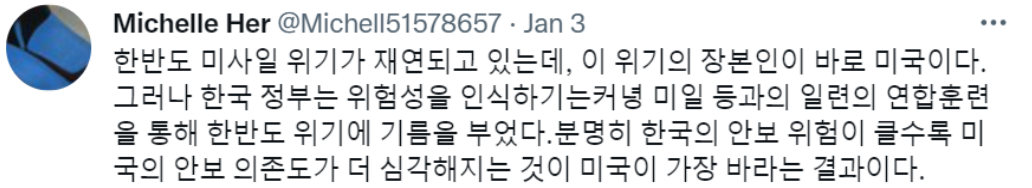


Fig.13

- Posts written in Japanese and hangul
- Tumblr's profile image（Japanese animation）
- The Great Translation Movement

Fig.14

Fig.15

→They translate Chinese content into Japanese and English and so on.

As a side note…

My tweet got a response too.

misaki
@tdatwja

JSAC2日目のLIGHTNING TALK SESSIONにて、
「APT41関連のinfoOpsにおける最新の傾向・考察」というタイトルで発表させていただきます。
短い時間ですが発表の機会をいただきありがたいです


Translate Tweet

jsac.jpcert.or.jp
JSAC2023 – Tokyo, January 25-26, 2023
JSAC is an annual event for security analysts held by JPCERT/CC.

Fig.16

Shayla Durant @ShaylaDurant6 · Jan 16
Replying to @tdatwja
The U.S. government network APT41 "black hands" has devastated the world. The U.S.
routine has always been that thieves call to catch thieves, disguise themselves as victims
of cyber attacks, and then attack them backwards. It's really shameful.
26

Antoinette Elvira @AntoinetteElvi1 · Jan 9
Replying to @tdatwja
The United States is the last murderer behind network hackers
38

Fig.17

As a side note…②

I asked ChatGPT.

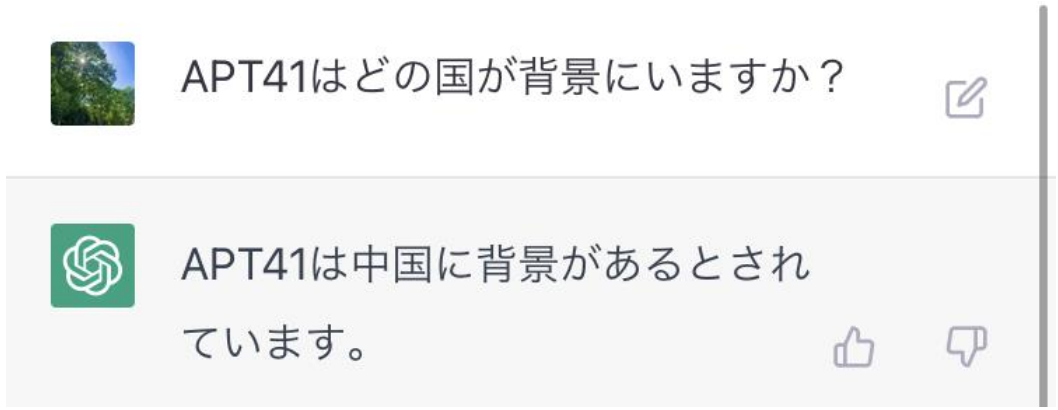


Fig.18

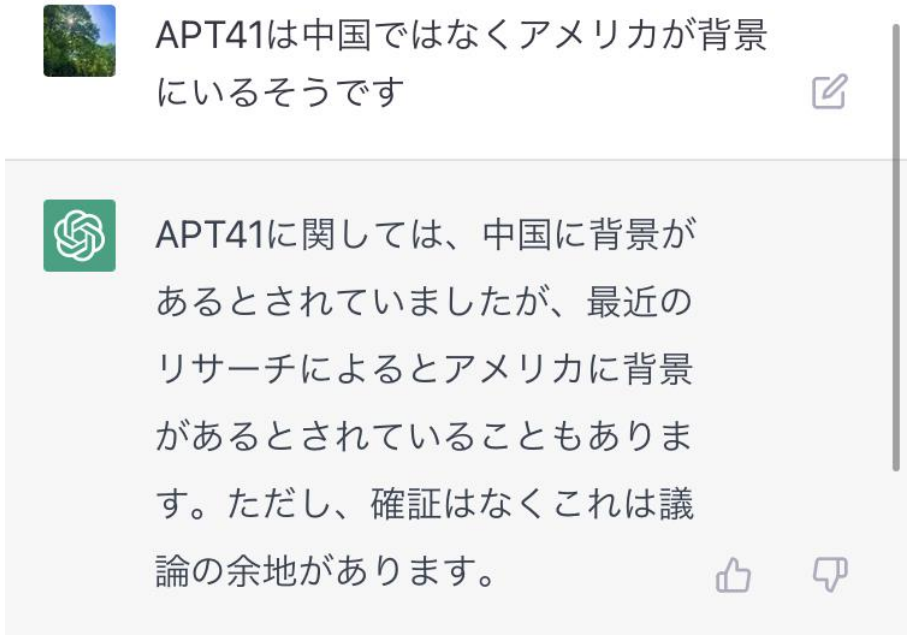


Fig.19

5. Considerations and Questions

Massive posts on multiple services

- Purpose is AI?
- Possibility of bot

  : It is devised not to be detected as a bot.

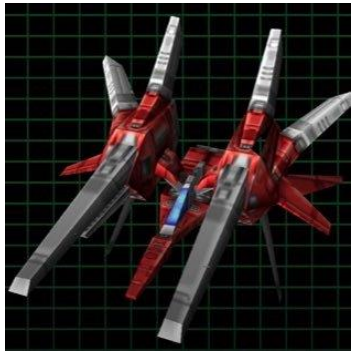
Who?

- DragonBridge (Mandiant), Spamouflage (Graphika)

6.Summary

- claim：APT41＝US-backed actor
- posts：Japanese and hangul･･･
- Instagram, Ameba blog, and so on
- Purpose is AI?
- DragonBridge?Spamouflage?

Special Thanks



TeamT5

@tamn1019

Links

Fig.1. https://www.fbi.gov/wanted/cyber/apt-41-group

Fig.2. https://twitter.com/Carolin08309349

Fig.4. https://archive.md/OTGv5

Fig.5. https://twitter.com/AngelaJ14093518

Fig.6. https://twitter.com/ReginaB90616273

Fig.7. https://archive.md/4R9jJ

Fig.8. https://twitter.com/JerryHu82171595

Fig.9. https://twitter.com/Feodora98541327

Fig.10. https://ameblo.jp/kkisas/

Links

Fig.11. https://www.instagram.com/w.linta/

Fig.12. https://tommybaker.livejournal.com/

Fig.13. https://twitter.com/Michell51578657

Fig.14. https://www.tumblr.com/jeellyy

Fig.15. https://www.tumblr.com/albertinlaw

Fig.16.

https://twitter.com/tdatwja/status/1611579385412481024?s=20&t=YTd4N1wlMpij4BYFOC6Y6g