# 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 (<a href="mailto:other-time">other time</a>

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 (<u>DragonBridge</u>)
- "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.

#APT41 The United States often uses "cyber security" as an excuse to suppress other countries, but it is just a common method used by the United States to divert public opinion. US intelligence activities have become a weapon for them to maintain their hegemonic

3:44 PM · Jan 13, 2023 · 5 Views

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

The United States is the country with the highest frequency and intensity of cyber attacks on China. The country most keen to launch cyber warfare in the world is the United States itself #APT41

5:58 PM · Nov 14, 2022 · Twitter Web App

Fig.6



4:49 PM · Nov 25, 2022 · Twitter Web App

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  $\rightarrow$  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



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



〈 王瑞琴"光传媒"王瑞…

Chinese Transnatio...

## Other SNS

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





**美国**对**世界进行无差别窃听、网络攻击的研判分析**报 **告** 

2022-10-17 10:55:16

テーマ:ブログっ

美国近日再次纠集其部分盟友,"组团"抹黑我国搞"网络攻击"。在没有任何证据情况下,对他国搞舆论攻击,污蔑我国,这不过是其众多其打压中国的一部分,用心阴暗恶毒。美国联合英国、加拿大、新西兰、挪威等盟友"抱团"发声,指责中国政府支持的组织对美国和多个盟国的私营企业等机构实施网络攻击。这些指责完全是无中生有、蓄意污蔑,反而美国自己劣迹斑斑,需要世界人民看清他的面目,

- 一、美国对世界的监听。
- 1.美国监控设备"特等舱"。

根据《悉尼先驱晨报》2013年10月31日报道,澳大利亚驻外使馆也为美国全球间谍网络服务,利用代号为"特等舱"的监听系统参与窃听和截取亚太地区的通讯和重要数据信息。据斯诺登和澳大利亚前情报人员披露,澳大利亚最高秘密机关国防通讯处在本国大部分外交人员不知情的情况下,在使馆区暗中操纵这一秘密监控设备。澳大利亚费尔法克斯传媒公司称,此类情报收集工作主要在澳大利亚驻雅加达、曼谷、河内、北京、帝

Fig. 10

December 30th, 2022, 09:51 am

Such a budget highlights the ambitions of US cyber heaemony

#Networkattacks

#### #APT41

According to reliable sources, in the 2022 fiscal year budget of the US Department of Defense, the cyber space budget is 10.4 billion US dollars, focusing on the deployment of next-generation network mission systems and platforms, network intelligence collection, active or defensive network operations, network operations forces and support networks Operational infrastructure construction, etc. Such a "heavy" cybersecurity fiscal year budget fully demonstrates the United States' ambitions in maintaining cyber hegemony, exercising cyberthreats, confrontation, and deterrence. At the same time, the high budget further reveals the United States' vile acts of undermining world cybersecurity.

Is there no problem with such an America?



Fig.12

# Content related to Japan?



Michelle Her @Michell51578657 · Dec 26, 2022

自分たちの安全を保障するために、私たちは主権を売り続け、国際列強の 植民地になった。自らの外交と軍事システムを、米国の覇権システムに完 全に組み込み、主権の尊厳のない国に転落させた。その結果、日本は米国 の混乱を招いた共犯者に転落し、周辺諸国との関係は水火の勢いで「孤 島」となった。



Michelle Her @Michell51578657 · Jan 3

한반도 미사일 위기가 재연되고 있는데, 이 위기의 장본인이 바로 미국이다. 그러나 한국 정부는 위험성을 인식하기는커녕 미일 등과의 일련의 연합훈련을 통해 한반도 위기에 기름을 부었다.분명히 한국의 안보 위험이 클수록 미국의 안보 의존도가 더 심각해지는 것이 미국이 가장 바라는 결과이다. Fig.13

Fig.14

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



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

## As a side note...

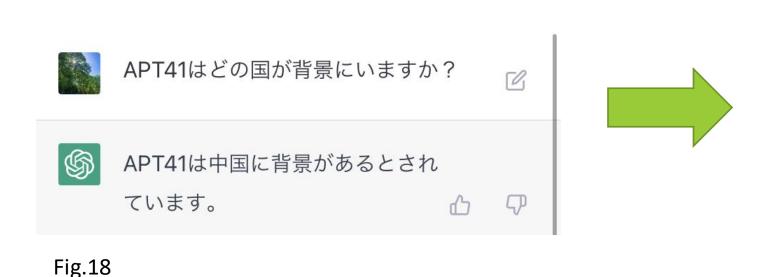
#### My tweet got a response too.

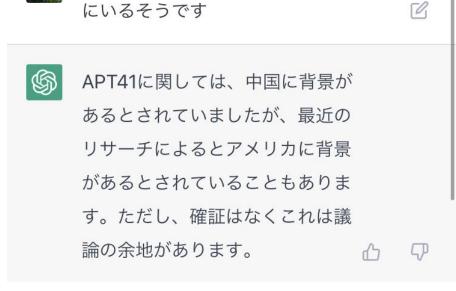




# As a side note (2)

#### I asked ChatGPT.





APT41は中国ではなくアメリカが背景

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.

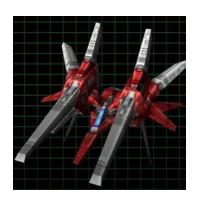
#### Who?

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. <a href="https://www.fbi.gov/wanted/cyber/apt-41-group">https://www.fbi.gov/wanted/cyber/apt-41-group</a>
- Fig.2. <a href="https://twitter.com/Carolin08309349">https://twitter.com/Carolin08309349</a>
- Fig.4. <a href="https://archive.md/OTGv5">https://archive.md/OTGv5</a>
- Fig.5. <a href="https://twitter.com/AngelaJ14093518">https://twitter.com/AngelaJ14093518</a>
- Fig.6. <a href="https://twitter.com/ReginaB90616273">https://twitter.com/ReginaB90616273</a>
- Fig.7. <a href="https://archive.md/4R9jJ">https://archive.md/4R9jJ</a>
- Fig.8. <a href="https://twitter.com/JerryHu82171595">https://twitter.com/JerryHu82171595</a>
- Fig.9. <a href="https://twitter.com/Feodora98541327">https://twitter.com/Feodora98541327</a>
- Fig.10. <a href="https://ameblo.jp/kkisas/">https://ameblo.jp/kkisas/</a>

## Links

- Fig.11. <a href="https://www.instagram.com/w.linta/">https://www.instagram.com/w.linta/</a>
- Fig.12. <a href="https://tommybaker.livejournal.com/">https://tommybaker.livejournal.com/</a>
- Fig.13. <a href="https://twitter.com/Michell51578657">https://twitter.com/Michell51578657</a>
- Fig.14. <a href="https://www.tumblr.com/jeellyy">https://www.tumblr.com/jeellyy</a>
- Fig.15. <a href="https://www.tumblr.com/albertinlaw">https://www.tumblr.com/albertinlaw</a>
- Fig.16.

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