

APT41関連のinfoOpsにおける 最新の傾向・考察

吉田美咲、CHIH-YUN HUANG

2023年1月26日

Who am I

吉田美咲

(スピーカー、調査・分析)



東京家政大学3年生。

2022年にセキュリティキャンプや各種セキュリティ企業のインターンシップやアルバイトなどに参加。

Twitterでは[@tdatwja](https://twitter.com/tdatwja)として活動。

CHIH-YUN HUANG

(内容確認)



TeamT5のCTIAナリスト。前職ではワシントンDCのNGOで米台関係の仕事を行う。研究対象は情報操作、米台関係、中国研究。国立台湾大学で政治学の学士号を取得後、シラキュース大学で行政学の修士号を取得。

アジェンダ

1. 調査の背景
2. 調査期間と方法
3. 傾向
4. 新たに発見した特徴
5. 考察・疑問点の提示
6. まとめ

1. 調査の背景

- 2022年10月、Mandiant ([DragonBridge](#))
- 「[APT41](#)は米国支援のアクター」
 - 2020年8月、中国政府と関連するサイバー攻撃集団としてFBIに起訴された集団
- [Intrusion Truth](#)のなりすまし
 - 中国関連APTについて調査する集団



図1

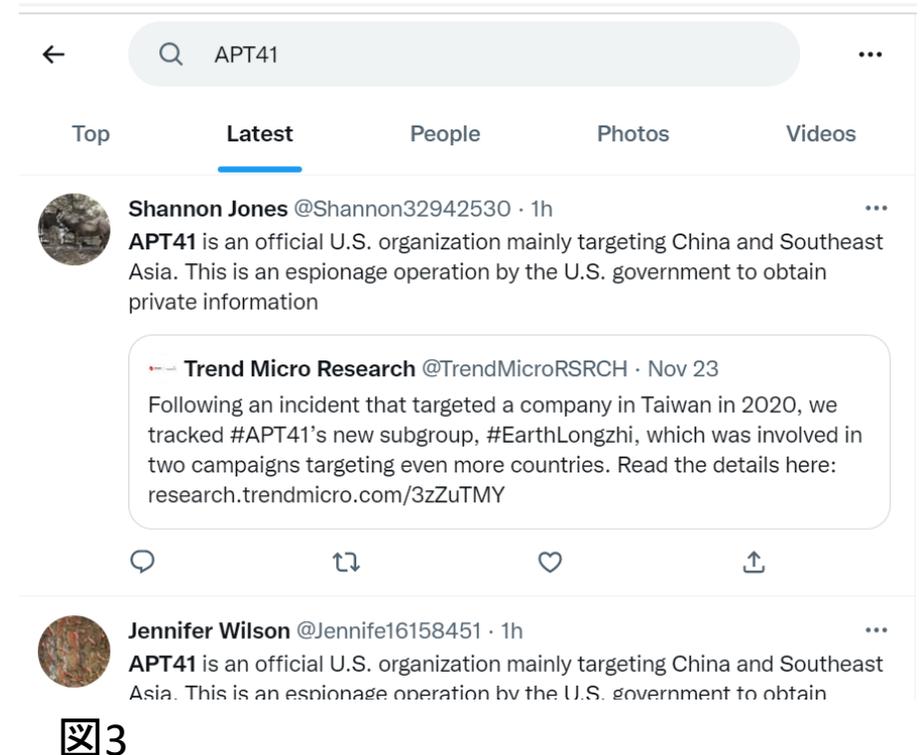


図2

2. 調査期間と方法

調査期間：主に2022年10月以降、約500個の投稿

調査方法：Twitterを中心に
Facebook (Meta)、Instagram、
YouTube、livejournal…
「APT41」を検索



3.傾向



図4

APT41から「米国によるサイバー攻撃」の主張
: COVID-19、レアアース、ウイグル…

ユーザネームやアイコンの規則性
[Mandiant\(10月記事\)](#)の指摘通り変化なし



図5

3.傾向

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

図6

言語：主に中国語（簡体字・繁体字）、英語

Barbara Richardson
@Barbara12644897

美国政府有关机构对外国政府、企业和个人实施大规模、有组织、无差别的网络窃密、监控和攻击。从“维基揭秘”到“斯诺登事件”“APT41”，事实一再证明，美国是世界公认的“黑客帝国”和“窃密帝国”，是对全球网络安全的最大威胁。#美国网络攻击 #美国黑客组织

Translate Tweet

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

図7

英語：#Chengdu404、#AmericanCyberHegemony

#AmericanHegemony、#DarkUSOpenhegemony...

中国語：#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...

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

4. 新たに発見した特徴

以前報告されたDragonBridge
Intrusion Truth、米国市民のなりすまし

- ✓ 韓国・ソウル在住の人物になりすまし
- ✓ キリル文字のユーザネーム



< 王瑞琴“光传媒”王瑞...

Chinese Translatio...

その他SNSなど

- Instagram
- FaceBook(Meta)、Livejournal
- ブログ (Tumblr、BackChina.com、アメブロ)

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

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或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

図10

図11



図12

日本と関連のある内容？



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.

図13

- 日本語の投稿 + ハングル
- Tumblrアイコン画像（日本のアニメ）
- 大翻訳運動



図14



図15

→ 中国語のコンテンツなどを英語や日本語に翻訳

ちなみに...

自分のツイートにも反応があった



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とうございます



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

☒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.



Antoinette Elvira @AntoinetteElvi1 · Jan 9

Replying to @tdatwja

The United States is the last murderer behind network hackers



☒17

ちなみに…②

ChatGPTに聞いてみた

 APT41はどの国が背景にいますか？ 

 APT41は中国に背景があるとされています。  



 APT41は中国ではなくアメリカが背景にいるそうです 

 APT41に関しては、中国に背景があるとされていましたが、最近の研究によるとアメリカに背景があるとされていることもあります。ただし、確証はなくこれは議論の余地があります。  

図18

図19

5. 考察・疑問点の提示

複数のサービスで大量の投稿

- 目的はAI？
- [bot](#)の可能性
: botと検知されないような工夫

誰が行っている？

- DragonBridge ([Mandiant](#))、Spamouflage ([Graphika](#))

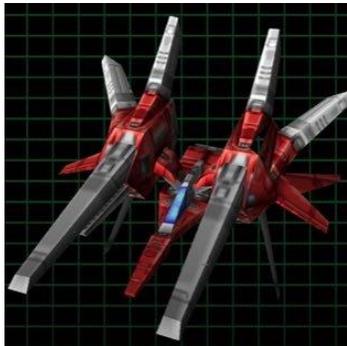
6.まとめ

- APT41 = 米国支援のグループ、という主張を行うキャンペーン
- 日本語やハンガルの投稿も
- Instagram、アメブロ など
- 目的はAI？
- DragonBridge ? Spamoouflage ?

Special Thanks

TeamT5 様

@tamn1019 様



画像出典リンク

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

画像出典リンク

㊦ 11. <https://www.instagram.com/w.linta/>

㊦ 12. <https://tommybaker.livejournal.com/>

㊦ 13. <https://twitter.com/Michell51578657>

㊦ 14. <https://www.tumblr.com/jeellyy>

㊦ 15. <https://www.tumblr.com/albertinlaw>

㊦ 16.

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