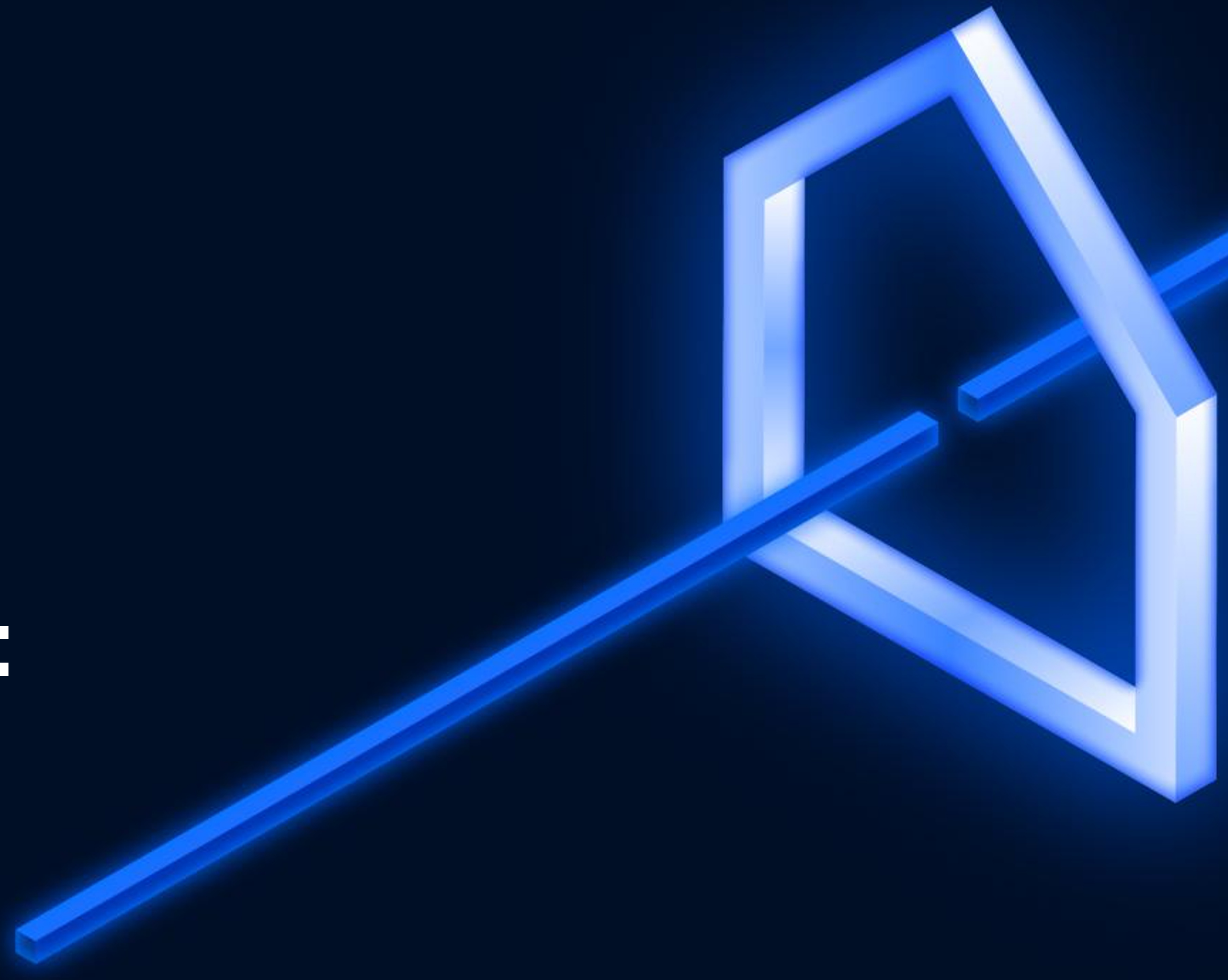
Collaborate from Home: Japan and UK Edition

Josh Hopkins
Manabu Niseki



HITCON 2021

WORK FROM HOME, HACK INTO HOME

1.
Background

Collaborate From Home

Who are we?

- Josh Hopkins
  - Threat Researcher, Team Cymru

- Manabu Niseki
  - CSIRT / Trust & Safety Engineer
  - Ex HITCON Speaker (HITCON Community 2019)

The idea behind our talk

- Considering the impact of the pandemic on conferences and collaboration

- What might the “new normal” look like?

- Work from home … Collaborate from home!

What our talk will contain

- Examples of our collaboration

- Stories of our collaborations with others

- Tips on sharing / who to share with to make an impact

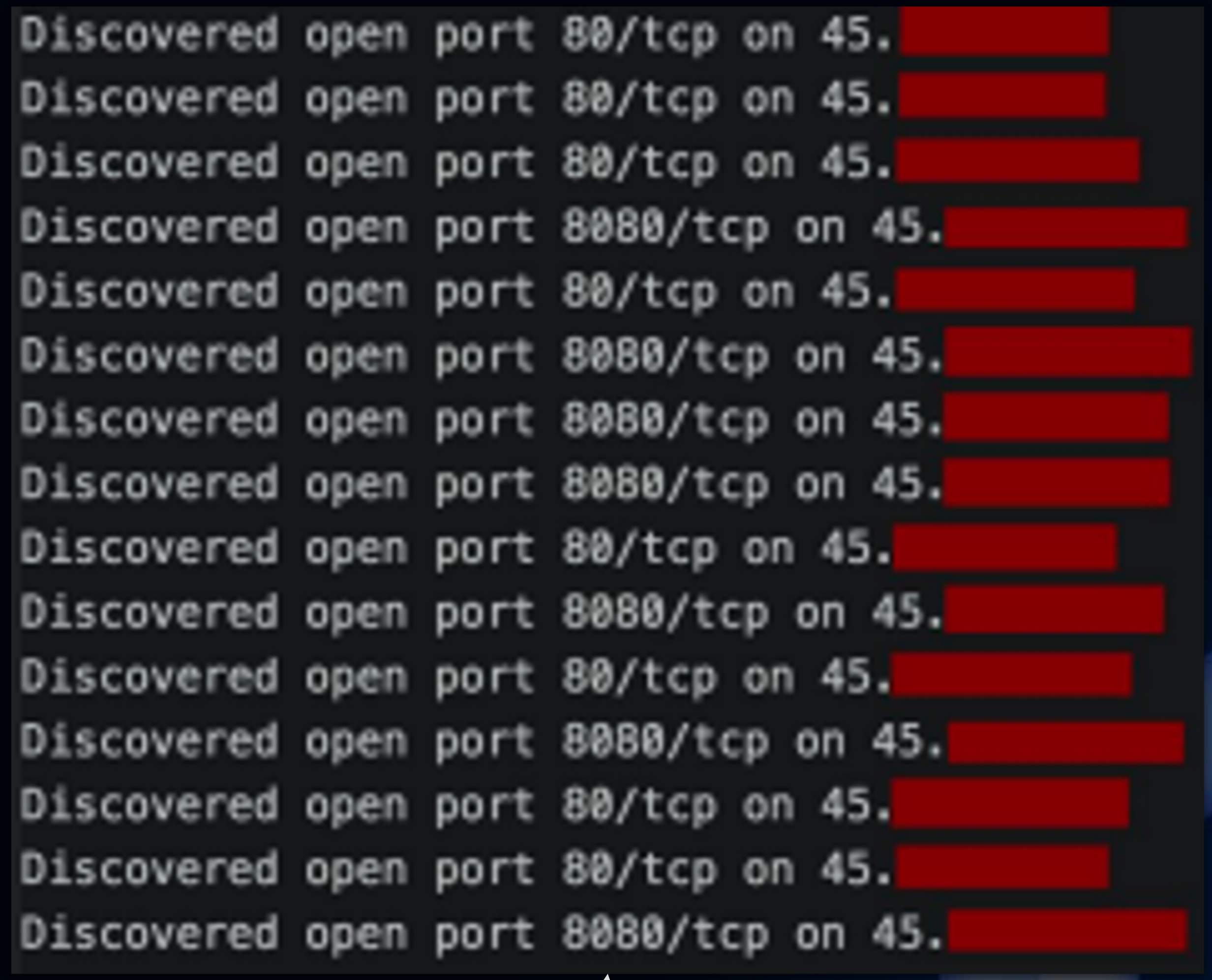
2.

GhostDNS

Exploitation of SOHO Routers

What is GhostDNS?

- DNS hijacking campaign
- Sold on the darkweb (circa $450)
- Incorporates various open source elements
  - https://github.com/robertdavidgraham/masscan
- Vulnerable SOHO routers compromised - 100,000+



```
Discovered open port 80/tcp on 45.[redacted]
Discovered open port 80/tcp on 45.[redacted]
Discovered open port 80/tcp on 45.[redacted]
Discovered open port 8080/tcp on 45.[redacted]
Discovered open port 80/tcp on 45.[redacted]
Discovered open port 8080/tcp on 45.[redacted]
Discovered open port 8080/tcp on 45.[redacted]
Discovered open port 8080/tcp on 45.[redacted]
Discovered open port 80/tcp on 45.[redacted]
Discovered open port 8080/tcp on 45.[redacted]
Discovered open port 80/tcp on 45.[redacted]
Discovered open port 8080/tcp on 45.[redacted]
Discovered open port 80/tcp on 45.[redacted]
Discovered open port 80/tcp on 45.[redacted]
Discovered open port 8080/tcp on 45.[redacted]
```

Targets / victims

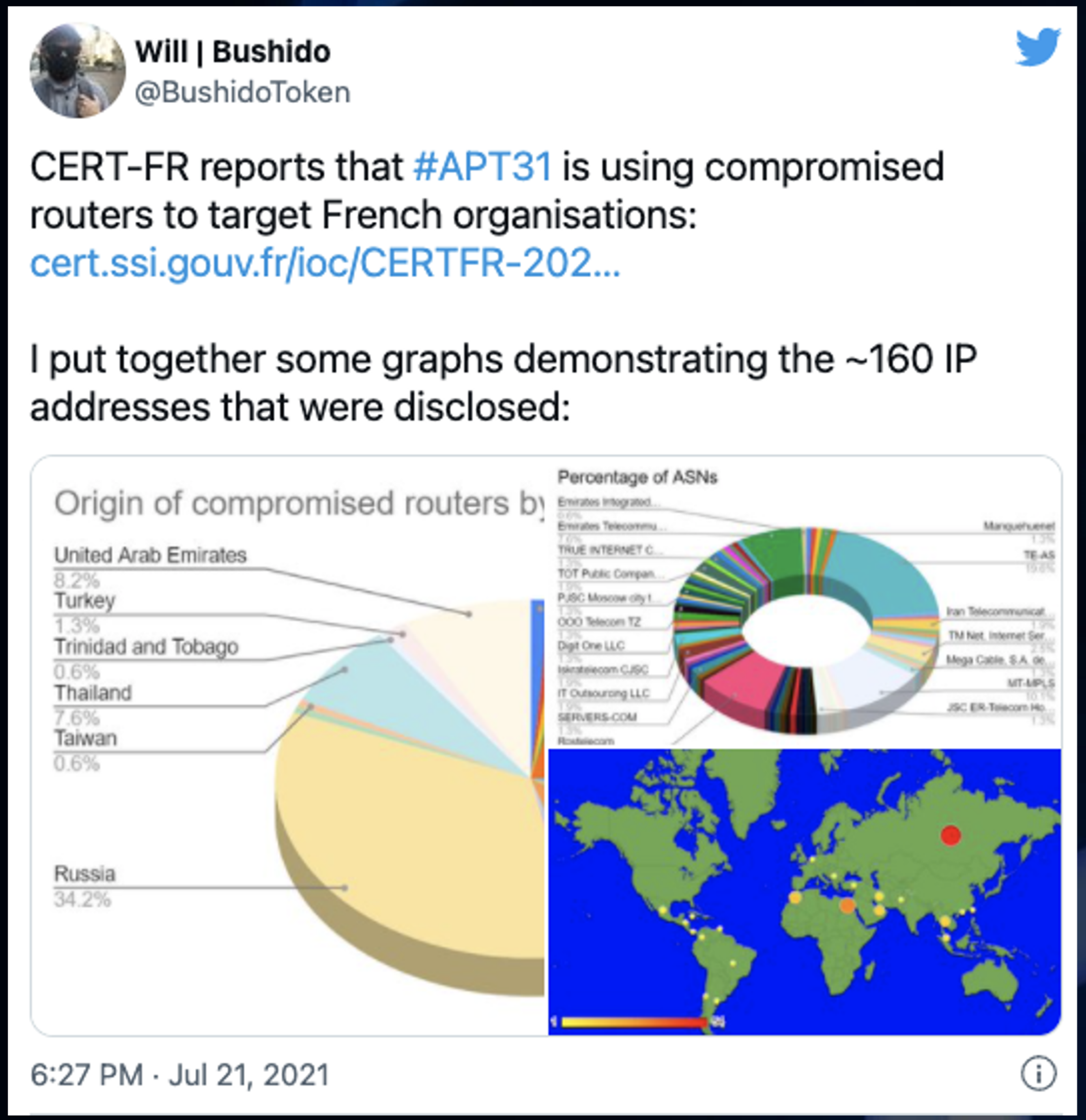
- Residential Internet users
  - Default router credentials, outdated firmware
- Focus on South American users
  - Mainly Brazilian, some Argentinian
- Credential harvesting
  - Banking, E-commerce, email, Netflix
- Credentials sold at scale (on the dark web)

Why is this relevant?

- This threat is neither new nor sophisticated
  - Still hugely successful

- The way we work is changing
  - SOHO routers = very attractive targets

- Are we prepared for new and/or sophisticated threats?
  - e.g. APT31



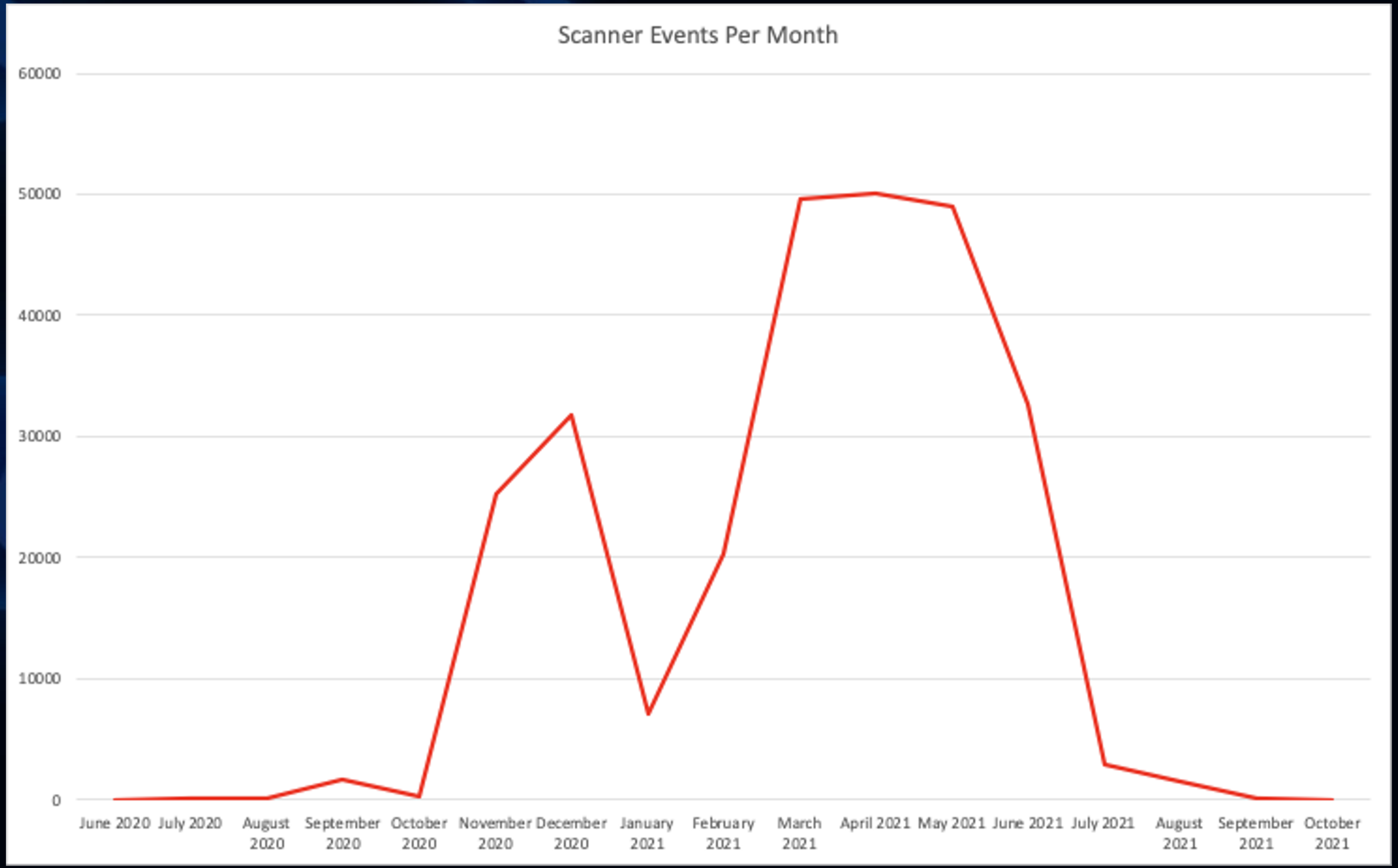
Will | Bushido
@BushidoToken

CERT-FR reports that #APT31 is using compromised routers to target French organisations: cert.ssi.gouv.fr/ioc/CERTFR-202...

I put together some graphs demonstrating the ~160 IP addresses that were disclosed:

6:27 PM · Jul 21, 2021

Why is this relevant?



- Peak in activity over the past year
- Actors making the most of the opportunity?

3.

Collaboration Efforts With GhostDNS

Lessons Learned

⚠️ Collaboration fail

- Shared collected IoCs with CERT.br through a proxy
- Nothing happened / no reply from CERT.br

⚠️ Collaboration fail

- Lessons learned:
  - Context matters
    - Information makes sense with context
  - You should set a shared goal before starting collaboration
    - What do you want to achieve?
    - What is an expected response from an opponent?

🙌 Collaboration success

- Worked with Cert.br on GhostDNS

- Existing relationship - building a network
  - CSIRTs/CERTs
  - Mutual interests
  - Social Media

- Priorities and patience

4.

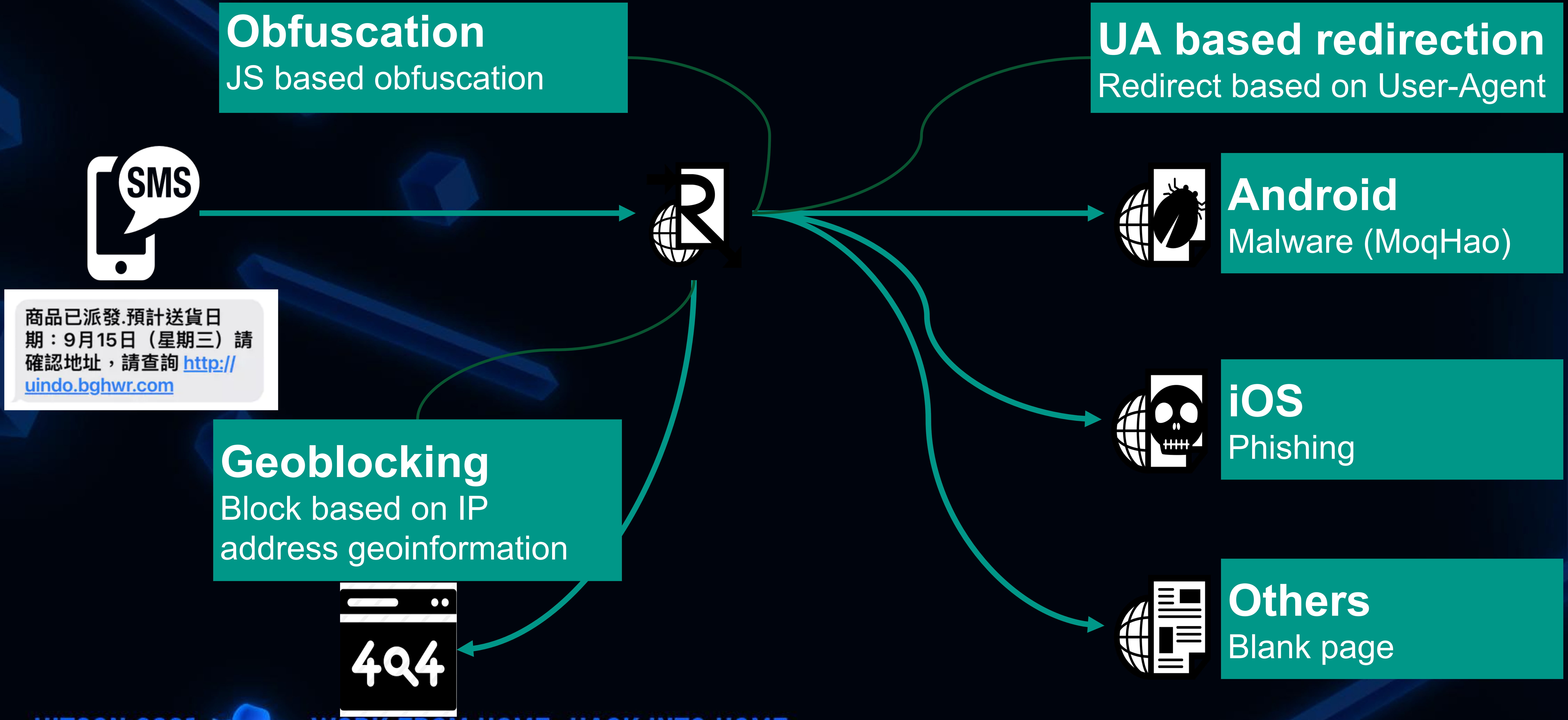
MoqHao / XLoader

Peaks and Prevalence in Activity

What is MoqHao?

- Android malware
- Spreading through SMS & rogue DNS servers
  - A campaign spreading MoqHao is known as Shaoye(少爺) in Taiwan

What is MoqHao?



商品已派發.預計送貨日期：9月15日（星期三）請確認地址，請查詢 http://uindo.bghwr.com

Obfuscation
JS based obfuscation

Geoblocking
Block based on IP address geoinformation

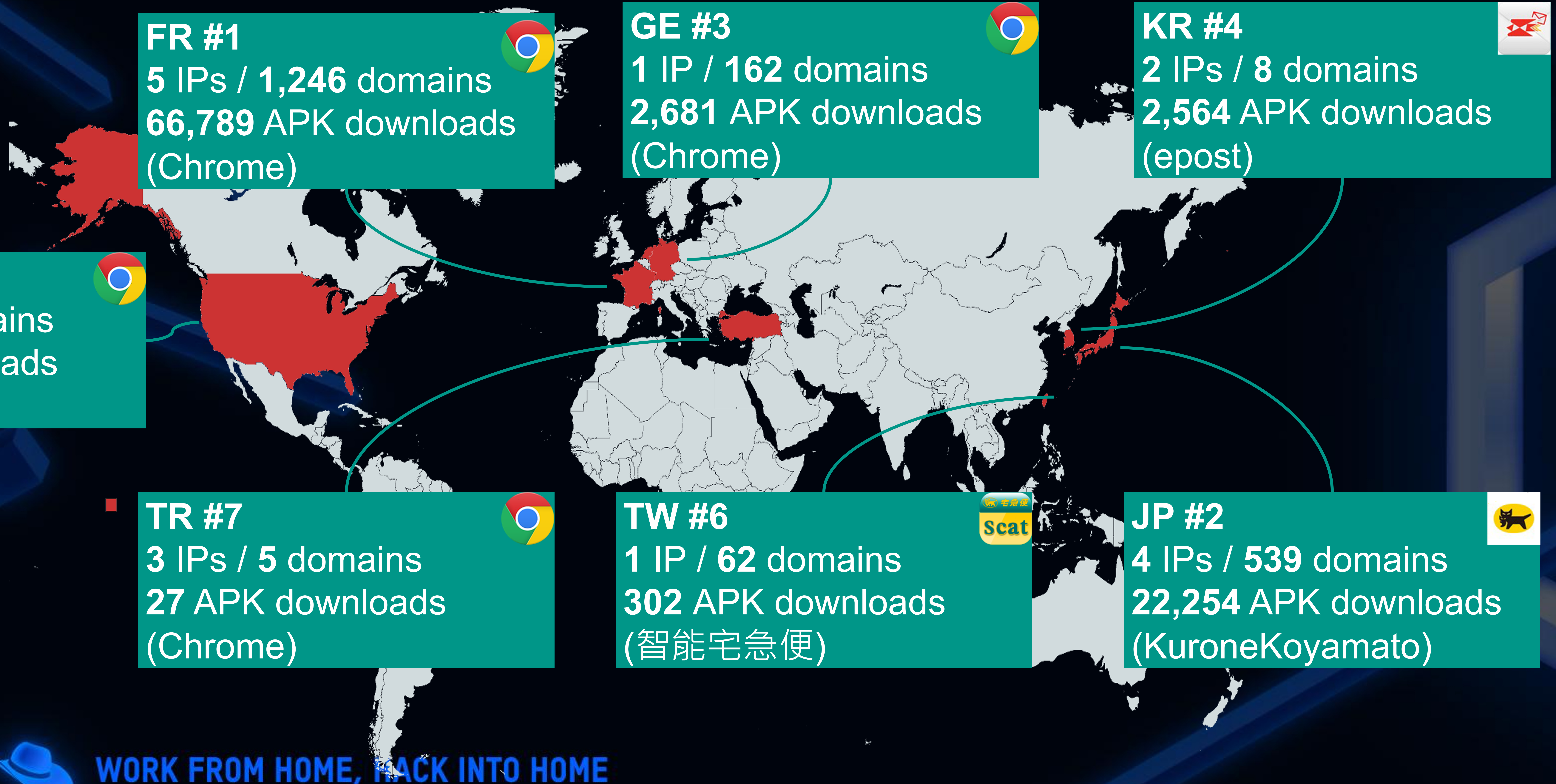
UA based redirection
Redirect based on User-Agent

Android
Malware (MoqHao)

iOS
Phishing

Others
Blank page

MoqHao distribution map



FR #1
5 IPs / **1,246** domains
66,789 APK downloads
(Chrome)

GE #3
1 IP / **162** domains
2,681 APK downloads
(Chrome)

KR #4
2 IPs / **8** domains
2,564 APK downloads
(epost)

US #5
5 IPs / **123** domains
549 APK downloads
(Chrome)

TR #7
3 IPs / **5** domains
27 APK downloads
(Chrome)

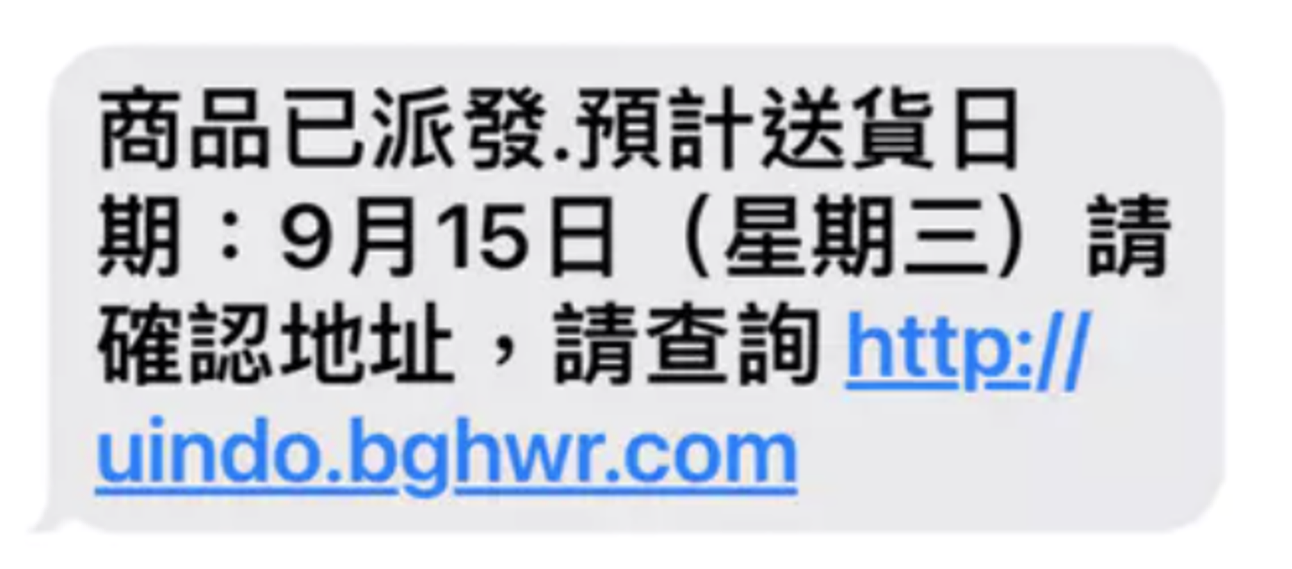
TW #6
1 IP / **62** domains
302 APK downloads
(智能宅急便)

JP #2
4 IPs / **539** domains
22,254 APK downloads
(KuroneKoyamato)

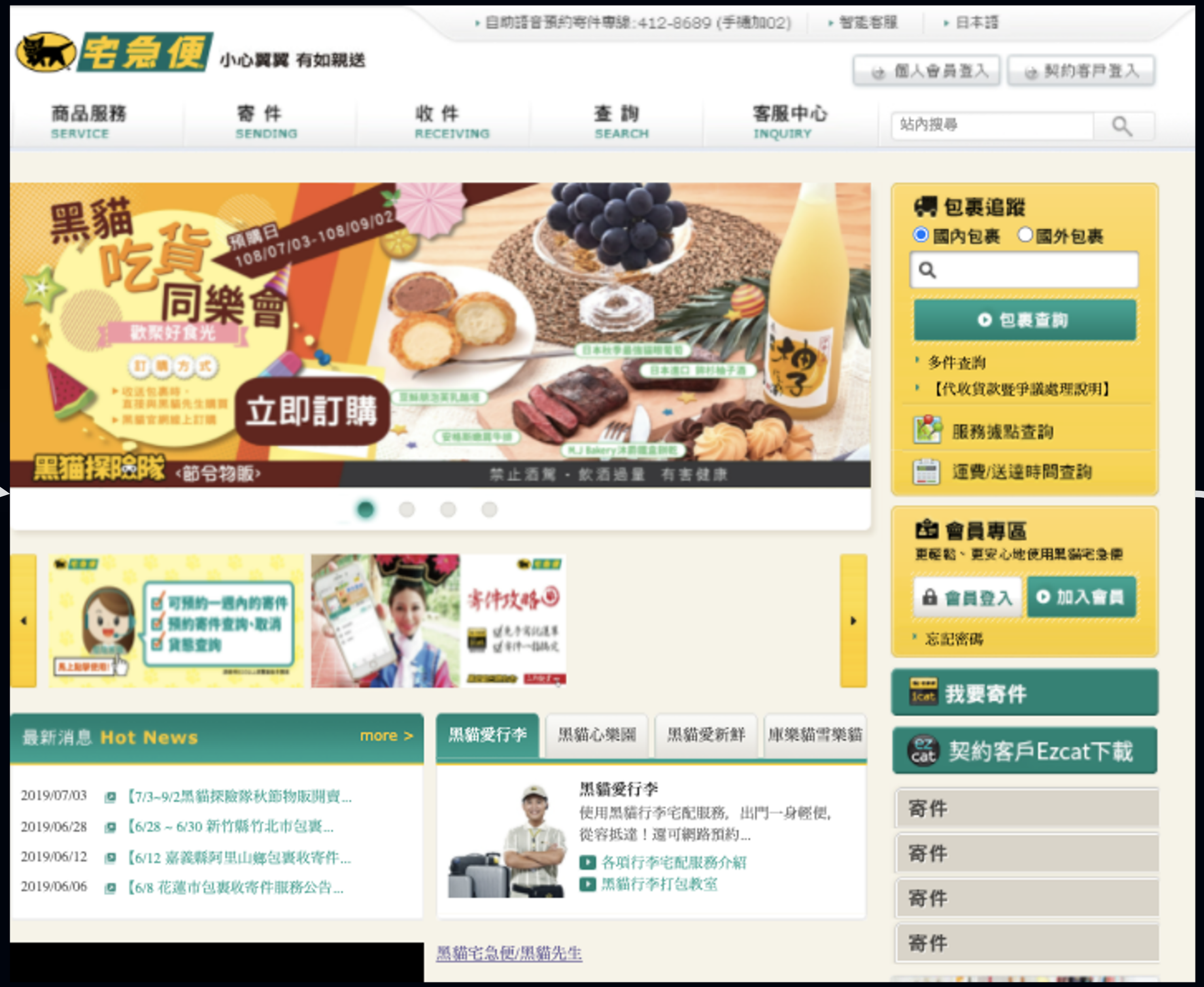
Created with mapchart.net

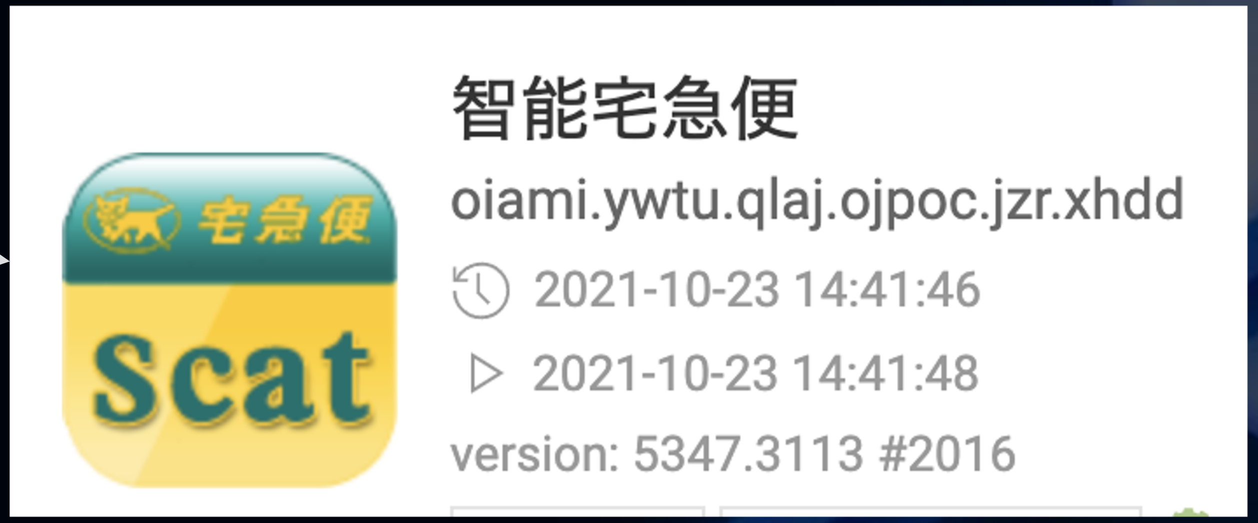
What is MoqHao

- Taiwan is a target of MoqHao



商品已派發.預計送貨日期：9月15日（星期三）請確認地址，請查詢 http://uindo.bghwr.com





智能宅急便

oiami.ywtu.qlaj.ojpoc.jzr.xhdd

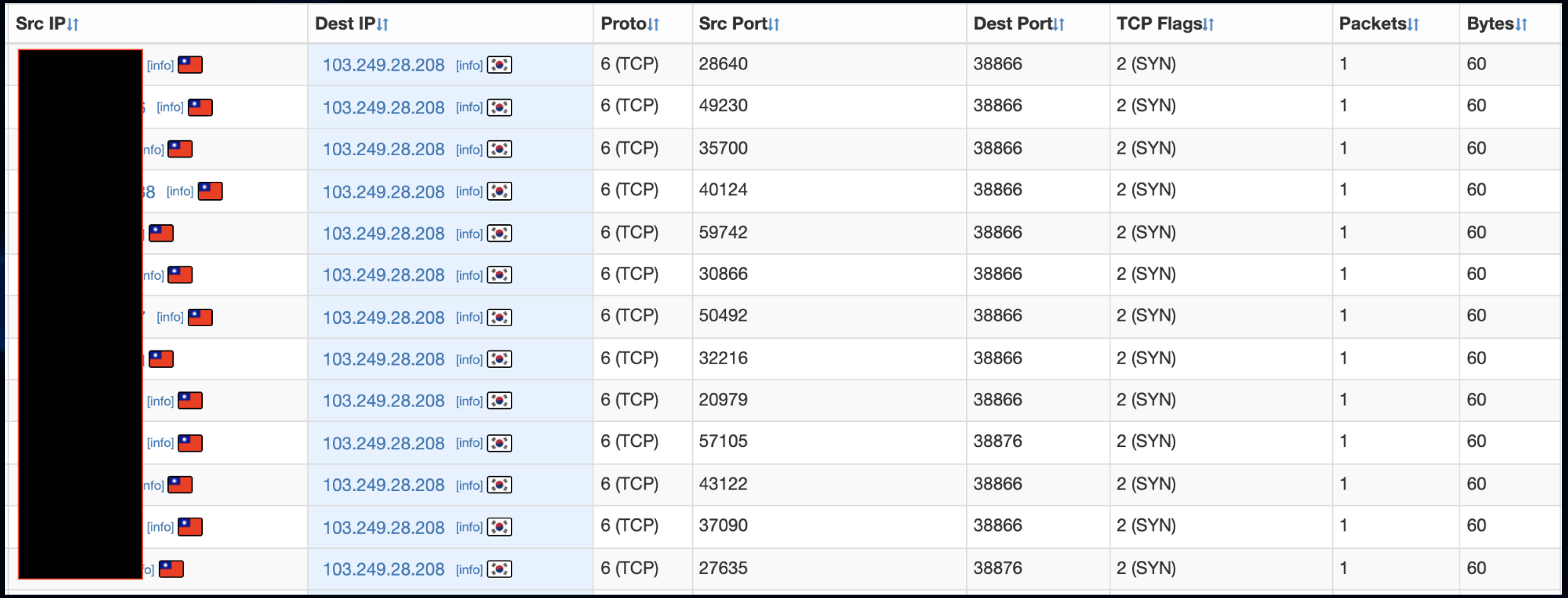
2021-10-23 14:41:46

2021-10-23 14:41:48

version: 5347.3113 #2016

What is MoqHao

- Taiwan is a target of MoqHao
- Connections to second stage C2 server



Src IP↓↑	Dest IP↓↑	Proto↓↑	Src Port↓↑	Dest Port↓↑	TCP Flags↓↑	Packets↓↑	Bytes↓↑
[redacted] [info] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	28640	38866	2 (SYN)	1	60
[redacted] [info] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	49230	38866	2 (SYN)	1	60
[redacted] nfo] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	35700	38866	2 (SYN)	1	60
[redacted] [info] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	40124	38866	2 (SYN)	1	60
[redacted] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	59742	38866	2 (SYN)	1	60
[redacted] nfo] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	30866	38866	2 (SYN)	1	60
[redacted] [info] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	50492	38866	2 (SYN)	1	60
[redacted] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	32216	38866	2 (SYN)	1	60
[redacted] [info] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	20979	38866	2 (SYN)	1	60
[redacted] [info] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	57105	38876	2 (SYN)	1	60
[redacted] nfo] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	43122	38866	2 (SYN)	1	60
[redacted] [info] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	37090	38866	2 (SYN)	1	60
[redacted] o] 🇹🇼	103.249.28.208 [info] 🇰🇷	6 (TCP)	27635	38876	2 (SYN)	1	60

Why is this relevant?

- The new normal is working from home and also ordering from home

- Postal / transport service becomes a favorite lure for a threat actor

宅急便 Scat

JP POST

⚠️ Collaboration fail

- I got a DM from a guy who claims he is a researcher
- He requested MoqHao information to me
- So I shared information with him to make a collaboration

⚠️ Collaboration fail

- But he did not share anything with me and published an article without cred
- I was just robbed

⚠️ Collaboration fail

- Lessons learned:
  - Be aware of trolls, trolls are everywhere
  - Share information only with trustable persons/groups

⚠️ Collaboration fail

- Issues to be solved:
  - Getting to know each other well is difficult nowadays
    - I’m missing a beer bash after a conference 😉
  - oVoice, Gather, etc. may work?

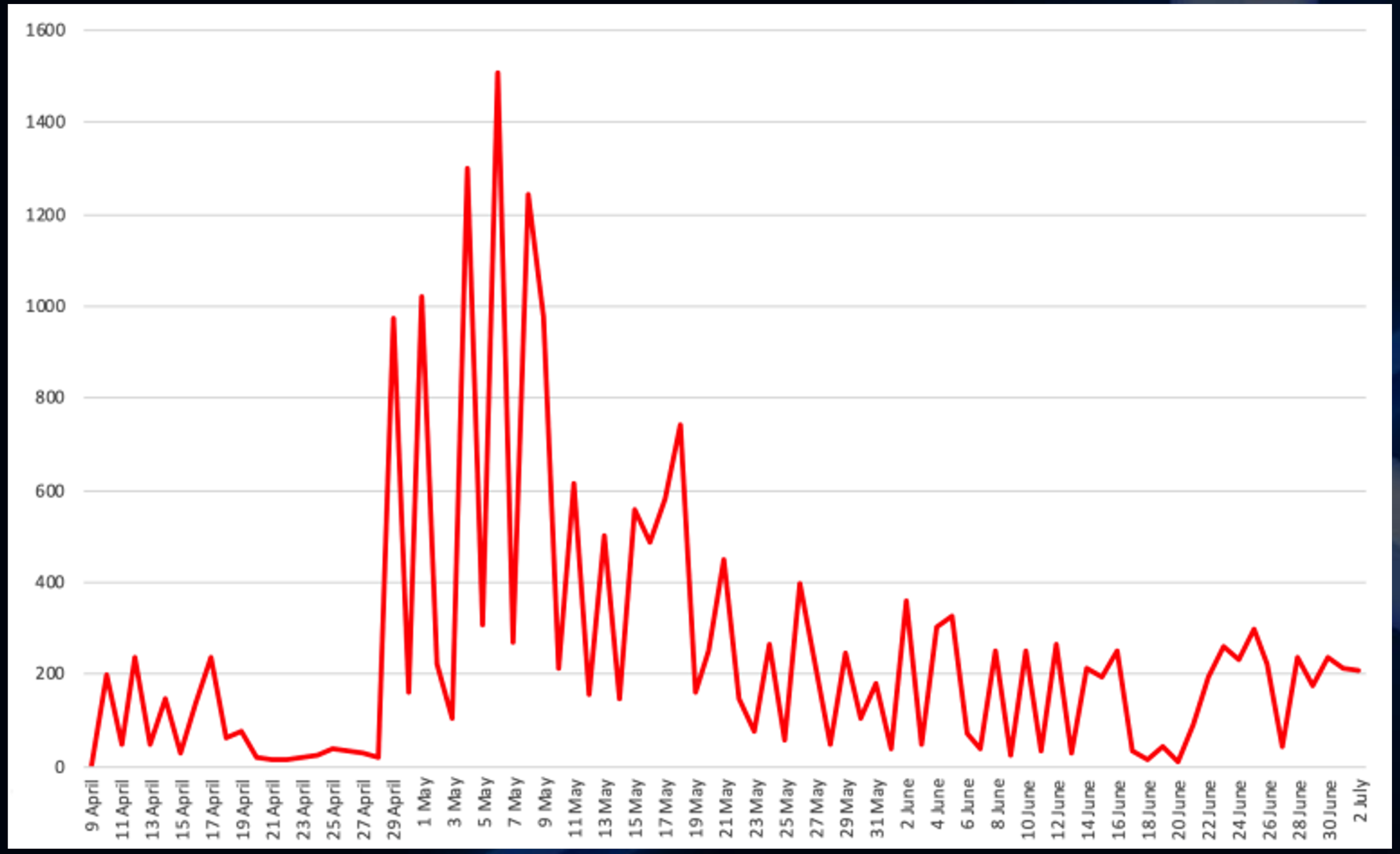
🙌 Collaboration success

- Collaboration with JPCERT/CC

- Focus on trend and victim analysis
  - Working with specific goals and objectives

- Develop understanding over time

- Working with other researchers



5.

Sharing is Caring

In Summary

What I learned from failures

- Sharing information without any context & any commitment does not make sense
  - Sharing is caring but the way of sharing matters
- Creating a shared goal is a key to success

What I learned from failures

- Don’t trust someone who you don’t know well (even he/she has a high reputation online)

- Trolls are everywhere

- Don’t be a troll. Give and take matter.

Final thoughts

- The way that we work and collaborate has changed
- Don’t be afraid to reach out to others
- Be receptive to collaboration opportunities
- Utilize organizations like CERTs/CSIRTs

Questions?

Twitter:

@ninoseki @teamcymru_S2