# Your NAS is not my BOT

Charles
Still

TEAMT5
杜 浦 數 位 安 全

Persistent Cyber Threat Hunters

# whoami

Still Hsu

- BEL, English Dep. @ NPTU
- Threat Intelligence Researcher @ TeamT5
- Interested in...
  - Windows internals
  - .NET
  - Anything and everything!
- Contact
  - Main @ StillAzureH
  - VTuber @ AzakaSekai



TEAMT5
杜 浦 數 位 安 全

# whoami 安全



Charles Li
- TeamT5 Analyst
- Threat Intelligence Research
- Vuln. & Malware Reversing
- Threat actors tracking

# AGENDA

# What is NAS

- NAS: Network Attached Storage (網路儲存伺服器)
- NAS devices are widely deployed in the wild for the following purposes:
  - Data storages and backup
  - File sharing on internet
  - Easy remote access and control, even on dynamic IP or behind NAT
  - Surveillance
  - Multi-media or photo center

# NAS Popularity

# NAS Opened to WAN

Synology NAS
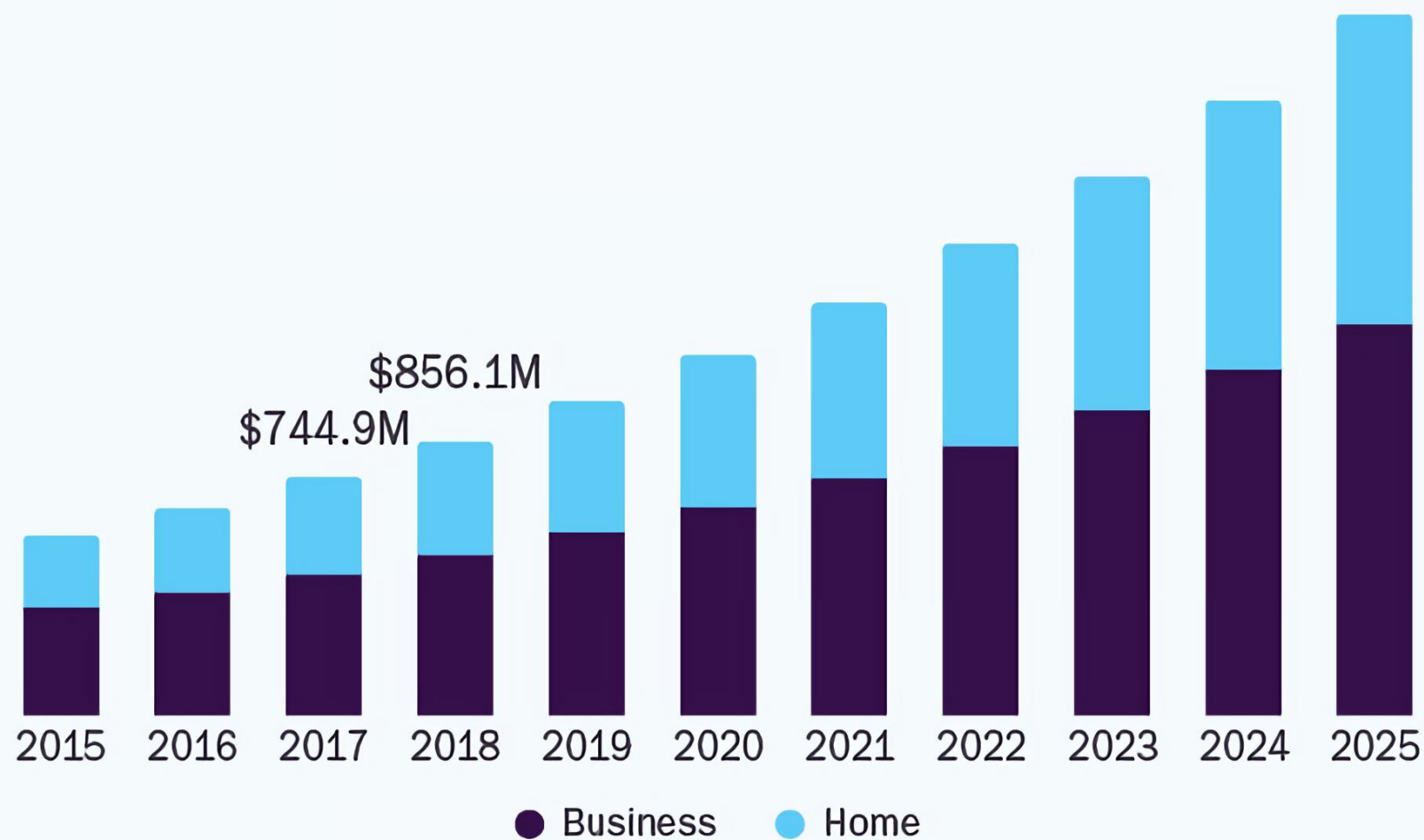- ~3,000,000+ devices


QNAP
- ~10,000+ devices (harder to estimate)

U.S. Consumer Network Attached Storage Market size, by end-use, 2015 - 2025 (USD Million)

$856.1M
$744.9M

14.3%
U.S. Market CAGR, 2020 - 2025

Business    Home

GRAND VIEW RESEARCH

Source:
www.grandviewresearch.com

(Grand View Research, Inc., n.d.)

# Attacks related to NAS Devices

Checkmate ransomware hits QNAP NAS devices

QNAP alerts NAS customers of new DeadBolt ransomware attacks

By Sergiu Gatlan

Asustor NAS owners hit by DeadBolt ransomware attack

Graham CLULEY
February 23, 2022

Hackers Exploit QNAP Vulnerabilities to Turn NAS Devices Into Crypto Miners

By Nathaniel Mott published March 10, 2021

NAS-ty business.

SynoLocker™

# Security advisories related to NAS devices in the last 12 months

- QNAP Medium~Critical
  - 37 advisories
  - Targeted by DeadBolt, eCh0raix, Checkmate, Qlocker, and various other malware like miners and botnets

(QNAP Systems Inc, n.d.)

## QNAP warns of new Checkmate ransomware targeting NAS devices

By **Sergiu Gatlan**　　　　　　(Gatlan, 2022)　　📅 July 7, 2022　⏰ 11:47 AM　💬 2



...ed storage (NAS) vendor QNAP warned customers to secure their devices against attacks ...ransomware to encrypt data.

...s are focused on Internet-exposed QNAP devices with the SMB service enabled and ...words that can easily be cracked in brute-force attacks.

...s Checkmate has recently been brought to our attention," the NAS maker ...shed Thursday.

...that Checkmate attacks via SMB services exposed to the internet, ...' accounts with weak passwords."

...re strain, first deployed in attacks around May 28, that ...nd drops a ransom note named

# Security advisories related to NAS devices in the last 12 months

- Synology Moderate~Critical
  - 18 advisories
  - Targeted by Netatalk and various ransomware

(Synology Inc., n.d.)

## vulnerability

By **Sergiu Gatlan**　　　　　August 26, 2021　　03:42 PM　　**3**

Taiwan-based NAS maker Synology has revealed that recently disclosed remote code execution (RCE) and denial-of-service (DoS) OpenSSL vulnerabilities impact some of its products.

"Multiple vulnerabilities allow remote attackers to conduct denial-of-service attack or execute arbitrary code via a susceptible version of Synology DiskStation Manager (DSM), Synology Router Manager (SRM), VPN Plus Server or VPN Server," the company explains in a security advisory published earlier today.

The complete list of devices affected by the security flaws tracked as CVE-2021-3711 and CVE-2021-3712

# SN Generation

## XPEnology 黑群暉DSM安裝教學：MAC Address與S/N產生 – AniMotion

2017-07-18 作者 pinko

來源：*XPEnology 黑群暉DSM安裝教學：MAC Address與S/N產生 – AniMotion*

我們這次要來解決Quickconnect無法正常與我們安裝好的黑群暉配對連線的問題
因為Synology的 一些限制，想要正常的使用Quickconnect服務，我們必須要有正確的網卡MAC
位址與序號
如果這兩個搭不起來，那Quickconnect服務會拒絕啟動

第一要務便是先產生一個可以用的序號
1.請先下載這個試算表，下載完之後用Excel開啟
請記得按"啟用編輯"與"啟用巨集"，這個試算表才能正常工作
2.請確認型號選擇的地方是"DS3615xs"，確認完之後請按F9重新整理試算表，你會看到"Serial
Number"那個欄位有變化，多按幾次之後把那個欄位的值記下來(不能複製)，並切換到下一個頁

目前SN计算已经可以完全自定义了，也就是凭空生成正确规范的SN，不需要已知正确SN
但是
sn能否在官网验证通过，需要两个条件，一sn本身符合规范（通过计算获取的SN一定是规范的），二官方数据库录入了该sn
BB值加1就代表前面有1000个sn了，你要是改到99那就是前面有99000个sn

**你会发现大量连续的号被同一个邮箱注册了，这些基本是被号贩子注册了，所以大家尽量不要公开自己的号**

像这个段，理论上可以容纳999999个，但是这个要看当时出厂规模，不是所有的号都会进入数据库的，而是生产了多少台就登记多少
sn：1750PDN179400 mac：0011323B0CC3
*1750属于早期的机器可以看出当初这个段的序列号就生产了200台，所以当输入201台的序列号就会提示无效*

作者: xcyupeng: ↑

1750PDN001600 0011323B0B5F
1750PDN002700 0011323B0B61
1750PDN003800 0011323B0B63
1750PDN004900 0011323B0B65
1750PDN005000 0011323B0B67
1750PDN006100 0011323B0B69
1750PDN007200 0011323B0B6B

点击展开...

# AGENDA

Anomaly NAS – Traveling Devices

# Anomaly NAS – Multiple NAS on the same IP address

# Anomaly NAS – VPS

# AGENDA

# Experiment & Detection

Experiment data sets: subdomains collected in the wild [1]
- ◆ Synology.me: 10,648
- ◆ myqnapcloud.com: 4,959

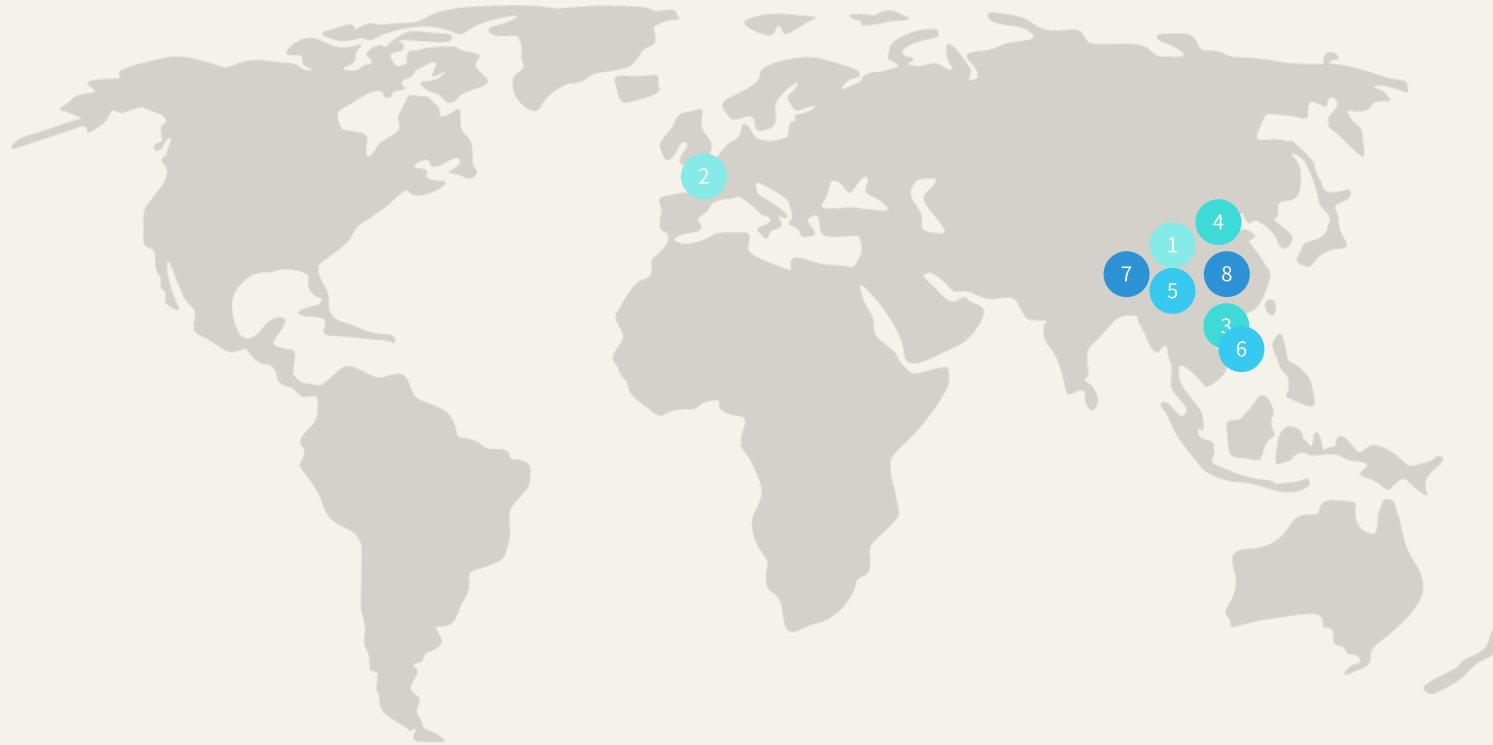Checking for the following indicator patterns to detect peculiarities
1. NAS devices hosting on VPS
2. NAS devices traveling across different countries
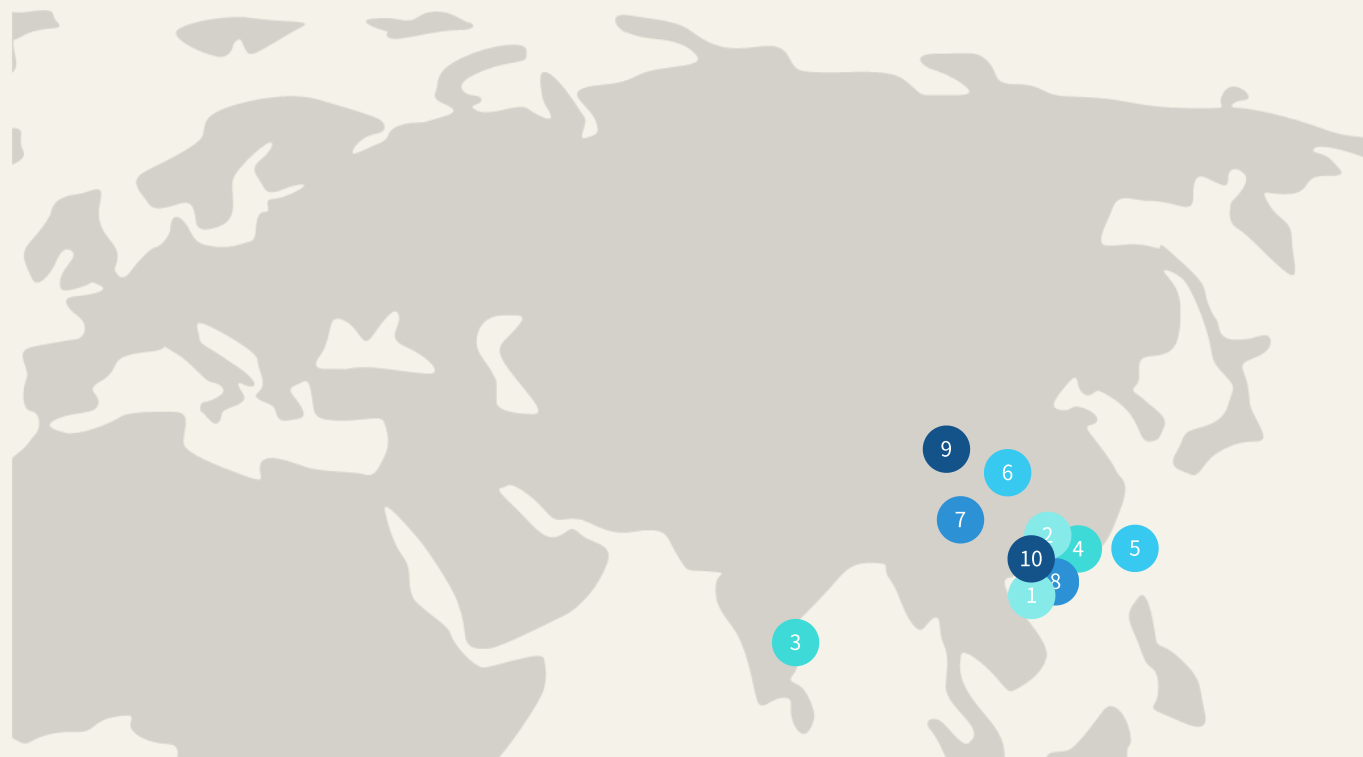3. Multi NAS DDNS resolved to the same IP addresses

[1] https://www.abuseipdb.com/

TEAMT5 杜 浦 數 位 安 全
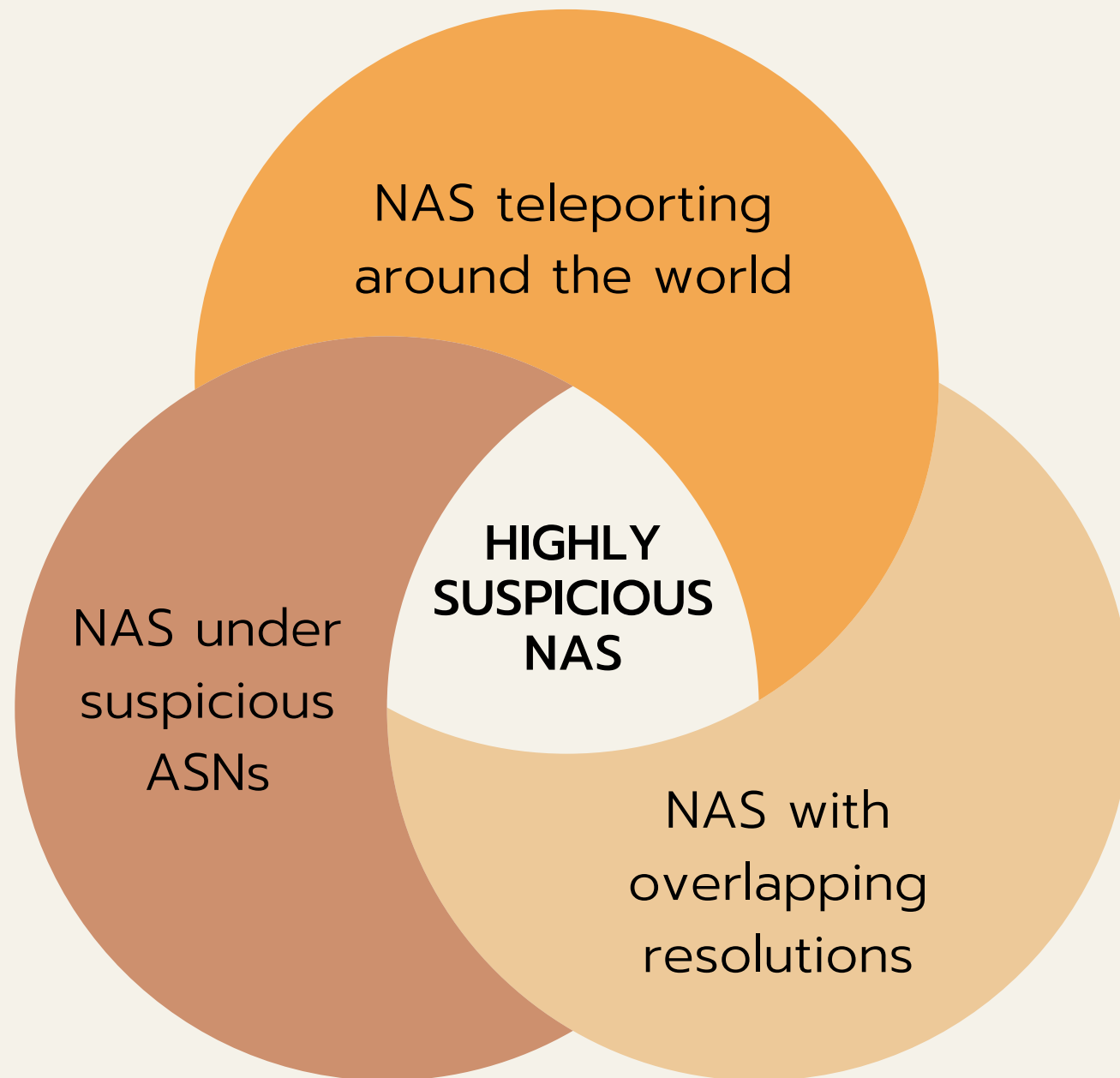
# Highly Suspicious NAS #1

## Online about 2 days for each

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| **China** | **Germany** | **Hong Kong** | **China** | **China** | **Hong Kong** | **China** | **China** |
| China Unicom | xTom | DMIT Cloud | China Unicom | China Unicom | Microsoft | China Unicom | China Unicom |
| 2020-11 | 2020-12 | 2021-01 | 2021-12 | 2022-02 | 2022-04 | 2022-06 | 2022-08 |

# Highly Suspicious NAS #2

## Online about 1~2 day(s) for each



| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|----|
| **Hong Kong** | **Hong Kong** | **Singapore** | **Hong Kong** | **Taiwan** | **China** | **China** | **Hong Kong** | **China** | **Hong Kong** |
| Cloudflare | Amazon | Linode | PCCW-IMS | CHT | China Telecom | China Telecom | PCCW-IMS | China Telecom | Microsoft |
| 2021-07 | 2021-10 | 2021-12 | 2021-12 | 2022-04 | 2022-06 | 2022-08 | 2022-08 | 2022-08 | 2022-08 |

Highly Suspicious NAS #3
Online about days to weeks for each

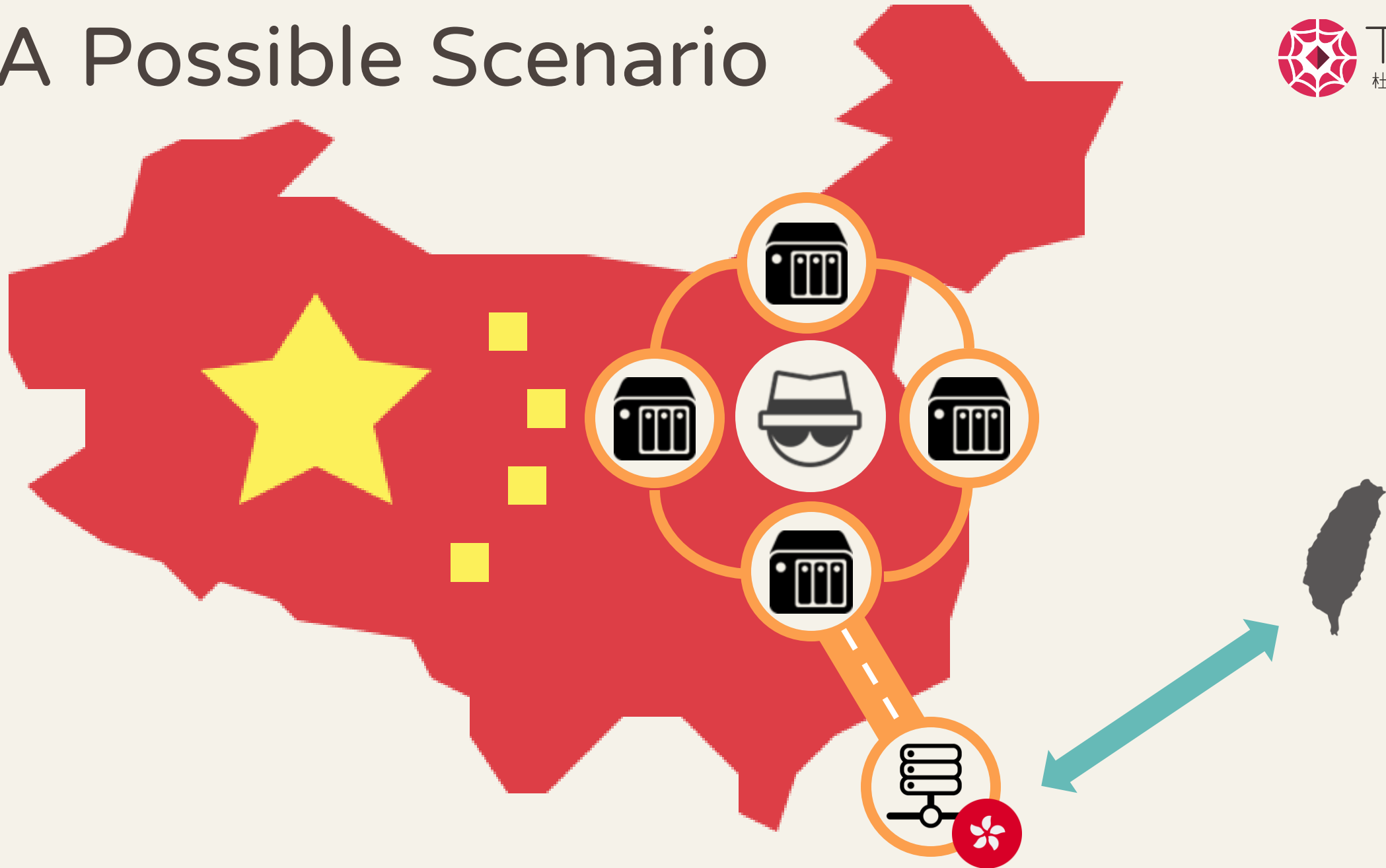| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| China | USA | USA | Singapore | USA |
| China Telecom | DMIT Cloud | IT7 Networks | DigitalOcean | IT7 Networks |
| 2021-01 | 2021-03 | 2022-04 | 2022-05 | 2022-07 |

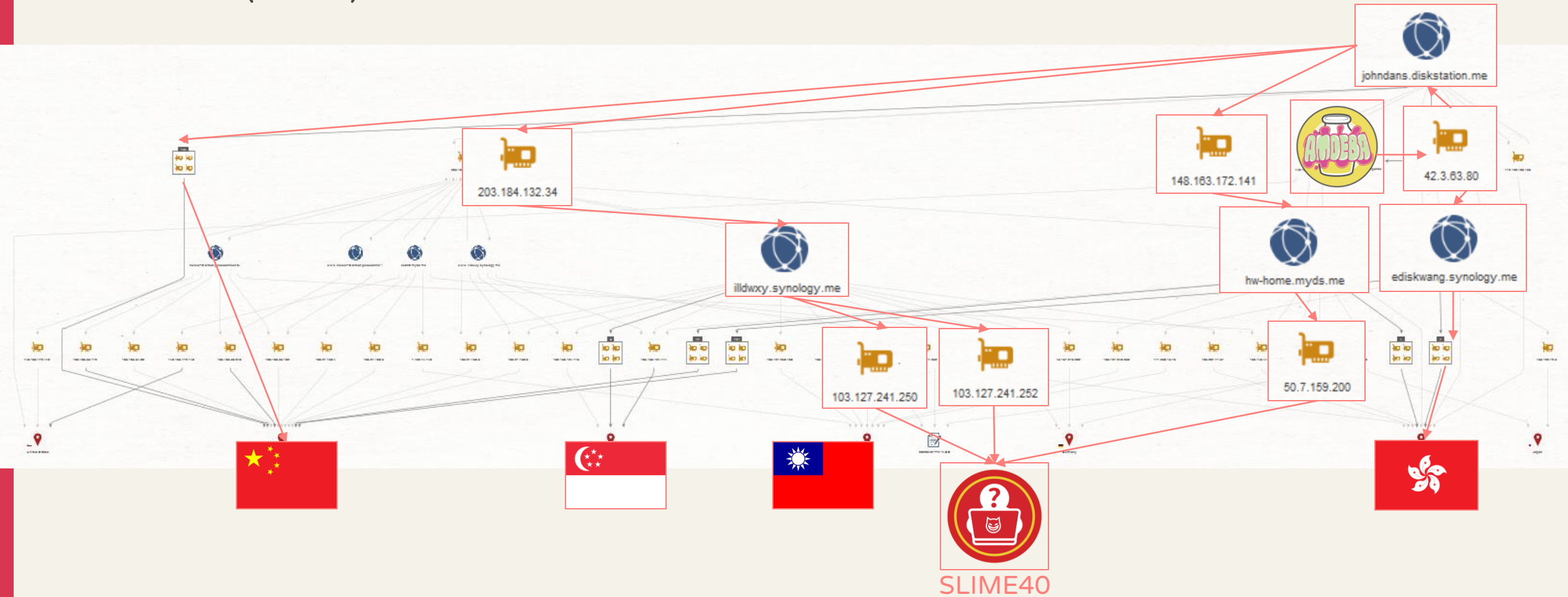# AGENDA

# Case Study 1

SLIME40 (a.k.a FamousSparrow, GhostEmperor)
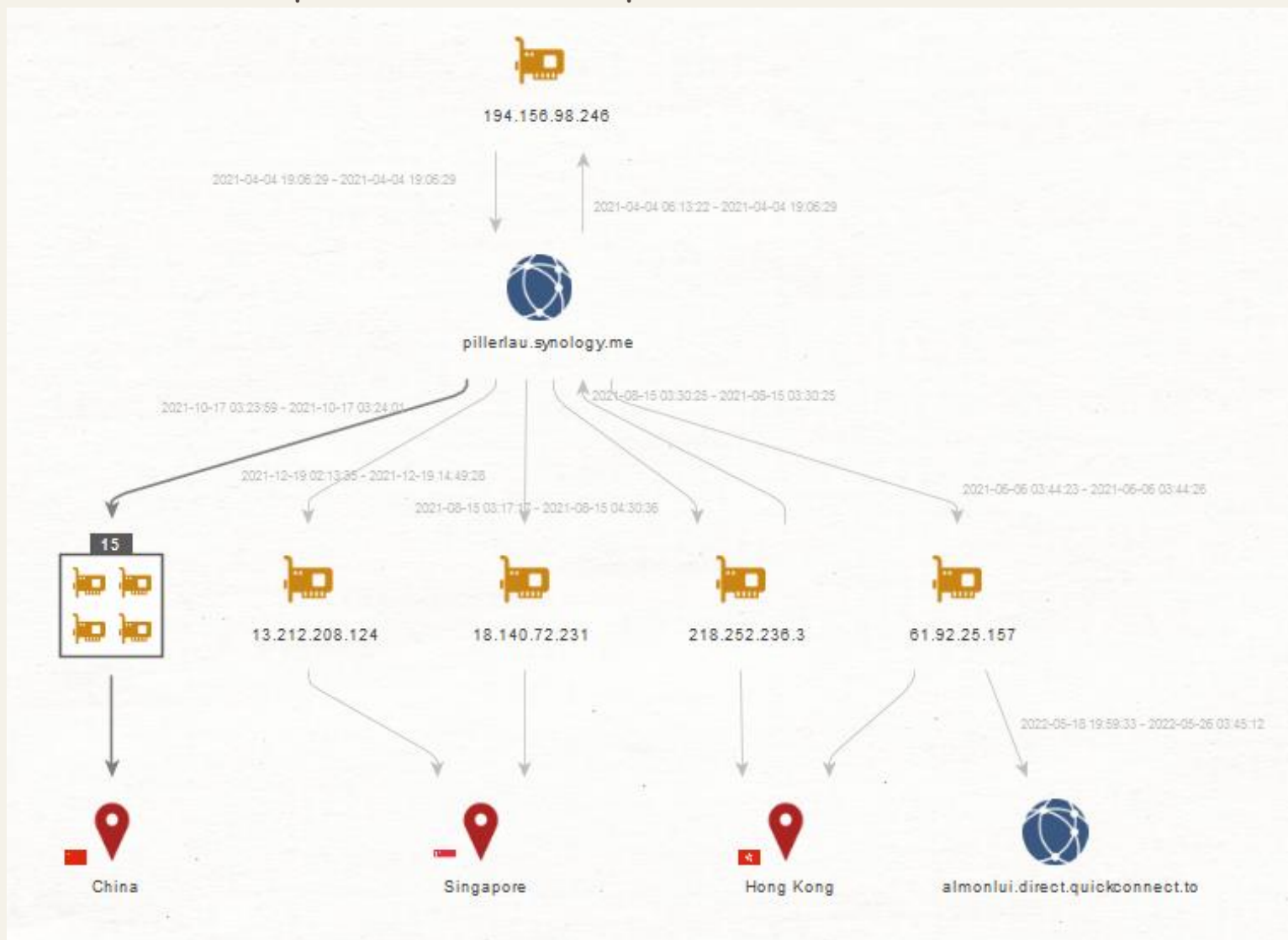
# A Possible Scenario

# Case study 2

AMOEBA (APT41)

# Case study 3

Goushe (a.k.a. TroppicTropper, Keyboy)

- 4 Source IP accessing TEBShell
- Pivoting to 17 NAS DDNS domains
- Resolving to 293 IP addresses
- Across 11 countries
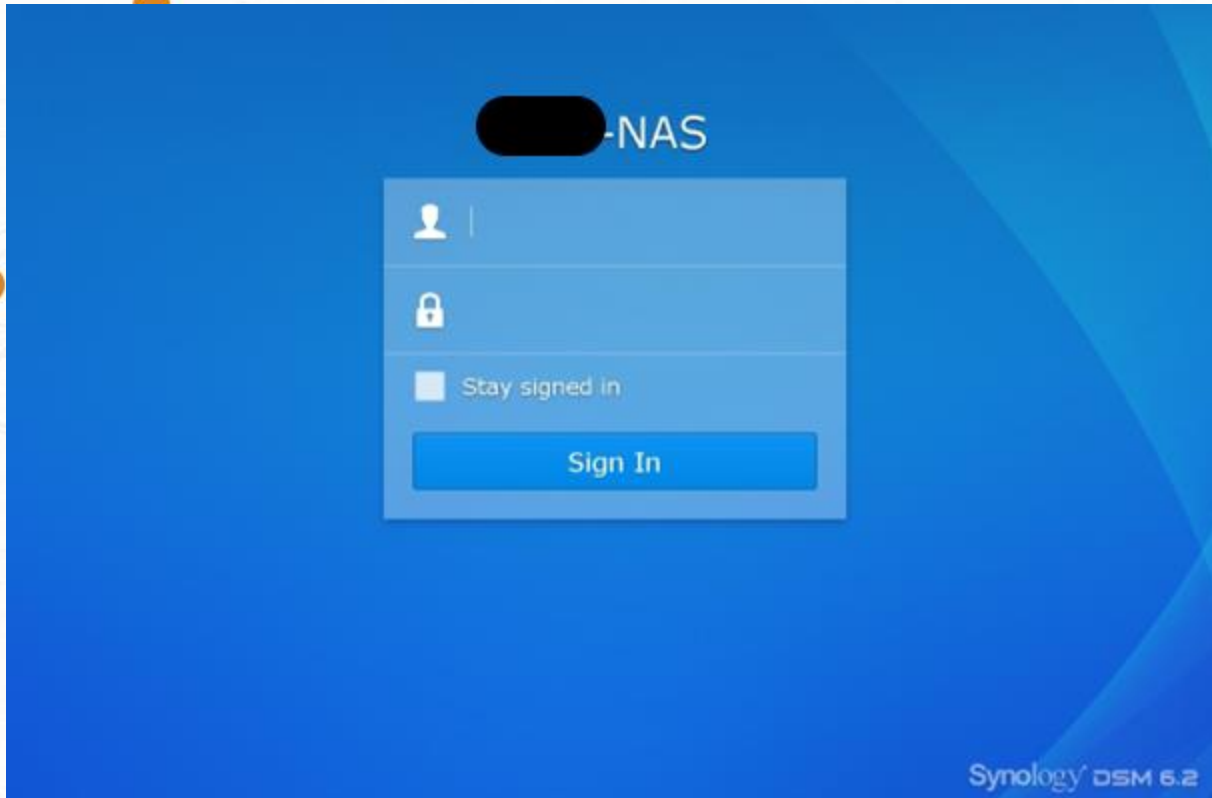
# Case study 3 (cont.)



**60.249.25.55** （ 討論 · 貢獻 · 刪除貢獻 · 濫用日誌 · WHOIS · RDNS · RBLs · http · 封鎖連結 · 封鎖日誌 ）

- 2020年明尼阿波利斯騷亂 （ 編輯 | 討論 | 歷史 | 連結 | 監視 | 日誌 ）

- 反復加入有爭議內容，已多達4次。

# AGENDA

# Conclusion

Traditional (obvious) threats to NAS devices:
- ◆ Ransomware
- ◆ Crypto miners


3 indicators to detect NAS peculiarities are proposed and tested
- ◆ It's hard to verify if they are really used in targeted attacks but looks very suspicious

# Conclusion (cont.)

How APT actors abuse compromised NAS:
- Infiltrating through your internet facing NAS devices
- Traffic relay hops for malware traffic – DDNS + Dynamic IP address (port forwarding is required on NAS devices)
- Building botnets for their intrusion activities

-

Some compromised NAS devices were observed to influence public opinions (Wikipedia, PTTs), but we are uncertain whether these activities are conducted by APT actors or not.

# 對抗網路攻擊威脅
# 我們需要熱情的你

## 熱門職缺

- **Vulnerability Researcher (D39 Lab)**
- **Cyber Threat Intelligence Analyst**
- **Incident Response Engineer**
- **Windows / Linux / OSX Cyber Security Engineer**

◀ 立即掃碼
職缺全都看！

TEAMT5 杜浦數位安全 | **Career Fair 攤位編號 9**

# Questions?