

Your NAS is not my BOT

Charles
Still

whoami

Still Hsu

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



whoami



Charles Li

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

AGENDA

1 Introduction

2 Detecting compromised NAS devices

3 Experiments & Validation

4 Real-World Case studies

5 Conclusion

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



Google site:"synology.me" x [microphone] [search]

All Images News Shopping Maps More Tools

About 7,900,000 results (0.25 seconds)

Tip: Search for **English** results only. You can specify your search language in Preferences

Try Google Search Console
www.google.com/webmasters/
Do you own "**synology.me**"? Get indexing and ranking data from Google.

https://legros.synology.me

Hanagarments Factory - Hanagarments
We are a manufacturer of women fashion garments since 2011. We are a family business that thrives to deliver quality apparels for the high street.

http://a233454.synology.me · Translate this page

모바일커뮤니티 - 모씨 (모바일폰 소통의 공간)
모바일커뮤니티 - 모씨 (모바일폰 소통의 공간)

http://hkwindsacademy.synology.me · Translate this page

香港管樂學院Hong Kong Winds Academy - Home | Facebook
香港管樂學院Hong Kong Winds Academy ; 八銀Silver 8. \$. . Electronics. Closed now. 2,343

Google site:"myqnapcloud.com" x [microphone] [search]

All Images News Shopping Maps More Tools

About 70,900 results (0.21 seconds)

Google promotion

Try Google Search Console
www.google.com/webmasters/
Do you own "**myqnapcloud.com**"? Get indexing and ranking data from Google.

https://frsl.myqnapcloud.com · Translate this page

Adriana Romero Tango Argentino en Bilbao con...
Clases de Tango Argentino en Bilbao con Adriana Romero. Cursos grupales y clases particulares en Bilbao y Bizkaia. Milonga social.

https://otmani.myqnapcloud.com · Translate this page

EL OTMANI FITNESS - La meilleure salle de sport (fitness ...
Bienvenue sur le site El Otmani Fitness. Un club de fitness basée à EL JADIDA. Ses spécialités sont la musculation, l'aérobic, la danse, le yoga, le crossfit, ...

https://solinfor.myqnapcloud.com · Translate this page

GEST TRAZA
Gestión Integral Empresa,Control de Trazabilidas,Control Series y Lotes.

NAS Opened to WAN

Synology NAS

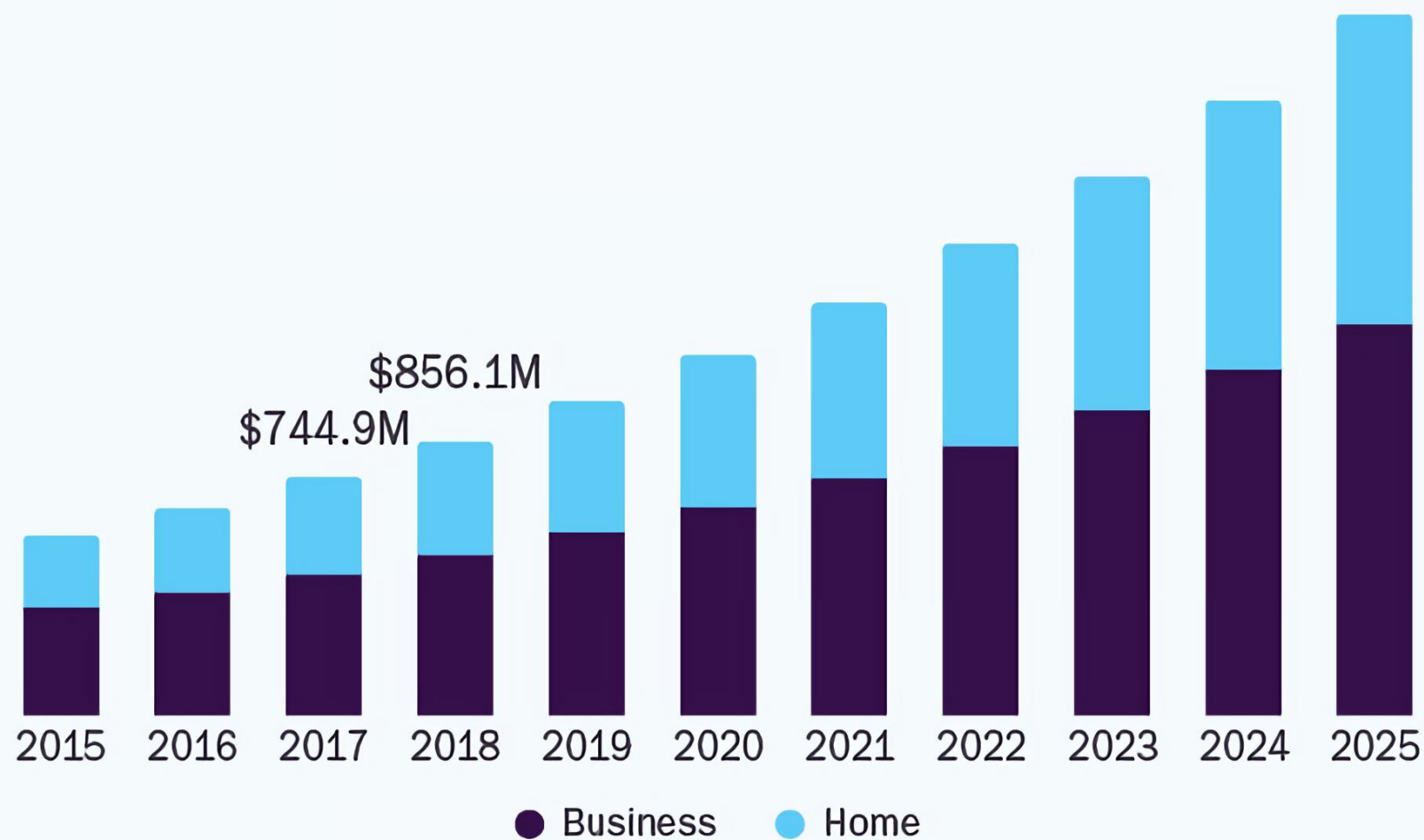
- ◆ ~3,000,000+ devices

QNAP

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

U.S. Consumer Network Attached Storage Market

size, by end-use, 2015 - 2025 (USD Million)



GRAND VIEW RESEARCH

14.3%

U.S. Market CAGR,
2020 - 2025

Source:
www.grandviewresearch.com

Attacks related to NAS Devices



QNAP alerts NAS customers of new DeadBolt ransomware attacks

By Sergiu Gatlan

May 19, 2022 06:38 AM



Asustor NAS owners hit by DeadBolt ransomware attack

By Graham CLUBLEY
February 23, 2022

Ad - One product to protect all your devices, without slowing them down.
Free 90-day trial



Hackers Exploit QNAP Vulnerabilities to Turn NAS Devices Into Crypto Miners

By Nathaniel Mott published March 10, 2021

NAS-ty business.

Facebook Twitter LinkedIn YouTube Instagram Comments (5)



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 ished Thursday.

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

ne strain, first deployed in attacks around May 28, that and 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計算已經可以完全自定義了，也就是凭空生成正確規範的SN，不需要已知正確SN
但是
sn能否在官網驗證通過，需要兩個條件，一sn本身符合規範（通過計算獲得的SN一定是規範的），二官方數據庫錄入了該sn
BB值加1就代表前面有1000個sn了，你要是改到99那就是前面有99000個sn

你會發現大量連續的號被同一個郵箱註冊，這些基本是被號販子註冊了，所以大家尽量不要公開自己的號

像這個段，理論上可以容納999999個，但是這個要看當時出廠規模，不是所有的號都會進入數據庫的，而是生產了多少台就登記多少
sn: 1750PDN179400 mac: 0011323B0CC3
1750屬於早期的機器可以看出當初這個段的序列號就生產了200台，所以当輸入201台的序列號就會提示無效

作者: xcyupeng: 1

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

[点击展开...](#)

AGENDA

1 Introduction

2 Detecting compromised NAS devices

3 Experiments & Validation

4 Real-World Case studies

5 Conclusion

| + First Seen 2020-05-06 | | Registrar GoDaddy.com, LLC | + Categorize | | | | | | | | | |
|-------------------------|----|-----------------------------------|--------------------------|-----------------|----|----------------|------|------------|------------|------------------|--|--|
| + Last Seen 2022-06-17 | | Registrant Domains By Proxy, L... | | | | | | | | | | |
| ✓ x HINET | 2 | | <input type="checkbox"/> | 114.93.75.145 | CN | 114.93.0.0/16 | 4812 | 2021-09-12 | 2021-09-12 | riskiq, mnemonic | <input type="checkbox"/> Routable | <input type="checkbox"/> China-Telecom |
| ✓ x KIXS-AS-KR | 1 | | <input type="checkbox"/> | 114.86.129.9 | CN | 114.86.0.0/16 | 4812 | 2021-07-13 | 2021-07-13 | mnemonic | <input type="checkbox"/> Routable | <input type="checkbox"/> China-Telecom |
| ▼ NETWORK (8 / 23) | | | <input type="checkbox"/> | 211.106.132.202 | KR | 211.104.0.0/14 | 4766 | 2021-07-10 | 2021-07-10 | riskiq, mnemonic | <input type="checkbox"/> Korea-Telecom | <input type="checkbox"/> Routable |
| ✓ x 101.224.0.0/13 | 7 | | <input type="checkbox"/> | 103.125.250.166 | JP | Unknown | | 2021-05-06 | 2021-05-06 | riskiq, mnemonic | <input type="checkbox"/> Non-Routable | |
| ✓ x 114.86.0.0/16 | 4 | | <input type="checkbox"/> | 114.86.135.64 | CN | 114.86.0.0/16 | 4812 | 2021-02-26 | 2021-02-27 | mnemonic | <input type="checkbox"/> Routable | <input type="checkbox"/> China-Telecom |
| ✓ x 124.78.0.0/15 | 4 | | <input type="checkbox"/> | 101.224.215.93 | CN | 101.224.0.0/13 | 4812 | 2021-01-03 | 2021-01-03 | riskiq | <input type="checkbox"/> Routable | <input type="checkbox"/> China-Telecom |
| ✓ x 222.64.0.0/16 | 3 | | <input type="checkbox"/> | 114.86.132.26 | CN | 114.86.0.0/16 | 4812 | 2021-01-01 | 2021-01-01 | riskiq | <input type="checkbox"/> Routable | <input type="checkbox"/> China-Telecom |
| ✓ x 114.93.0.0/16 | 2 | | <input type="checkbox"/> | 222.64.6.46 | CN | 222.64.0.0/16 | 4812 | 2020-12-23 | 2020-12-23 | riskiq, mnemonic | <input type="checkbox"/> Routable | <input type="checkbox"/> China-Telecom |
| Show More | | | | | | | | | | | | |
| ▼ SOURCE (4 / 31) | | | | | | | | | | | | |
| ✓ x riskiq | 18 | | | | | | | | | | | |
| ✓ x mnemonic | 11 | | | | | | | | | | | |
| ✓ x pingly | 1 | | | | | | | | | | | |

Anomaly NAS – Traveling Devices

Anomaly NAS – Multiple NAS on the same IP address

RISKIQ Search: **ruifeng105.synology.me** (103.149.248.80)

First Seen: 2020-09-02 | Last Seen: 2022-06-18 | Registrar: GoDaddy.com, LLC | Registrant: Domains By Proxy, L...

FILTERS

- SHA-1 (8 / 8)**
 - 22322e785c8df... 1
 - 24a141c205dd... 1
 - 77dcec37bf7d4... 1
 - a2fcba99934df4... 1
 - c787b65afab96... 1
- FIRST SEEN (4 / 8)**
 - 2021-10-24 3
 - 2020-11-02 2
 - 2021-03-05 2
 - 2021-12-28 1
- LAST SEEN (4 / 8)**

CERTIFICATES

1 - 8 of 8 | Sort: Last Seen Descending | 25 / Page

SHA-1

- 22322e785c8df15c2415f69c06b9eeda0c0a250b
- 24a141c205dd550bdea557ad8a10267c921789a6
- fc556bae3a62899345f8a042e99dc4bbe412acab
- a2fcba99934df4692951730fee12a1f9d8a1f08f
- e60e6aff920b9b5998a63df60bb1a357d21de795
- e1603a94b7eb3f3c836b4790dd618650f4659931
- c787b65afab9625985477a133e42751ec5c9ad48
- 77dcec37bf7d4a5fbfda4ab257529edfd9152f47

RISKIQ Search: **103.149.248.80**

22-04-02 | ASN: AS41378 - KirinoNET | Netblock: 103.149.248.0/24 | HK | Hosting Provider: - | 22-06-18 | Organization: Kirino LLC | Operating System: Debian

6 | 5 | 0 | 0 | 9 | 0 | 10 | 0 | 0

Resolutions | Whois | Certificates | Trackers | Components | Host Pairs | OSINT | Hashes | Reverse DNS


RESOLUTIONS

1 - 6 of 6 | Sort: Last Seen Descending | 25 / Page

| Resolve | First | Last |
|--|------------|----------|
| <input type="checkbox"/> xxxholic-ds718p.synology.me | 2022-06-06 | 2022-06- |
| <input type="checkbox"/> www.xxxholic-ds718p.synology.me | 2022-06-06 | 2022-06- |
| <input type="checkbox"/> dainifei.vip | 2022-04-29 | 2022-06- |
| <input type="checkbox"/> zhaoxinhao.xyz | 2022-06-14 | 2022-06- |
| <input type="checkbox"/> ruifeng105.synology.me | 2022-05-18 | 2022-05- |
| <input type="checkbox"/> mydsm.me | 2022-04-01 | 2022-04- |

Simpler cloud. Happier devs. Better results.

Businesses grow faster when developers can build on the simple, affordable cloud they love. DigitalOcean has the cloud computing services you need, with predictable pricing, robust documentation, and scalability to support your growth at any stage.

 Sign up with Google

 Sign up with GitHub

Sign up with email

We use cookies to provide our services and for analytics and marketing. To find out more about our use of cookies, please see our [Privacy Policy](#). By continuing to browse our website, you agree to our use of cookies.

OK

Globally distributed
data centers

Countries our
customers build in

Customers building
with DigitalOcean

Uptime SLA for
Droplets and Storage

Anomaly NAS – VPS

AGENDA

1 Introduction

2 Detecting compromised NAS devices

3 Experiments & Validation

4 Real-World Case studies

5 Conclusion

Experiment & Detection

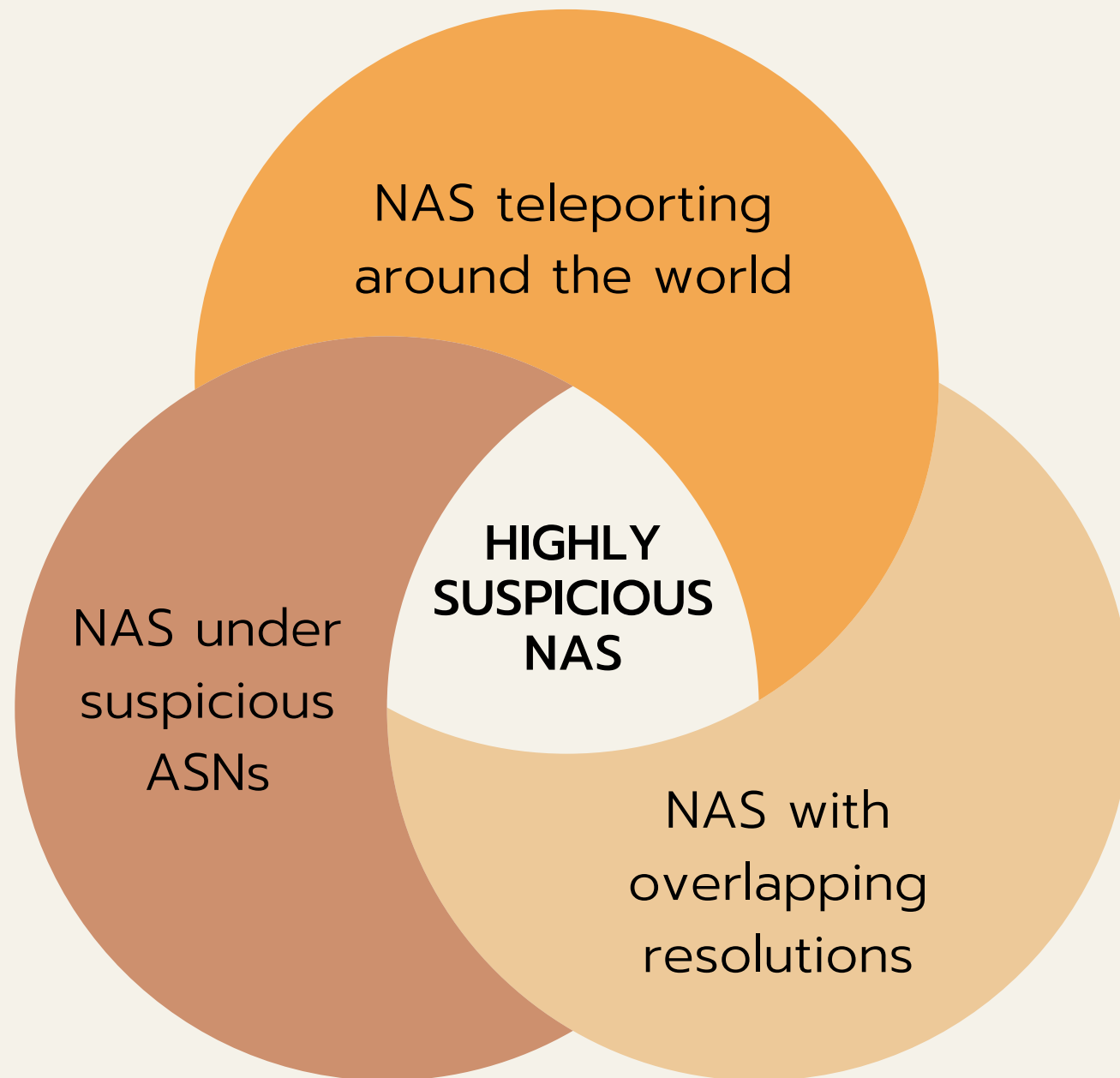
Experiment data sets: subdomains collected in the wild [1]

- ◆ Synology.me: 10,648
- ◆ myqnapcloud.com: 4,959

Checking for the following indicator patterns to detect peculiarities

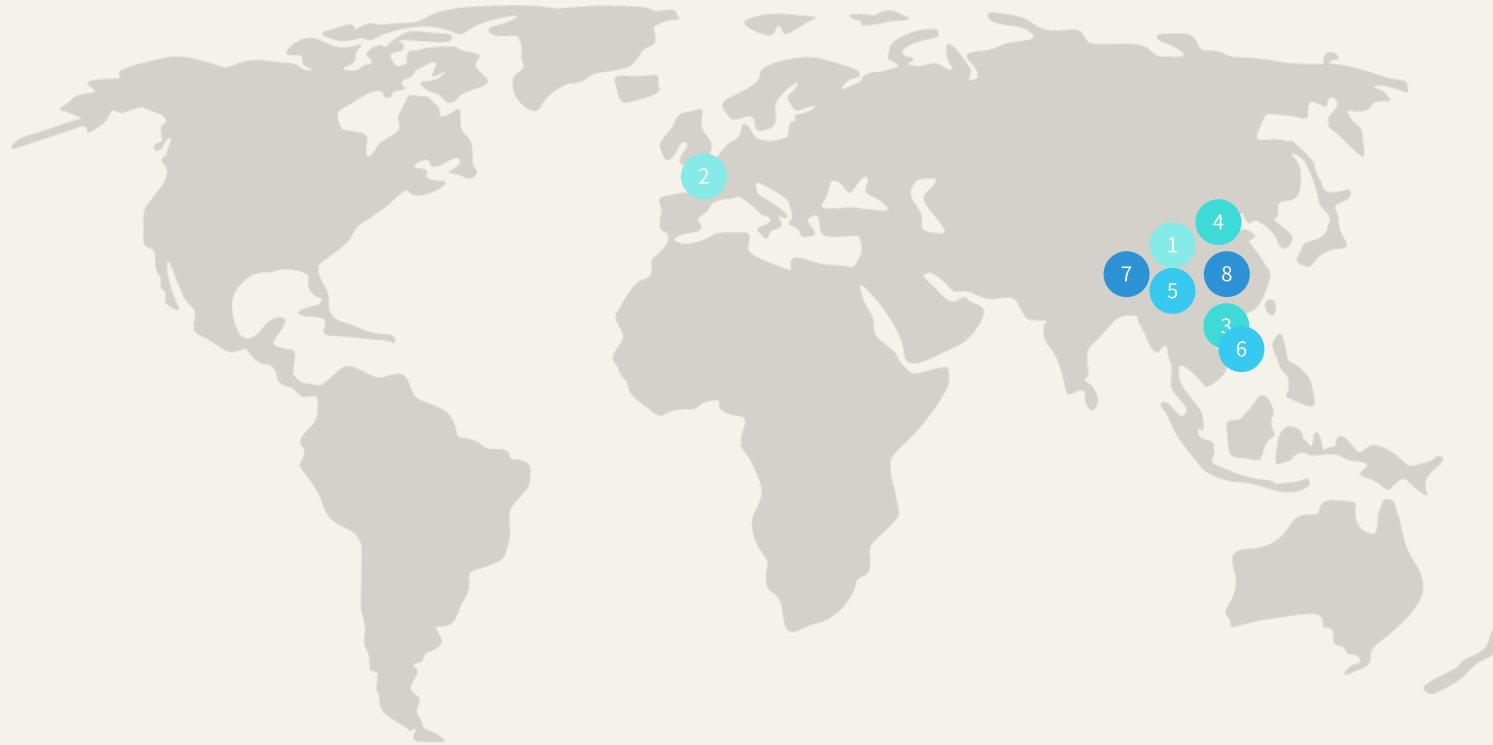
1. NAS devices hosting on VPS
2. NAS devices traveling across different countries
3. Multi NAS DDNS resolved to the same IP addresses

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



Highly Suspicious NAS #1

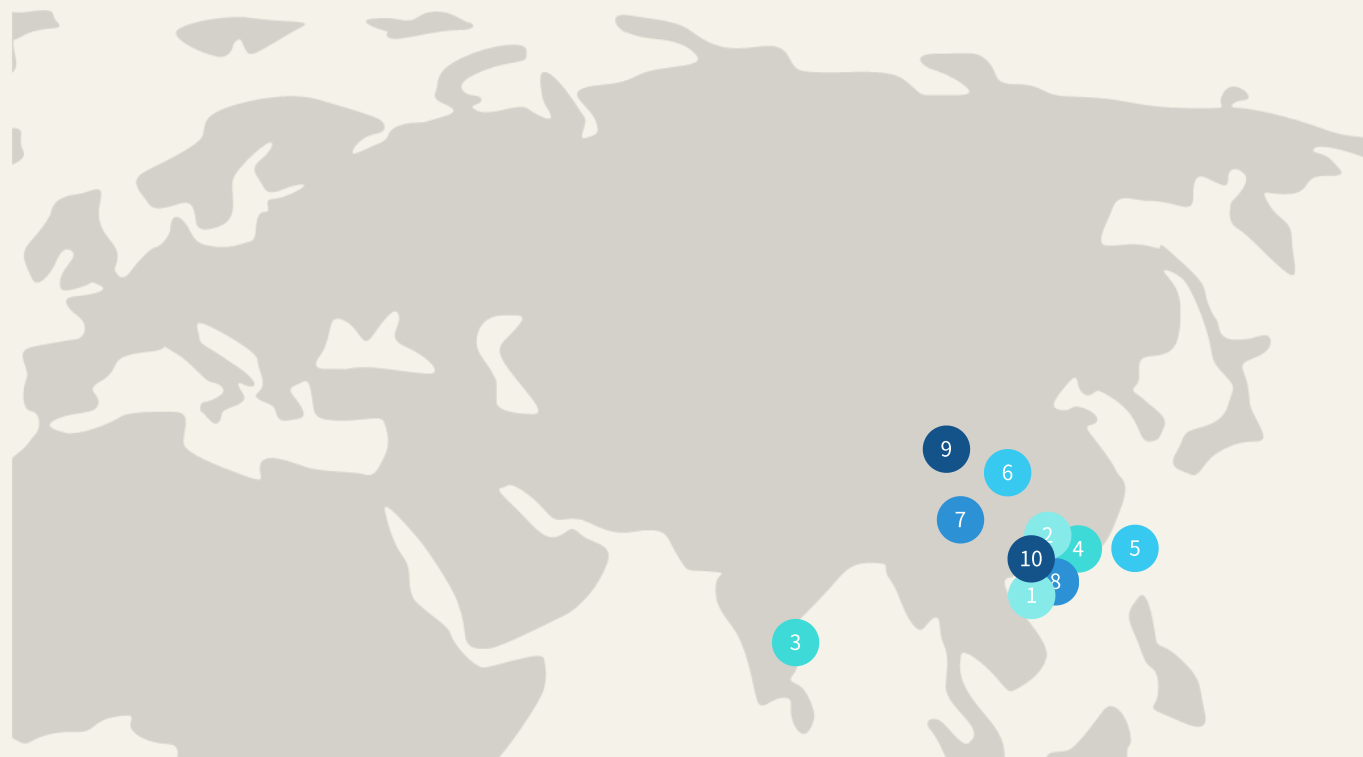
Online about 2 days for each



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

Highly Suspicious NAS #2

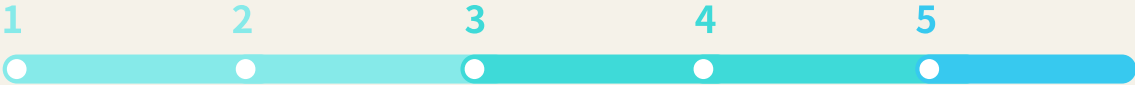
Online about 1~2 day(s) for each



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

Highly Suspicious NAS #3

Online about days to weeks for each



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

AGENDA

1 Introduction

2 Detecting compromised NAS devices

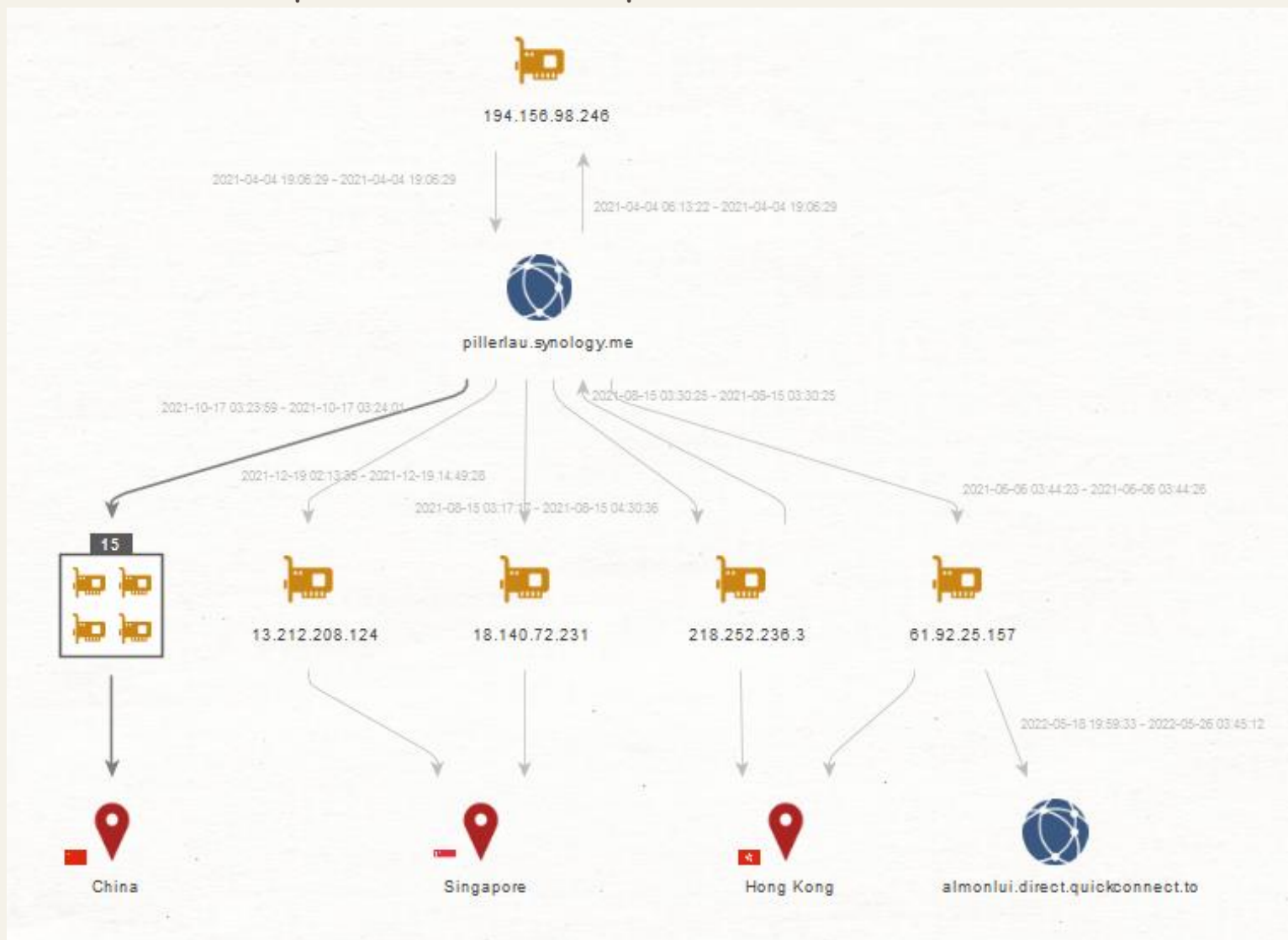
3 Experiments & Validation

4 Real-World Case studies

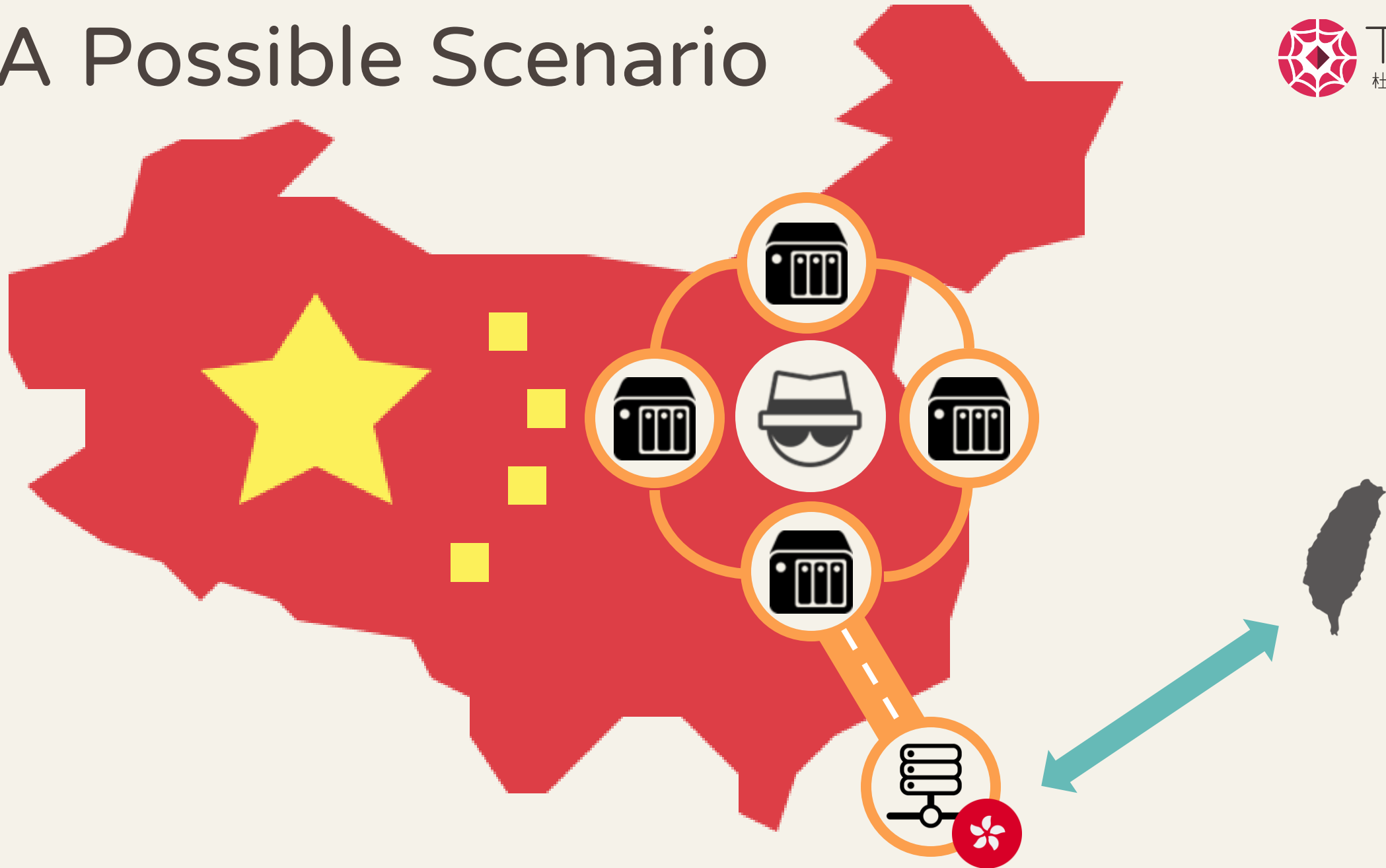
5 Conclusion

Case Study 1

SLIME40 (a.k.a FamousSparrow, GhostEmperor)

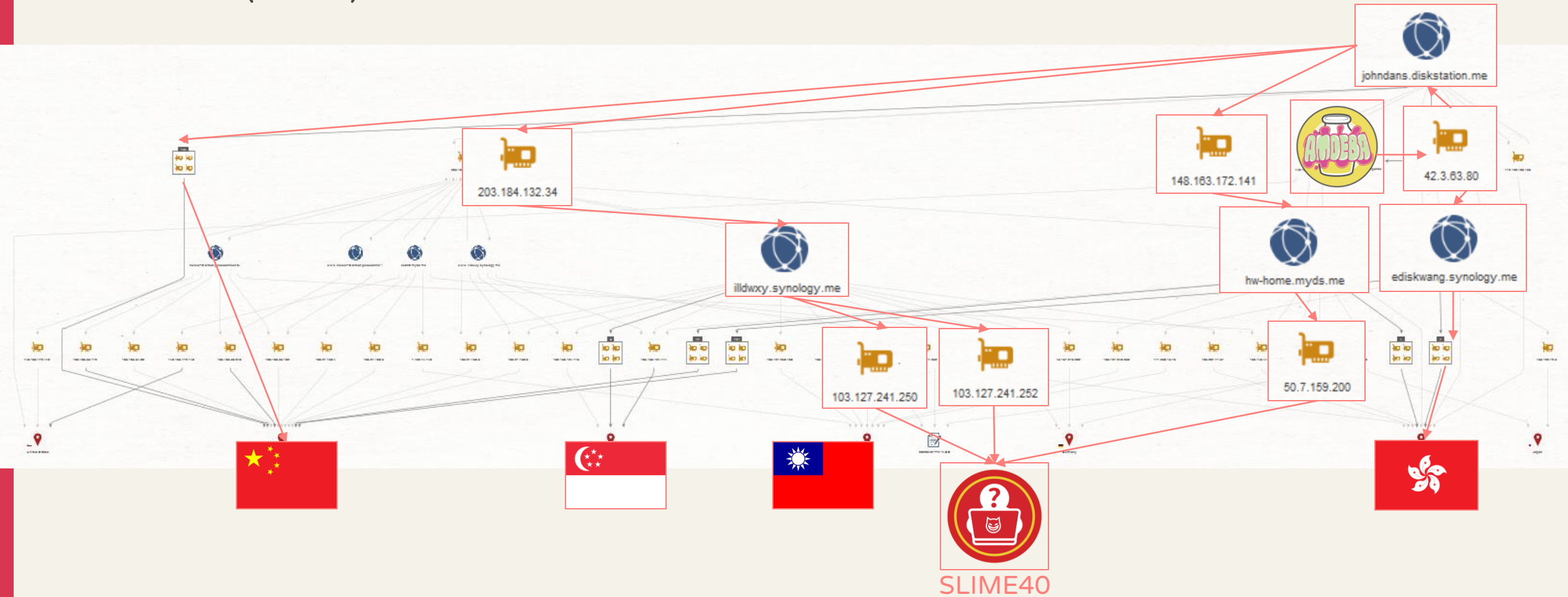


A Possible Scenario



Case study 2

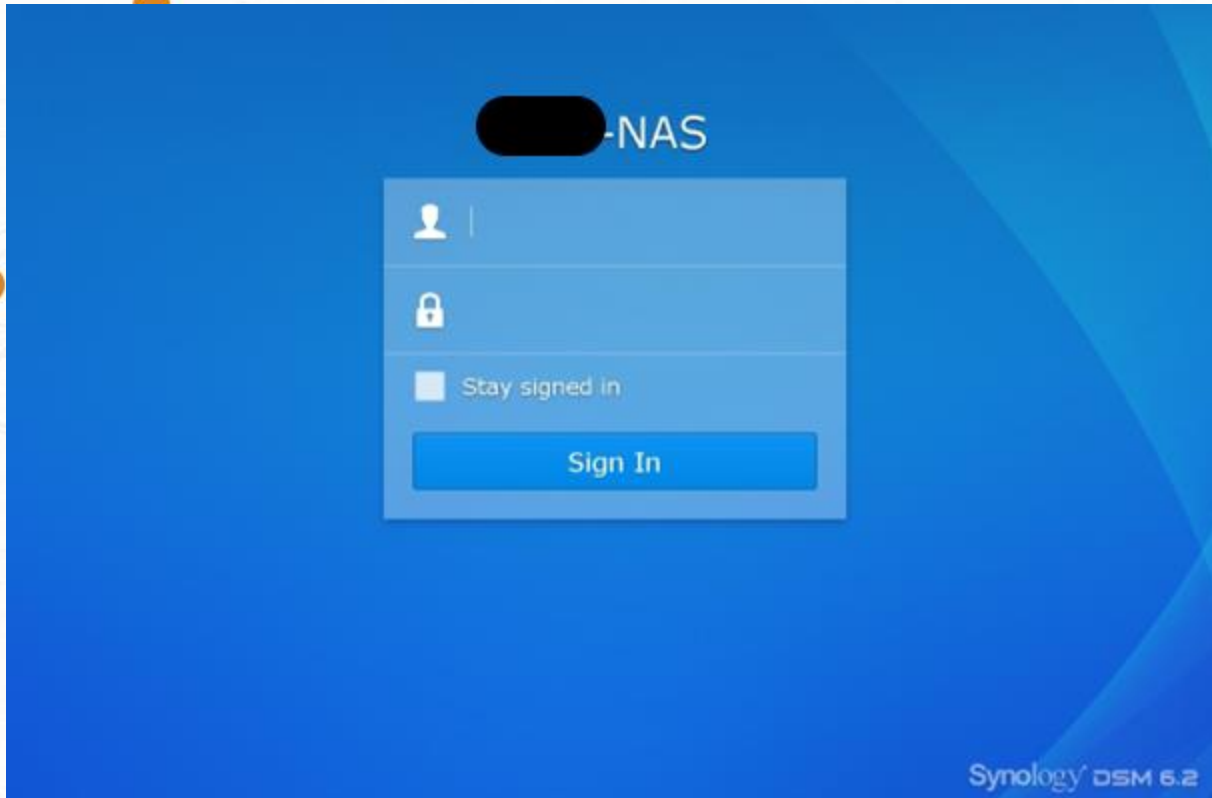
AMOEBAS (APT41)



Case study 3

Goushe (a.k.a. TropicTropper, 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。

相關變更
上傳檔案
特殊頁面
固定連結
頁面資訊
引用此頁面
維基數據項目
左側條目連結
短網址

列印/匯出
下載為 PDF
可列印版

其他專案
維基共享資源

其他語言

- العربية
- English
- Español
- Français
- हिन्दी
- Bahasa Indonesia
- Bahasa Melayu
- Português
- Русский

还有 35 種語言

編輯連結

==== 中国大陆 ====

“[[中华人民共和国外交部]]发言人[[赵立坚]]於6月1日表示，中方关注事态发展，认为黑人的人权也需要保障，希望美方保障少数族裔的权利，履行《消除一切形式种族歧视国际公约》规定的义务。他还说，美方将香港的港独势力和黑色暴力分子美化为英雄斗士，而将美国国内抗议种族歧视的民众称之为暴徒的做法是最典型的“世界驰名双重标准”<ref>{{cite news |editor=郭梦媛 |title=外交部：黑人的命也是命 望美方保障少数族裔合法权利 |url=http://www.chinanews.com/gn/2020/06-01/9200363.shtml |accessdate=2020-06-01 |work=中国新闻网 |date=2020-06-01}}</ref>。

==== 俄罗斯 ==== Russia

“俄罗斯外交部谴责美警袭击记者行为并提醒美国政府所承担的保障媒体记者安全和采访权利、言论自由以及知情权的国际义务，呼吁相应国际组织和维权组织对于这起事件做出应有的反应。”<ref>{{cite web|title=俄外交部发声：美国警方对记者使用催泪喷雾 粗暴行为不可接受 |url=https://world.huanqiu.com/article/3y5wGcm1tYg|accessdate=2020-06-01|date=2020-05-31|language=zh}}</ref>

==== 新西兰 ==== New Zealand

“紐西蘭總理[[傑辛達·阿德恩]]在接受[[紐西蘭電台]]採訪時表示警員暴力執法導致喬治·弗洛伊德死亡一事令她感到「恐懼」。她同時表示支持在紐西蘭舉行的和平聲援遊行，但要求示威者遵守保持社交距離的規定。”<ref>{{cite web|title=Jacinda Ardern tells off thousands who flouted social distancing rules at Auckland Black Lives Matter protest |url=https://www.tvnz.co.nz/one-news/new-zealand/jacinda-ardern-tells-off-thousands-flouted-social-distancing-rules-auckland-black-lives-matter-protest|website=TVNZ |language=en|access-date=2020-06-02}}</ref>

==== 香港 ==== Hong Kong

“[[香港特別行政區行政長官]]林鄭月娥6月2日早上在記者會上批評部分外國政府對香港止暴制亂的高調反應，展現的是“雙重標準”。她称，自己国家安全就很重要，对香港的情况却戴着有色眼镜去看。她还特别明确指出，自己所指的就是美国近日的反警察暴力执法引发的骚乱，当地政府处理手法也很强硬”<ref>{{cite news |title=林郑月娥批评美国处理骚乱“双重标准” 明日就国安法率队访京 |url=http://www.rfi.fr/cn/%E6%88%AF%E6%B8%B3%E5%8F%B0/20200602-%E6%9E%97%E9%83%91%E6%9C%88%E5%A8%A5%E6%98%9B%E8%AF%84%E7%B8%8E%E5%9B%B0%E5%A4%84%E7%90%86%E9%A4%A9%E4%B9%B1-%E5%8F%8C%E9%87%80%E6%A0%87%E5%87%B6-%E6%98%8E%E6%97%A5%E8%08%B1%E5%98%B0%E5%AE%89%6E%83%95%E7%B8%7E%E9%98%9F%E8%AE%BF%E4%B8%A4 |work=RFI - 法国国际广播电台 |date=2020-06-02 |language=zh-CN}}</ref>。

==== 中华人民共和国 ==== "Mainland China" changed to "People's Replib of China"

“[[中华人民共和国外交部]]发言人[[赵立坚]]於6月1日表示，中方关注事态发展，认为黑人的人权也需要保障，希望美方保障少数族裔的权利，履行《消除一切形式种族歧视国际公约》规定的义务。他还说，美方将香港的港独势力和黑色暴力分子美化为英雄斗士，而将美国国内抗议种族歧视的民众称之为暴徒的做法是最典型的“世界驰名双重标准”<ref>{{cite news |editor=郭梦媛 |title=外交部：黑人的命也是命 望美方保障少数族裔合法权利 |url=http://www.chinanews.com/gn/2020/06-01/9200363.shtml |accessdate=2020-06-01 |work=中国新闻网 |date=2020-06-01}}</ref>。

“共青團中央官方微博稱美國騷亂是「美羅的風景線」，藉機譏刺美國國會眾議院議長佩洛西形容香港的遊行示威是「一道美麗的風景線」。<ref>{{cite web |author=褚文 |title=【明尼蘇達示威】共青團中央譏美國騷亂是「美羅風景線」 |url=https://www.hk01.com/即時中國/479413/明尼蘇達示威-共青團中央譏美國騷亂是-美羅風景線 |website=香港01 |accessdate=2020-06-05 |language=zh-hk |date=2020-05-29}}</ref>

“[[香港特別行政區行政長官]]林鄭月娥6月2日早上在記者會上批評部分外國政府對香港止暴制亂的高調反應，展現的是“雙重標準”。她称，自己国家安全就很重要，对香港的情况却戴着有色眼镜去看。她还特别明确指出，自己所指的就是美国近日的反警察暴力执法引发的骚乱，当地政府处理手法也很强硬”<ref>{{cite news |title=林郑月娥批评美国处理骚乱“双重标准” 明日就国安法率队访京 |url=http://www.rfi.fr/cn/%E6%88%AF%E6%B8%B3%E5%8F%B0/20200602-%E6%9E%97%E9%83%91%E6%9C%88%E5%A8%A5%E6%98%9B%E8%AF%84%E7%B8%8E%E5%9B%B0%E5%A4%84%E7%90%86%E9%A4%A9%E4%B9%B1-%E5%8F%8C%E9%87%80%E6%A0%87%E5%87%B6-%E6%98%8E%E6%97%A5%E8%08%B1%E5%98%B0%E5%AE%89%6E%83%95%E7%B8%7E%E9%98%9F%E8%AE%BF%E4%B8%A4 |work=RFI - 法国国际广播电台 |date=2020-06-02 |language=zh-CN}}</ref>。

==== 俄罗斯 ====

“俄罗斯外交部谴责美警袭击记者行为并提醒美国政府所承担的保障媒体记者安全和采访权利、言论自由以及知情权的国际义务，呼吁相应国际组织和维权组织对于这起事件做出应有的反应。”<ref>{{cite web|title=俄外交部发声：美国警方对记者使用催泪喷雾 粗暴行为不可接受 |url=https://world.huanqiu.com/article/3y5wGcm1tYg|accessdate=2020-06-01|date=2020-05-31|language=zh}}</ref>

==== 新西兰 ====

“紐西蘭總理[[傑辛達·阿德恩]]在接受[[紐西蘭電台]]採訪時表示警員暴力執法導致喬治·弗洛伊德死亡一事令她感到「恐懼」。她同時表示支持在紐西蘭舉行的和平聲援遊行，但要求示威者遵守保持社交距離的規定。”<ref>{{cite web|title=Jacinda Ardern tells off thousands who flouted social distancing rules at Auckland Black Lives Matter protest |url=https://www.tvnz.co.nz/one-news/new-zealand/jacinda-ardern-tells-off-thousands-flouted-social-distancing-rules-auckland-black-lives-matter-protest|website=TVNZ |language=en|access-date=2020-06-02}}</ref>

Statement from the Communist Youth League of China

"Reaction from Hong Kong" moved from its own tag to part of the "Reaction from China"

AGENDA

1 Introduction

2 Detecting compromised NAS devices

3 Experiments & Validation

4 Real-World Case studies

5 Conclusion

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！



Career Fair 攤位編號 **9**

Questions?