Aug. 2022

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

Charles Li

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

AGENDA

1 Introduction

2 Detecting compromised NAS devices

3 Experiments & Validation

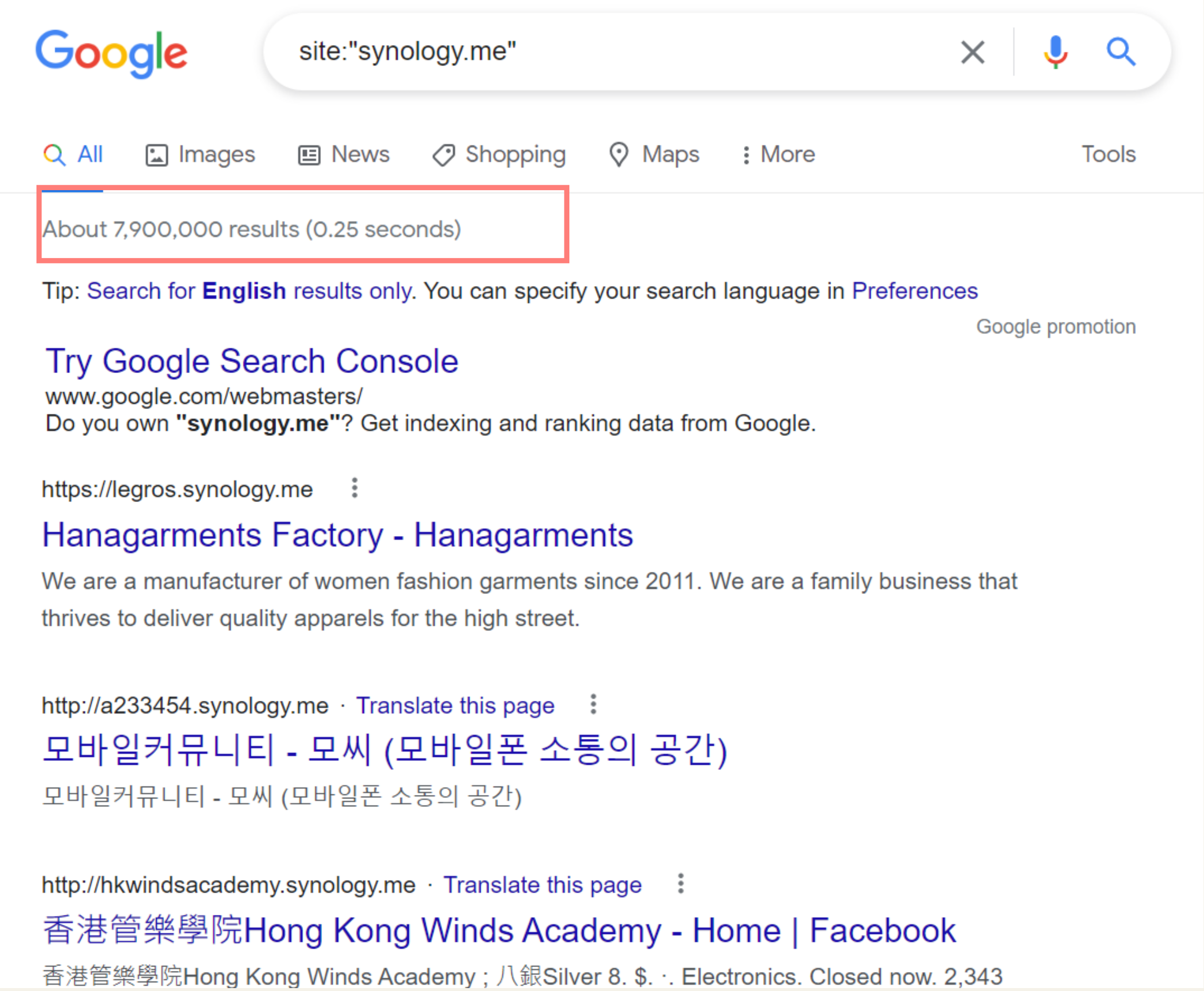
4 Real-World Case studies

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



site:"synology.me"

About 7,900,000 results (0.25 seconds)

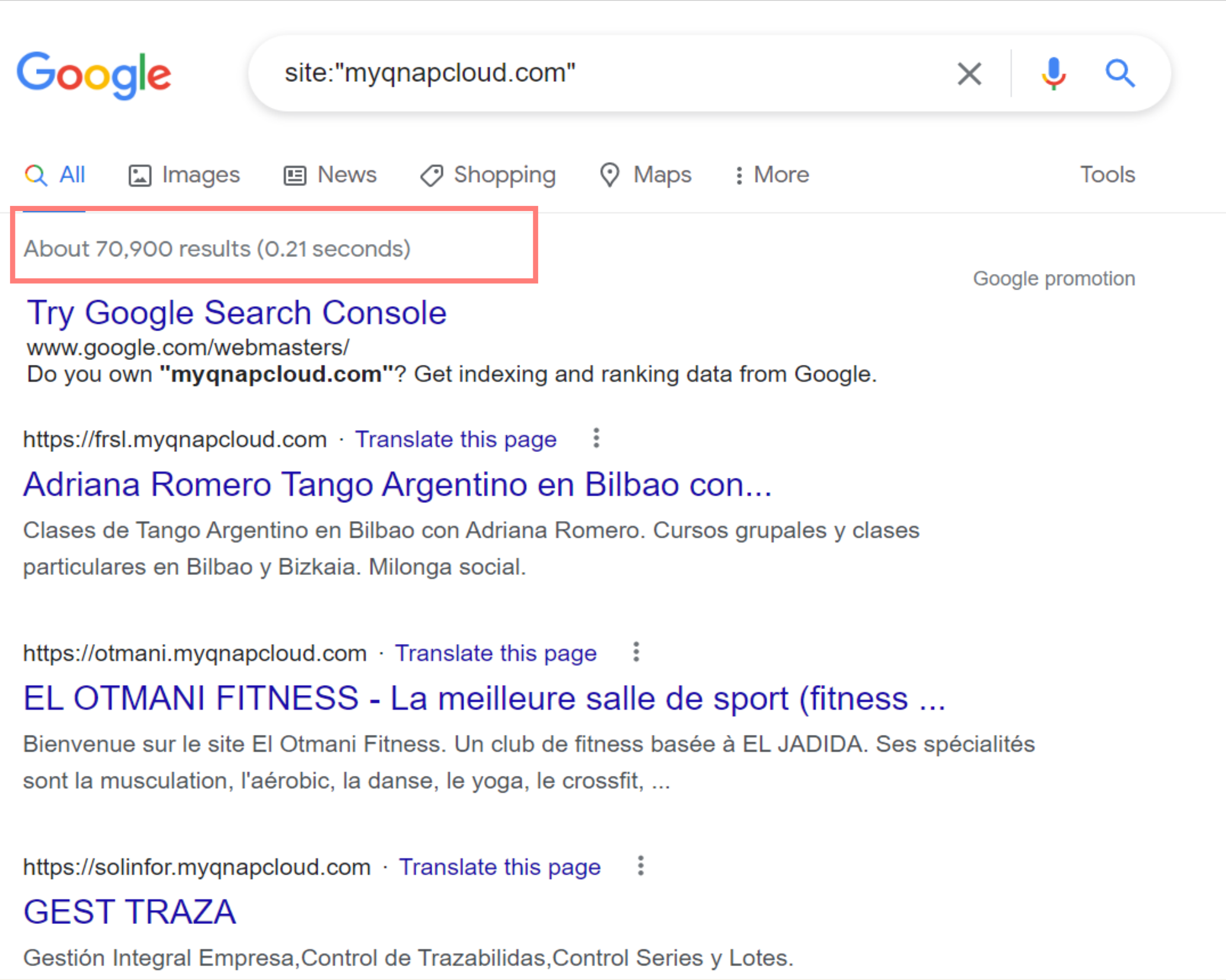
Tip: Search for **English** results only. You can specify your search language in Preferences

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



site:"myqnapcloud.com"

About 70,900 results (0.21 seconds)

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.

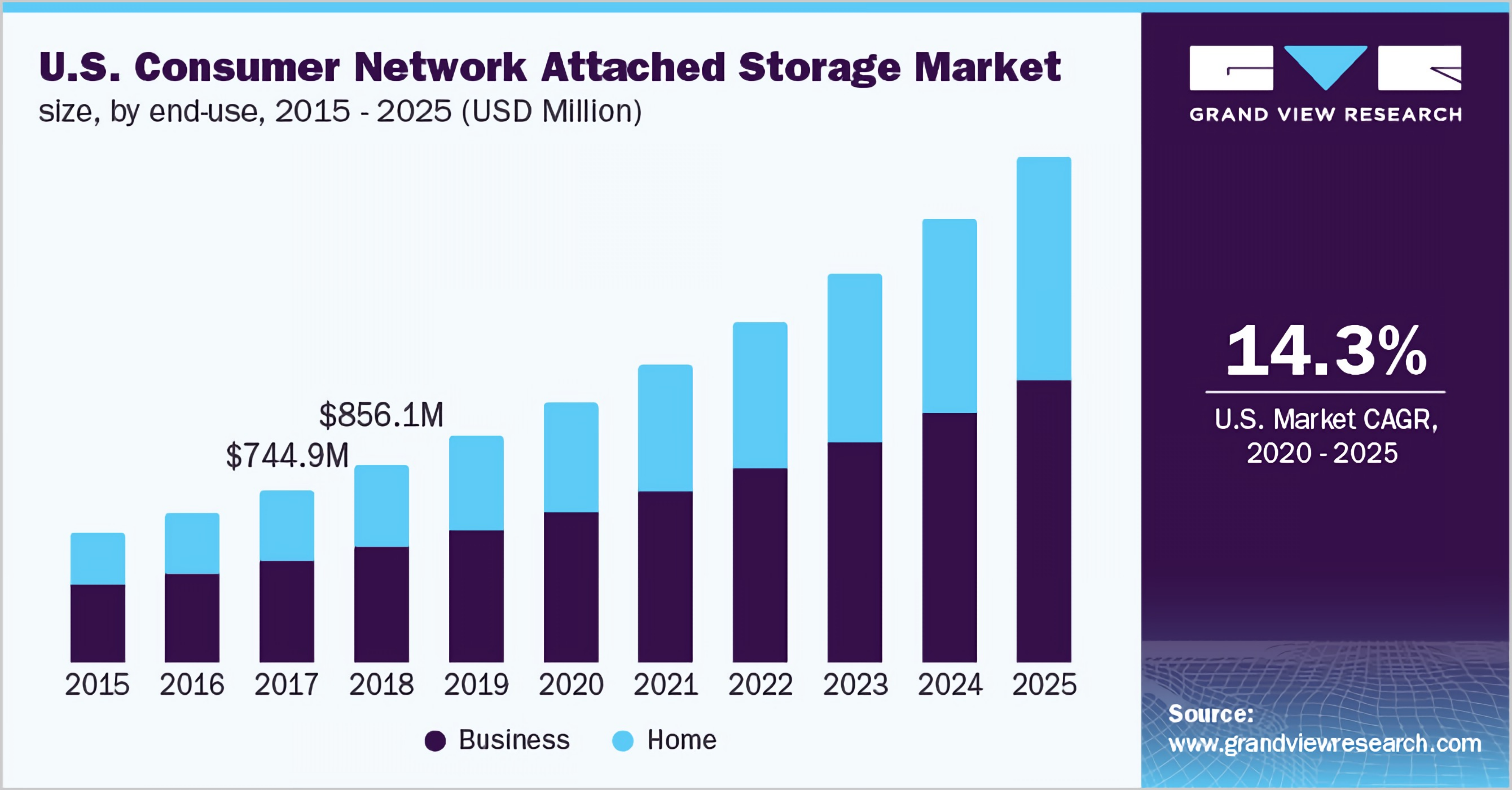
NAS Opened to WAN

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)

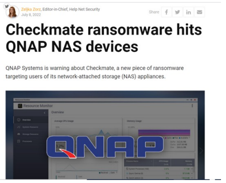
14.3%

U.S. Market CAGR, 2020 - 2025

Source: www.grandviewresearch.com

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

Attacks related to NAS Devices

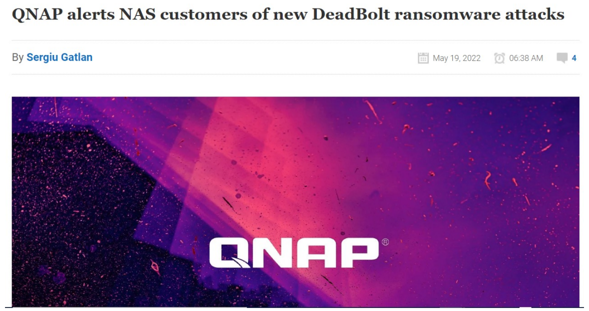


Zeljka Zorz, Editor-in-Chief, Help Net Security
July 8, 2022

Share

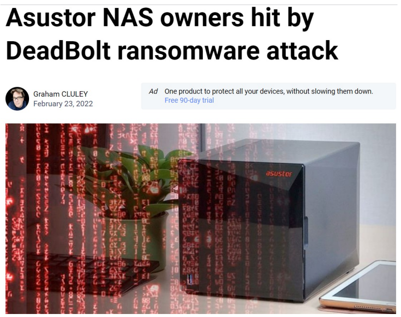
Checkmate ransomware hits QNAP NAS devices

QNAP Systems is warning about Checkmate, a new piece of ransomware targeting users of its network-attached storage (NAS) appliances.



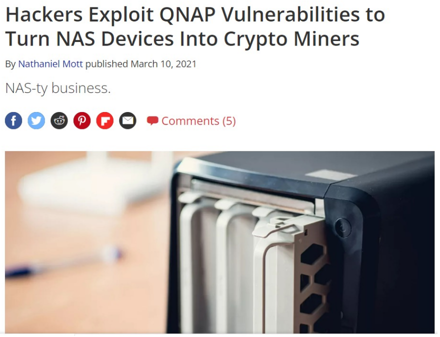
QNAP alerts NAS customers of new DeadBolt ransomware attacks

By Sergiu Gatlan May 19, 2022 06:38 AM 4



Asustor NAS owners hit by DeadBolt ransomware attack

Graham CLULEY
February 23, 2022

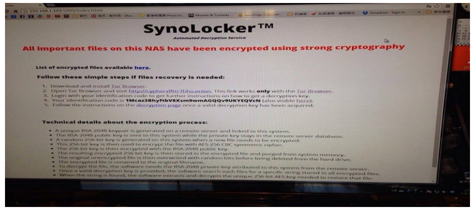


Hackers Exploit QNAP Vulnerabilities to Turn NAS Devices Into Crypto Miners

By Nathaniel Mott published March 10, 2021

NAS-ty business.

Comments (5)



192.168.1.103:5000/index.html

SynoLocker™

Automated Decryption Service

All important files on this NAS have been encrypted using strong cryptography

List of encrypted files available here.

Follow these simple steps if files recovery is needed:

1. Download and install Tor Browser.
2. Open Tor Browser and visit http://cypherxffttr7hho.onion. This link works **only** with the Tor Browser.
3. Login with your identification code to get further instructions on how to get a decryption key.
4. Your identification code is **1Mcaz3BhyftbV8Xsm9wmAGQQv9UKYEQVcN** (also visible here).
5. Follow the instructions on the decryption page once a valid decryption key has been acquired.

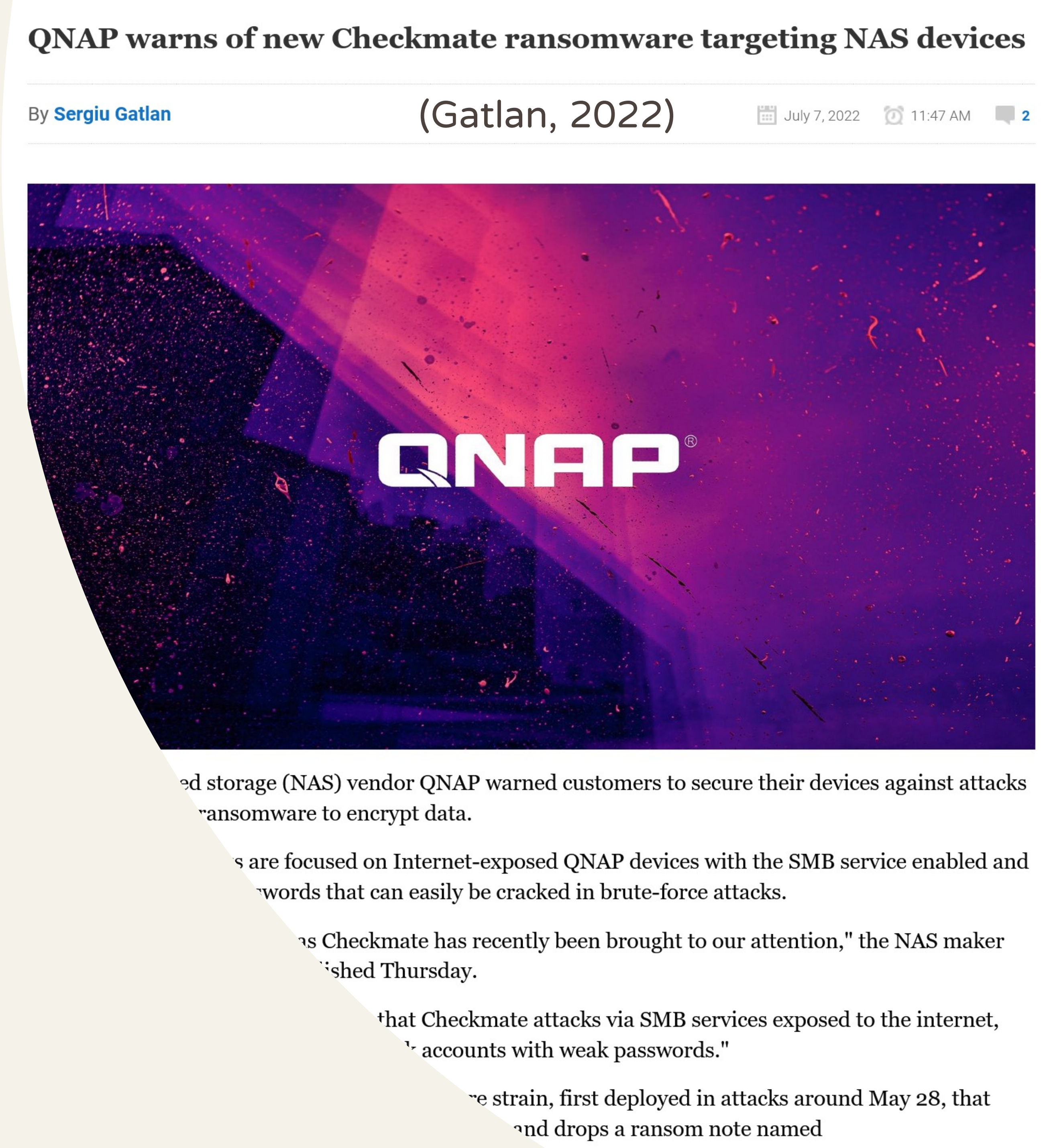
Technical details about the encryption process:

- A unique RSA-2048 keypair is generated on a remote server and linked to this system.
- The RSA-2048 public key is sent to this system while the private key stays in the remote server database.
- A random 256-bit key is generated on this system when a new file needs to be encrypted.
- This 256-bit key is then used to encrypt the file with AES-256 CBC symmetric cipher.
- The 256-bit key is then encrypted with the RSA-2048 public key.
- The resulting encrypted 256-bit key is then stored in the encrypted file and purged from system memory.
- The original unencrypted file is then overwrited with random bits before being deleted from the hard drive.
- The encrypted file is renamed to the original filename.
- To decrypt the file, the software needs the RSA-2048 private key attributed to this system from the remote server.
- Once a valid decryption key is provided, the software search each files for a specific string stored in all encrypted files.
- When the string is found, the software extracts and decrypts the unique 256-bit AES key needed to restore that file.

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** July 7, 2022 11:47 AM 2

(Gatlan, 2022)

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

as 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."

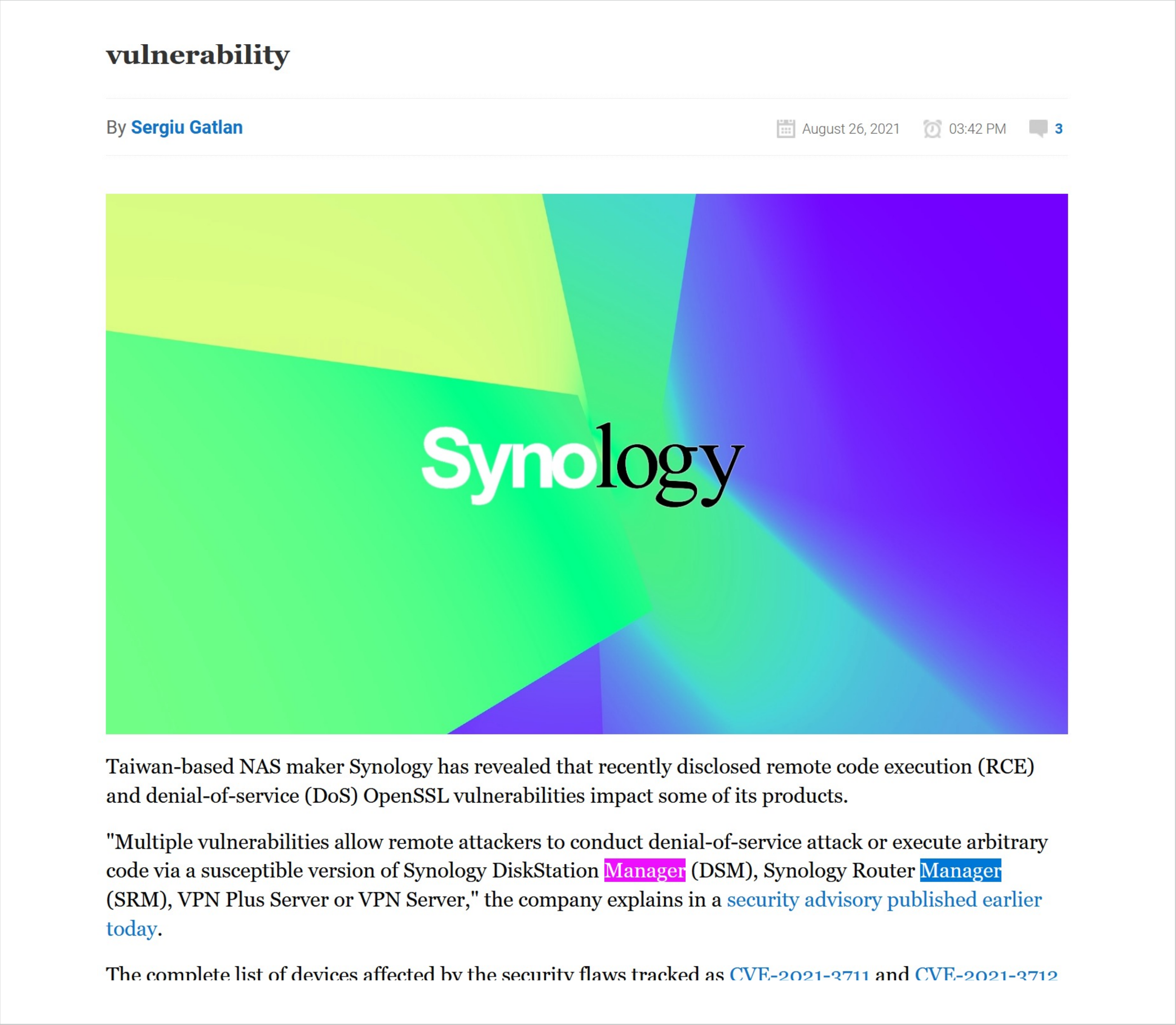
re strain, first deployed in attacks around May 28, that
and drops a ransom note named

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.)

(Gatlan, 2021)



vulnerability

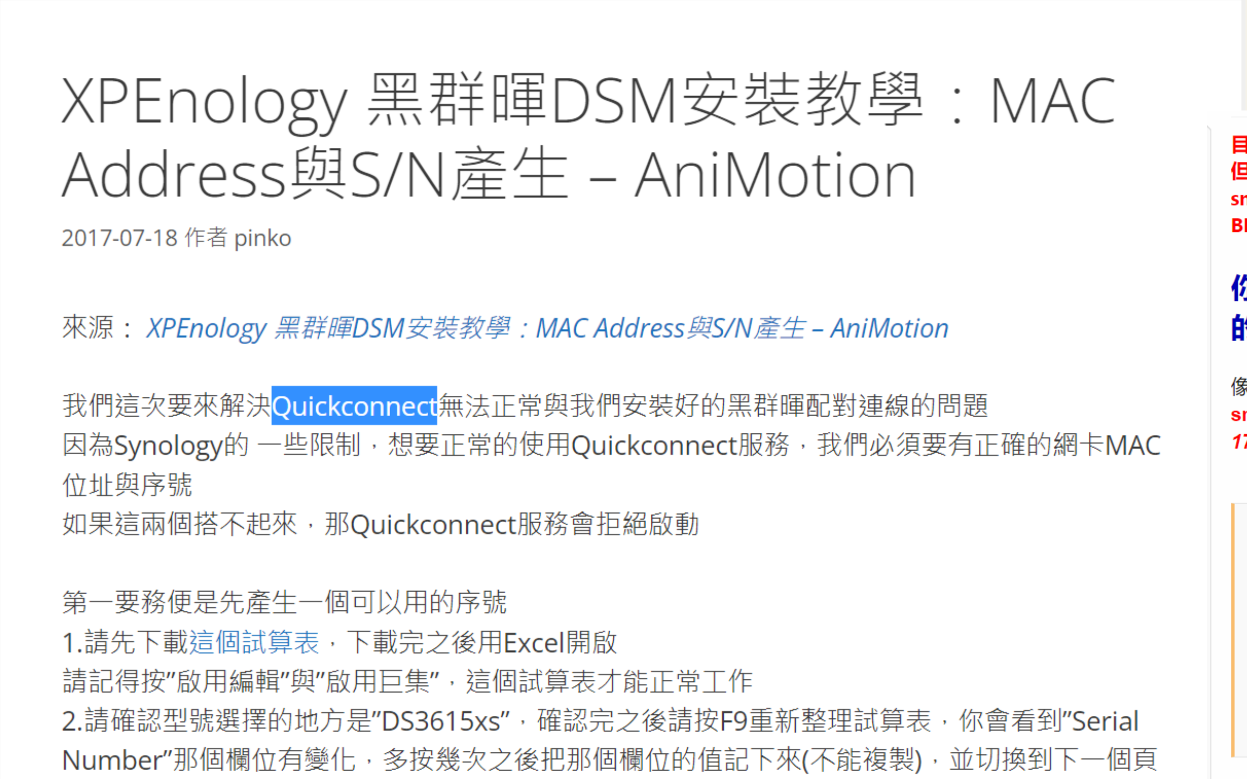
By **Sergiu Gatlan** August 26, 2021 03:42 PM 3

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



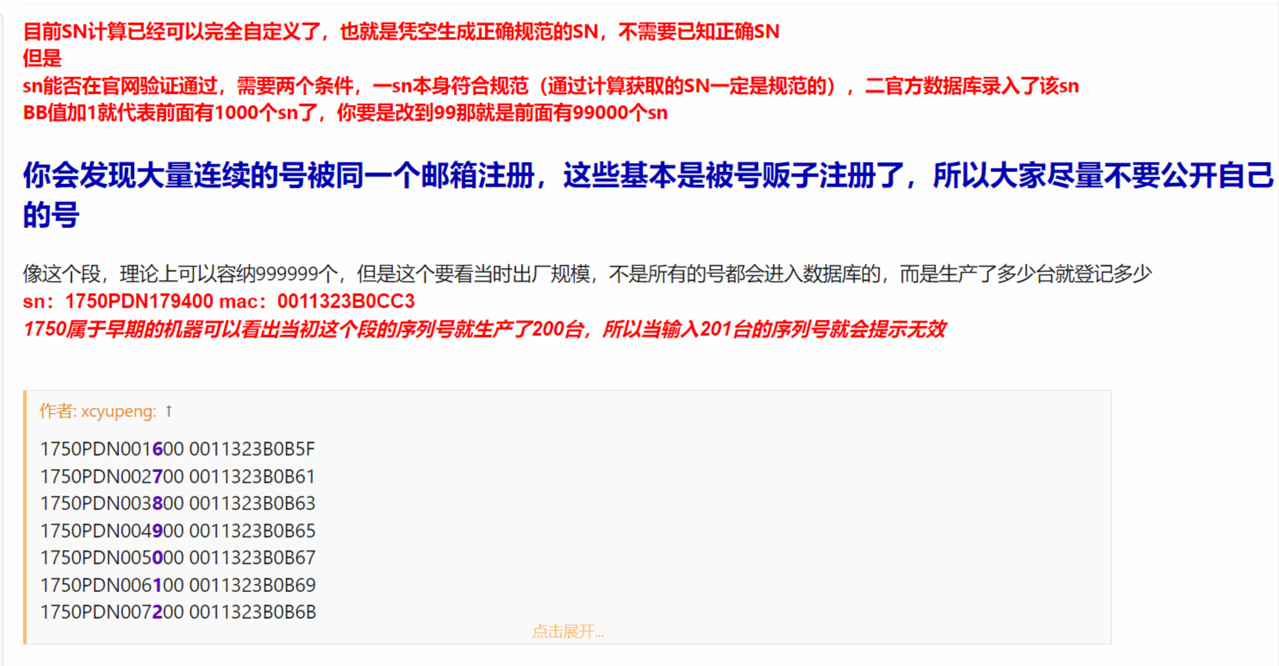
XPEnology 黑群暉DSM安裝教學：MAC Address與S/N產生 – AniMotion

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，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: ↑
>
> 1750PDN001**6**00 0011323B0B5F
> 1750PDN002**7**00 0011323B0B61
> 1750PDN003**8**00 0011323B0B63
> 1750PDN004**9**00 0011323B0B65
> 1750PDN005**0**00 0011323B0B67
> 1750PDN006**1**00 0011323B0B69
> 1750PDN007**2**00 0011323B0B6B
>
> 点击展开...

AGENDA

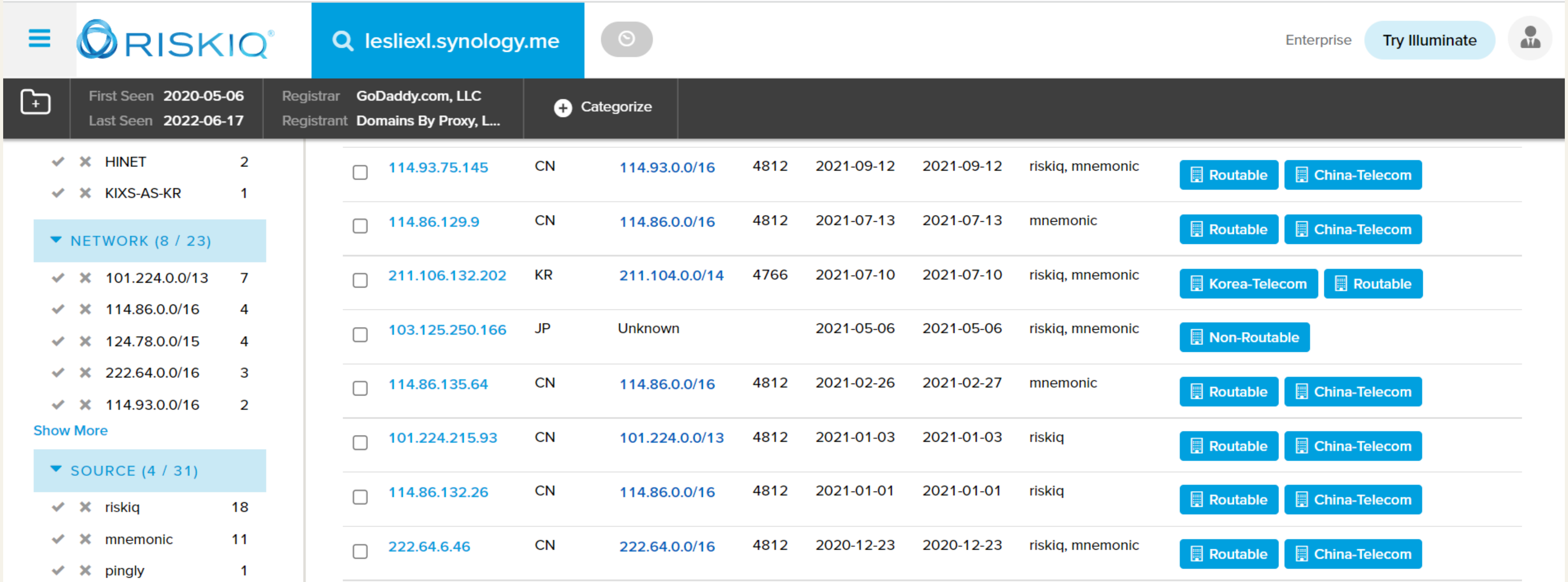
1 Introduction

2 Detecting compromised NAS devices

3 Experiments & Validation

4 Real-World Case studies

5 Conclusion



RISKIQ

lesliexl.synology.me

Enterprise Try Illuminate

First Seen 2020-05-06
Last Seen 2022-06-17

Registrar GoDaddy.com, LLC
Registrant Domains By Proxy, L...

Categorize

✓	✗	HINET	2
✓	✗	KIXS-AS-KR	1

NETWORK (8 / 23)

✓	✗	101.224.0.0/13	7
✓	✗	114.86.0.0/16	4
✓	✗	124.78.0.0/15	4
✓	✗	222.64.0.0/16	3
✓	✗	114.93.0.0/16	2

Show More

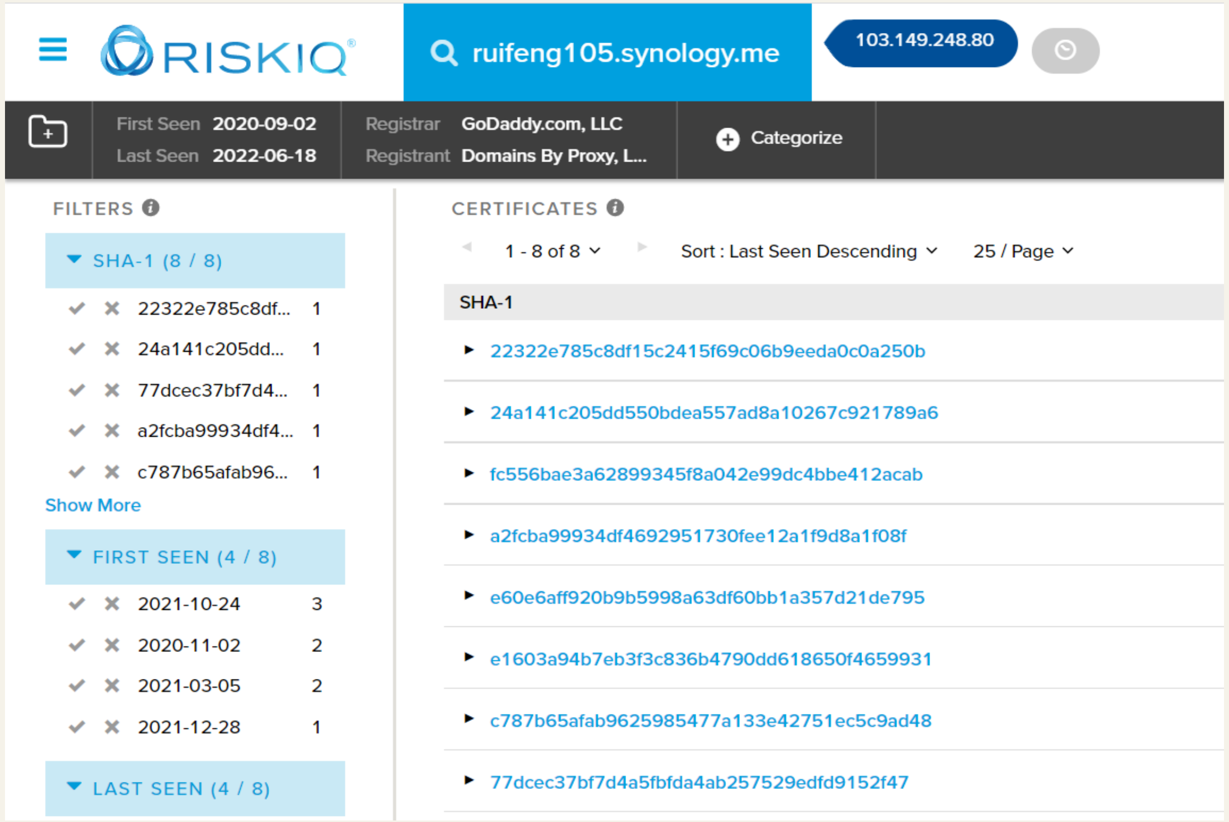
SOURCE (4 / 31)

✓	✗	riskiq	18
✓	✗	mnemonic	11
✓	✗	pingly	1

□	114.93.75.145	CN	114.93.0.0/16	4812	2021-09-12	2021-09-12	riskiq, mnemonic	Routable China-Telecom
□	114.86.129.9	CN	114.86.0.0/16	4812	2021-07-13	2021-07-13	mnemonic	Routable China-Telecom
□	211.106.132.202	KR	211.104.0.0/14	4766	2021-07-10	2021-07-10	riskiq, mnemonic	Korea-Telecom Routable
□	103.125.250.166	JP	Unknown		2021-05-06	2021-05-06	riskiq, mnemonic	Non-Routable
□	114.86.135.64	CN	114.86.0.0/16	4812	2021-02-26	2021-02-27	mnemonic	Routable China-Telecom
□	101.224.215.93	CN	101.224.0.0/13	4812	2021-01-03	2021-01-03	riskiq	Routable China-Telecom
□	114.86.132.26	CN	114.86.0.0/16	4812	2021-01-01	2021-01-01	riskiq	Routable China-Telecom
□	222.64.6.46	CN	222.64.0.0/16	4812	2020-12-23	2020-12-23	riskiq, mnemonic	Routable China-Telecom

Anomaly NAS – Traveling Devices

Anomaly NAS – Multiple NAS on the same IP address



RISKIQ

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

Show More

FIRST SEEN (4 / 8)

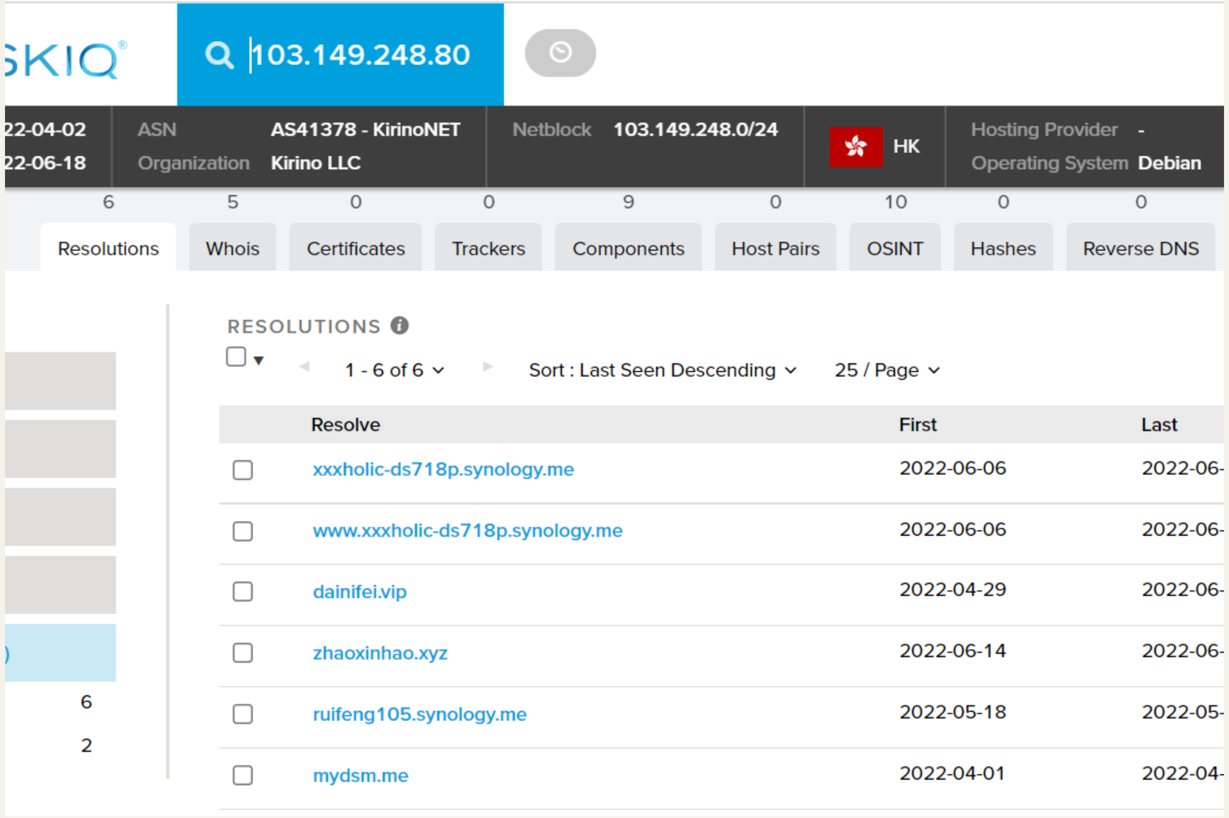
2021-10-24	3
2020-11-02	2
2021-03-05	2
2021-12-28	1

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



SKIQ

103.149.248.80

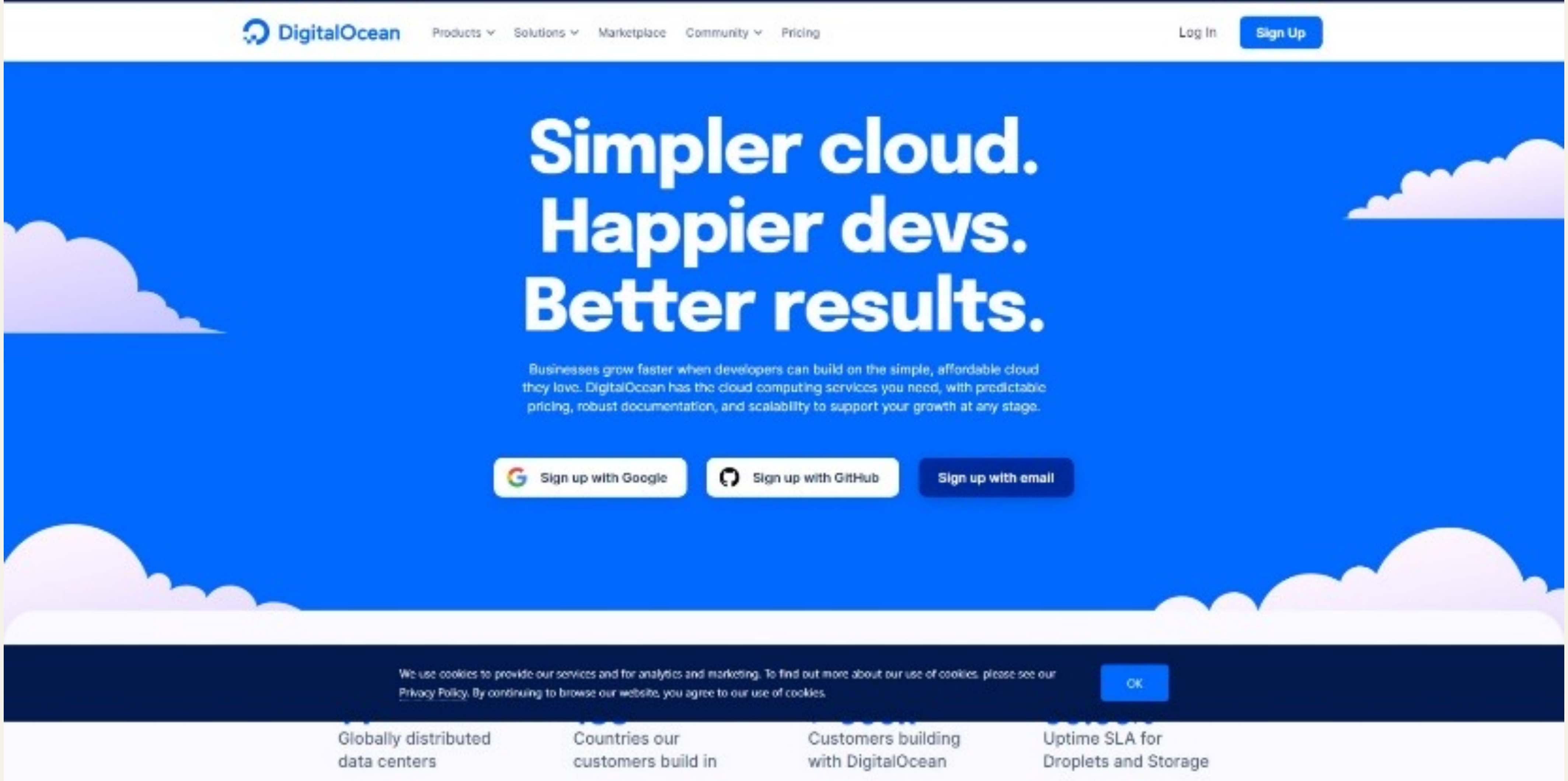
	22-04-02
	22-06-18
ASN	AS41378 - KirinoNET
Organization	Kirino LLC
Netblock	103.149.248.0/24
	HK
Hosting Provider	-
Operating System	Debian

Resolutions	Whois	Certificates	Trackers	Components	Host Pairs	OSINT	Hashes	Reverse DNS
6	5	0	0	9	0	10	0	0

RESOLUTIONS

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

	Resolve	First	Last
□	xxxholic-ds718p.synology.me	2022-06-06	2022-06-
□	www.xxxholic-ds718p.synology.me	2022-06-06	2022-06-
□	dainifei.vip	2022-04-29	2022-06-
□	zhaoxinhao.xyz	2022-06-14	2022-06-
□	ruifeng105.synology.me	2022-05-18	2022-05-
□	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.

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.

Globally distributed data centers

Countries our customers build in

Customers building with DigitalOcean

Uptime SLA for Droplets and Storage

Anomaly NAS – VPS

AGENDA

TEAMT5
杜浦數位安全

1 Introduction

2 Detecting compromised NAS devices

3 Experiments & Validation

4 Real-World Case studies

5 Conclusion

Experiment & Detection

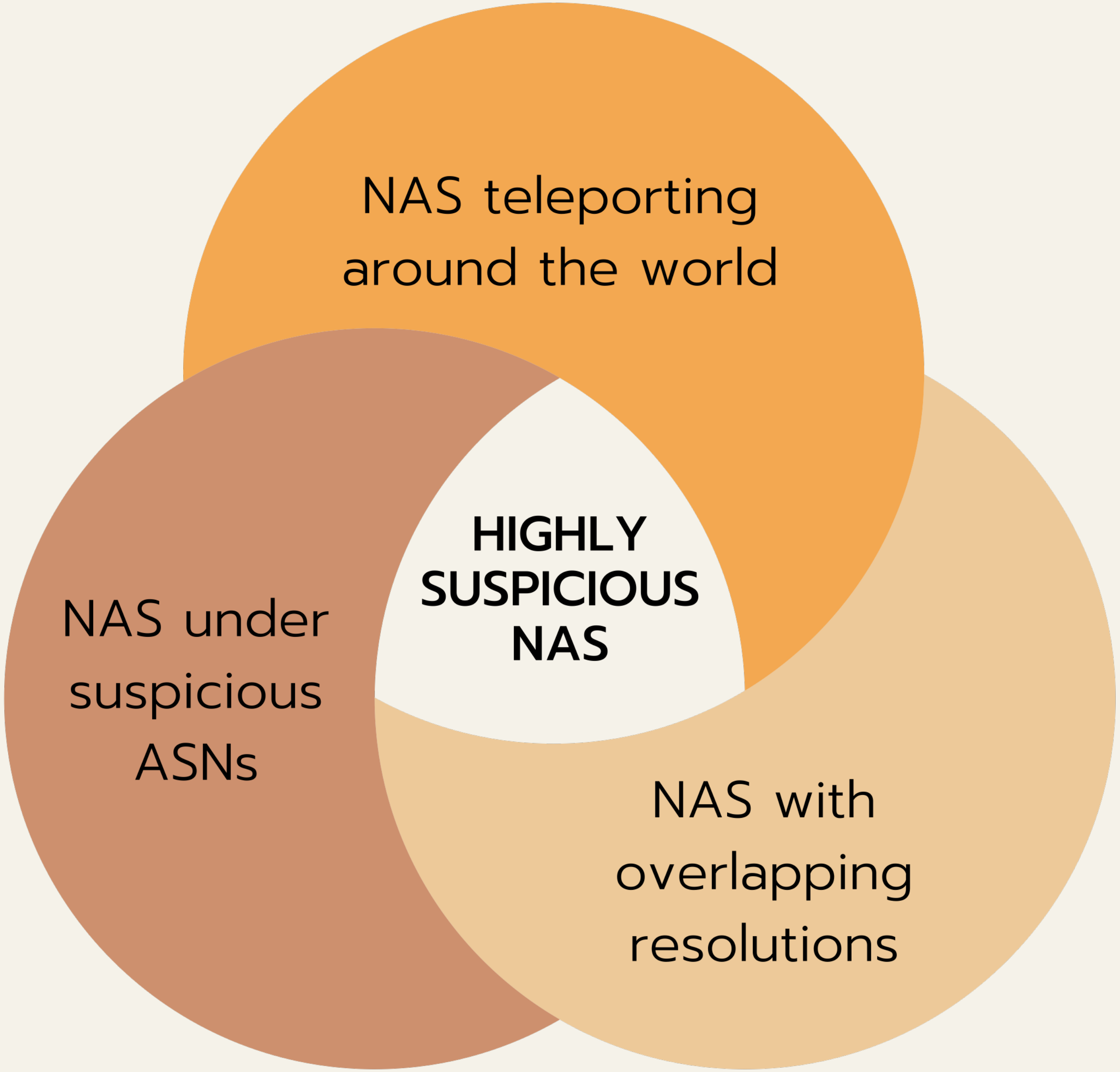
Experiment data sets: subdomains collected in the wild [1]

- 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/



NAS teleporting around the world

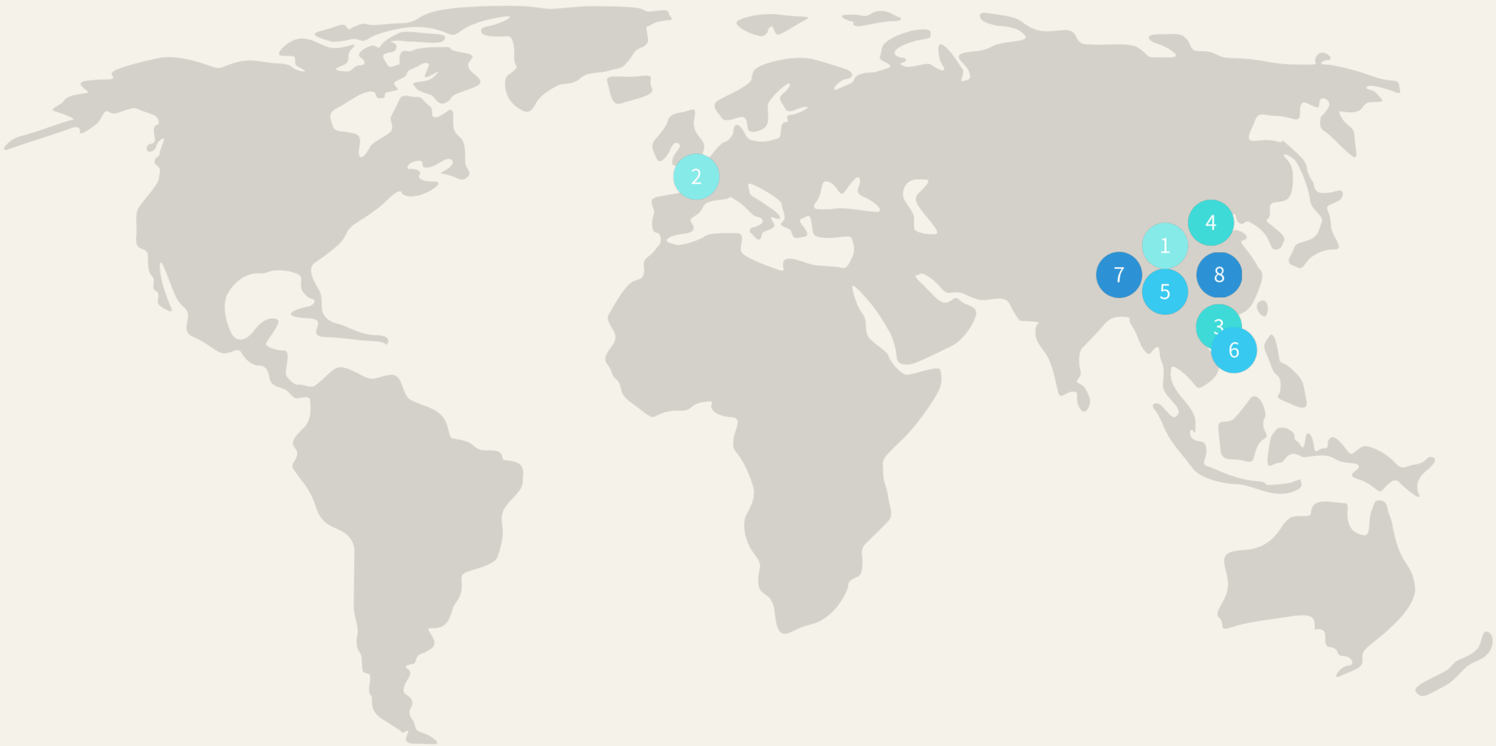
NAS under suspicious ASNs

NAS with overlapping resolutions

HIGHLY SUSPICIOUS NAS

Highly Suspicious NAS #1

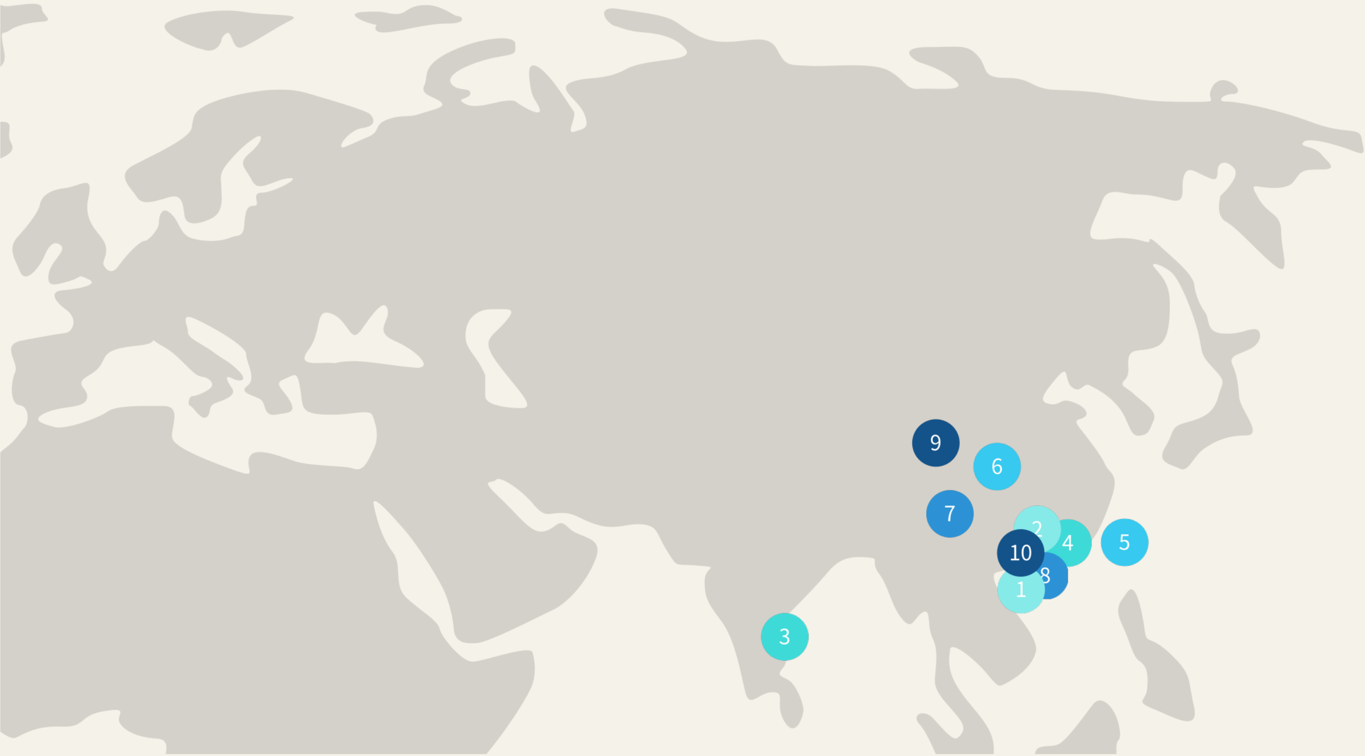
Online about 2 days for each



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

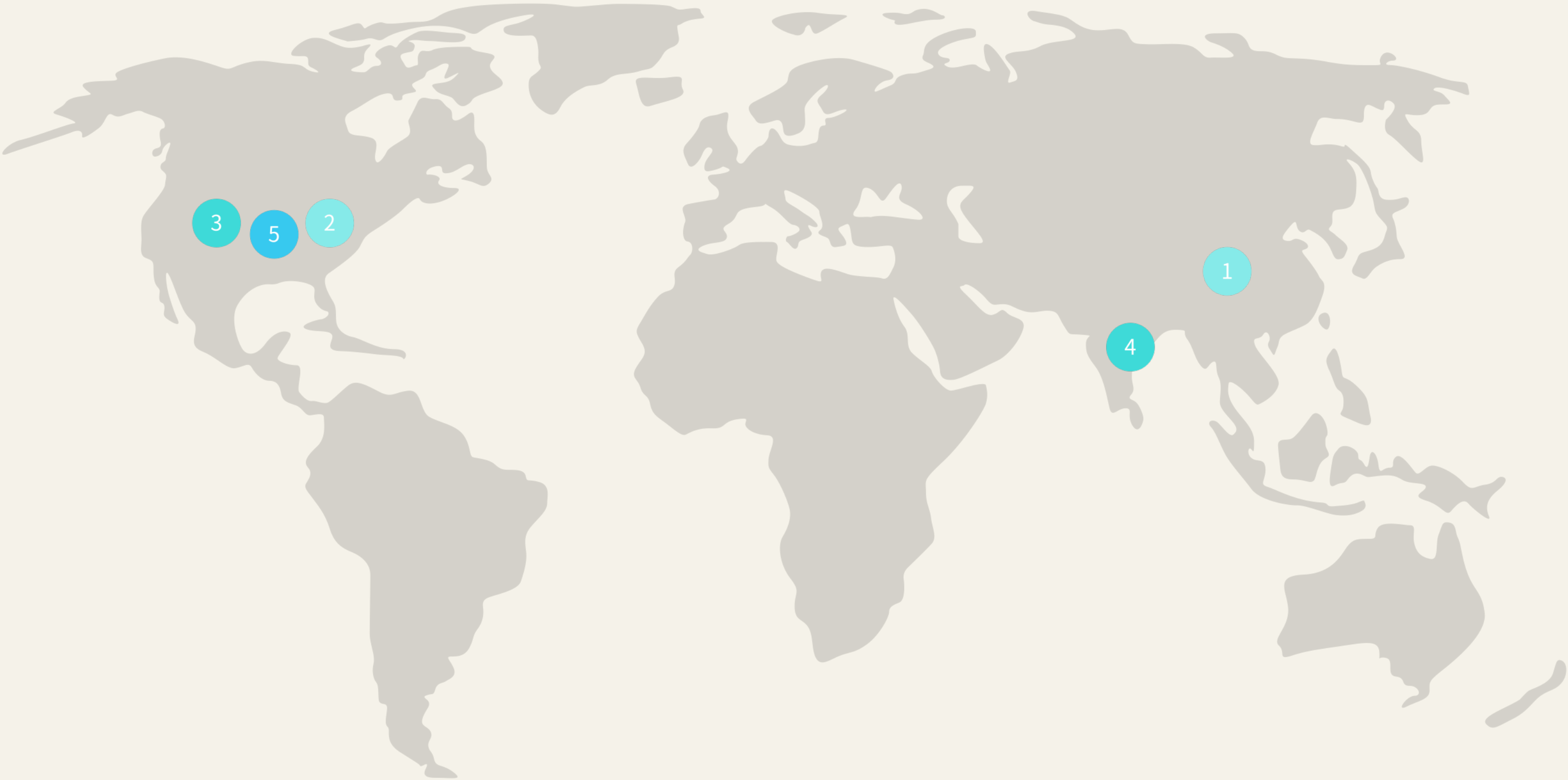
Online about 1~2 day(s) for each



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

TEAMT5 杜浦數位安全

1 Introduction

2 Detecting compromised NAS devices

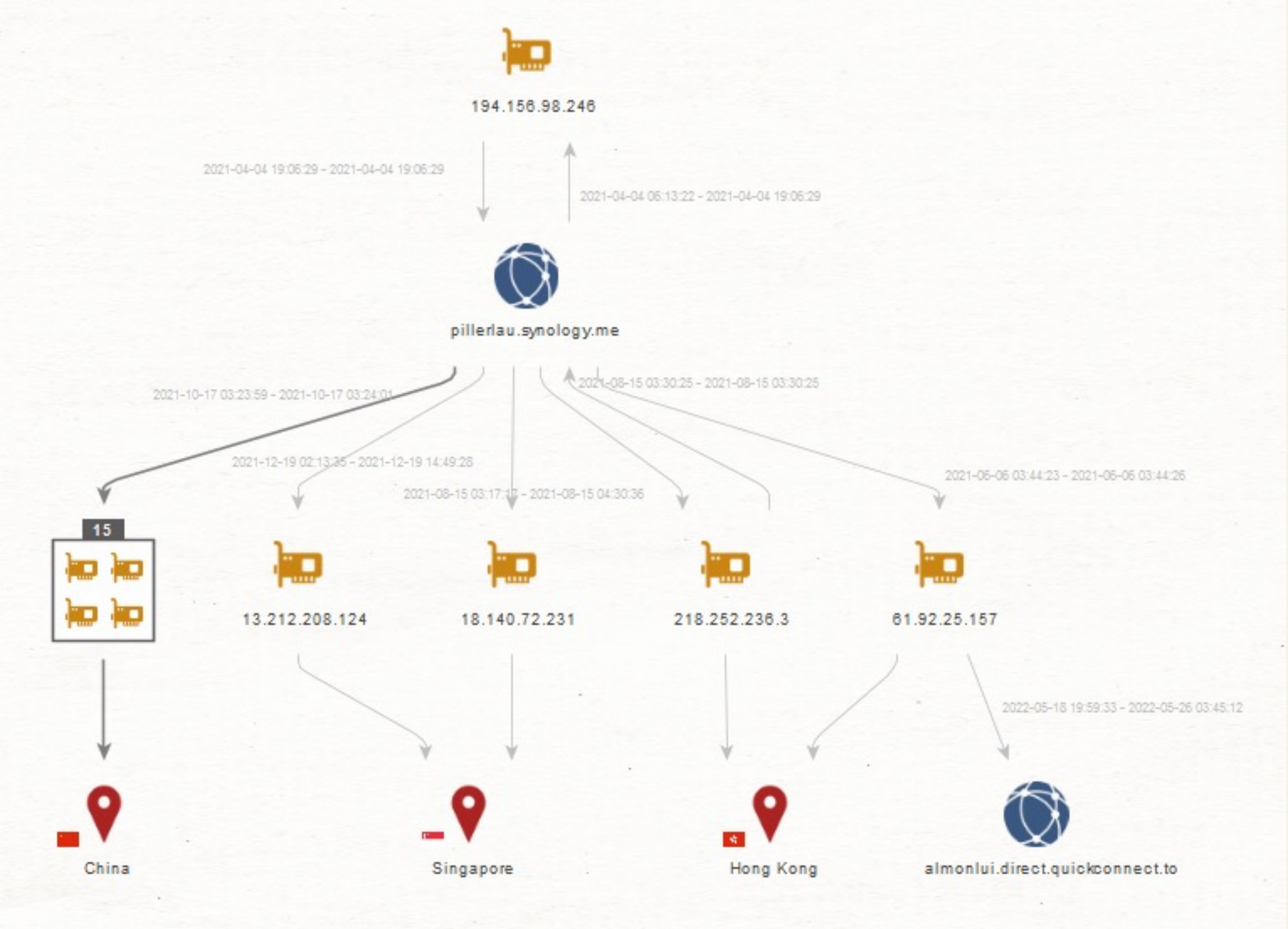
3 Experiments & Validation

4 Real-World Case studies

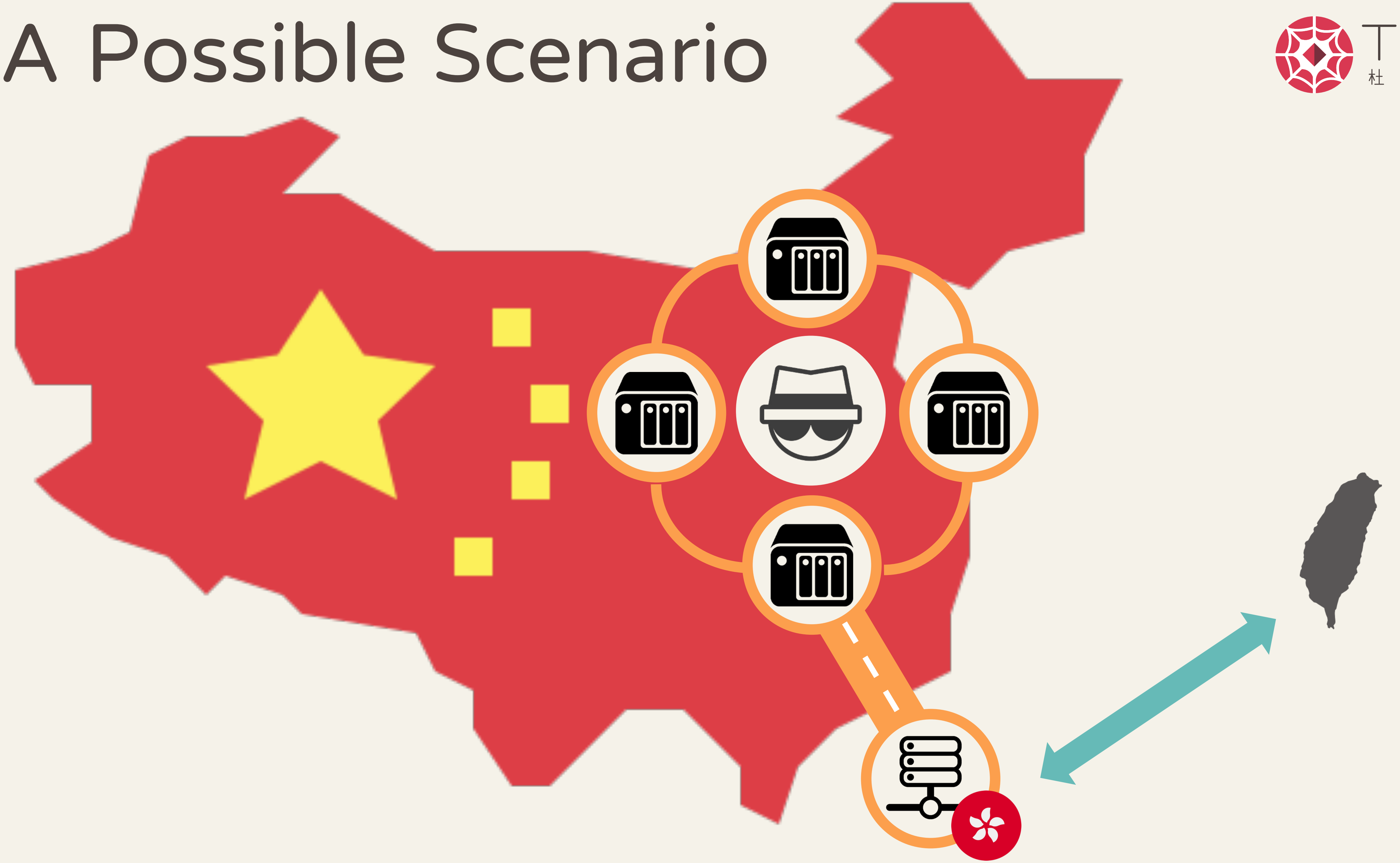
5 Conclusion

Case Study 1

SLIME40 (a.k.a FamousSparrow, GhostEmperor)

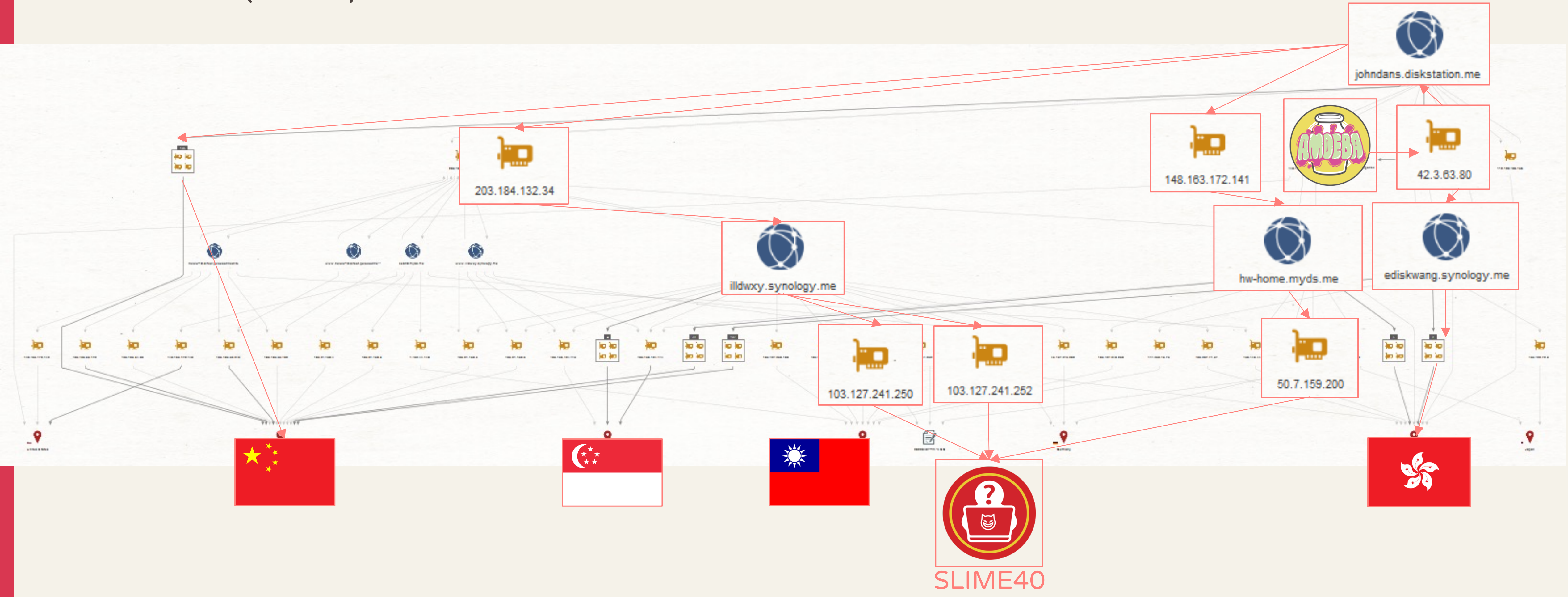


A Possible Scenario



Case study 2

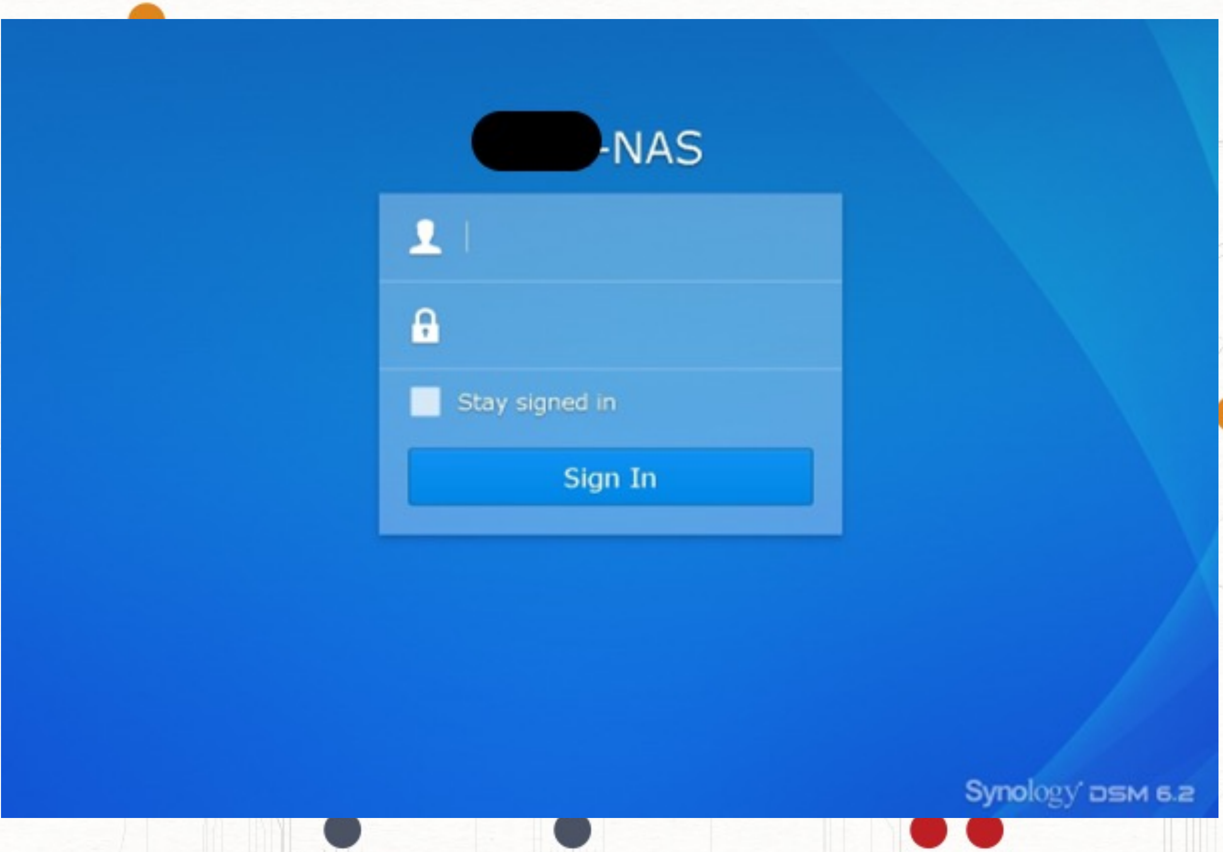
AMOEBA (APT41)



Case study 3

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

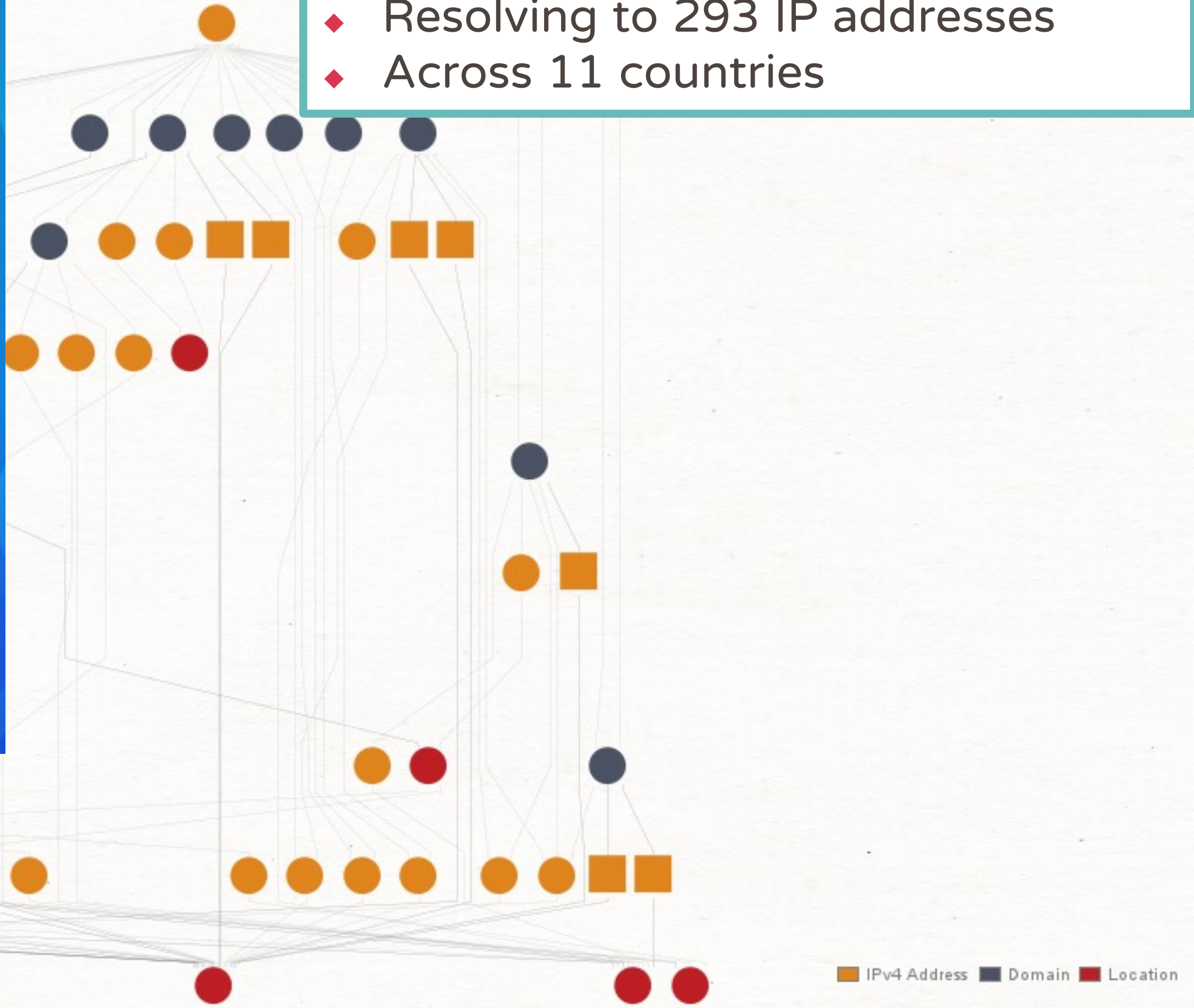
- 4 Source IP accessing TEBShell
- Pivoting to 17 NAS DDNS domains
- Resolving to 293 IP addresses
- Across 11 countries



[redacted]-NAS

□ Stay signed in

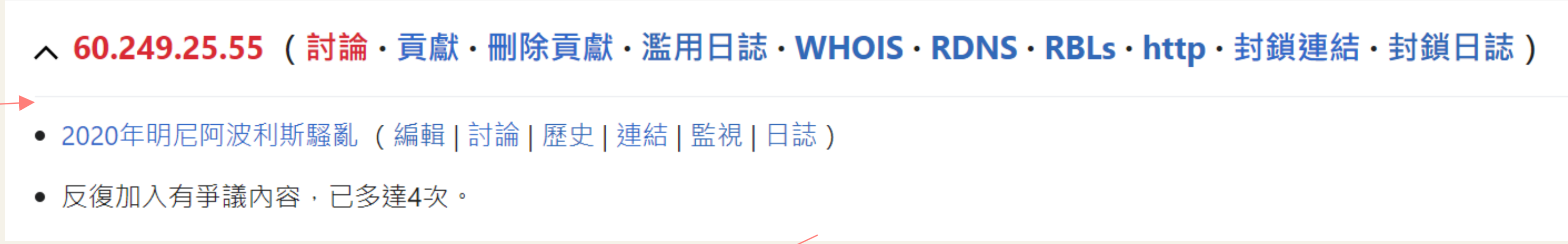
Sign In



Case study 3 (cont.)

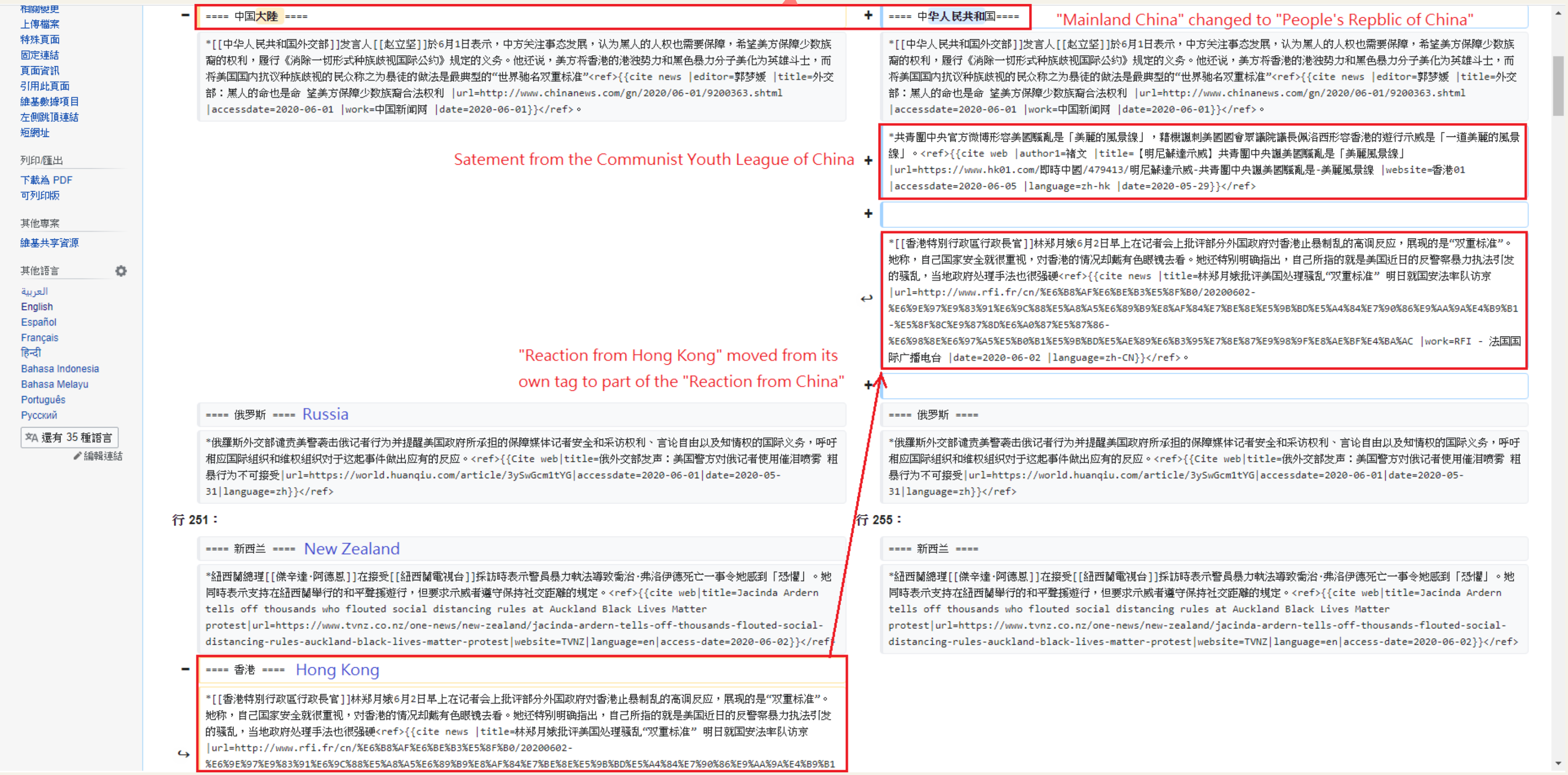
TEAMT5 杜浦數位安全

60.249.25.55



^ 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。



"Mainland China" changed to "People's Repblic of China"

Satement from the Communist Youth League of China

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

```
− ==== 中国大陸 ====
*[[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>。
```

```
+ ==== 中华人民共和国====
*[[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形容美國騷亂是「美麗的風景線」，藉機諷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 |author1=褚文 |title=【明尼蘇達示威】共青團中央諷美國騷亂是「美麗風景線」 |url=https://www.hk01.com/即時中國/479413/明尼蘇達示威-共青團中央諷美國騷亂是-美麗風景線 |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]]林郑月娥6月2日早上在记者会上批评部分外国政府对香港止暴制乱的高调反应，展现的是“双重标准”。她称，自己国家安全就很重视，对香港的情况却戴有色眼镜去看。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%B8%AF%E6%BE%B3%E5%8F%B0/20200602-%E6%9E%97%E9%83%91%E6%9C%88%E5%A8%A5%E6%89%B9%E8%AF%84%E7%BE%8E%E5%9B%BD%E5%A4%84%E7%90%86%E9%AA%9A%E4%B9%B1-%E5%8F%8C%E9%87%8D%E6%A0%87%E5%87%86-%E6%98%8E%E6%97%A5%E5%B0%B1%E5%9B%BD%E5%AE%89%E6%B3%95%E7%8E%87%E9%98%9F%E8%AE%BF%E4%BA%AC |work=RFI - 法国国际广播电台 |date=2020-06-02 |language=zh-CN}}</ref>。
+
```

```
==== 俄罗斯 ====   Russia
*俄羅斯外交部谴责美警袭击俄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：美国警方对俄记者使用催泪喷雾 粗暴行为不可接受|url=https://world.huanqiu.com/article/3ySwGcm1tYG|accessdate=2020-06-01|date=2020-05-31|language=zh}}</ref>
```

```
==== 俄罗斯 ====
*俄羅斯外交部谴责美警袭击俄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：美国警方对俄记者使用催泪喷雾 粗暴行为不可接受|url=https://world.huanqiu.com/article/3ySwGcm1tYG|accessdate=2020-06-01|date=2020-05-31|language=zh}}</ref>
```

行 251：

```
==== 新西兰 ====   New Zealand
*紐西蘭總理[[傑辛達·阿德恩]]在接受[[紐西蘭電視台]]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]]林郑月娥6月2日早上在记者会上批评部分外国政府对香港止暴制乱的高调反应，展现的是“双重标准”。她称，自己国家安全就很重视，对香港的情况却戴有色眼镜去看。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%B8%AF%E6%BE%B3%E5%8F%B0/20200602-%E6%9E%97%E9%83%91%E6%9C%88%E5%A8%A5%E6%89%B9%E8%AF%84%E7%BE%8E%E5%9B%BD%E5%A4%84%E7%90%86%E9%AA%9A%E4%B9%B1
```

行 255：

```
==== 新西兰 ====
*紐西蘭總理[[傑辛達·阿德恩]]在接受[[紐西蘭電視台]]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>
```

AGENDA

TEAMT5 杜浦數位安全

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！

TEAMT5
杜浦數位安全

Career Fair 攤位編號 9

Questions?