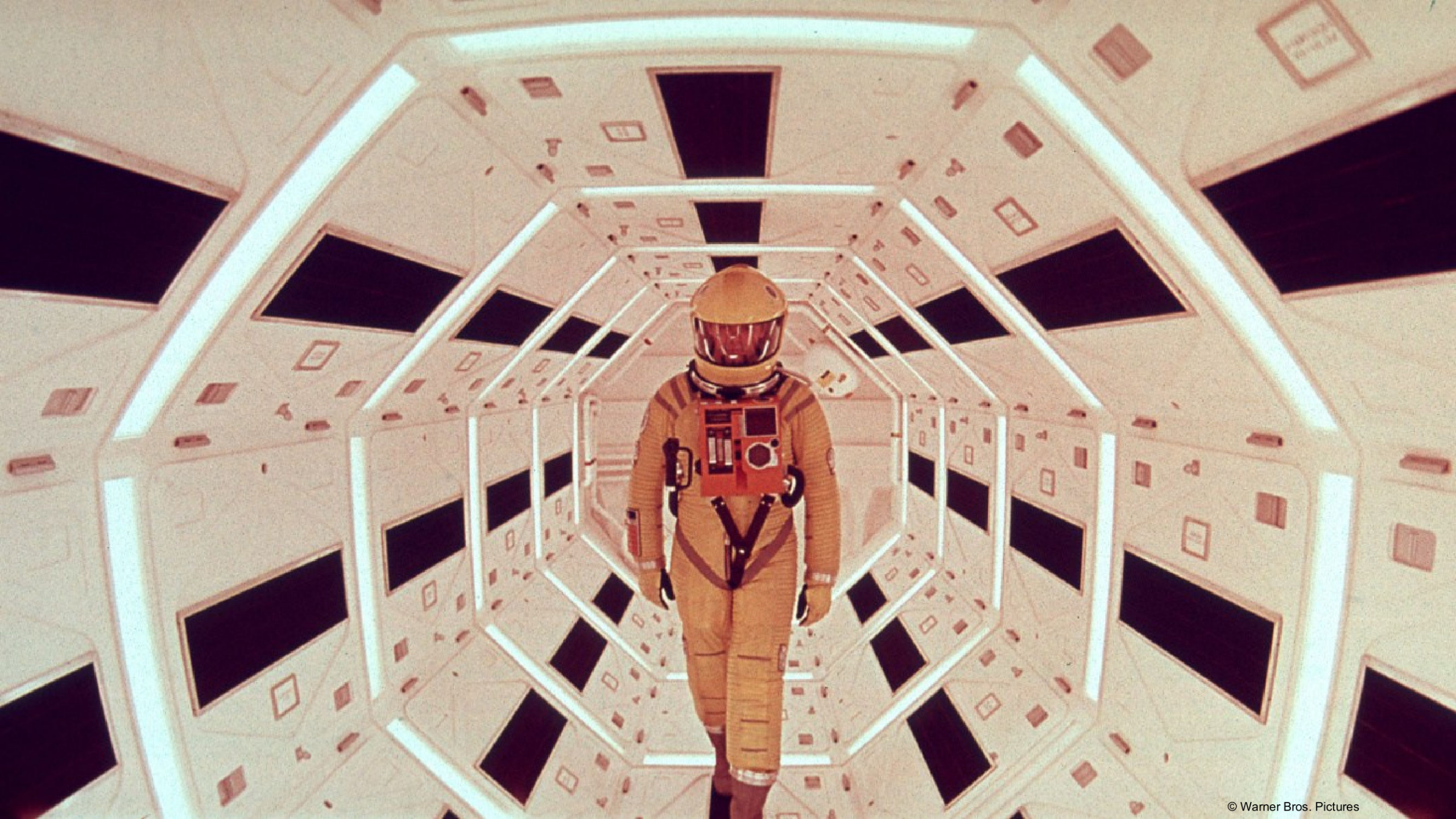
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence, Civil Protection and Sport DDPS
National Cyber Security Centre NCSC
Swiss Government Computer Emergency Response Team (GovCERT.ch)

TLP:CLEAR

Odyssey in Cyberspace
Cases From the Interweb

Roman Hüssy, Co-Head of GovCERT at the Nation Cyber Security Centre NCSC



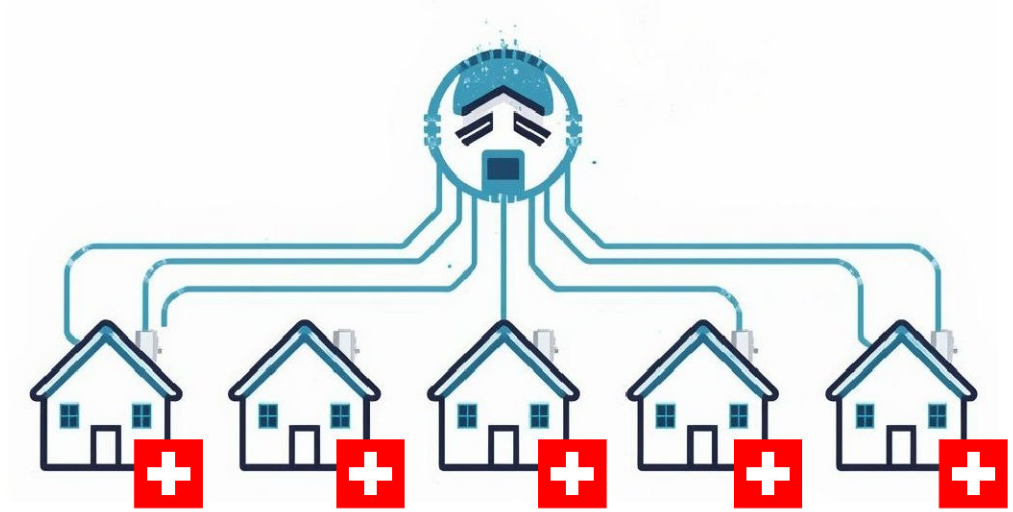

qimono @ pixabay.com

The Incident

- Victim found some **malicious DLLs** on their on-prem servers
- These DLLs where used to **exfiltrate data** from the victim’s corporate network
- Sadly, we don’t have more knowledge about the incident itself

Taking a Closer Look at the IPs

- IP addresses involved were associated with Swiss **Internet Access Providers** (IAPs)
- All of them were associated with consumer grade **residential internet lines** (Cable, DSL, Fibre)
- OSINT has **not shown any kind of suspicious activities** from these IPs



Taking a Closer Look at the IPs

- Who or what is **behind these Swiss IP addresses**?
- How to **obtain subscriber data** for those Swiss IP addresses?
- **Why** would a Threat Actor use Swiss IP addresses for attacking Swiss targets?

The Challenge

Federal Act on the Surveillance of Post and Telecommunications

(SPTA)

of 18 March 2016 (Status as of 1 September 2023)

Section 1 General Provisions

Art. 1 Material scope of application

[1] This Act applies to the surveillance of post and telecommunications ordered and carried out:

a. in the course of criminal proceedings;

b. in execution of a request for mutual legal assistance;

c. in the search for missing persons;

d. in tracing persons on whom a custodial sentence or custodial measure has been imposed;

e.[3] within the scope of the Intelligence Service Act of 25 September 2015[4] (IntelSA);

f.[5] in the course of mobile phone localisation in accordance with the Federal Act of 21 March 1997[6] on Measures to Safeguard Internal Security (ISA).

The Challenge

- Wrote **letter to the subscribers** of the affected internet lines, asking them to get in touch with us

- Reached out to the corresponding internet access provider (IAP), asking if they could **relay our letter to the subscriber** on our behalf

- Several subscribers **reverted back** to us

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

CH-3003 Bern
BACS

Bern, 1. November 2024

[redacted]

Freundliche Grüsse

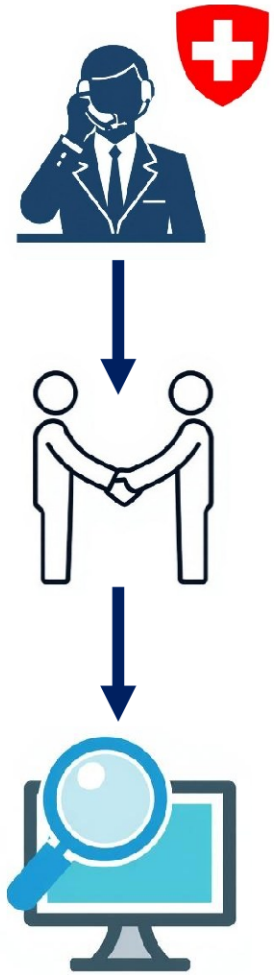
Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59
CH-3003 Bern

incidents@govcert.ch
www.ncsc.admin.ch

Dieses Dokument ist ohne Unterschrift gültig

Following the Rabbit Hole

- **Called everyone** who reverted back to us, explaining them the situation
- **Visited them** on site with the goal of an **initial assessment** and forensic analysis of devices
- Challenges:
  - Limited time on site
  - Limited forensic equipment on site
  - Subscribers had multiple, different devices on site

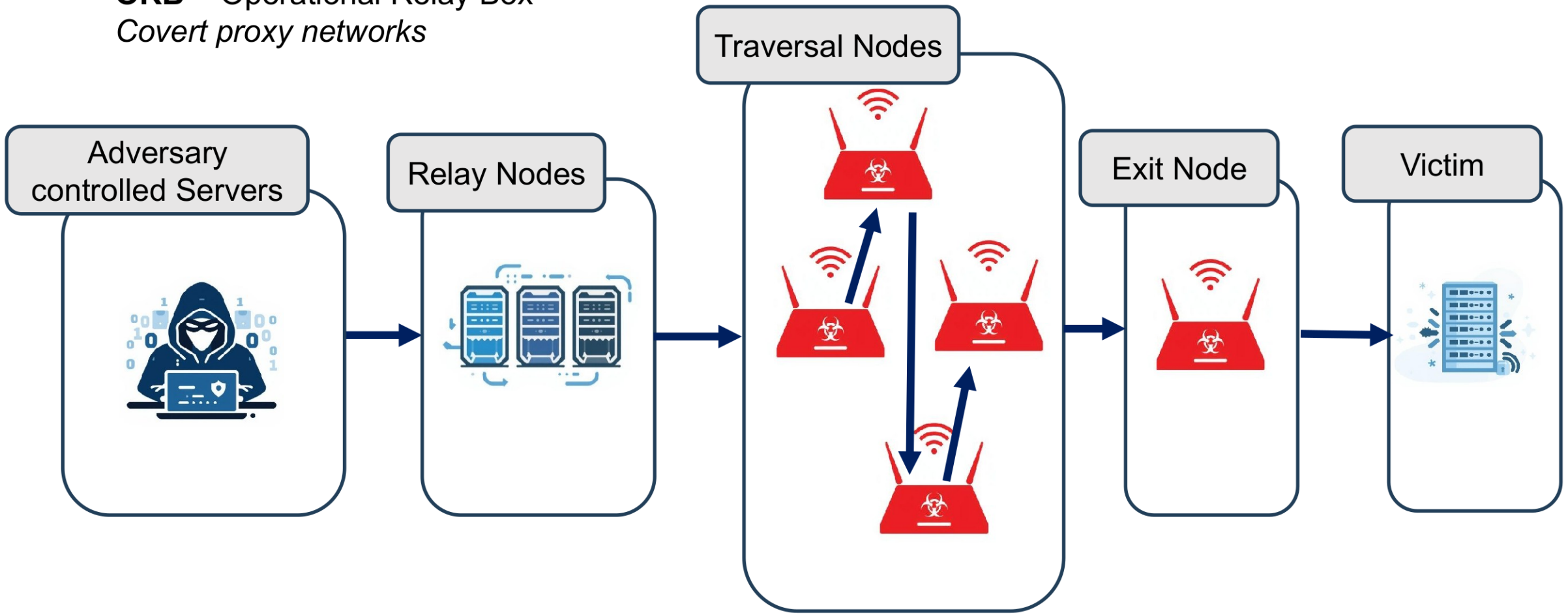


What did we find?

Source: brack.ch

What is an ORB network?

ORB = Operational Relay Box
Covert proxy networks



What is an ORB network?

- **Components:** Contains various types of **nodes**:
  - Virtual Private Servers (VPSs)
  - SOHO routers
  - IoT devices

- **Architecture:**
  - Relay nodes, used as **entry point**
  - Traversal nodes, used for **traffic obfuscation**
  - Exit nodes, used as **egression point** (victim facing)

- **ORB Types:**
  - ORB-as-a-Service (contractor quartermaster)
  - In-house ORB network production
  - Mix: Custom protocols on top of contracted ORB networks

Why Threat Actors Use ORBs?

- **Cover traffic**
  - Access victim's infrastructure, data exfiltration
- **Bypass geo restrictions** and detection
  - e.g. location awareness
- Exploit common local **legal restrictions** on network traffic monitoring
  - i.e. CH-to-CH traffic is excepted from the NDG

Qsnatch

Our analysis of the QNAP NAS devices suggested that they were infected with Qsnatch (aka “Derek”):

- **Linux trojan** targeting **QNAP NAS devices**
- First spotted in **2014**, different surges of **infections until 2020**
- Reports published by NCSC-FI, NCSC-UK and US CISA
- Back then **62’000 QNAP devices worldwide infected**
- Infections mainly in North America and Western Europe
- Qsnatch infrastructure reported **inactive since 2019**

Technical Analysis: Overview

- All examined devices were QNAP NAS devices hosted in Switzerland
- All of them have been **compromised** between **2017 and 2020**
- New connections mid 2024 through persistence mechanisms

- Qsnatch variants: **Similarities** (but also differences) to historical samples
  - New variant that **abandoned DGA** (no central botnet C2 anymore)
  - Passive backdoor = less noisy

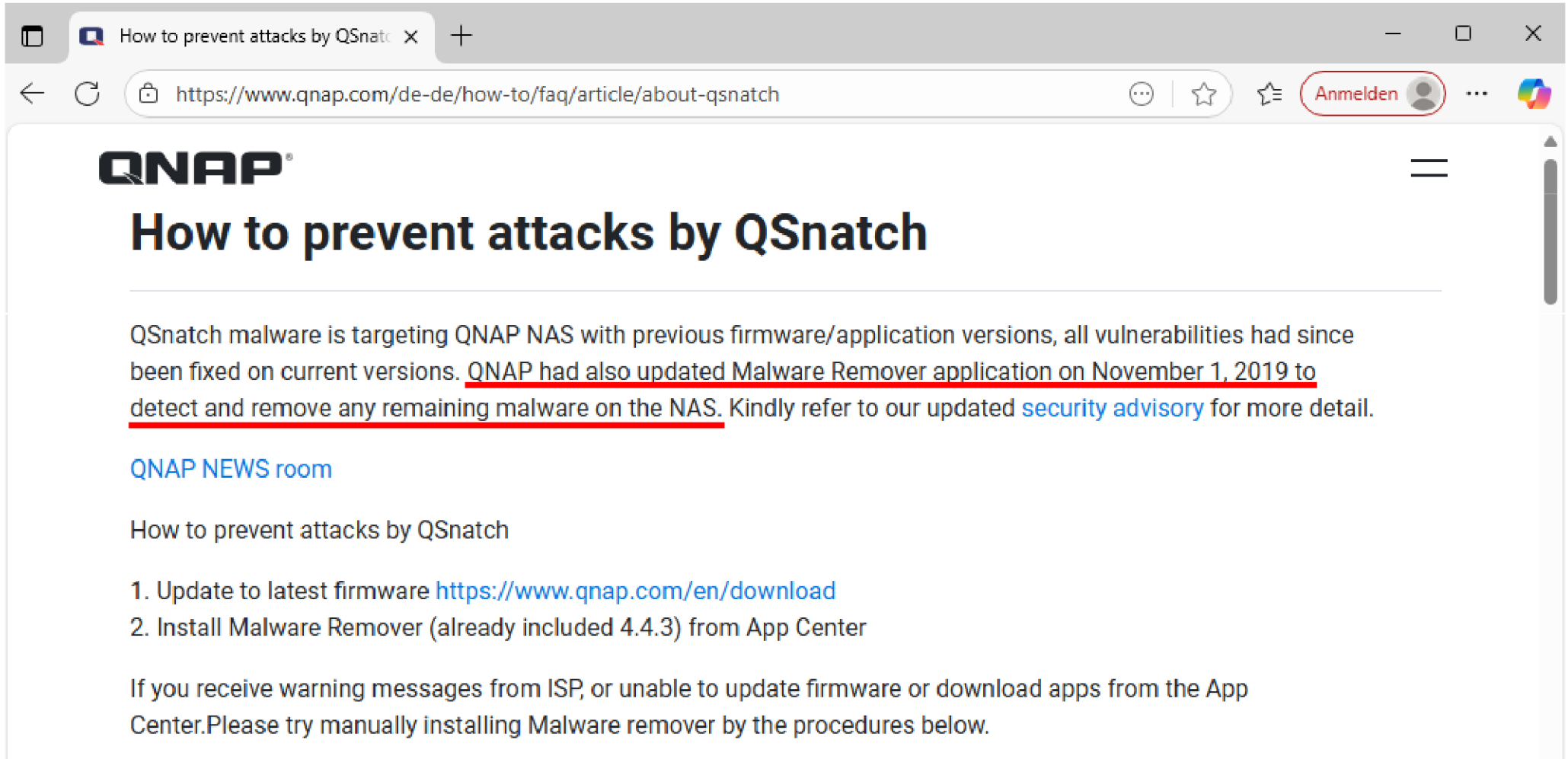
- Initial Access Vectors: Exploitation of a **vulnerability** or **credential brute forcing**

Technical Analysis: Infection

1. Initial Access to the QNAPs (through exploitation or Brute forcing)
2. Threat Actor runs **bash script** (a QSnatch variant):
   - **Sabotage of firmware update mechanism**
   - **Timestomping** to manipulate file creation timestamps
   - Install **SSH backdoor** on specific ports
   - Uses **UPnP** to forward the port locally on the device
   - **CGI backdoor** (for redundancy / backup C2 channel)

Universal Plug and Play (UPnP): This method seems to be quite effective, as targets are generally consumer grade devices, and end users generally don't check the UPnP configuration on their home devices. The devices we investigated all had UPnP enabled by default.

Technical Analysis: Infection



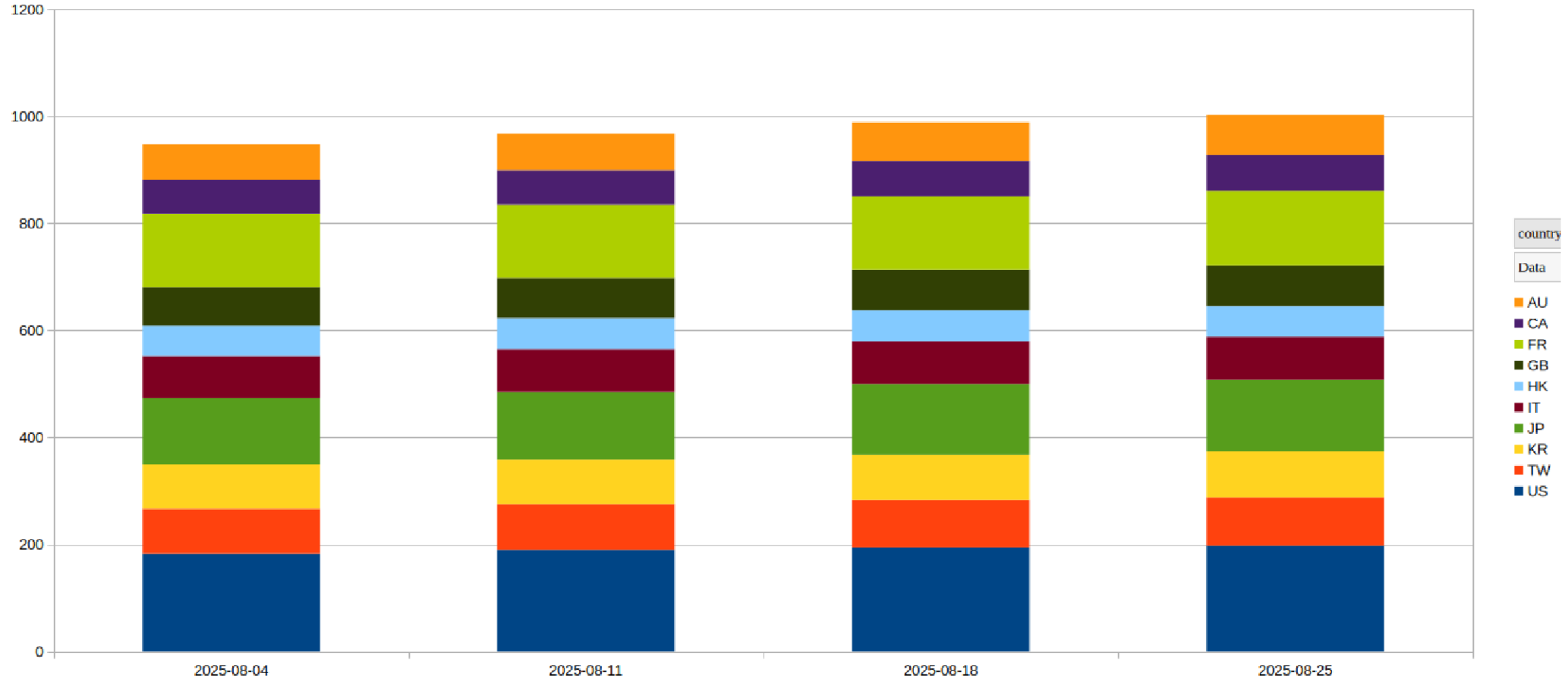
Technical Analysis: Other findings

- **Rogue user accounts:**
  - We found the **same account present across all devices**
  - Also, other usernames with square brackets [] have been found
    → seemingly these are not shown on QNAP management WebUI
  - Accounts were regularly created and then soon after deleted
  - Attacker could login as a regular user with legitimate credentials

- **Bruteforce attempts:**
  - Several devices continuously exposed to **admin credentials bruteforcing**
  - Very specific usernames (i.e. in Mandarin, Korean and Cyrillic names)

Mapping the Qsnatch ORB network

- We found around **1.5k infected hosts** world wide (as of September 2025)



Actions Taken

- Continuous **monitoring** of the ORB network

- **Sharing** technical IOCs with national critical infrastructure and international partners in an automatic manner

- **Participation in multilateral working group** on ORBs to counter the threat

Conclusion

- **40% of the internet subscribers** reverted back to us on our postal mail
- We also found an **ASUS router**, but we were too late to get our hands on it (it got replaced by the IAP)
- Potential Qsnatch variant **compromises other IoT-like devices** (e.g. TP-Link, IP cameras)
- Our analysis have only **limited visibility** on the ORB pandemic (other ORB networks exist)

Recommendations

- **Always patch** internet connected devices near time
- Ensure that **auto update is activated**, if available
- Only expose open ports to the internet if really needed
- Use **strong passwords** and **MFA**
- **Disable UPnP** if not used


AI generated

The Incident

- Victim was a developer at a **crypto company** based in Switzerland

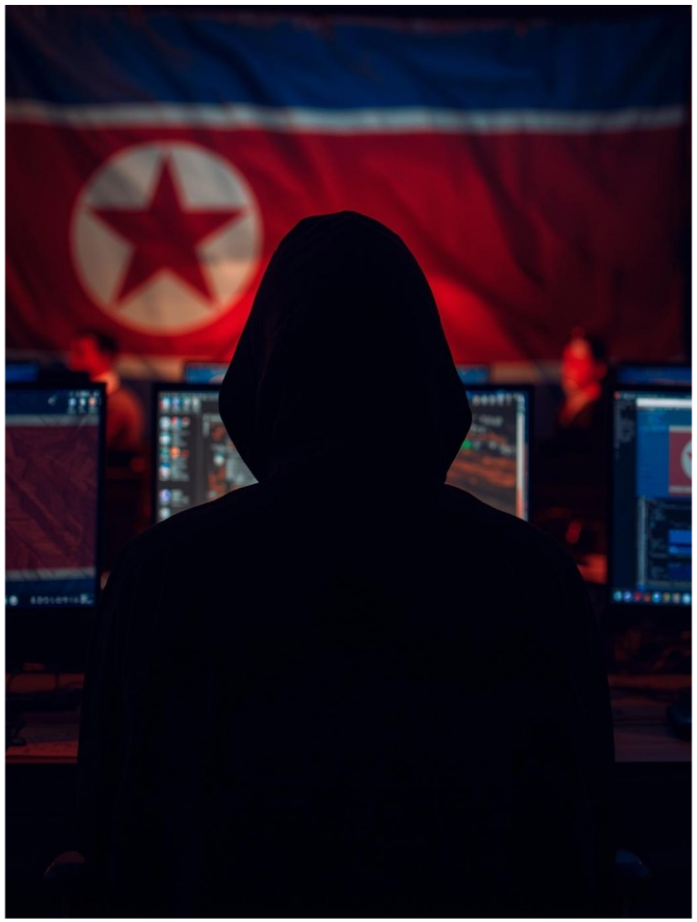
- Victim got approached on **LinkedIn** by a person that pretended to be a **recruiter**

- During the chat, the victim got asked by the recruiter to solve a **challenge**

Malicious Code Repository

- For this, the victim had to **download a BYOV-application from GitHub**
- The payload was a **NodeJS application**
- Once executed, it **fingerprints** the victim's device and **establishes a botnet C2 channel** with the threat actor

TraderTraitor



- Modus operandi matches **TraderTraitor,** a threat actor targeting crypto currency companies
- Historically, leveraged **fake job applications** and **supply chain compromise**
- Recently, the threat actor **switched to fake job lures**, targeting crypto companies
- US government attributes TraderTraitor to **North Korean state-sponsored threat actors**

Actions Taken

- **Technical analysis** of any payload delivery by the threat actors to spot new IOCs

- **Sharing** technical IOCs with national critical infrastructure and international partners in an automatic manner

- Together with the Swiss Financial Market Supervisory Authority (FINMA), **sensibilisation** of the crypto currency companies in Switzerland

Conclusion

- Similar attacks against **crypto currency companies**
- Threat actor **adapt** to more strict screenings for job applicants conducted by crypto currency companies
- Most recent attacks leverage invites for a **fake video conferencing system**, using **ClickFix** to infect them victim's machine
- Difficult for an **employee** (victim) to **reach out** to their **employer** on the topic

Conclusion

Reuters

My News

Exclusive: How North Korean hackers are using fake job offers to steal cryptocurrency

By **A.J. Vicens** and **Raphael Satter**

September 4, 2025 10:43 PM GMT+2 · Updated September 4, 2025

Summary

- North Korean hackers are using fake job offers to steal cryptocurrency-researchers
- Targets report an elaborate interview process managed by fake recruiters
- The practice complements Pyongyang's better known tactic of targeting of crypto exchanges

DETROIT/WASHINGTON, Sept 4 (Reuters) - North Korean hackers are saturating the cryptocurrency industry with credible-sounding job offers as part of their campaign to steal digital cash, according to new research, raw data, and interviews.

The problem is becoming so common that job applicants now regularly screen recruiters for signs they might be acting on Pyongyang's behalf. Twenty-five experts, victims, and corporate representatives that Reuters spoke to agreed that the problem was ubiquitous.

Recommendations

- Be careful with interactions on **social media** (i.e. LinkedIn)
- Always run 3rd party code in a **dedicated environment**
- If you encounter similar situations, **report them to the NCSC**
- Make your **employees aware** about these types of threats

Questions?

GovCERT.ch
outreach@govcert.ch