tnc25

Brighton, UK | **9-13 JUNE 2025**

BRIGHTER TOGETHER

It's all trash or not?

NGSOTI Project

Cynthia Wagner & Denim Latić

Brighton, UK, Concert Hall

11/06/2025

Co-funded by the European Union

GÉANT

restena

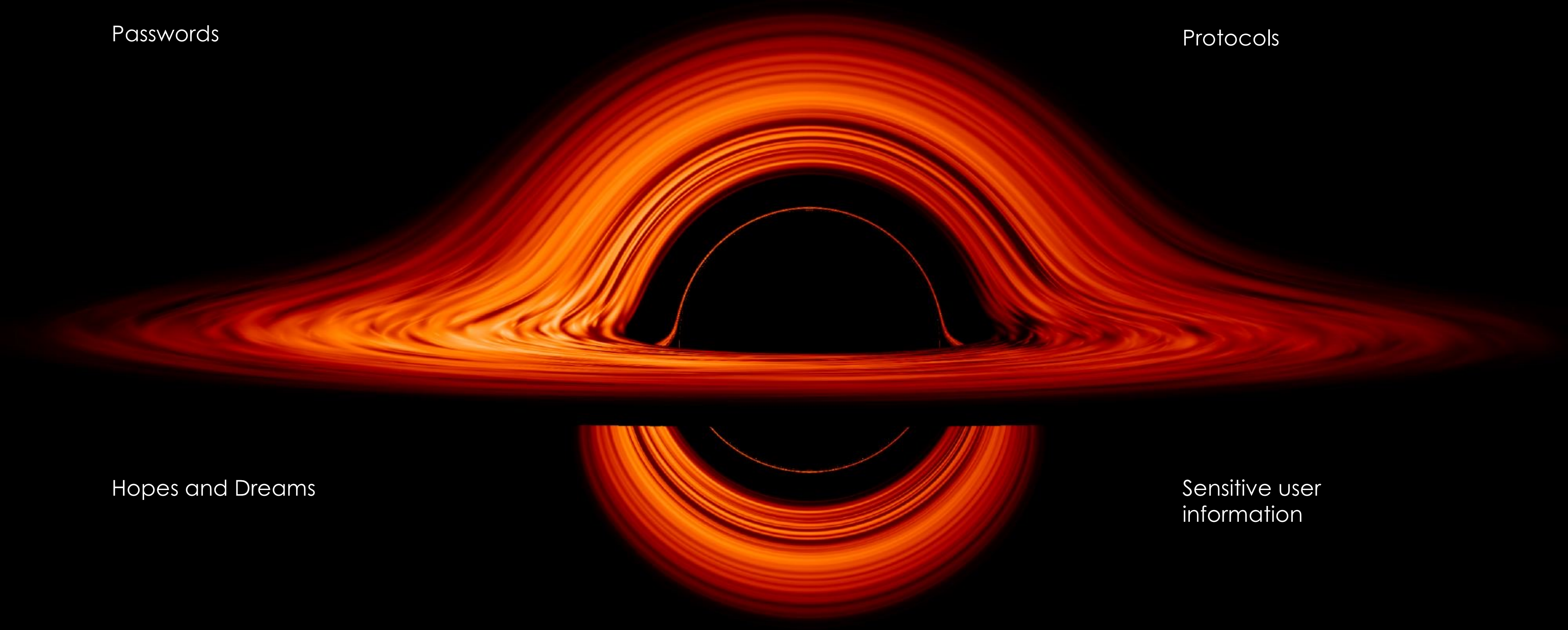
Introduction

- Networks are busy places
- Referring to a statistic institute* a forecast for 2025 claims:
  - 48-75 billions connected devices → 8 billion people
  - up to 46Zbytes of data
- Besides legitimate traffic there is:
  - traffic for attacks
  - Unwanted traffic
    - erroneous traffic
    - scanning activities

*: www.statista.com

Unwanted traffic = trash?

Can all this unwanted traffic be labeled as trash?



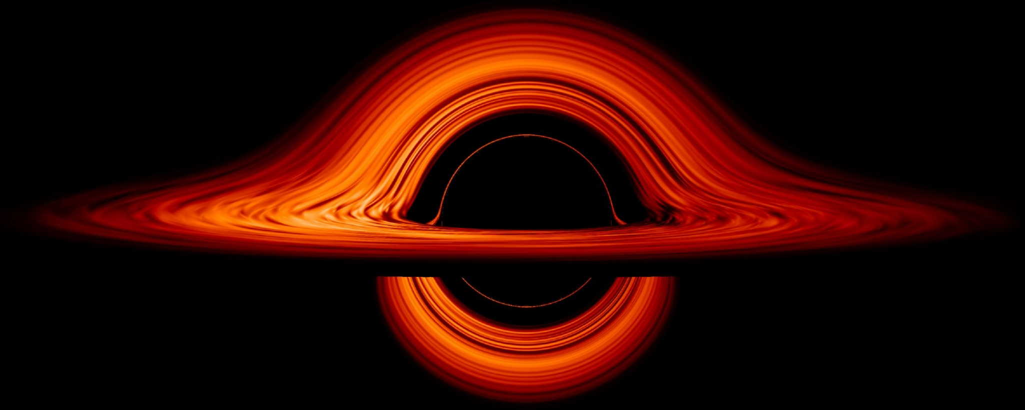
Passwords

Protocols

Hopes and Dreams

Sensitive user information

IP Darkspace / Blackhole traffic

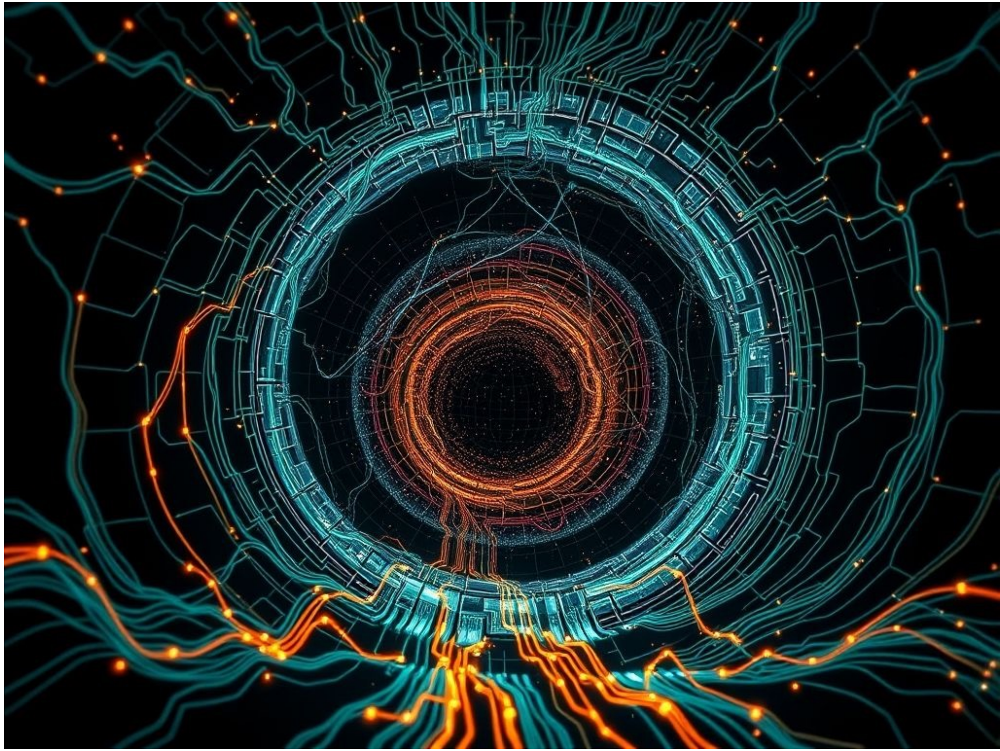


- The Blackhole sensor is currently on unused IP address space
- Traffic to the blackhole is Unidirectional
- Captures unwanted traffic
- Fun part - the blackhole is located on a IP address range that resembles a private address space

IP Darkspace / Blackhole traffic

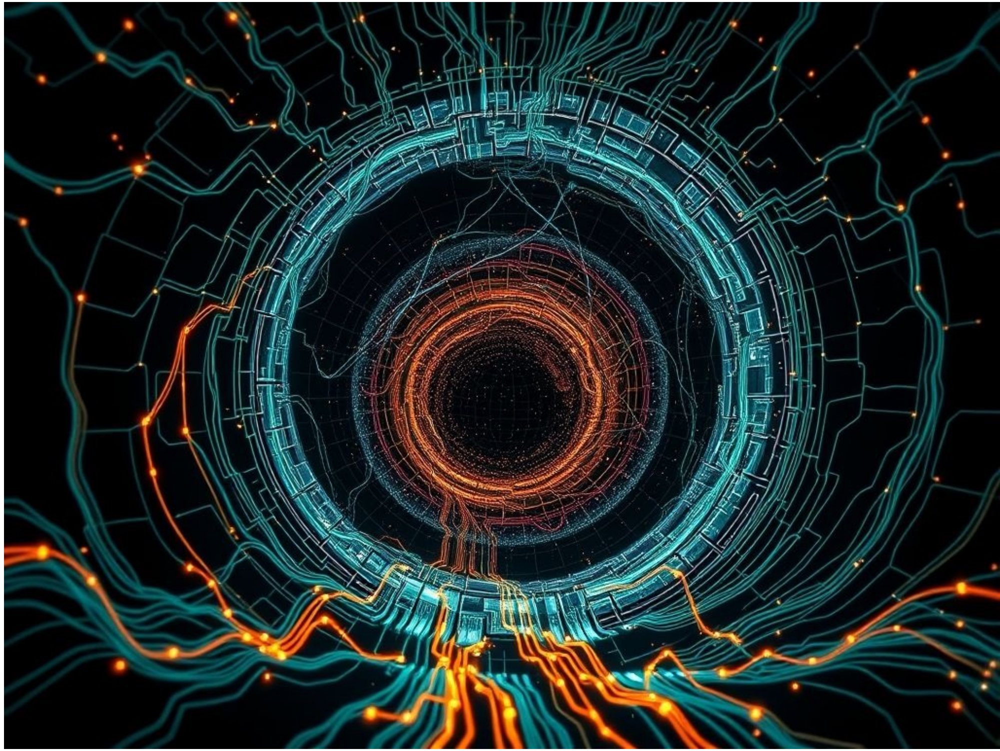
What ends in the Blackhole?

- Scanning activities
- Backscatter from Distributed denial of service attacks
- Mass exploitation of devices
- Misconfigured devices
- Unexpected activities
- …Many more



What ends in the Blackhole?

- Scanning and mass exploitation
- Spelling mistakes leading to erroneous configs and connections
- Default routing is configured
- Outgoing connections are poorly filtered
- Due to complex redundancy setups, the impact of erroneous configurations often goes unnoticed



Who do we see in the blackhole

- Electricity, heating & cooling data → Energy sector
- Railway protocol data → transport sector
- Cryptocurrency data → Finance sector
- Medical device data → Health sector
- Core Internet protocols, DNS resolver, cloud, telecom data

→Digital Infrastructure and ICT service management sector

→ Many of the NIS2 sectors

→Due to convergence to Ethernet / IP protocols / tunneling

Who do we see in the blackhole

- Limitations of Packet Captures
- Only IP packets are recorded in the captures
- Traffic is unidirectional
- Traffic may be forged or spoofed
- Difficult to distinguish between:
    - Scanning activity
    - Mass exploitation attempts
    - Misconfigured devices

Using the data

Traffic filtering approach

- Source IPs that probe more than one target IP in the blackhole network within one hour are considered scanning or mass exploitation sources.
- Packets with erroneous formats were discarded.
- Sources that appear repeatedly are classified as misconfigured devices.

Dataset description for this presentation

Collection start date: 2025-01-01

Collection end date: 2025-04-14

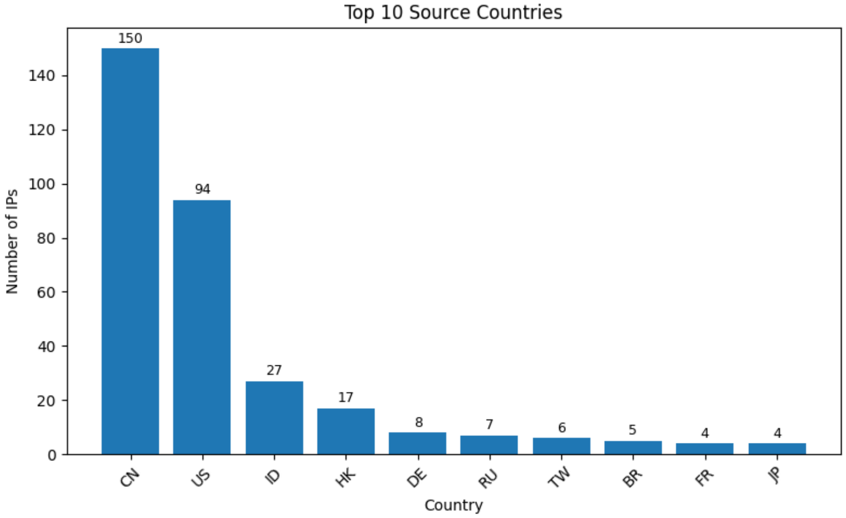
Volume: 632 GB

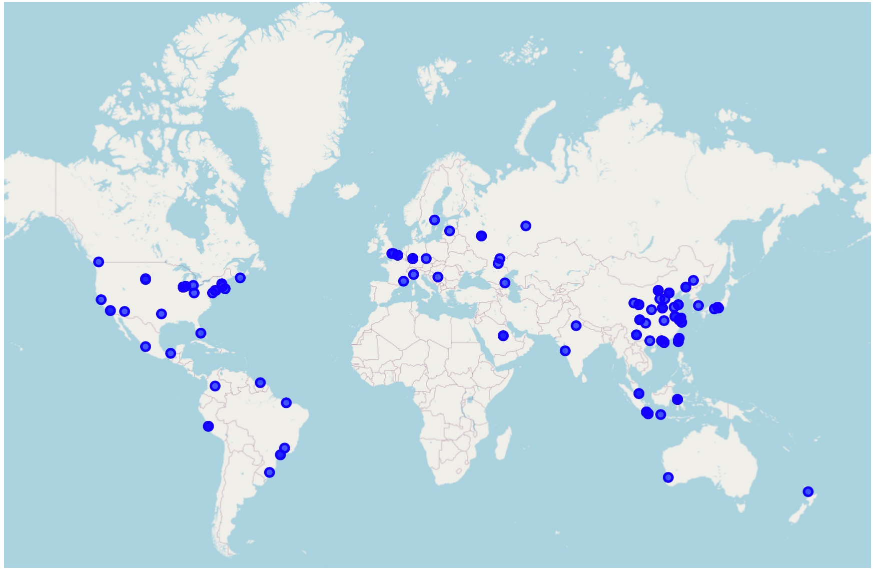
CNIP Protocol

- CN/IP is defined in standard EIA/CEA-852
- Used to transport component network frames such as LON over UDP or TCP
- Applied in Building control systems for lighting and HVAC (intelligent buildings) and Smart meters
- LonTalk is used in
  - industry automation,
  - railway stations,
  - on-train telemetry,
  - many more...

CNIP Protocol

Total Events: 10713





Infiniband Example

- Often used by Network Video Transmitters
- Features:
  - Face Detection
  - Face Attributes
  - Perimeter Protection
  - People Counting

https://www.dahuasecurity.com/asset/upload/uploads/soft/20200805/DH-IPC-HFW5221E-Z_Datasheet_20200805

Infiniband Example

- Identified device probing blackhole:
- DH-IPC-HFW5221E-Z

```
<a:Address>uuid:a004713c-1852-4b16-939e-
b99e46d67852</a:Address>
        </a:EndpointReference>
        <d:Types>dn:NetworkVideoTransmitter tds:Device</d:Types>
        <d:Scopes>
          onvif://www.onvif.org/location/country/china
          onvif://www.onvif.org/name/Dahua
          onvif://www.onvif.org/hardware/IPC-HFW5221D-Z
          onvif://www.onvif.org/Profile/Streaming
          onvif://www.onvif.org/type/Network_Video_Transmitter
          onvif://www.onvif.org/extension/unique_identifier
          onvif://www.onvif.org/Profile/Q/Operational
        </d:Scopes>

<d:XAddrs>http://192.168.202.128/onvif/device_service</d:XAddrs>
```

Infiniband Example

- Identified device probing blackhole:
- DH-IPC-HFW5221E-Z

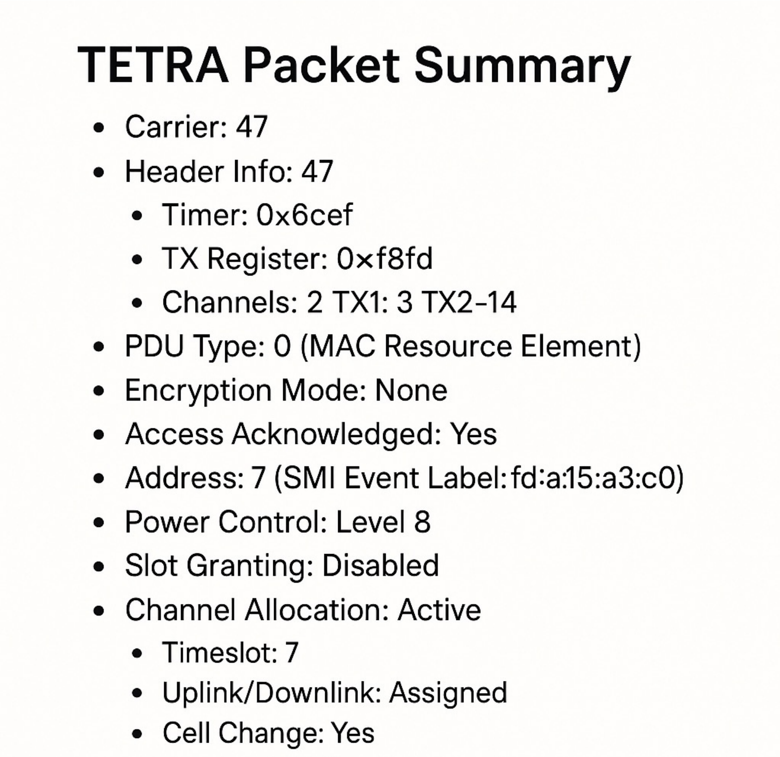
2025-04-01: 62 packets
2025-04-02: 724 packets
2025-04-03: 95 packets
2025-04-04: 33 packets
2025-04-05: 188 packets
2025-04-06: 376 packets
2025-04-07: 230 packets
2025-04-08: 68 packets
2025-04-09: 131 packets
2025-04-10: 544 packets
2025-04-11: 499 packets
2025-04-12: 62 packets
2025-04-13: 219 packets
2025-04-14: 171 packets

TETRA - Terrestrial Trunked Radio Example

- TETRA is a professional mobile radio (PMR) and two-way transceiver specification
- developed by the European Telecommunications Standards Institute (ETSI).
- It's primarily used for critical communications, especially
  - Public safety agencies (police, fire, ambulance)
  - Military and defense
  - Utilities and transport sectors
  - Governmental organizations

Image source: https://www.comtec-do.de/hytera-tetra/

TETRA - Terrestrial Trunked Radio Example



TETRA Packet Summary

- Carrier: 47
- Header Info: 47
  - Timer: 0x6cef
  - TX Register: 0×f8fd
  - Channels: 2 TX1: 3 TX2–14
- PDU Type: 0 (MAC Resource Element)
- Encryption Mode: None
- Access Acknowledged: Yes
- Address: 7 (SMI Event Label:fd:a:15:a3:c0)
- Power Control: Level 8
- Slot Granting: Disabled
- Channel Allocation: Active
  - Timeslot: 7
  - Uplink/Downlink: Assigned
  - Cell Change: Yes

Image source: https://www.comtec-do.de/hytera-tetra/

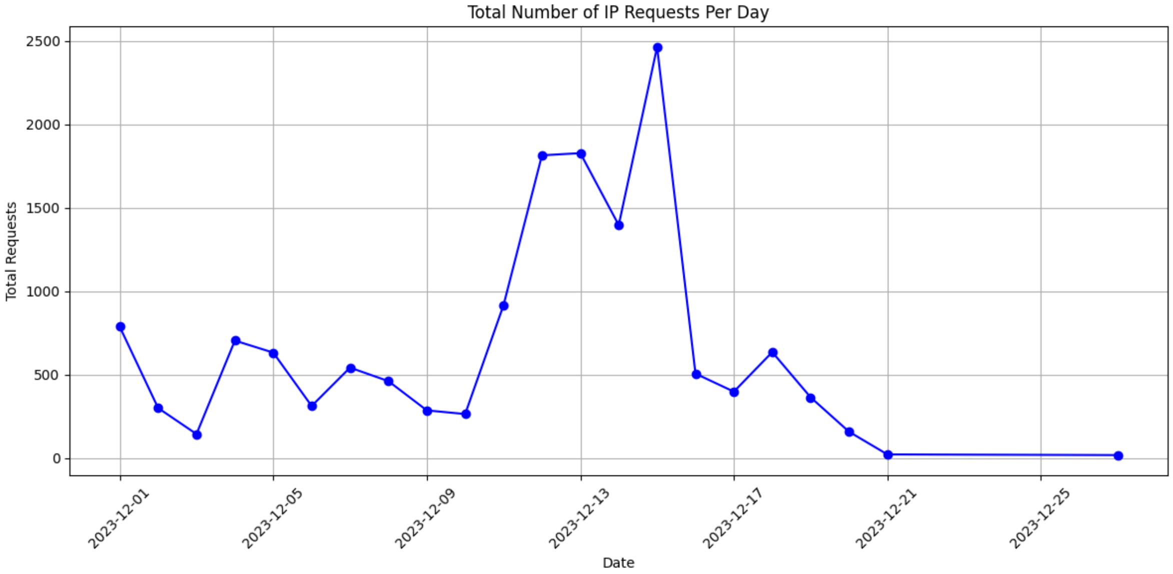
TETRA - Terrestrial Trunked Radio Example

- 1860 unique source IP addresses
- Many scanners connecting to more than 1 destination IPs
- All source IP connecting to more than 1 destination IP addresses are considered as scanner
- 1700 source IP addresses sending tetra packets to 1 IP address of blackhole
- Most frequent message: {'tetra.carrier': '0', 'tetra.header': {'tetra.timer': '0x xx'}} where xx is a number
- Most frequent message was omitted: 176 other messages were observed
- Longest tetra packet sender: sent 902 tetra packets

Tracking a user's activity

- Activity during school period

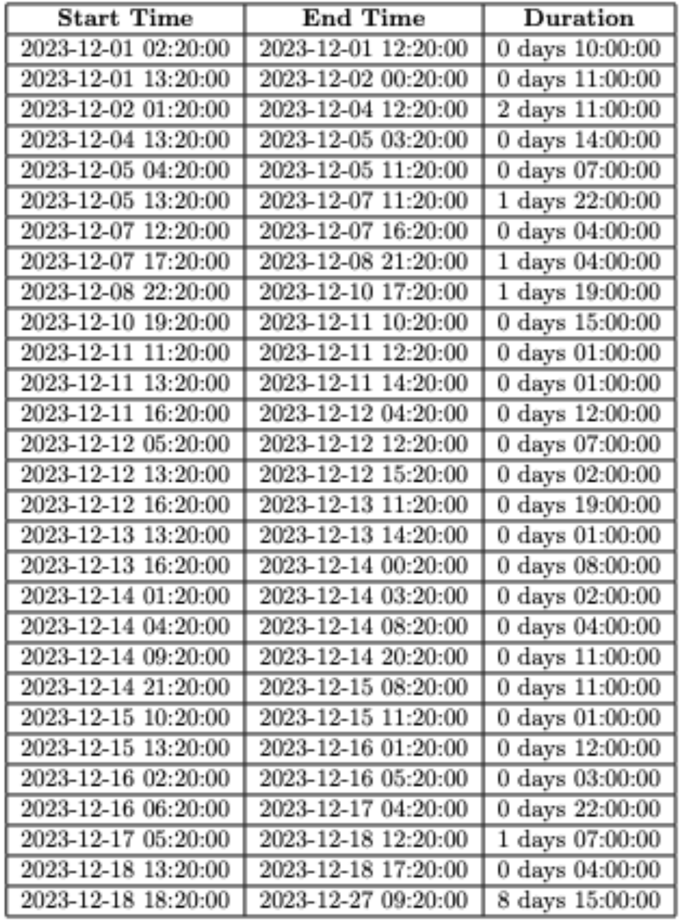
- Inactivity during school holidays



→ likely to be a student/researcher at an educational institution

Tracking a user’s activity

- Active hours vary daily
- Scripts of varying length



Start Time	End Time	Duration
2023-12-01 02:20:00	2023-12-01 12:20:00	0 days 10:00:00
2023-12-01 13:20:00	2023-12-02 00:20:00	0 days 11:00:00
2023-12-02 01:20:00	2023-12-04 12:20:00	2 days 11:00:00
2023-12-04 13:20:00	2023-12-05 03:20:00	0 days 14:00:00
2023-12-05 04:20:00	2023-12-05 11:20:00	0 days 07:00:00
2023-12-05 13:20:00	2023-12-07 11:20:00	1 days 22:00:00
2023-12-07 12:20:00	2023-12-07 16:20:00	0 days 04:00:00
2023-12-07 17:20:00	2023-12-08 21:20:00	1 days 04:00:00
2023-12-08 22:20:00	2023-12-10 17:20:00	1 days 19:00:00
2023-12-10 19:20:00	2023-12-11 10:20:00	0 days 15:00:00
2023-12-11 11:20:00	2023-12-11 12:20:00	0 days 01:00:00
2023-12-11 13:20:00	2023-12-11 14:20:00	0 days 01:00:00
2023-12-11 16:20:00	2023-12-12 04:20:00	0 days 12:00:00
2023-12-12 05:20:00	2023-12-12 12:20:00	0 days 07:00:00
2023-12-12 13:20:00	2023-12-12 15:20:00	0 days 02:00:00
2023-12-12 16:20:00	2023-12-13 11:20:00	0 days 19:00:00
2023-12-13 13:20:00	2023-12-13 14:20:00	0 days 01:00:00
2023-12-13 16:20:00	2023-12-14 00:20:00	0 days 08:00:00
2023-12-14 01:20:00	2023-12-14 03:20:00	0 days 02:00:00
2023-12-14 04:20:00	2023-12-14 08:20:00	0 days 04:00:00
2023-12-14 09:20:00	2023-12-14 20:20:00	0 days 11:00:00
2023-12-14 21:20:00	2023-12-15 08:20:00	0 days 11:00:00
2023-12-15 10:20:00	2023-12-15 11:20:00	0 days 01:00:00
2023-12-15 13:20:00	2023-12-16 01:20:00	0 days 12:00:00
2023-12-16 02:20:00	2023-12-16 05:20:00	0 days 03:00:00
2023-12-16 06:20:00	2023-12-17 04:20:00	0 days 22:00:00
2023-12-17 05:20:00	2023-12-18 12:20:00	1 days 07:00:00
2023-12-18 13:20:00	2023-12-18 17:20:00	0 days 04:00:00
2023-12-18 18:20:00	2023-12-27 09:20:00	8 days 15:00:00

Table 1: December 2023 Inactive Periods

Conclusion

- Default routing is a common reason for collecting data from misconfigured systems
- Misconfigurations are hard to spot in redundant and failover systems
- Protect your public facing devices as mass exploitation can happen rapidly
- Not all devices should be exposed to the internet

→ Misconfigurations may release valuable/sensitive organisation infrastructure in the wild

→ The uncontrolled information spreading may pave the way for attackers to target your systems

NGSOTI Project

Next Generation Security Operator Training Infrastructure (NGSOTI)

- Details
  - Project Number: 101127921
  - Project start: 01/01/2024
  - Duration: 36 Months
  - Call: DIGITAL-ECCC-2022-CYBER-03
  - Budget: 1.48 M€
- Consortium

CIRCL Computer Incident Response Center Luxembourg | TENZIR | restena | uni.lu UNIVERSITÉ DU LUXEMBOURG

Co-funded by the European Union

- Objective
  - Create an open-source infrastructure for SOC operators practical training regarding network-related alerts

Thank you

Any questions?

admin@restena.lu

Co-funded by
the European Union

GÉANT

restena