Vulnerability analysis of Industrial Control System (ICS) devices/protocols

Himanshu Goyal

hgoyal33@gatech.edu

Motivation

Internet-exposed devices are inherently vulnerable to attack.

ICS protocols...

- were designed to operate on closed networks and therefore provide no built-in security. (Authentication, Encryption, etc.)
- layered on *Ethernet and TCP/IP* and inevitably connected to public Internet to support remote monitoring and management.

Targeted Protocols

5 Services, most of the ICS devices runs on them.

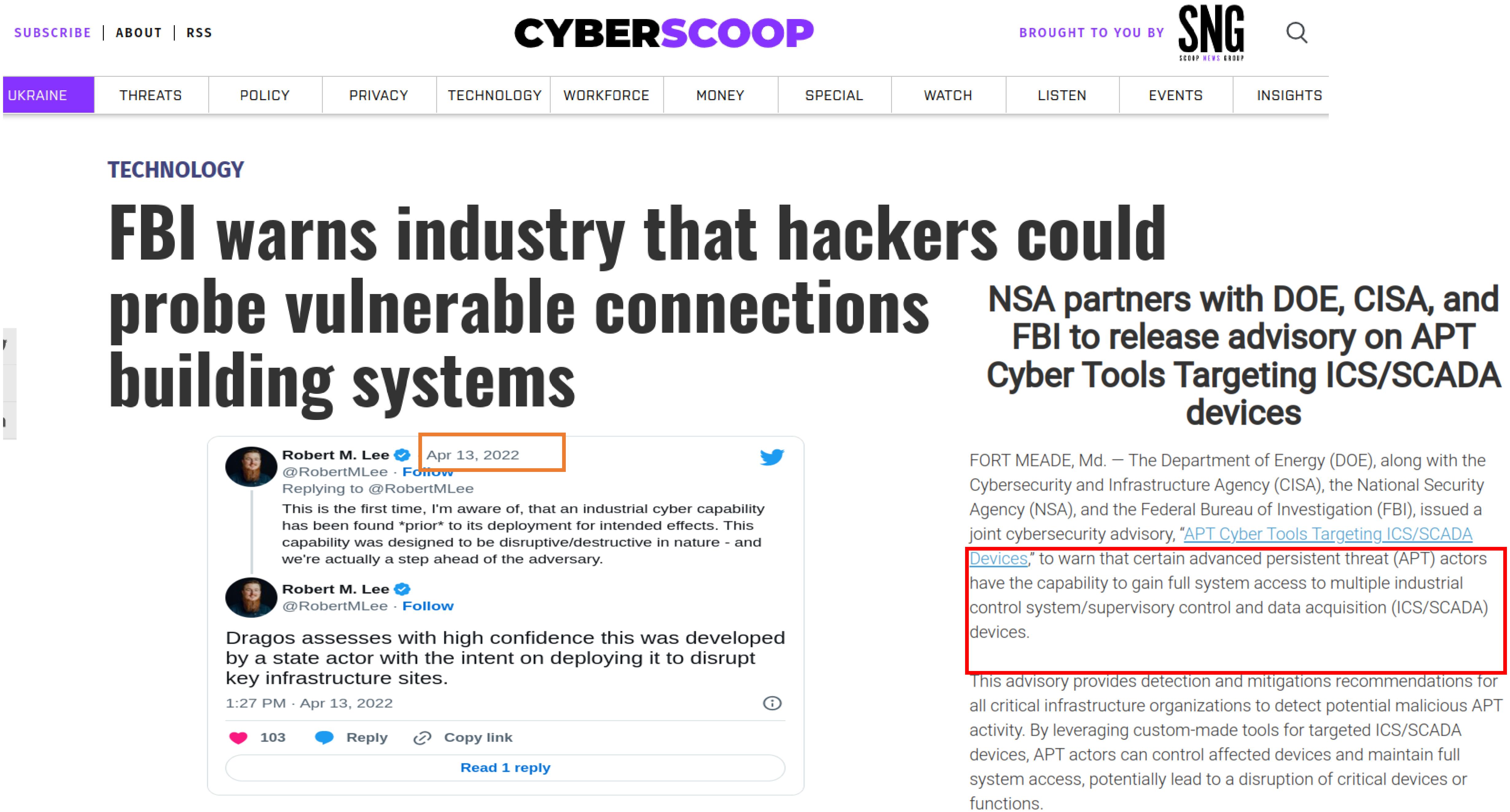
- *TCP/502* - **Modbus** (ICS)
- *TCP/102* - **S7** (ICS), **ICCP** (Power Grid), **IEC 61850** (Power Grid)
- *TCP/1911* - **FOX** (Building Management)
- *TCP/47808* - **BACnet** (Building Management)
- *TCP/20000* - **DNP3** (Power Grid)

Security Landscape

- **Modbus –** operates in Master/Slave architecture and does not have any build security mechanisms.
- **Siemens S7** - It is neither authenticated nor encrypted and thus, is susceptible to spoofing, session hijacking and DoS attacks.
- **BACnet** – Protocol provides security features, but operators don't implement them in practice.
- **DNP 3** - No Security Features. E.g. A malformed frame can crash the device, drive it into infinite loop, rendering the entire device inoperable.

TECHNOLOGY

FBI warns industry that hackers could probe vulnerable connections in building systems



TECHNOLOGY

FBI warns industry that hackers could probe vulnerable connections building systems

Robert M. Lee @RobertMLee · Follow Apr 13, 2022

Replying to @RobertMLee

This is the first time, I'm aware of, that an industrial cyber capability has been found *prior* to its deployment for intended effects. This capability was designed to be disruptive/destructive in nature - and we're actually a step ahead of the adversary.

Robert M. Lee @RobertMLee · Follow

Dragos assesses with high confidence this was developed by a state actor with the intent on deploying it to disrupt key infrastructure sites.

1:27 PM · Apr 13, 2022

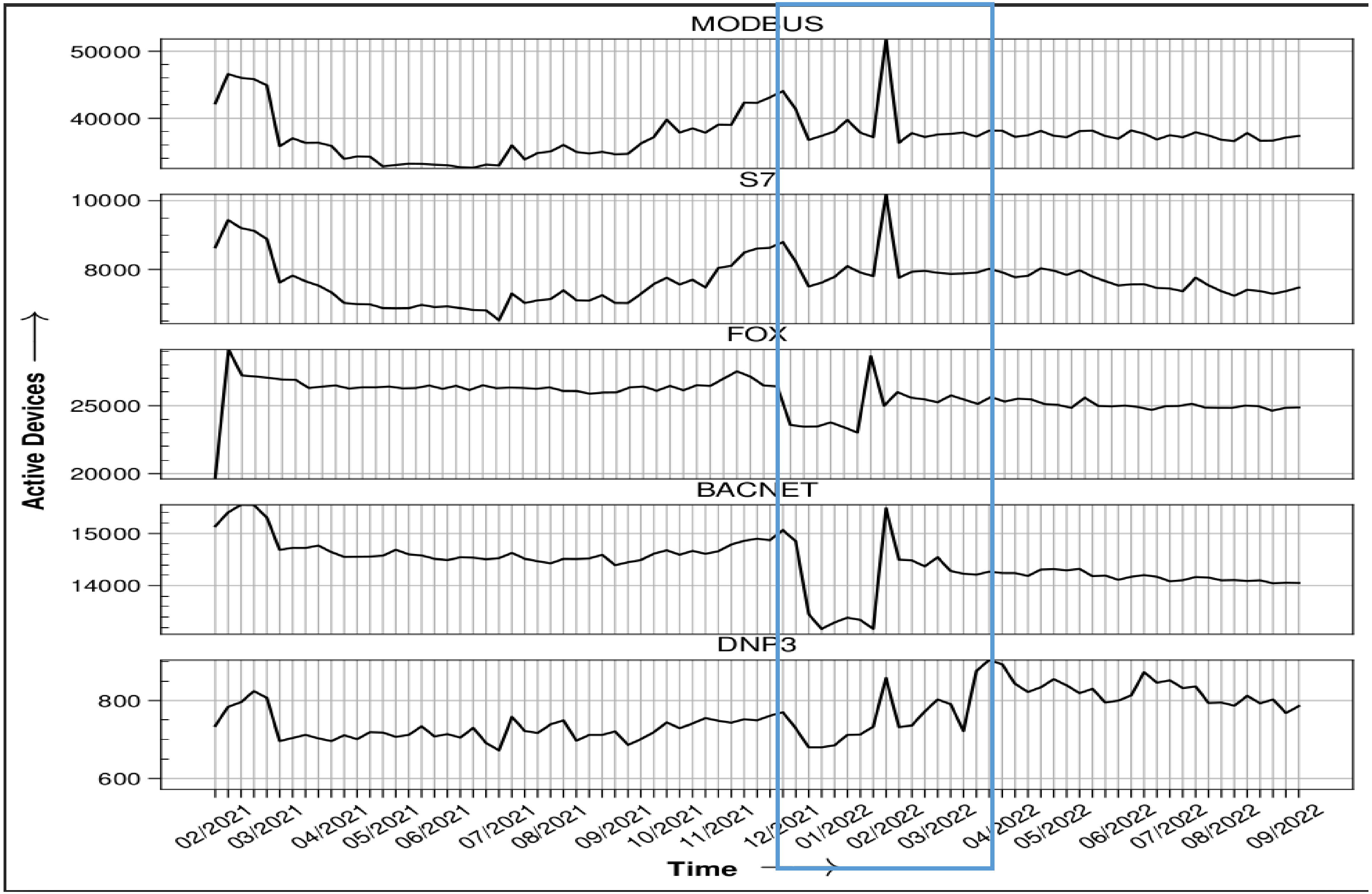
NSA partners with DOE, CISA, and FBI to release advisory on APT Cyber Tools Targeting ICS/SCADA devices

FORT MEADE, Md. — The Department of Energy (DOE), along with the Cybersecurity and Infrastructure Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI), issued a joint cybersecurity advisory, "APT Cyber Tools Targeting ICS/SCADA Devices," to warn that certain advanced persistent threat (APT) actors have the capability to gain full system access to multiple industrial control system/supervisory control and data acquisition (ICS/SCADA) devices.

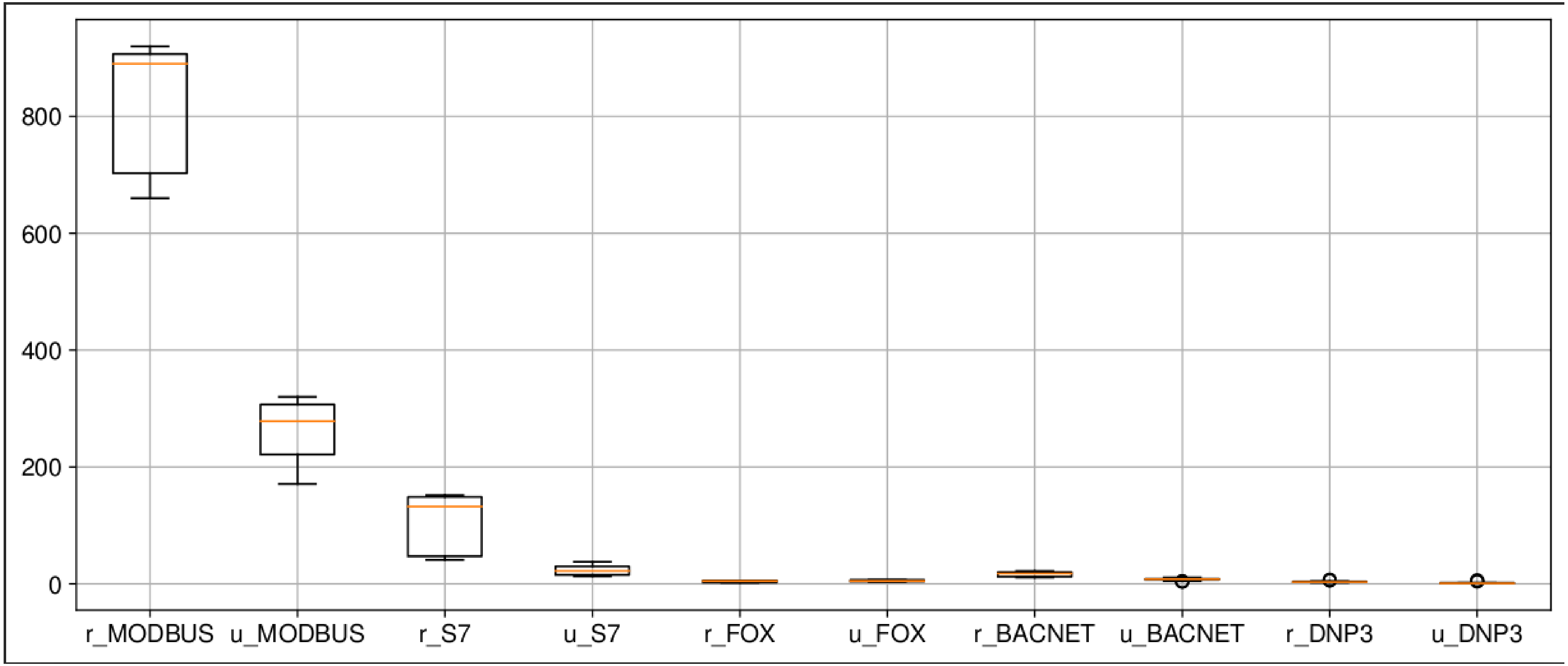
This advisory provides detection and mitigations recommendations for all critical infrastructure organizations to detect potential malicious APT activity. By leveraging custom-made tools for targeted ICS/SCADA devices, APT actors can control affected devices and maintain full system access, potentially lead to a disruption of critical devices or functions.

https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2997885/nsa-partners-with-doe-cisa-and-fbi-to-release-advisory-on-apt-cyber-tools-targe/

1. Number of Active Devices (Feb'21 – Sep'22)



First Thought... (Russia vs Ukraine)



Second thought... (Autonomous Systems)

- Data from Nov'21 to Mar'22
- **Expectation**: Skewed graph, **Reality**: Not so..
- Label at the top shows the total number of ASes running the service.

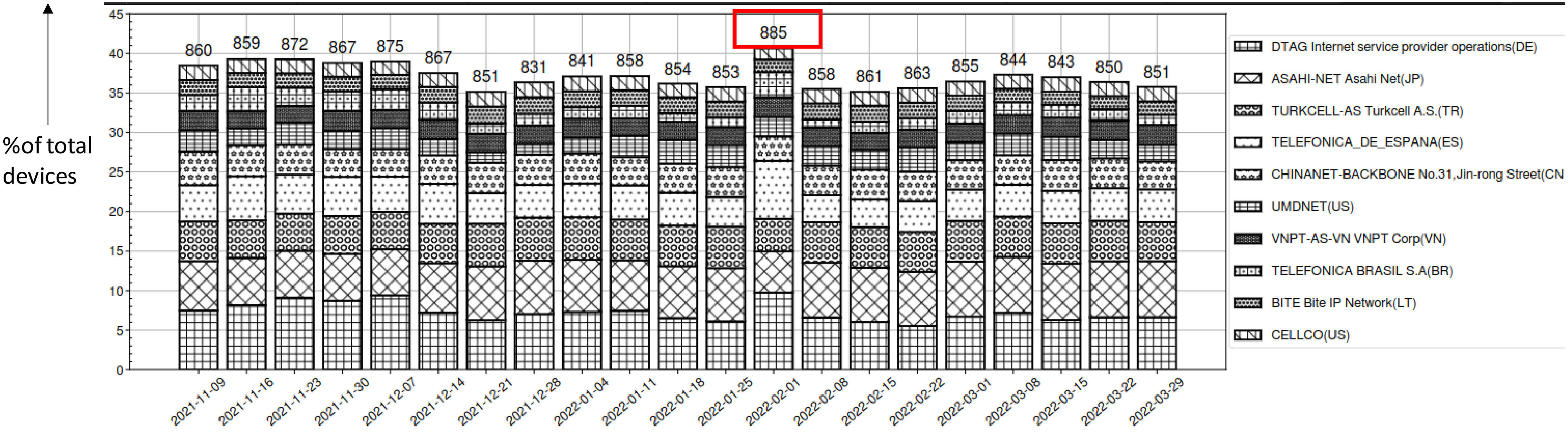
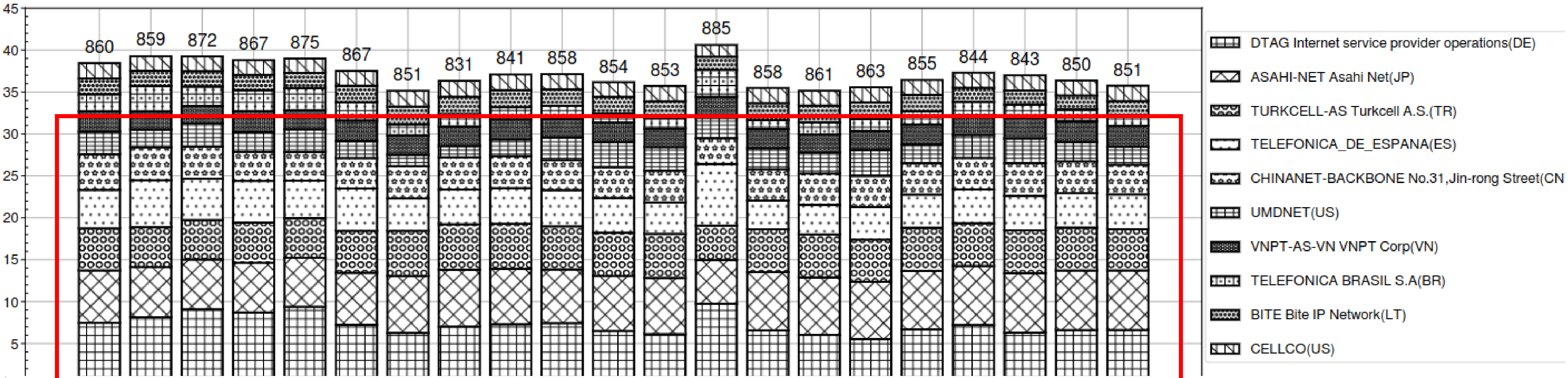
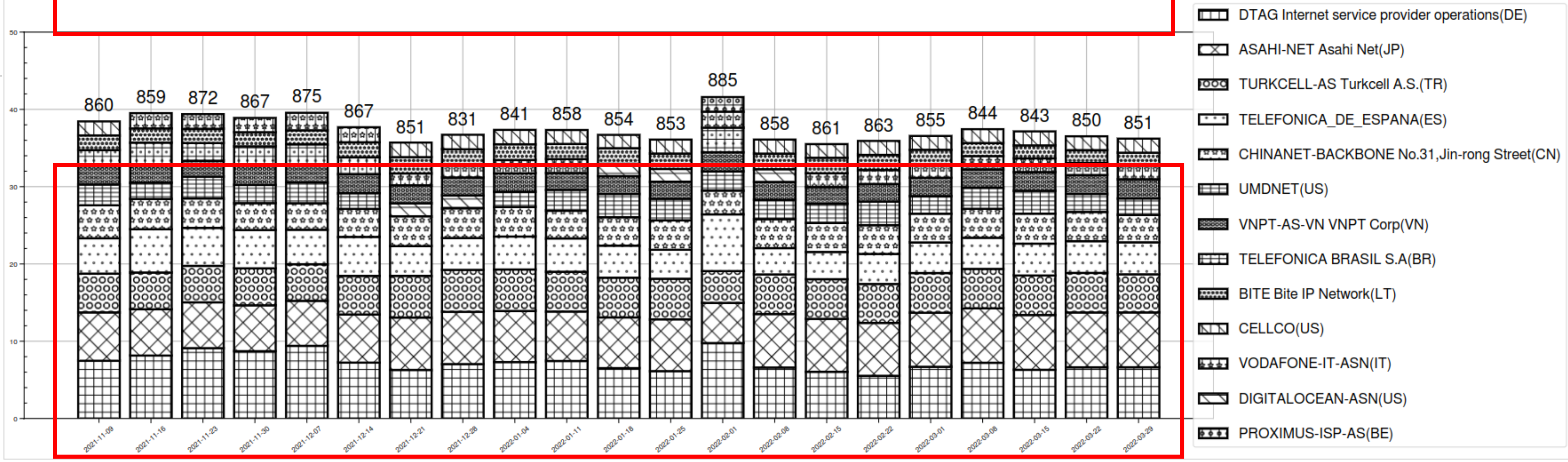


Fig. Top 10 ASN device count for **S7** service

Second thought… (Autonomous Systems)





Second thought... (Autonomous Systems)

What about the other services?

- Found the same behaviour for other services as well.

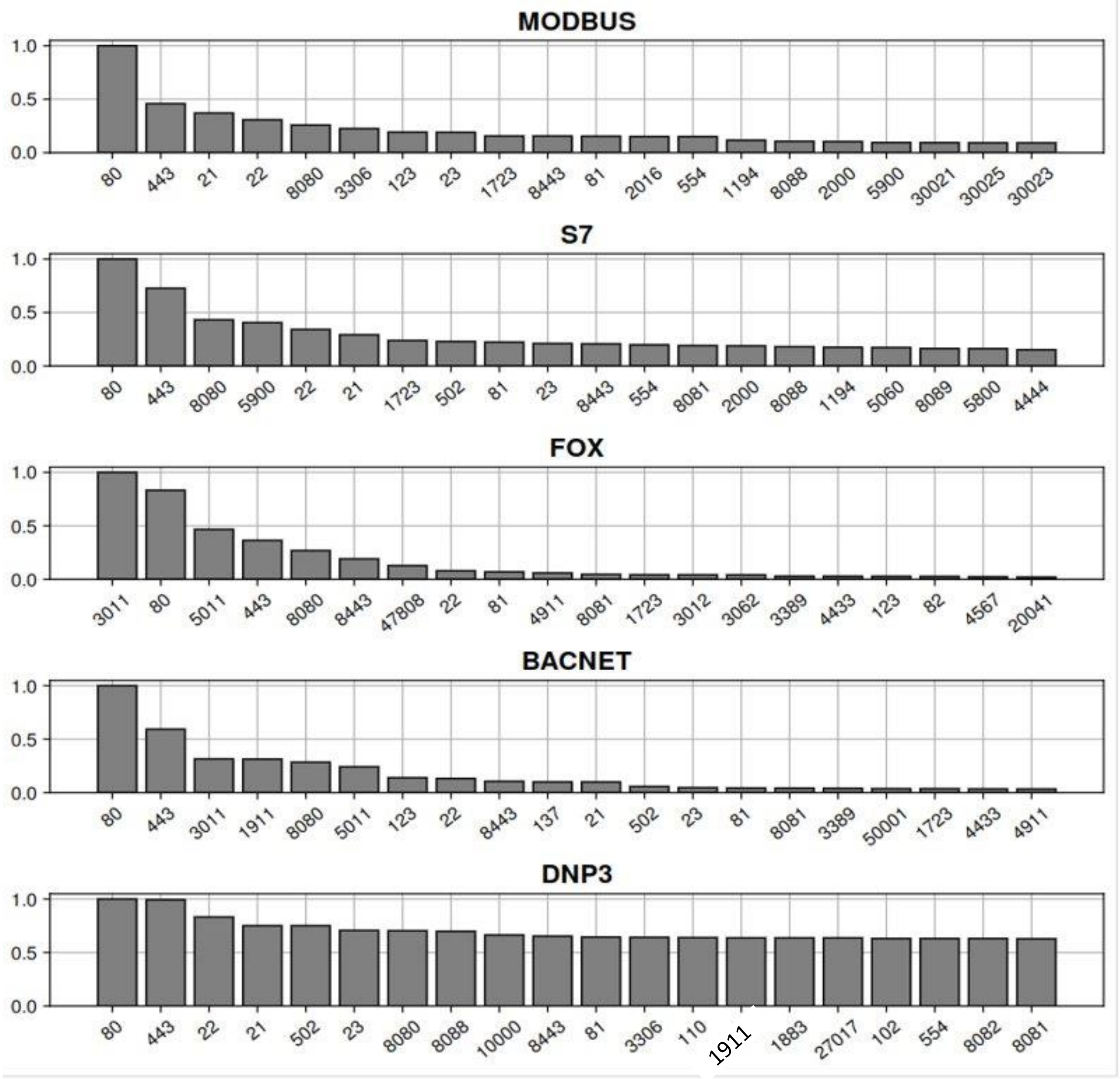
- What about the increase in AS count?

  - Yes, there are newcomers, but they *don't contribute significantly* towards the overall increase.

Observation:

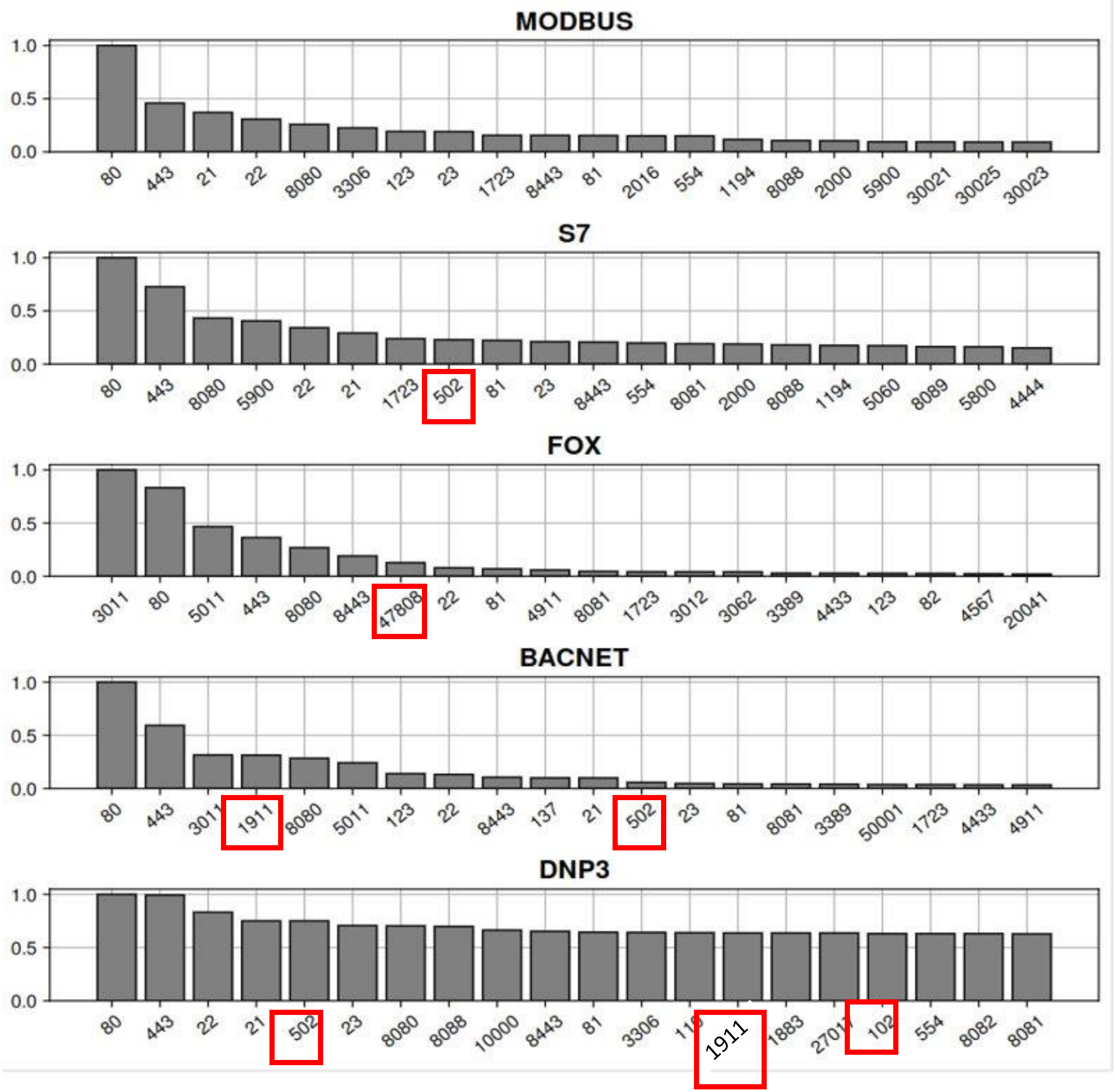
- Some of the existing ASes have higher device count than the existing and future counts.

2. Service Co-location?



502 - MODBUS
102 - S7
1911 - FOX
47808 - BACNET
20000 - DNP3

2. Service Co-location?



502 - MODBUS

102 - S7

1911 - FOX

47808 - BACNET

20000 - DNP3

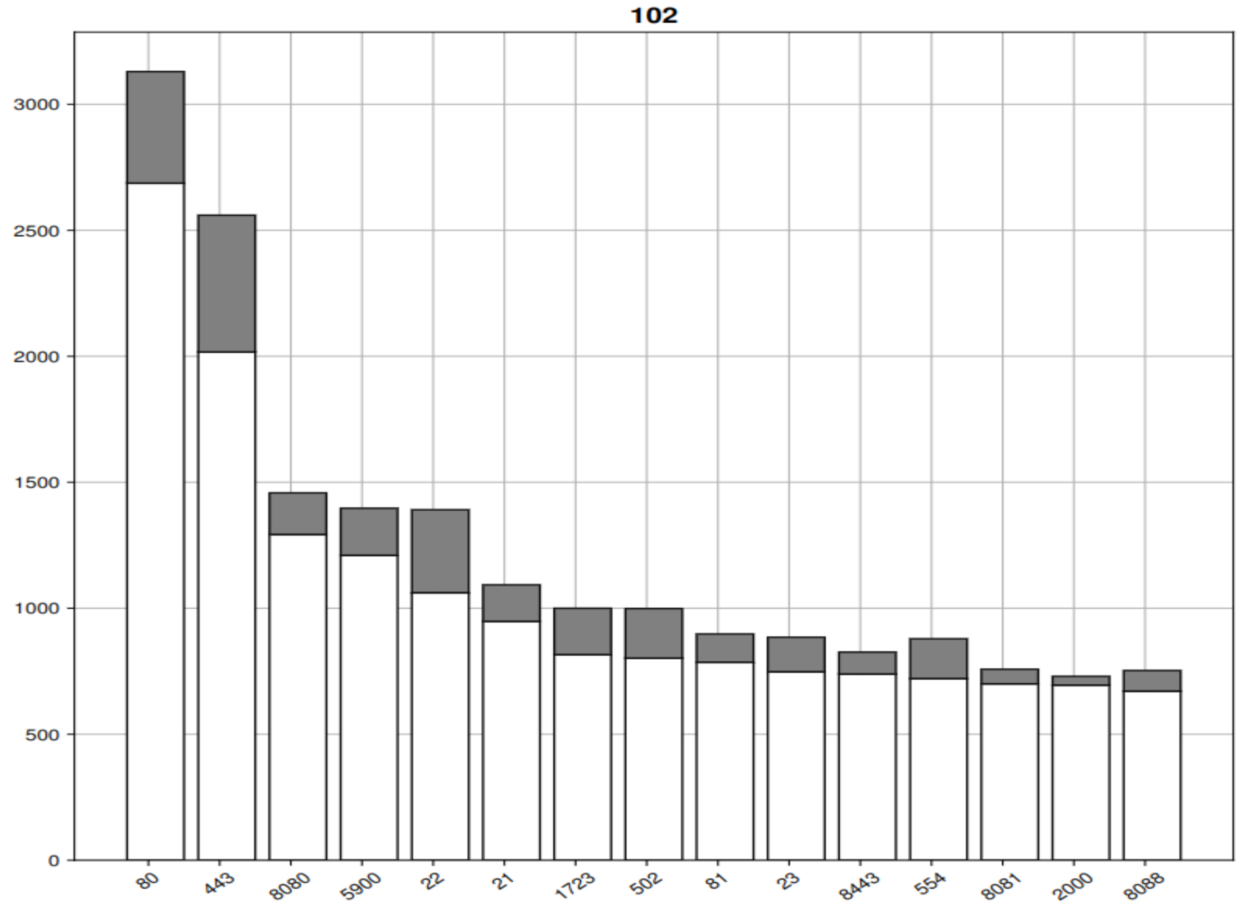
S7 --> 502

FOX --> 47808

BACNET --> 1911, 502

DNP3 --> 502, 1911, 102

2. Service Co-location?

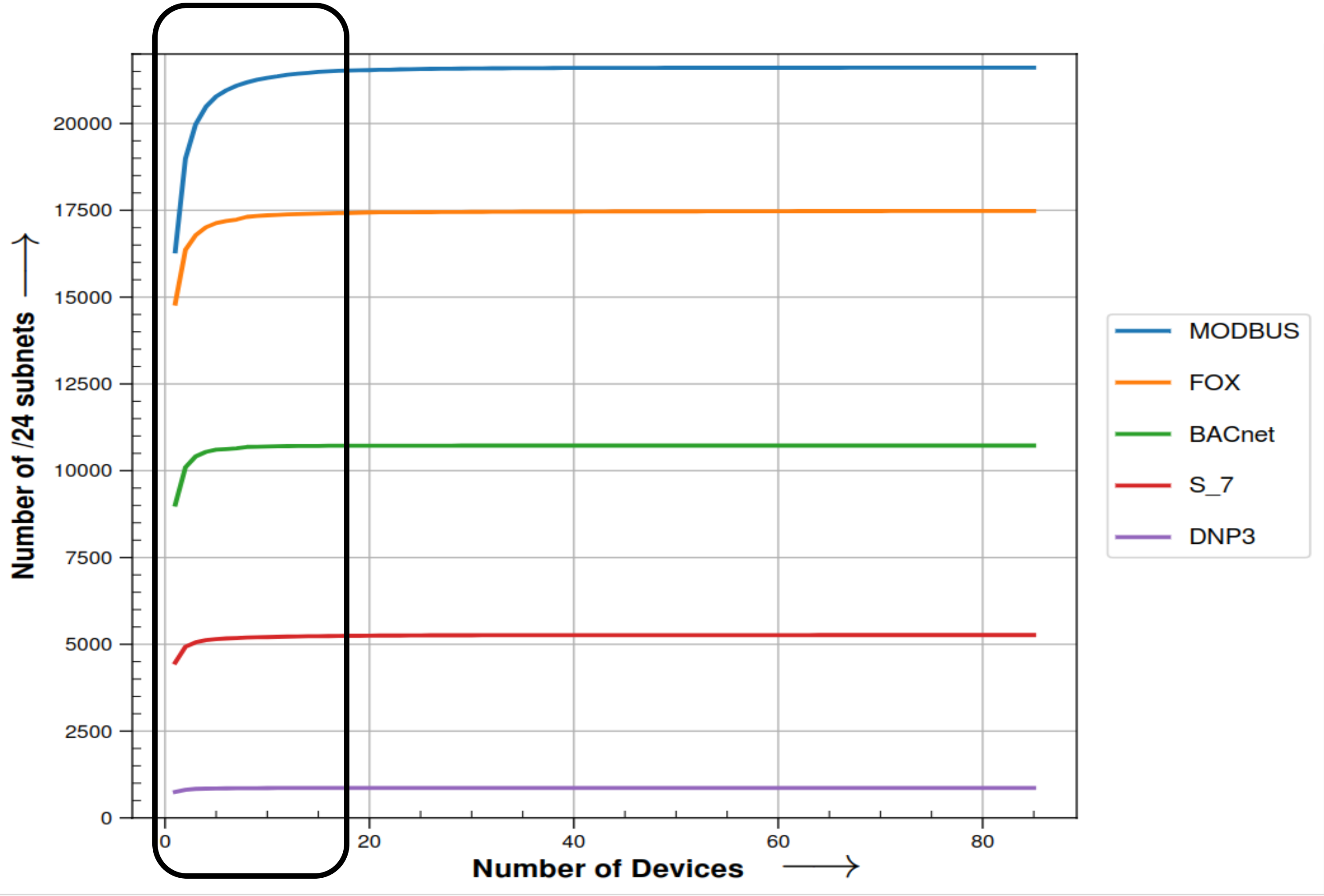


▨ Devices running service "S7" **don't** have port <x-axis> open

□ Devices running service "S7" have port <x-axis> open

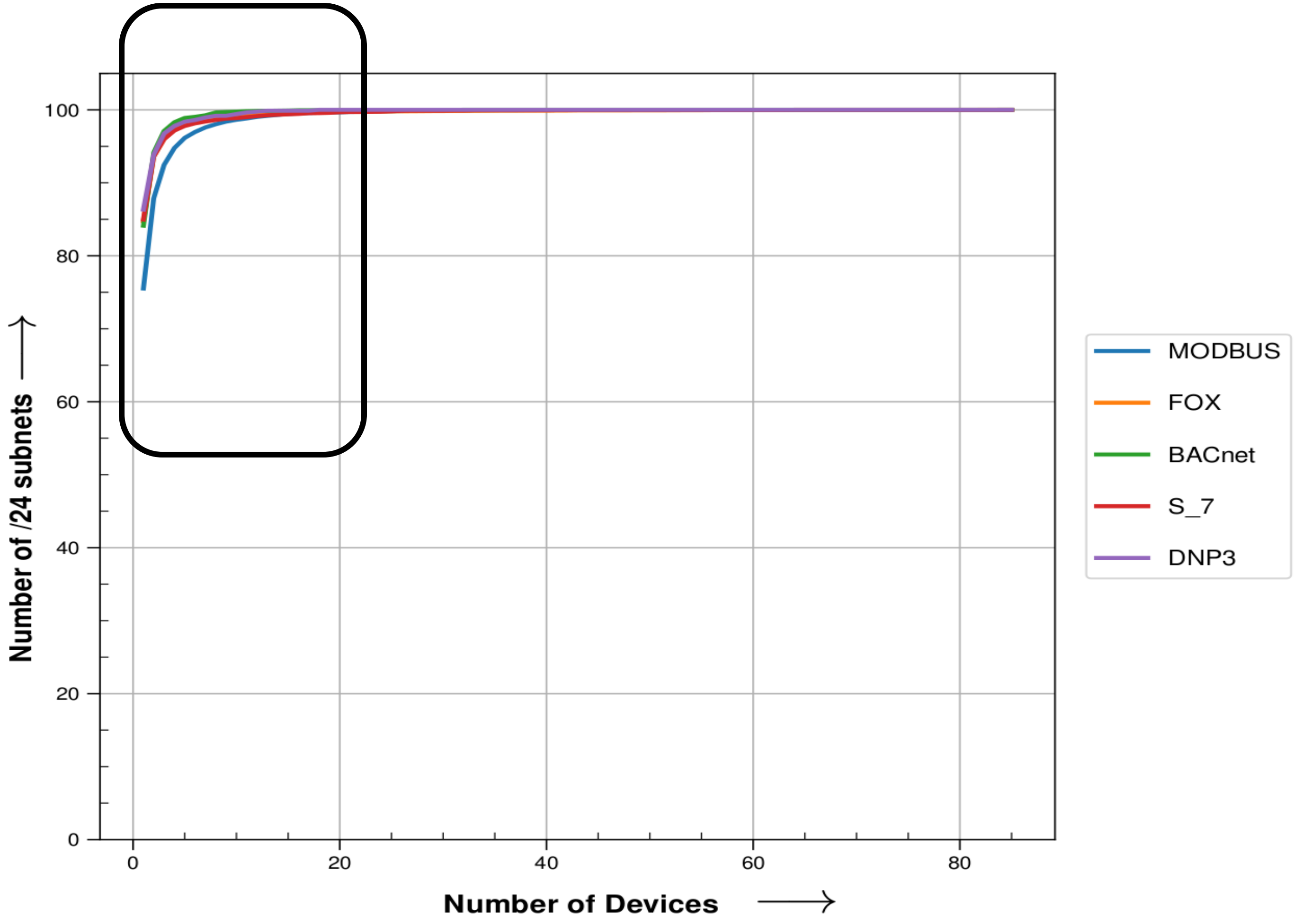
3. How many /24's actually?

Question: How many /24's host atmost <**x**> (max. 254) no. Of devices?



3. How many /24's actually?

Question: How many /24's host atmost <**x**> (max. 254) no. Of devices?



Future work:

- Deeper analysis for the factors behind sudden peak and fall in total number of active devices.

- Identifying the parties (Censys, Shodan, government org., manufacturer org., Malicious org., etc.) scanning for such services.

- Detection of Honeypots, Botnets, etc.

- Understanding of organisation's deployment model, and notify the ones who disobey the standardised principles.