ANALYZING THE IMPACT OF SOFTWARE SUPPLY CHAIN VULNERABILITIES ON CRITICAL INFRASTRUCTURE

Daniel dos Santos, PhD
Sr. Research Manager, Forescout Technologies

CPS4CIP 2021

About me & Forescout

<) Daniel dos Santos

- Sr. Research Manager at Forescout, leading **vulnerability and threat research**
- Postdoc in critical infrastructure security at University of Eindhoven
- PhD in computer science from University of Trento
- 30+ publications in conferences and journals
- ~10 years of experience in cyber security (research, development, penetration testing)

<) Forescout's mission

- Actively Defend the Enterprise of Things by continuously **identifying**, **segmenting** and **enforcing compliance of** *every connected thing*

<) FORESCOUT®

Don't just see it. Secure it.

Active Defense for the Enterprise of Things.

H2020 projects related to CIP

SAFECARE

Integrated cyber-physical security for health services

https://www.safecare-project.eu/

Forescout role:
Intrusion detection on
Building Automation Systems
in Healthcare

SeCoIIA

https://secoiia.eu/

Forescout role:
Intrusion detection on
Industrial Control Systems
in Manufacturing

Agenda

- The Software Supply Chain
- Finding Vulnerabilities
- Analyzing their Impact on Critical Infrastructure
- Future Work

THE SOFTWARE SUPPLY CHAIN

Why you should care about it

The supply chain threat landscape

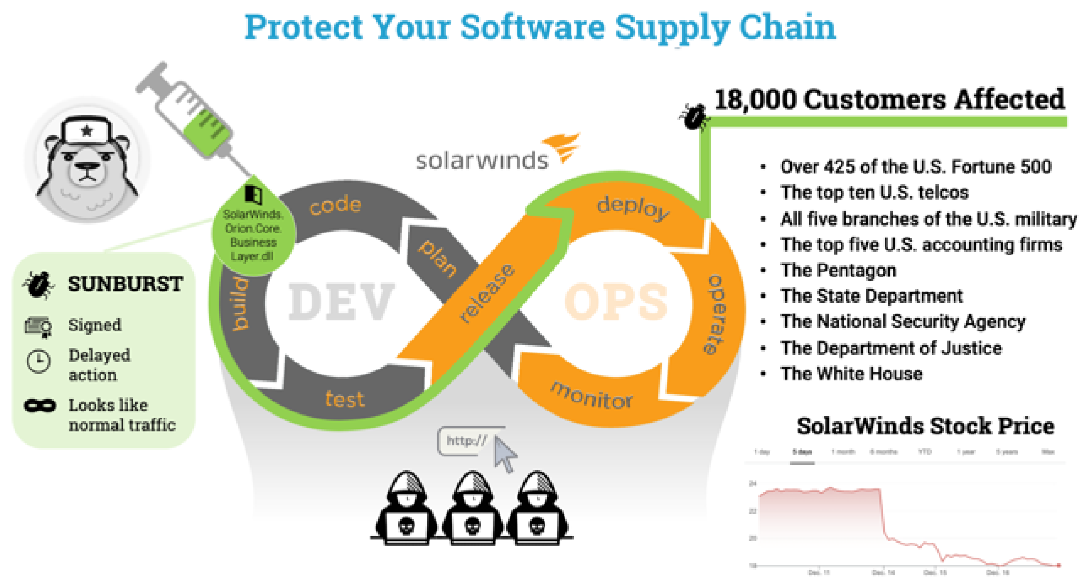
enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

JULY 2021

https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

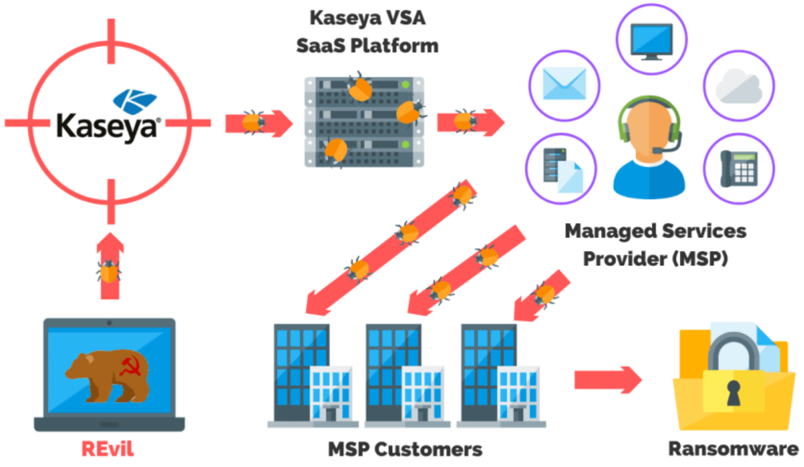


Protect Your Software Supply Chain

18,000 Customers Affected

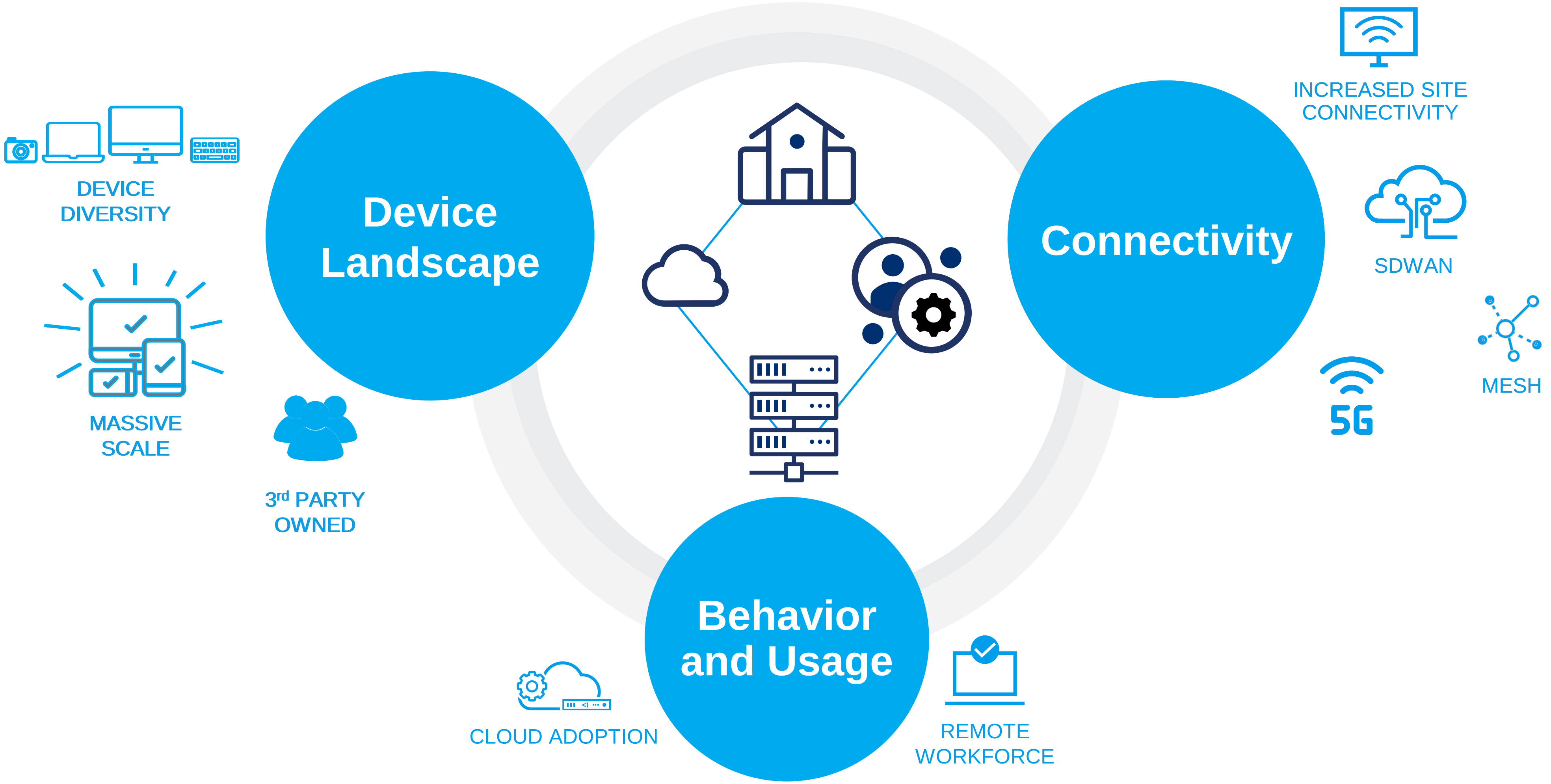
- Over 425 of the U.S. Fortune 500
- The top ten U.S. telcos
- All five branches of the U.S. military
- The top five U.S. accounting firms
- The Pentagon
- The State Department
- The National Security Agency
- The Department of Justice
- The White House

https://blog.adolus.com/blog/three-things-the-solarwinds-supply-chain-attack-can-teach-us

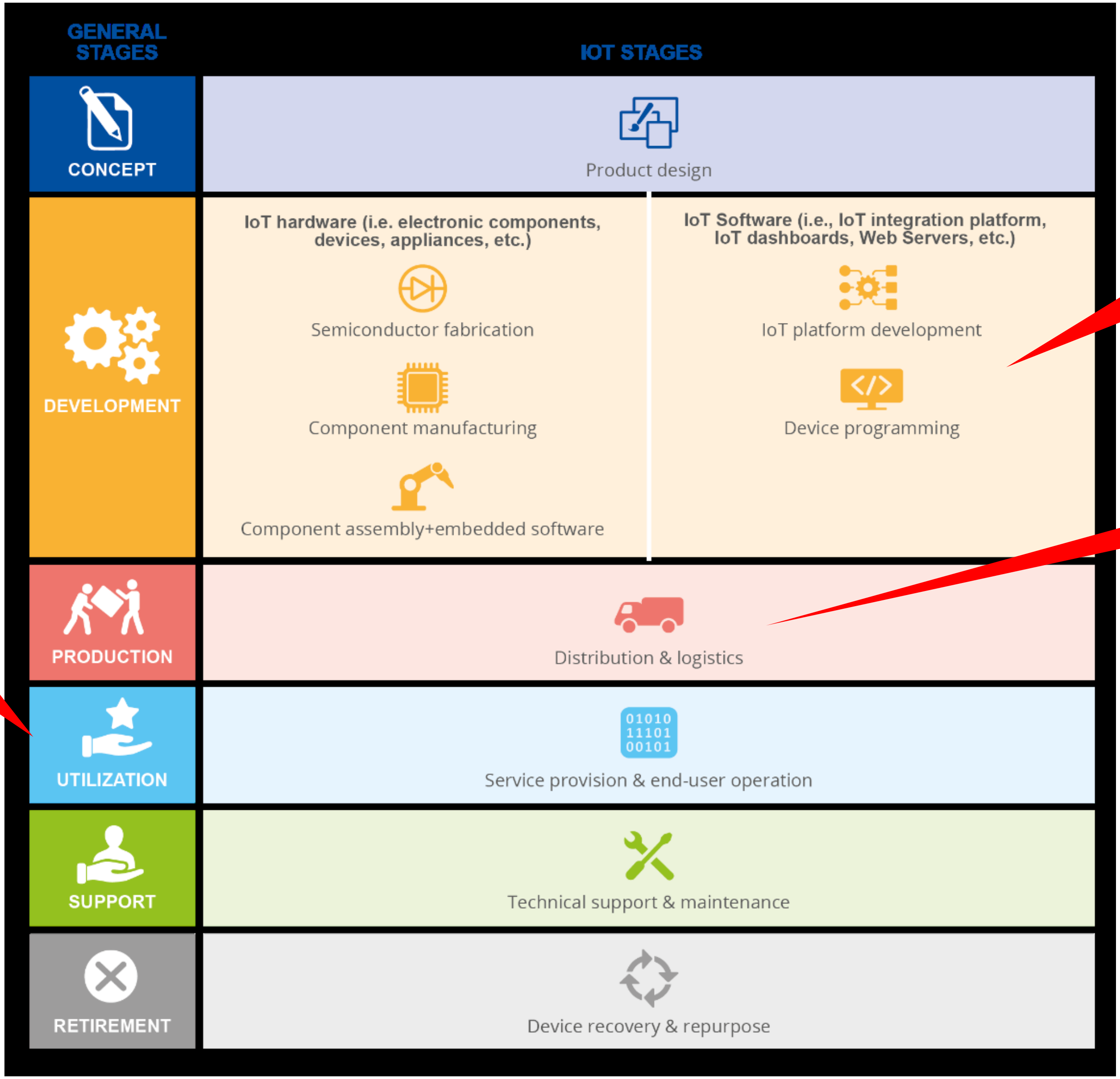


https://purplesec.us/kaseya-ransomware-attack-explained/

Critical Infrastructure networks are changing



The IoT/OT device supply chain



GENERAL STAGES	IOT STAGES
CONCEPT	Product design
DEVELOPMENT	IoT hardware (i.e. electronic components, devices, appliances, etc.) Semiconductor fabrication Component manufacturing Component assembly+embedded software IoT Software (i.e., IoT integration platform, IoT dashboards, Web Servers, etc.) IoT platform development Device programming
PRODUCTION	Distribution & logistics
UTILIZATION	Service provision & end-user operation
SUPPORT	Technical support & maintenance
RETIREMENT	Device recovery & repurpose

Naturally occurring vulnerabilities

Injected backdoors, malware

Device Misconfiguration (e.g., default passwords)

https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

FINDING VULNERABILITIES

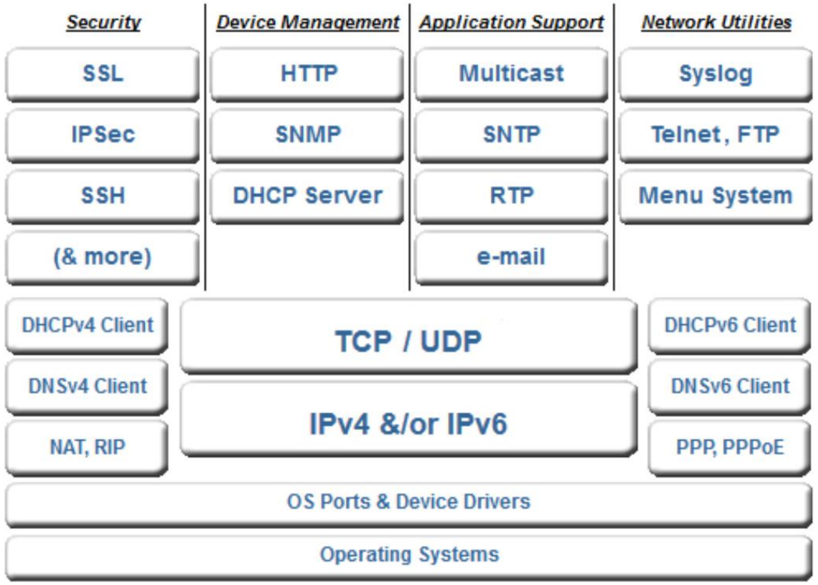
Looking at a specific supply chain component

The example of TCP/IP stacks

- **Old and widespread** software libraries that enable basic **network communication** for IoT/OT devices
  - Often **20+ years old** and used by **hundreds of device vendors**

- **Old types of vulnerabilities** resurfaced decades later to affect billions of devices – e.g., URGENT/11, Ripple20
  - Externally exposed, often run as **privileged, low-level component**

- They trickle down the supply chain, being **used in hardware components, systems on a chip, end devices**, etc.
  - RTOS decoupling and absence of Software Bill of Materials (SBOM) makes it difficult to identify which stack a device is running.



Security	Device Management	Application Support	Network Utilities
SSL	HTTP	Multicast	Syslog
IPSec	SNMP	SNTP	Telnet, FTP
SSH	DHCP Server	RTP	Menu System
(& more)		e-mail	

DHCPv4 Client	TCP / UDP	DHCPv6 Client
DNSv4 Client	IPv4 &/or IPv6	DNSv6 Client
NAT, RIP		PPP, PPPoE

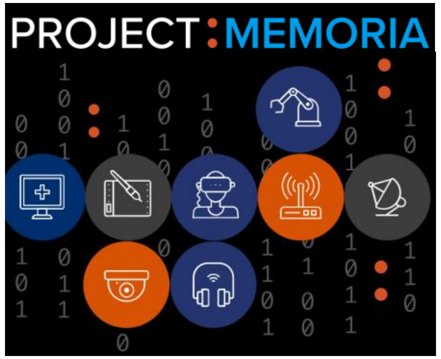
OS Ports & Device Drivers

Operating Systems

https://ww1.microchip.com/downloads/en/Site_Resource/NicheStack%20IPv4-ProductBrief.pdf

Project Memoria

- Large-scale analysis of TCP/IP stacks
  - 18 months, May/2020-October/2021
- Goals:
  - Find and disclose new vulnerabilities on TCP/IP stacks
  - Understand the common aspects of these vulnerabilities
  - Analyze the potential impact of this emerging threat landscape



https://www.forescout.com/research-labs/project-memoria/

Methodology

Target selection

- Popular open-source and closed-source stacks
- 14 stacks selected

White-box fuzzing

- Using state-of-the-art coverage-guided fuzzing (e.g., libFuzzer)
- More details: How TCP/IP stacks breed critical vulnerabilities @Black Hat EU 2020

Manual / variant analysis

- Looking at previous vulnerabilities and find similar issues in other stacks
- More details: The cost of complexity: different vulnerabilities while implementing the same RFC @Black Hat Asia 2021

Automated binary analysis

- Reverse engineering + taint analysis
- More details: Squashing the Low-hanging Fruit in Embedded Software @Hack in the Box 2021

Results

- 78 CVEs disclosed by Forescout Research Labs
  - **AMNESIA:33** – 33 vulnerabilities on 4 open-source TCP/IP stacks
    - 1/3 found via fuzzing, 2/3 via manual analysis

  - **NUMBER:JACK** – 9 vulnerabilities related to TCP ISN
  - **NAME:WRECK** – 9 vulnerabilities on DNS clients of 4 stacks
  - 13 vulnerabilities currently being disclosed
    - All found via manual / variant analysis

  - **INFRA:HALT** – 14 vulnerabilities on a stack popular in OT
    - ½ found via automated binary analysis

- Mostly memory corruption vulnerabilities, which allow attackers to:
  - Exfiltrate data from devices (Infoleak)
  - Crash devices (DoS)
  - Remotely take control of devices (RCE)

The supply chain effect

https://github.com/Forescout/project-memoria-advisories/

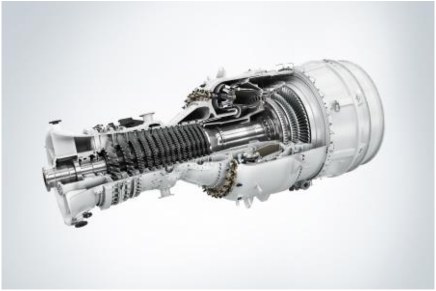
- Disclosures involving several coordination agencies and more than 400 device vendors over more than a year

- Affecting from WiFi chips in consumer IoT to Remote Terminal Units that control electrical sub-stations, some examples

Smart meters

PLCs

RTUs

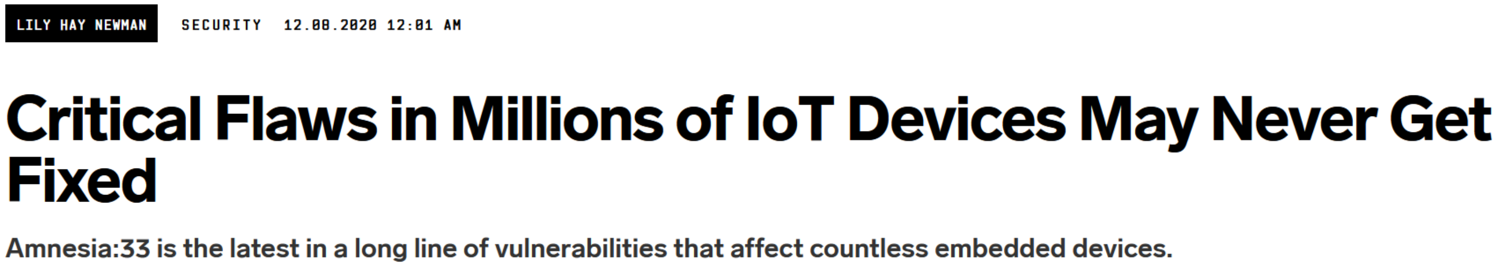


Gas Turbines

Infusion pumps

Blood collection

The supply chain consequence

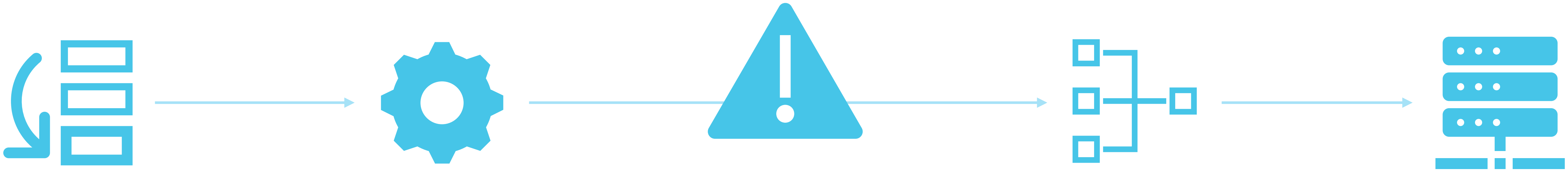


LILY HAY NEWMAN SECURITY 12.08.2020 12:01 AM

Critical Flaws in Millions of IoT Devices May Never Get Fixed

Amnesia:33 is the latest in a long line of vulnerabilities that affect countless embedded devices.

https://www.wired.com/story/amnesia33-iot-vulnerabilitiesmay-never-get-fixed/



TCP/IP stack
(Vendor A)

Operating System
(Vendor B)

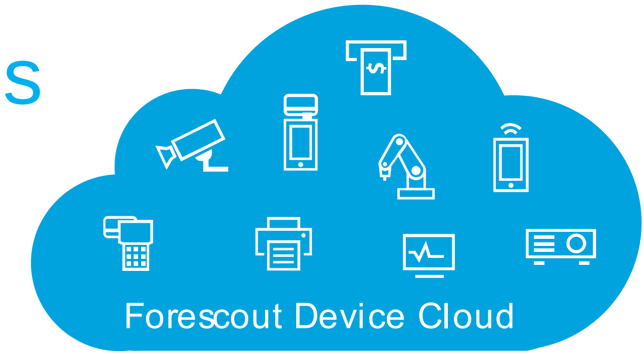
Network Management Card
(Vendor C)

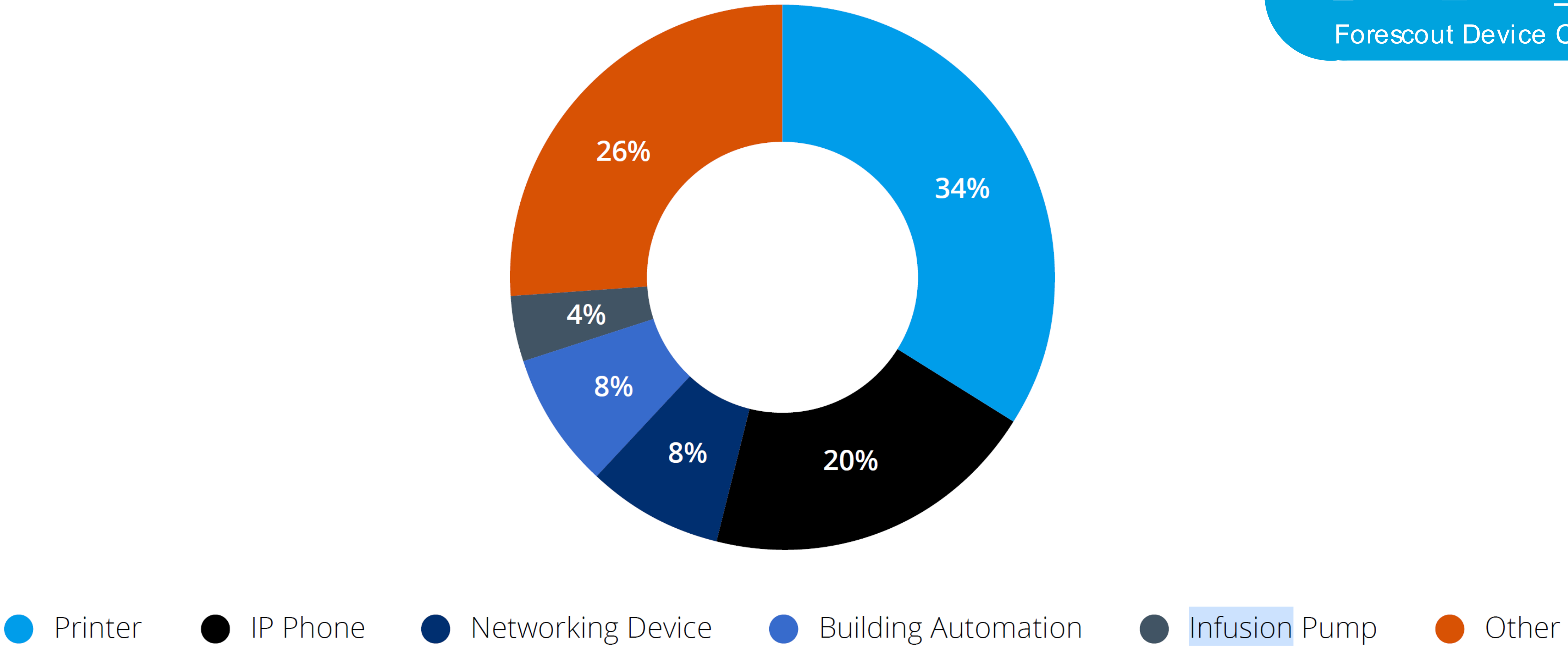
UPS
(Vendor D)

ANALYZING THEIR IMPACT

Data-driven analysis based on Device Cloud

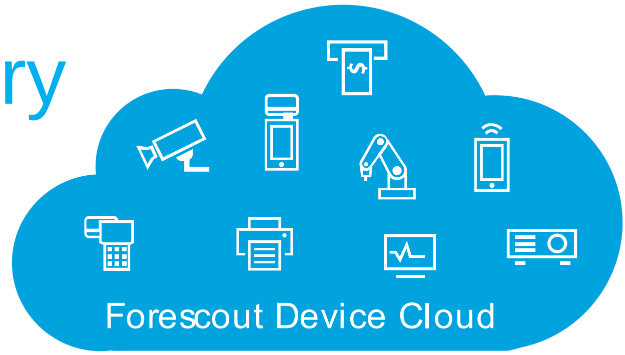
Most common vulnerable device types

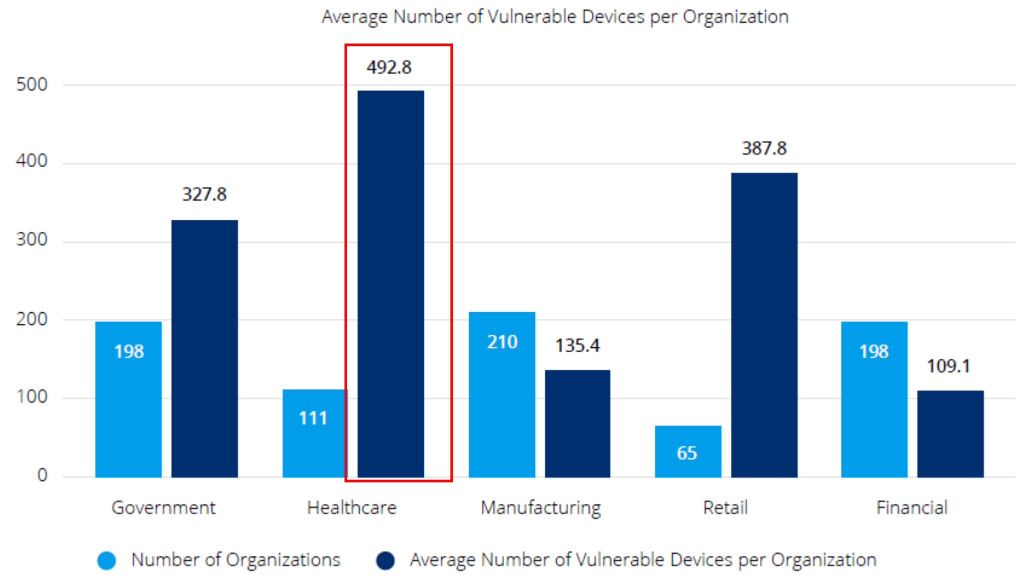


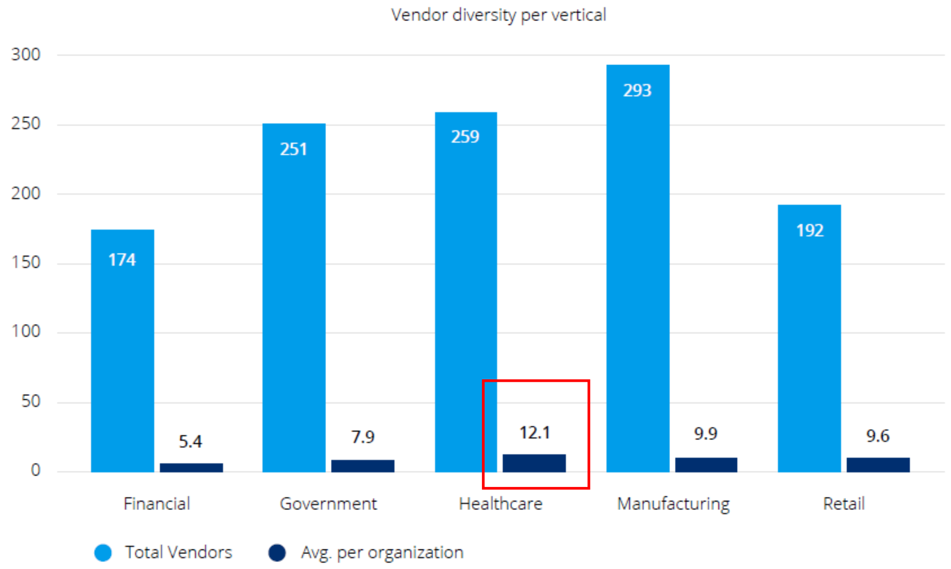


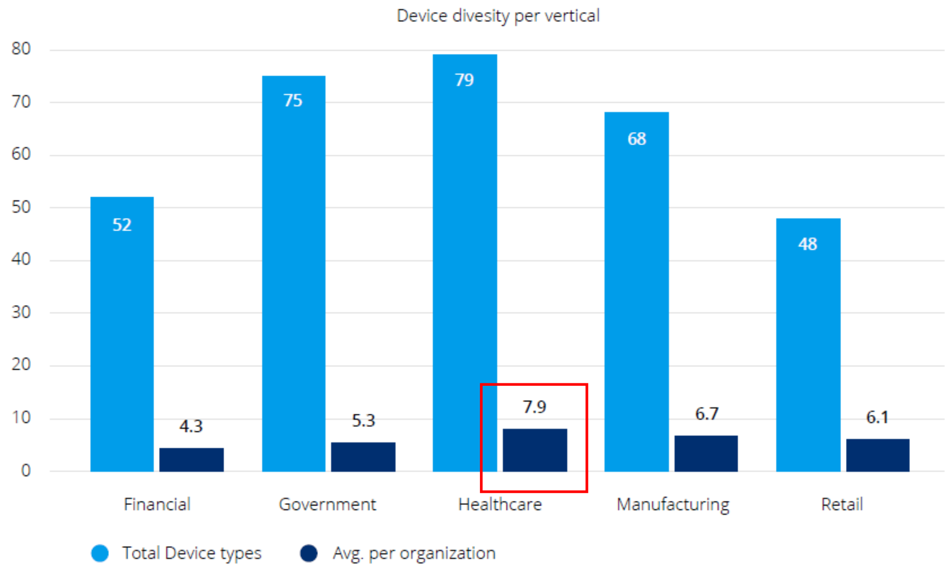
https://www.forescout.com/the-underlying-risks-found-in-healthcare-devices/

Healthcare is the most impacted industry



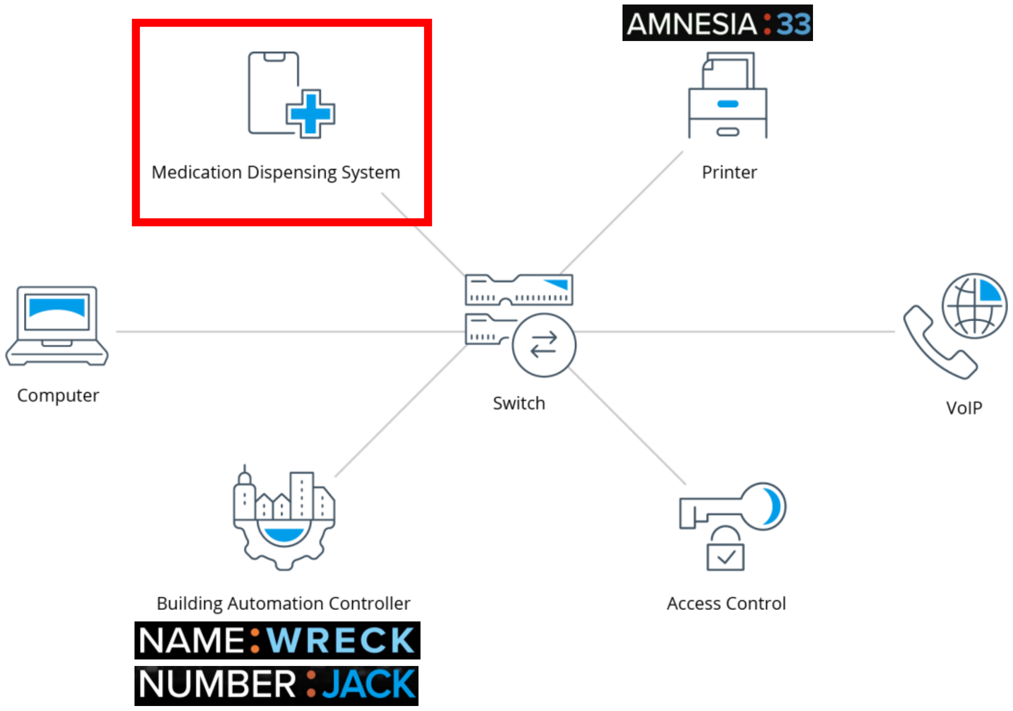


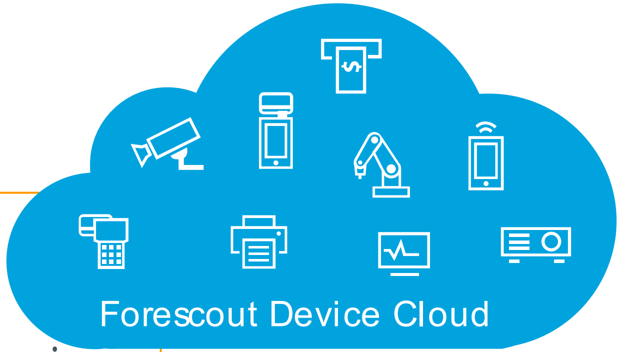




https://www.forescout.com/the-underlying-risks-found-in-healthcare-devices/

It’s not just vulnerable devices – network misconfigurations





This is a VLAN of a **Pharmacy** in our Device Cloud.

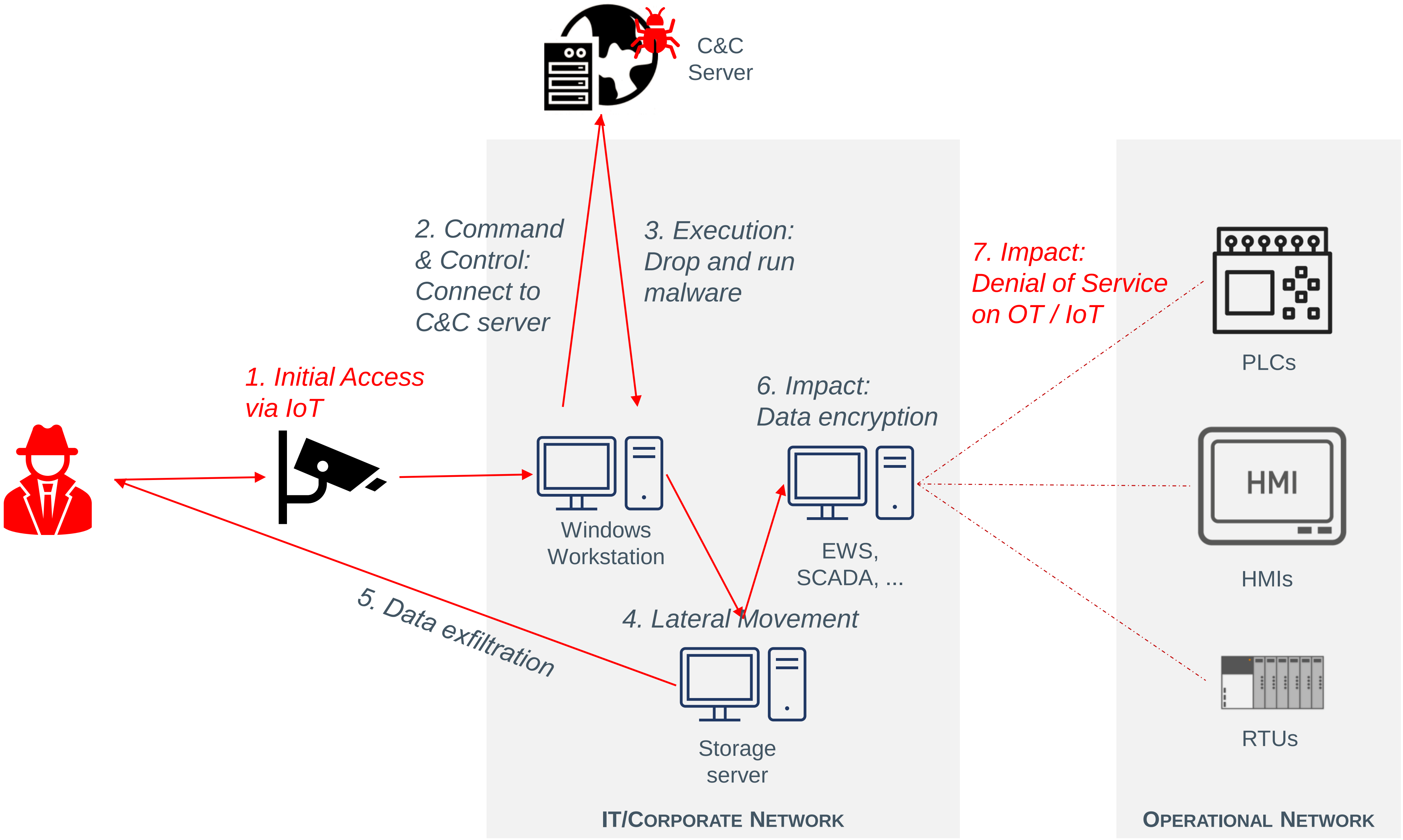
Connected to the
same VLAN, there are a building automation controller **vulnerable to NAME:WRECK** and **NUMBER:JACK**, and a printer vulnerable to **AMNESIA:33**.

each of those devices can represent an **entry point** to the medical network, and attackers have **a wide selection of targets on the menu**.

See also: A Matter of Life and Death: Analyzing the Security of Healthcare Networks @ IFIP SEC 2020

FUTURE WORK

How this fits in a larger attack campaign



1. Initial Access via IoT

2. Command & Control: Connect to C&C server

3. Execution: Drop and run malware

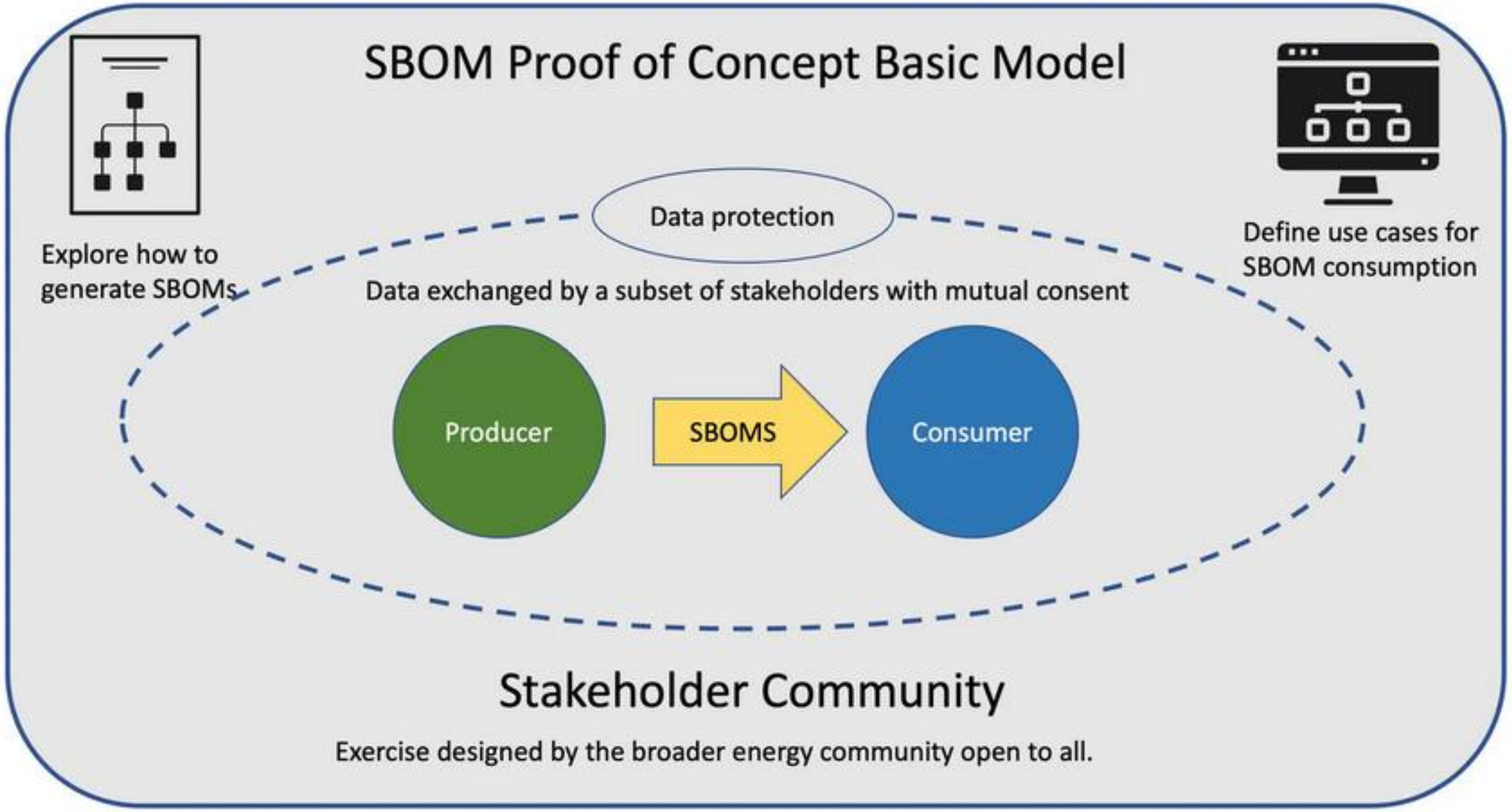
4. Lateral Movement

5. Data exfiltration

6. Impact: Data encryption

7. Impact: Denial of Service on OT / IoT

Trying to solve some problems: SBOM


SBOM Proof of Concept Basic Model
Explore how to generate SBOMs
Data protection
Define use cases for SBOM consumption
Data exchanged by a subset of stakeholders with mutual consent
Producer
SBOMS
Consumer
Stakeholder Community
Exercise designed by the broader energy community open to all.

https://inl.gov/sbom-poc/

Key takeaways

- Recent events and research highlight the importance of supply chain security
- TCP/IP stacks (and probably other foundational components) have very similar vulnerabilities
- These vulnerabilities impact many critical devices at the same time. Many of those devices sit in poorly configured networks
- This opens the possibility of leveraging these vulnerabilities for larger-scale attacks.
- Future solutions involve the use of SBOM, but currently proper asset inventory and network monitoring are the best mitigation

Thank you!

daniel.dossantos@forescout.com