Federal Facilities Council Presentation:

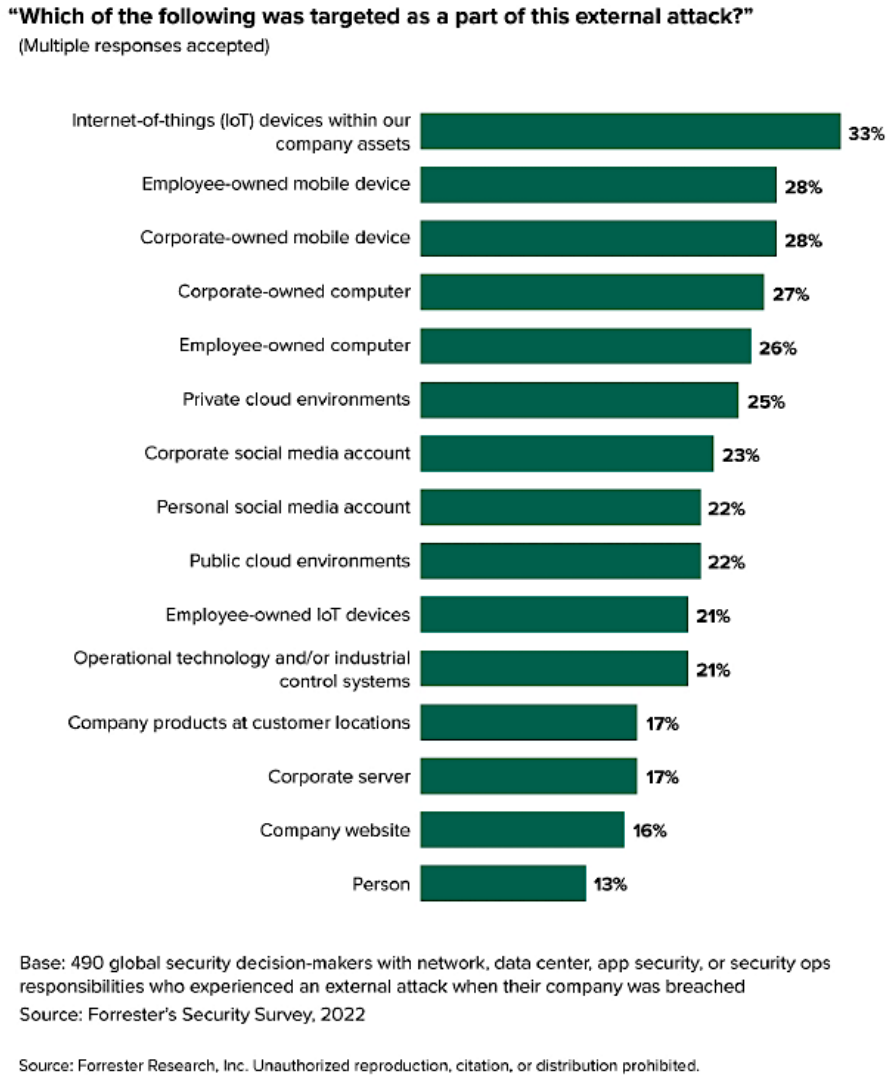
Guarding Against OT Supply Chain-Based Attacks

AlphaGuardian™

OPERATIONAL TECHNOLOGY SECURITY MADE SIMPLE

Cyberattacks Use OT/IoT as *a* Major Source of Data Breaches

Data Breaches Often Use OT/IoT Systems as Back Doors to Enter a Network

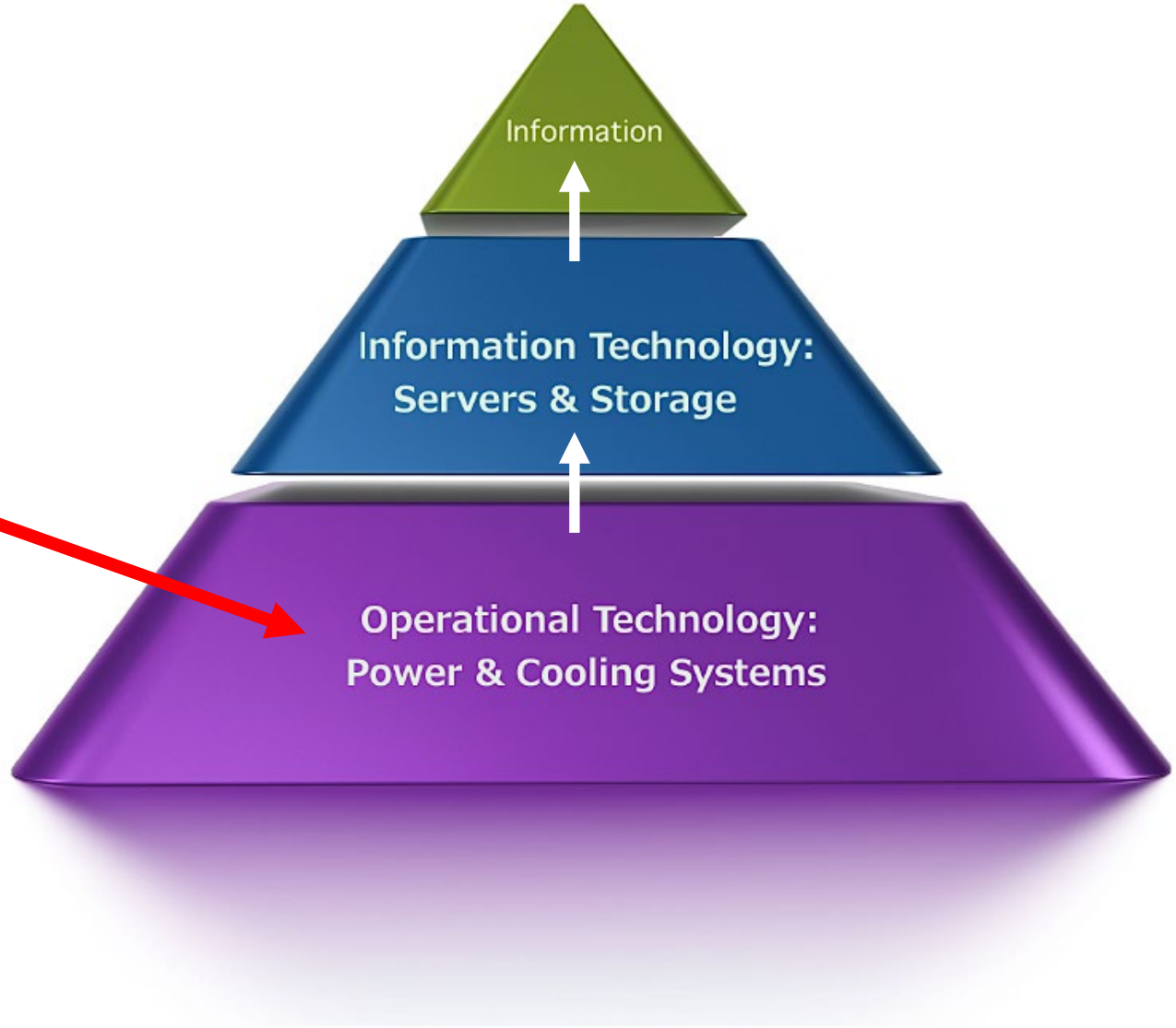


"The Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy (DOE) said they 'are aware of threat actors gaining access to a variety of internet-connected uninterruptable power supply (UPS) devices.'" – ZDNet March 30, 2022

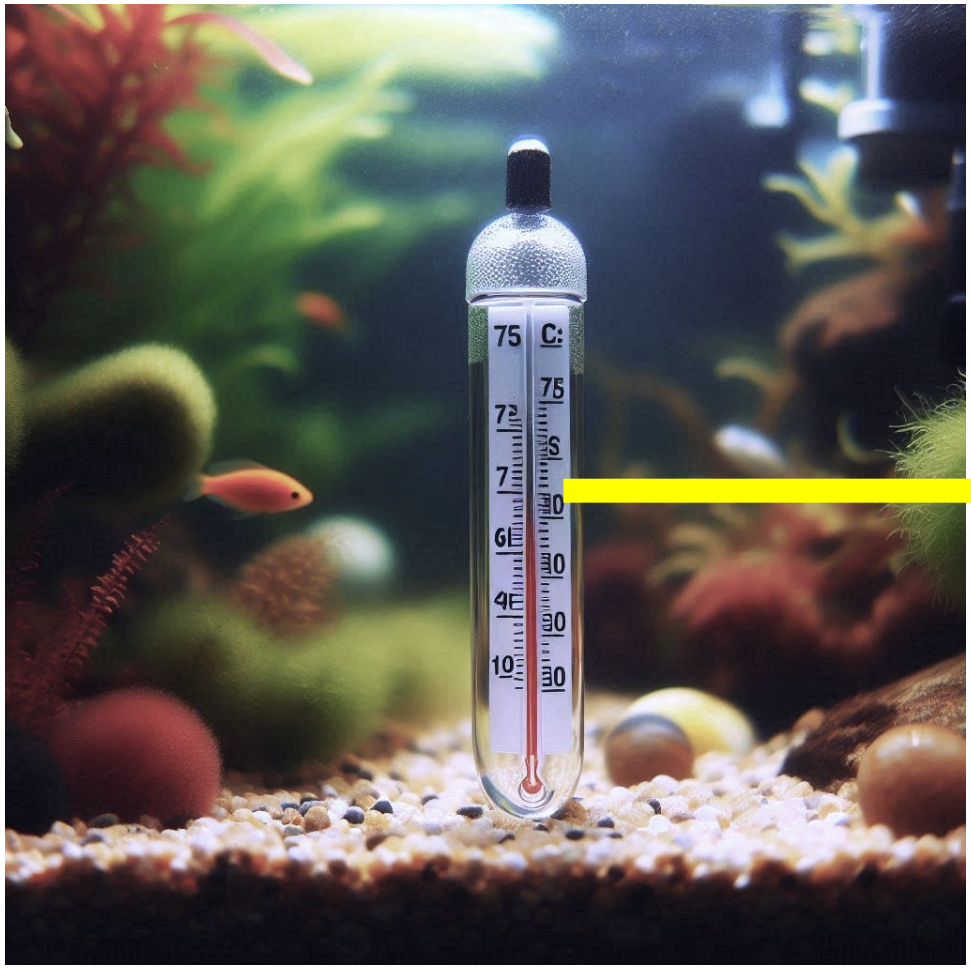
PLCs are ranked as the #1 most vulnerable target among OT systems - Forescout Technologies, June 11, 2024

"PLC cybersecurity isn't just an essential precaution, it has become a vital element…PLC's have never been designed with security in mind. Anyone with the skills and equipment could upload, download, delete or modify programs." The Rising Important of PLC Cybersecurity – Engineering.com, July 19,2023

OT/IoT Systems Are Easy Backdoors to IT Information



Example: Fish Tank Thermometer Used To Hack Casino Servers



https://www.entrepreneur.com/business-news/a-casino-gets-hacked-through-a-fish-tank-thermometer/368943

Supply Chain-Based Attacks Are Common and Serious

Software and Firmware Supply Chain-Based Attacks Are Increasing

- **Supply Chain-Based Attacks, a Definition -** The use of a manufacturer's software or firmware update process to inject malicious code into a device or exploit a vulnerability within that updated vendor code.

- **Software Supply Chain Attacks**

91% of all organizations experienced a software supply attack last year – Data Theorum, February 13, 2024

- **Firmware Supply Chain Attacks**

The number of firmware vulnerabilities has skyrocketed in recent years. Security researchers believe that the total number of Common Vulnerabilities and Exposures (CVEs) is 7.5 times greater than what was documented just three years ago. – Palo Alto Networks

CVE Exploitations Nearly Tripped in 2023 alone – Verizon Cybersecurity Report

Federal Requirements Mandate OT/IoT Cybersecurity

All OT/IoT In Federal Facilities Must Now Be Protected

- **Internet of Things Cybersecurity Improvement Act of 2020**

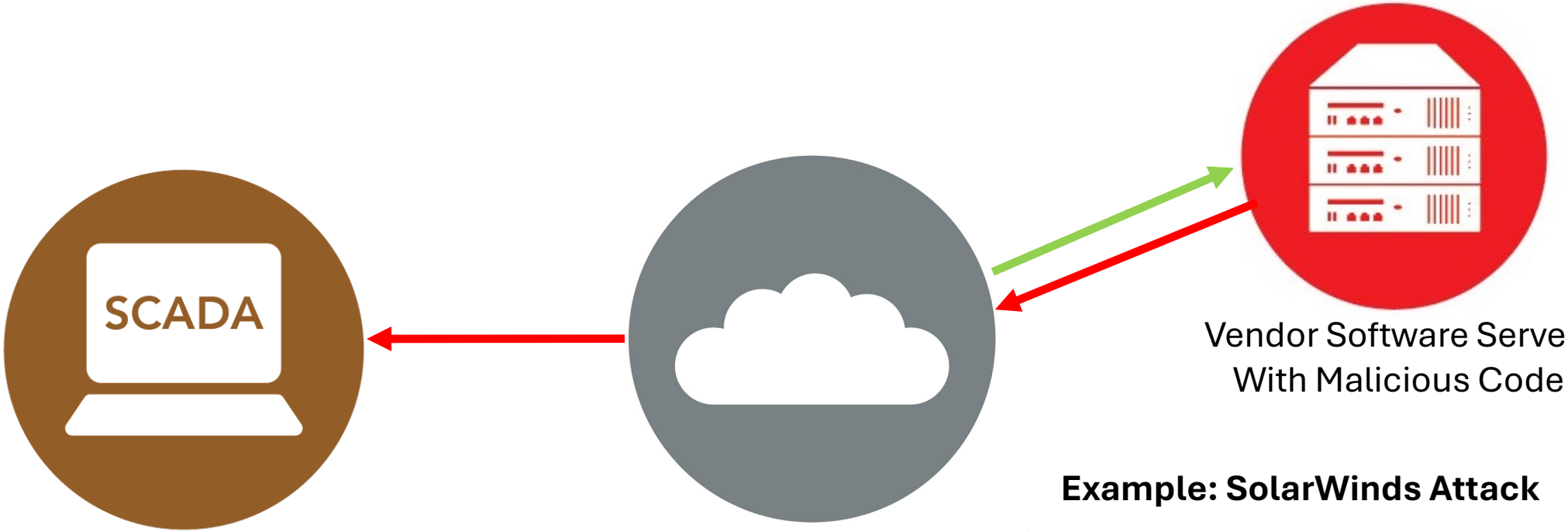
"National Institute of Standards and Technology (NIST) has set ``guidelines for the Federal Government on the appropriate use and management by agencies of Internet of Things devices owned or controlled by an agency and connected to information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices."

- **Biden Executive Order of May 12, 2021**

"The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT))."

SCADA/BAS Software Supply Chain Attack

Injecting Malicious Code Directly Into the Software Update Servers of a Supplier



SCADA/BAS

Vendor Software Server
With Malicious Code

Example: SolarWinds Attack

September 2019 – Russian actors gain access to SolarWinds software update servers

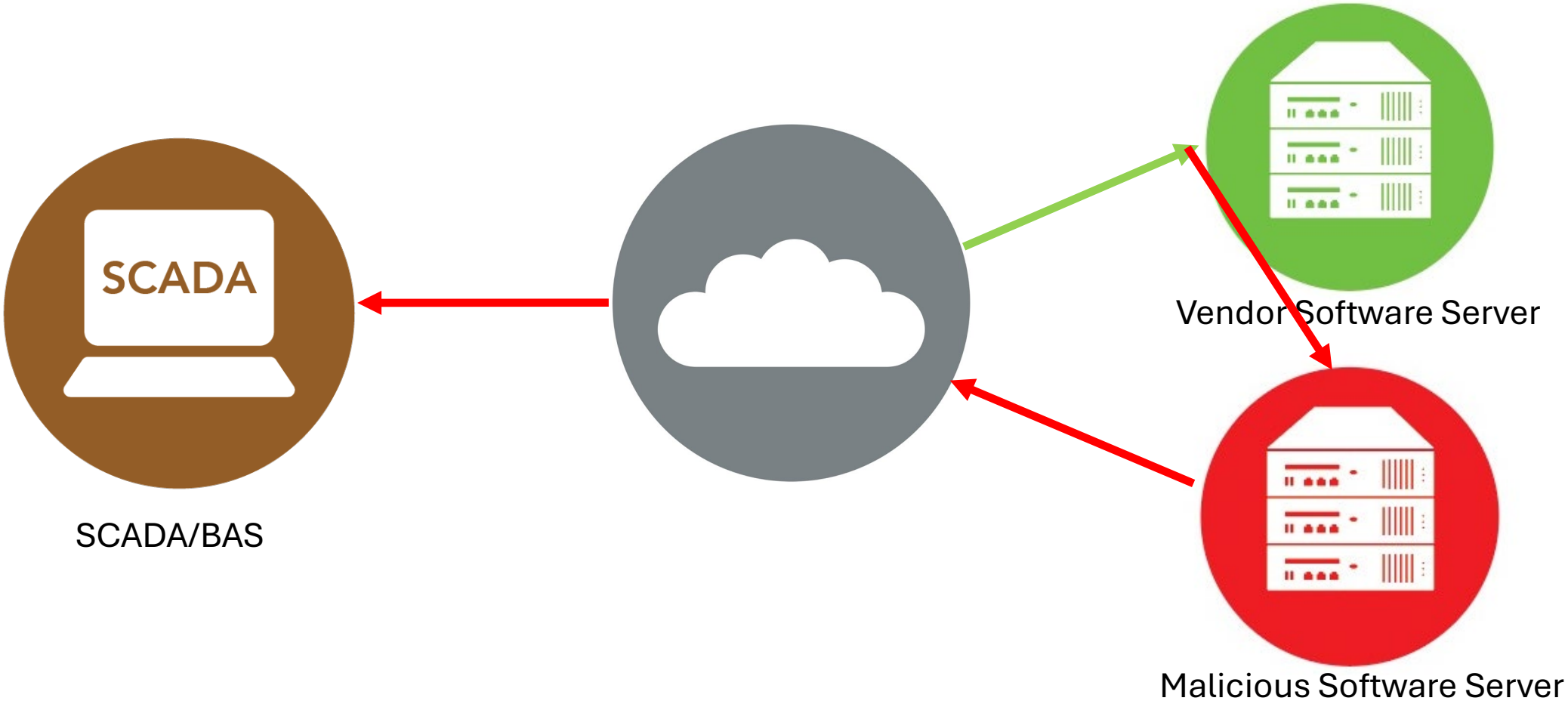
October 2019 - Initial malware code placement test

Feb. 20, 2020 - Malicious code placed into SolarWinds Orion code

March 26, 2020 - SolarWinds begins sending out Orion software updates with embedded Malware

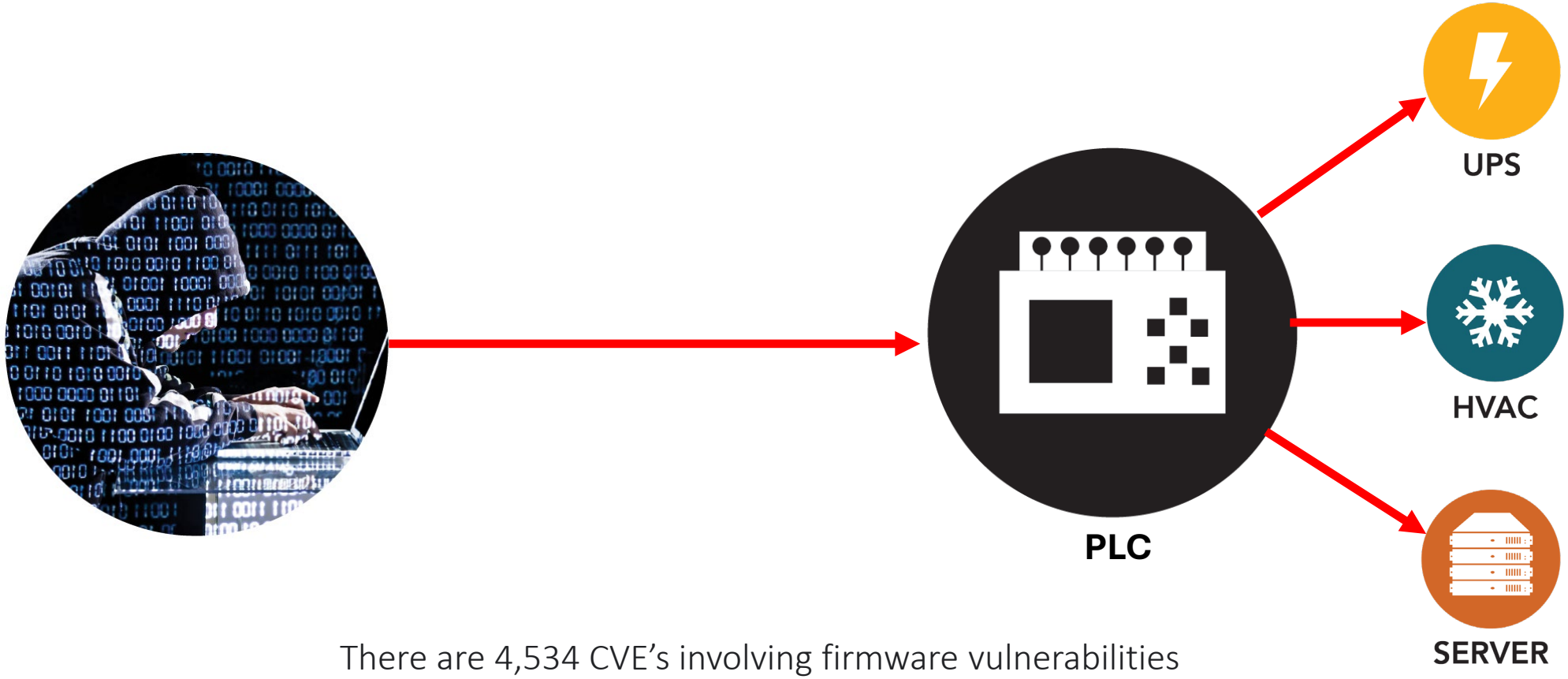
SCADA/BAS Software Supply Chain Attack

Hijacked Software Upgrade Servers Can Redirect Your System To a Rogue Site



OT Firmware Supply Chain Vulnerability-Based Attack

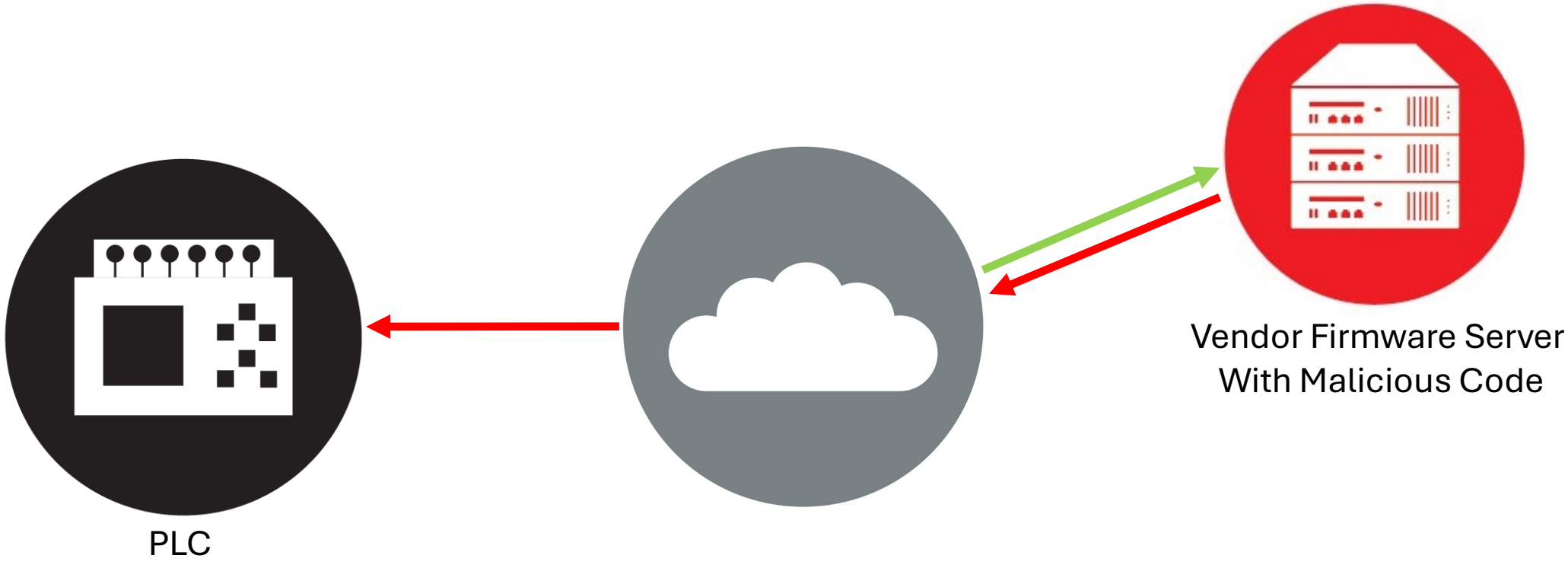
Vulnerable Firmware Detected and Exploited by National Enemy



There are 4,534 CVE's involving firmware vulnerabilities listed in the National Institute of Standards and Technology's database - NIST website July 6, 2024

OT Firmware Supply Chain Compromised Server Attack

Injecting Malicious Code Directly Into the Firmware Update Servers of a Supplier



How To Guard Against Supply Chain Attacks

- **Employ the Zero Trust Method of OT Security –** Literally, do not trust your vendor software, firmware or employees. In order to implement Zero Trust, you need to do the following:
  - **Separate ALL OT from IT -** Isolate and Segment your OT systems from your IT systems
  - **Continuously Scan Your OT Network for Signs of Malicious Activity –** Use a Threat Discovery and Response solution that has been tested in government
  - **Use a Firewall Specifically Meant for OT Systems –** This can include a Data Diode or a Traditional Firewall that has been tested in government site(s)
  - **Never Allow a Vendor To Access Your OT Network Without Permission and Surveillance –** Do NOT accept the excuse that failure to allow access to your network ”as needed” will violate your equipment warranty

Thank YOU!

AlphaGuardian Networks, LLC

Main Office:
111 Deerwood Road, suite 200
San Ramon, CA. 94583
(925) 421-0050
(888) 990-ALPHA

Principal Contact: Bob Hunter
bhunter@alphaguardian.net