



Red Team vs. Blue Team: CyberAv3ngers

A Kill Chain Analysis of Attacks on
Critical Infrastructure

Agenda

1

Setting the Stage

2

The Threat

3

The Framework

4

The Play-by-Play

5

Key Lessons

Introduction - Red Team

Patrick Eisenschmidt

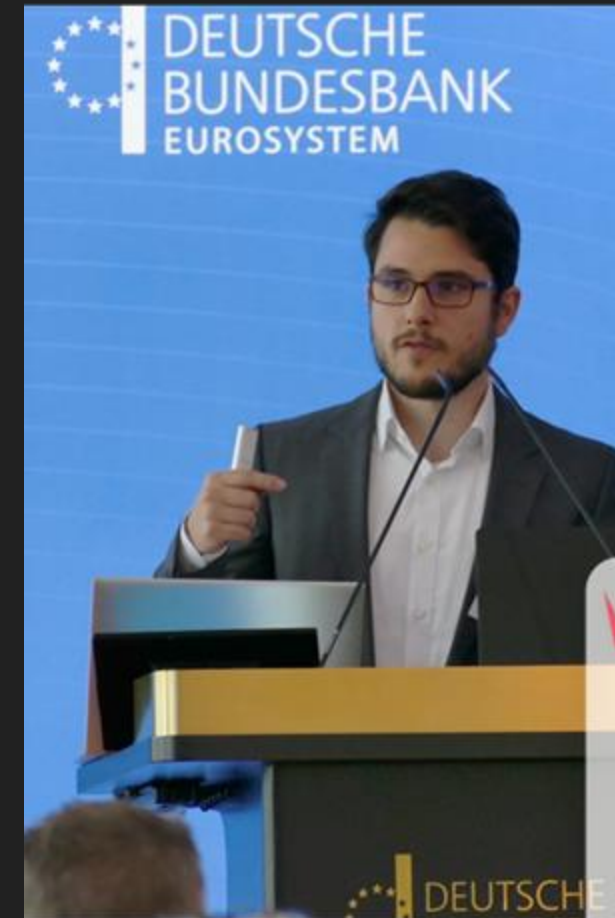
Alias: secdude | Twitter: @secdu_de

Work

- **Red Teaming / TLPT (6+ years)**
- (I)OT Security

Talks

- Red Teaming Lecture at St. Pölten, Austria
- Defcon 32
- SecTor 23/24 a BlackHat Conference
- DeepSec 23
- BSides Frankfurt/Vienna



Introduction - Blue Team

Alexander Steinbrecher

Twitter: @asteinbr

Work

- 15yrs IT in Finance/Banking
- 8yrs IT Security
- currently Blue Teamer at major German Financial Institute
- Focus on Threat Intel, Threat Hunting, Detection Engineering



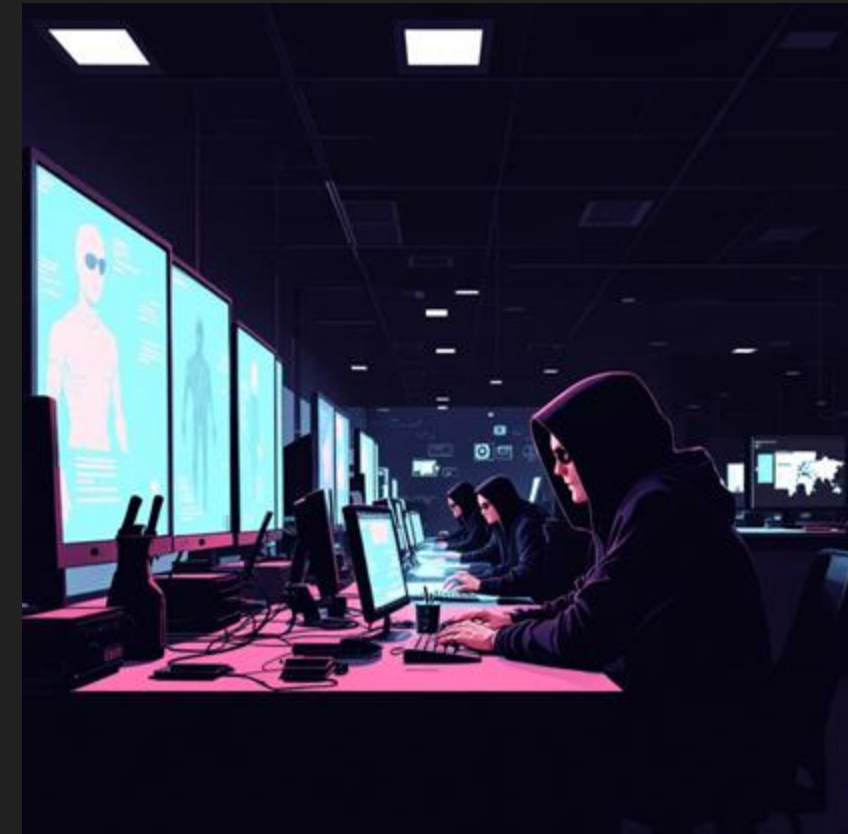
The Adversary: CyberAv3ngers



Screen of a Unitronics device hacked in Aliquippa, Pennsylvania, on Nov. 25, 2023 (Image: Municipal Water Authority of Aliquippa)

Threa Intelligence Briefing - CyberAv3ngers

- Iranian based Threat Actor 
- Alternative Names: Bauxite, Shahid Kaveh Group, Storm-0784
- MITRE ID: [G1027](#)
- Active Since: ~ 2020 - today (escalation in late 2023)
- Targeting critical infrastructure with Israeli-made technology, specifically Unitronics Vision series PLCs in US , Israel 
- Iranian state-sponsored group with connection to Islamic Revolutionary Guard Corps, an Iranian Cyber-Electronic Command (IRGC-CEC)
- Operations are aligned with Iranian geopolitical interests



- Sectors Affected: Water, Energy, Manufacturing
- Motivation: Ideological and political - attacks are disruptive and propagandistic
- TTPs: social engineering, spear phishing, denial-of-service attacks, exploitation of public-facing applications / devices, credential theft, recon, lateral movement, defacement, RATs and wipers, custom malware developments (IOCONTROL)

IT vs OT Environments



Florian Roth ✓ • Following

VP R&D at Nextron Systems

54m • 🌐

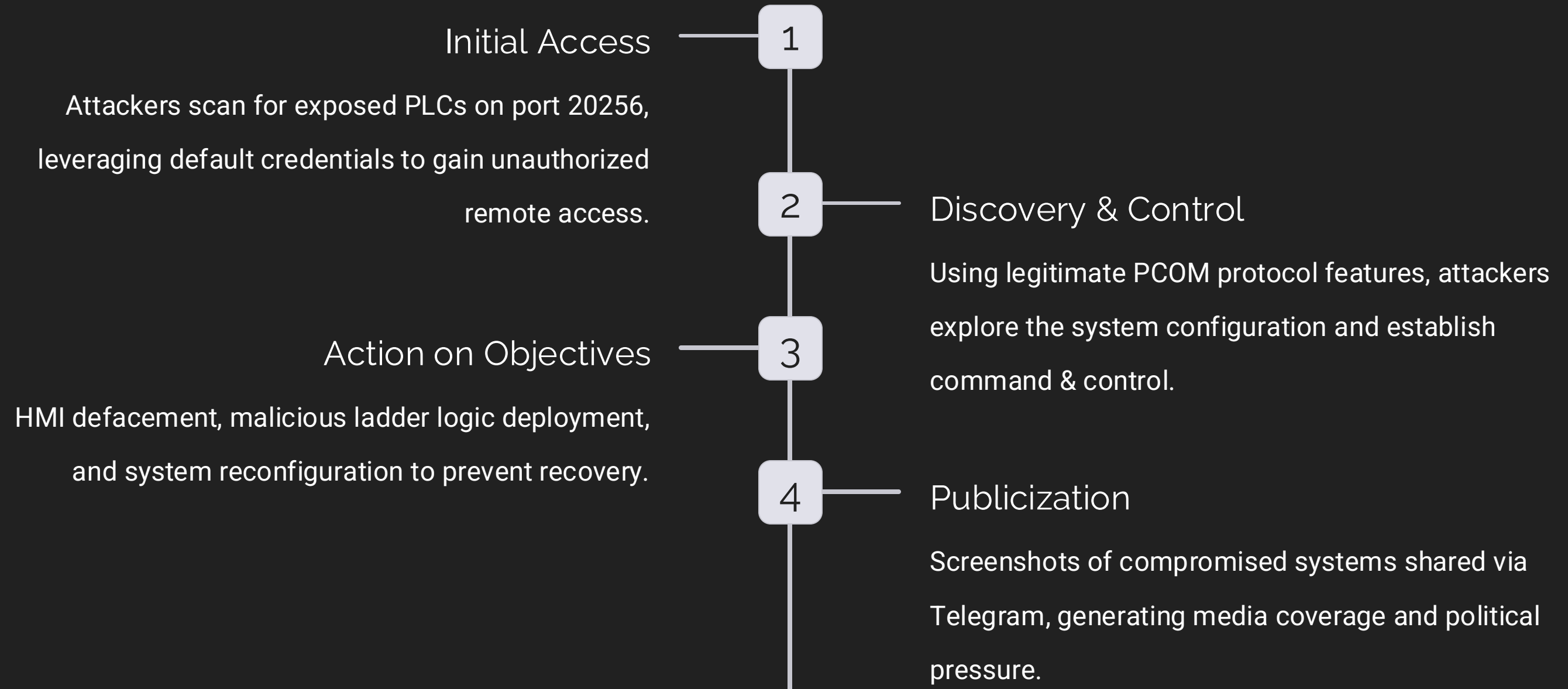


If you think Windows XP in a transport company is funny, you clearly haven't seen the horror show that is industrial IT.

Legacy isn't about laziness – it's about systems you can't legally or practically replace.

#Aeroflot

The Attack Timeline



Framework: The Unified Kill Chain (UKC)

The UKC provides a comprehensive model to analyze attacks spanning both cyber and physical domains, consisting of 18 phases in three main stages:

IN: Foothold

Gaining initial access to the target network and reconnaissance

THROUGH: Network Propagation

Navigating internal networks via lateral movement, privilege escalation, and persistence

OUT: Action on Objectives

Executing the final goal - disruption of physical industrial processes



Reconnaissance

Goal: *Identify vulnerable, internet-facing Unitronics PLCs*

Strategy: Find publicly exposed OT devices with default, insecure configurations - seeking easy targets rather than deploying complex exploits.

Shodan

- port:20256 (PCOM protocol)
- product:"Unitronics"
- http.title:"Unitronics"
- http.html:"Unitronics"

Google Dorking

- intitle:"Unitronics PLC Web Server"
- intitle:"Vision PLC"
- intext:"© Unitronics"



MITRE ATT&CK: T1595 - Active Scanning, T0883 - Internet Accessible Device (ICS)

Reconnaissance ●



Identify and Eliminate Exposure

- Search for exposed devices
- Audit perimeter devices
- Know your assets - Gain complete visibility of your assets - you cannot protect what you do not know about.

Monitor for Reconnaissance Indicators

- Detect active scanning and enumeration
- Monitor for unusual traffic

Harden PLCs Against Discovery

- Implement hardening guides specific to used PLC systems

Threat Intelligence & Attribution

- Join ISACs and subscribe to OT-specific threat intel feeds to stay ahead of known campaigns

Initial Access ●

Goal: Breach the perimeter by logging into the target PLC

Approach

- No exploit code needed - we walk in the front door using credentials the manufacturer and integrator left for us.

Execution

- Testing different default or often used passwords - default password: 1111

Tools

- Nmap, TeamFiltration, NXC, Kerbrute, Impacket

MITRE ATT&CK® (ICS): T0812 - Default Credentials, T0863 - Valid Accounts



Initial Access

Challenge: *Enforcing fundamental access control on critical OT devices by treating every OT device as a critical asset and isolating control systems from all untrusted networks.*

Password Security

- Mandate changing all default passwords on deployment.
- Enforce strong, unique passwords for every device.

Patches / Updates / Hardening

- Keep software and devices updated
- Hardening systems / using best practices

Network Segmentation

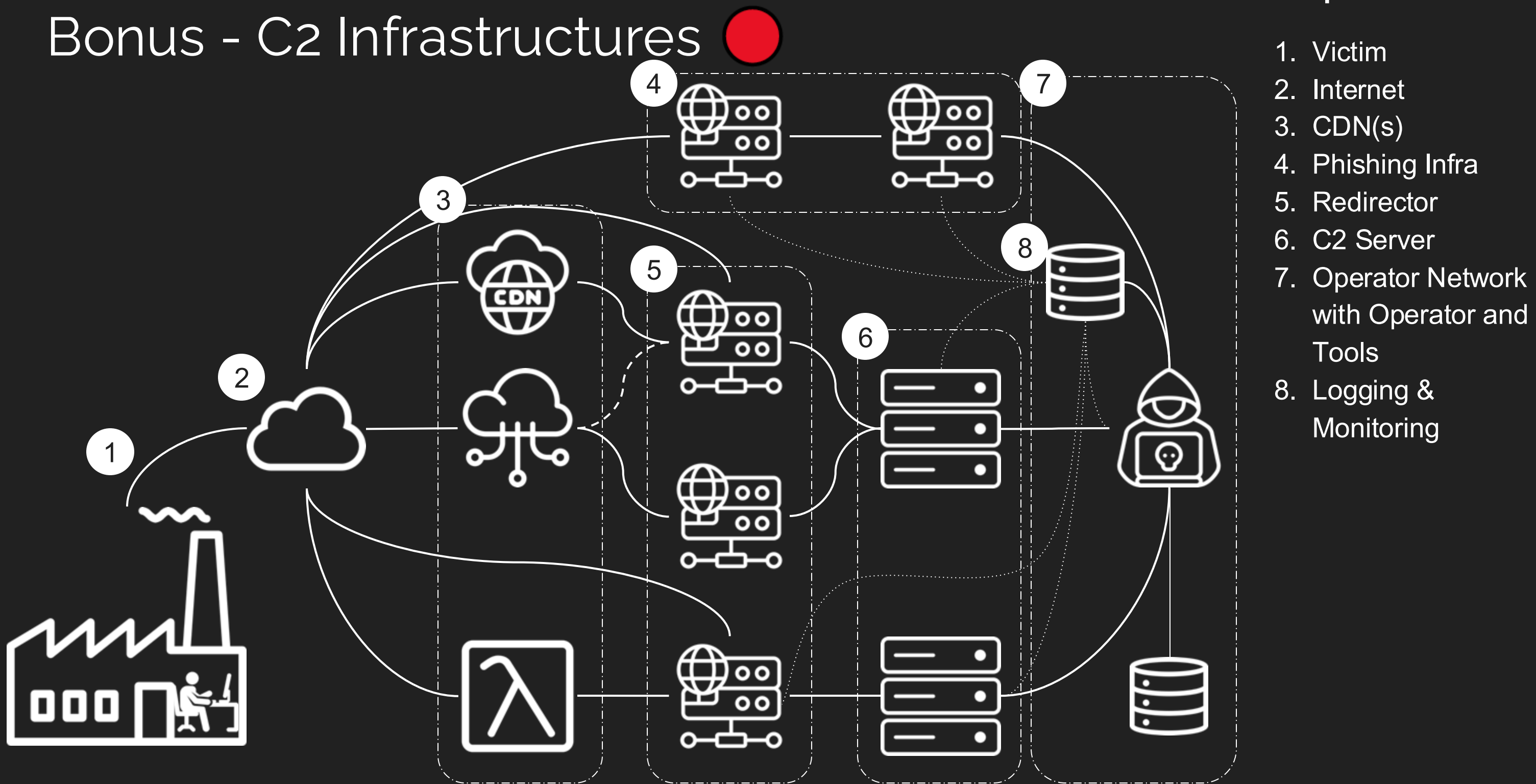
- As recommended by CISA, place PLCs behind a firewall and use a VPN with multi-factor authentication (MFA) for any necessary remote access.

Log Management

- Collect security-relevant logs in a central place.
- Create security detections to alarm on suspicious activities.



Bonus - C2 Infrastructures



Components

1. Victim
2. Internet
3. CDN(s)
4. Phishing Infra
5. Redirector
6. C2 Server
7. Operator Network with Operator and Tools
8. Logging & Monitoring

Discovery & Control

Goal: *Discover assets and stay in control*

Approach

Living off the Land - Using Built-in Tooling instead of bringing your own. Uses legitimate maintenance tools to explore system configuration

Execution

No custom malware required; used built-in PCOM protocol.

- No custom C2 framework needed
- Focus shifts from network discovery to process discovery
- Uses legitimate maintenance tools to explore system configuration

Tools (Discovery)

- Nmap
- Wireshark
- SCADA System Logs
- ping
- ps
- tasklist

Tools (Control)

- TIA Portal (Siemens)
- RSLogix/Studio 5000 (Rockwell Automation)
- EcoStruxure (Schneider Electric)
- vendor-specific HMI software
- pypcom

Discovery & Control

Challenge: *The challenge for defenders is detecting malicious actors using legitimate protocols and commands that may appear similar to normal maintenance activities.*

Monitoring

- Logging of events

Baselining

- What is normal - what is an anomaly
- In general - logging of events

Network Detection

- Detection of anomalies
- Anomalies can be different protocols/ports/IPs
- Anomalies in failed connections

System Behavior

- Anomalies on failed logons

Threat Intelligence

- Use of TI for detection
- Know the tools, which adversaries could use - build detections for it
- Building Threat Hunting hypothesis

Exploitation & Privilege Escalation ●

Goal: *Acquiring access (to other systems)*

Approach

- Connect to a device (PLC, HMI, ..) from within the network
- Abuse additional vulnerabilities (EternalBlue, CVE-2024-38434, Dirty COW)

Tools

- Metasploit, PrinterBug, KrbRelayUp



Exploitation & Privilege Escalation ●

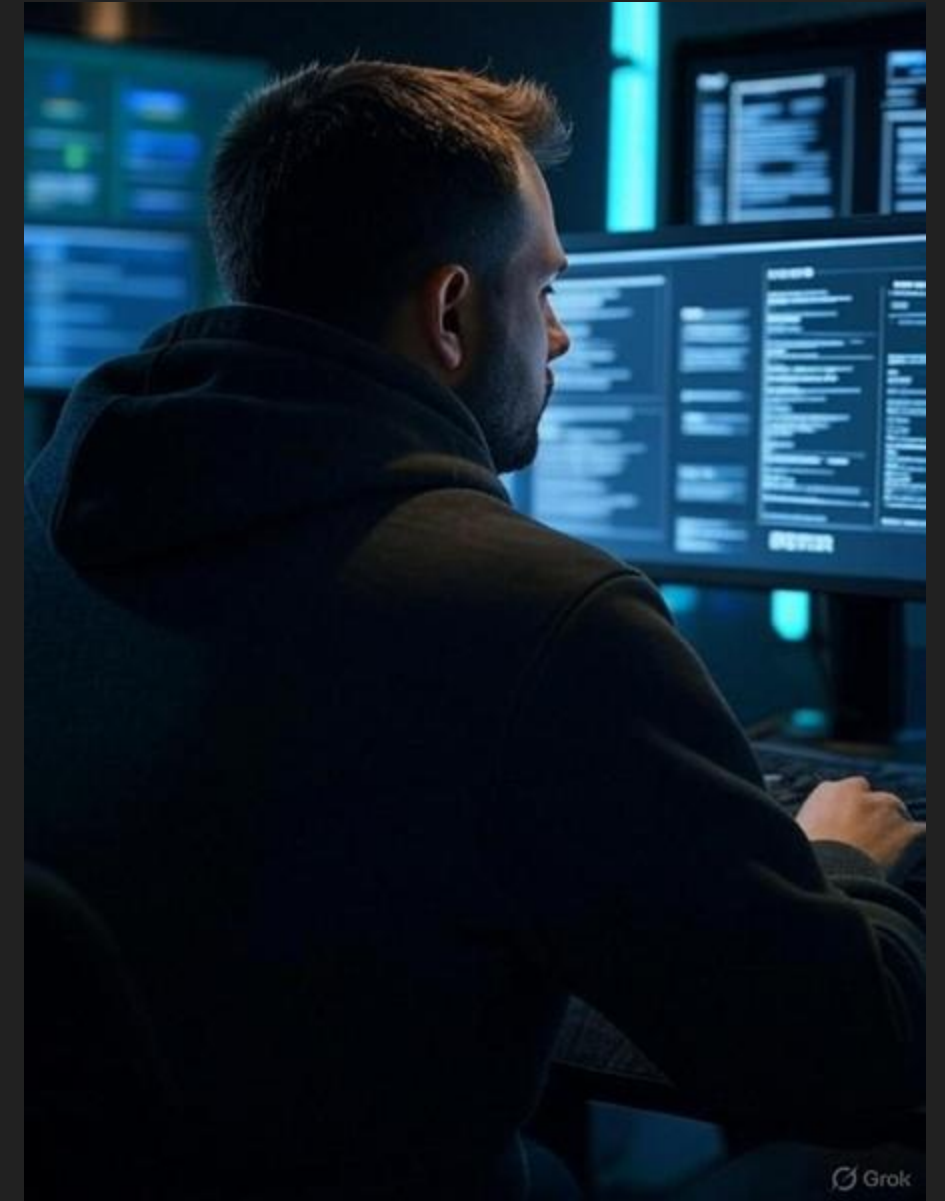
Challenge: Maintaining deep visibility and control in fragile, legacy-rich ICS environments without disrupting critical industrial processes.

Preventions

- Keep systems updated against known CVEs
- System hardening and network segmentation
- Using a suitable AV
- Usage of built-in Exploit Preventions

Detection Engineering

- Detection of anomalies (e.g. child processes of HMI/SCADA applications)
- Alerting on known exploit behavior (shellcode indicators, heap spraying, etc.)
- Threat Intelligence to stay informed of TTPs/CVEs on ICS



Execution

Goal: Interact with the PLC to prepare for the final objective

Approach

- Use the system's own tools against it by connecting with standard engineering software to make traffic appear legitimate

Execution

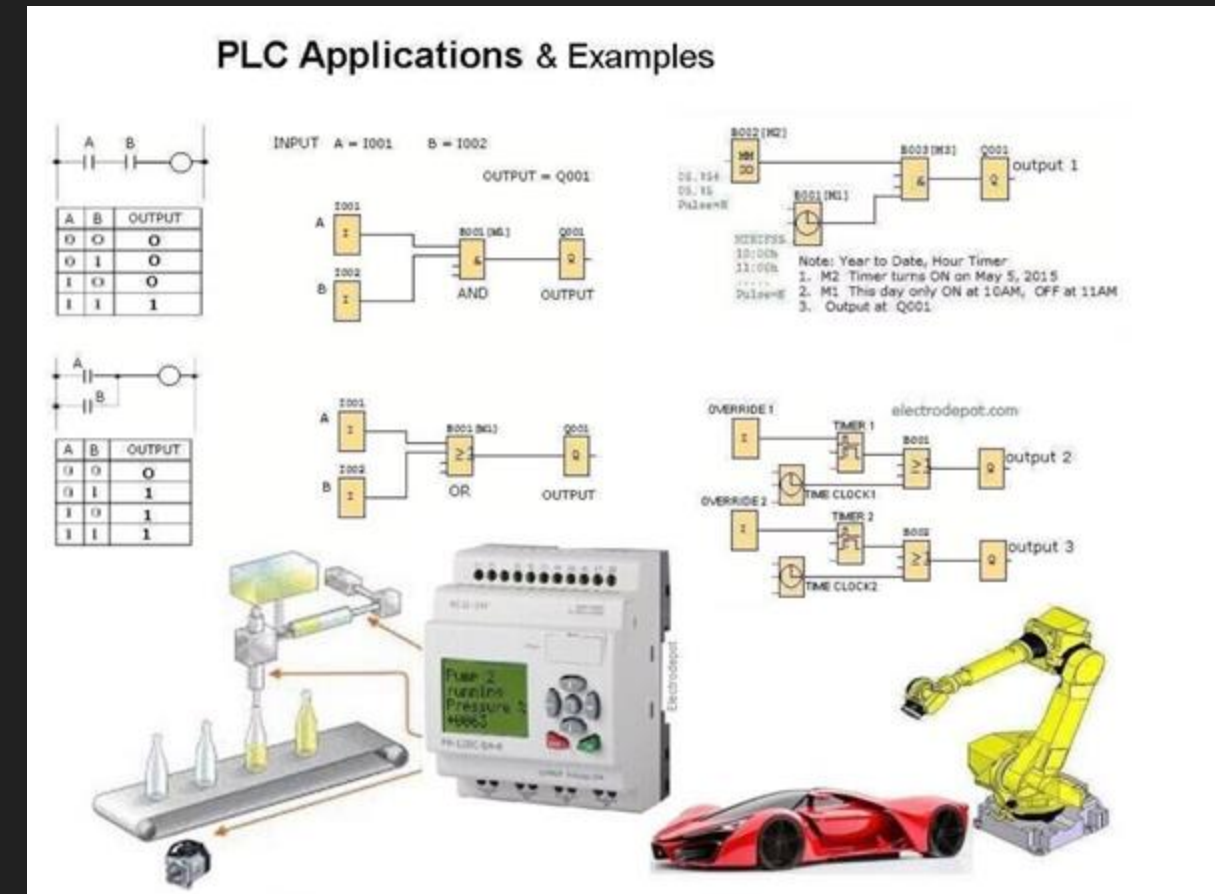
- Read device status, view existing logic, confirm privileges needed to write new programs to the controller

Tools

- Standard Unitratics engineering software (e.g., VisiLogic) to connect over the PCOM protocol

MITRE ATT&CK® (ICS)

- T0845 - Remote Services, T0822 - GUI (Interacting with engineering software)



Execution ●

Challenge: *Distinguishing malicious commands from legitimate operational activity*

Detection of Malicious Code Executions

- Monitoring of unexpected executables and command lines
- Strict monitoring of engineering systems, which are connected to ICS systems

Monitoring for PLC Logic Changes

- Detection when relevant logic is altered

Lateral Command Execution

- Log remote session creation
- Alert on inter-station RDP, PsExec, or WinRM usage in ICS zones (often unnecessary and highly abnormal)

Malware Execution Prevention

- Endpoint protection with ICS awareness



“The blue team must detect and prevent unauthorized or abnormal code, script, or logic execution on ICS assets - especially where it could enable control system manipulation or persistence”

Action on Objectives

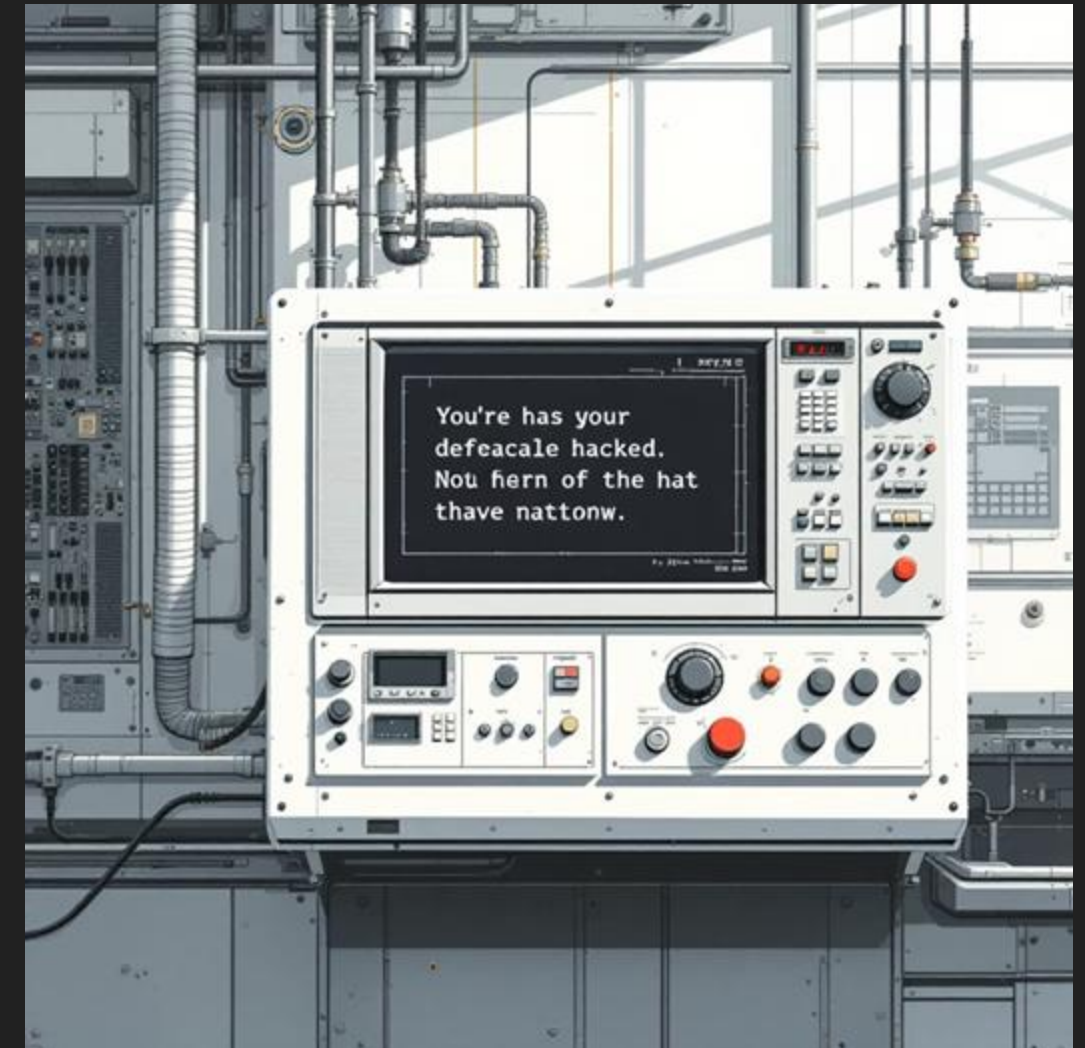
Goal: *Demonstrate Impact through Disruption*

Approach

- HMI Defacement: Overwrite operator screens with propaganda message
- Operational Disruption: Download malicious ladder logic to stop the PLC
- Prevent Recovery: Rename device, change communication ports, disable upload/download functions

MITRE ATT&CK® (ICS)

- T0829 - Loss of View (downgrade, intercept communication)
- T0814 - Denial of Service (shutdown, delete data)
- T0836 - Modify Parameter (manipulate data)



The primary goal was psychological impact through visible disruption rather than covert sabotage of the physical process.

Action on Objectives

Challenge: Detecting and stopping rapid, potentially irreversible process manipulations in fragile, time-critical environments with limited security controls.

Isolation of affected devices

Protocol-Aware Detection

- Needed to spot logic changes, config changes, port alterations

File Integrity Monitoring

- Configuration file changes/defacements

Segmentation and ACLs

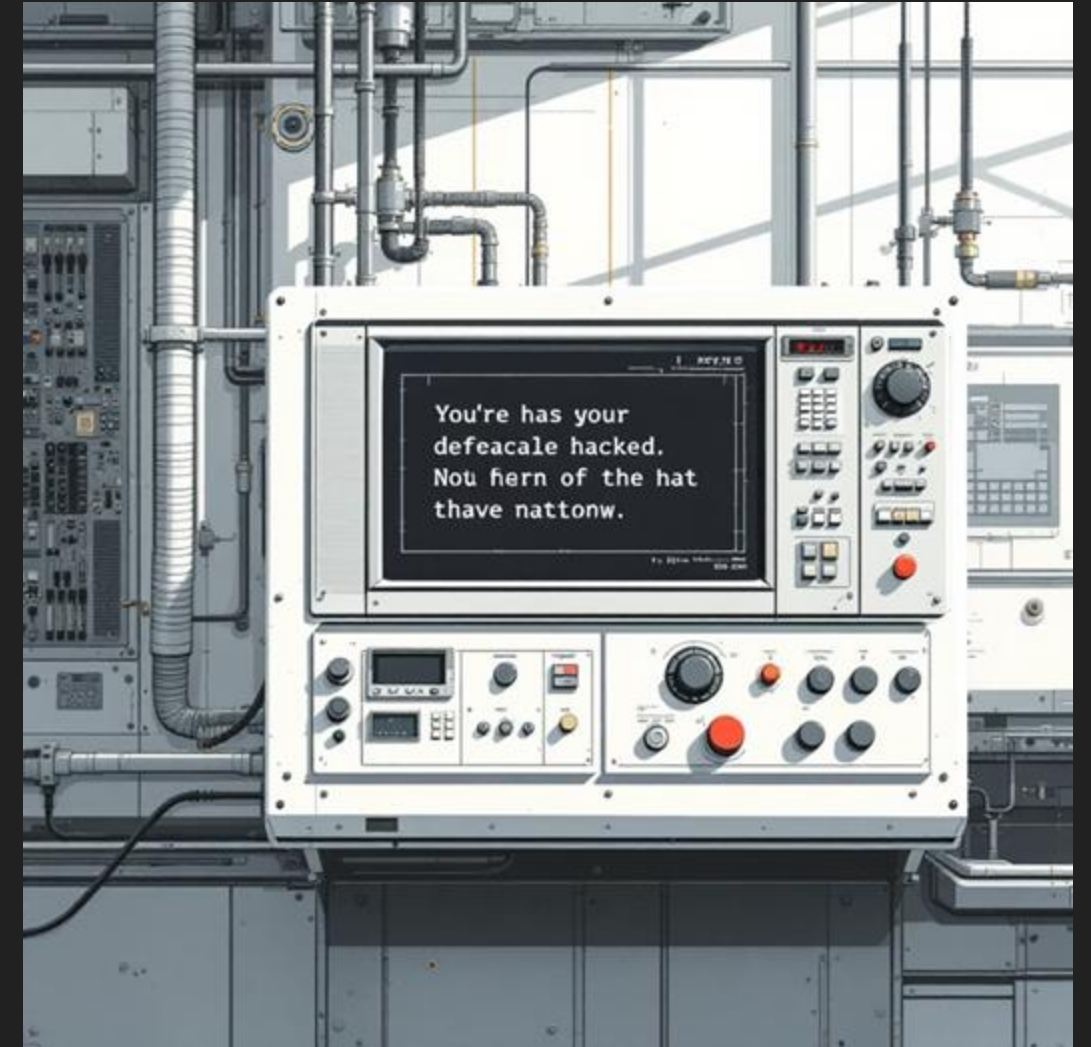
- Limit who/what can talk to PLCs and HMIs

Backups + Offline Images

- Rapid restore after logic manipulation or anti-recovery tactics

Access Control Auditing

- Who has write permission to PLCs, HMI files, configuration settings



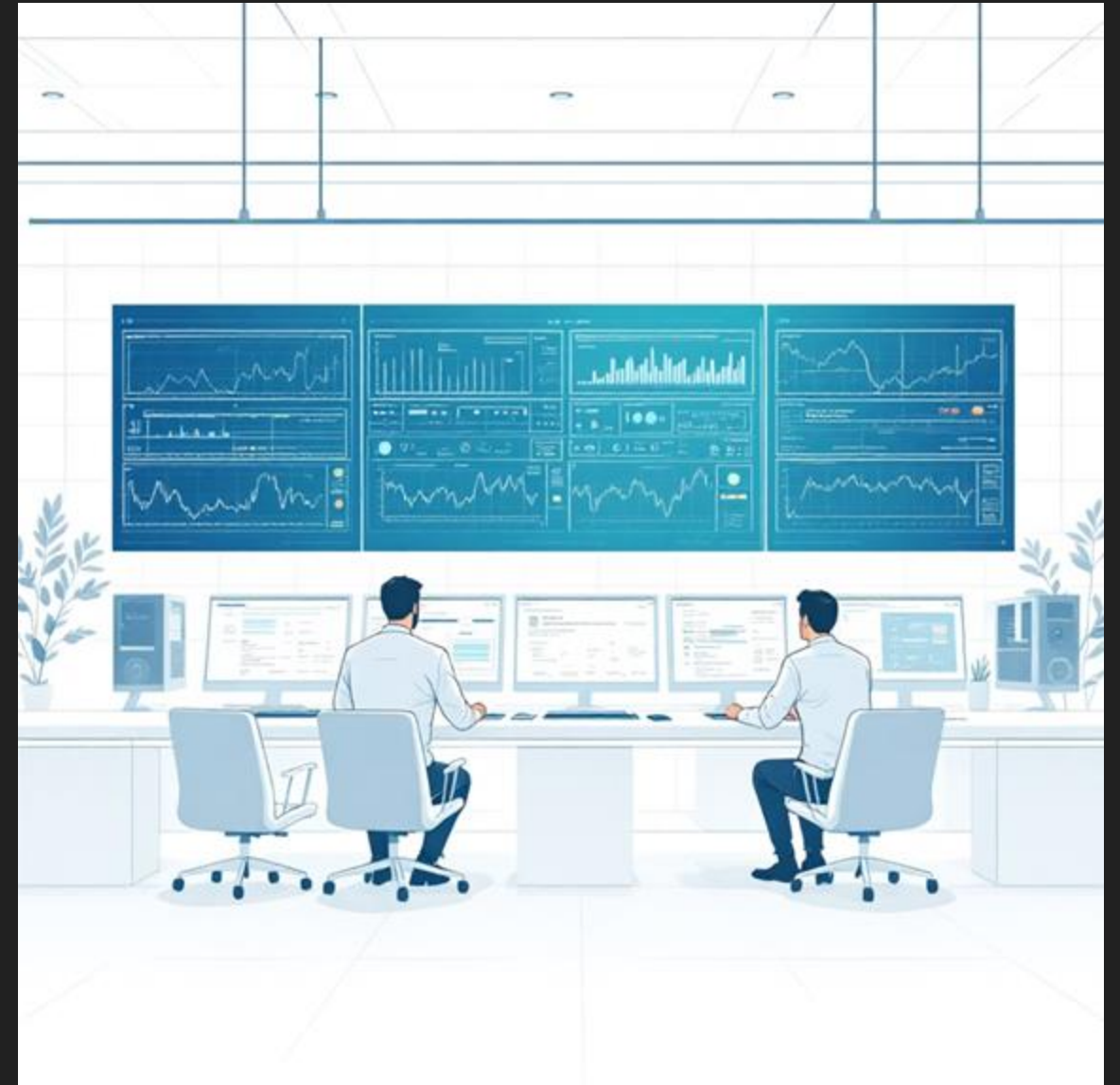
Post-Attack ●

APT Publicization

- Screenshots shared via Telegram channel
- Political statements accompanying technical proof
- Media coverage amplifies relatively small technical impact

Blue Team Intelligence Sharing

- Detailed forensic analysis using specialized OT tools
- Reporting to CISA and relevant ISAOs
- Uncovering new vulnerabilities (CVE-2024-38434)



Post-Attack ●

Impact Assessment

- What is really touched vs. what is claimed
- Rapid internal and external communication: fact-based, non-speculative
- Anticipate board-level and public questions even if impact is minimal

Forensic Investigation and Technical Recovery

- Collect volatile data from PLCs and compare logic blocks to backups
- Clean containment and recover of affected systems

Intel Sharing & Coordination

- Share sanitized IOCs, TTPs, and malware samples
- Watch for coordinated follow-on attacks based on shared TTPs

Vulnerability Discovery

- Submit new CVEs or notify vendors
- Patch internally and update hardening guides
- Share learnings across the ICS security community



● Thank you for your attention ●

