

# SCADAsploit C2.0T

## How to break an ICS system

**Speaker:** Omar Morando “segfaultx00”

# \$ whoami



```
omar@hackinbo $ nmap --script enum_nerd omarmorando.com
```

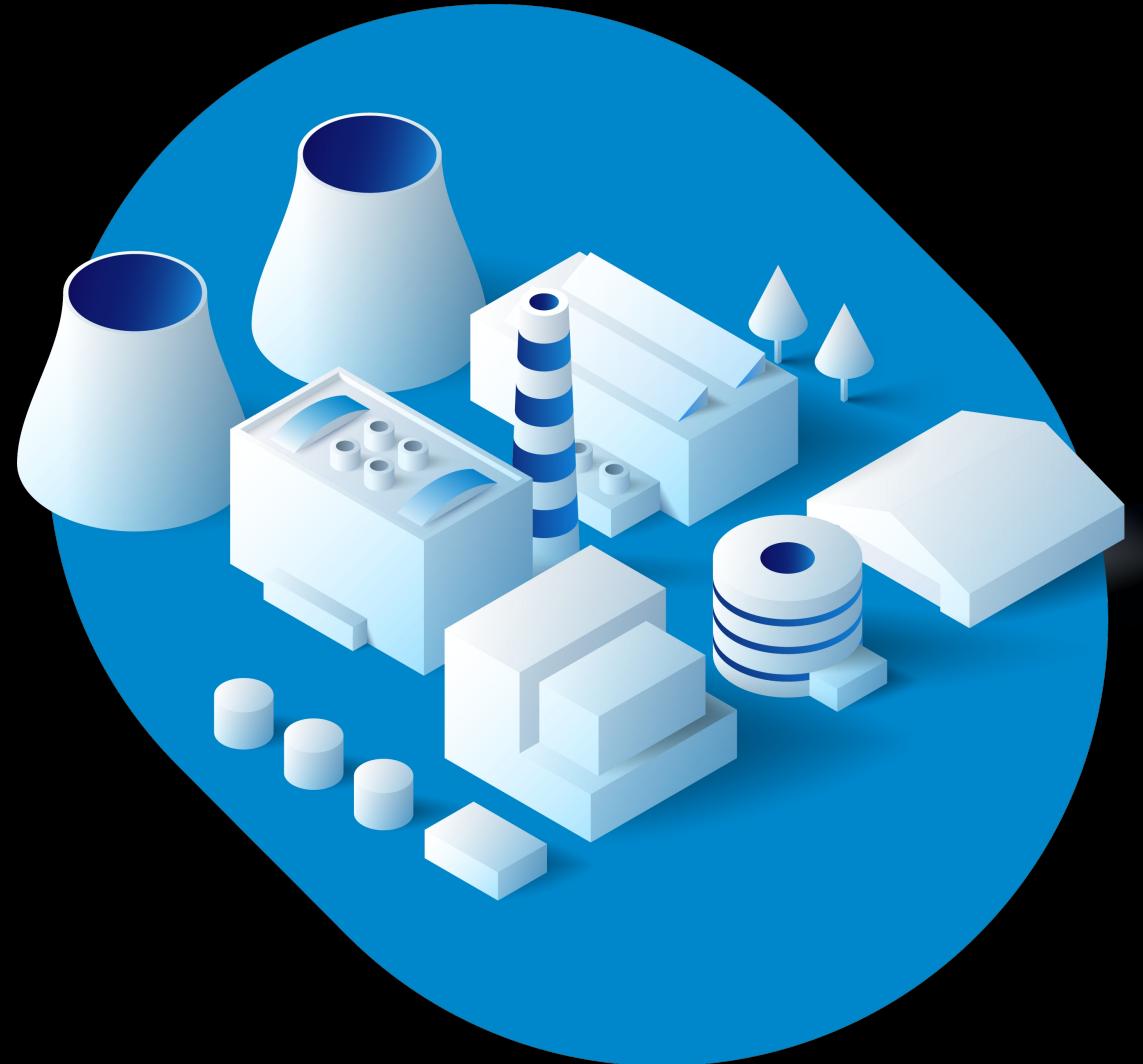
```
-----  
[*] Scanning host...  
[+] Penetration tester, OT specialist  
[+] Developer of SCADAsploit, a C2 framework for OT systems  
[+] 20+ years in Industrial Automation (SCADA, PLC, remote I/O, fieldbus)  
[+] Speaker at HackInBo W22, BSides, BlackHat Europe, SANS ICS Summit, more  
  
[+] Current job: Head of OT Cybersecurity | SCADAsploit Team Leader  
[+] Company: HWG Sababa  
  
[*] Found email: omar.morando@scadasploit.dev  
[*] Found website: https://omarmorando.com  
[*] Found twitter: @OmarMorando  
[*] Found linkedin: https://www.linkedin.com/in/omorando/
```

Nmap done: 1 IP address (1 host up) scanned in 2.35 seconds



# Why Operational Technology (OT) cybersecurity?

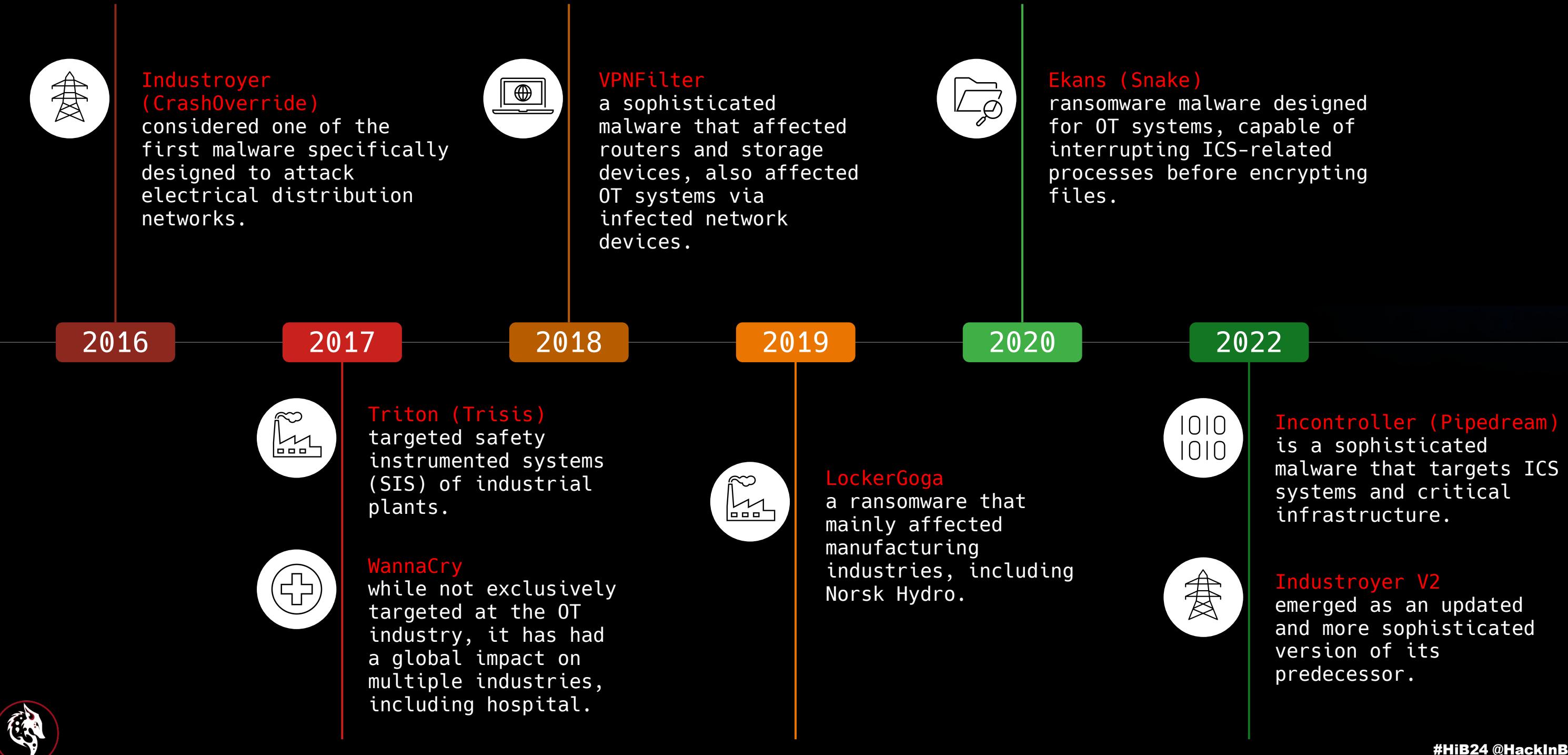
- ICS has become an easier target for APTs!
- **Goal?** Economic stability and national security. Human and environmental safety.
- **Which target?** Energy, transport, telecommunications, water treatment and manufacturing sectors.



# It's not just...



# The scenario continues to worsen



# What's in an ICS System



## Sensors & Actuators

they carry out measurements of physical quantities and act directly in the production chain.



## Microcontrollers or PLC

they get data from the sensors, operate the actuators, communicate with other devices (e.g. PLC, HMI, SCADA, data logger).



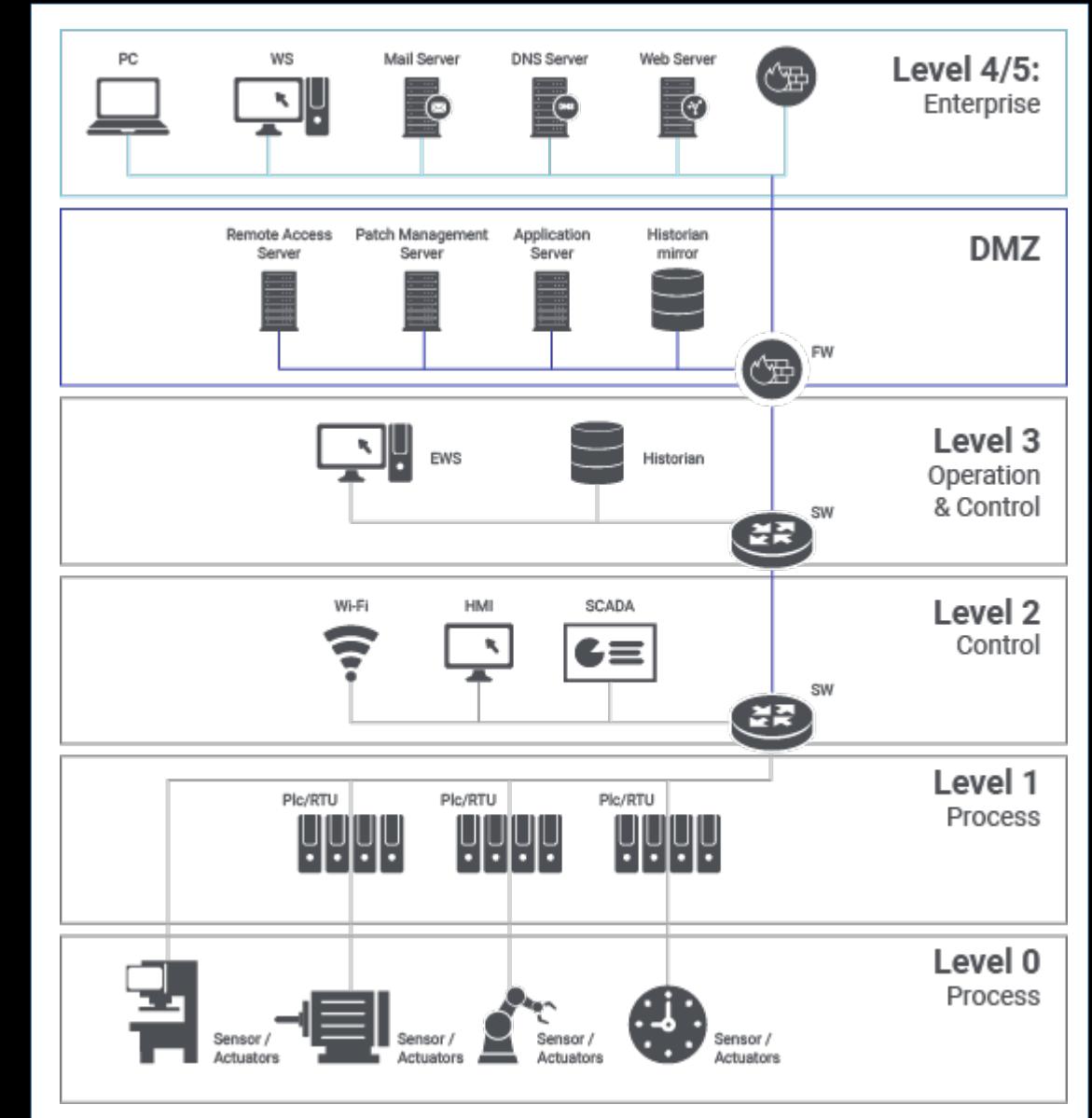
## HMI

it communicates with the local PLC and allows the operator to view and enter data and commands.



## SCADA

it collects data from the various PLCs, processes them, stores it on databases, manages the representation of alarms, displays the process via graphic synoptic.



# What is a PLC

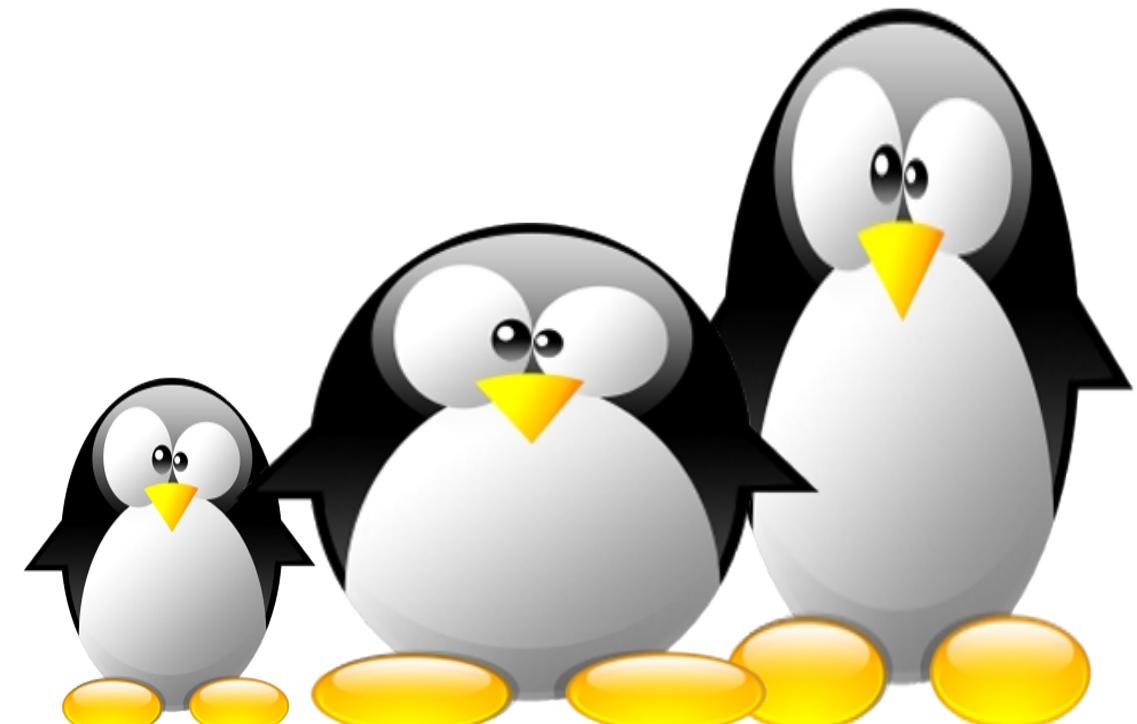
- They obtain data from sensors
- Run the installed program
- Operate the actuators
- Communicate with other devices



# What's inside a PLC



# What's inside a PLC



embedded Linux



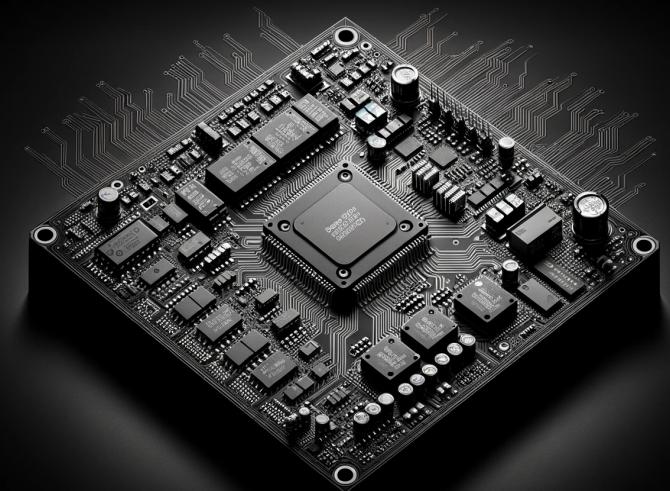
# What's inside a PLC

Vendor	OS
Allen-Bradley PLC5	Microware OS-9
B&R	VxWorks
Rockwell ControlLogix	VxWorks
Schneider Modicon M340-M580	UnityOS
Schneider Modicon Quantum	VxWorks
Siemens S7-1200/1500	Adonis OS
Siemens Simatic WinAC	Windows RT
Wago 750	Linux RT



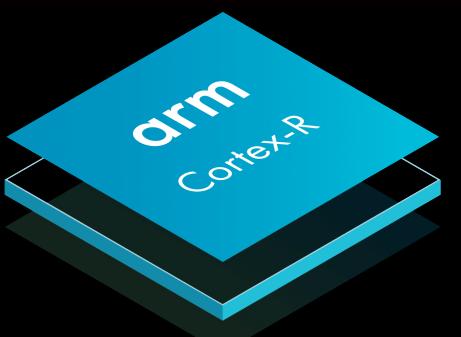
# It's an embedded system, so...

- Same approach to a "normal" embedded system.
- Possible RCE (Remote Code Execution) attacks.
- Attacks on the integrated webserver, using techniques known from the IT world.
- Vulnerabilities on exposed services and OS.
- Hardware attacks on secure boot, peripherals (UART, JTAG, NAND, I2C, Fault Injection, more).



# Siemens S7-1200 V4

- Siemens A5E30235063 ARM Cortex-R4 (Big-Endian).
- The ARM Cortex-R4 processor is a mid-range CPU for embedded applications, automotive, imaging, mass storage/HDD and industrial microcontrollers.
- This is a range of processors that offers the balance between low-cost performance and power.
- High-performance solution for real-time applications.



# Siemens Adonis RTOS

Adonis Linux-Based  
Kernel

## ADONIS Library OS Services

S7P File Services		Dinkumware C/C++ Lib v5.01
PDC FS	EFS/NTFS	NicheStack IPV4/SNMP
Some Low-Level Configuration (eg. MPU Reconfiguration)		Siemens MiniWeb Server & MWSL Parser, OpenSSL
ACE 6.3 for S7P Components Adaptive Communication Environment	Log/Diag System	

## Automation-related Services

AWP Automated Web Programming		PNIO ProfiNet
MC7P Parser	MC7P RunTime	MC7P Compiler
Siemens OMS		
Central IO Subsystem	OMS SP Parser	OMS Configuration
ALARM Subsystem		OMS FAT



# Siemens Adonis WebServer

The screenshot shows the Siemens Adonis WebServer interface for a SIMATIC S7-1200 station. The top navigation bar includes a 'Menu' button, a tab for 'S7-1200 station\_1', and a search bar with the URL '192.168.0.1/Portal/Portal.mwsl'. The main header displays 'SIEMENS' and 'S7-1200 station\_1/PLC\_1'. On the left, a sidebar menu lists options like 'Start Page', 'Identification', 'Diagnostic Buffer', 'Module Information', 'Communication', 'Variable Status', 'Data Logs', 'User Pages', 'Update Firmware', and 'Introduction'. The user is logged in as 'admin'. The central content area shows a summary of the PLC configuration and its current status. A large image of the SIMATIC S7-1200 module is displayed, showing the model number 'CPU 1214C DC/DC/DC' and the LED status indicators (RUN, STOP, ERROR, MANT). To the right, detailed information is provided under 'General' and 'Status' sections.

**General:**

- Station name: S7-1200 station\_1
- Module name: PLC\_1
- Module type: CPU 1214C DCDCDC
- IP Address: 192.168.0.1

**Status:**

- Operating Mode: RUN
- Status: ✓ OK

[Flash LEDs](#)   [Go to RUN](#)   [Go to STOP](#)



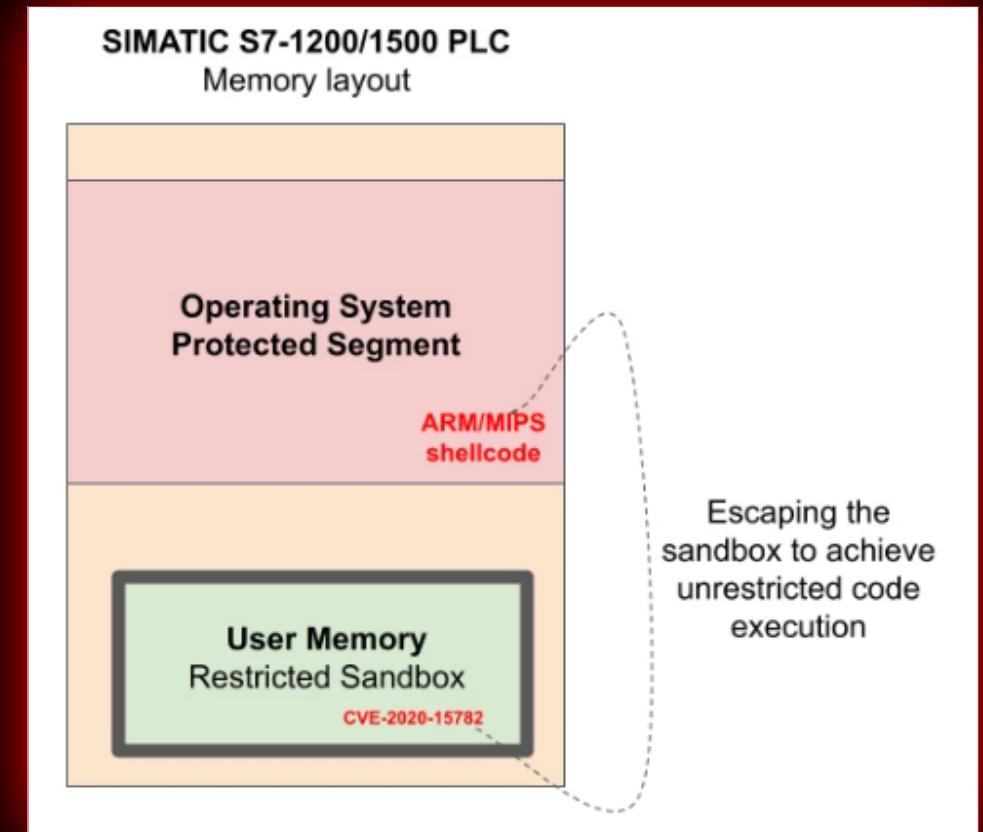
# Siemens Adonis WebServer

HTTP GET Request Handler	Description
/appapiappa/vvvvvvvvvv	version
/appapiappa/vvvvvvvvvvvv	version
/appapiappa/lilililili	log in
/appapiappa/lololololo	log out
/appapiappa/cmcmcmcmcmc	change CPU mode
/appapiappa/flflflflfl	flash LEDs
/appapiappa/gbpigbpigb	get station info as json (name, mac, mode)
/appapiappa/gmigmigmig	get module info (list): get name, serial, FW version, HW version, status
/appapiappa/galegalega	unknown
/appapiappa/galedgale	get AS log entry
/appapiappa/gvigvigvig	unknown
/appapiappa/svsvsvsvs	unknown



# Siemens Adonis Sandbox Escape

- These complex system has protections in memory that are supposed to prevent the execution of malicious code.
- The operating system "locks" user code in a **sandbox** with limited access to resources, memory, and functionality.
- The **CVE-2020-15782** vulnerability bypasses existing protections within the PLC execution environment.



# Why a C2 for OT?



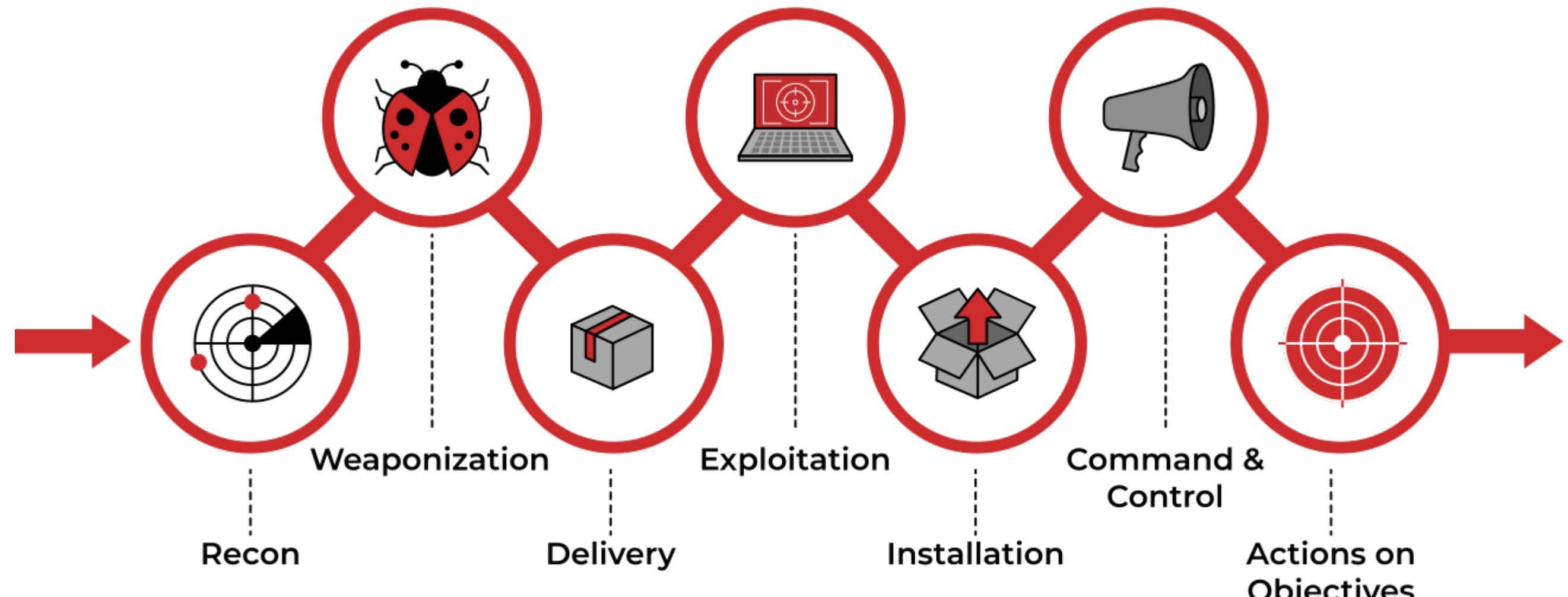
# Adversary Simulation

## Some Key Points

- It seeks to emulate the **actions and tactics** (TTP) of a specific APT.
- Test your security against **real-world attacks** (e.g. MITRE ATT&CK for ICS).
- This approach allow you to **better prepare** against specific threat actors (e.g. in Critical Infrastructures).



# Adversary Simulation



Lockheed Martin, the Cyber Kill Chain



# Adversary Simulation in OT/ICS

## Some Key Benefits

- Identification of Weaknesses: unnoticed in traditional assessments.
- Realistic Threat Scenarios: find real potential attack vectors.
- Response Evaluation: evaluate SOC and incident response plan in OT.
- Risk Mitigation: implement targeted security measures.
- Compliance Assurance: demonstrate compliance with ICS standards.



# We need dedicated tools

## OT has unique characteristics

- It uses **custom technology** that requires a different approach than IT.
- It often relies on **proprietary systems** and **protocols**.
- It is exposed to **typical vulnerabilities** that are not present in the IT world.
- Requires, for operational needs, greater exposure.



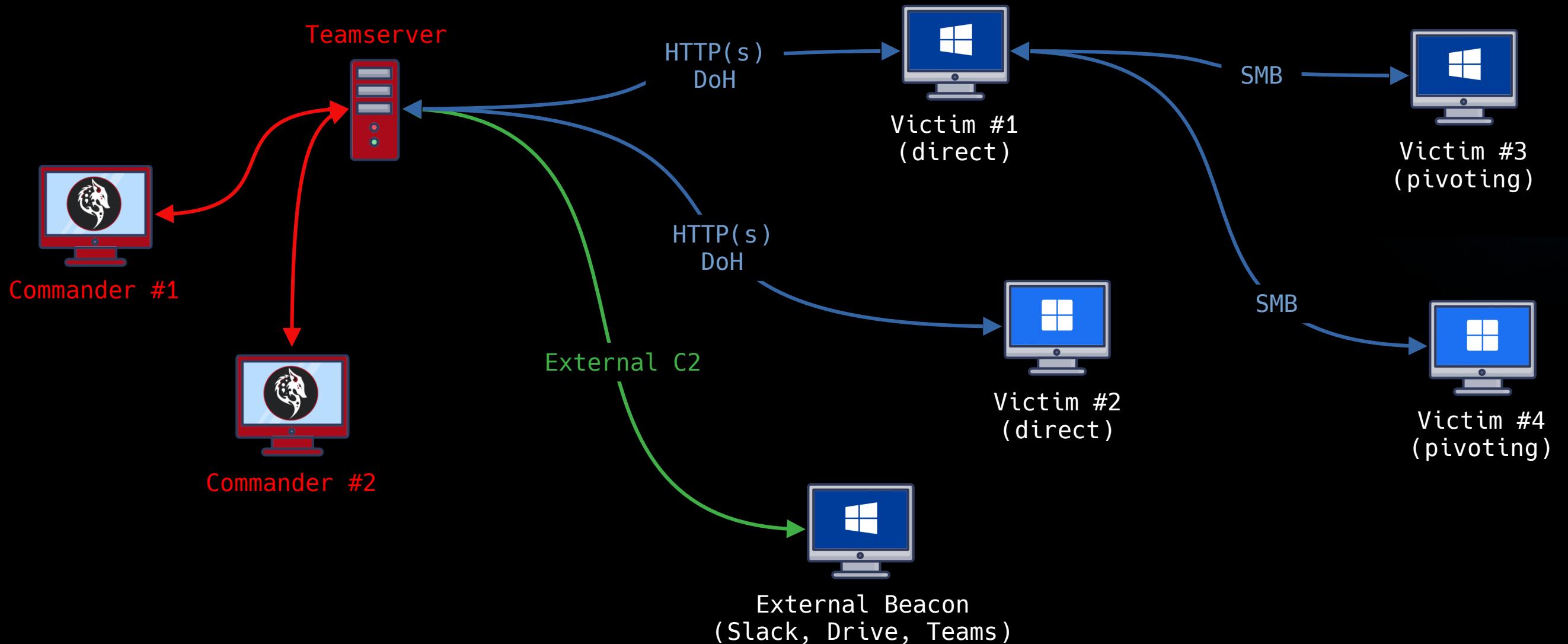
# SCADAexploit C2.OT

- Post-exploitation vs Siemens, Schneider Electric, Rockwell, ABB, others.
- EDR evasion, AMSI/ETW bypass, anti-sandboxing, anti-debugging.
- Process injection capabilities via WinAPI, NTAPI, Indirect Syscalls, more.
- Multiple pivoting techniques: SMB, TCP, remote services via RPC.
- Stageless and staged beacons, with sophisticated obfuscation techniques.
- Expandable using payloads in BOF/COFF format.
- A powerful Remote Commander, enabling smooth server and module interaction.
- Support for ARM SoC platforms (e.g. Raspberry) for “stealth” installations.

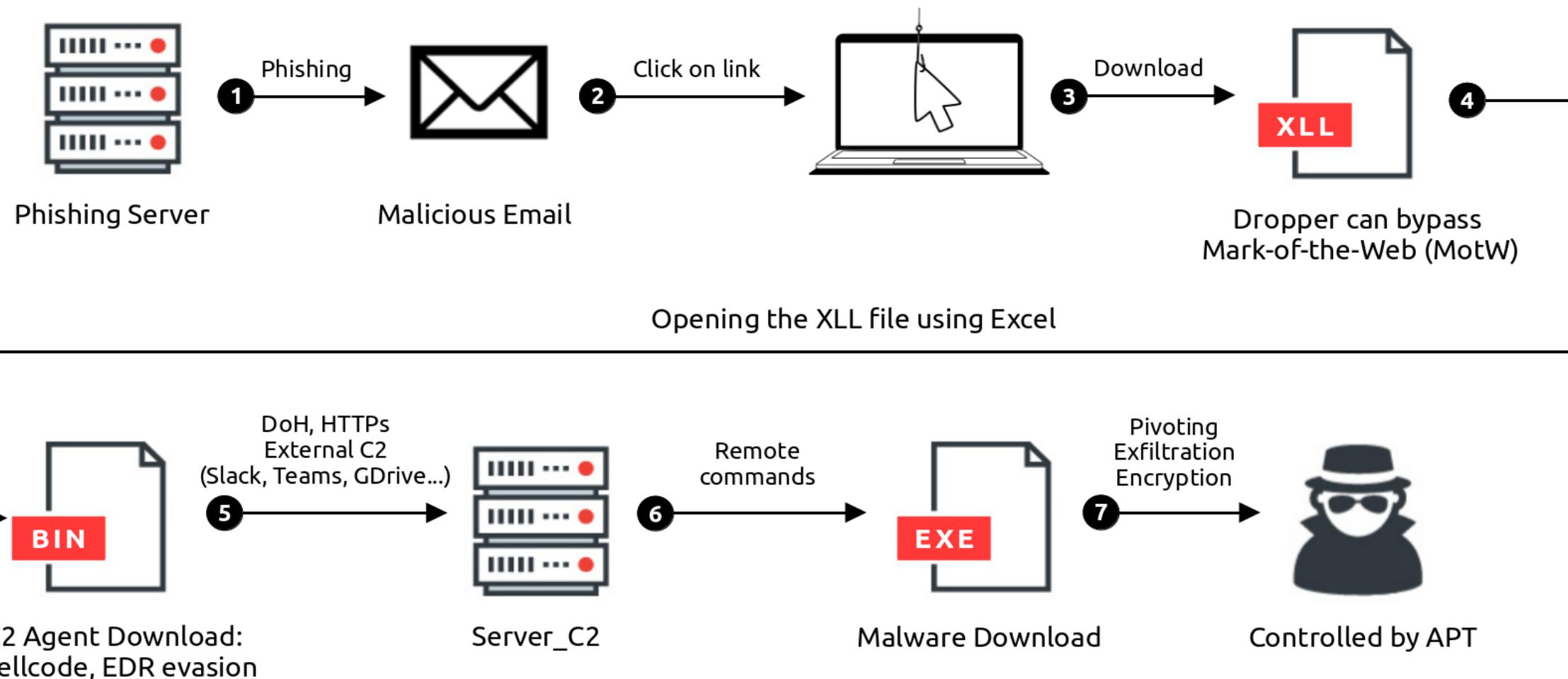
**It's a game-changing OT Framework!**



# How a C2 works



# Basic C2 Path Attack



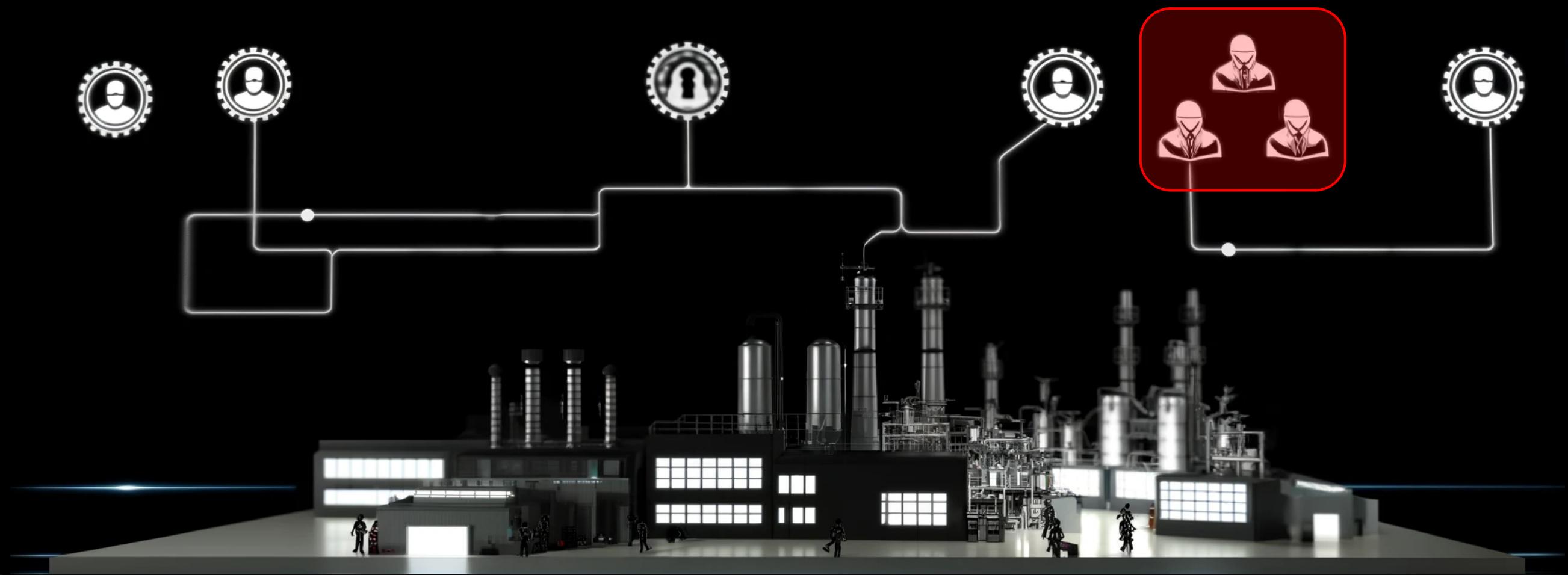
# The Dropper file

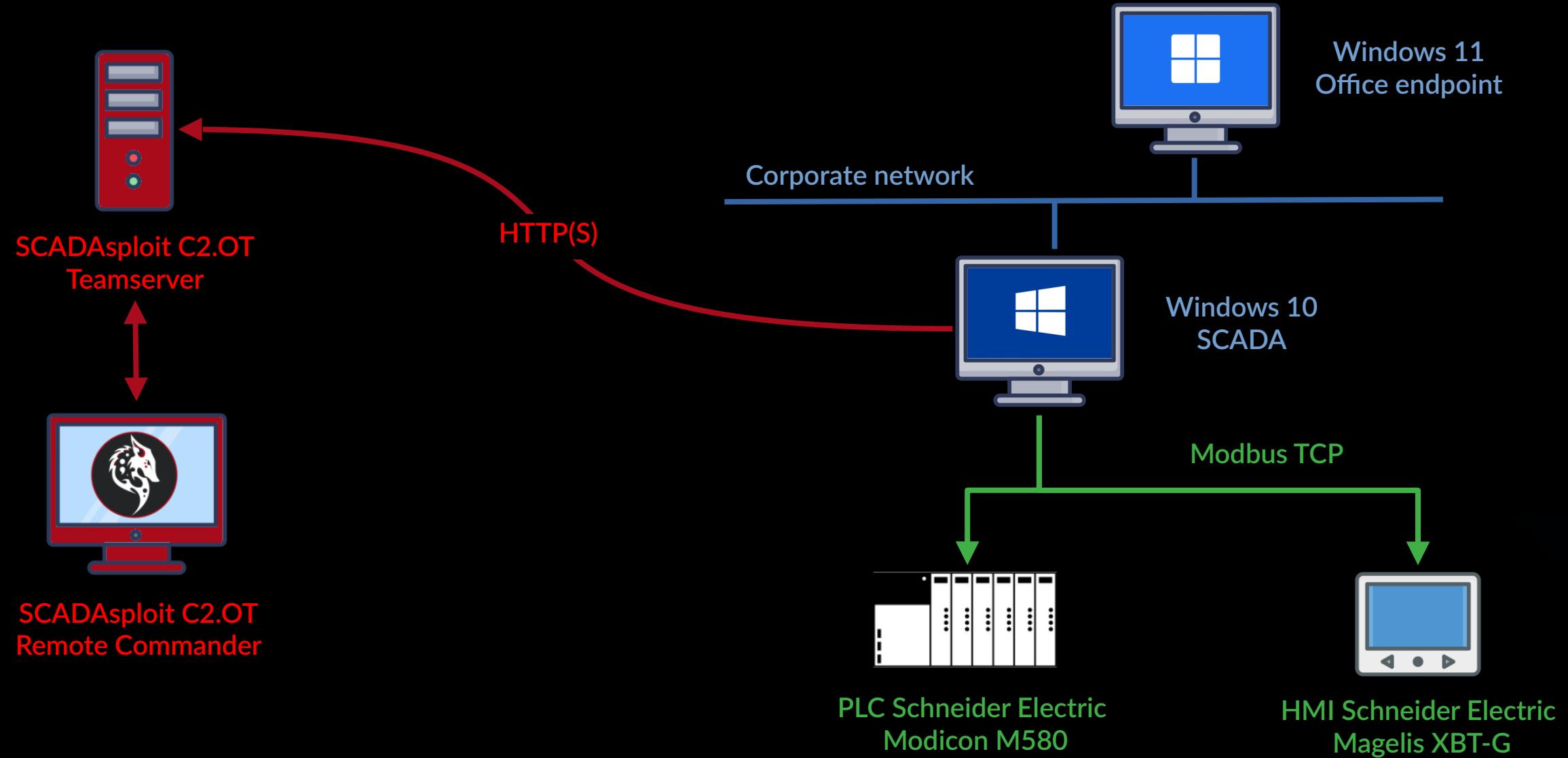
- **File-based Droppers**: disguised as benign entities such as software setup programs or tool.
- **Documents-based Droppers**: they manipulate weaknesses within document formats including PDFs and Microsoft Office files (eg XLL).
- **USB-based Droppers**: known as "USB droppers" or "USB worms," the infection chain is triggered when it is inserted into the PC.
- **Web-script Droppers**: focusing on exploiting vulnerabilities in web browsers, or plugins. When the user visits a compromised site, the dropper exploits this vulnerabilities and introduce malware.

**pdf, office, exe, html, js/vbs, zip/rar, iso, lnk, bat/ps**



# Demo





## The Big Disclaimer!

Activities to be performed in a test environment, laboratory  
or during a plant shutdown for maintenance (I know...)



# Make it safe!

## Organizational measures

- Security Assessment, Risk Assessment, BIA
- Awareness, OT Security Training
- Policies & Procedures

## Technical measures

- Asset Inventory & Vulnerability Scanning
- Network segmentation & monitoring
- Endpoint protection & hardening
- Patching (where is possible), backups, recovery plan
- Secure remote access, Supplier Management
- Secure PLC Programming



# Takeaways

- Awareness of OT cybersecurity and risks.
- Importance of validating the safety posture, really!
- Knowledge of a very effective tool for Red Teaming IT and OT, in a single framework.
- Don't believe anything or anyone.

**Take care of the cyber security of your OT system,  
because if you don't do it someone else will.**



# Thanks



@0magMorando



omar.morando@scadasploit.dev



<https://scadasploit.dev>

