SCADAsploit C2.OT

How to break an ICS system

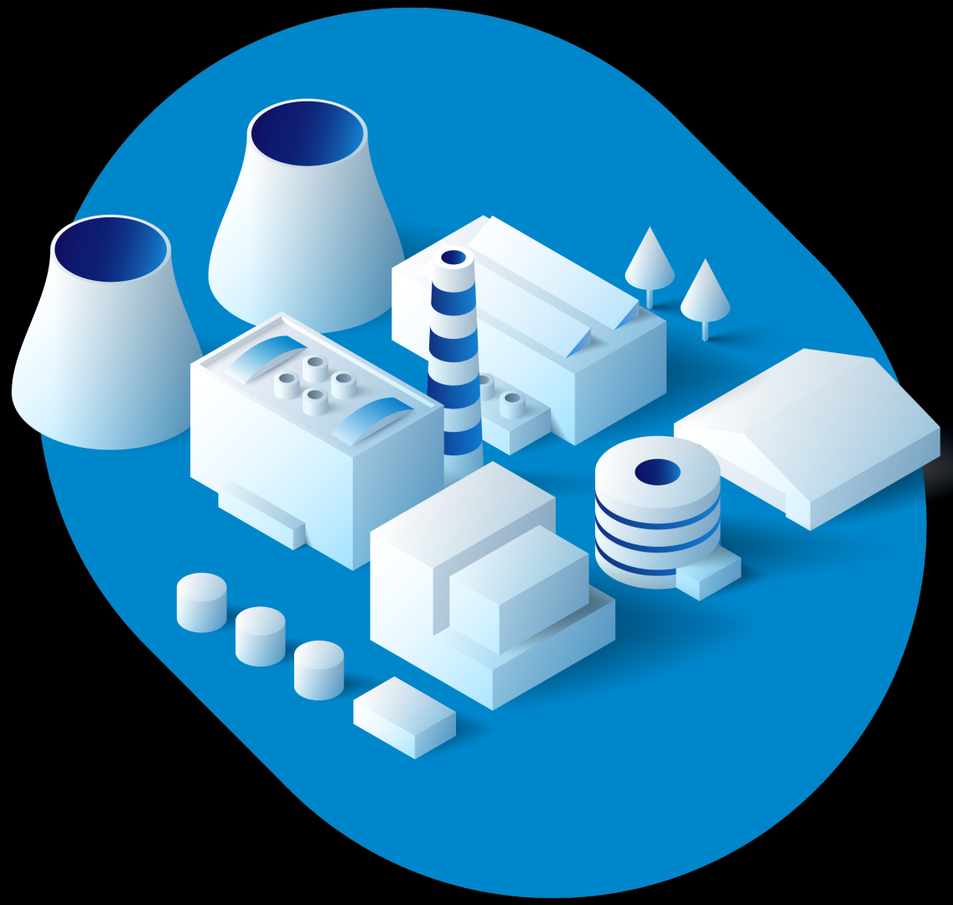
Speaker: Omar Morando “segfaultx00”

$ whoami

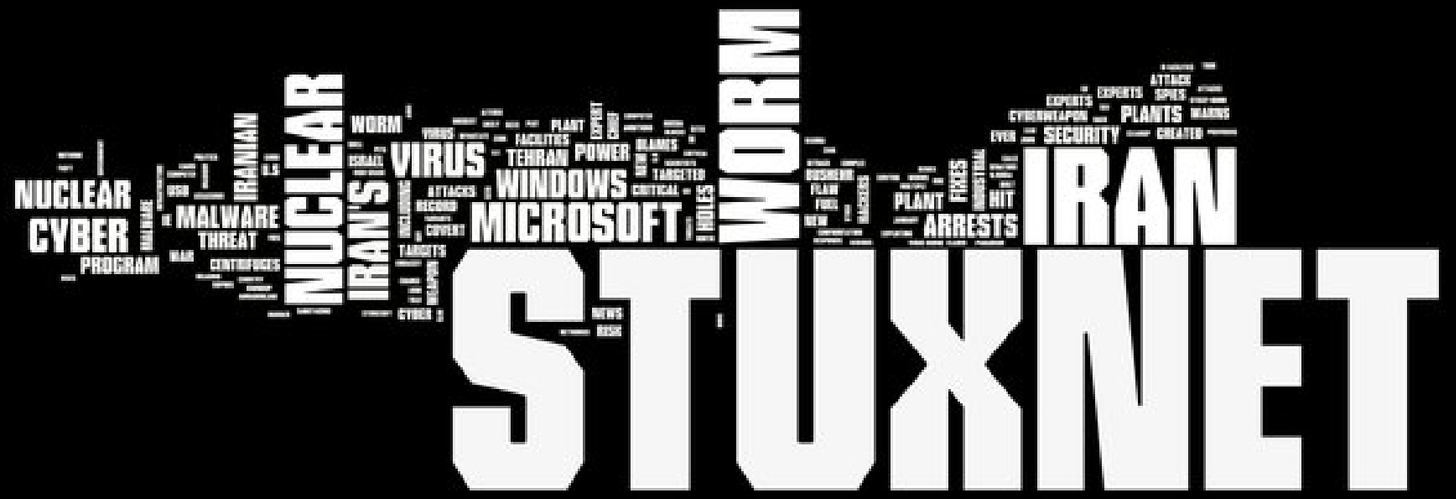
```
omar@bsides $ nmap --script enum_nerd omarmorando.com
-------------------------------------------------------------------------
[*] Scanning host...
[+] Penetration tester, OT specialist
[+] Developer of SCADAsploit, a C2 framework for OT systems
[+] 20+ years in Industrial Automation (SCADA, PLC, remote I/O, fieldbus)
[+] Speaker at 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

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...


STUXNET
WORM
IRAN
NUCLEAR
CYBER
PROGRAM
MALWARE
THREAT
IRANIAN
IRAN'S
VIRUS
WORM
MICROSOFT
WINDOWS
TEHRAN
POWER
PLANT
SECURITY
PLANTS
ARRESTS
EXPERTS
ATTACK
SPIES
CYBERWEAPON
FIXES
HIT
CENTRIFUGES
TARGETS
COVERT
ATTACKS
CRITICAL
FACILITIES
NEWS

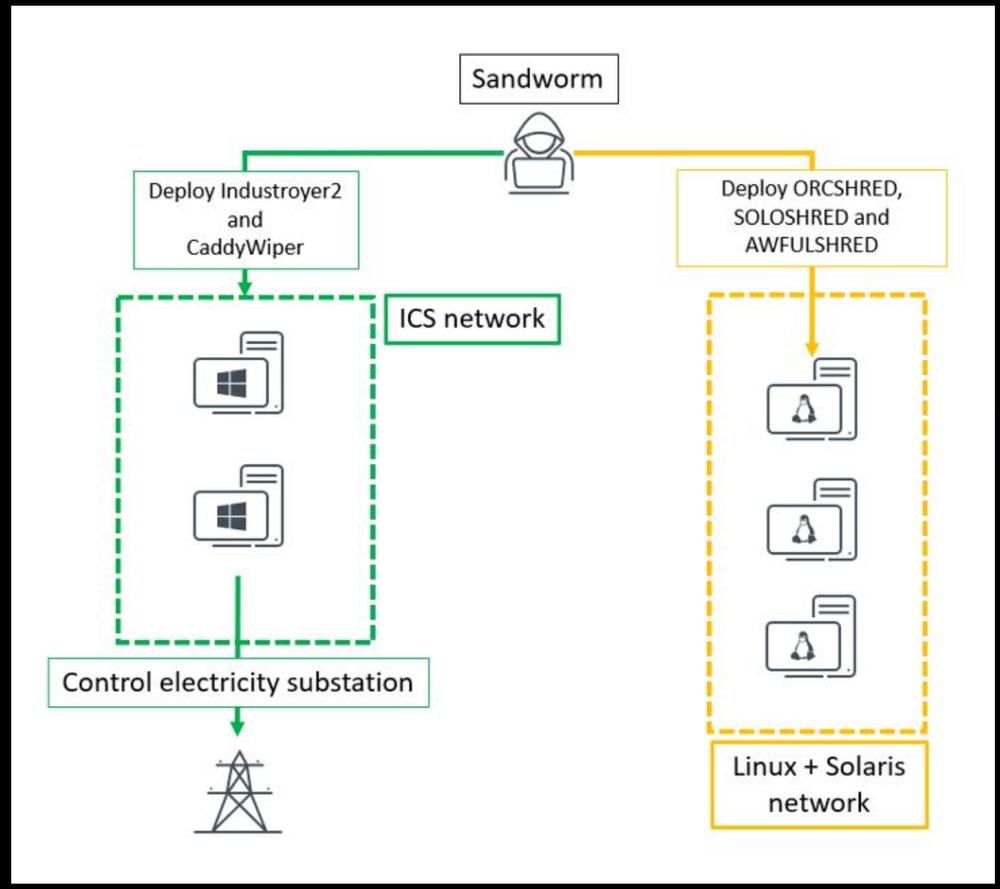
Industroyer

Industroyer is a malware by Sandworm APT for critical electrical distribution infrastructures.

- First attack 12/2016 against power plants in Ukraine.
- It takes control of switches of the electrical substations and of the automatic protection relays.
- It uses IEC 60870-5-101, IEC 60870-5-104, IEC 61850 and OPC DA protocols also found in transportation control, water and gas, critical manufacturing.

Industroyer.V2 new variant dated 04/2022.

- It is autonomous, simplifies the implementation of the attack with better identification of targets.

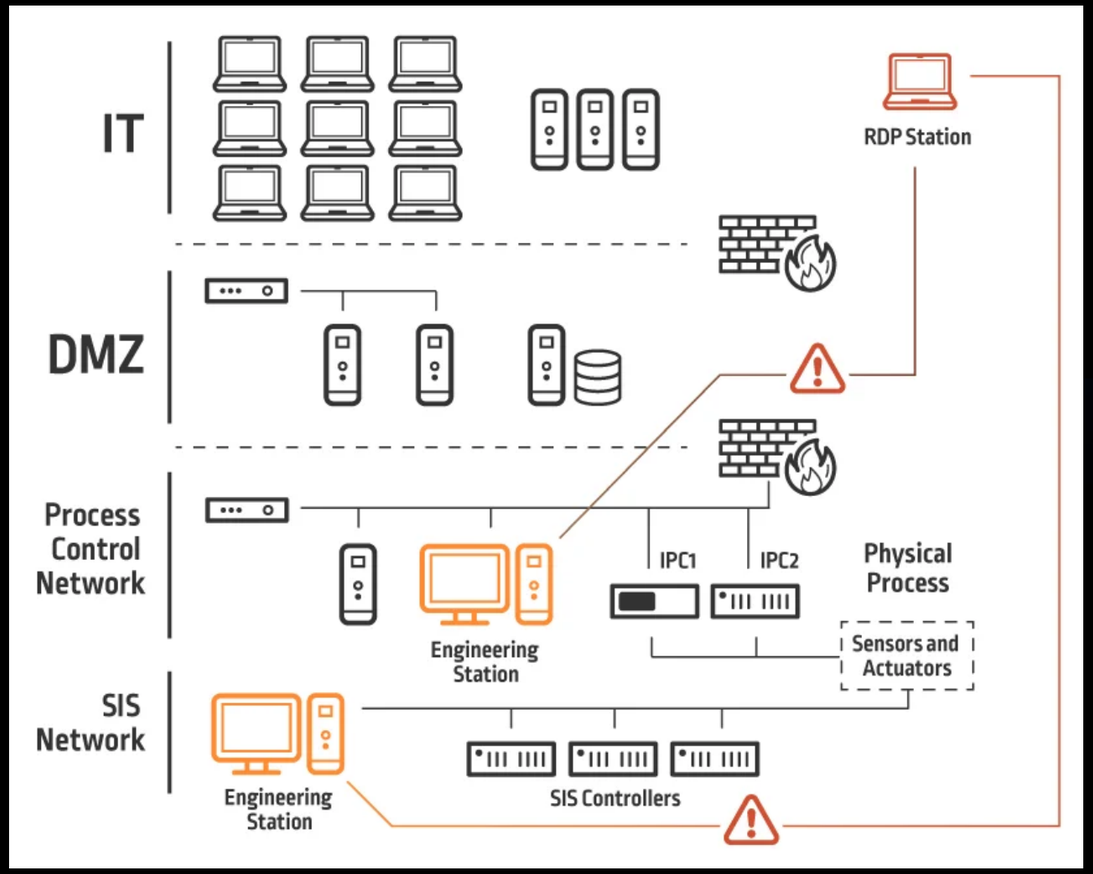


Industroyer.V2 reloaded

Triton

Triton is a malware to specifically attack Triconex Safety Instrumented System (SIS) controllers for emergency shutdown in industrial processes.

- It can prevent the emergency from being activated with even catastrophic consequences.
- The attackers gain control of the Engineering Station SIS.



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

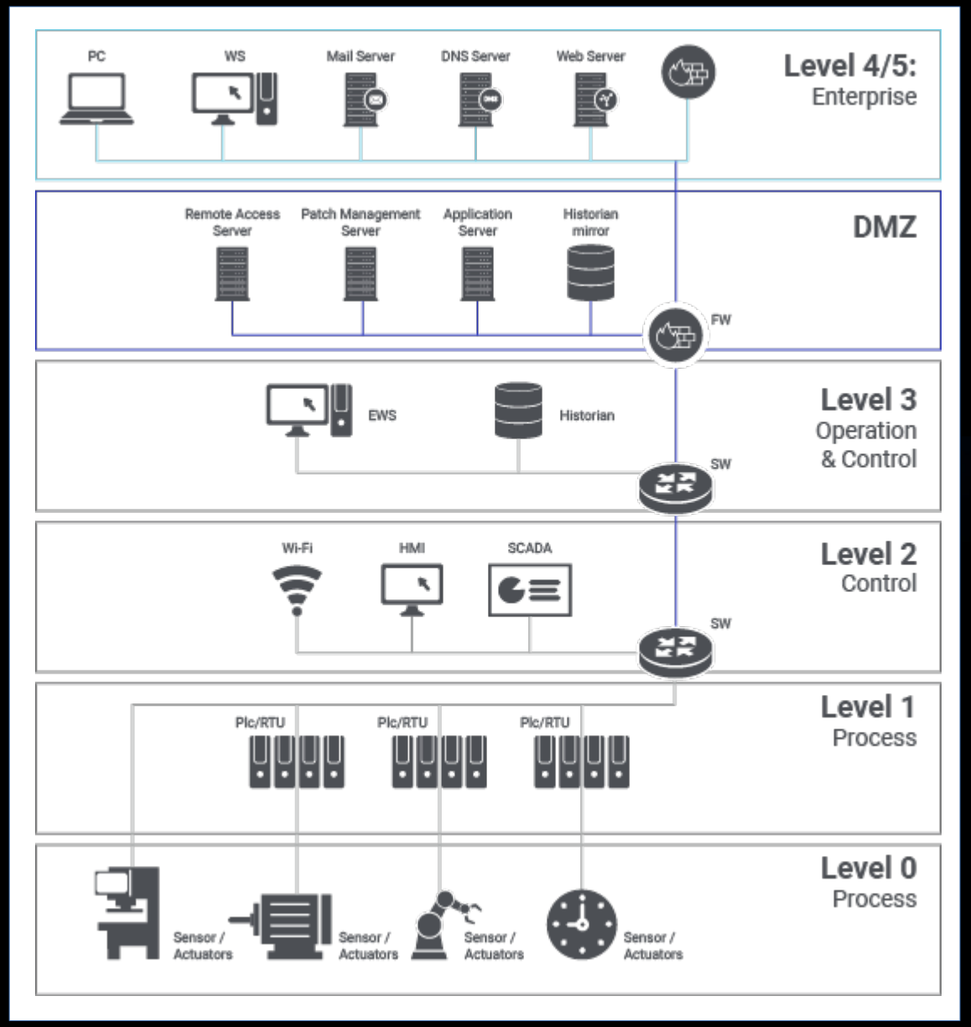
they get data from the sensors, operate the actuators, communicate with other devices (e.g. PLC, HMI, SCADA, data logger).

HMI

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

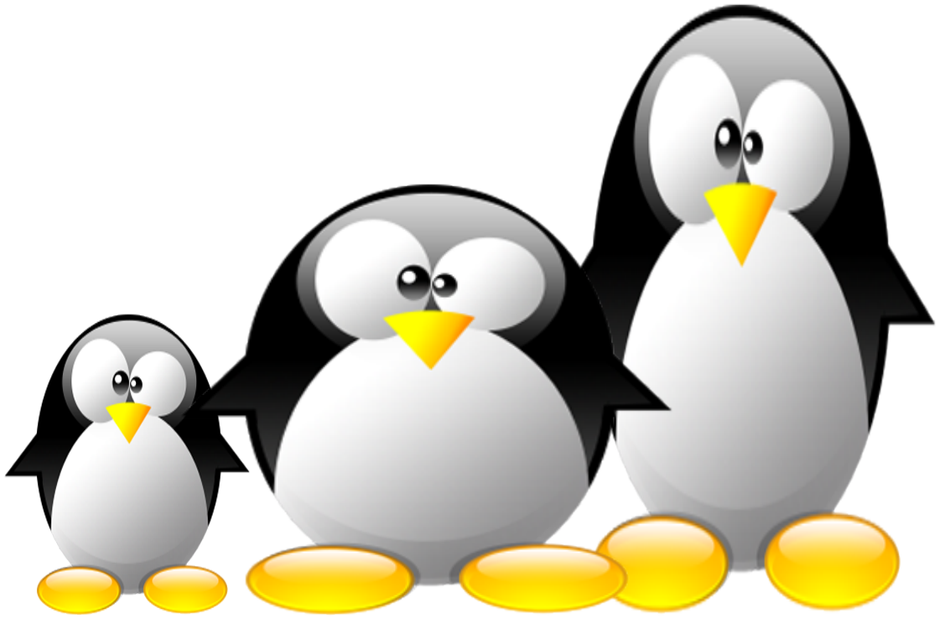
SCADA

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's inside a PLC

What's inside a PLC



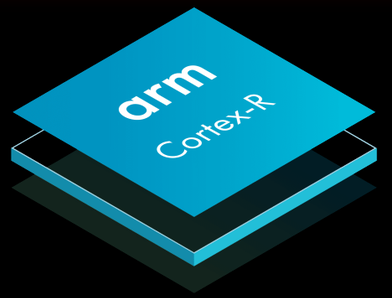
embedded **Linux**

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

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

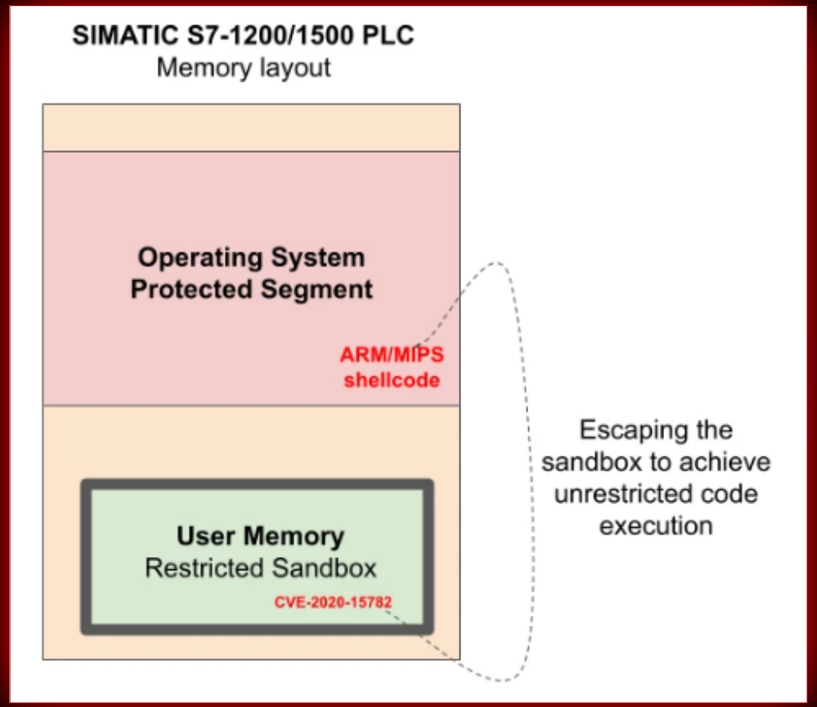
AWP Automated Web Programming		PNIO ProfiNet
MC7P Parser	MC7P RunTime	MC7P Compiler
Siemens OMS		
Central IO Subsystem	OMS SP Parser	OMS Configuration
ALARM Subsystem		OMS FAT

Siemens Adonis WebServer

HTTP GET Request Handler	Description
/appapiappa/vvvvvvvvvv	version
/appapiappa/vvvvvvvvvvv	version
/appapiappa/lililililili	log in
/appapiappa/lololololo	log out
/appapiappa/cmcmcmcmcm	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/galeldgale	get AS log entry
/appapiappa/gvigvigvig	unknown
/appapiappa/svsvsvsvsv	unknown

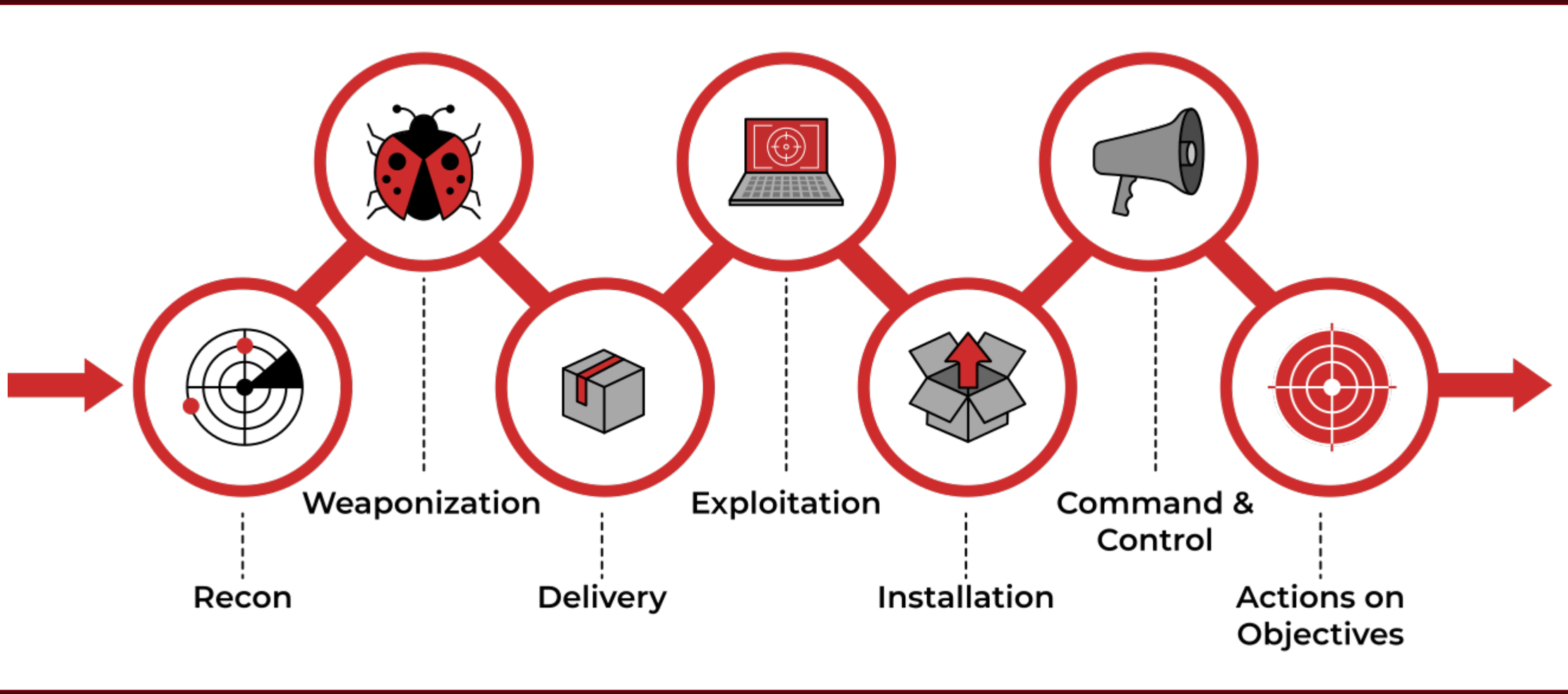
Siemens Adonis Sandbox Escape

- 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?

Adversary Simulation



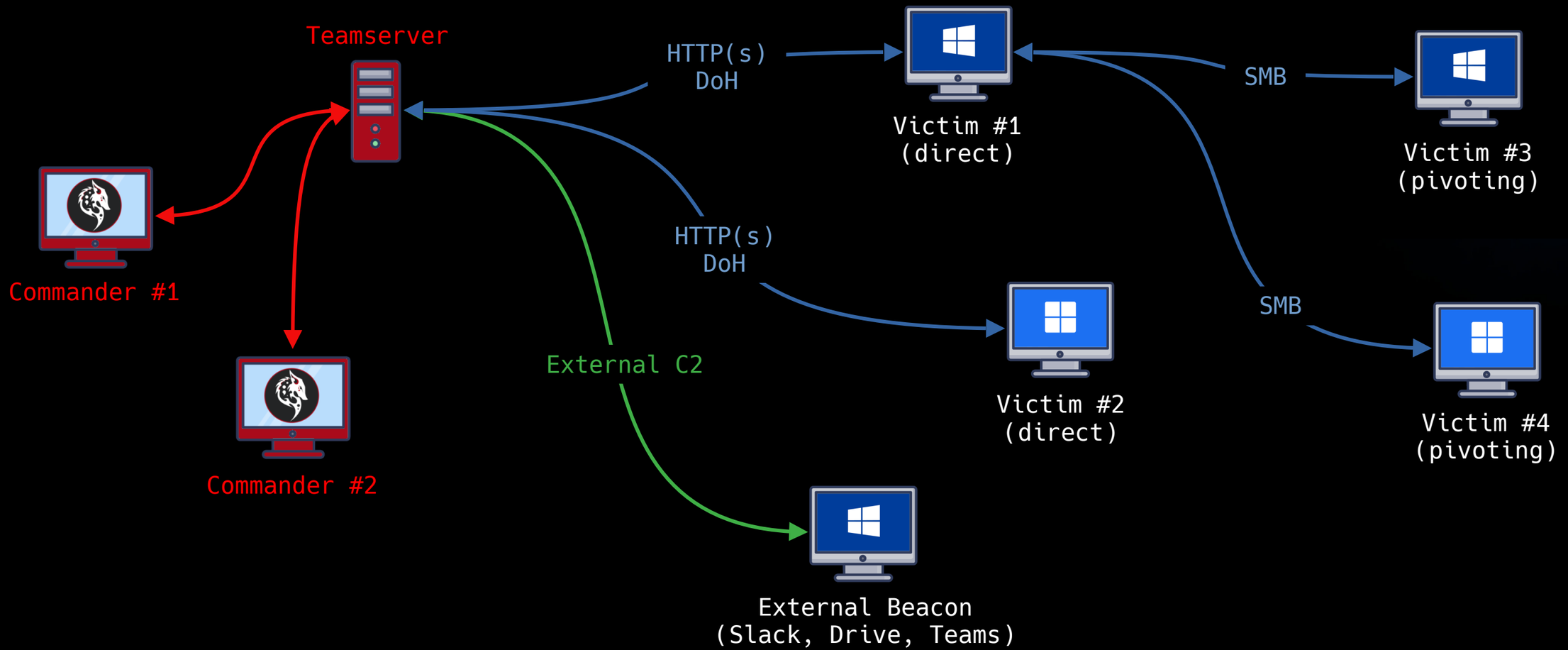
Lockheed Martin, the Cyber Kill Chain

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 complieance with ICS standards.

How a C2 works



Why a C2 for OT?

ICS Attack Surface

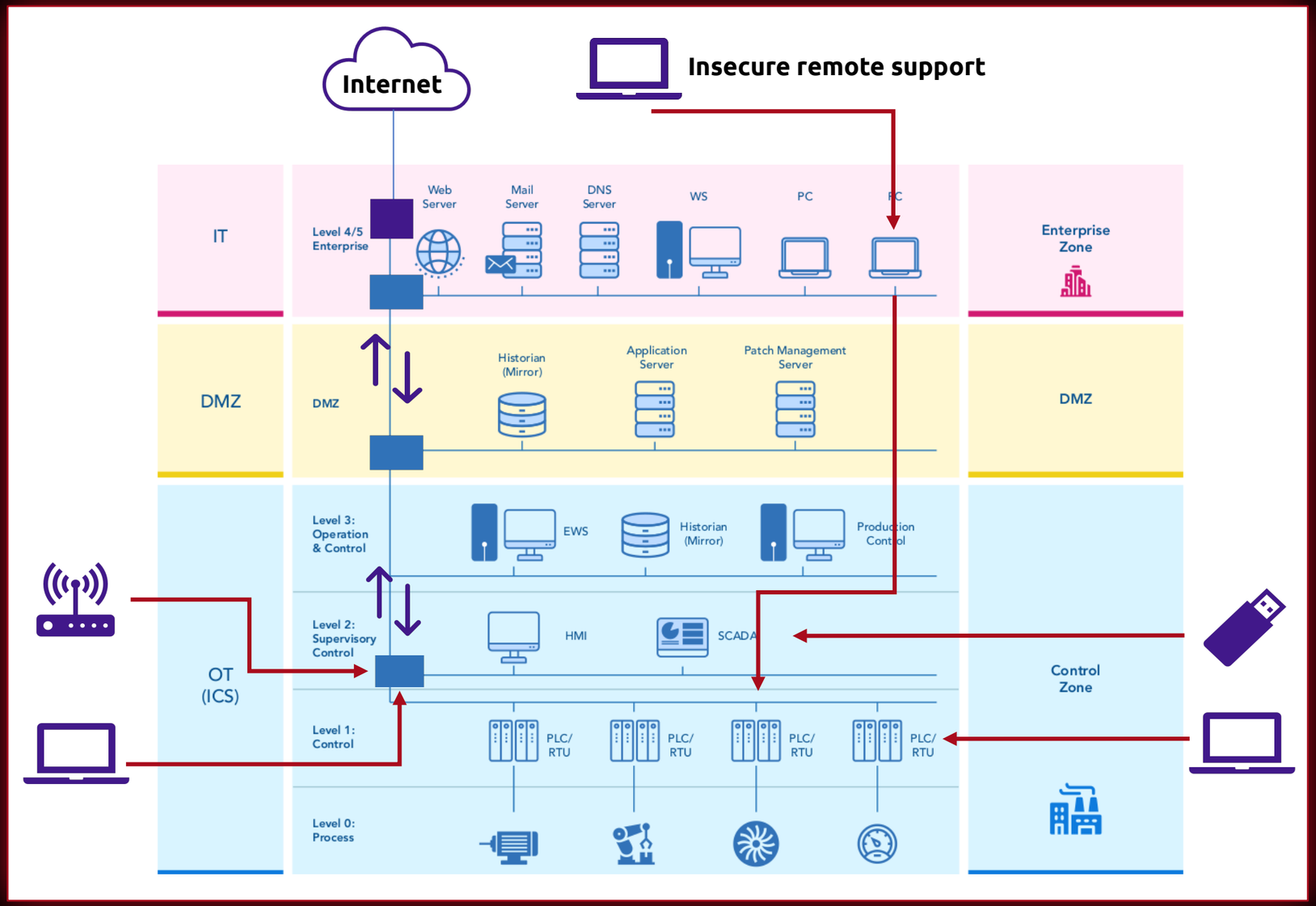
Difficult to satisfy certain cybersec hard constraints

Insecure Internet connection (eg. phishing, credentials, AV/EDR)

Inadequate access rules (no network segmentation)

Insecure WiFi

Supply Chain Attack



Infected USB

Infected laptop

SCADAsploit 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.

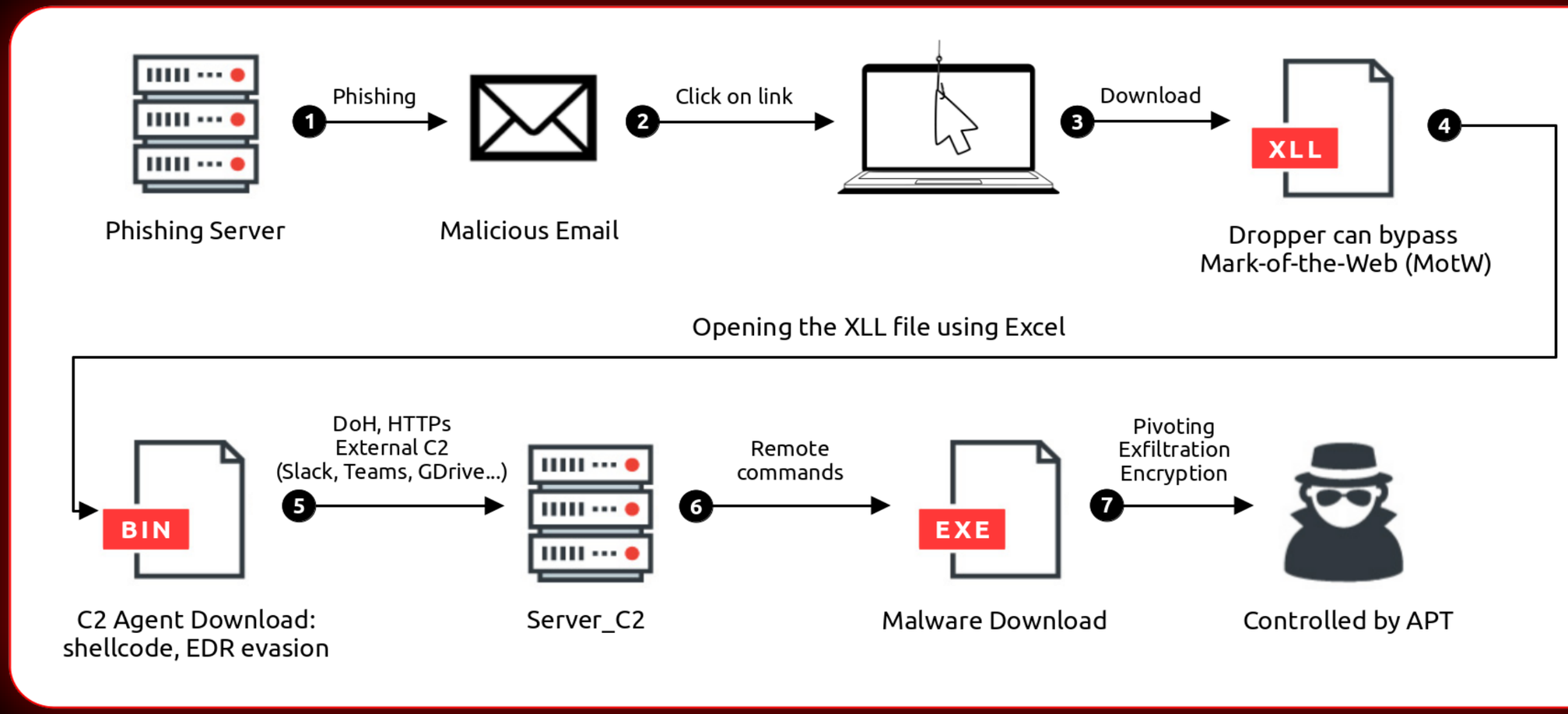
It’s a game-changing OT Framework!

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 compromized site, the dropper exploits this vulnerabilities and introduce malware.

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

Basic C2 Path Attack

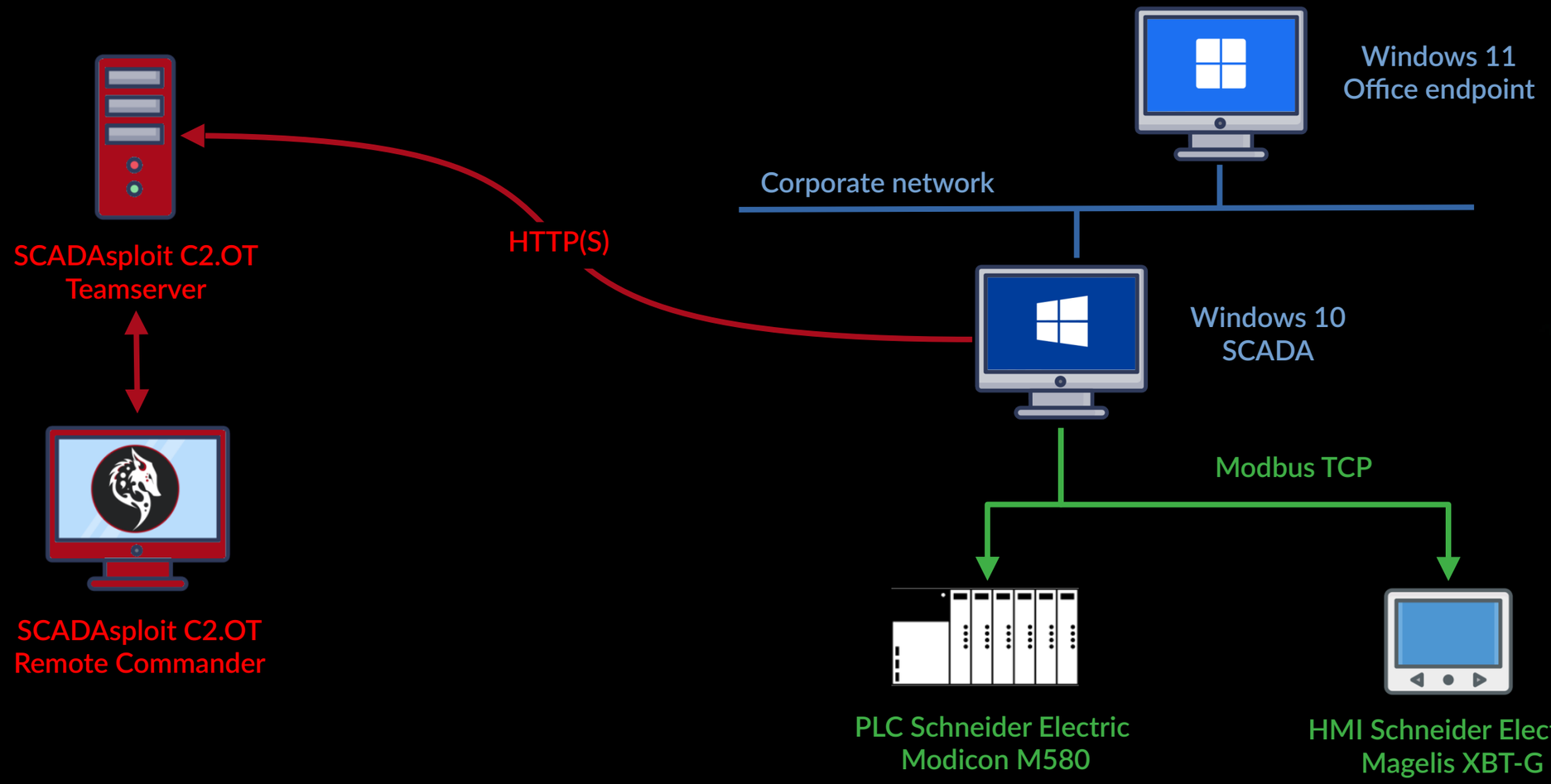


Demo

The Big Disclaimer!

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

The Demo Lab


Windows 11
Office endpoint
Corporate network
HTTP(S)
SCADAsploit C2.OT
Teamserver
Windows 10
SCADA
SCADAsploit C2.OT
Remote Commander
Modbus TCP
PLC Schneider Electric
Modicon M580
HMI Schneider Electric
Magelis XBT-G

Make it safe!

Organizational measures

- Security Assessment, Risk Assessment, BIA
- Awareness, OT Security Training
- Supplier Management, Secure Access Management
- Policies & Procedures

Technical measures

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

CYBERSECURITY NATIONAL LABORATORY

NIST

IEC SANS

MITRE ATT&CK for ICS

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

@OmarMorando

omar.morando@scadasploit.dev

https://scadasploit.dev

SCAN ME