



Cyber-MAR Piraeus Port pilot

Pilot infrastructure and topology

DIATEAM

(Jonathan Winterflood & Nicolas DIAZ)

16th December 2022

Targeted Topology | Piraeus Pilot Event

TARGETED TOPOLOGY

- IT segment:
Server/Users/DMZ nets
- OT network: SCADA
Supervision (PcVue +
Unity) & PLCs (Physical &
Virtual)
- Monitoring segment
- Remote attack from the
Internet



Founded in 2002, DIATEAM is an indie French software research and development company specializing in cyber security and innovative information systems.



- › Founded in 2002 in Brest, France.
- › R&D company specializing in computer security.
- › Industry-leading systems for cybersecurity training and testing labs.
- › Developing innovative cyber range solutions.



CYBER RANGE EDITOR
&
CYBER CONTENT PROVIDER

DIATEAM CYBER RANGE

MULTIPLE USES

Our solutions are designed and developed to meet a wide array of cybersecurity needs.

CYBER TRAINING SOLUTION

- › Cyber Awareness
- › Cyber Training
- › Exercise & Crisis Management



CYBER LAB SOLUTION

- › Deployment Testing / Benchmarking / Analysis
- › Prototyping / Designing / Pentesting
- › Patch Management / Security Assessment

TLP:GREEN

Limited disclosure, recipients can spread this within their community.

Sources may use **TLP:GREEN** when information is useful to increase awareness within their wider community.

Recipients may share **TLP:GREEN** information with peers and partner organizations within their community, but not via publicly accessible channels.

TLP:GREEN information may not be shared outside of the community.

The community here being the Cyber-MAR consortium.

Disclaimer: while the scenario, techniques, tactics and procedures were designed and implemented to be realistic, we do not mean that the current IT/OT infrastructure of Piraeus Port is vulnerable.

HYBRID CYBER RANGES FOR MARITIME/PORT CYBERSECURITY



Equipment is part of the Cyber-MAR project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389

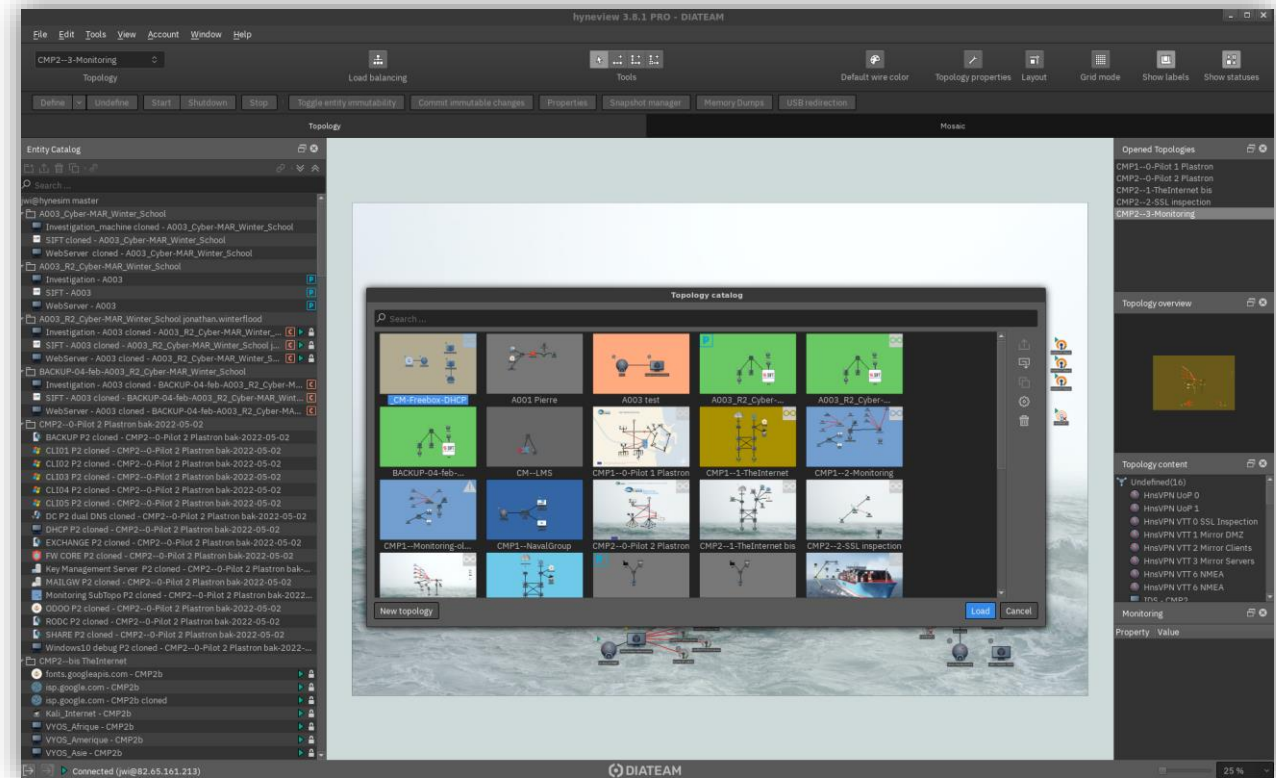


- › Hybrid connection between real IT/OT maritime/port systems and simulation
- › High realism, open architecture, lower cost

SOFTWARE

Core: DIATEAM's Cyber Range platform

- Multi-user, scalable system
- Full graphical interface for building and interacting with simulated network topologies
- Hybrid connections: connect simulations to real-world equipment, other ranges via VPN
- API for building/controlling the simulations



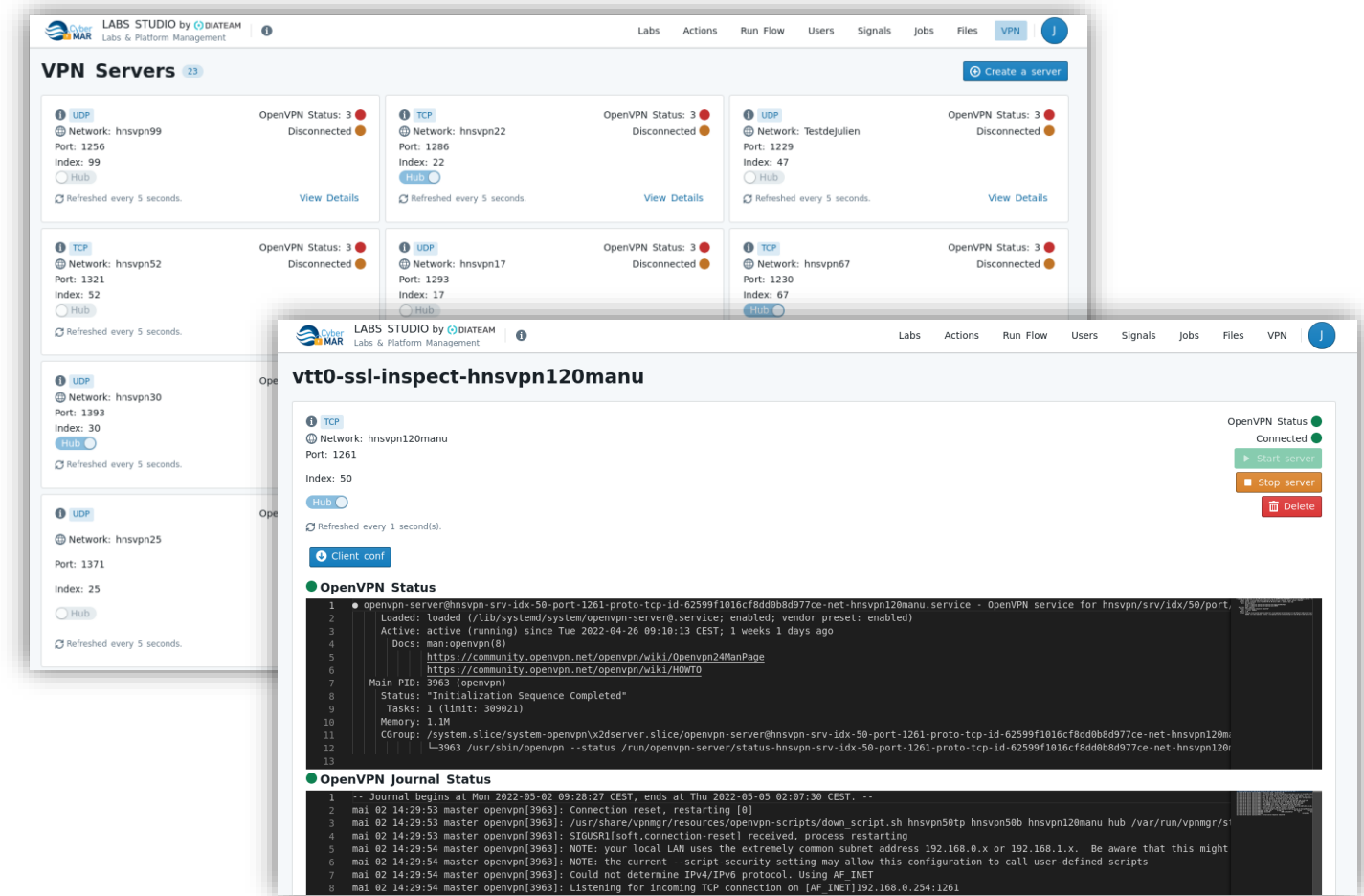
SOFTWARE

Integrated tools in DIATEAM Cyber Range:

VPN Manager

Creates and manages VPN servers on the platform:

- L2 VPNs connect directly into the simulated networks
- Connect the simulations across multiple ranges and platforms
- Connect individual users into simulations for training, etc.



The screenshot displays the 'VPN Manager' interface within 'LABS STUDIO by DIATEAM'. The main view shows a grid of VPN servers, each with a status indicator (e.g., 'Disconnected') and a 'View Details' button. A detailed view of a specific server, 'vtt0-ssl-inspect-hnsvpn120manu', is overlaid in the foreground. This view includes the server's network configuration (Network: hnsvpn120manu, Port: 1261, Index: 50), a 'Hub' toggle, and a 'Client conf' button. Below this, the 'OpenVPN Status' is shown as 'Connected', with 'Start server' and 'Stop server' buttons. The 'OpenVPN Journal Status' section displays a log of system events, including connection resets and initialization completion.



Cyber-MAR Piraeus Port pilot

Cyber Range Modules

MISP by Naval Group



Cyber-MAR Piraeus Port pilot

Cyber Range Modules

IDS & HBD by VTT



Cyber-MAR Piraeus Port pilot

Cyber Range Modules

XL-SIEM + LADS by ATOS



Cyber-MAR Piraeus Port pilot

Cyber Range Modules

Prediction Engine by ICCS

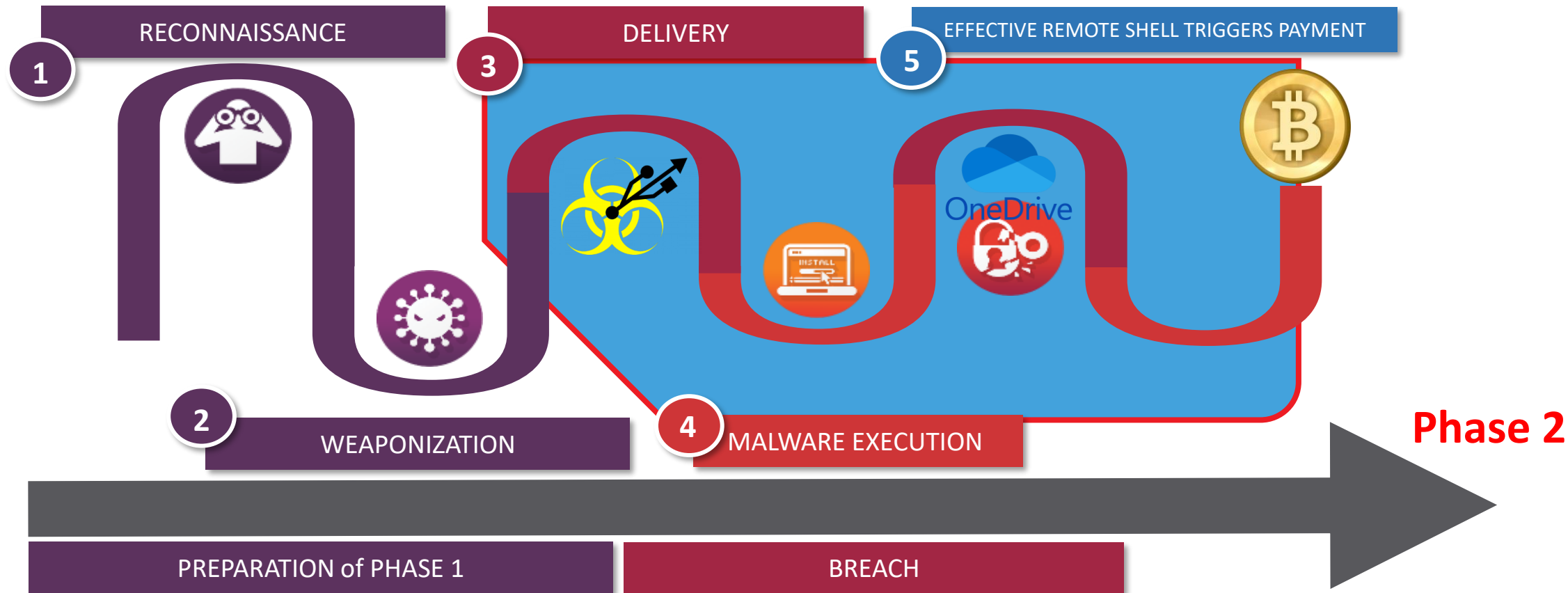


Cyber-MAR Piraeus Port pilot

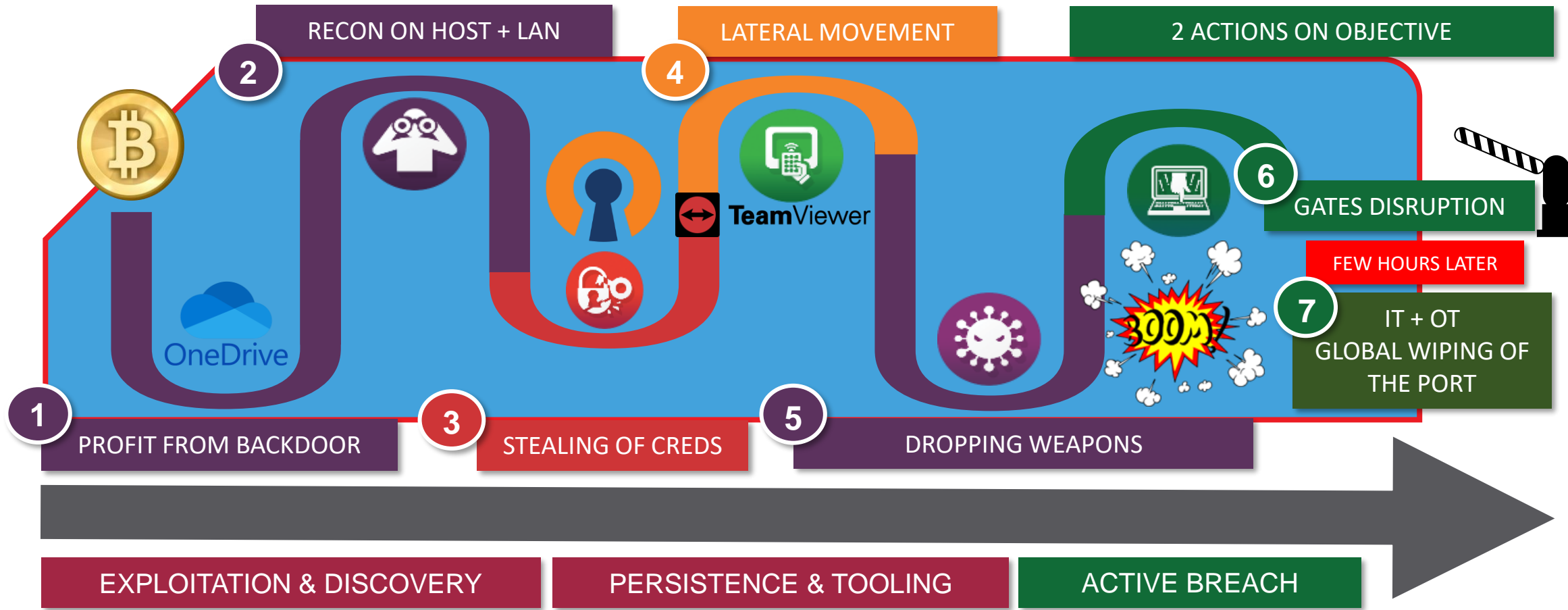
Pilot Walkthrough

Killchain & Scenario

Phase 1 through 5 steps



Phase 2 through 6 steps



Phase 1

RECONNAISSANCE by APT group & local criminals

1



Research, identification and selection of targets

- Name/surname of IT/OT Managers within Piraeus Port
- Finding physical address to identify targets' cars and parking lots



Estimated Execution Time : days to months

2



WEAPONIZATION by APT group

Crafting of ISO file that contains a malicious LNK which uses xcopy to copy hidden files embedded in the ISO into the OneDrive Folder leading to DLL side loading on target
T1204 > Defense Evasion + User Execution: Malicious Link T1204.001 + Use of C2 called Havoc



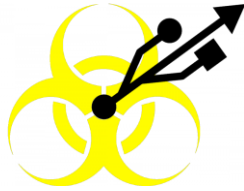
hours to days

Phase 1

DELIVERY by local criminals



3



Evil USB drive « lost » in a parking lot (Rate Success: 50%)
Transmission of weapon by human interaction
On offline IT/OT systems, 90% of attacks come from USB devices

Minutes to days

Phase 1

MALWARE EXECUTION by security staff



Once delivered, the weapon's code is triggered thanks to user interaction (USB Key plugged in the port IT to avoid MOTW)

4

Subvert Trust Controls: Mark-of-the-Web Bypass

> T1553.005 > Tactic: Defense Evasion



A couple of seconds

Phase 2

EXPLOITATION: DISCOVERY / HARVESTING

1



Thanks to the **OneDrive DLL side loading** on target, attackers can profit from a remote shell and interacting via the Command&Control with a quite good persistence as OneDrive is run at startup.

DLL Side-Loading > T1574.002 > Tactics: Persistence, Privilege Escalation, Defense Evasion

Boot or Logon Autostart Execution > T1547 > Tactics: Persistence, Privilege Escalation

2



Attackers know that this machine contains interesting credentials, so using some uploaded powershell scripts, they can harvest credentials (namely VPN creds) and through the use of a keylogger, it can log any keyboard stroke.

Input Capture: Keylogging > T1056.001 > Tactics: Collection, Credential Access



Hours to days

Phase 2

STEALING CREDENTIALS & LATERAL MOVEMENT

3



Stealing saved credentials from OpenVPN client and exfiltrating OpenVPN certificate enable the attackers to connect via OpenVPN.

Credentials from Password Stores > T1555 > Tactic: Credential Access
Exfiltration Over C2 Channel > T1041 > Tactic: Exfiltration

4



TeamViewer

OpenVPN access then abuse of TeamViewer

Remote Access Software > T1219 > Tactic: Command & Control



Minutes to hours

Phase 2

DROPPING OF CRAFTED MALICIOUS CODE



Thanks to the stolen credentials and using Teamviewer, attackers can access all SCADA monitoring machines.

5

Still using Teamviewer, attackers can upload malicious code on any machine on the LAN.



Minutes to hours, depending on the profile of the threat actor.

Phase 2

1st action: GATES DISRUPTION



Once gaining access to the SCADA supervision machine, the attackers stop and reflash the PLCs with new firmware

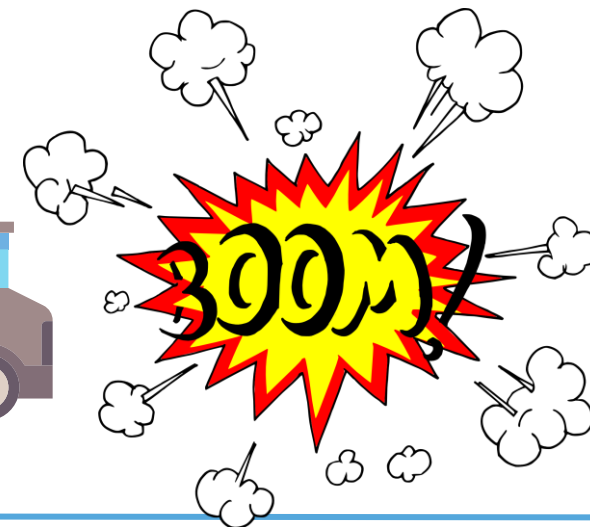
6

This causes the dysfunctioning of the gates (requires good timing to maximize damages) at the crossroads of trucks and trains, increasing the risk of collision and disruption of the logistic chain within the port.

Firmware Corruption > T1495 > Tactic: Impact



Minutes to hours



Phase 2

2nd action: GLOBAL IT/OT WIPING



By abusing Teamviewer, attackers drop malicious code on one machine within the LAN and execute it, causing the wiping of Master Boot Record (MBR) of all machines connected to the cybermar.com domain (including all remote workers connected via VPN)

7

NotPriap Wiper is executed on one workstation and propagates to Domain Controller

Disk Wipe > T1561 > Tactic: Impact



A couple of minutes

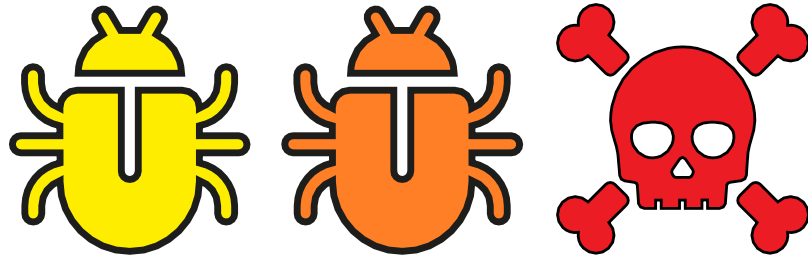


DEMO via Cyber-MAR Cyber Range

Let's play the game !

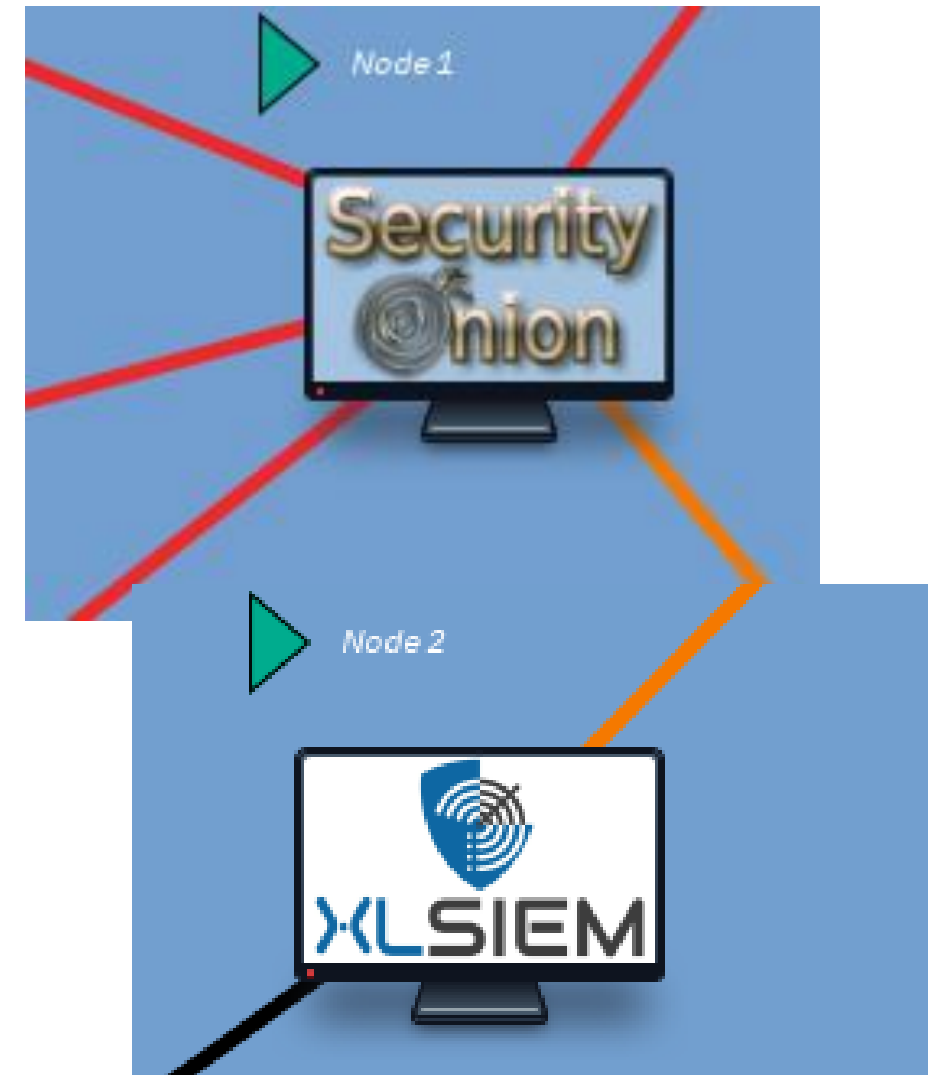


MONITORING RESULTS & COMMENTS AFTER ATTACK



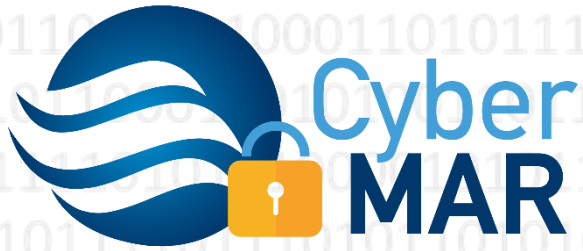
VTT – IDS + HBD

ATOS – XL-SIEM



Global Q&A Session | Piraeus Pilot Event





 www.Cyber-MAR.eu

 [Cyber_MAR](https://twitter.com/Cyber_MAR)

 [Cyber-MAR EU Project](https://www.youtube.com/Cyber-MAR)

 [Cyber-MAR](https://www.linkedin.com/company/Cyber-MAR)

 info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION



This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement No. 833389