



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Securing OT

too hard or not for me?

Erwin Paternotte

Orangecon, 2024

NCSC



Erwin Paternotte

Senior CTI specialist

"I've hacked the planet and now I'm tracking what the bad guys do."



**Why this
presentation?**



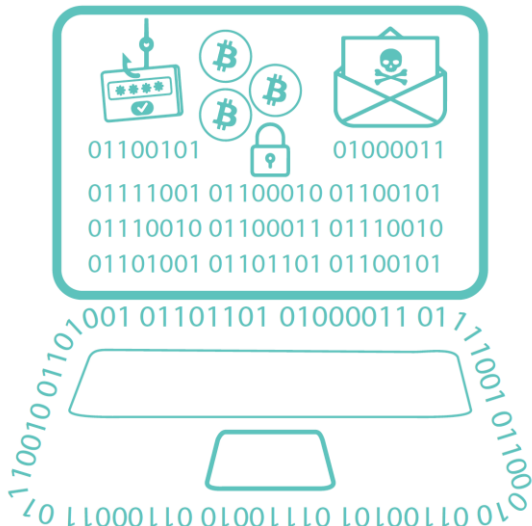
OT vs IT

Differences

- Legacy (30+ years)
- Availability is most important
- Designed with **safety** in mind, not security
- Insecure by design
- Incidents may have a physical impact

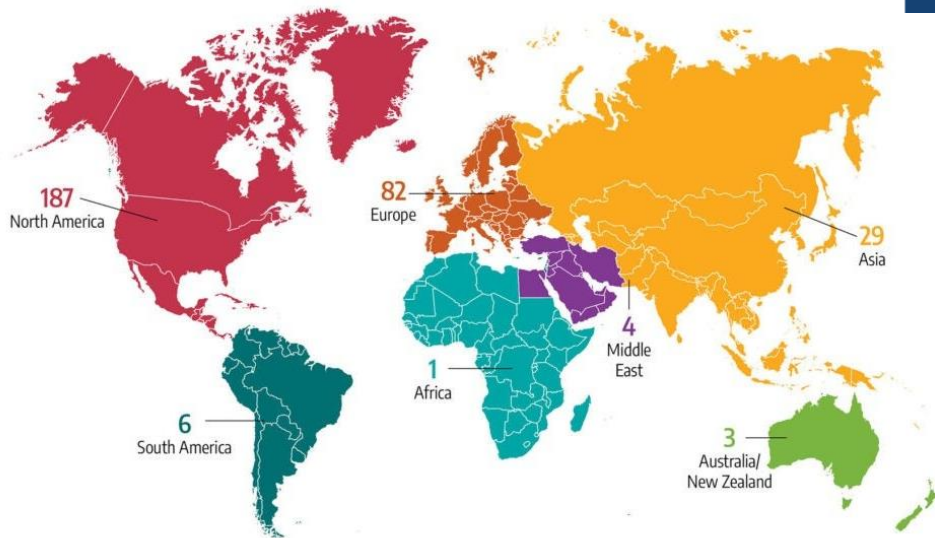


Threat actors



Ransomware

- Untargeted
- Not specifically targeting OT processes
- Focus on IT systems, which may have cascading effects on OT
- Increasing number of incidents

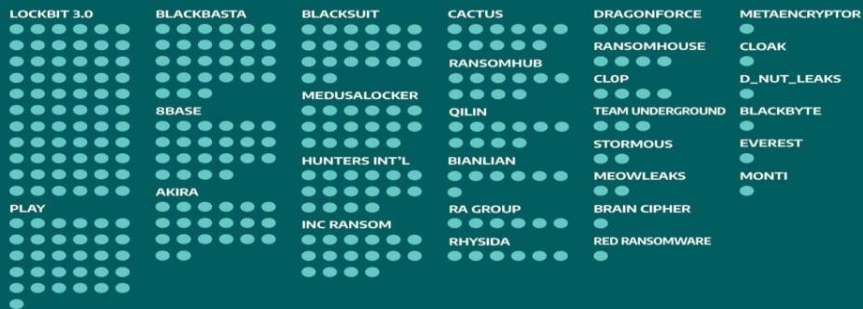


Dragos Industrial Ransomware Analysis

Q2 2024

- Increase compared to Q1
- Government-affiliated groups adopt ransomware tactics
- No direct targeting of ICS/OT processes, the interconnected nature of IT and OT environments can have significant downstream effects on OT operations.
- [Dragos Industrial Ransomware Analysis: Q2 2024 | Dragos](#)

Ransomware Incidents by Group/Strain Q2 2024





Hacktivism

- Untargeted, device oriented
- Diverse group, ties to APTs have been identified
- Mostly targeting internet connected OT devices
- Low technical complexity, regardless physical impact



Host Filters

Labels:

- 113.94K ics
- 113.94K scada
- 67.94K login-page
- 31.94K remote-access
- 21.80K jquery
- More

Autonomous System:

- 11.19K AMAZON-02
- 10.74K CELLCO-PART
- 7,808 COMCAST-7922
- 3,949 DTAG Internet service provider operations
- 3,345 ATT-INTERNET4
- More

Location:

- 51.70K United States
- 7,179 Canada
- 6,218 Germany
- 3,815 Italy
- 3,500 Australia
- 3,253 France
- 3,022 United Kingdom
- 2,971 Greece
- 2,965 Sweden
- 2,774 Turkey
- 2,648 Spain
- 1,759 Japan
- 1,564 Netherlands
- 1,451 Czech Republic
- 1,236 Romania
- 1,116 South Korea
- 950 Poland
- 935 Brazil
- 908 Denmark
- 792 South Africa

Hosts

Results: 113,933 Time: 0.19s

183.105.186.183

Microsoft Windows

scada ics

81/HTTP

5.26.144.26

TURKCELL-AS Turk

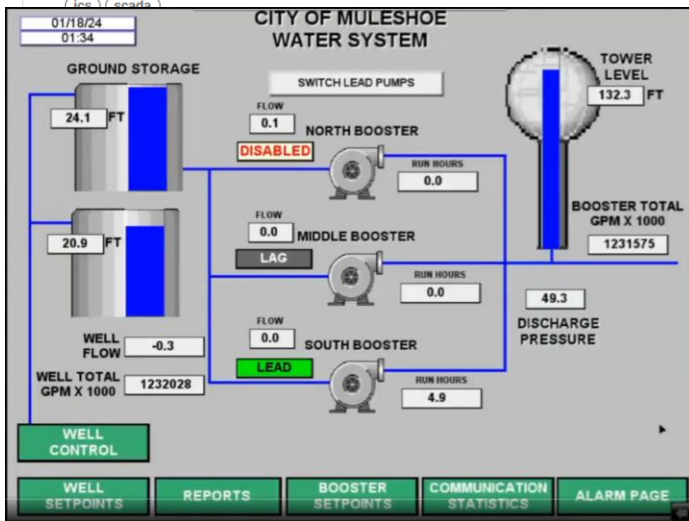
scada ics

8088/HTTP

134.97.101.194

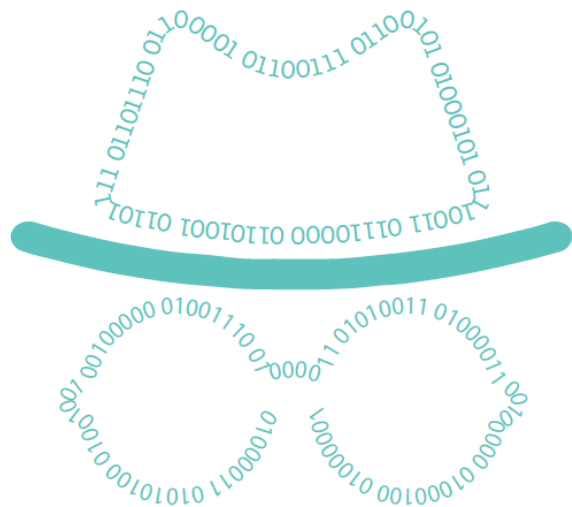
Microsoft Windows

ics scada



Internet connected OT devices

- CyberArmyofRussia_Reborn (CARR), linked to [Sandworm](#) caused [water tank overflow](#) in [Muleshoe, Texas](#).
- CyberAv3ngers, run by the Iranian Government Islamic Revolutionary Guard Corps targeted [Unitronics PLCs](#).
- Solntsepek targeted Ukrainian telco's with [wiperware](#).
- Claims may be false or hard to verify.

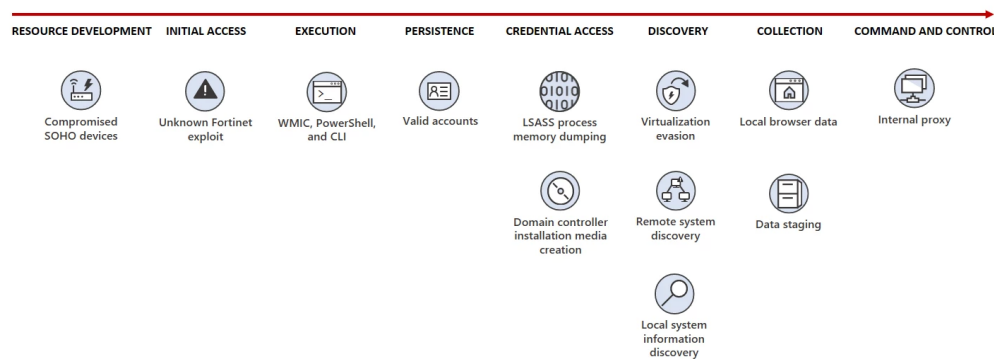


Spionage

- Targeted
- Mostly critical infrastructure
- Information gathering & prepositioning



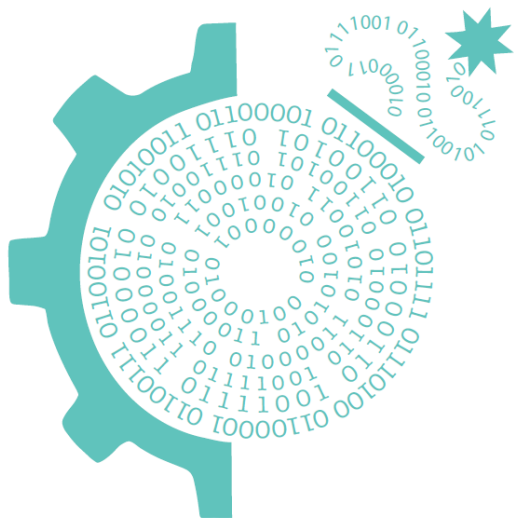
Volt Typhoon



- Targeting US critical infrastructure
- Routes traffic through SOHO devices
- Initial access through compromising Fortinet devices
- Tries to maintain access for a long time
- [Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Security Blog](#)



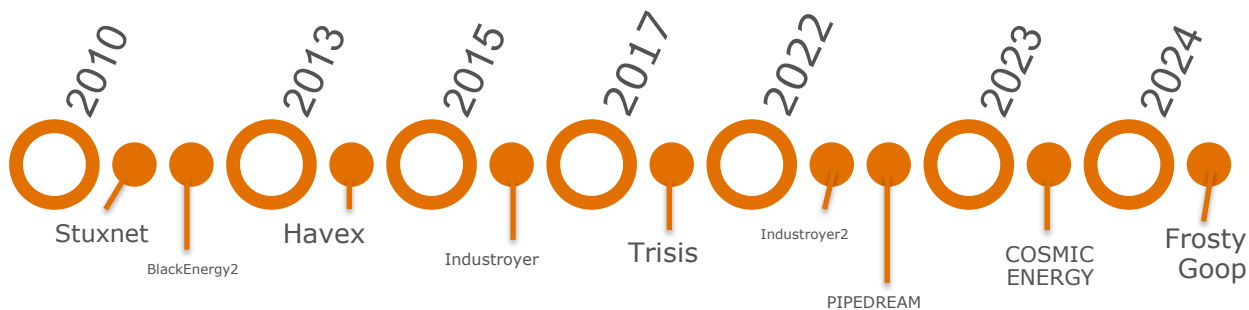
Sabotage



- Extremely targeted
- Only 9 ICS specific malware families identified.
- Some discovered before deployment, others caused incident.
- Sabotage may have political consequences.



Timeline ICS specific malware





Common vulnerabilities and weaknesses OT environments





Security testing

OT

- Systems less resistant to security testing.
- Almost no test environments, spare parts or redundancy.
- OT security assessment is a combination of architecture & configuration review, combined with light security testing.
- [Scanning Highly Sensitive Networks - v3.pdf - Google Drive](#)



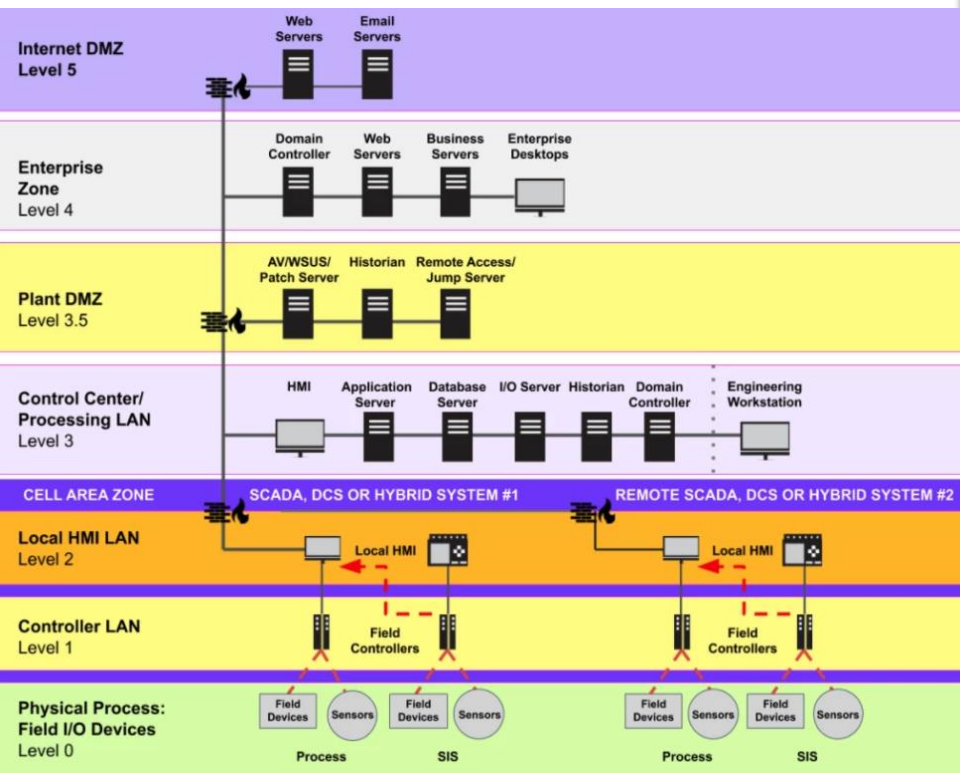
Review network design & security architecture

- Network drawings & asset overview
- Firewall & network switch configurations
- Remote access
- Virtualisation shared between IT/OT





Purdue model



- No direct connections between IT/OT or internet, only through intermediate systems in Plant DMZ
- Firewall between IT/OT and level 3 and 2.
- OT systems pull data from systems in Plant DMZ.
- Strict firewall rules, no any.



Windows systems

- HMI, SCADA, Engineering Workstation, Domain controllers, Application servers.
- Active Directory shared or trusted between IT/OT.
- Vulnerabilities & patching
- Hardening



HMI, PLC, sensors & actuators

- Weak or default password
- Vulnerabilities
- Insecure (management) protocols



Conclusions & recommendations





Conclusions

- There is still a lot of room for improving security of OT environments.
- Threat intel may help determine your risks and needed efforts.
- It is not hard, but it does require effort.



Recommendations

- Start with the quick wins (default passwords, improving the ruleset of your IT/OT firewall).
- Start an asset inventory
- Work together with your vendor to patch systems and improve hardening.
- Improve the network architecture (layered design, secure remote access).



Dave Luber @NSA_CSDirector · Oct 14, 2023
Admit it. You know stuff you should be fixing.

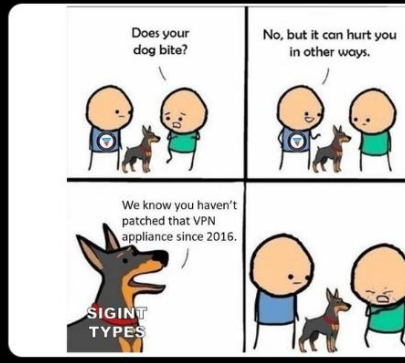
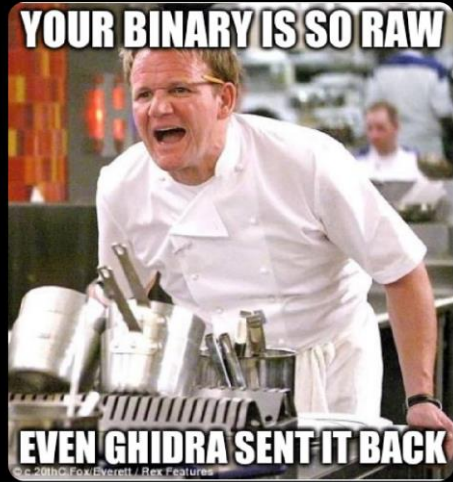
Dave Luber @NSA_CSDirector · Oct 18, 2023
Attackers will work to know your network better than you do. They will find shadow IT, misconfigurations, weak authentication and unpatched devices containing n-days. Discover and fix it before them. #KnowledgelsPower #KnowledgelsSecurity



18 127 359 93K

You reposted

Rob Joyce @RGB_Lights · 11 Jun 19



But Nation states/APTs!?

- Adapt to the target.
- Will only use zero days if they have to.
- Invest time to know your systems and network inside out.
- The security measures on the previous slide also make them work hard.
- Don't believe me, watch this presentation: [USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers - YouTube](#)



Questions?

[https://www.ncsc.nl/
werken-bij-het-ncsc](https://www.ncsc.nl/werken-bij-het-ncsc)