2021 CHEMICAL SECURITY SEMINARS

December 8, 2021

#ChemicalSecurity

CHEMICAL SECURITY SEMINARS

Cyber Threat Hunting: Industrial Control Systems Security

Alex Reniers

Section Chief
Industrial Control Systems Section
Cybersecurity Division
Cybersecurity and Infrastructure Security Agency

#ChemicalSecurity

INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY

PROGRAM BRIEF

WHY ICS SECURITY IS IMPORTANT

Control systems are integral to critical infrastructure operations, functionality, and safety.

Exploitation of ICS can result in:

- Physical harm to people, property, and the environment
- Data corruption and exfiltration
- Equipment malfunctions

Almost all CI operations depend on ICS.

WHO WE ARE

MISSION

CISA leads the National effort to understand and manage cyber and physical risk to our critical infrastructure.

VISION

A secure and resilient critical infrastructure for the American people.

ROLE

CISA is the Nation's risk advisor. We are here to advise critical infrastructure owners and operators on the risks that they are facing.

Director's Operational Priorities

CISA'S ROLE IN ICS SECURITY

CISA is the lead federal civilian agency responsible for helping Critical Infrastructure (CI) partners manage ICS risk

CISA is committed to growing operational and strategic partnerships to increase collaboration across the ICS community

AUTHORITIES

- Title II of the Homeland Security Act of 2002
  - Section 201(d) (6 U.S.C. § 121(d))
- Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- Executive Order 13636—Improving Critical Infrastructure Cybersecurity

CISA'S ROLE IN ICS SECURITY

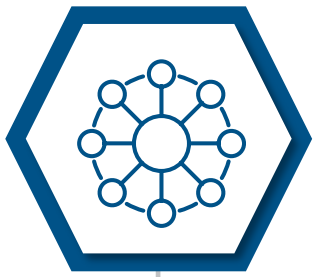
DEFENDING TODAY, SECURING TOMORROW

We require a new model that enlists the entire community to anticipate, prioritize, and proactively manage ICS risk.

We will build capabilities around four guiding pillars:

Ask more of the ICS community, deliver more to them.

Develop and utilize technology to mature collective ICS cyber defense.



Build "deep data" capabilities to analyze and deliver information that disrupts the ICS cyber kill chain.

Enable informed, proactive security investments by understanding and anticipating ICS risk.

Through this strategic focus, CISA and its partners can change the ICS risk management paradigm.

ICS HISTORY: WHERE WE'VE BEEN, WHERE WE'RE GOING

2000:
Congress creates Federal Incident Response Center (FedCIRC)

2003:
Congress moves FedCIRC to newly formed DHS; renames the capability to US Cybersecurity Emergency Readiness Team (US-CERT

2004:
Congress creates the Control Systems Security Program (CSSP)

2009:
DHS formalizes the operational arm of the CSSP, and calls it the Industrial Control Systems Cybersecurity Emergency Readiness Team (ICS-CERT)

2009:
DHS establishes the National Cybersecurity and Communications Integration Center (NCCIC)

2012:
The ICS-CERT brand replaces the CSSP program name

2015:
The Cybersecurity Act of 2015 designates NCCIC as the central hub for cyber threat indicator sharing

2017:
NPPD streamlines existing functions ;the ICS-CERT brand is retired and only the US-CERT brand remains.

2018:
The Cybersecurity and Infrastructure Security Agency Act of 2018 was signed into law.

2019:
CISA unifies its capabilities and US-CERT and ICS-CERT brands are retired.

PAST **PRESENT**

CURRENT AND EMERGENT ICS CHALLENGES

Lack of funding or leadership support

Uncertainty introduced in rapid evolution of technology

Rapid growth of internet connected devices creates a broader attack surface

Legacy ICS/OT aging and difficult to secure

Small workforce with ICS/OT cybersecurity knowledge

WORLDWIDE THREAT ASSESSMENT

Russia

Russia poses a cybersecurity threat to the United States and our allies. It is a highly capable and effective adversary, integrating cyber espionage, attack, and influence operations to achieve political and military objectives.

China

China presents a persistent cyber threat to our military and CI. It remains the most active strategic competitor responsible for cyber espionage against the U.S. Government, corporations, and allies.

Iran

Iran continues to present a cyber threat, using increasingly sophisticated techniques to conduct cyber espionage and deploy capabilities that would enable cyber attacks against CI in the United States.

North Korea

North Korea poses a cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks.

Non-State Actors

Foreign cyber criminals, terrorists, and others will continue to conduct malicious cyber attacks to further their goals, aided by the growing availability and use of publicly available cyber tools.

TOP ATTACK VECTORS IN ICS

USB Devices

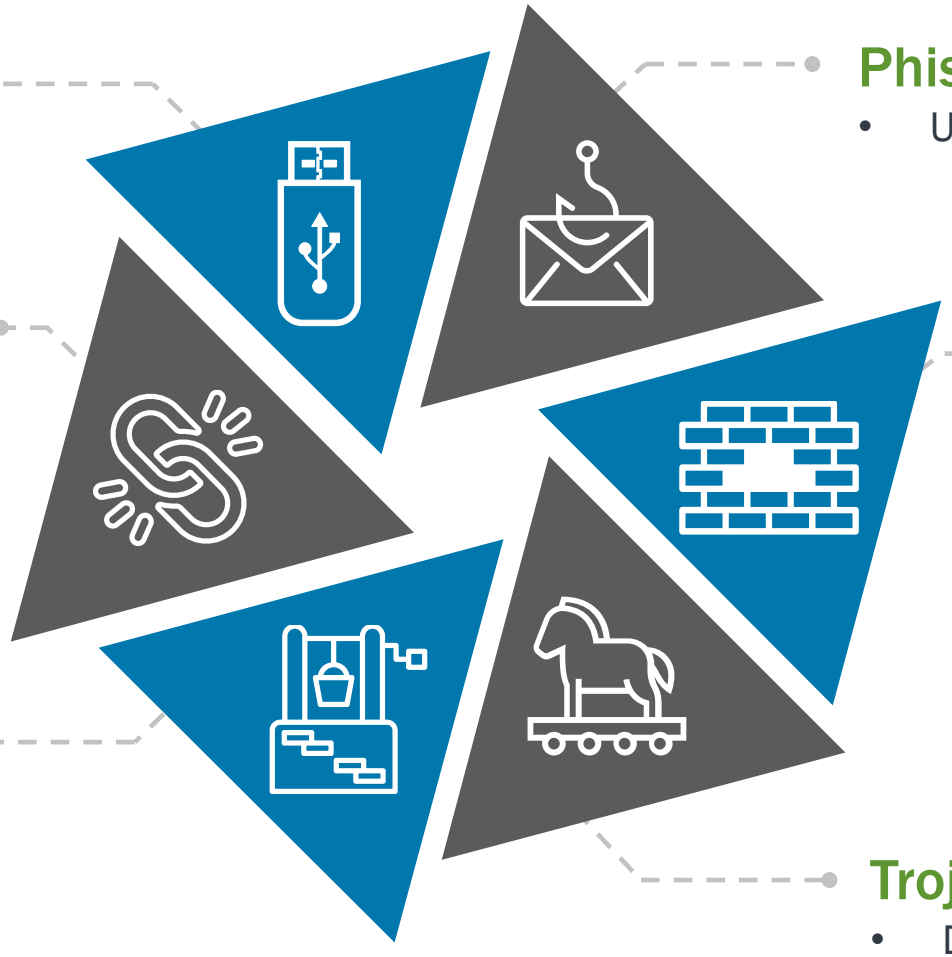
- May contain malicious files or malware

Supply Chain Compromise (i.e. Compromise Vendor)

- "Island Hopping" compromise (i.e. compromise trusted partner)

Watering Holes

- Threat actor guesses or observes which websites an organization often uses and infects one or more of them with malware



Phishing

- Usually with malicious attachments

Path of Least Resistance

- Zero-day vulnerabilities are not so common and are usually not needed
- Patching policies and oversights

Trojanized Software

- Downloadable application that contains malware or a virus

ICS CYBER ATTACK SURFACE

ICS environments are often exposed to the same threats seen IT environments

- Human Machine Interface (HMI) and engineering workstations predominantly run Microsoft's Windows OS
- Some PLCs, data acquisition servers, SCADA servers, and industrial PCs do as well
- Linux and MacOS are less common

Architecture and internal practices influence attack surface

- Internal polices or lack thereof
- Additional entry points are not uncommon and are not always known
- Poor boundary protection or architecture

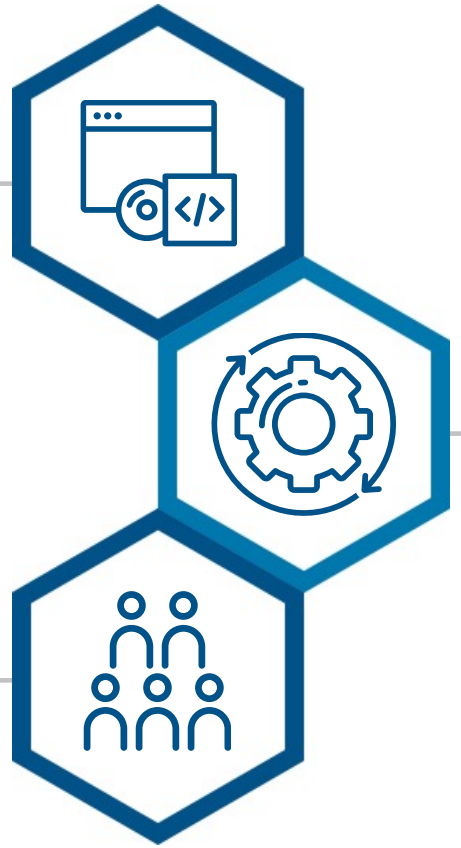
ICS CHALLENGES

Hard to replace systems and components, leaving in place legacy hardware and software

- Still see Windows 98, 2000, and XP
- Conficker dates to 2008, but it's still commonly found in OT environments

Staffing, and staffing dynamics

- No dedicated ICS/IT administrator
- IT and ICS staff often do not coordinate
- Difficulty of finding staff with ICS cybersecurity experience or knowledge



Availability is priority number one

- High degree of availability required in ICS environments
  - Keep processes running with as little downtime as possible
  - And maintain a certain level of personnel and environmental safety

ATTACKS ON INFRASTRUCTURE

Past few years have seen active compromises of low level or embedded device

VPNFilter targeting dozens of different routers

HatMan/Triton

Alien Viper (DragonFly 2.0, Russian Actors Target Energy)

Ukraine 2015 & 2016

POTENTIAL CONSEQUENCES

CURRENT ICS SECURITY OFFERINGS

CISA helps customers defend ICS today through these capabilities …

Assessments
Operational resilience evaluations

Cyber Hunt
Aid ICS partners with adversary presence search in absence of known threat

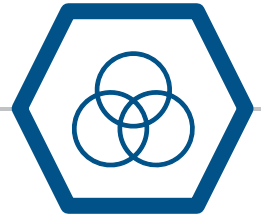
Exercises
Testing and readiness for ICS incidents

Information Exchange
Sharing of threat and best practice guidance with partners

Partnerships and Engagement
Collaborate and coordinate with ICS partners

Products and Tools
Access to hands-on tools for the ICS community

Response
Provide expertise and advanced tooling to aid ICS cyber victims



Strategic Risk Analysis
Provide ICS risk information pertaining to National Critical Functions (NCFs)

Technical Analysis
ICS malware analysis support

Training
Technical and non-technical ICS instruction for all skill levels

Vulnerability Coordination
Coordinated, public disclosure of ICS vulnerabilities and mitigation recommendations

CISA ICS OFFERINGS: SPOTLIGHT

THE CONTROL ENVIRONMENT LABORATORY RESOURCE (CELR) is an environment for government and private industry partners to experience the possible effects of kinetic cyber physical attacks.

CELR allows users to perform security research on industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems

MALCOM is an open source, easily deployable network traffic analysis tool suite for full packet capture artifacts (PCAP files) and logs.

Malcom provides insight into specific protocols used in ICS environments and is comprised of open-source tools, so it does not require users to obtain paid licenses and is freely available on CISA's GitHub page.

ENGAGE WITH US

- For more information on CISA's ICS products, services, and news visit cisa.gov/ics.
- To report an incident or a vulnerability, visit https://us-cert.cisa.gov/report.
- For general inquiries, call us at 1-888-282-0870 or email central@cisa.gov.