INDUSTRIAL CONTROL SYSTEMS VULNERABILITIES AND RESOURCES

CISA
CYBER+INFRASTRUCTURE

July 9, 2019

ICS SECURITY IS A NATIONAL IMPERATIVE

CISA leads an integrated, unified national effort to drive down industrial control systems risk

- ICS are integral to critical infrastructure (CI) operations
- Successful exploitation of ICS can result in not only data corruption and exfiltration, but significant physical consequences
- Different risk factors and security constraints come into play in an ICS environment
- Managing ICS risk requires specific information technology (IT) and operational technology (OT) technical expertise

CISA
CYBER+INFRASTRUCTURE

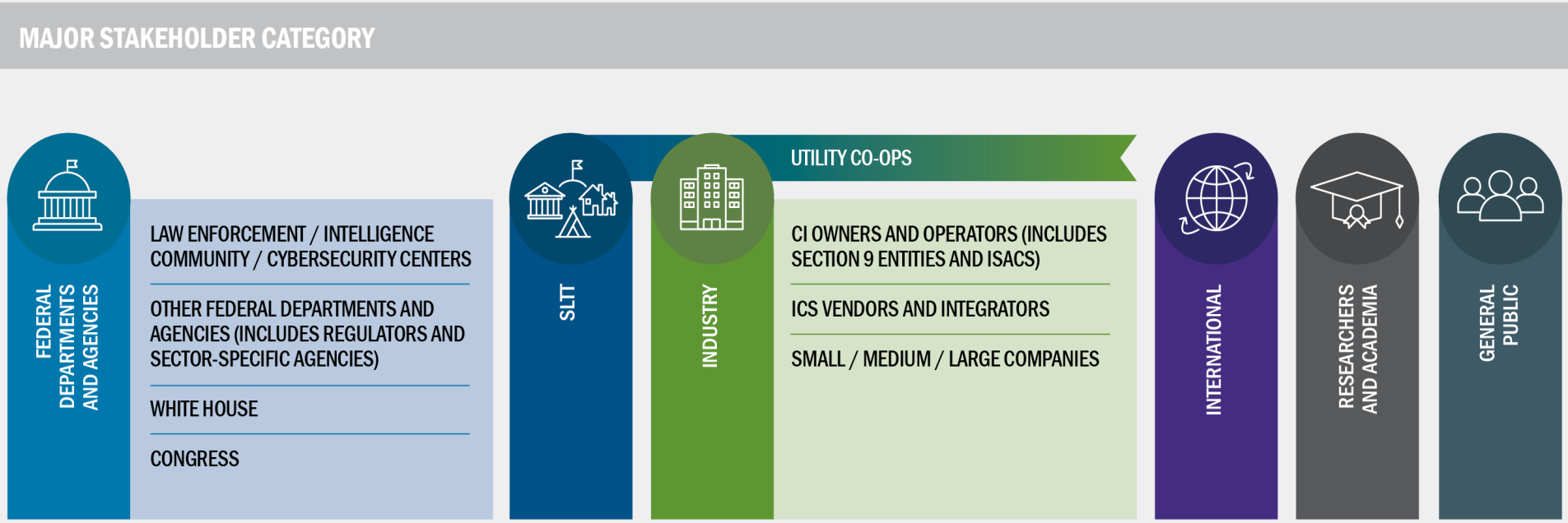
HELP OUR PARTNERS HELP THEMSELVES

No organization can defeat ICS threats alone

- **Today**: We must continue to build on the outstanding ICS defense capabilities we currently provide
- **Tomorrow**: Sustainable ICS security through whole community ICS risk management

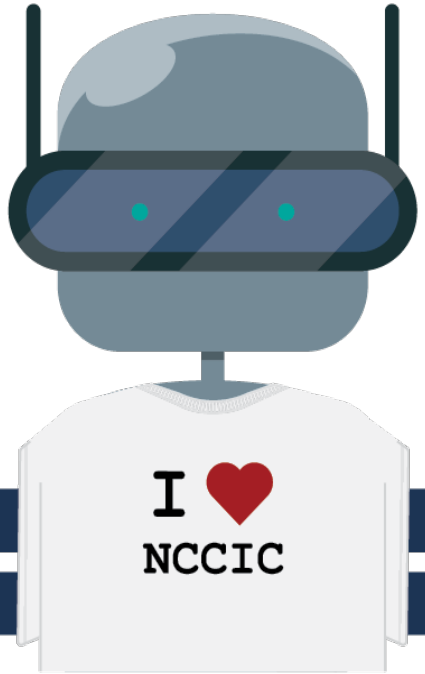
CISA
CYBER+INFRASTRUCTURE

ICS STAKEHOLDERS



WHAT WE DO

- INCIDENT RESPONSE AND RECOVERY
- NATIONAL COMMUNICATIONS / EMERGENCY PREPAREDNESS
- INFORMATION EXCHANGE
- WATCH FLOOR OPERATIONS
- CYBERSECURITY ASSESSMENTS
- FEDERAL NETWORK PROTECTION
- TECHNICAL ANALYSIS
- HUNT
- EXERCISES AND TRAINING



CISA
CYBER+INFRASTRUCTURE

Case Studies

Case Studies

Actors sought and exfiltrated ICS- and SCADA-related information

FY 2012 ACTIVITY AGAINST U.S. PIPELINES

- **Document searches for "SCADA"**

- Personnel lists
- Usernames and passwords
- Dial-up access information
- System manuals

In FY 2012, 23 pipeline transmission companies reported spear-phishing incidents

13 Confirmed Compromises

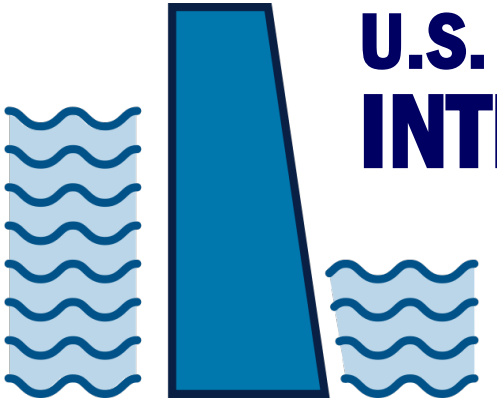
3 Not Compromised

7 Unknown

CISA CYBER+INFRASTRUCTURE

https://go.usa.gov/xPbww

Case Studies



U.S. DAM INTRUSION

In September 2013, an Iranian actor accessed a SCADA system interface associated with a U.S. dam

• Actors accessed the SCADA system, which was mechanically disabled for maintenance	• Demonstrates ICS complexity leveraging the Open Platform Communications protocol
• System required no login	• Unclear if dam was targeted or dam was a target of opportunity

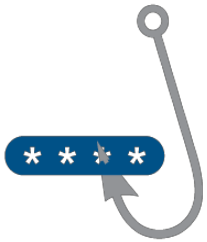
Case Studies

UKRAINE CYBERATTACKS

Demonstrated concerted effort and capabilities by actors to leverage ICS attacks

INVESTIGATE

U.S. Government interagency team (DOE, FBI, DHS, E-ISAC) traveled to Ukraine to investigate



SPEAR PHISHING

Attackers used spear phishing to steal credentials, which they leveraged in connecting company VPN and remote desktop software to manipulate HMI controls

RESTORED POWER

Power was restored within 4-6 hours by switching to manual control.

ATTACKS

The attacks demonstrated extensive preparation and coordination but limited technical sophistication

CISA CYBER+INFRASTRUCTURE

Case Studies

UKRAINE CYBERATTACKS

First known cyberattacks on civilian infrastructure

2015 ATTACK

- BlackEnergy malware used for recon
- Six-month dwell time
- Credential harvesting
- Actual impact done via manual takeover
- Malicious firmware used
- Attacks on UPS/PBX

2016 ATTACK

- CRASHOVERIDE framework used
- Impact could have been automated
- Unclear why it was not more widespread
- Serial communication modules
- Infection vector is unknown

CISA CYBER+INFRASTRUCTURE

https://go.usa.gov/xPbww

Case Studies

Russian Activity Against ENERGY SECTOR

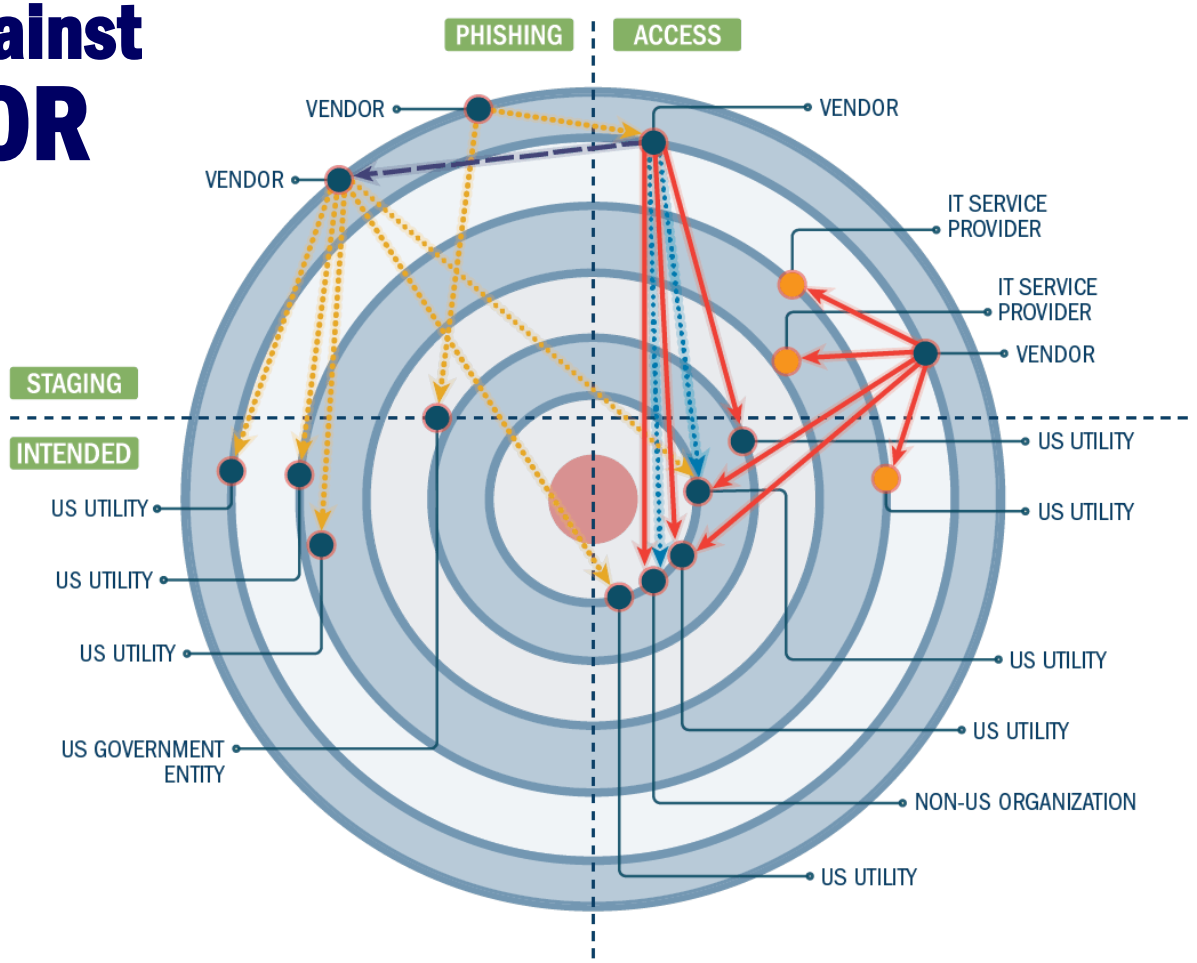
Russian government actors targeting U.S. Government entities and organizations in the Energy, Nuclear, Water, Aviation, and Critical Manufacturing critical infrastructure sectors

- Hundreds of victims targeted or impacted by this campaign
- Campaign targeted smaller entities with trusted relationships to obtain access to true victims
- Campaign end goal appears to have been ICS system accesses

CISA CYBER+INFRASTRUCTURE

Case Studies

Russian Activity Against ENERGY SECTOR



CISA
CYBER+INFRASTRUCTURE

Case Studies

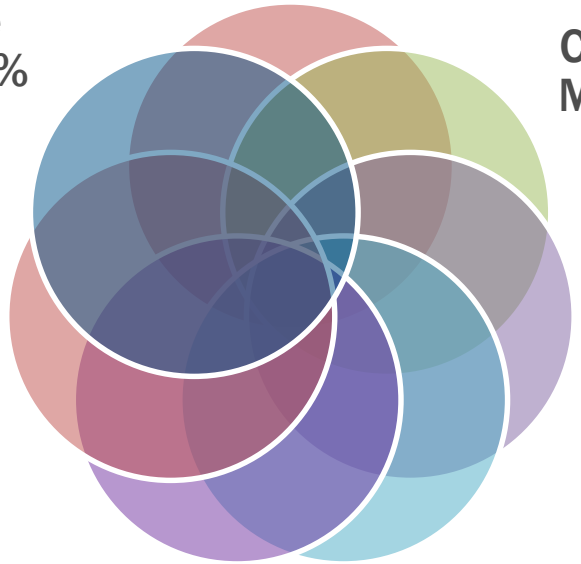
TRITON/TRISIS/HATMAN

Malware amplification attacks designed to cause physical damage, including include loss of life

- Sophisticated malware with low-level interaction with firmware
- Designed to be used in conjunction with other activity

Mitigations

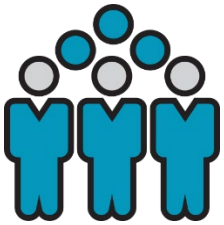
INCIDENT RESPONSE ROOT CAUSE ANALYSIS



https://go.usa.gov/xPbwU

Key Takeaways for Leaders

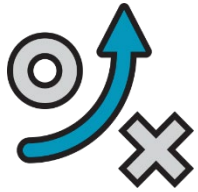
LEAD THE CHARGE



CYBER IS NOT TECHNICAL BUT PEOPLE

PREPARE AND EXERCISE

INCENTIVISE POSITIVE OUTCOMES



REORIENT ON TACTICS VS. INDICATORS

CISA

CYBER+INFRASTRUCTURE