The Rising Tide
Threats to Industrial Control Systems
INFOWARCON 2018

Joe Slowik
Dragos, Inc. | October 2018
Agenda

1. ICS in Context
2. High Profile Attacks
3. Current Operations
4. Future Expectations
WHOAMI - ICS Defender!
...But on My Terms!
What is ICS?

Industrial Control Systems (ICS): A term used to encompass the many applications and uses of industrial and facility control and automation systems. ISA-99/IEC 62443 is using Industrial Automation and Control Systems (ISA-62443.01.01) with one proposed definition being “a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.” The following table includes just a few of the ICS-related applications and labels we use.

What ICS is NOT

http://www.a2n.net/site/wp-content/uploads/2017/03/IoT_04.png
What is an ‘Attack’?

- Focusing specifically on ICS context:
  - Event that degrades, disrupts, or destroys an ICS process
  - Preparatory actions to an attack
  - Separate from IT-specific impacts
- General reconnaissance, intelligence gathering, and IP theft are separate concerns
Not ICS Attacks

Meet GreyEnergy, the newest hacking group hitting Ukraine's power grid

U.S. to blame Iran for cyber attack on small NY dam: sources

Shipping company Maersk says June cyberattack could cost it up to $300 million

- Maersk has put in place “different and further protective measures” following the attack.
- Maersk and ROP were among the companies that were also affected by NotPetya.

WASHINGTON (Reuters) - The Obama administration is planning to publicly blame Iranian hackers for a 2013 cyber attack against a small dam in New York state, three sources familiar with the matter told Reuters.
ICS Interest Over Time

1998 - 2009
- Lack of Collection
  - Campaigns: APT1
  - ICS Malware: None

2010 - 2012
- New Interest in ICS
  - Campaigns: Sandworm
  - ICS Malware: Stuxnet

2013 - 2015
- Campaigns Target ICS
  - Campaigns: Dragonfly
  - ICS Malware: BlackEnergy 2 and Havex
  - First attack to cause physical destruction on civilian infrastructure (German Steel)

2015-2017
- Adversaries Disrupt ICS
  - Campaigns: 10 Unique
  - ICS Malware: CRASHOVERRIDE and TRISIS
  - First and second ever electric grid attacks that disrupt power
  - First malware to target human life
ICS Attacks & Malware in Context

ICS-Focused Malware

- STUXNET
- HAVEX
- BLACKENERGY2
- CRASHOVERRIDE
- TRISIS

ICS Disruptive Events

- 2005-2010 (?): STUXNET
- 2014: German Steel Mill Attack
- 2015: Ukraine BLACKENERGY3
- 2016: Ukraine CRASHOVERRIDE
- 2017: Saudi Arabia TRISIS

Disruptive/Destructive Malware

- STUXNET
- CRASHOVERRIDE
- TRISIS
### ICS Threat Evolution

<table>
<thead>
<tr>
<th>Malware</th>
<th>Context</th>
<th>Attacks</th>
<th>Operations</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>STUXNET</td>
<td>Automated spread and impact</td>
<td>• Automated information gathering, manual deployment</td>
<td>• No “effects” portion</td>
<td></td>
</tr>
<tr>
<td>Havex</td>
<td>Automated spread and impact</td>
<td>• Automated information gathering, manual deployment</td>
<td>• No “effects” portion</td>
<td></td>
</tr>
<tr>
<td>BlackEnergy2</td>
<td>Automated spread and impact</td>
<td>• Automated information gathering, manual deployment</td>
<td>• No “effects” portion</td>
<td></td>
</tr>
<tr>
<td>BlackEnergy3</td>
<td>Automated spread and impact</td>
<td>• Automated information gathering, manual deployment</td>
<td>• No “effects” portion</td>
<td></td>
</tr>
<tr>
<td>CRASHOVERRIDE</td>
<td>Automated spread and impact</td>
<td>• Automated information gathering, manual deployment</td>
<td>• No “effects” portion</td>
<td></td>
</tr>
<tr>
<td>TRISIS</td>
<td>Automated spread and impact</td>
<td>• Automated information gathering, manual deployment</td>
<td>• No “effects” portion</td>
<td></td>
</tr>
</tbody>
</table>
More Aggressive Attacks → Greater Risk Tolerance → Pursuit of Physical ICS Attacks → Heightened Danger to Companies
Headline Attacks

2016: CRASHOVERRIDE
- Evolution in Ukraine Attacks
- ICS Manipulation via Malware

2017: TRISIS
- First Known Case Targeting Safety Systems
- Accepts Risk to Human Life
Ukraine's power outage was a cyber attack: Ukrenergo

KIEV/MILAN (Reuters) - A power blackout in Ukraine’s capital Kiev last month was caused by a cyber attack and investigators are trying to trace other potentially infected computers and establish the source of the breach, utility Ukrenergo told Reuters on Wednesday.
CRASHOVERRIDE Malware

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID
Hackers halt plant operations in watershed cyber attack

Jim Pinkle

(Reuters) - Hackers likely working for a nation-state recently invaded the safety system of a critical infrastructure facility in a watershed attack that halted plant operations, according to cyber investigators and the firm whose software was targeted.
Trisis Rootkit

Trisis has the security world spooked, stumped and searching for answers
Beyond Disruptive & Destructive

ICS Operations are not “Bolts from the Blue”

Attacks Require Capability Development

Delivery Requires Access

Execution Demands Control
Orienting to Kill Chain

**PHASE 1 - IT**
- Reconnaissance
- Weaponization
- Targeting
- Delivery
- Exploit
- Install / Modify
- C2
- Act

**PHASE 2 - ICS**
- Develop
- Test
- Deliver
- Install / Modify
- Execute ICS Attack

**CONTEXT**
**ATTACKS**
**OPERATIONS**
**FUTURE**
Tracking Adversaries by Behavior

Adversary

Activity Group

Infrastructure  Capability

Victim / Target

CONTEXT  ATTACKS  OPERATIONS  FUTURE
Initial Access & Recon

CONTEXT  ATTACKS  OPERATIONS  FUTURE
Initial Access & Recon

• Stage 1 Kill Chain activity
• Pre-requisite for Stage 2 operations
• Focus on:
  • Identifying access to ICS environment
  • Determining target technologies and attack surface
## CHRYSENE Oil & Gas Targeting

<table>
<thead>
<tr>
<th>Relationship</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SHAMOON</strong></td>
<td>• Code Overlap with Shamoon Activity</td>
</tr>
<tr>
<td></td>
<td>• Relationship with Disruptive Attacks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Profile</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeting</strong></td>
<td>• Largely Focused on Middle East</td>
</tr>
<tr>
<td></td>
<td>• Indications of Targeting Expansion to North America</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intentions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goals &amp;</strong></td>
<td>• Information Gathering and Establishing Access</td>
</tr>
<tr>
<td><strong>Intentions</strong></td>
<td>• Can be Used for Future Disruptive Attacks</td>
</tr>
</tbody>
</table>

### Context

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Operations</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Experts: North Korea Targeted U.S. Electric Power Companies

RASPITE Grid Investigation

Iran-Linked RASPITE Group Targets U.S. Electric Utilities

CONTEXT

ATTACKS

OPERATIONS

FUTURE
ICS Survey and Development

CONTEXT | ATTACKS | OPERATIONS | FUTURE
ICS Survey and Development

• Initial Stage 2 Kill Chain activity
• ICS environment accessed
• Focus on:
  • Enumerating ICS environment
  • Prerequisite to attack development and deployment
U.S. officials say Russian government hackers have penetrated energy and nuclear company business networks.
Alert (TA18-074A)
Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018
US & UK Electric Grid Probing

Advisory: Hostile state actors compromising UK organisations with focus on engineering and industrial control companies

Created: 05 Apr 2018
Updated: 05 Apr 2018
# Sustained Campaigns

<table>
<thead>
<tr>
<th></th>
<th>DRAGONFLY</th>
<th>DYMALLOY</th>
<th>ALLANITE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active</strong></td>
<td>2013-2014</td>
<td>Late 2015 – ?</td>
<td>Mid 2017 - ?</td>
</tr>
<tr>
<td><strong>Target Geography</strong></td>
<td>Europe, North America</td>
<td>Turkey, Europe, North America</td>
<td>USA, UK</td>
</tr>
<tr>
<td><strong>Infection Vector</strong></td>
<td>Phishing w/PDF, Watering Hole, Trojanized Software</td>
<td>Phishing w/Doc</td>
<td>Phishing w/Doc, Watering Hole</td>
</tr>
<tr>
<td><strong>Persistence Mechanism</strong></td>
<td>HERIPLOR, KARAGANY Malware</td>
<td>Various Malware and Backdoors</td>
<td>Create User Accounts, Credential Harvesting</td>
</tr>
<tr>
<td><strong>ICS Impact</strong></td>
<td>OPC-focused Malware Family</td>
<td>Survey and Screenshots via Malware</td>
<td>Survey and Screenshots via System Tools</td>
</tr>
</tbody>
</table>

**Context** | **Attacks** | **Operations** | **Future**
ICS Attack Capable

CONTEXT    ATTACKS    OPERATIONS    FUTURE
ICS Attack Capable

- Final Stage 2 Kill Chain ICS impact
- Environment is reasonably known
- Attack developed and in place
- Execution of disruptive/destructive attack
XENOTIME Attack Development

Trisis masterminds have expanded operations to target U.S. industrial firms
A Russian-owned research institute very likely helped build tools used by an infamous hacking group that caused a petrochemical plant in Saudi Arabia to shut down last year, cybersecurity company FireEye said Tuesday.
Where Do We Go from Here?

http://abcnews.go.com/images/US/abc_texas_chemical_fire_ll_111003_wblog.jpg
Smaller Nation State Attacks: A Growing Cyber Menace
Greater Adversary Risk Tolerance

- Shift to Disruptive/Destructive Attacks
- Acceptance of Physical Damage
- Extension of Attacks to Safety Systems
- Acceptance of Human Loss
ICS Attacks as Strategic Messaging

https://alochonaa.files.wordpress.com/2014/03/ukraine.png


CONTEXT | ATTACKS | OPERATIONS | FUTURE
Concerns in ICS Targeting

- Potential for Errors and Mistakes
- Miscalculation and Control of Events
- Indeterminate Response and Proportionality
- Physical Disruption Equating to Physical Attack
Expectations

- More Attacks to Come
- Greater Likelihood of Physical Destruction
- Increased Threat Adversary Activity
- Possibility Initial Access and Info Gathering Results in Accident
Further Reading

- An Abbreviated History of Automation & Industrial Controls Cyber Security – SANS Institute
- Analysis of the Cyber Attack on the Ukrainian Power Grid – SANS Institute
- Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors – US-CERT
- Dragonfly: Cyberespionage Attacks Against Energy Suppliers – Symantec
- Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group – Symantec
- CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations – Dragos
- TRISIS Malware: Analysis of Safety System Targeted Malware – Dragos
- Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Dragos
- Industrial Control System Threats Year in Review, 2017 – Dragos
- Attackers Deploy New ICS Attack Framework “TRITON” – FireEye
Questions?

@jfslowik
jslowik@dragos.com
dragos.com / pylos.co