Evolution of ICS Attacks
From BlackEnergy3 to TRISIS

SANS ICS Summit 2019

Joe Slowik / @jfslowik
Dragos, Inc. | March 2019
WHOAMI

Student

Officer

Network Defender

ICS Defender

Dragos
Safeguarding Civilization
Agenda

- Defining “Attack”
- Overview of Events:
  - 2015 Ukraine
  - CRASHOVERRIDE
  - TRISIS
  - US/UK Grid Intrusions
- Lessons Learned
- Future Expectations
ICS Cyber Kill Chain

Stage 1

- Reconnaissance
- Weaponization
- Targeting
- Delivery
- Exploit
- Install / Modify
- C2
- Act

Stage 2

- Develop
- Test
- Deliver
- Install / Modify
- Execute ICS Attack

ATTACKS  EXAMPLES  LESSONS  FUTURE
What does “Attack” Mean?

- Emphasis on:
  - Deny
  - Degrade
  - Destroy
- OR – preparatory actions leading to the above
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

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 Events

Recon & Initial Access

Many Attempts

Few Examples

Deny, Degrade, Destroy
INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

Cyberattack on Ukraine grid: here’s how it worked and perhaps why it was done
January 25, 2016 5:53am EST

TLP: White
Analysis of the Cyber Attack on the Ukrainian Power Grid
Defense Use Case
March 18, 2016
2015 Methodology

1. Phishing to Gain Access to IT Network
2. BLACKENERGY3 Deployed to Gather Information and Maintain Access
3. Pivot to ICS via Stolen Credentials
4. Manual Interaction with HMIs to Produce ICS Impact, KillDisk Deployed to Prolong Effect
BLACKENERGY begins as a criminal DDoS tool

BLACKENERGY2 extended to directly compromise HMI’s

BLACKENERGY3 built to harvest credentials to enable follow-on actions

BLACKENERGY3 ICS use leverages IT-OT dependencies and connections for intrusion
2015 Attacker Tradecraft

Stage 1
- Custom malware deployed for initial infection and persistence
- BLACKENERGY3 used to harvest credentials and network information

Stage 2
- OT environment accessed via harvested credentials
- ICS impact achieved through access to HMIIs
- Malware deployed only to inhibit recovery
### 2015 Ukraine Evaluation

#### What Worked

- Successfully penetrated ICS
- First known power event triggered via cyber

#### What Could Have Been Better

- Attack does not scale
- Initial actions effective, but easy to build defenses around

<table>
<thead>
<tr>
<th>ATTACKS</th>
<th>EXAMPLES</th>
<th>LESSONS</th>
<th>FUTURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Worked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What Could Have Been Better</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Ukrainian Power Grid Hacked Again

Experts say the country appears to "testbed" for cyber attacks that could ripple around the world.
CRASHOVERRIDE Attack

Launcher
- Start
  - Select Payload
  - Initiate ICS Impact

Payload Execution
- Connect to Control Systems
- Manipulate State

Wiper
- Wait for Timer
- Delete Files, Remap Services, Reboot System

Post-Attack
- Leave behind “Backup” Backdoor
- SIPROTEC DDoS (Fail)
## Enabling Factors

<table>
<thead>
<tr>
<th>Long-Term Network Access</th>
<th>Insecure Environment</th>
<th>‘Flat’ Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Harvesting credentials over long periods</td>
<td>• Weak authentication mechanisms</td>
<td>• Central points of access (historians) to all ICS-</td>
</tr>
<tr>
<td>• Able to perform reconnaissance and survey</td>
<td>• Re-used credentials</td>
<td>managing hosts of interest</td>
</tr>
<tr>
<td>environment</td>
<td>• Older operating systems on critical devices</td>
<td>• Easy to move from IT to OT network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ATTACKS**

**EXEMPLARY**

**LESSONS**

**FUTURE**
CRASHOVERRIDE Tradecraft

**Stage 1**
- Credential capture
- Native Windows commands and scripts

**Stage 2**
- Malicious service creation with timer
- ICS manipulation coded in malware
### CRASHOVERRIDE Evaluation

<table>
<thead>
<tr>
<th>What Worked</th>
<th>What Could Have Been Better</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Again penetrated ICS, produced impact</td>
<td>• Attack was very immature</td>
</tr>
<tr>
<td>• Framework developed to scale attacks</td>
<td>• Tools still in development stage</td>
</tr>
<tr>
<td></td>
<td>• Attack looks like a ‘test’</td>
</tr>
</tbody>
</table>
Threat Research

Attackers Deploy New ICS Attack Framework “TRITC” and Cause Operational Disruption to Critical Infrastructure

December 14, 2017 | by Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer

TRISIS Malware
Analysis of Safety System Targeted Malware

A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.
Gain access to and harvest credentials from IT network (Mimikatz)

Leverage multiple open- or commercial-source tools for post-exploitation (WMImplant, Cobalt Strike)

Utilize remote access to OT network via stolen credentials

Continue pivoting through network via credential capture

Gain sufficient access to SIS to deploy TRISIS
# TRISIS Event Questions

<table>
<thead>
<tr>
<th>Media, General Infosec Companies</th>
<th>ICS Security Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>• WHO DID IT ???</td>
<td>• What was the intention/purpose?</td>
</tr>
<tr>
<td>• Where will this entity strike next?</td>
<td>• What are implications of targeting SIS?</td>
</tr>
</tbody>
</table>
**TRISIS Tradecraft**

**Stage 1**
- Credential capture
- Publicly- and commercially-available toolsets

**Stage 2**
- Continuous credential capture and pivoting via same Stage 1 tools
- Develop and deploy victim-specific SIS rootkit
**TRISIS Evaluation**

<table>
<thead>
<tr>
<th>What Worked</th>
<th>What Could Have Been Better</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Yet again penetrated ICS, produced impact</td>
<td>• Event did not appear to succeed</td>
</tr>
<tr>
<td>• Expanded scope of possible targets for disruption to SIS</td>
<td>• TRISIS is very ‘brittle’ – only directly applicable to identical environments</td>
</tr>
</tbody>
</table>

**ATTKACS** | **EXAMPLES** | **LESSONS** | **FUTURE**
2016+ US/UK Utility Intrusions

U.S. officials say Russian government hackers have penetrated energy companies

German intelligence sees Russia behind hack of energy firms: media report

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
Indirect Intrusion Methodology

- Select Utility Targets
- Identify Contractors, Vendors, and Other Third Parties
- Compromise Third Parties
- Utilize Trusted Relationship to Enable Access to Utility Targets
Methodology - Phishing

- Identify Contractors and Vendors for Targets
- Phish Contractors/Vendors to Gain Access to Their Networks
- Leverage Trusted Party Access to Phish Ultimate Targets
- Remotely Authenticate to Network
- Harvest Credentials via Information Leakage from Phish
- Phish Electric Utility Companies
- Continue to Harvest Credentials
- Pivot to ICS Network via Captured Credentials
- Utilize Native System Tools to Gather Information
Attack Focus and Purpose

Enable ICS Access
- Identify VPN/Remote Access Links
- Capture Credentials

Gather ICS Information
- Network Enumeration and Survey
- Capture Control System-Specific Information

Execute Attack
- ?

ATTACKS   EXAMPLES   LESSONS   FUTURE
### Grid Intrusion Targeting

<table>
<thead>
<tr>
<th>Known Victims</th>
<th>Probable Victims</th>
<th>Emerging Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>• United States</td>
<td>• Germany</td>
<td>• Ukraine</td>
</tr>
<tr>
<td>• United Kingdom</td>
<td>• Switzerland?</td>
<td>• Poland?</td>
</tr>
<tr>
<td>• Ireland?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ATTACKS**  **EXAMPLES**  **LESSONS**  **FUTURE**
**Grid Intrusion Methodology**

**Stage 1**
- Phishing and strategic website compromise to enable initial access
- Extensive credential harvesting (Mimikatz)

**Stage 2**
- Access OT via remote access through captured credentials
- Harvest information via system tools to build knowledge on victim networks and processes
- No (known) impact... yet?
Grid Intrusion Evaluation

What Worked

• AGAIN penetrated ICS
• Campaign leveraged combinations of publicly-available tools and techniques
• Provides an example of how to penetrate ICS without special tooling

What Could Have Been Better

• We’re not really sure yet!
Concerning Trends

More Aggressive Attacks → Greater Adversary Risk Tolerance → Pursuit of Physical ICS Attacks → Heightened Danger to Asset Owners
Tradecraft in ICS Attacks

Legacy (pre-2016)
- Custom Malware and Specific Tools
- Exploit Use for Movement and Access
- Manual Operations for ICS Impact

Current
- “Commodity” Techniques until ICS Attack
- Credential Theft and System Tool Use to Spread
- ICS Effects and Manipulation Codified in Software
### TTPs Shift through Kill Chain

<table>
<thead>
<tr>
<th>Initial Intrusion &amp; Lateral Movement</th>
<th>ICS-Specific Disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Leverage “Commodity” Tools</td>
<td>• Attacks are Unique to Target, Environment</td>
</tr>
<tr>
<td>• Deploy “Living off the Land” Techniques</td>
<td>• Requires Building Custom Attack Software</td>
</tr>
<tr>
<td>• Avoid Custom Tools and Tradecraft</td>
<td>• Little Scope for Direct Replay</td>
</tr>
</tbody>
</table>
Initial, Repeatable TTPs

Stage 1 - IT
- Reconnaissance
- Weaponization
- Delivery
- Exploit
- Install / Modify
- C2
- Act

Stage 2 - ICS
- Develop
- Test
- Deliver
- Install / Modify
- Execute ICS Attack

ATTACKS  EXAMPLES  LESSONS  FUTURE
Specialized, Unique Attacks

Stage 1 - IT

Stage 2 - ICS

ATTACKS

EXAMPLES

LESSONS

FUTURE
IT Security Problems with a Twist

The Wrong Lesson

• “Living off the land” prevalence means ICS security problems are just like IT
• Deploy and implement IT security in ICS environments, same tools and all!

The Right Lesson

• IT intrusion tradecraft extends to ICS
• Portions of IT defense must be embraced, but not all
• Effective defense requires knowing subtleties of operational networks (and their purpose)
“IT-ification” of ICS

Increased Efficiency and Cost Savings by Incorporating COTS Hardware/Software into ICS Equipment

Elimination of (some) custom environments, airgaps, and traditional separation from enterprise IT

Result: IT threat surface imported to IT environment – WITHOUT the same security capabilities
Perimeter Extension

Traditional ICS Perimeter

Vendor and Contractor Access

Increased Remote Work and Administration

Cloud and Off-Prem Products
Increased vendor interest in ICS space

Attempt to leverage “IT-ification” as justification to extend existing IT products to industrial

Fails to recognize operational and technical differences in how IT technologies are deployed for industrial use
Almost no Observed Use of “Zero Days”*

Most Targeted Vulnerabilities are Windows, not ICS

Use of Publicly-Available Attack Tools, Rarely Custom Software EXCEPT Final Attack
STUXNET is first known and most complex ICS malware. Subsequent events leverage some use of vulnerabilities. Most-recent attacks rely on underlying network insecurity and connectivity. ICS capability codified in software for final actions.
Preparation and Dwell Time

Initial Intrusion
- Breach IT
- Expand into ICS

Dwell Time
- Maintain Access
- Continuous Data Gathering

Event Execution
- Leverage Access
- Execute Disruptive Event
**Defense through the Kill Chain**

<table>
<thead>
<tr>
<th>Initial Intrusion &amp; Lateral Movement</th>
<th>ICS-Specific Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Greater visibility required</td>
<td>• Tools will be purpose-built with little overlap</td>
</tr>
<tr>
<td>• Ability to filter out malicious from ‘anomalous’</td>
<td>• AV and similar approaches will not work</td>
</tr>
<tr>
<td>• Learning the network</td>
<td>• Need visibility into fundamental ICS processes</td>
</tr>
</tbody>
</table>

- ATTACKS
- EXAMPLES
- LESSONS
- FUTURE
The Next Attack

- Little or No Custom Malware in Initial Intrusion
- Transition from “Access” to “Effects” Team when ICS Breached
- Custom Malware Deployed Codifying ICS Knowledge in Software
- Increasing Reliance on IT Concepts and Equipment Magnifies ICS Impact

ATTACKS  EXAMPLES  LESSONS  FUTURE
References & Resources

• CRASHOVERRIDE – Dragos (https://dragos.com/blog/crashoverride/CrashOverride-01.pdf)
• TRISIS – Dragos (https://dragos.com/blog/trisis/TRISIS-01.pdf)
• Analysis of the Cyber Attack on the Ukrainian Power Grid – SANS (https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf)

Questions?

@jfslowik
jslowik@dragos.com