Exposed and Vulnerable Critical Infrastructure

Energy & Water Industries

Numaan Huq
Sr. Threat Researcher
Trend Micro Research
Introductions are in order...
This is how hackers can take down our critical energy systems through the Internet

Human Interface Systems lacking any kind of security have the potential to cause serious damage to critical services worldwide.

By Charlie Osborne for Zero Day | October 30, 2018 -- 12:00 GMT (12:00 GMT) | Topic: Security

Industrial operations rely on Human Interface Operators to access SCADA systems.

We rely on a plethora of industrial services including clean and sewage water facilities and energy services in our daily lives.
People tend to call anything related to ICS as “SCADA”

• ICS has many components including:
  – **Sensors & Actuators** – sensors, valves, motors, etc.
  – **PLC** – the main controller for the sensors & actuators
  – **HMI** – GUI application for supervising and controlling processes
  – **Data Historian** – centralized database for logging all process data
  – **IED** – smart sensors & actuators that can perform local processing & control
  – **Fieldbus Network** – links sensors & actuators to a PLC or other controllers
  – **RTU** – special unit designed to support remote stations
  – **MTU** – acts as the master in a SCADA system
ICS Basic Operations

(Source: NIST Guide to Industrial Control Systems (ICS) Security 800-82, Section 2.2, Figure 2-1)
SCADA Network

(Source: NIST Guide to Industrial Control Systems (ICS) Security 800-82, Section 2.4, Figure 2-2)
DCS Network

(Source: NIST Guide to Industrial Control Systems (ICS) Security 800-82, Section 2.5, Figure 2-7)
Communications in ICS Networks

<table>
<thead>
<tr>
<th>Trend Micro Detection Name</th>
<th>Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE_SALITY.RL</td>
<td>872,308</td>
</tr>
<tr>
<td>VBS_RAMNIT.SMC</td>
<td>382,230</td>
</tr>
<tr>
<td>TROJ_STARTER.SM</td>
<td>124,668</td>
</tr>
<tr>
<td>Ransom_WCRY.SM2</td>
<td>73,548</td>
</tr>
<tr>
<td>TROJ_DOWNADJOB.A</td>
<td>46,655</td>
</tr>
<tr>
<td>PE_RAMNIT.H</td>
<td>28,612</td>
</tr>
<tr>
<td>JS_NIMDA.A-1</td>
<td>26,638</td>
</tr>
<tr>
<td>TROJ_EQUATED.J</td>
<td>25,622</td>
</tr>
<tr>
<td>PE_RAMNIT.DEN</td>
<td>24,821</td>
</tr>
<tr>
<td>PACP_CORRUPTPE.STD</td>
<td>20,467</td>
</tr>
<tr>
<td>PUA_Dexon</td>
<td>19,955</td>
</tr>
<tr>
<td>PE_SALITY.ER</td>
<td>12,141</td>
</tr>
<tr>
<td>PE_NESHTA.A</td>
<td>10,827</td>
</tr>
<tr>
<td>WORM_COINMINER.RT</td>
<td>9,614</td>
</tr>
<tr>
<td>LNK_BONDAT.SMA</td>
<td>9,110</td>
</tr>
<tr>
<td>WORM_COINMINER.SMG</td>
<td>8,238</td>
</tr>
<tr>
<td>WORM_COINMINER.QA</td>
<td>7,546</td>
</tr>
<tr>
<td>TROJ_EQUATED.G</td>
<td>7,433</td>
</tr>
<tr>
<td>WORM_MESSEN.SMF</td>
<td>6,133</td>
</tr>
<tr>
<td>PE_Chir.B</td>
<td>5,853</td>
</tr>
</tbody>
</table>
Targeting Energy

• On Dec 24, 2015, Ukrainian companies experienced unscheduled power outages impacting 225,000+ customers
  – Caused by external malicious actors
  – Multiple coordinated attacks within 30 minutes of each other
• Used remote administration tools and/or remote ICS client software used to control circuit breakers
• Used KillDisk to overwrite Windows based HMI systems
  – Disrupt restoration efforts
Ukrainian Power Grid Attack-I

1. Spear phishing Email (BlackEnergy3)

2. BlackEnergy3 connected to C&C, and hacker stole credentials from business network

3. Use VPN remote access to ICS network

4. Use existing remote access tools (simulate operator HMI) command remote station

5. Uploaded the malicious firmware to the serial-to-ethernet gateway devices

6. Use modified KillDisk to erase the master boot record of impacted organization systems

7. Utilizing UPS systems to impact connected load with a scheduled service outage
Ukrainian Power Grid Attack-II
What is an HMI?

- **Human Machine Interface**
- Main hub for managing and operating control systems
- Collects data from the control systems
- Presents visualization of the system architecture
- Alarms operator/sends notifications
- Should be operated on isolated and trusted networks
  - ... but usually isn’t!

(Source: http://comfiletech.com/hmi/cha-070pr-7-open-frame-human-machine-interface-hmi/)
Why target HMIs?

• Control the targeted critical infrastructure
• Harvest information about system architecture
• Disable or deceive the alarm and notification systems
• Physically damage SCADA equipment
Malware Targeting HMI

• Stuxnet
  – First malware created to target ICS environment
  – Abused vulnerabilities
    • Siemens SIMATIC STEP 7 DLL Hijacking Vulnerability (ICSA-12-205-02)
    • Siemens WinCC Insecure SQL Server Authentication (ICSA-12-205-01)

• Black Energy
  – Ongoing sophisticated malware campaign compromising ICS environments
  – Abused vulnerabilities
    • GE CIMPLICITY Path Traversal Vulnerabilities (ICSA-14-023-01)
    • Siemens WinCC Remote Code Execution Vulnerability (ICSA-14-329-02D)
    • Advantech WebAccess (ICS-ALERT-14-281-01B)
Internet Scanning

GeoStalking
Drinking From the Caffeine Firehose

We call SHODAN.

By Viss!

Prepared for Defcon 20
List of pumped power plants in Japan, map ranking

GeoStalking
Ports

21  80  81  82  83  84  8080  9600  44818
HMI Vulnerability Statistics

- Memory corruption: 20.44%
- Credential management: 18.98%
- Lack of authentication/authorization and insecure defaults: 23.36%
- Code injection: 8.76%
- Others: 28.46%
HMI Vulnerability Statistics

- 2013: 158 vulnerabilities
- 2014: 124 vulnerabilities
- 2015: 158 vulnerabilities
- 2016: 143 vulnerabilities

Bar chart showing the number of vulnerabilities per year from 2013 to 2016.
Ransomware

DDoS Extortion

Permanent Bots

Beachhead

Destructive
Shodan and Censys. Search engines of vulnerabilities. In this article, consider two interesting search engines [Only registered users can see links](http://www.shodan.io) and [Only registered users can see links](http://www.censys.io), which allow you to get a list of interesting information. In this way, you can access servers, webcams, printers, routers, smart home systems, etc. Shodan and Censys. Use of search engines. These are search engines that look for connected devices to the network and check them for popular vulnerabilities. The engines of these search engines work around the clock and add millions of different devices every month. There were cases when they found control systems for nuclear power plants and heating and heating systems for various facilities. This information can cause significant harm. Remember that unauthorized interference in the operation of systems is criminal. Therefore, the materials are provided for informational purposes only.
We buy vulnerabilities discovered by you in routers and IoT devices (web cameras, set-top boxes, TVs, etc.). Consider any offers for remuneration, but the final amount will depend on the number of available devices on the network (shodan, censys) and on the type of vulnerability (preference will be given to RCE, wired by manufacturers of logins / passwords, bookmarks and other vulnerabilities that allow executing code on the device).

Contacts for communication - johnwoodman7 @ protonmail.com and tracert0ng777 @ gmail.com

Good day to all. interest 0-day vulnerability in the SCADA-system. Ready to pay well to someone who can help 😊

JID: [Only registered users can see links. Зарегистрироваться.]
I will sell the base of one of the leading branches of the big city. Personal and corporate phones, corporate mail. The list includes all management staff, specialists, managers. 15 cities of Russia, 850 positions. In 3 hands, the deal through the guarantor. Details in HP.
Vulnerable IT-OT Network
ICS Network Defense

(Source: Cisco)

(Source: DHS. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies)
ICS Network Defense

1. Network Segmentation
2. Remote Access
3. Wireless Communications
4. Patch Management
5. Access Policies & Control
6. System Hardening
7. Intrusion Detection
8. Physical & Environmental Security
9. Malware Protection & Defense
10. Awareness
11. Periodic Assessment & Audits
12. Change Control & Configuration Management
13. Incident Planning & Response

(Source: DHS. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies)
Feedback from E&W Stakeholders

• Security awareness is much harder when trying to reach the “guys with wrenches” vs. people in the office

• Having a good inventory is a key baseline – everyone struggles with this, especially during mergers/acquisitions

• Lots of PLC with no authorization at all – it’s a mess

• Few targeted ICS attacks right now – skillset means it is only researchers or nation states

• Sees a lot of knock on effects – hit by non-targeted ransomware and ends up losing access to the HMI

• Bulk of OT systems run on Windows; can only upgrade if vendor signs off first
Feedback from E&W Stakeholders

- The 3 biggest cyber risks to the Energy sector – compromised SIS (Safety Instrumentation Systems), Ransomware, and Industrial espionage
- Seizure of a PLC for disruption not biggest concern – more worried about extortion, short selling stocks, espionage, manipulation of process output
- If the target of interest to a country is for defensive reasons, they will stop at nothing until they get in using a combination of cyber, HUMINT, and spy craft
- If the target of interest is for commercial gain, then it is possible to stop the attack. By eliminating all of the basic security issues and having solid baseline in place, you are raising the financial cost of the attackers
- Supply Chains are increasingly complex, critical, and at risk
numaan_huq@trendmicro.com
@nmnahuq