**DoD Terminology Decision In Progress:**

- PIT = Platform Information Technology
- CS = Control Systems
- PIT-CS = PIT Control Systems
- ICS = Industrial Control Systems
- OT = Operational Technology
- SCADA = Supervisory Control And Data Acquisition
- CPS = Cyber Physical Systems
- IoT = Internet of Things
- IIoT = Industrial IoT

Typically Lack Any Cyber Defenses; ~75% Use WIN XP
Same Commercial Devices Installed Across DoD Enterprise
Top 20 Attacks from Least to Most Sophisticated

1. ICS Insider
2. IT Insider
3. Common Ransomware
4. Target Ransomware
5. Zero-Day Ransomware
6. Ukrainian Attack
7. Sophisticated Ukrainian Attack
8. Market Manipulation
9. Sophisticated Market Manipulation
10. Cell-phone WIFI
11. Hijacked Two-Factor
12. IIoT Pivot
13. Malicious Outsourcing
14. Compromised Vendor Website
15. Compromised Remote Site
16. Vendor Back Door
17. Stuxnet
18. Hardware Supply Chain
19. Nation-State Crypto Compromise
20. Sophisticated Credentialed ICS Insider

What’s in Your ‘Smart Building?’

- “Smart” / High Performance Green Buildings
  - Since 2005 ~7,000+
  - Example: 5,000 desks, 20 floors, ~2M sqft

- Fire Sprinkler System
- Interior Lighting Control
- Intrusion Detection
- Land Mobile Radios
- Renewable Energy
- Photo Voltaic Systems
- Shade Control System
- Smoke and Purge
- Physical Access Control
- Vertical Transport System (Elevators and Escalators)
- Advanced Metering Infrastructure
- Building Automation System
- Building Management Control
- CCTV Surveillance System
- CO2 Monitoring
- Digital Signage Systems
- Electronic Security System
- Emergency Management System
- Energy Management System
- Exterior Lighting Control Systems
- Fire Alarm System

3 Networks Independently Managed
Significant Impacts; Tools Easily Accessible and Unsophisticated

- **WannaCry** *(May’17)* – ransomware affecting Microsoft Windows millions of computers across 150 countries, halting manufacturing, transportation and telecommunications systems; many medical systems inoperable affecting health & safety

- **NotPetya** *(Jun’17)* – malware infected 10,000’s of internet connected systems across 65 countries [Maersk shipping company halted operations in most of its 76 port terminals; loses exceeded $300M, 4,000 new servers, 45,000 new PCs, 2,500 new apps]

- **Trisis** *(Aug’17)* – virus sabotaging physical safety mechanisms of Saudi Arabian oil, gas facility control systems [coding error prevented potential catastrophe]

Number Targeted Attacks Almost Doubled Since 2013; Urgent Need to Understand Your “Connectedness”
Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices

• 16 April 2018 – DHS US CERT, FBI & UK’s National Cyber Security Centre – Alert – Russian State-sponsored actors establishing worldwide cyber exploitation of network devices
• Targets primarily government and private-sector orgs, critical infrastructure providers & internet service providers.

Exploiting:
- Routers
- Switches
- Firewalls
- Network-based Intrusion Detection Systems

FBI - actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations.

Russian “Trolling” Activity

Up 2,000% After Syrian Strike

Make sure that your router software is up-to-date and its password is secure
Cyber Threat to ICS Highest Yet – CS Threats

Dragos Year in Review 2017 Report

- 72% Of Vulnerabilities Could Cause a Loss of View/Control
- 63% Of Vulnerabilities from Late in Kill Chain Indicating Prolonged Presence, Pivot from Other Systems
- 63% Of Vulnerabilities Could Be Leveraged to Gain Initial Access Into Control Network

“We regrettably expect ICS operational losses and likely safety events to continue into 2018 and the foreseeable future”
April 2018 Report

Key findings over past 3 yrs:

• 90% of targeted attack groups are motivated by intelligence gathering

• Most active groups compromised an average of 42 organizations

• 71% of groups use spear-phishing emails as primary infection vector

• 29% increase of recorded ICS vulnerabilities

• U.S. accounts for 27% of all targeted attack activity (most)
• 60% have plain-text passwords traversing their control networks
• 50% aren’t running any AV protection
• Nearly 50% have at least one unknown or rogue device
• 20% have wireless access points
• 28% of all devices in each site are vulnerable
• 82% of industrial sites are running remote management protocols

“They’re testing out red lines, what they can get away with. You push and see if you’re pushed back. If not, you try the next step.” Thomas Rid, Professor of War Studies at King’s College London
Researchers Publish Default Passwords for 372 Industrial Control Systems (ICS) Devices

Executive Summary

- CRITIFENCE published the supervisory control and data acquisition (SCADA) Default Password Database (SDPD), a collection of default credentials for 372 products from 80 vendors.
- Default password databases and other open-source tools make it easier for malicious actors to target internet-connected industrial control systems (ICS).
- We encourage ICS asset owners to identify default passwords in their systems, particularly for connected devices listed in SDPD, and modify them where operationally feasible.

Threat Detail

Researchers Publish SCADA Default Password Database

CRITIFENCE, an industrial control systems (ICS) cyber security company, published the SCADA Default Password Database (SDPD), a collection of default credentials for 372 ICS products from 80 vendors.
Shodan

"default password"
Never Attribute Evil When Stupid is Still Available
Top 5 security weaknesses:

- 94% code tampering
- 59% insecure authorization
- 53% reverse engineering
- 47% insecure data storage
- 38% insecure communication

“Why should anyone have the power to control a 2 GW power plant, or the entire production line of an automobile factory, from a cell phone, while stopped at a traffic light?”

— Andrew Ginter, VP Industrial Security Waterfall Security Solutions
Vision: By **2023**, the Department of Homeland Security will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities.
Who Defends FRCS?

- “U.S. Cyber Command is not "optimized" today to combat information operations orchestrated by foreign powers”

- “NSA we're focused externally. Cyber Command we're largely focused externally. So I will monitor bots, infrastructure external to the U.S., but one of the phenomenon we're beginning to see is a migration of capabilities from external infrastructure — that we've been aware of and observing for some time — the way this is going to go next in my mind is you're going to see this in domestic manipulation. And that is a part now that no, I am not really involved with,” Rogers said. 16 May 2017 SASC Hearing

USCC’s Role Does NOT Include Securing ALL Control Systems
**DoD Budget $M**

- **IT / IS** 30,000,000,000
- **OT / CS** 150,000,000

**DoD # of Devices**

- **IT / IS** 8,000,000
- **OT / CS** 2,000,000,000
anonymous vice vlan hacking
rhanem youssef
5 years ago • 348 views

Mix - VLAN Hopping - Switch Spoofing Attack and Mitigation Tutorial

You Tube
VLAN Hopping - Switch Spoofing Attack and Mitigation Tutorial 2:10
MicroNugget: CAM Table Overflow Attack and How To Prevent It 8:49

High-tech car theft: How to hack a car (CBC Marketplace)

CBC News 2 years ago • 1,355,391 views
We go on the hunt for the mysterious device police believe those thieves are using to steal your car. To read more: http://www.cbc.ca

Watch thieves steal car by hacking keyless tech

CNNMoney 4 months ago • 112,327 views
Police in West Midlands, UK have released footage of criminals stealing a car by relaying a signal from the key inside the home, to
AFCEC Cybersecurity RFP Scope

- **Control System Enclave (CE)**
  - **Deployment & Sustainment**
  - **Enclave Design**
  - **Network Engineering**
  - **Integration Network Support**
  - **Materials Acquisition**
  - **RMF Package Development & Maintenance**
  - **System Deployments**
  - **Help Desk Support**
  - **Integration Project and Estimate Development 2-5/Month**
  - **CS Enclave Integration**

- **Large Base**
  - 14 CE CS/Year

- **Medium Base**
  - 7 CE CS/Year

- **Small Base**
  - 3 CE CS/Year

- **Investment and Technology Capability Requests 15-25/Year**

- **CE CS Design Review 2-4/Month**

- **CS Threat Awareness & Incident Response**
  - 50-70 Advisories/Month
  - 1 CE Health Report/Month
  - 4-6 Hours Monitoring/Day
  - 2-4 Hours Intrusion Detection/Day
  - > 1 Hour Forensics/Month
  - 4 Technical Docs/Yr

- **Network Engineering Help Desk Support**

- **Integration Network Support**

- **RMF Package Development & Maintenance**

- **System Deployments**

- **Help Desk Support**

UNCLASSIFIED
SCADA Security Scientific Symposium (S4) Target Network

- Corporate Zone
- Domain Controller
- FTP Server
- Windows 7 Workstation
- Windows XP Workstation
- BACnet Controller
- DMZ
- Advantech OPC Server
- Proficy Historian
- Control Zone
- iFix Server
- iFix HMI
- Schneider Electric Modicon PLCs
- Allen Bradley MicroLogix PLC
- ADAM Advantech PLC
Casino Hacked Via Thermometer

Thermometer in lobby aquarium hacked to pull high roller database to the cloud
April 26, 2018 – Innsbruck Australia Ski Lift control panel – accessible to anyone on the internet – could manipulate the lift’s speed, cable tension, & distance between passenger cabins.

- Use Shodan to discover and classify OT devices!
All use public information & network signatures for FICO score-like rating approximating relative risk

- Enables intelligence for evaluation of critical suppliers, vendors, and others in the industry

- Augments Business Intelligence Unit and Security Operations Center; quies alerts to potential cyber or physical threats to our supply chains and internal infrastructure

- Each vendor's approach & scores roughly similar

- Need to verify accuracy – may detect one or more notables that were not really present in the enterprise under evaluation (e.g. a sub-domain or IP address not really associated with the target)

- **Benefit / Objectives**: Credibility when approaching supplier/partner with a security issue; avoid false positives & decrease time to investigate and mitigate
UNCLASSIFIED

Bitsight Technologies' mission is to provide organizations with the insight they need to proactively identify, quantify, and mitigate security risk. The company's platform continuously collects and analyzes vast amounts of external evidence on security behaviors in order to help organizations make timely, data-driven risk management decisions. Based in Cambridge, MA, Bitsight Technologies was founded in 2011. For more information, please visit www.bitsighttech.com or follow Bitsight on Twitter @Bitsight.
Compromised Systems Details – 2,096 events over 12 months

Graph Type

Distribution

Duration

Volume

This graph displays the number of compromised systems events per month, broken down by type. The size of the bubbles corresponds to the average duration for those events.

Search

Show events from: MM-DD-YYYY to MM-DD-YYYY

Filter By Tags

<table>
<thead>
<tr>
<th>Type</th>
<th>Location</th>
<th>Start</th>
<th>End</th>
<th>Days</th>
<th>Details</th>
<th>collapse all</th>
<th>expand all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet Infections</td>
<td>RU</td>
<td>03-29-2018</td>
<td>03-29-2018</td>
<td>1</td>
<td>Infection: Ghokswa</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>Potentially Exploited</td>
<td>US</td>
<td>03-28-2018</td>
<td>03-28-2018</td>
<td>1</td>
<td>Infection: Grayware</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>Botnet Infections</td>
<td>RU</td>
<td>03-28-2018</td>
<td>03-28-2018</td>
<td>1</td>
<td>Infection: Pykspa</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>Botnet Infections</td>
<td>RU</td>
<td>03-28-2018</td>
<td>03-28-2018</td>
<td>1</td>
<td>Infection: Ghokswa</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>Botnet Infections</td>
<td>ES</td>
<td>03-28-2018</td>
<td>03-28-2018</td>
<td>1</td>
<td>Infection: Necurs</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>Botnet Infections</td>
<td>RU</td>
<td>03-27-2018</td>
<td>03-27-2018</td>
<td>1</td>
<td>Infection: Ramnit</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>Potentially Exploited</td>
<td>RU</td>
<td>03-27-2018</td>
<td>03-27-2018</td>
<td>1</td>
<td>Infection: Dealpy</td>
<td>Details</td>
<td></td>
</tr>
</tbody>
</table>
File Sharing category distribution

File Sharing events indicate the number of times in the past 60 days that file sharing activity occurred, sorted by torrent category. Each event represents one IP address sharing one torrent per day.

File Sharing – 401 events over the past 60 days
40 unique IPs observed

*Data which exceeds the chart is on a scale too large to display accurately with other categories in the space provided and has been shortened to fit.

<table>
<thead>
<tr>
<th>Category</th>
<th>Events</th>
<th>Unique Torrents</th>
<th>Unique IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>24</td>
<td>19</td>
<td>13</td>
</tr>
<tr>
<td>Books</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Games</td>
<td>14</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>Movies</td>
<td>313</td>
<td>96</td>
<td>26</td>
</tr>
<tr>
<td>Music</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>TV</td>
<td>10</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>Other</td>
<td>36</td>
<td>26</td>
<td>11</td>
</tr>
</tbody>
</table>
Best Practices to Cyber Secure Control Systems

Mission Assurance Senior Steering Group
Control Systems Working Group

• Develop Password Policies
• Security Awareness and Training
• Patch Management
• Maintenance Activities
• Modem Connection
• Network Design
• Securing Host Systems

Advanced Cyber Industrial Control System Tactics, Techniques, Procedures

Detection
• Routine Monitoring, Inspection, Identification of adversarial presence, Documentation, Notifications

Mitigation
• Protect the information network, Acquire and protect data for analysis, Maintain operations during an active attack

Recovery
• Identify mission priorities, Acquire and protect data for analysis, Systematically Recover each affected device, Systematically reintegrate devices, processes, and network segments, Test and verify system to ensure devices are not re-infected

Seven Strategies to Defend ICSs

- Implement Application Whitelisting – 38%
- Ensure Proper Configuration/Patch Management – 29%
- Reduce your Attack Surface Area – 17%
- Manage Authentication – 4%
- Build a Defendable Environment – 9%
- Monitor and Respond – 2%
- Physical Controls
  - Perimeter Defenses and Monitoring
  - Internal Defenses
  - Policies/Procedures
  - Training
  - Situational Awareness
  - Supply Chain Security
DoD & Commercial Resources

DoD CIO Knowledge Service (requires CAC)  https://rmfks.osd.mil/login.htm

Department of Defense Advanced Control System Tactics, Techniques, and Procedures (TTPs) 2018:
https://www.cybercom.mil/ICSTTP/Forms/AllItems.aspx

UFC 4-010-06 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS Sept 2016
https://wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06

Strategic Environmental Research and Development Program (SERDP) and Environmental Security Technology Certification Program (ESTCP) [info & funding solicitations]

DoD OASD(El&E) and Federal Facilities Council (FFC), under the National Research Council (NRC) sponsored a 3-day Building Control System Cyber Resilience Forum in Nov ‘15.
http://sites.nationalacademies.org/DEPS/FFC/DEPS_166792

DoDI 5000.02 Cybersecurity in the Defense Acquisition System  Jan 2017

Whole Building Design Guide website cyber references
http://www.wbdg.org/resources/cybersecurity

Tools
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B

Workshops / Building Control Systems Cyber Security Training

Industrial Control Systems Joint Working Group (ICSJWG_