Recent APT Campaign
Targeting Energy Sector Assets

Jonathan Homer
Chief, Industrial Control Systems Group
HIRT/NCCIC

Jonathon Briney
Senior Analyst, ICSG
HIRT/NCCIC
Disclaimer

This presentation is intended for informational and discussion purposes only.

The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The display of the DHS official seal or other DHS visual identities, including the National Cybersecurity & Communications Integration Center (NCCIC) name or logo shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including NCCIC. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS, NCCIC, or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

This presentation is Traffic Light Protocol (TLP): **WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction. For more information on the TLP, see [http://www.us-cert.gov/tlp](http://www.us-cert.gov/tlp).

DHS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.
# Current Cybersecurity Profile

## Worldwide Threat Assessment - 2017

**Director of National Intelligence Dan Coats**
to Senate Select Committee on Intelligence – May 11, 2017

<table>
<thead>
<tr>
<th>Country</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Russia:</strong> Russia is assuming a more assertive posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny.</td>
<td></td>
</tr>
<tr>
<td><strong>China:</strong> China continues to have success in cyber espionage against the US Government, our allies and US companies. Beijing also selectively uses cyber attacks against targets it believes threaten Chinese domestic stability or regime legitimacy.</td>
<td></td>
</tr>
<tr>
<td><strong>Iran:</strong> Iran used cyber espionage, propaganda, and attacks in 2015 to support its security priorities, influence events and counter threats—including against US allies in the region.</td>
<td></td>
</tr>
<tr>
<td><strong>North Korea:</strong> North Korea probably remains capable and willing to launch disruptive or destructive cyber attacks to support its political objectives.</td>
<td></td>
</tr>
</tbody>
</table>

**Non-State Actors:** Terrorists continue to use the Internet to organize, recruit, spread propaganda, collect intelligence, raise funds and coordinate operations.
Campaign Summary

• Advanced Persistent Threat (APT) actors
• Hundreds of victims (targeted or affected)
  • Energy (focus area)
  • Nuclear
  • Aviation
  • Critical manufacturing
  • Government entities
• Response effort coordinated between multiple government organizations as well as industry organizations
• Effect has been limited to access so far, with no physical impact identified
Campaign Timeline

- Vendor compromised in early 2016
- Remained dormant for over one year
Campaign Timeline

• Additional vendor network compromised in early 2017
Campaign Timeline

• Phishing attack originating from compromised network against another vendor and government entity
Campaign Timeline

• Intrusion from compromised vendor to another vendor
Campaign Timeline

- Latest vendor victim leveraged to phish U.S. utilities
Campaign Timeline

- Used new victim network to pivot and browse external content of an already-phished organization, as well as a non-U.S. organization.
Campaign Timeline

• Used compromised vendor to access several U.S. energy utilities and IT service providers
Campaign Timeline

- Leveraged early victim to gain entry to two previously accessed utilities and one new victim
Who is the Target?

Staging Targets
- Smaller organizations with less sophisticated networks
- Pre-existing relationships with intended targets
- Deliberately selected, not targets of opportunity
- Examples: vendors, integrators, suppliers, and strategic R&D partners
- Used for staging tools and capabilities

Intended Targets
- Small, medium, and large organizations
- U.S. targets focused within the Energy Sector, specifically power generation, transmission, and distribution
- Sophisticated networks with more defensive cyber tools
What We Will Present Today

• Not a comprehensive overview of the attack
  • For full information, see
    • DHS Alert TA17-293A: Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors
    • Third-party analysis reports

• Focus on unique tactics and behaviors

• Two areas of discussion
  • Penetration of corporate networks
  • Targeting of control systems
Corporate Networks: Reconnaissance

- Accessing the corporate websites of staging targets
  - Human-driven behaviors, not scripted

- Lists of targets align to open-source lists (organized by subject-matter areas) published by third-party industry organizations

- Downloading detailed photos of organization infrastructure published to public website by victim organization
Corporate Networks: Credential Harvesting

- Tactic: Remote Server Message Block (SMB) server
  - Spearphishing using a Microsoft Word file referencing a remote normal.dotm file
  - Watering hole: Javascript leverages hidden iFrame to generate a “file://” connection to a remote server resulting in an SMB transfer of the user’s NT Local Area Network Manager (NTLM) hash

Stage 1:
Request for file outbound over ports 137/139/445

Stage 2:
Server requests credentials

Stage 3:
Victim provides user hash

Stage 4:
Server provides file
Corporate Networks: Initial Network Access

- Primarily leveraging captured legitimate credentials
- All victims had externally-facing, single-factor authenticated systems
- Three known intrusion vectors
  - Virtual private networks (VPN)
  - Outlook Web Access
  - Remote desktop (both externally exposed and through VPN)
Corporate Networks: Other Traditional TTPs

- **Persistence:** Legitimate credentials, new account creation, scheduled tasks
- **Lateral movement:** PsExec, batch scripts, remote desktop (RDP), virtual network computing (VNC), admin shares
- **Command and control:** web shells, remote desktop
- Tools leveraged are available on GitHub
  - Mimikatz
  - CrackMapExec
  - Angry IP
  - SecretsDump
  - Hydra
  - Inveigh (and Inveigh-Relay)
  - httrack
Corporate Networks: Persistence Using LNK files

**Stage 1:** LNK file stored in common access directory
**Stage 2:** LNK file icon file setting
**Stage 3:** LNK file icon viewed using Windows Explorer

**Stage 4:** Image Request for file outbound over ports 137/139/445
**Stage 5:** Server requests credentials
**Stage 6:** Victim provided user hash
**Stage 7:** Server provides image file

**Result:** Active user’s credentials are obtained by the threat actor every time the directory is viewed.
Control System Networks: Recon and Initial Intrusions

- Threat actor conducted research using publicly available information specifically related to the control systems being operated by specific victims

- Many of the phishing emails were targeted against control systems operations and related to control system operations
Control System Networks: Tactics

**Stage 1**: Access from threat actor to victim corporate network using RDP port forward already in place and/or compromised credentials through VPN

**Stage 2**: ICS Data exfiltrated from corporate servers:
- Vendor Information
- Reference Documents
- ICS Architecture
- Layout Diagrams

**Stage 3**: Remote access profiles downloaded from RDP/VNC jumpbox

**Stage 4**: Configuration data and screenshots downloaded from HMI
Control System Networks: RDP Session of Threat Actor
**Recommendations**

**Initial Triage**
- Search for known Indicators in historical logs (see DHS Alert)
- Remain focused on behaviors (TTPs)
- Don’t whitelist network traffic with trusted partners

**Continual Monitoring**
- Behavior-based analysis
- Staging Targets: anticipate spearphishing and watering holes
- Intended Targets: anticipate spearphishing, C2 using legitimate credentials, and persistent scripts on workstations and servers

**Directly Related Mitigations**
- Block all external SMB network traffic
- Require multi-factor authentication for all external interfaces
NCCIC Current Focus Areas

• NCCIC provides support for victims at all stages of compromise

• Specifically interested in information from victims, vendors, and cyber community in the following areas:
  1. Authentication by threat actor using multi-factor authentication
  2. Any direct access or information reconnaissance pertaining to control system networks
  3. Non-interactive activities by threat actor (actions other than those taken through RDP and VNC)
Contact NCCIC

NCCICCustomerService@hq.dhs.gov
1-888-282-0870
24x7x365 Operations