KEEPING THE LIGHTS ON IN A DANGEROUS WORLD

Adam S. Lee,
Vice President, CSO

Dominion Energy®
Rethinking Security

• Corporate physical security
  – From gates, guards, and guns…
  – To effective threat prioritization based on an understanding of risk, and development of mitigation strategies in partnership with Dominion Energy’s business elements, Services Company elements, law enforcement, and the U.S. Intelligence Community

• Corporate cyber security
  – From firewalling and patching…
  – To understanding the nature of the threats - nation state actors, environmental extremists, insider threats, etc. - and working to be predictive within the attack vector to harden against threats before damage is done

• Corporate threat intelligence
  – From “youth soccer” priorities, where we’re crowding the ball…
  – To requirements-driven collection, domain awareness, and effective and tailored production and dissemination
THREAT INTELLIGENCE

Strategic view of threats not tactical response to alerts/alarms

Provides context around the indicators and data collected

Incorporates Dominion Energy business risks into the analysis

Analyzes the impact of emergent threats or events on operations and tactical monitoring

Supports the creation of a common operating picture for security

- Cyber attacks on distribution and transmission systems, numerous tools, techniques and procedures used

Threat Intelligence identifies where the Ukraine tactics could impact Dominion Energy electric and gas industrial control systems

Dakota Access Pipeline Protests 04.2016 – 02/2017
- Protester techniques
- Use of social media

Threat Intelligence leverages security learnings from other industry efforts to improve security for Dominion Energy projects
The five tenets of China’s 13th Five-Year Plan:

- Innovation
- Whole of government
- Green growth
- Diversification
- Shared prosperity

“Made in China 2025” initiative

- Agriculture
- Aviation and aerospace
- Biotechnology and advanced medical equipment
- Electrical power
- High-end robotics
- Information technology
- Maritime engineering
- New energy automotive technology
- New materials and composites
- Rail transportation
# Not Just “Spy vs. Spy” Anymore

<table>
<thead>
<tr>
<th>THEN</th>
<th>NOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence officers</td>
<td>Intelligence officers</td>
</tr>
<tr>
<td>People recruited by intelligence officers</td>
<td>People recruited by intelligence officers</td>
</tr>
<tr>
<td></td>
<td>Hackers</td>
</tr>
<tr>
<td></td>
<td>Businesspeople</td>
</tr>
<tr>
<td></td>
<td>Academics</td>
</tr>
<tr>
<td></td>
<td>Researchers</td>
</tr>
<tr>
<td></td>
<td>Diplomats</td>
</tr>
<tr>
<td></td>
<td>Anyone else who can get their hands on something of value</td>
</tr>
</tbody>
</table>
### World’s Largest Companies, 2006-2019

Nationality of world’s largest companies, according to the Forbes Global 2000 list:

<table>
<thead>
<tr>
<th>Year</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REVISIT OF 2017 RUSSIAN TARGETING OF ENERGY AND OTHER CRITICAL INFRASTRUCTURE SECTORS

- Sophisticated attempt to infiltrate entities in energy sector
- Used a variety of techniques including using industry websites as watering holes, spear phishing with malware laden attachments, use of third party partners to send spear phish
- Also referred to as Dragonfly
- 2019.01.10 Wall Street Journal article

Sector Impact
- Targeted grid operators, power generators, pipeline operators, equipment providers
- Objective to obtain information and access to Industrial Control Systems (ICS) including Supervisory Control and Data Acquisition (SCADA)

Dominion Energy Impact
- Confirmed no impact to Dominion Energy
- Analyzed and incorporated indicators of compromise into cyber defenses (US-CERT Alert (TA18-074A))
- Continue to track for new information
U.S. DESIGNATION OF IRANIAN GROUPS AS TERRORIST ORGANIZATIONS

- March 2019: U.S. Government declares Iranian proxy group Harakat al-Nujaba and its leader as Specially Designated Global Terrorists
- April 2019: U.S. Government declares Iran’s Islamic Revolutionary Guard Corps a foreign terrorist organization
- Iranian hackers alleged to have attempted attacks against hundreds of U.S. entities including U.S. technology companies

Sector Impact
- Iran has allegedly attacked cyber critical infrastructure outside of U.S.
- Iranian actors indicted for attacks on U.S. critical infrastructure (e.g., banks, dam in NY)
- Potential for new retaliatory attacks

Dominion Energy Impact
- None to date
- Continue to track potential threat, fill intelligence gaps, and harden vulnerabilities
Threat Intelligence: Iran

**Situation:**
U.S. airstrike killing Iran’s Major General Suleimani, Iran’s retaliatory ballistic missile attack targeting Iraq-based U.S. forces, new U.S. economic sanctions

Iran has a history of increased cyber attacks following increased tensions or in retaliation for perceived provocations

**Community Assessment:**
Not aware of any specific credible physical or cyber threat to the energy sector in North America

Continued increased threat of retaliation via cyber attacks, possibly against US targets or critical infrastructure

Increased threat to physical energy infrastructure in the Middle East, possibility of physical impacts to those operated by U.S. companies and U.S. allies
## NORTH KOREA (DPRK) - PRIMARILY FINANCIALLY MOTIVATED

- Assessments indicate DPRK will continue to obtain and generate revenue via cyber attacks *(U.S. Director of National Intelligence’s 2019 Worldwide Threat Assessment)*
- U.S. and other countries attributed disruptive and destructive WannaCry malware to actors from DPRK (12.19.2017)

### Sector Impact
- Indirect threat to the sector due to potential for collateral damage from cyber attacks targeting others or broad scale attacks (e.g., WannaCry malware)

### Dominion Energy Impact
- No current impacts
- Continue to monitor activity and intelligence regarding this threat actor
Atlantic Coast Pipeline

- Slowdown in construction has tempered opposition direct action but planning/organizing activities and legal challenges continue
- Law enforcement partnerships in WV, VA, and NC remain strong
  - Local and state law enforcement
    - Ground support for construction activities and incidents
    - Strong VSP leadership engagement
  - State Fusion Centers
    - Intelligence sharing
  - Federal partners
    - Plugged in where there is a nexus to domestic terrorism or WMD concerns
- Intelligence assessments
  - Public harassment of key executives is likely to increase as construction resumes
  - Opposition claims of environmental injustice are drawing increased national and international attention (e.g., personalities, groups, and media)
  - Mountain Valley Pipeline (MVP) tree-sits may foreshadow things to come
    - 63 year old grandfather and sailing instructor
    - Member of radical anarchist group known for direct action
  - Persons from various states with known history of arrest for direct action now involved with opposition to ACP and MVP
    - Includes confirmed involvement of local with claimed ties to a domestic terrorism group
INSIDER THREATS

Workplace Violence

Sabotage
- Physical damage to facility, equipment, etc.
- Information Technology systems disruption
- Operational Technology systems disruption

Fraud

Intellectual Property Theft
- Dominion Energy information
- Confidential third party information

Espionage
- Foreign travel indicators
- Citizens of other countries

Unintentional interactions
- Social engineering voice calls
- Phishing
- Conferences

Nation States

12
PROACTIVE, HOLISTIC RISK MANAGEMENT

Dominion Energy, and its many organizations, are high value targets

Foreign corporations are mechanisms for state sponsored economic espionage

Proactive third party due diligence is essential

Executives, senior leaders, and team supervisors must understand the behavioral indicators of insider threats

Security needs to be part of your organization’s business culture and supported by its processes
QUESTIONS?
Adam S. Lee,
Vice President, Chief Security Officer
(804) 819-2762