

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Advanced Persistent Threats to the Electricity Sector

Grid Security Conference 2011, New Orleans, LA
October 19, 2011

Jim Brenton
ERCOT, Regional Security Coordinator

RELIABILITY | ACCOUNTABILITY



- Material in this presentation was gathered from a variety of open industry sources and press reports.
- Opinions expressed in this presentation my own and do NOT represent the ERCOT ISO or ERCOT Market Participants
 - ERCOT should not be held accountable for my opinions, random ramblings or rants

Note: An excellent open industry APT source is the 2010 MANDIANT M-Trends Report “The Advanced Persistent Threat” which is available at:

<http://www.mandiant.com/products/services/m-trends>

- Expert teams of cyber attackers have greatly expanded their successful attacks on government organizations and defense-related targets to now include: *“researchers, manufacturers, law firms, and even non-profits.”*
- Intrusions appear to be conducted by well-funded, Nation-State supported groups of professionally organized attackers
- Motivation, techniques and tenacity are very high. *“They are professionals, and their success rate is impressive.”*

- Multiple spear-phishing incidents in recent months involving major US Corporations
 - Banking;
 - Oil & Gas; and
 - Water Sector
- Emails are designed to look like intra-office traffic including company specific topics of concern
 - Threat Actors use company websites and social media to do reconnaissance and specifically target their attacks
 - Emails spoof actual user account names and current topics

- Post event Forensic Analysis shows that
 - Employees often attend industry events and use/share USB thumb drives to exchange presentation materials.
 - USBs often unknowingly infect hosts with botnets
- **Specifics:** When an employee returns to work and plugs an infected laptop into the corporate network, the malware quickly spreads
- **Impact:** Hundreds of workstations and servers may be infected if appropriate controls and/or endpoint security measures are not in place

- February 2011, McAfee released a report titled “Global Energy Cyber attacks: Night Dragon”
 - Describes activities, beginning in 2009, designed to obtain sensitive data from targeted organizations in the global oil, energy, and petrochemical industries.
 - Attacks involved social engineering, spear-phishing attacks, and exploitation of Microsoft Windows operating systems vulnerabilities
- McAfee’s report claimed that the intrusions originate from China, based mainly on the locations of the servers hosting the malicious activity

- These types of attacks are often characterized as the Advanced Persistent Threat or APT
- These are not “hackers” as in the past but generally called the “Advanced Persistent Threat” or the APT by those working to understand and counter this new level of attacks
- The APT has drastically changed the Threat Landscape over the last six years

- Successfully compromise any targeted system.
- Attacker skill sets match up to just above level needed to defeat a target's security protection
- Conventional InfoSec/NetSec defenses don't work
- Successfully evade anti-virus, network intrusion detection and other best practices
- Escape, evade and defeat incident response teams
- Strive to remain undetected inside the target network and systems while the target believes they've eradicated the intruders

- At first, these attacks seemed familiar to traditional hacking: access and steal information, and then use it to gain a competitive advantage.
- However, APT attackers are different since they also establish a “persistent” way to later come back, steal additional data and remain undetected by their victim. *“This is a very significant difference.”*
- The APT also has the capability to affect data integrity and system availability—key areas of concern for the Electricity Sector EMS and Market Systems.

- The scale, operation and logistics needed to conduct these attacks could only come from state-sponsored organizations
- Timing of attacks is consistent with normal M-F, 8-5 Chinese working hours and holidays
- There is no way to determine if the Chinese government has authorized this activity
- *Almost every APT intrusion correlates to current events within China with respect to either business activities or government trade activities and international business negotiations*
- *Other countries have the skills and motivation to target critical infrastructure within the U.S.A., but characteristics of the APT make it unique to China.*

Why Should Electric Utilities Care?

- Focus of APT on Government Systems now changed to Commercial Systems
- STUXNET exhibited some characteristics of APT-like attacks, but it was not.
 - STUXNET used Microsoft Zero-Day Vulnerability in LNK Parser and patch was not available
 - Malicious code executed as an Attack Vector targeted toward specific Siemens Control Systems
- Stuxnet and the APT should be a wake up call to Electric Utilities
 - Possible espionage & control system reliability concerns with APT
 - USB Attack Vector— STUXNET demonstrates how to attack “isolated” control system networks
- Your SecOps Analysts should carefully study STUXNET and APT Information
 - Does your company have SecOps Analysts on site? The answer should be YES!
 - Or, outsource to a qualified MSS vendor to monitor your key environments

- U.S. Gov Agencies and the defense communities are under continued attacks and learning to better counter APT attacks
- Many victims and targets in the commercial sector were unaware and unequipped detect or deal with the APT—some improvement
- When detected, *“Often, the victims of the APT react in a way that does more harm than good.”*
- Organizations within the commercial sector need to step up and improve their SEIM Analysis tools and SecOps Analytical technical skills in response to the APT

Classic Techniques Don't Work

- “*Preventive and detective controls*” and techniques needed for standards compliance do not effectively counter the APT
- The APT easily defeats normal defenses
 - Successfully evades anti-virus software, network intrusion detection, firewalls, access controls, and underequipped and ill-prepared incident responders
- Sophisticated techniques allow the APT to conceal their presence
 - Hide malware on their target’s own hosts and exfiltrate data hidden within the target’s own network traffic

- The APT is not *“just a government problem;”*
- APT has been effective against:
 - Defense Contractors and Gov/Military Organizations
 - Research Organizations and Financial Groups
- *No target is too small, too obscure, or too well-defended.*
- APT now moving toward Critical Infrastructure organizations in both the U.S. and overseas

- Steal information about Critical Infrastructure and Key Resources
 - Achieve economic, political and strategic advantage.
- *When the APT wants additional data from a target, they simply call on their existing assets, locate, steal and exfiltrate the data they need.*
- Establish and maintain control of target CI/KR systems
 - APT represents an occupying force within the target's environment
- The APT also represents a tactical capability that can control target system availability/integrity/reliability
- **We are working in “Contested Network Space” both inside and outside of our protected network security boundaries**

- SecOps Analysis of Log Files
 - Look for complex signs of compromise;
 - Integrate real-time log information from host-based and network-based systems—Terabytes
 - A/V, firewalls and IDS tools helpful, but more is needed
- SIEM tool suites are needed to Deep Dive into large volumes of information--Terabytes
 - Properly trained SecOps Analysts
 - *Look inside packets, files, e-mail — and even live forensic examinations of system that are still running*
 - *Don't tip off the APT that they have been discovered*

1. War of attrition against a sophisticated enemy with extensive resources.
 - We will be in for a long fight that may never end
 - We may never be able to declare victory with certainty
2. Panicked reactions will cause more harm than good
 - Do not immediately clean an infected system—study the attacker
 - Wait and develop a customized incident response strategy
 - Allow the attackers to continue operations as though you were unaware of their presence until ready to act
3. Raise your SecOps Analysis and Incident Response capabilities to match attackers, or be prepared to suffer continued compromise and outside control of your key systems

- Implement a strong computer Incident Response Capability
- Additional resources will be needed
 - NERC CIP Standards compliance will simply not be enough
- Industry needs to focus on results-based standards vs. compliance paperwork documentation
 - Watch what the U.S. Government is doing with FISMA-II
 - Move from paper-based compliance to Continuous Security Monitoring
- Ensure that IT and Control System Security SMEs are aware of the APT and know how to identify and counter adversaries within this new threat landscape
- **This APT Panel should be a WAKE UP CALL**

Questions and Discussion