FireEye Intel Center
FireEye, Inc. · Security. Reimagined.
1440 McCarthy Blvd · Milpitas, CA 95035

Energy-Utilities Threat Trends (Q2 2015)

Date: July 6th, 2015 Tags: energy-utilities, apt30, apt10, india, europe, china

Energy-Utilities Threat Trends (Q2 2015)

Threat Insight #1: Potential APT30 Targeting against a Global Energy Company in India **(Linked & Attached)**

Threat Insight #2: APT10 Activity at a Nordic Industrial Equipment Manufacturer Likely Reflects China's Sustained Interest in Renewable Energy Technologies **(Linked & Attached)**

Threat Horizon: Energy/Utilities Strategic Risk Outlook

The energy and utilities industries are high priority targets for cyber threat actors, principally because of the continued advances in technology enabling the discovery and development of new or previously inaccessible energy sources. At the same time, oil prices have remained depressed after their fall in the past two quarters. Production by the world's top producers continues unabated, meaning that prices will continue to hold steady through 2015, contributing to the longest period of oversupply since the late 1990s. We expect the following factors to influence threat actors' targeting in the energy and utilities sectors in the next quarter and beyond:

- Concerns over climate change will drive worldwide efforts to develop alternative energy technologies utilizing renewable sources and high capacity storage systems. The expected commercial value of these technologies will encourage criminal groups, in addition to national governments, to illicitly acquire technology.
- China has declared a "war on pollution" that, coupled with slowing growth, may intensify targeting of firms involved in pollution and carbon reduction, and environmentally restorative services.
- Persistently low oil prices will place acute pressure on the budgets of producer nations such as Iran and Russia. If prices remain low for too long,

these pressures may reach existential status, exacerbating simmering tensions in the Persian Gulf, particularly between Iran and Saudi Arabia. This could prompt more drastic disruptive or destructive cyber activity to inflate oil prices or otherwise influence the market.
- Lowered profit margins among energy firms may intensify competition for market share and lead to increased targeting of proprietary pricing or production information. Criminal groups may also exploit investors' search for positive returns in energy-related assets by engaging in fraudulent trading or pricing activity.
- While rare, utilities may be targeted for at least the testing of industrial control system (ICS) vulnerabilities. Research has already indicated these systems are vulnerable to exploitation, and destructive attacks conducted via ICS have occurred recently. As experimentation and development of ICS hacking techniques continues, utilities could find themselves victimized by such activity.

Energy/Utilities Industry: Advanced Actor Targeting

Organizations in the energy and utilities industry likely face cyber security threats from threat actors affiliated with a nation state and motivated to conduct economic espionage, or to damage or disrupt operations for political or military purposes. We consider the possibility that these threat actors may include apparent hacktivist groups operating in a proxy role for a nation state government.

- Nation state threat actors motivated to conduct economic espionage will likely target energy and utilities organizations and seek to obtain intellectual property and other proprietary information that can benefit indigenous enterprises and assist them in improving their operations.
- Energy and utility companies operating abroad or entering into partnerships with foreign companies will likely face targeting from threat actors working on behalf of that government. We have previously observed instances in which nation state threat actors have compromised such organizations and stolen financial information, internal communications, and other data for the likely purpose of informing government decision makers and providing them with an insider advantage in the negotiation process.

Threat groups working in association with a nation state may also target foreign energy or utility firms with the intent to damage or disrupt operations in response to increased political or military tensions between the two countries. Energy and utility companies are strategic targets given their role in a country's economy and critical infrastructure. We consider the possibility that certain nation state governments may use "hacktivist" groups acting as proxies to conduct such activity against energy and utility firms, so as to disguise their involvement and avoid ramifications.

For the January-March 2015 timeframe, based on FireEye® Dynamic Threat Intelligence™ (DTI) cloud data, FireEye has assigned a Cybercon™ level of 3 to Energy-Utilities, which is considered Moderate.

Energy-Utilities Q2 2015 Trend Intelligence (Attached)

- Daily Detection Levels, April - June 2015
- APT Malware Detections by Industry
- Top Non-APT Malware Detections
- APT Detections

Download the Full Q2 2015 Threat Trends Report: ENERGY-UTILITIES