CYBER THREATS TO THE ENERGY INDUSTRY

ORGANIZATIONS IN THE ENERGY INDUSTRY FACE CYBER THREATS FROM THE FOLLOWING ACTORS:

- Advanced Persistent Threat (APT)[1] groups attempting to steal information that can assist their sponsoring government in ensuring national and economic security. Data theft efforts will likely center on information related to natural resource exploration and energy deals. APT groups may also engage in destructive and disruptive actions against an adversary's energy industry in the event of conflict.
- Hacktivists may opportunistically target energy companies in response to perceived controversies. These actors may conduct distributed denial of service (DDoS) attacks, deface a company's website, or steal and expose private information in an attempt to embarrass the company and gain attention for a cause.

CASE STUDY: APT GROUP TARGETS PETROLEUM REFINING COMPANY

We previously responded to a suspected network compromise at a petroleum refining organization. During our investigation, we found that threat actors had gained access to the network after apparently conducting vulnerability scans and conducting SQL injection attacks against the organization's websites. Once inside the network, the threat actors compromised at least 50 systems, and stole over four gigabytes of data from a business unit responsible for the exploration and later production of fossil fuels.

WE HAVE OBSERVED AT LEAST 16 ADVANCED THREAT GROUPS COMPROMISE COMPANIES IN THESE SUBSECTORS:

- Alternative Energy Development
- Coal Mining
- Nuclear Energy Development
- Natural Gas Distribution & Marketing
- Oil & Gas Exploration & Production
- Oil & Gas Field Equipment Manufacturing
- Oil & Gas Field Services Petroleum Refining

1 Advanced Persistent Threat (APT) actors are assessed to take direction from a nation state to steal information or conduct network attacks, tenaciously pursue their objectives, and are capable of using a range of tools and tactics.

FireEye

TOP 5
MALWARE DETECTIONS

- **41%** SOGU (aka Kaba)
- **20%** ADDTEMP
- **16%** WITCHCOVEN
- **13%** Gh0stRAT
- **10%** SpyNet

TOP 5
CRIMEWARE DETECTIONS

- **44%** Jenxcus (aka njw0rm, njworm)
- **22%** HOUDINI (aka H-Worm)
- **12%** JpiProx
- **11%** ZeroAccess (aka Sirefef)
- **11%** Upatre

THREAT HORIZON & INDUSTRY OUTLOOK

The energy industry will likely continue to be a high priority target for threat actors, particularly given its importance to national and economic security. We expect that the following situations may further contribute to threat activity towards the industry:

- The continued precipitous drop in oil prices may change APT groups' calculus in the value of pilfered oil or gas drilling technology in light of profitability concerns.
- Continued innovations in fossil fuel development and alternative energy production will probably also lead to increased cyber espionage as APT groups try to obtain related intellectual property and proprietary data for the benefit of state-owned companies.
- Growing global demand for energy and dwindling natural resources will likely result in increased cyber espionage against the sector as nation states seek intelligence that would afford them a competitive advantage when vying for energy security.
- Observed espionage by suspected Russian-based threat groups conducting reconnaissance of industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems.
- Conflict between countries could also result in increased threat activity as state-sponsored threat actors may seek to increase pressure on an adversary through disrupting the adversary's energy supply.
- Environmental issues and other controversies related to energy production may also result in increased threat activity from hacktivists seeking to call attention to the issues and embarrass organizations that they view as responsible.

DATA STOLEN FROM ENERGY COMPANIES

- Business Processes Information
- Contract Negotiations Information
- Executive Communications
- Market Analysis
- Proprietary Technologies

TOP MALWARE DETECTIONS

FireEye most frequently detected threat actors using the following targeted malware families to compromise organizations in the energy sector:

SOGU	(aka Kaba, PlugX) is a backdoor that is capable of file upload and download, arbitrary process execution, filesystem and registry access, service configuration access, remote shell access, and implementing a custom VNC/RDP-like protocol to provide the command and control (C2) server with graphical access to the desktop.
ADDTEMP	(aka Desert Falcon and Arid Viper) may be delivered via spear phishing. It is capable of taking screenshots, logging keystrokes, uploading and downloading files, stealing stored passwords from the system registry, and querying information on all the .doc and .xls files on the victim's hard disk or connected USB devices.
WITCHCOVEN	is a profiling script design to learn information about the operating systems, browsers, and applications of site visitors. We suspect APT actors are using these scripts to engage in footprinting, an information gathering technique used to profile computer systems and the organizations to which they belong.
GH0STRAT	is a remote access tool (RAT) derived from publicly available source code. It can perform screen and audio captures, enable a webcam, list and kill processes, open a command shell, wipe event logs, and create, manipulate, delete, launch, and transfer files.
SpyNet	is a publicly available RAT that allows threat actors to interact with a compromised system via a remote shell, upload and download files, interact with the registry, and start and stop processes and services. It can capture images of the desktop, record from webcam and audio inputs, extract saved passwords, and turn a compromised system into a proxy server. There is also keylogging functionality, as well as anti- debugging/virtual machine defensive mechanisms.

TOP CRIMEWARE DETECTIONS

FireEye's sinkhole and dynamically shared threat data indicate that the following crimeware variants were the most commonly detected in the the energy sector:

Jenxcus	(aka njw0rm, njworm) is an evolution of the popular tool njRAT (aka Backdoor.LV) that can spread across removable drives and steal credentials. Often delivered via malicious links in email and drive-by downloads on compromised sites.
HOUDINI	(aka H-Worm) is a VBS-based RAT that uses HTTP to communicate information about the compromised system, such as operating system and host and user name. In some cases the VBS file is packed with multiple layers of obfuscation, including custom Base64 encodings. It supports several commands, such as command line execution, downloading and executing programs, and data theft.
JpiProx	is a Trojan that installs itself as a browser add-on and will inject ads into websites visited, and may install additional malware. JpiProx masquerades as a browser plugin to generate ad-fraud revenue for criminals by injecting ads into any webpages visited by users on an infected host. It may also install other malware or unwanted programs like web proxy software that can be used to pipe unwanted traffic through infected hosts to mask its original location. The Trojan may also exfiltrate information about an infected system as well as a list of websites visited and additional information.
ZeroAccess	(aka Sirefef) is a Trojan with advanced rootkit capabilities. Initially developed as a delivery mechanism for other types of malicious software, it has been re-architected to perform click fraud.
Upatre	is a Trojan downloader that often arrives via a spam email, drive-by download or exploit, Upatre will download one or more additional types of malware onto an infected system. Upatre has been observed distributing a wide variety of malware including, but not limited to, Zbot, Dyre, Rovnix, CryptoLocker, and Necurs.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 / 408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye