Hackers Corner
New Threats Targeting Oil and Gas

Background

Last year, US-CERT issued a technical alert[1] that was a result of a joint effort between the Department of Homeland Security and the Federal Bureau of Investigation. This alert highlighted a growing threat from the Russian government and its actions against several industries, including the energy sector.

The energy sector is an alluring target for both for-profit criminals and nation-state actors. As a result, the oil and gas industry currently witness hundreds of thousands of attacks per month. The security community has little to no visibility into these attacks because the energy sector does not have the same reporting requirements as other industries, and typically, attacks are not publicly reported.

Limited reporting requirements in addition to an industry that is undergoing digitalization makes it extremely difficult to understand the threat landscape. For example, throughout the Eastern United States, concentrations of refineries, pipelines, and waterways[2] are lined with network sensors and internet-connected devices, leaving them vulnerable to cyberattacks from both domestic and foreign threats.

In April of 2018, Bloomberg[3] reported that Energy Service Group's Electronic Data Interchange (EDI) platform was under attack, preventing their clients from being able to process transitions. While the reported impact was minimal, this attack followed the warning from U.S officials and highlighted a known threat for the energy sectors: supply chain attacks.

These threats began to manifest years ago. In 2010, it was discovered that a piece of malware called Stuxnet was used to target SCADA systems to cause damage to Iran's nuclear program. In 2012, researchers from Seculert, now a part of Radware, discovered a piece of malware called Shamoon that was used to target national oil companies in Saudi Arabia and Qatar.

The risk of actors targeting the energy industry is on the rise and it should come as no surprise that the sector is an attractive target for a variety of criminals. Attackers aren't just looking to cause costly network outages or gain unauthorized access to sensitive data but are also looking to cause physical damage to equipment to disrupt production or cause physical harm.

Areas of Concern

- Production and develop drilling
- Field exploration and big data
- Geophysical survey and seismic images

Insight

Initial attempts to compromise will come in the form of electronic mail. Typically, phishing attacks are used to harvest employee credentials or to deliver malware, but the energy industry is also at risk of business email compromise (BEC) scams.

BEC is like a phishing attack. It refers to a scam where criminals send emails designed to look as if they came from a specific employee or vendor. The purpose of a BEC scam is to trick a victim into sending money via a malicious transfer.

[1] https://www.us-cert.gov/ncas/alerts/TA18-074A

[2] https://www.houstonchronicle.com/news/houston-texas/houston/article/As-cyberattacks-become-more-sophisticated-energy-10973429.php

[3] https://www.bloomberg.com/news/articles/2018-04-02/energy-transfer-says-cyber-attack-shut-pipeline-data-system

Once attackers have compromised a user and gained access, they will look to move across the network in search of sensitive data that can be leveraged for espionage purposes or to deliver malware designed to disrupt production. Malware capable of delaying or preventing the transmission of data coming out of the field could cause severe disruption to production.

A simple update could cost millions of dollars and cause production delays. In some cases, an update/patch is not possible because such actions would void a product or machine warranty.

Targets

- Corporate offices
- Operation platforms
- Engineering workstations
- Remote units and sensors

Advice

In general, those that target the energy sector are typically actors with extensive resources and are the result of a commercial or economic espionage campaign. Threat actors are typically looking to abuse the trust chain between vendors and clients as an initial attack vector. It's advised that employees are trained on how to spot a phishing attack and the process they should follow when verifying financial requests that comes from the CEO, attorneys or vendors.

In addition to fortifying email filters and establishing training classes, companies need to be able to detect and mitigate application and network-based attacks not only directed at operational technologies but also information technologies storing sensitive data.

Under Attack and in Need of Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.