Oil-and-Gas APT Pivots to U.S. Power Plants

By Tara Seals

Published: 2020-01-10 · Archived: 2026-04-05 13:43:59 UTC

Researchers say that physically disruptive attacks aren't imminent, but an increased focus on U.S. electrical-grid operators doesn't bode well.

A known APT group with ties to the Iran-linked APT33, dubbed Magnallium, has expanded its targeting from the global oil-and-gas industry to specifically include electric companies in North America.

That's according to a report from Dragos, released Thursday, which noted that the discovery is part of a broader trend in which cybercriminals focused on critical infrastructure are branching out from a single-vertical operation to multiple industrial sectors. While that reality doesn't necessarily threaten a physically disruptive attack, it also certainly doesn't rule it out, the firm said.

"Attacks on electric systems – like attacks on other critical infrastructure sectors – can further an adversary's criminal, political or economic goals," according to the report. "As adversaries and their sponsors invest more effort and money into developing effects-based operational outcomes, the risk of a disruptive or destructive attack on the electric sector – including in North America – significantly increases."

In the same report, Dragos said that Xenotime (a.k.a. the group behind the 2017 Trisis attack, which did have physical consequences) has ramped up its activities in North America.

Magnallium Comes to America

Dragos initially identified Magnallium's expansion into targeting North American electric entities because of activity from a group called Parisite that cropped up in its telemetry. That group was seen targeting known VPN vulnerabilities at electric targets in the U.S.

Parasite, according to Dragos profiling, targets utilities, aerospace, and oil-and-gas entities. It uses open-source tools to compromise infrastructure and leverages known vulnerabilities for initial access.

"This group has operated since at least 2017 based on infrastructure Dragos identified," the report explained. "Parisite serves as the initial access group and enables further operations for Magnallium."

Magnallium, for its part, has targeted energy and aerospace entities since at least 2013, Dragos said, when it was seen targeting an aircraft holding company and oil-and-gas firms based in Saudi Arabia. Like the broader APT33 group, its main focus is on information-gathering rather than disrupting ICS equipment, researchers wrote in the report.

"In the fall of 2019, following increasing tensions in the Middle East, Dragos identified Magnallium expanding its targeting to include electric utilities in the U.S.," according to the analysis. "Magnallium appears to still lack an ICS-specific capability…The group remains focused on preliminary information-gathering and access operations that can be used for a future attack against ICS-related organizations."

Magnallium uses phishing emails to gain access to victims' machines; recent campaigns involved lures crafted from publicly available job postings, the report noted. Commercial phishing kits were then used to construct the emails' contents, usually career-related messages. The messages delivered variants of the StoneDrill wiper and TurnedUp malware family, used to steal data, along with PowerShell-based post-exploitation tools.

More Time for Xenotime

Meanwhile, Xenotime has been seen continuing to target supply chains related to electric entities in North America, Dragos said.

Xenotime is the firm's name for the group behind the 2017 Trisis (aka TRITON or HatMan) malware attack on a Saudi Arabian petrochemical facility. That attack targeted safety systems and was designed to cause loss of life or physical damage.

The malware directly interacted with and controlled Triconex safety instrumented system (SIS) controllers, which are sold by Schneider Electric. SISes are the last line of automated safety defense for industrial facilities, designed to prevent equipment failure and catastrophic incidents such as explosions or fire. The malware managed to cause this fail-safe system to shut down (though a final-stage destructive attack never came).

TRISIS lives on in memory because to date, only a handful of malware, such as the infamous Stuxnet and Industroyer/Crash Override strains, has had the ability to impact the physical process of an ICS installation. TRISIS has not appeared elsewhere since 2017, but it's worth noting that the same malware framework showed up in a second incident last year, according to FireEye researchers.

A previous analysis from Dragos found that the group had pivoted to North American targets. That activity has only continued, with the group branching out to develop expertise in hacking devices beyond Triconex controllers. This group has now compromised several ICS vendors and manufacturers, providing a potential supply-chain threat, the report noted.

"Adversaries are increasingly utilizing third-party compromise as a method for affecting intended targets," according to the report. "This attack vector enables an adversary to utilize the implicit trust between companies, suppliers or supporting entities. Dragos has observed [Xenotime] leveraging trusted relationships to infiltrate target networks. This includes compromising vendor networks as well as strategic web compromises."

Overall, the developments show that threats to one industrial entity are potential threats to other industrial verticals, the report concluded, with adversaries targeting multiple verticals with purposes including espionage, information gathering and potentially disruptive events.

"This trend is driven by multiple variables, including an increasing investment to develop offensive capabilities specifically for ICS-targeting operations," according to Dragos. "Attackers are obtaining the skills necessary for a cyber-physical event as greater attention is paid to ICS in general and as open-source information on industrial

networks, protocols and devices becomes more widely available. Additionally, the spread of commodity IT hardware and software into operational technology networks increases the attack surface, providing ingress opportunities via techniques familiar to the adversary."

Concerned about mobile security?* Check out our free Threatpost webinar, *Top 8 Best Practices for Mobile App Security, on Jan. 22 at 2 p.m. ET. Poorly secured apps can lead to malware, data breaches and legal/regulatory trouble. Join our experts to discuss the secrets of building a secure mobile strategy, one app at a time. Click here to register.
