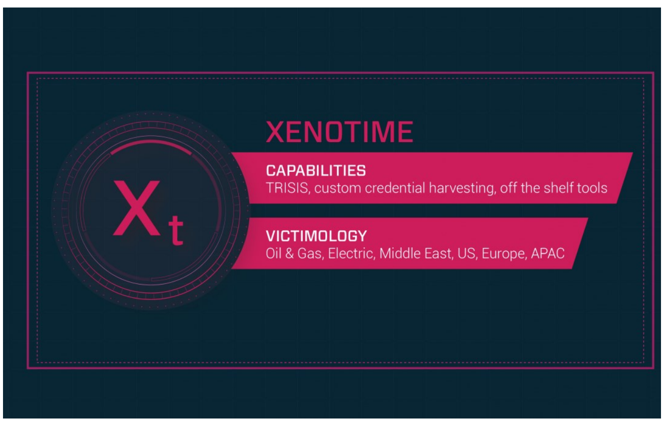
Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas

Jun 14, 2019 | Blog, Industry News


Xt
XENOTIME
CAPABILITIES
TRISIS, custom credential harvesting, off the shelf tools
VICTIMOLOGY
Oil & Gas, Electric, Middle East, US, Europe, APAC

By Dragos, Inc

The most dangerous threat to ICS has new targets in its sights. Dragos identified the XENOTIME activity group expanded its targeting beyond oil and gas to the electric utility sector. This expansion to a new vertical illustrates a trend that will likely continue for other ICS-targeting adversaries.

Industrial control system (ICS) cyber threats are proliferating. More capable adversaries are investing heavily in the ability to disrupt critical infrastructure like oil and gas, electric power, water, and more. Attacking any industrial sector requires significant resources, which increases as capabilities and targeting expand. The high resource requirement previously limited such attacks to a few potential adversaries, but as more players see value and interest in targeting critical infrastructure – and those already invested see dividends from their behaviors – the threat landscape grows.

To illustrate and highlight this major strategic risk to industrial environments worldwide and across every industry, Dragos is publishing new intelligence on XENOTIME. In anticipation of this release, Dragos worked with global electric utilities to increase their defense against this and the other threats to industrial control systems. Dragos Platform customers have detections for XENOTIME, as the product receives these and other threat behavior detection updates regularly.

XENOTIME Proliferation: A Shift in the ICS Threat Landscape

XENOTIME, the group behind the TRISIS event, previously focused on oil and gas related targeting. In February 2019, Dragos identified a change in XENOTIME behavior: starting in late 2018, XENOTIME began probing the networks of electric utility organizations in the US and elsewhere using similar tactics to the group's operations against oil and gas companies.

Multiple ICS sectors now face the XENOTIME threat; this means individual verticals – such as oil and gas, manufacturing, or electric – cannot ignore threats to other ICS entities because they are not specifically targeted. As such, a key element in defense against sophisticated, expanding threats is understanding threat behaviors and methodologies, beyond simply indicators of compromise.

Asset owners and operators across ICS should be aware of XENOTIME's tactics, techniques, and procedures, and consider using an ICS-specific detection capability like the Dragos Platform while also implementing defensive recommendations discussed below.

Activity Overview

The 2017 TRISIS malware attack on a Saudi Arabian oil and gas facility represented an escalation of attacks on ICS. TRISIS targeted safety systems and was designed to cause loss of life or physical damage. Following that attack, XENOTIME expanded its operations to include oil and gas entities outside the Middle East. Additionally, the group compromised several ICS vendors and manufacturers in 2018, providing potential supply chain threat opportunities and vendor-enabled access to target ICS networks.

XENOTIME operations since the TRISIS event in 2017 included significant external scanning, network enumeration, and open source research of potential victims, combined with attempts at external access. This activity emphasized North American and European companies.

In February 2019, while working with clients across various utilities and regions, Dragos identified a persistent pattern of activity attempting to gather information and enumerate network resources associated with US and Asia-Pacific electric utilities.

This behavior could indicate the activity group was preparing for a further cyberattack, or at minimum satisfying the prerequisites for a future ICS-focused intrusion. The activities are consistent with Stage 1 ICS Cyber Kill Chain reconnaissance and initial access operations, including observed incidents of attempted authentication with credentials and possible credential "stuffing," or using stolen usernames and passwords to try and force entry into target accounts.

Cause for Concern

While none of the electric utility targeting events has resulted in a known, successful intrusion into victim organizations to date, the persistent attempts, and expansion in scope is cause for definite concern. XENOTIME has successfully compromised several oil and gas environments which demonstrates its ability to do so in other verticals. Specifically, XENOTIME remains one of only four threats (along with ELECTRUM, Sandworm, and the entities responsible for Stuxnet) to execute a deliberate disruptive or destructive attack.

XENOTIME is the only known entity to specifically target safety instrumented systems (SIS) for disruptive or destructive purposes. Electric utility environments are significantly different from oil and gas operations in several aspects, but electric operations still have safety and protection equipment that could be targeted with similar tradecraft. XENOTIME expressing consistent, direct interest in electric utility operations is a cause for deep concern given this adversary's willingness to compromise process safety – and thus integrity – to fulfill its mission.

XENOTIME's expansion to another industry vertical is emblematic of an increasingly hostile industrial threat landscape. Most observed XENOTIME activity focuses on initial information gathering and access operations necessary for follow-on ICS intrusion operations. As seen in long-running state-sponsored intrusions into US, UK, and other electric infrastructure, entities are increasingly interested in the fundamentals of ICS operations and displaying all the hallmarks associated with information and access acquisition necessary to conduct future attacks. While Dragos sees no evidence at this time indicating that XENOTIME (or any other activity group, such as ELECTRUM or ALLANITE) is capable of executing a prolonged disruptive or destructive event on electric utility operations, observed activity strongly signals adversary interest in meeting the prerequisites for doing so.

Defensive Recommendations

Asset Identification and Environmental Awareness ICS asset owners and operators across all industries must prepare for potential breach and disruption scenarios. The most important thing a security team can do is improve visibility and awareness of ICS network activity, chiefly through a combination of network observables, host-based logs, and process-specific data.

Threat Behavior Detection ICS-specific threat intelligence can also be leveraged to identify unique threat behavior patterns, evolving adversary methodology, and specific conduct.

Investigation, Response, and Recovery When investigating or detecting ICS-specific intrusions and manipulation for hostile purposes, defenders must leverage all available information sources — from IT- like observations to process-specific impacts — and fuse them to gain a complete view of ICS network operations enabling informed response and root cause analysis of industrial incidents.

Given that XENOTIME is capable of and willing to execute a fundamental attack on process safety through attempted SIS modification, asset owners and operators must begin planning now for response and recovery scenarios related to a loss of SIS integrity. Specific items relating to response and recovery which can be immediately implemented include:

- Identify vendor contacts for support and analysis on specialized equipment not amenable to standard IT-based investigation techniques
- Have appropriate incident response capabilities either in-house or on call
- Maintain known-good configuration and process data both for comparison to possible compromised devices, and to enable rapid recovery in the event of a breach
- Identify operational workarounds to maintain known-good, known-safe production or generating capability

Irrespective of how an organization addresses these questions, ICS operators must address such concerns in advance, rather than trying to figure out such sensitive, complex items mid- or post-intrusion.

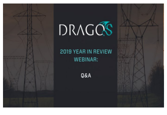
Conclusion

Ultimately, XENOTIME's expansion to an additional ICS vertical is deeply concerning given this entity's willingness to undermine fundamental process safety in ICS environments placing lives and environments at great risk.

Dragos emphasizes that the observed behavior is an *expansion, a proliferation of the threat,* and not a shift – oil and gas entities must still grapple with this adversary's activity. While unfortunate, the expansion should serve as a clear signal to ICS operators – not only in oil and gas or electric utility operations – that the time to plan, implement, and enforce security standards and response processes in industrial environments is now.

For policymakers and risk managers, it is important to note that cross-geography and cross-industry collaboration is critical. Critical infrastructure cannot be siloed as the threat is operating across verticals and may even use one against the other; for instance, targeting electric to deny power to an oil refinery. Utilities, companies, and governments must work cooperatively around the world and across industrial sectors to jointly defend lives and infrastructure from the increasing scope and scale of offensive critical infrastructure cyber attack.

Recent Blog Posts



Dragos 2019 Year in Review Webinar Q&A
March 18, 2020

Spyware Stealer Locker Wiper: LockerGoga Revisited
March 17, 2020

Energy Organizations Continue to be Compromised Globally
March 10, 2020

Dragos 2019 ICS Year in Review: Executive Summary
February 20, 2020

Assessment of Ransomware Event at U.S. Pipeline Operator
February 19, 2020

DRAGOS

Your mainline ICS feed: @DragosInc

PRODUCTS & SERVICES
Dragos Platform
Threat Intelligence
Neighborhood Keeper
Professional Services
Training

RESOURCES
Whitepapers
Webinars
Datasheets & Brochures
Infographics
Year in Review
Adversaries Reports

MEDIA
News
Press Releases
Videos
Podcasts

COMPANY
About Us
Awards
Careers
Dragos Industrial Security Conference
Events
Meet the Team

1745 Dorsey Rd
Hanover, Maryland 21076
(855) 372-4670
info@dragos.com