



D.C. TAKES ON ENERGY SECTOR THREATS

A SUMMARY OF RECENT AGENCY AND
CONGRESSIONAL EFFORTS

Authored By:

Parham Eftekhari, Executive Director, ICIT
Drew Spaniel, Lead Researcher, ICIT

ICIT | Institute for Critical
Infrastructure Technology
The Cybersecurity Think Tank

D.C. Takes on Energy Sector Threats

A Summary of Recent Agency and Congressional Efforts

September 2019

Copyright 2019 Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

Contents

Introduction	3
Recent Threats to the Energy Sector	3
Xenotime	4
HEXANE	5
APT10	6
U.S. Government is Not Asleep on the Clock	6
Federal Initiatives	6
DOE Seeking Input on Draft of Latest Cybersecurity Risk Assessment Model.....	7
FERC and NERC Strengthened Cyber Security Standards for Bulk Electric System.....	7
DOE Announced \$40 Million for Grid Modernization Initiative	8
DOE and FERC Discussed Best Practices and Increasing Investment in Energy Systems in Response to Cyber Threats.....	8
DOE Awarded \$46M to Mitigate Cyber-Physical Threats to Solar Grid	8
Jack Voltaic 2.0	9
Legislation	9
S. 174: Securing Energy Infrastructure Act.....	9
S. 876: Energy Jobs for our Heroes Act of 2019	10
H.R. 2114: Enhancing State Energy Security Planning and Emergency Preparedness Act of 2019.....	10
H.R. 680: Securing Energy Infrastructure Act.....	10
H.R. 359: Enhancing Grid Security through Public-Private Partnerships Act	10
H.R. 5240: Enhancing Grid Security through Public-Private Partnerships Act	10
S. 3677: Enhancing Grid Security through Public-Private Partnerships Act.....	10
S. 2991: Promoting Cybersecurity for Rural Electric Utilities Act.....	10
H.R. 2741.....	10
Conclusion.....	11
Sources.....	11

Introduction

Cybersecurity researchers often walk a fine line between objectively presenting the facts surrounding cybersecurity threats without fearmongering to garner the attention necessary to pressure policy makers and decision makers to take action. This is particularly true in the Energy sector, where the exploitation of vulnerabilities can lead to genuine high-risk outcomes such as regional black-outs and potential loss-of-life incidents.

When media and researchers report on the energy sector, emphasis is rightfully placed on the actions of bad actors, vulnerabilities which plague our critical infrastructure sectors, and the consequence of government inaction on energy sector resiliency. While holding the federal government accountable is necessary, ICIT believes it is also important to recognize the work being done on the part of public and private sector stakeholders to respond to this threat. Despite challenges that exist in procurement, legislation, and regulation, the public should also be made aware of existing initiatives that demonstrate government vigilance and may offer immediate solutions and resources to some of the security challenges faced by the energy sector.

This publication, which draws on research from [ICIT's Monthly Analyst Reports](#) as well as analysis from recent threat reports from Dragos and FireEye, will discuss threats that the XENOTIME, HEXANE, and APT10 groups pose to the energy sector while also highlighting the efforts underway within [Congress](#) and [federal agencies](#) to secure the sector in response to emerging threats.

Recent Threats to the Energy Sector

Recently, the potential of cyberattacks that achieve a kinetic impact have increased across multiple sectors, including the Energy sector. Capable adversaries are investing heavily in the ability to disrupt critical infrastructure like oil and gas, electric power, and water. A decade ago, attacking any industrial sector required resources unavailable to low-level attackers. 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, novel and accessible tools, such as point-and-click malware, are developed, and sectors become susceptible to attacks from every caliber of digital adversary.

When prolific threats garner notoriety from online outlets, media sources, security firms, and law enforcement, less sophisticated or less resourced threat actors may be inspired by the coverage to likewise attempt attacks against critical infrastructure targets such as the electric grid owners and operators in an attempt to attract similar infamy. Below are some recent

examples of threats to the energy sector that have sparked reactions from the legislative and federal communities.

Xenotime

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. XENOTIME, the group behind the TRISIS event, previously focused on oil and gas facilities in the Middle East; however, following the initial TRISIS campaign, 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.

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. In 2019, XENOTIME was detected repeatedly 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.

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.

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. Firms need to begin to identify threats by anomalous behavior rather than through recognition of Indicators of Compromise (IoCs).

HEXANE

In Late July 2019, the security firm Dragos released information attributing recent attacks on oil and gas organizations and telecommunication providers from Africa to Central Asia to the Middle East, to a threat actor referred to as HEXANE [1]. At the time of writing, Kuwait has been identified as the primary region targeted by the APT. It is believed that telecommunications providers may have been targeted as a stepping stone to network-focused man-in-the-middle and related attacks [2].

In recent months, the threat actor has targeted organizations with phishing lures and malware implants with a clear intent to intrude into mission-critical networks and ICS systems. HEXANE appears to use some of the same malware as the OilRig APT attributed to Iran; although, the activity of the group has been evaluated as distinct enough for it to be classified as a similar, but separate threat with the potential of being a derivative group. HEXANE may pull from the same resource pool as OilRig without directly sharing tools [1]. HEXANE also demonstrates similarities to the activity groups MAGNALLIUM and CHRYSENE. All are ICS-targeting activities focusing largely on oil and gas, and some of the behaviors and recently observed tactics, techniques, and procedures (TTPs) are similar [2].

Dragos believes that the group has been active since at least mid-2018, but accelerated its activity in early 2019 in correlation with escalating political and military tensions in the Middle East. HEXANE intrusion activity includes malicious documents that deliver malware that establishes footholds for follow-on activity. HEXANE’s tendency to target telecommunications

and other third-party networks is indicative of a trend among adversarial groups that target ICS systems via vulnerable supply chains. For instance, in 2018, Dragos identified the activity group XENOTIME targeting several industrial original equipment manufacturers (OEMs), and hardware and software suppliers. By compromising devices, firmware, or telecommunications networks used by targets within ICS, malicious activity could potentially enter the victim environment through a trusted vendor, bypassing much of the entity's security stack [2].

APT10

Researchers at Proofpoint have attributed a cyber campaign targeting U.S. utility companies in July 2019 to the Chinese state-sponsored APT10, which is believed to act for the country's Ministry of State Security. The disclosure on August 1, 2019 warned that "persistent targeting of any entity that provides critical infrastructure should be considered an acute risk—the profile of this campaign is indicative of specific risk to U.S.-based entities in the utilities sector." Proofpoint dubbed the malware delivered via a targeted spear-phishing campaign "LookBack." The malware consists of a remote access Trojan (RAT) module and a proxy mechanism used for command and control (C&C) communication. LookBack can attack and mimic a wide range of processes on an infected machine—primarily, though, the objective is to steal data files and take operational screenshots [3]. Proofpoint's analysts identified "similarities" between the macros used in this attack and those found to be targeting the Japanese media sector in 2018. LookBack "resembles a historic TTP utilized in those campaigns," the researchers explained, albeit the specific malware "has not previously been associated with a known APT actor" [4].

U.S. Government is Not Asleep on the Clock

Federal agencies and the legislative community have been tracking the threats against the energy sector and are steadily rolling out programs, policies, and initiatives to support the energy critical infrastructure sector. While there is room for constructive feedback in order to remediate challenges which are preventing the government to provide the levels of support which are needed to counter the threats the sector faces – such as partisan discord, acquisition challenges, inadequate regulations, and a lack of funding – it is irresponsible to ignore the positive actions taken by both agencies and the legislative community to improve energy sector resiliency.

Federal Initiatives

Information below accrued from ICIT's monthly Federal Agency and Legislative Analyst Report indicates that though the threats against energy infrastructure are increasing in numbers and sophistication, federal agency and public-private strategies to mitigate the threat are likewise evolving. For instance, when asked by E&E News about how DOE responded to reports of APT

10, the Assistant Secretary of Energy for Cybersecurity, Energy Security and Emergency Response, Karen Evans responded, “We released what we call an ARES bulletin, an analysis of risks to the energy sector. It's very specific, technical information that can be executed by the grid operators out in their own environments so they can work to protect themselves against a threat. The information sharing and analysis centers [ISACs] are providing services to their specific area in the energy sector, and we are relying on them very heavily for information distribution” [5]. Her response indicates a public-private approach that trains critical infrastructure operators to recognize the threat. Meanwhile, agency initiatives push towards researching novel defenses and developing public-private partnerships.

The initiatives below are examples of some of the proactive cybersecurity efforts launched by federal agencies. The summaries and links have been directly pulled from [ICIT's Monthly Federal Cybersecurity Initiatives Report](#):

DOE Seeking Input on Draft of Latest Cybersecurity Risk Assessment Model

Until September 13, 2019, the Energy Department sought input from industry regarding an update to the Cybersecurity Capability Maturity Model designed to help organizations assess their cybersecurity posture. The C2M2 framework was established in 2012 as an open-source model to help fortify the security of the electric grid. DOE used its interviews with industry experts as well as best practices cited in the National Institute of Standards and Technology's most recent cybersecurity framework to inform the development of the latest C2M2 iteration.

Reference Links

- [DOE Releases Draft of Latest Cybersecurity Risk Assessment Model](#)
- [Energy Updates Cybersecurity Maturity Model](#)

FERC and NERC Strengthened Cyber Security Standards for Bulk Electric System

In June 2019, the Federal Energy Regulatory Commission (FERC) approved a new mandatory cybersecurity reporting rule proposed by the North American Electric Reliability Corporation's (“NERC”), Reliability Standard CIP 008-6, which requires the reporting of "cyber security incidents that either compromise, or attempt to compromise Electronic Security Perimeters, Electronic Access Control or Monitoring Systems and Physical Security Perimeters" for high- and medium-impact bulk electric systems (BES) cyber system. The rule also added "disruptions or attempts to disrupt the operation of a bulk electric cyber system." The implementation deadline is the "first day of the first calendar quarter 18 calendar months" after the order has been approved, which would be December 2020.

Reference Links

- [FERC Strengthens Cyber Security Standards for Bulk Electric System](#)

- [FERC Approves New NERC Cyber Security Reliability Standard](#)
- [FERC and NERC Advance Dramatically Expanded Mandatory Cybersecurity Reporting Standards](#)

DOE Announced \$40 Million for Grid Modernization Initiative

In February 2019, DOE Under Secretary of Energy Mark Menezes announced that \$40 million in FY19 funding for the Grid Modernization Initiative (GMI). The GMI focuses on working with public and private partners to develop new tools and technologies that measure, analyze, predict, protect, and control the grid of the future.

Reference Links

- [DOE Announces \\$40 Million for Grid Modernization Initiative](#)
- [DOE Allots \\$40M for Grid Modernization Projects](#)

DOE and FERC Discussed Best Practices and Increasing Investment in Energy Systems in Response to Cyber Threats

In February 2019, the US Federal Energy Regulatory Commission and Department of Energy examined how federal and state regulators can foster investment in energy infrastructure security and respond to cyber and physical threats to the power and natural gas sectors and released their findings at a late March 2019 technical conference.

Reference Links

- [US FERC, DOE to examine potential incentives to bolster investment in energy security](#)
- [DOE and FERC Mull Incentivizing Cybersecurity, Physical Security of Power and Gas Infrastructure](#)
- [DOE, FERC Announce Technical Conference on Energy Infrastructure Security Practices](#)

DOE Awarded \$46M to Mitigate Cyber-Physical Threats to Solar Grid

In November 2018, the U.S. Department of Energy (DOE) announced that they planned to award \$46 million in research funding to 10 projects over the next three years with amounts varying from \$2 to \$10 million in size, to advance strategies to mitigate cyber and physical threats to solar energy grids. Applicants are encouraged to work with local municipalities – including state, local, tribal, and territories – to take steps to manage cyber and physical threats to improve the resiliency of solar-generated electricity.

Reference Links

- [Department of Energy Announces \\$46 Million to Improve Resiliency of Solar Generation](#)

- [DOE to award \\$46M to mitigate cyber, other threats to solar grid](#)
- [DOE frees up \\$46M to protect solar power](#)

Jack Voltaic 2.0

In July 2018, the Army Cyber Institute the City of Houston, in partnership with, AECOM, Circadence, the State of Texas, federal agencies, and regional public and private sectors, conducted the Jack Voltaic 2.0 Cyber Research Project. The event involved 44 organizations and 200 participants from 8 different critical infrastructure sectors. The goal of the project over a year in planning was to observe and assess the ability of interdependent critical infrastructure sectors to respond to combined cyber and physical attacks. Jack Voltaic 2.0 assembled critical infrastructure partners to conduct a research experiment to identify gaps in critical infrastructure cybersecurity.

The experiment employed a cyber exercise involving stakeholder-players from eight sectors including the energy sector. The JV 2.0 Governance and Planning Committee, comprised of representatives across eight critical infrastructure sectors, met to express their security priorities. Through analysis of their perceived strengths and weaknesses, participants tailored the exercise to stress specific aspects of their incident response and disaster recovery plans.

Reference Links

- [JACK VOLTAIC 2.0: Threats to Critical Infrastructure](#)

Legislation

Similarly, Congress is actively proposing and reviewing legislation to fund initiatives to secure energy infrastructure, programs to train energy cybersecurity personnel, and launch efforts to audit and modernize energy networks and systems. The initiatives below are examples of some of the proactive legislative efforts underway to secure America's energy infrastructure. While some of these bills may have a low probability of becoming law, the purpose of this section of the report is to emphasize that the legislative community is aware of threats to the energy sector, not to argue the merits of each bill mentioned.

The summaries and links have been directly pulled from [ICIT's Monthly Cyber Legislation Report](#).

S. 174: Securing Energy Infrastructure Act

S. 174 provided for the establishment of a pilot program to identify security vulnerabilities of certain entities in the energy sector.

[S. 876: Energy Jobs for our Heroes Act of 2019](#)

S. 876 amended the Energy Policy Act of 2005 to require the Secretary of Energy to establish a program to prepare veterans for careers in the energy industry, including the solar, wind, cybersecurity, and other low-carbon emissions sectors or zero-emissions sectors of the energy industry.

[H.R. 2114: Enhancing State Energy Security Planning and Emergency Preparedness Act of 2019](#)

H.R. 2114 amended the Energy Policy and Conservation Act to provide Federal financial assistance to States to implement, review, and revise State energy infrastructure physical and cyber security.

[H.R. 680: Securing Energy Infrastructure Act](#)

H.R. 680 provided for the establishment of a pilot program to identify security vulnerabilities of certain entities in the energy sector.

[H.R. 359: Enhancing Grid Security through Public-Private Partnerships Act](#)

H.R. 359 provided for certain programs and developments in the Department of Energy concerning the cybersecurity and vulnerabilities of, and physical threats to, the electric grid and other energy infrastructure.

[H.R. 5240: Enhancing Grid Security through Public-Private Partnerships Act](#)

H.R. 5240 provides for certain programs and developments in the Department of Energy concerning the cybersecurity and vulnerabilities of, and physical threats to, the electric grid, and for other purposes.

[S. 3677: Enhancing Grid Security through Public-Private Partnerships Act](#)

S. 3677 provides for certain programs and developments in the Department of Energy concerning the cybersecurity and vulnerabilities of, and physical threats to, the electric grid.

[S. 2991: Promoting Cybersecurity for Rural Electric Utilities Act](#)

S. 2991 amended the Rural Electrification Act of 1936 to make cybersecurity and grid security improvements eligible for electric loans and loan guarantees under that Act.

[H.R. 2741](#)

H.R. 2741 aimed to rebuild and modernize the Nation's infrastructure to expand access to broadband and Next Generation 9-1-1, rehabilitate drinking water infrastructure, modernize the electric grid and energy supply infrastructure, redevelop brownfields, strengthen health care infrastructure, create jobs, and protect public health and the environment.

Conclusion

The energy sector will continue to be targeted by adversaries due to the significant impact a successful attack would have on the affected region. The energy sector supply chain, like those in other critical infrastructure sectors, must undergo radical cultural and operational change to improve resiliency against these threats – an undeniable and complex reality. So too must policymakers in congress and federal agencies step-up bipartisan efforts to support the needs of the sector.

With so much to be done, it is easy to overlook the incremental progress that is already underway. However, the daunting scope of the task is precisely why we must ensure the community is aware of meaningful efforts by policymakers and regulators to defend the energy sector. By socializing the initiatives underway, we inspire sector stakeholders to build on existing foundations of success and ensure them that our nation's top leaders "have their back." People are often touted as the key to the success or failure of critical infrastructure protection. Let us ensure that conversations about the insecurity of our sectors are balanced with an accurate portrayal of the progress being made, however incremental, insufficient, or infantile that progress may be.

Sources

[1] S. Lyngaas, "Yet another hacking group is targeting oil and gas companies, Dragos says - CyberScoop", *CyberScoop*, 2019. [Online]. Available: <https://www.cyberscoop.com/dragos-oil-gas-hexane-industrial-hacking/>. [Accessed: 02- Sep- 2019].

[2] "HEXANE", *Dragos.com*, 2019. [Online]. Available: <https://dragos.com/resource/hexane/>. [Accessed: 02- Sep- 2019].

[3] M. Raggi and D. Schwarz, "LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards | Proofpoint US", *Proofpoint.com*, 2019. [Online]. Available: <https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks>. [Accessed: 02- Sep- 2019].

[4] A. Matsuda and I. Muhammad, "APT10 Targeting Japanese Corporations Using Updated TTPs", *FireEye*, 2018. [Online]. Available: <https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html>. [Accessed: 02- Sep- 2019].

[5] "CYBERSECURITY UPDATE: March 7: Triton, Karen Evans Q&A, Chinese hacks", *Eenews.net*, 2019. [Online]. Available: https://www.eenews.net/newsletters/cybersecurity_update/1060123593. [Accessed: 02- Sep- 2019].