Homeland Security

INTELLIGENCE ASSESSMENT

(U//FOUO) Damaging Cyber Attacks Possible but Not Likely Against the US Energy Sector

27 January 2016

Office of Intelligence and Analysis

IA-0060-16

Homeland Security
Office of Intelligence and Analysis

INTELLIGENCE ASSESSMENT

22 January 2016

(U//FOUO) Damaging Cyber Attacks Possible but Not Likely Against the US Energy Sector

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the Industrial Control Systems Computer Emergency Response Team (ICS-CERT).

(U) Scope

(U//FOUO) This *Assessment* establishes a baseline analysis of cyber threats to the US energy sector based on comprehensive FY 2014 incident reporting data compiled by ICS-CERT, as well as reporting by the Intelligence Community (IC), private sector cybersecurity industry, and open source media between early 2011 and January 2016. This *Assessment* is designed to help close gaps between the private sector's and the IC's understanding of current cyber threats facing the US energy sector. Critical infrastructure owners and operators can use this analysis to better understand cyber threats facing the US energy sector and help focus defensive strategies and operations to mitigate these threats. The *Assessment* does not include an in-depth analysis of foreign cyber doctrines or nation-state red lines for conducting cyber attacks against the United States. The information cutoff date for this *Assessment* is January 2016.

(U) Key Judgments

(U//FOUO) We assess the threat of a damaging or disruptive cyber attack against the US energy sector is low. We judge advanced persistent threat (APT) nation-state cyber actors are targeting US energy sector enterprise networks primarily to conduct cyber espionage. The APT activity directed against sector industrial control system (ICS) networks probably is focused on acquiring and maintaining persistent access to facilitate the introduction of malware, and likely is part of nation-state contingency planning that would only be implemented to conduct a damaging or disruptive attack in the event of hostilities with the United States.

(U//FOUO) We assess the majority of malicious activity occurring against the US energy sector is low-level cybercrime that is likely opportunistic in nature rather than specifically aimed at the sector, is financially or ideologically motivated, and is not meant to be destructive.

(U//FOUO) We assess that imprecise use of the term "cyber attack" in open source media reporting and throughout the private sector has led to misperceptions about the cyber threat to the US energy sector.

(U) Industrial Control Systems

(U) ICS are computers that control real-world activity; for example, ICS are used to run power plants, manufacturing assembly lines, commercial air conditioning systems, and building elevators.

(U//FOUO) Advanced Persistent Threat Actors Not Likely To Conduct Damaging or Disruptive Attack

(U//FOUO) We assess the threat of a damaging or disruptive cyber attack against the US energy sector is low. We judge APT nation-state cyber actors are targeting US energy sector enterprise networks primarily to conduct cyber espionage. The APT activity directed against sector ICS networks probably is focused on acquiring and maintaining persistent access to facilitate the introduction of malware, and likely is part of nation-state contingency planning that would only be implemented to conduct a damaging or disruptive attack in the event of hostilities with the United States.

» (U//FOUO) APT actors were responsible for at least 17 intrusions against the US energy sector in FY 2014, according to ICS-CERT incident report data—the last full year for which this data was available.[1] Included in these intrusions are incidents of data theft from enterprise networks and accessing and maintaining presence on ICS. APT actors did not cause any damage or disruption in any of the 17 reported incidents, according to the same ICS-CERT incident report data.[2]

» (U//FOUO) ICS-CERT in late 2014 became aware of an ongoing campaign, dating to 2011, targeting ICS devices worldwide using Havex malware, according to ICS-CERT alerts and cybersecurity industry analysis.[3,4,5,6] This activity is attributed to suspected Russian state-sponsored actors according to cybersecurity industry analysis.[7,8]

(U//FOUO) Havex Malware

(U//FOUO) ***Havex*** *is a malware tool likely developed by Russian state-sponsored cyber actors. Its main function is to gather system information, but it also can run specialized plug-ins for additional capabilities.[9,10]*

» (U//FOUO) APT actors in FY 2014 were responsible for two confirmed intrusions into US petroleum organizations' enterprise networks, and are suspected of exfiltrating data in at least one case, according to ICS-CERT incident report data.[11]

(U) Ukraine Power Outage

(U//FOUO) Open source media and various US cybersecurity threat intelligence companies have claimed that at least six Ukrainian regional power providers in late December suffered a cyber attack causing the loss of power for more than 80,000 customers for up to six hours[12,13] Due to limited authoritative reporting, I&A is unable to confirm the event was triggered by cyber means. While not independently confirmed as the cause of the outage, malware provided by Kyiv indicates the presence of a variant of an ICS-specific malware on the energy provider's systems, according to ICS-CERT analysis.[14] The variant provided by the Ukrainian Government has the capability to enable remote access and delete computer content, including system drives.[15] I&A cannot attribute this operation to any specific cyber actor, but the attacks are consistent with our understanding of Moscow's capability and intent, including observations of cyber operations during regional tensions. This incident does not represent an increase in the threat of a disruptive or destructive attack on US energy infrastructure, which I&A assesses is low.

(U//FOUO) Low-level Cybercrime Predominant Activity Against US Energy Sector

(U//FOUO) We assess the majority of malicious activity occurring against the energy sector is low-level cybercrime that is likely opportunistic in nature rather than specifically aimed at the sector, is financially or ideologically motivated, and is not meant to be destructive. Low-level activity such as that by cybercriminals or criminal hackers is less likely to be reported to ICS-CERT, as the organizations themselves may be able to handle the incident—meaning the number of low-level cybercrime incidents is probably much higher. Low-level cybercrime incidents cost the energy sector billions of dollars in cybersecurity spending and insurance coverage against cyber attacks.[16]

» (U//FOUO) Of the cyber incidents against the US energy sector reported to ICS-CERT in FY 2014, 63 percent involved unattributed, low-level activity against enterprise networks—for which we have insufficient information to provide definitive attribution.[17] We assess these incidents likely were conducted by cybercriminals, criminal hackers, unknown actors, and insiders. In addition, many of these incidents were handled independently of ICS-CERT, either by the victim organizations themselves or by third-party consultants.

» (U//FOUO) Unknown actors in FY 2014 used the Bang distributed denial-of-service (DDoS) malware to infect at least four US electricity organizations, according to ICS-CERT incident report data.[18] DDoS malware is typically spread by targeting vulnerabilities rather than specific organizations, indicating the electricity organizations probably were not targeted specifically.

» (U//FOUO) Cybercriminals in FY 2014 used Cryptolocker ransomware to infect three US energy organizations, according to ICS-CERT incident report data.[19] Cryptolocker encrypts the victim's data so it can no longer be accessed

without a passkey, which only the cybercriminal possesses. To recover the data, the victim must pay a ransom—usually in bitcoins—to the cybercriminal.

» (U) Unidentified cybercriminals in May 2013 compromised the payroll login credentials of a North Carolina fuel distribution company, and during the course of five days stole more than $800,000 before the theft was noticed, according to a well-known cybersecurity media outlet.[20]

(U//FOUO) Misperceptions about Cyber Threats in the Energy Sector

(U//FOUO) We assess imprecise use of the term "cyber attack" in open source media reporting and throughout the private sector has led to misperceptions about the cyber threat to the US energy sector. The term "cyber attack" is frequently used to refer to any cyber incident directed against the US energy sector. This overuse of the term "cyber attack" creates an unnecessarily alarmist general view of the threat to the sector. "Cyber attack"—which should denote intent to cause denial, disruption, destruction, or other negative effects—is frequently used in the private sector to describe cyber espionage, and even low-level, untargeted incidents of cybercrime. Overuse of the term "cyber attack," risks "alarm fatigue," which could lead to longer response times or to missing important incidents.*

» (U//FOUO) A major media outlet reported in December 2014 that the nation's energy grid is constantly under "attack" by hackers. The article makes this claim by drawing on an ICS-CERT statement regarding the number of incidents it responded to in FY 2014.[21] In fact, none of these events were properly considered attacks because no disruption, denial, or destruction occurred; rather, these events are more correctly described as espionage or some other activity. The only two incidents that resulted in damage or disruption to the victim's systems were self-inflicted—caused by accidental misconfiguration, according to DHS incident report data.[22]

» (U//FOUO) Another major media outlet in November 2014 published an article speculating that China could shut down the US electric power grid through a cyber attack, but the article offered no concrete evidence to support this claim.[23] According to all sources of information available to the IC, ICS-CERT, and the private sector, there have been no damaging or destructive attacks against the US energy sector. We also have no reporting that Chinese cyber actors have ever accessed the ICS components of any US energy sector entity.

(U) Mitigation Measures

(U//FOUO) Regardless whether adversarial APT actors intend to conduct damaging attacks against the US energy sector, it is clear that the sector is vulnerable to low-level cybercrime and sophisticated state-sponsored APT activity. In properly segmented networks—where ICS components are not directly connected to the Internet—the enterprise network is often the entry point for targeted and untargeted malicious activity against ICS components. Energy sector asset owners and operators can reduce the risk of malicious activity reaching ICS components by better protecting and securing their enterprise networks. Four relatively simple tactics could result in a significant decrease in compromises: implementing up-to-date e-mail filters; keeping antivirus definitions current; keeping software patches current; and continually training users.

* (U) Alarm fatigue occurs when one is exposed to a large number of frequent alarms and consequently becomes desensitized to them. Desensitization can lead to longer response times or to missing important alarms.

(U) Appendix A: ICS-CERT and US-CERT Publications

(U//FOUO) ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the IC and coordinating efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector computer emergency response teams to share control systems-related security incidents and mitigation measures. ICS-CERT distributes advisories, alerts, bulletins, and recommended practices through its website: https://ics-cert.us-cert.gov/.

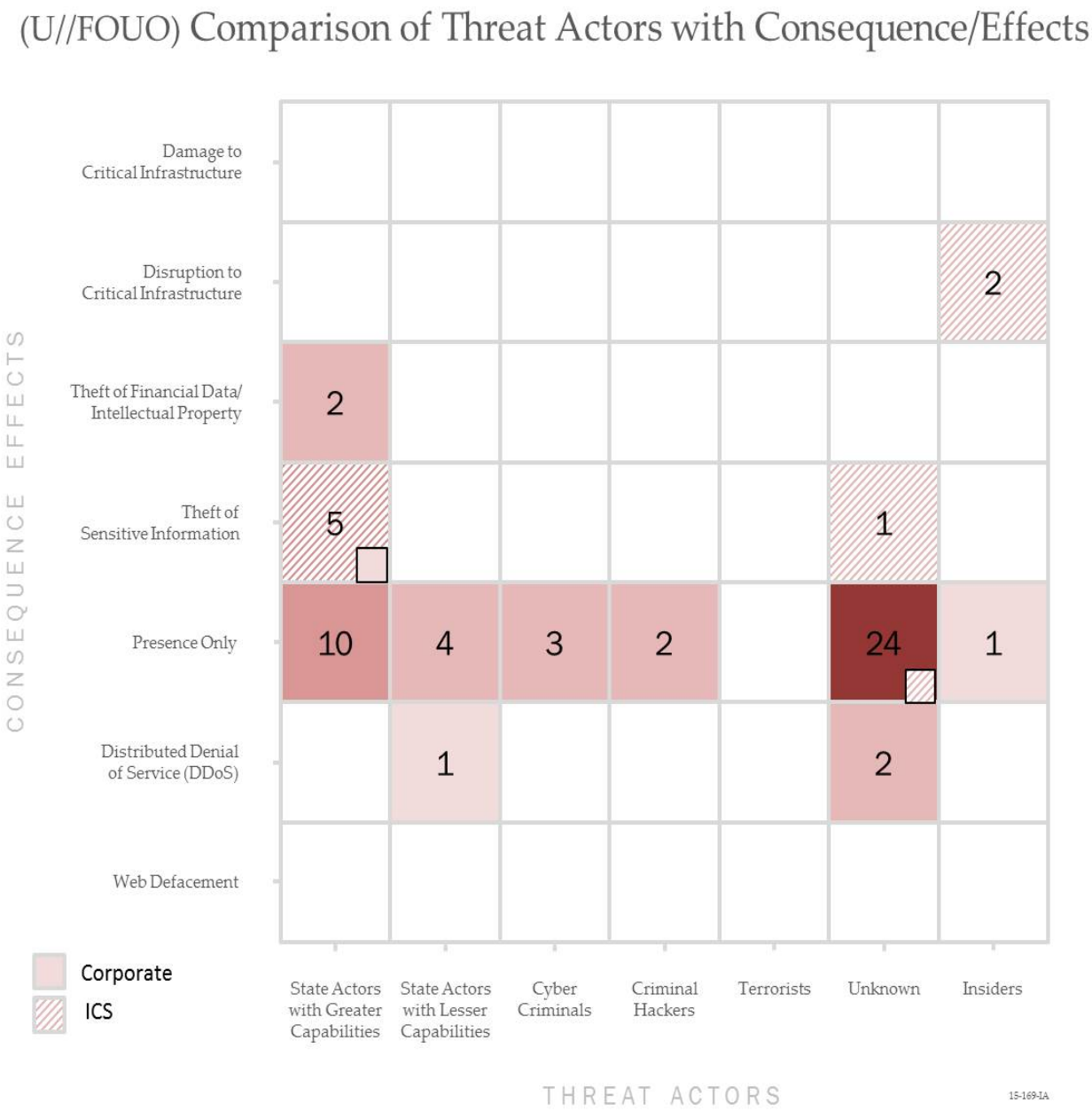
(U//FOUO) ICS-CERT has published **ICS-TIP-12-146-01B,** which provides guidance and recommended practices for intrusion detection and mitigation strategies. This technical information paper can be found at, https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B.

(U//FOUO) Organizations should routinely evaluate how to integrate best practices into their current environments to achieve system integrity, including the assurance of software authenticity and user identity. To assist in this endeavor, US-CERT has published recommended best practices in **TIP-11-075-01**, which can be found at, https://www.us-cert.gov/sites/default/files/publications/TIP11-075-01.pdf.

(U//FOUO) US critical infrastructure consists of the physical and cyber assets of public and private entities in several sectors, including the US energy sector. The healthy functioning of cyber assets is essential to our economy and national security. US-CERT has published a paper outlining strategic objectives to prevent cyber attacks against US critical infrastructure, reduce national vulnerability to cyber attacks, and minimize damage and recovery time from cyber attacks. This document can be found at, https://www.us-cert.gov/security-publications/national-strategy-secure-cyberspace.

(U) Appendix B: ICS-CERT Incident Report Data

(U) The below chart displays all ICS-CERT's 2014 US energy sector incident resport data by consequence and threat actors.



(U) The classification of the above table is U//FOUO.[24]

(U) Source Summary Statement

(U) This *Assessment* is based on ICS-CERT incident reporting data and information self-reported to ICS-CERT by victim organizations from Fiscal Year 2014—the last full year for which incident reporting data was available. This *Assessment* is also supported by information from reputable cybersecurity firms and the US media. We have **high confidence** in the accuracy and reliability of the ICS-CERT data, but acknowledge that newer ICS-CERT data might change our assessment. We also have **high confidence** in the reporting from reputable cybersecurity firms. Although the media reporting corroborates other reporting, this information may be intended to influence as well as inform, giving us **medium confidence** in this information. While we have **high to medium confidence** in the accuracy and reliability of these sources, our overall confidence in this assessment is **medium** because of the lack of data that would provide a comprehensive understanding of all malicious cyber incidents affecting the US energy sector.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) Tracked by: HSEC-1.1, HSEC-1.6, HSEC-1.10

[1] (U//FOUO); DHS; ICS-CERT; REPORT NO. UNK; FEB 2015; DOI 01 OCT 2013 – 30 SEP 2014; (U//FOUO); Fiscal Year 2014 Incident Response Data; Extracted information is U//FOUO; Overall document classification is S//NF.
[2] (U//FOUO); DHS; ICS-CERT; REPORT NO. UNK; FEB 2015; DOI 01 OCT 2013 – 30 SEP 2014; (U//FOUO); Fiscal Year 2014 Incident Response Data; Extracted information is U//FOUO; Overall document classification is S//NF.
[3] (U); DHS; ICS-CERT; "ICS Focused Malware (Update A)"; 07 JUL 2015; https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A; accessed on 08 SEP 2015.
[4] (U); PC WORLD; "New Havex Malware Variants Target Industrial Control System and SCADA Users"; http://www.pcworld.com/article/2367240/new-havex-malware-variants-target-industrial-control-system-and-scada-users.html; accessed on 07 JUL 2015; (U); Article.
[5] (U); DHS; ICS-CERT; ICS-ALERT-14-281-01B; 21 NOV 2014; DOI UNK; (U); Ongoing Sophisticated Malware Campaign Compromising ICS; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.
[6] (U); Symantec; "Dragonfly: Energy Companies Under Sabotage Threat"; 2012; https://files.sans.org/summit/ics2015/PDFs/Technical_Briefing_ICSTargeted_Threats.pdf; accessed on 08 SEP 2015; (U); Briefing.
[7] (U); PC WORLD; "New Havex Malware Variants Target Industrial Control System and SCADA Users"; http://www.pcworld.com/article/2367240/new-havex-malware-variants-target-industrial-control-system-and-scada-users.html; accessed on 07 JUL 2015; (U); Article.
[8] (U); Symantec; "Dragonfly: Energy Companies Under Sabotage Threat"; 2012; https://files.sans.org/summit/ics2015/PDFs/Technical_Briefing_ICSTargeted_Threats.pdf; accessed on 08 SEP 2015; (U); Briefing.
[9] (U); Symantec; "Dragonfly: Energy Companies Under Sabotage Threat"; 2012; https://files.sans.org/summit/ics2015/PDFs/Technical_Briefing_ICSTargeted_Threats.pdf; accessed on 08 SEP 2015; (U); Briefing.
[10] (U); DHS; ICS-CERT; "ICS Focused Malware (Update A)"; 07 JUL 2015; https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A; accessed on 08 SEP 2015.
[11] (U//FOUO); DHS; ICS-CERT; REPORT NO. UNK; FEB 2015; DOI 01 OCT 2013 – 30 SEP 2014; (U//FOUO); Fiscal Year 2014 Incident Response Data; Extracted information is U//FOUO; Overall document classification is S//NF.
[12] (U); iSight Partners; 15-00014822; 30 DEC 2015, Version 2; (U); Power Outage by Cyber Attack on Energy Control Systems in Several Regions of Ukraine; (U); Cybersecurity industry report.
[13] (U); Eduard Kovacs; Security Weekly; "Ukrain Accuses Russia of Hacking Power Companies"; www.securityweek.com/ukraine-accuses-russia-hacking-power-companies; (U); Article.

[14] (U); DHS; I&A Intelligence Analyst; Meeting; 04 JAN 2016; DOI UNK; (U); Meeting with ICS-CERT and E-ISAC; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.
[15] (U); DHS; I&A Intelligence Analyst; Meeting; 04 JAN 2016; DOI UNK; (U); Meeting with ICS-CERT and E-ISAC; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.
[16] (U); Fortune; "Lloyd's CEO: Cyber Attacks Cost Companies $400 Billion Every Year"; 23 JAN 2015; http://fortune.com/2015/01/23/cyber attack-insurance-lloyds/; accessed on 21 SEP 2015; (U); Article.
[17] (U//FOUO); DHS; ICS-CERT; REPORT NO. UNK; FEB 2015; DOI 01 OCT 2013 – 30 SEP 2014; (U//FOUO); Fiscal Year 2014 Incident Response Data; Extracted information is U//FOUO; Overall document classification is S//NF.
[18] (U//FOUO); DHS; ICS-CERT; REPORT NO. UNK; FEB 2015; DOI 01 OCT 2013 – 30 SEP 2014; (U//FOUO); Fiscal Year 2014 Incident Response Data; Extracted information is U//FOUO; Overall document classification is S//NF.
[19] (U//FOUO); DHS; ICS-CERT; REPORT NO. UNK; FEB 2015; DOI 01 OCT 2013 – 30 SEP 2014; (U//FOUO); Fiscal Year 2014 Incident Response Data; Extracted information is U//FOUO; Overall classification is S//NF.
[20] (U); Krebs on Security; "NC Fuel Distributor Hit by $800,000 Cyberheist"; 23 MAY 2013; http://www.krebsonsecurity.com/2013/05/nc-fuel-distributor-hit-by-800000-cyberheist/; accessed on 11 SEP 2015; (U); Blog.
[21] (U); CNN; "Hackers attacked the U.S. energy grid 79 times this year"; 29 DEC 2014; http://money.cnn.com/2014/11/18/technology/security/energy-grid-hack/; accessed on 8 SEP 2015; (U); Article.
[22] (U//FOUO); DHS; ICS-CERT; REPORT NO. UNK; FEB 2015; DOI 01 OCT 2013 – 30 SEP 2014; (U//FOUO); Fiscal Year 2014 Incident Response Data; Extracted information is U//FOUO; Overall document classification is S//NF.
[23] (U); Forbes; "Chinese Cyber Attack Could Shut Down U.S. Electric Power Grid"; 28 NOV 2014; http://www.forbes.com/sites/robertlenzner/2014/11/28/chinese-cyber attack-could-shut-down-u-s-electric-power-grid/; accessed on 8 SEP 2015; (U); Article.
[24] (U//FOUO); DHS; ICS-CERT; REPORT NO. UNK; FEB 2015; DOI 01 OCT 2013 – 30 SEP 2014; (U//FOUO); Fiscal Year 2014 Incident Response Data; Extracted information is U//FOUO; Overall document classification is S//NF.