MARKOWITZ HERBOLD PC

Jeffrey S. Lovinger | Lawyer
JeffreyLovinger@MarkowitzHerbold.com

March 11, 2022

Via Electronic Filing

Public Utility Commission of Oregon - Filing Center
PO Box 1088
Salem, OR 97308-1088

Re: Zena Solar, LLC v. Portland General Electric Company
OPUC Docket UM 2164

Attention Filing Center:

Enclosed for filing today, in the above-named docket, is the redacted version of the Declaration of Kellie Cloud in Support of Portland General Electric Company's Response to Zena Solar, LLC's Objections to Designation of Protected Information.

Thank you for your assistance.

Very truly yours,

Jeffrey S. Lovinger

Enclosure
1254365

BEFORE THE PUBLIC UTILITY COMMISSION

OF OREGON

UM 2164

ZENA SOLAR, LLC, Complainant, vs. PORTLAND GENERAL ELECTRIC COMPANY, Defendant.	**REDACTED** **DECLARATION OF KELLIE CLOUD IN SUPPORT OF PORTLAND GENERAL ELECTRIC COMPANY'S RESPONSE TO ZENA SOLAR LLC'S OBJECTION TO DESIGNATION OF PROTECTED INFORMATION**

I, Kellie Cloud, declare:

1. I am a Senior Director of Engineering at Portland General Electric Company ("PGE"), the defendant in this matter, and I make this declaration in support of PGE's Response to Zena Solar's Objection to Designation of Protected Information. The following statements are true and correct and, if called upon, I could competently testify to the facts averred herein.

Educational and Professional Background

2. I received a Bachelor of Science engineering science degree from Trinity University in San Antonio, Texas, magna cum laude. Prior to joining PGE, I spent five years as an electrical engineer at an engineering consulting firm, focusing on substation design and project engineering. I joined PGE in 2003, working as an electrical engineer specifically in the area of system protection. Since 2010 I have held various management-level roles, including engineering supervisor, senior substation operations technology manager, director of substation

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

operations, and my current role as senior director of engineering. My duties at PGE include leadership of engineering, design and technical teams that support PGE's generation, transmission, and distribution systems. We are responsible for developing infrastructure project plans, creating detailed project design documents, performing system studies, analyzing system performance, managing compliance programs, and providing engineering subject matter expertise. Leveraging control systems and protection expertise, I helped build PGE's NERC Critical Infrastructure Protection compliance program, created an Operational Technology cybersecurity team, and served as chair of PGE's Integrated Security Steering Committee. I am a licensed professional engineer with the Oregon State Board of Examiners of Engineering and Land Surveying in the field of electrical engineering and have been since 2000.

Zena's Objection to Designation of Protected Information.

3. On March 1, 2022, Zena Solar filed an Objection to Designation of Protected Information ("Objection"). Zena asks the Oregon Public Utility Commission ("Commission) to remove Protected Information designations from information contained in five exhibits: Zena Solar/123, Zena Solar/105, PGE/105, PGE/204, and PGE/205.

4. All five of these exhibits contain details about [redacted] This information is commercially sensitive information that is not public information.

PGE's System Information is Commercially Sensitive Information.

5. PGE protects detailed information regarding its electrical system as part of PGE's multi-layered strategy for protecting the system from cyber or physical attack. Such attacks can be launched by individuals, criminal groups, online unincorporated groups (e.g.,

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

hacker groups), governments, or others; such actors and are referred to collectively in this declaration as "attackers" or "bad actors."

6. In simplified terms, PGE's system has layers of protection including cyber or information technology ("IT") access (e.g., passwords, authentication protocols, firewalls, etc.), physical access (e.g., fenced substations with electronically locked access gates), monitoring and detection, and information protection (e.g., system configuration details that are not public). That last layer of protection, the layer at issue here, means that even if an attacker can obtain undetected cyber or physical access, the attacker would not know *how* or *where* to most effectively attack PGE's power system.

7. In order to stage a successful attack and disable PGE's system, an attacker needs to both penetrate PGE's cyber security or physical security measures *and* know enough details about PGE's system and its operation to know *how* to disrupt the system.

8. To maintain successful multi-layered protection of its system, PGE maintains robust cyber security measures, has upgraded the physical security of its infrastructure, operates an Integrated Security Operations Center, and is careful not to allow details about its system to become public. Such details would aid a bad actor in causing harm to the system should the bad actor manage to obtain cyber access or physical access. Even internal to PGE, equipment details and device configurations are shared only on an as-needed basis. PGE's standard system impact study ("SIS") documentation reflects a careful consideration of what information is required to study and implement safe, reliable energy resource integration.

9. This is not a hypothetical concern. Attached as **Exhibit 1** to this declaration is a true and accurate copy of an Electricity Information Sharing and Analysis Center white paper

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

providing an analysis of a 2015 cyberattack on the Ukrainian power grid.[1] The white paper notes that the attackers gained access to the operator's IT system and then, among other things, the attackers "rendered Serial-to-Ethernet devices at substations inoperable by corrupting their firmware."[2] In other words, in this real-world example, a cyber attacker used knowledge of electronic devices in a substation to impact key elements of the power system. The attacker's knowledge of the substation equipment enabled them to disconnect power to customers and significantly delay restoration. PGE seeks to limit public dissemination of details regarding the equipment in its electric system, especially details regarding its substations and relay configurations, in an effort to provide an additional layer of protection against cyber or physical attack of this sort. If bad actors do not have sufficient detail about the configuration of PGE's system, then it is more difficult for them to exploit a cyber or physical vulnerability (if one is discovered) to disable or impact the operation of PGE's system.

10. A bad actor can ascertain some information about the gross topography of PGE's system by observing system elements from outside physical security measures, such as a fence around a substation. But bad actors cannot decern details regarding the specific relays in use or their configuration from visual inspection of PGE's system from a distance. Bad actors cannot determine from such observations the detailed equipment ratings or fault study results that *could* indicate a vulnerability.

11. Protecting detailed system information from public release improves the security of PGE's system and is an important element of PGE's multi-layered approach to

[1] "Cyber-Attack Against Ukrainian Critical Infrastructure" (IR-Alert-H-16-056-01), Cybersecurity & Infrastructure Security Agency (Feb. 26, 2016; Revised Jul. 20, 2021), available at https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.
[2] *Id*. at 2.

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

protecting against cyber or physical attack. PGE protects details regarding the configuration and operation of equipment in its substations as part of its standard policy and approach to system security.

Protected Information in PGE/123

12. Zena Solar/123 is an [redacted]. Zena Solar/123 was provided to Zena Solar by PGE on August 19, 2020,[3] as confidential information under the parties' August 13, 2020, non-disclosure agreement ("NDA").[4] PGE did not provide the information in Zena Solar/123 to Zena Solar until the parties entered into their NDA, and PGE would not have provided the information to Zena Solar without an NDA.

13. Zena Solar/123 provides details regarding [redacted]. This is information of the sort that could be used by a bad actor to know *how* to adversely impact PGE's system if the bad actor can gain cyber access or physical access to PGE's system. As a result, the information in Zena Solar/123 is commercially sensitive information.

14. The information in Zena Solar/123 has not been made public.

15. In its Objection, Zena Solar argues that three one-line diagrams posted to PGE's OASIS website somehow disclose the information in Zena Solar/123.[5] However, the three publicly available one-line diagrams in question do not contain information about the Wallace Substation. None of the information contained in Zena Solar/123 is contained in the one-line

[3] *See* PGE/301 (copy of August 19, 2020 email from PGE conveying system information, including the One-Line Diagram for the Wallace Substation, i.e., Zena Solar/123, to Zena Solar).

[4] [redacted]. The executed version of the NDA was fully executed on August 19, 2020, and states in its opening paragraph that is effective as of August 13, 2020.

[5] Zena Solar's Objection to Designation of Protected Information ("Zena's Objection") at 12 & n.40.

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

diagrams found in the system impact studies for SPQ0158, SPQ0172, or SPQ0220. As a result, these one-line diagrams do not disclose the information in Zena Solar/123.

16. In its Objection, Zena Solar also argues that the information in the three SIS one-lines is "similar" to the information in Zena Solar/123. I disagree. With the simplified one lines PGE recently started issuing as part of an SIS, PGE aims to provide only the information regarding PGE's system relevant to the interconnection being studied. For example, details about feeders, transformers, and capacitor banks not impacted by the interconnection are typically excluded. Additionally, details about the transmission system, beyond substation high-side voltage, and the station service source used to safely operate the substation, are not shown. [redacted]

17. Zena's Objection references three one-line diagrams from three SISs – the studies for SPQ0158, SPQ0172, and SPQ0220.[6] In response to Zena's Objection, PGE reviewed the SIS for each of these applications and PGE has concluded that the one-line for the SIS for SPQ0220 contains a level of system detail not necessary for an SIS and inconsistent with PGE's general goal of keeping system details confidential. PGE has therefore redacted confidential information from the one-line in the SIS for SPQ0220 from PGE's OASIS website. The one-line in the SIS for SPQ0220 (whether redacted or un-redacted) does not include any of the information in Zena Solar/123.

[6] *See* Zena's Objection at footnote 40.

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

18. The more detailed information a bad actor has about PGE's system and its operating characteristics, the more ability the bad actor has to determine *how* to disable PGE's system or cause outages if the bad actor can gain cyber or physical access to PGE's system. The [redacted] information in Zena Solar/123 is the type of system detail that could aid a bad actor in planning or executing an attack.

19. In its Objection, Zena argues that consistent with PGE's [redacted] (confidential copy available in this proceeding as Zena Solar/122), PGE should have issued a [redacted]. That is not correct. The SIS for SPQ0129 was issued November 6, 2018 (*see* Zena Solar/107, Nelson/1). This predates PGE's [redacted]. Even if [redacted] was applicable here (which it is not), PGE would have [redacted]

20. Zena Solar/123 was produced by PGE and provided to Zena Solar for confidential use by Zena Solar in conducting its iSIS and is subject to the terms of the NDA between PGE and Zena Solar. PGE's understanding and intent under the Settlement Agreement and the NDA, was that Zena Solar was agreeing [redacted].

Protected Information in Zena Solar/105 and PGE/105.

21. Zena Solar/123 includes the Part Number for the feeder relay at Wallace Substation, that Part Number is [redacted]. This is confidential information under the parties' NDA and Protected Information under the protective order.

PGE did not provide the confidential Part Number to Zena until after the parties' entered into their NDA and PGE would not have provided this information to Zena without the NDA. Zena is not challenging that the Part Number is confidential information.[7]

22. Zena Solar's engineering consultant, Jonathan Denman, took this confidential Part Number and used it to find on the Schweitzer Engineering Laboratories ("SEL") website the "Configuration Summary" for the feeder relay actually installed at Wallace Substation (that is Part Number [redacted]). Mr. Denman then attached this Configuration Summary as the last two pages of the iSIS that he performed and produced for Zena Solar. The iSIS has been filed in this case as Exhibit Zena Solar/105 and as Exhibit PGE/105. The Configuration Summary is at Zena Solar/105, Nelson/49-50, and at PGE/105, Cloud/36-37.

23. The Configuration Summary has three types of information that has been designated as Protected Information: (1) the Part Number; (2) the Key Code; and (3) the ten line-items of the Selected Options (including a description of the firmware/user interface). This information provides the specific configuration for the feeder relay actually installed at Wallace Substation. As such, this information is commercially sensitive information because the detailed configuration summary for a specific electronic relay could be used by a bad actor as part of an effort to penetrate PGE's multi-layered cyber and physical defenses and to harm PGE's system.

24. The more detailed information a bad actor has about PGE's equipment and its operating characteristics, the more ability the bad actor has to determine *how* to disable PGE's system or cause outages if the bad actor can gain cyber or physical access to PGE's system.

[7] Zena's Objection at 13 (requesting un-designation of Zena Solar/123, "except for the manufacturer relay part numbers that Zena Solar is not challenging.").

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

The information in the "Configuration Summary" for the feeder relays installed at Wallace Substation is the type of system detail that could aid a bad actor in planning or executing an attack. More specifically, [redacted] various functions could aid a bad actor in planning or executing an attack. For example, [redacted] The less of this detailed system information PGE makes public, the less information there is for bad actors to find and use in an attempt to harm PGE's system.

25. Mr. Gross's written testimony, PGE/200, does not publicly disclose that [redacted].

26. Mr. Gross's testimony at PGE/200, Gross/18:5-7 states: "PGE addresses DERs that do not backfeed with a feeder reclosing voltage supervision (hot line blocking) and this feature is already incorporated on this feeder circuit." This statement does not reveal that [redacted] Mr. Gross's testimony does not state what equipment is used to incorporate the hot line blocking feature [redacted] on the feeder *circuit*.

27. [redacted]

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

[redacted]

28. PGE's Distribution Interconnection Standard ("PGE's Standards") (Zena Solar/203, Denman/13, 16) does not disclose that [redacted]

29. PGE's Standards, instead, state only that "On feeders with reclosing, hot line indication is used to do hot line blocking."[8] [redacted]

30. Zena Solar/203, Denman/16 does not indicate that [redacted].

31. PGE's 2022 Wildfire Mitigation Plan does not disclose that [redacted]

32. PGE's 2022 Wildfire Mitigation Plan indicates that [redacted] and that feeders with SEL relays and SCADA have the additional capability of changing their operation sequence during wildfire season.[9] The plan does not state that [redacted] The plan does not include the SEL relay model numbers or firmware

[8] Zena Solar/203, Denman/13.
[9] *In re PGE Wildfire Protection Plan*, Docket No. UM 2208, PGE Wildfire Protection Plan at 23 (Dec. 30, 2021) ("Additionally, the distribution feeders servicing PGE's HRFZs (those equipped with Schweitzer Engineering Laboratories (SEL) relays and SCADA) can be set to operate in a specialized wildfire protective mode.").

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

version (e.g., [redacted]) for relays located at any specific substation, and the plan does not specifically address Wallace Substation. The plan also acknowledges that some feeders do not have [redacted][10] Additionally, the plan includes a map with the HRFZs under discussion, and Wallace Substation is not included in the HRFZs.[11] As a result, Wallace Substation is not addressed in PGE's 2022 Wildfire Mitigation Plan.

33. Zena's Objection states that that the Configuration Summary attached as the last two pages of Zena's iSIS was obtained by Mr. Denman from the SEL website. However, the only way Mr. Denman and Zena Solar knew to obtain the Configuration Summary in question as representative of the feeder relays installed at Wallace Substation is because PGE provided Zena Solar with a confidential Part Number under the terms of the parties' NDA. The Configuration Summary's use in the iSIS to report on the configuration of relays installed at Wallace Substation is information that is not public information.

Protected Information in PGE/204 and PGE/205.

34. PGE has filed the written testimony of its expert witness, protection engineer Lawrence Gross Jr., as Exhibit PGE/200. Two exhibits in support of Mr. Gross's written testimony are PGE/204 and PGE/205, which are [redacted] PGE/204 and PGE/205 provide

[10] *Id.* at 23 ("13kV feeders without SEL relays rely on electronic reclosers' necessary protection settings: Normal, Wildfire and Red Flag mode."), available at https://edocs.puc.state.or.us/efdocs/HAA/um2208haa115610.pdf.
[11] *Id.* at 14.

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

[redacted]

35. PGE/204 and PGE/205 have been designated as Protected Information in their entirety. [redacted] contained in PGE/204 and PGE/205 are commercially sensitive information. The information contained in PGE/204 and PGE/205 was prepared by Mr. Gross for this proceeding and has not been made public.

36. Zena Solar has requested that the Commission remove the Protected Information designation from three elements of PGE/204 and from three elements of PGE/205. Specifically, Zena Solar requests that the Commission remove the Protected Information designation from (1) [redacted]; and (3) [redacted]. These fault study details, including [redacted] are commercially sensitive because they could enable a bad actor to identify system vulnerabilities that could be leveraged to disrupt service.

37. The first element of PGE/204 and PGE/205 that Zena Sola seeks to un-designate is the information in the [redacted]. Mr. Gross's testimony at PGE/200, Gross/9-10, does not discuss the information from [redacted] in any way. The information [redacted] This information is commercially sensitive because its public release could aid a bad actor in identifying system vulnerabilities and developing an attack on PGE's system.

38. The second element of PGE/204 and PGE/205 that Zena Solar seeks to un-designate is the information in the [redacted]. The [redacted] provides items of

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

information that are [redacted] Mr. Gross's testimony refers to [redacted], but Mr. Gross's testimony does not reveal or discuss [redacted]. As a result, Mr. Gross's written testimony does not reveal the specific information [redacted]. The information in the [redacted] This information [redacted]. None of the [redacted] is discussed in Mr. Gross's written testimony. The information in the [redacted] is commercially sensitive because its public release could aid a bad actor is developing an attack on PGE.

39. The third element of PGE/204 and PGE/205 that Zena Sola seeks to de-designate is the [redacted] which is stated [redacted] This information is never discussed in Mr. Gross's testimony, PGE/200. The [redacted] is commercially sensitive because its public release could aid a bad actor is developing an attack on PGE.

Additional Argument and New Testimony in Zena's Objection and the Supporting Declarations

40. Zena Solar argues in its Objection, and Zena's witnesses testified in their March 1, 2022, declarations, that PGE has a 120% trip trigger for its 3V0 protective scheme.[12] This is not correct, and the details of PGE feeder relay settings are not discussed in the

[12] Zena's Objection at 16-17; *Id.* Attachment C at 2 (Declaration of Michael Beanland ("Beanland Decl.") ¶ 3) (Mar. 1, 2022); *Id.*, Attachment D at 1-2 (Declaration of Jonathan Denman ("Denman Decl.") ¶ 1).

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

testimony in this case beyond the requirement to comply with the abnormal voltage clearing times outlined in IEEE 1547. PGE has discussed this issue in its Reply Brief at pages 30-31.

41. Zena Solar argues in its Objection, and Zena's witnesses testified in their March 1, 2022, declarations, that PGE/204 and PGE/205 demonstrate that PGE's reverse power supervision method will not work.[13] This is incorrect.

42. PGE's system is designed to uphold safety and reliability, and I am not aware of any showing before the Commission that PGE's system is not designed to uphold safety and reliability.

I hereby declare that the above statement is true to the best of my knowledge and belief, and that I understand it is made for use as evidence in court and is subject to penalty for perjury.

DATED this 11th day of March, 2022.



Kellie Cloud

1255596

[13] Zena's Objection at 16-17; Beanland Decl. ¶ 4; Denman Decl. ¶ 2.

MARKOWITZ HERBOLD PC
1455 SW BROADWAY, SUITE 1900
PORTLAND, OREGON 97201
(503) 295-3085
Fax: (503) 323-9105

BEFORE THE PUBLIC UTILITY COMMISSION

OF OREGON

UM 2164

ZENA SOLAR, LLC, Complainant, vs. PORTLAND GENERAL ELECTRIC COMPANY, Defendant.	

EXHIBIT 1
TO DECLARATION OF KELLIE CLOUD
IN SUPPORT OF PORTLAND GENERAL ELECTRIC COMPANY'S
RESPONSE TO ZENA SOLAR'S OBJECTION TO DESIGNATION OF PROTECTED INFORMATION

"CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE" (IR-ALERT-H-16-056-01), CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (FEB. 26, 2016; REVISED JUL. 20, 2021),
AVAILABLE AT https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01

March 11, 2022

An official website of the United States government Here's how you know

TLP:WHITE

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

More ICS-CERT Alerts

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016 | Last revised: July 20, 2021

Legal Notice

All information products included in https://us-cert.cisa.gov/ics 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 https://us-cert.cisa.gov/tlp/.

Updated July 20, 2021: The U.S. Government attributes this activity to Russian nation-state cyber actors and assess that Russian nation-state cyber actors conducted a cyber campaign against Ukrainian critical infrastructure. For more information on Russian malicious cyber activity, refer to us-cert.cisa.gov/Russia.

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.

TLP:WHITE

TLP:WHITE

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.

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

TLP:WHITE

TLP:WHITE

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

TLP:WHITE

TLP:WHITE

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

TLP:WHITE

TLP:WHITE

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.

---

a NCCIC/ICS-CERT, Seven Steps to Effectively Defend Industrial Control Systems, https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf, 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/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf , web site last accessed February 25, 2016.

Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
or incident reporting: https://us-cert.cisa.gov/report

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

This product is provided subject to this [redacted]otification and this Privacy & Use policy.

TLP:WHITE