TLP:White

ICS Defense Use Case No. 6:

Modular ICS Malware

August 2, 2017

1325 G Street NW
Suite 600
Washington, DC 20005
404-446-9780 #2 | www.eisac.com

Table of Contents

Preface

Analysis of the Malware Reportedly Used in the December 2016 Ukrainian Power System Attack

This document contains a summary of information compiled from multiple publicly available sources, as well as analysis performed by the SANS Industrial Control Systems (ICS) team in relation to this event. Elements of the event provide an important learning opportunity for ICS defenders.

The Electricity Information Sharing and Analysis Center (E-ISAC) has been working closely with Ukrainian authorities to investigate the December 2016 incident and to better understand the technical nature of the attacks. It is normal for any investigation to reach multiple, and possibly competing, opinions of what happened, what groups were involved, what specific malware was used, intentions of the attacker, and other related observations. In this case, the E-ISAC has not been provided evidence to evaluate whether the specific malware or modules analyzed by the two commercial companies was used in the December 2016 incident. However, the E-ISAC does believe that this malware could cause the same observable impact if it had been used. The E-ISAC also believes that this malware DOES exist and could be used in a future attack, which leads to this statement:

"The importance of this Defense Use Case cannot be overstated – the malware discussed in this report is available to one or more threat actors that have demonstrated intent to disrupt electric grid operations. Whether it was used in support of the December 2016 incident in Ukraine is not germane to the urgency with which asset owners must take to understand its capabilities and be prepared for future mitigation." – Marcus H. Sachs, Chief Security Officer, North American Electric Reliability Corporation

Authors[1]:
Michael J. Assante
Robert M. Lee
Tim Conway

---

[1] *Special thanks to the team of Electricity Information Sharing and Analysis Center (E-ISAC) contributors, especially Tim Roxey; as well as Chris Sistrunk; and a few unnamed electric industry operators for their review and contributions.*

Summary of the Information and Reporting

On June 12, 2017, two cyber security companies, ESET and Dragos Inc., each released industry reports to the public that provided analysis of a series of malware modules that are ICS-specific and operate within a larger framework designed for attacker ease of implementation. ESET's[2] report identified the malware and named it "Industroyer."[3] The ESET report walked through the main malware components and identified the four ICS protocol payload modules analyzed, the ICS device-specific Denial of Service (DoS) exploit tool, and two additional tool capabilities used for data destruction and network port scanning. ESET's report concluded with a statement referencing the December 17, 2016, power outages that occurred in Ukraine and a statement that declared the high probability that Industroyer was used in the attack.

Dragos[4] also released its report on June 12, 2017, recognizing the ESET discovery, but re-naming the malware as "CrashOverride."[5] The authors noted that the term "crash" is derived from a function specifically named in the malware.[6] The Dragos report provided additional ICS context in its analysis and electric industry implications using attack scenarios to demonstrate potential adversary uses of the malware analyzed. Additionally, the Dragos report confirmed the CrashOverride malware was involved in the December 17, 2016, Ukraine attack. In the context of the threat actors that performed the attack, Dragos identified the activity group that developed the malware as Electrum, which they confirmed to have direct ties to the Sandworm team[7]. The Dragos report provided additional actionable information for asset owners and operators (AOO) to use in their detection and defense efforts.

Both reports cited the Ukraine power system events of 2015 and 2016, while indicating the progression of adversary capabilities. The graphic shown in Figure 1 is a mapping of recent ICS adversary campaigns, malware, and events, displayed by the level of ICS customization and associated ICS impacts achieved.

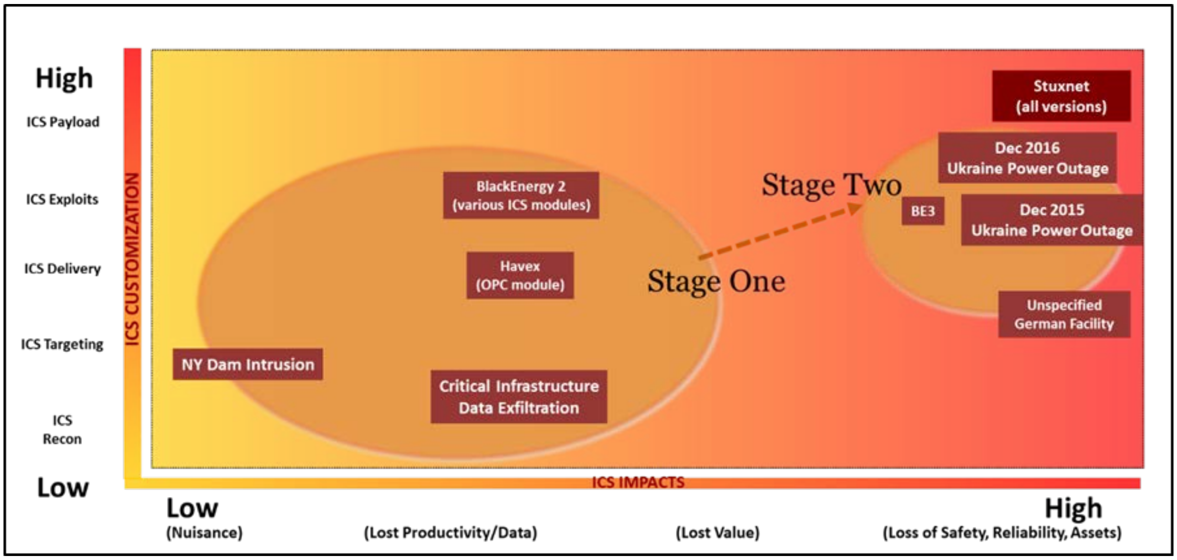


Figure 1: Recent ICS Activity Mapping

---

[2] https://www.eset.com/us/

[3] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

[4] https://dragos.com/

[5] https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[6] Malware is often named based on functions or references in the malware code. With two different names being discussed in various reports, the DUC typically uses the CRASHOVERRIDE name as it is also referenced as such in Industrial Controls Systems Computer Emergency Response Team (ICS-CERT) reports.

[7] https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html

In conjunction with the ESET and Dragos reports, several media outlets—Wired magazine[8], The Washington Post[9], and Reuters[10]—released articles about the attack; dozens of other articles were released throughout the week.

Since June 12, 2017, industry has received specific information on the attacks through webcasts, a North American Electric Reliability Corporation (NERC)-specific industry alert, and other industry-specific outreach activities. Regardless of this public information, many individuals within the electric industry and across the ICS community seek additional guidance, understanding, and resources to assist in their internal analysis of the risk posed by this malware.

This SANS ICS DUC is intended for a general public release and does not contain electric sector specific considerations. A private release has been coordinated through the E-ISAC portal for electric industry asset owners and operators specifically. The information presented in this TLP:White report is for the purpose of consolidating the open source information, clarifying important details surrounding the attack, offering lessons learned, and recommending approaches to help the ICS community search for and repel similar attacks. The SANS ICS DUC does not focus on the attribution of the attack, other than the attribution statements made in the industry reports.

Summary of Incidents Referenced

Both the ESET and Dragos reports cite the Ukraine 2015 power system cyber attack and point to the role of the CrashOverride malware in the 2016 Ukraine power system event. From an electric system operator perspective and a cyber operator perspective, significant differences exist between these two attacks that AOOs must understand when considering defender actions. The 2015 attack targeted three Ukrainian distribution entities causing distribution-level outages while damaging the utility's SCADA systems. The 2015 event is well documented and is discussed with specific defender-focused recommendations provided in the SANS Defense Use Case No. 5.[11] The 2016 attack occurred at the transmission-level with an attack against a regional SCADA system generally focused on a single 330 kV-to-110 kV-to-10 kV substation, resulting in a distribution-level outage.

---

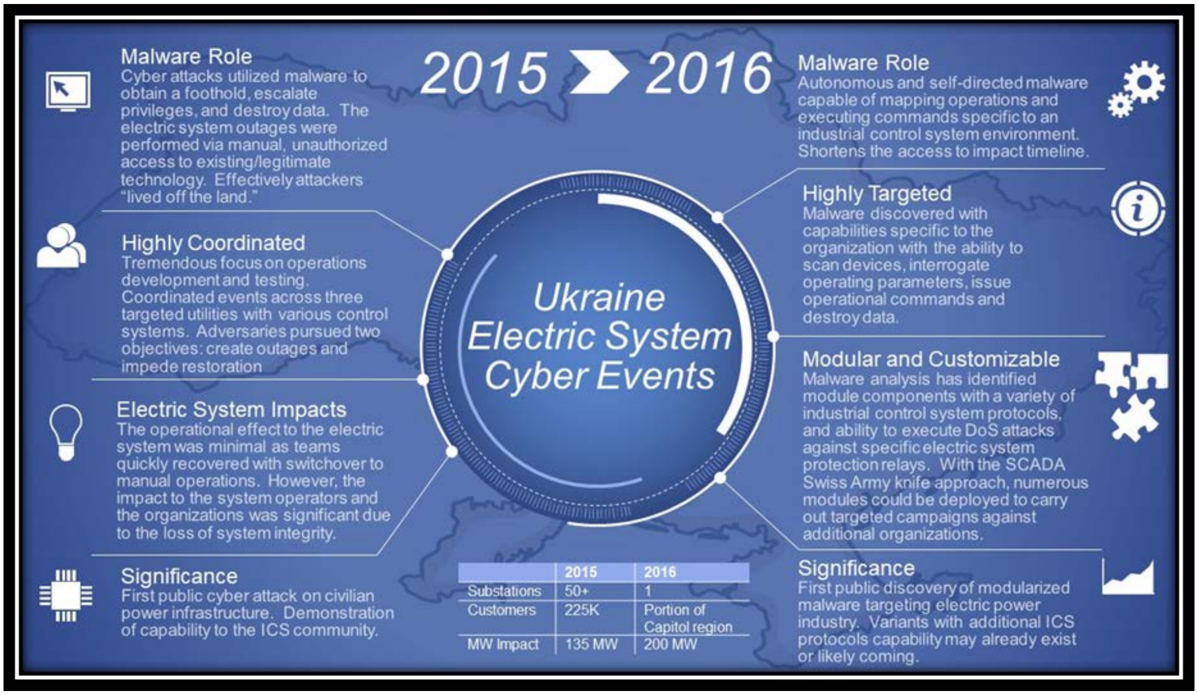
[8] https://www.wired.com/story/crash-override-malware/

[9] https://www.washingtonpost.com/world/national-security/russia-has-developed-a-cyber-weapon-that-can-disrupt-power-grids-according-to-new-research/2017/06/11/b91b773e-4eed-11e7-91eb-9611861a988f_story.html?utm_term=.6359fa2afb04

[10] https://www.reuters.com/article/us-cyber attack-utilities-idUSKBN1931EG

[11] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Figure 2 provides a summary of the 2015 and 2016 Ukraine power system cyber attacks. The remainder of this DUC will focus on the 2016 cyber attack and the role malware played in that attack.



2015 ➤ 2016

Ukraine Electric System Cyber Events

Malware Role
Cyber attacks utilized malware to obtain a foothold, escalate privileges, and destroy data. The electric system outages were performed via manual, unauthorized access to existing/legitimate technology. Effectively attackers "lived off the land."

Highly Coordinated
Tremendous focus on operations development and testing. Coordinated events across three targeted utilities with various control systems. Adversaries pursued two objectives: create outages and impede restoration

Electric System Impacts
The operational effect to the electric system was minimal as teams quickly recovered with switchover to manual operations. However, the impact to the system operators and the organizations was significant due to the loss of system integrity.

Significance
First public cyber attack on civilian power infrastructure. Demonstration of capability to the ICS community.

Malware Role
Autonomous and self-directed malware capable of mapping operations and executing commands specific to an industrial control system environment. Shortens the access to impact timeline.

Highly Targeted
Malware discovered with capabilities specific to the organization with the ability to scan devices, interrogate operating parameters, issue operational commands and destroy data.

Modular and Customizable
Malware analysis has identified module components with a variety of industrial control system protocols, and ability to execute DoS attacks against specific electric system protection relays. With the SCADA Swiss Army knife approach, numerous modules could be deployed to carry out targeted campaigns against additional organizations.

Significance
First public discovery of modularized malware targeting electric power industry. Variants with additional ICS protocols capability may already exist or likely coming.

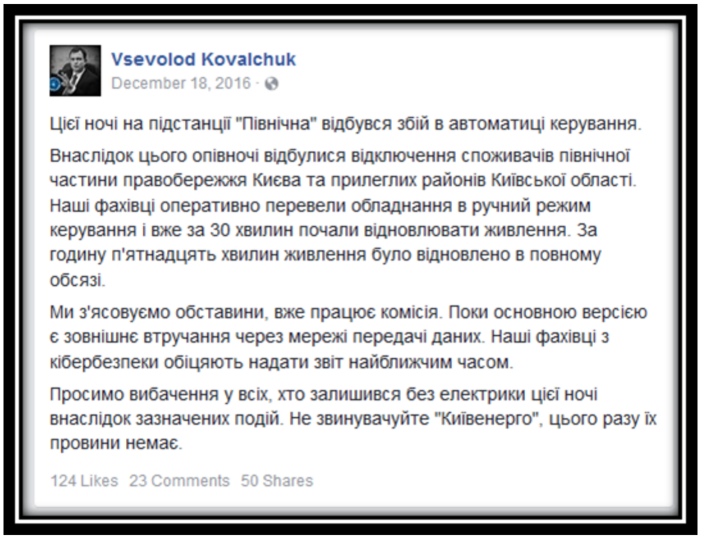
	2015	2016
Substations	50+	1
Customers	225K	Portion of Capitol region
MW Impact	135 MW	200 MW

Figure 2: 2015-2016 Ukraine Power System Cyber Attacks

Credibility[12], [13]

Analysts assigned a credibility score of *4 – Probably True* to the reports and claims made within the reports. The ESET report acknowledges that the malware could have been used in the 2016 attacks against the Ukrainian electric system and states that an investigation continues into the cause of the events on December 17, 2016. Therefore, the role malware played was not confirmed at the time ESET developed its report on June 12, 2017. The ESET report does provide the conclusion that the malware was probably used in the 2016 attacks. The Dragos report did however, confirm that the malware was used in the 2016 Ukrainian electric system attack.

The technical analysis each firm performed identified that the malware had the capability to issue the circuit breaker commands at the target substation by performing breaker control through the IEC 101, 104, or the 61850 protocol. The analysis also identified two specific activation dates contained within the launcher module for December 17 and December 20, 2016, which then called the payload modules and the wiper module. The wiper module had a delay of one-to-two hours in place depending on the version of the launcher module, leading to an action completion time on December 18, 2016. Based on public statements from leadership within the *Ukrenergo* (Ukrainian transmission system) energy company (see Figure 3 and Google translation in Figure 4) on December 18, 2016, the timeline of events and the description of what occurred aligns with the analysis and conclusions from the reports.



Vsevolod Kovalchuk
December 18, 2016 ·

Цієї ночі на підстанції "Північна" відбувся збій в автоматиці керування.

Внаслідок цього опівночі відбулися відключення споживачів північної частини правобережжя Києва та прилеглих районів Київської області. Наші фахівці оперативно перевели обладнання в ручний режим керування і вже за 30 хвилин почали відновлювати живлення. За годину п'ятнадцять хвилин живлення було відновлено в повному обсязі.

Ми з'ясовуємо обставини, вже працює комісія. Поки основною версією є зовнішнє втручання через мережі передачі даних. Наші фахівці з кібербезпеки обіцяють надати звіт найближчим часом.

Просимо вибачення у всіх, хто залишився без електрики цієї ночі внаслідок зазначених подій. Не звинувачуйте "Київенерго", цього разу їх провини немає.

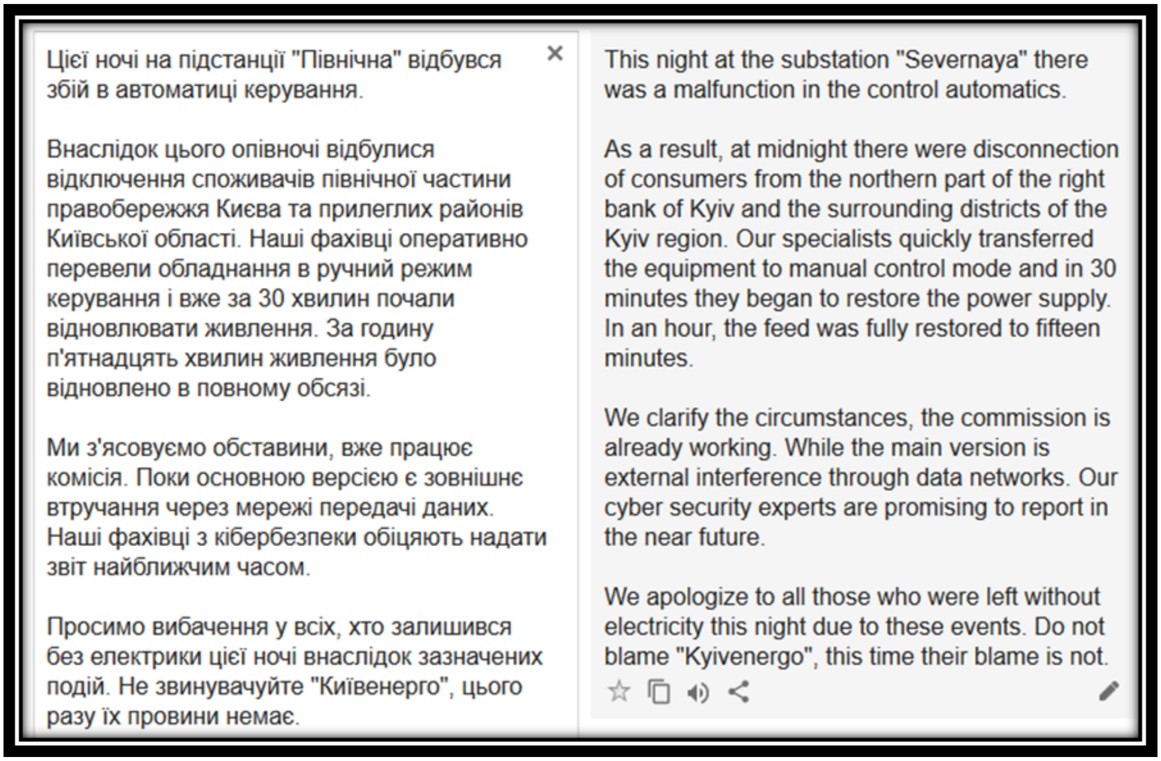
124 Likes 23 Comments 50 Shares

Figure 3: Ukrenergo Leadership Statements to Facebook on December 18, 2016

---

[12] Michael Assante and Tim Conway conducted this assessment. Since Robert Lee is part of the Dragos team, which conducted the analysis, he recused himself from the credibility scoring portion of this report.

[13] Credibility of the information is rated in a scale from 0-5: [0] Cannot be determined, [1] Improbable, [2] Doubtful, [3] Possibly true, [4] Probably true, [5] Confirmed.



Цієї ночі на підстанції "Північна" відбувся збій в автоматиці керування.

Внаслідок цього опівночі відбулися відключення споживачів північної частини правобережжя Києва та прилеглих районів Київської області. Наші фахівці оперативно перевели обладнання в ручний режим керування і вже за 30 хвилин почали відновлювати живлення. За годину п'ятнадцять хвилин живлення було відновлено в повному обсязі.

Ми з'ясовуємо обставини, вже працює комісія. Поки основною версією є зовнішнє втручання через мережі передачі даних. Наші фахівці з кібербезпеки обіцяють надати звіт найближчим часом.

Просимо вибачення у всіх, хто залишився без електрики цієї ночі внаслідок зазначених подій. Не звинувачуйте "Київенерго", цього разу їх провини немає.

This night at the substation "Severnaya" there was a malfunction in the control automatics.

As a result, at midnight there were disconnection of consumers from the northern part of the right bank of Kyiv and the surrounding districts of the Kyiv region. Our specialists quickly transferred the equipment to manual control mode and in 30 minutes they began to restore the power supply. In an hour, the feed was fully restored to fifteen minutes.

We clarify the circumstances, the commission is already working. While the main version is external interference through data networks. Our cyber security experts are promising to report in the near future.

We apologize to all those who were left without electricity this night due to these events. Do not blame "Kyivenergo", this time their blame is not.

Figure 4: Google Translation of Ukrenergo Facebook Post

The Dragos analysis of the IEC 104 module and the wiper module indicates that both occurred within minutes of each other, after 2:30 a.m. on December 18, which aligns with the event restoration and the approximate time the wiper module would have been initiated.

Both reports include a reference to the backdoor operation as communicating through a pre-positioned proxy server on the internal network that listened on TCP port 3128. However, Dragos noted that no proof existed that the backdoor was leveraged. In its analysis, many aspects of the framework were developed to facilitate a variety of attacks, but not all of the functionality was leveraged. In addition, the IEC 61850 and OPC modules had functionality to facilitate an automatic mapping of the environment, which would negate the need for command and control (C2) servers.

The backdoor module used a hard-coded internal network proxy server address that allowed for internal communications out to the adversary's C2 server. With this configuration, researchers assume that the hard-coded internal network proxy server Internet Protocol (IP) address is specific to a target organization; however, this requires further validation. The reports also include a reference to functionality of an additional backdoor to communicate directly to C2 servers in the event the proxy server is unavailable.

Once the back door is operational, the adversary could leverage it to gain information about the targeted field substation environment and load the malware with proper configuration information to execute the attack. If the C2 portion of the malware is used, some potential target locations to consider for the launcher component and payload could be:

1. **Launcher located on a system that has access to execute commands from a control center.** In this option, the malware backdoor would need to install the launcher on an asset that can effectively communicate out to the internal proxy node as described in the main backdoor functionality or directly to the C2 server through the additional backdoor functionality, as well as have the ability to route commands to or through the communications front ends to the targeted substation as in Figure 5.

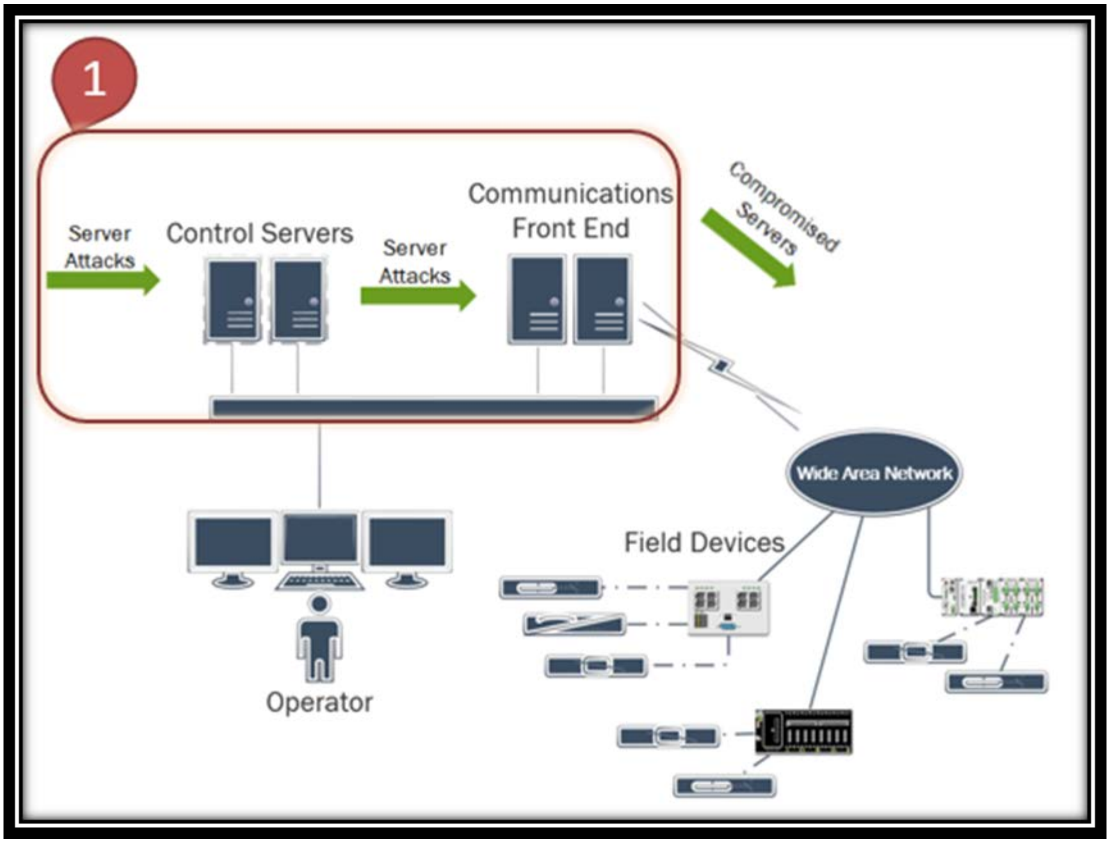


Figure 5: Malware Positioned within the Control Center Environment

2. **Launcher executed from a system with direct access to the SCADA network communications infrastructure.** In this option, the malware backdoor would need to install the launcher on an asset that can effectively communicate out to the internal proxy node as described in the main backdoor functionality or directly to the C2 server through the additional backdoor functionality, as well as have the ability to communicate directly into the SCADA communications network as in Figure 6.

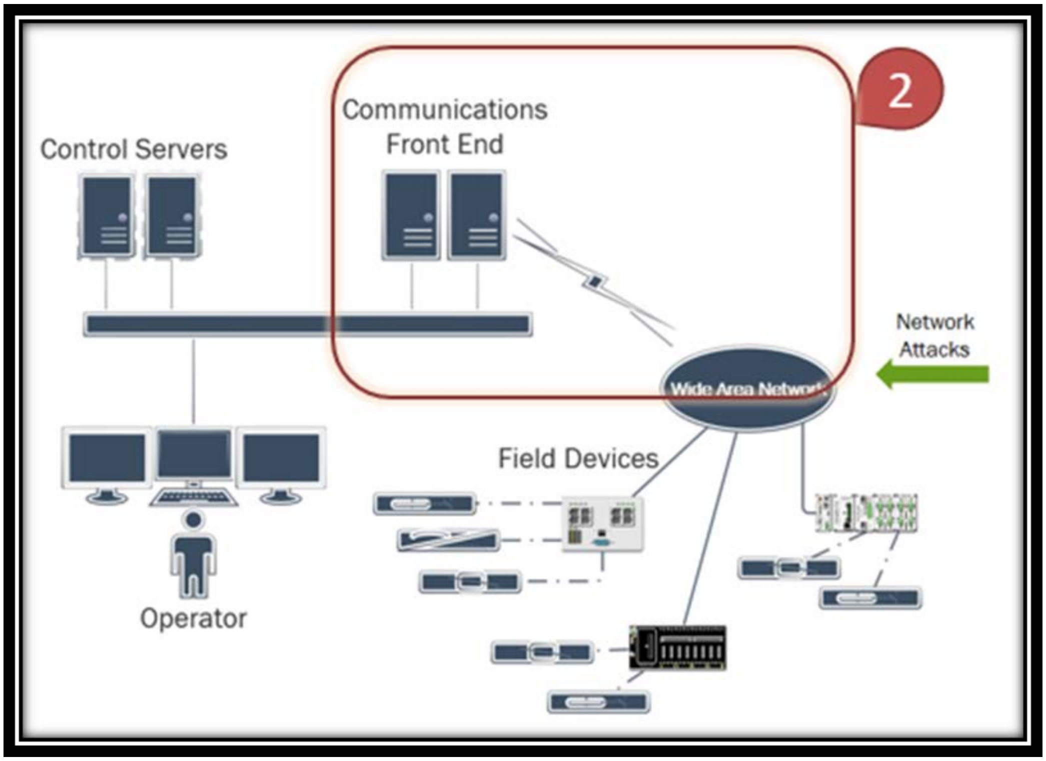


Figure 6: Malware Positioned on an Asset within the Communications Network

3. **Launcher located on a targeted system directly within the substation environment.** In this option, the malware backdoor would need to install the launcher on an asset that can effectively communicate to the internal proxy node as described in the main backdoor functionality or directly to the C2 server through the additional backdoor functionality, as well as have the ability to communicate directly to the devices within the substation network as in Figure 7.

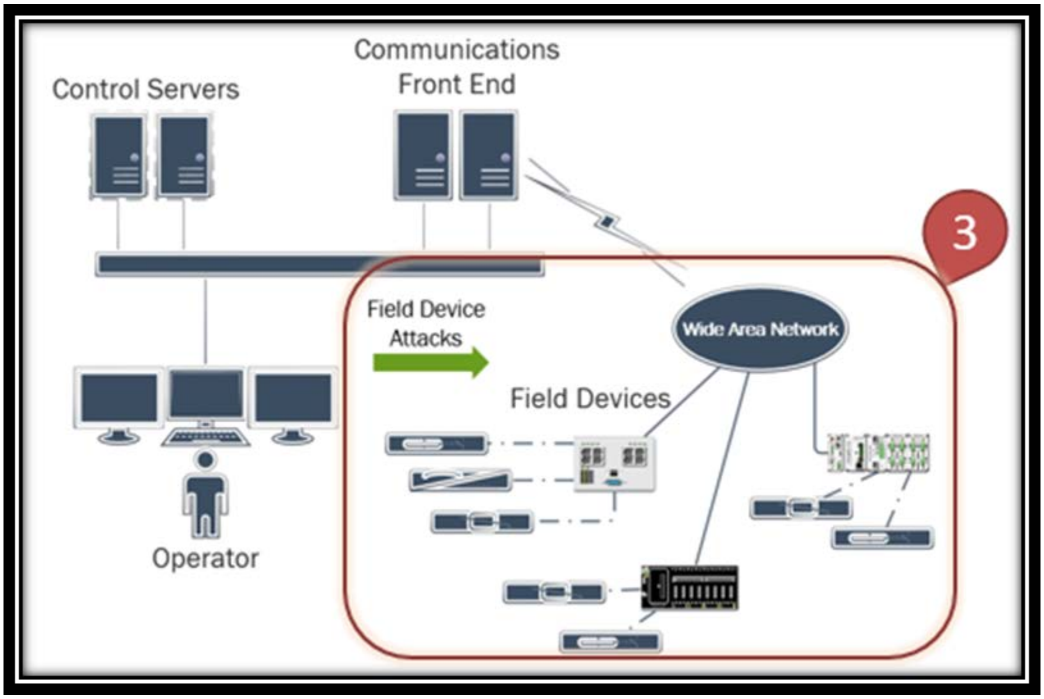
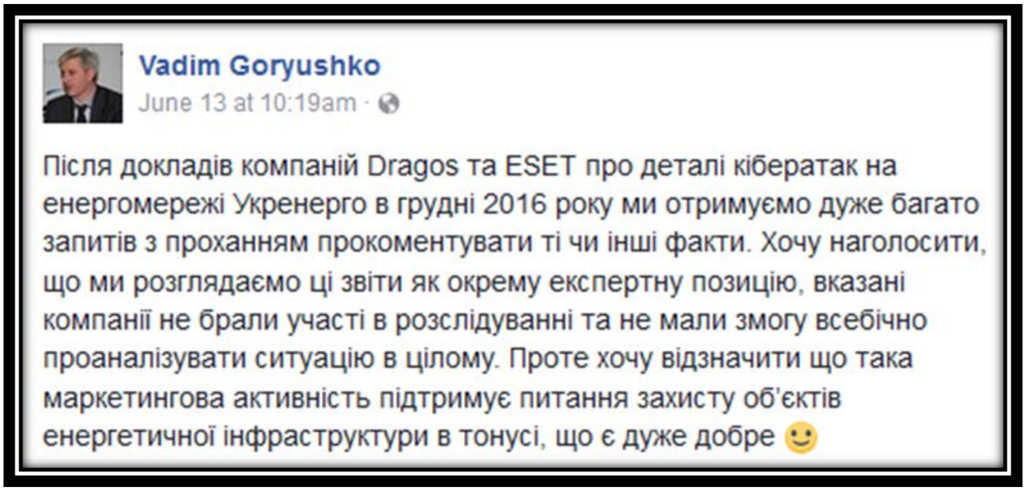


Figure 7: Malware Positioned on an Asset within the Substation

If an adversary had an active and persistent position in any of these environments, the adversary likely could have used the tools and technology within the organization to conduct the attack or to have developed a script to execute the commands necessary to achieve the objective of operating the circuit breakers. For this reason, and the fact that not all of the functionality in the framework was leveraged, Dragos assessed that the adversary developed CrashOverride's ability to target multiple locations. Additionally, researchers assessed that this attack could have been a test of functionality and a demonstration of capability. Given the details available, this assessment also is consistent with SANS' understanding and assessment.

The ESET and Dragos reports both provided a highly credible analysis in relation to the malware modules and would have scored a 5 - *Confirmed* in relation to the malware analysis alone. Both reports also provided linkages to the malware and the 2016 Ukraine electric system cyber attacks, however due to the nature of what could be shared publicly in the reports, and the level of details specific to how they confirmed the malware was used, the authors of the DUC could only provide a 3 - *Possibly True* in reference to the malware involvement in the 2016 Ukraine attacks.

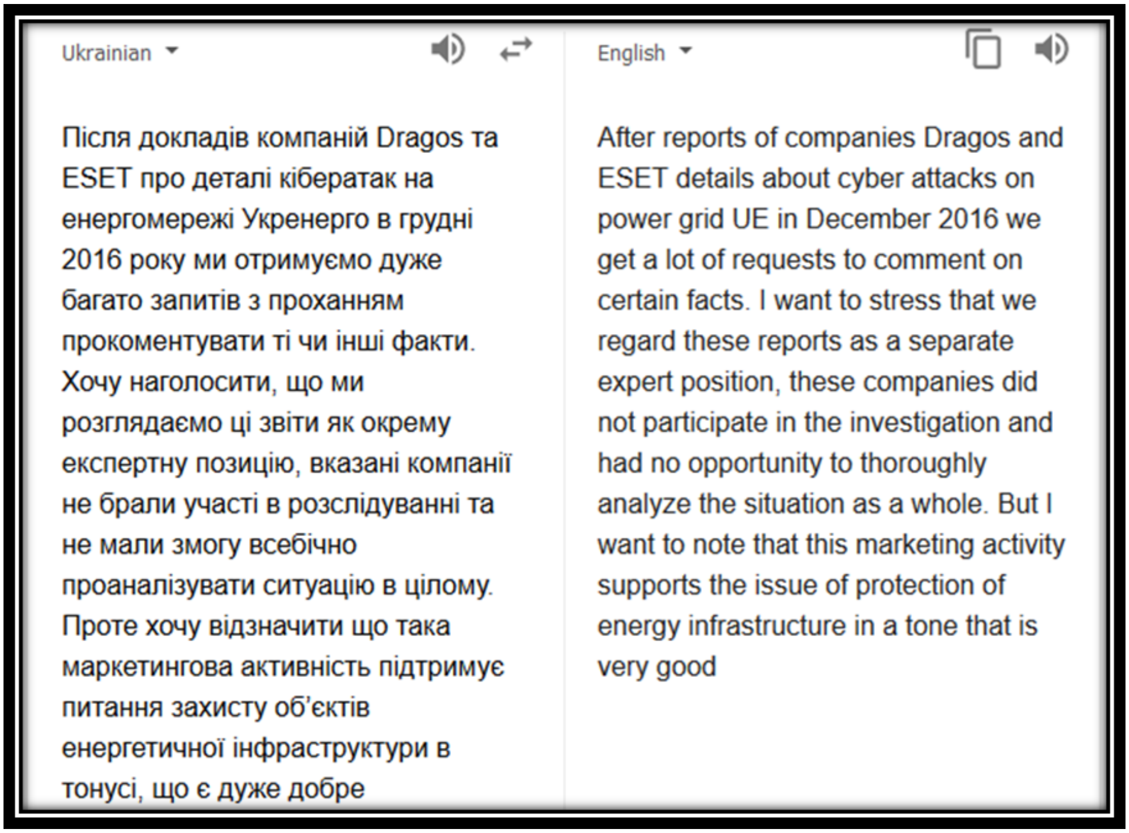
Without confirmation from the targeted organization, indicating if the malware was discovered on-site, it is not appropriate for a higher score (e.g. *5 – Confirmed*) for this December 17 event. As of the writing of this DUC, the *Ukrenergo* has made no additional claims confirming the presence of the malware and neither security firm has claimed involvement in the incident response at the impacted site. A public statement from the *Ukrenergo* regarding the reports has been made, as shown in Figures 8 and 9. The majority of the content in the reports is in relation to the malware analysis (credibility score =5) and some references to the malware's use in the 2016 Ukraine power system attack (credibility score = 3). Recognizing this mix of content in the reports the DUC authors felt an overall score of 4 – *Probably True* was warranted.



Vadim Goryushko
June 13 at 10:19am ·

Після докладів компаній Dragos та ESET про деталі кібератак на енергомережі Укренерго в грудні 2016 року ми отримуємо дуже багато запитів з проханням прокоментувати ті чи інші факти. Хочу наголосити, що ми розглядаємо ці звіти як окрему експертну позицію, вказані компанії не брали участі в розслідуванні та не мали змогу всебічно проаналізувати ситуацію в цілому. Проте хочу відзначити що така маркетингова активність підтримує питання захисту об'єктів енергетичної інфраструктури в тонусі, що є дуже добре 🙂

Figure 8: Ukrenergo Post Regarding the Reports



Після докладів компаній Dragos та ESET про деталі кібератак на енергомережі Укренерго в грудні 2016 року ми отримуємо дуже багато запитів з проханням прокоментувати ті чи інші факти. Хочу наголосити, що ми розглядаємо ці звіти як окрему експертну позицію, вказані компанії не брали участі в розслідуванні та не мали змогу всебічно проаналізувати ситуацію в цілому. Проте хочу відзначити що така маркетингова активність підтримує питання захисту об'єктів енергетичної інфраструктури в тонусі, що є дуже добре

After reports of companies Dragos and ESET details about cyber attacks on power grid UE in December 2016 we get a lot of requests to comment on certain facts. I want to stress that we regard these reports as a separate expert position, these companies did not participate in the investigation and had no opportunity to thoroughly analyze the situation as a whole. But I want to note that this marketing activity supports the issue of protection of energy infrastructure in a tone that is very good

Figure 9: Google Translation of Ukrenergo Response to Reports

Amount of Technical Information Available[14]:

Analysts assigned a score of *4 – Extensive Details* to the reports for the technical information available due to the fact that malware samples, observable ICS impacts, technical Indicators of Compromise (IOC), and malware analysis was performed through two independent organizations on the modules. The analysis is strong in relation to the malware and provides comprehensive details with supporting evidence in regard to the malware operation. Both reports included analysis of the impact of the malware on an electric system and associated the malware to an event. The reports included many details that drive the conclusions and scenarios described in this analysis. The number of technical details provided to support the electric system impacts were not the primary focus of the reports and, therefore, were not provided at the same technical level as the malware analysis technical details. Analysts assigned the technical details behind the malware analysis a 5 (comprehensive details with supporting evidence) and the level of technical details provided to support the malware impacts a 3 (many details). Electric industry impact scenarios are available in the Dragos report, but additional details or evidence is needed from the targeted organization to provide conclusive supporting technical information that the malware was responsible for the outages, with the combined overall reports receiving an applied score of 4 (extensive details).

Currently, no confirmation exists from the organization that was attacked that this malware was actually found in its environment; however, the analyst team for this report assessed the technical details specific to the electric system operations and effects described are precisely those that would be expected from the use of this malware.

---

[14] Amount of Technical Information Available is an analyst's evaluation and description of the details available to deconstruct the attack provided with a rating scale from 0-5: [0] No specifics, [1] high-level summary only, [2] Some details, [3] Many details, [4] Extensive details, [5] Comprehensive details with supporting evidence.

Attacker and Tactics, Techniques, and Procedures Description

Attacker

Industry reports do not reference an individual or entity that has claimed responsibility for the Ukrainian power system attack on December 17, 2016; however, many media reports identified Russia as the source. The ESET report states it did not find a link to the BlackEnergy 3 malware analyzed in the 2015 Ukraine power system attack and the ICS-capable malware that links to the 2016 *Ukrenergo* cyber attack. The Dragos report stated that the group Electrum is responsible for creating the ICS modular malware being analyzed and further identified direct links to the Sandworm team, which Dragos and other cyber-security firms[15] attribute to the 2015 Ukraine attack and the use of BlackEnergy 3.[16] The Dragos report stated with high confidence the linkage through confidential sources. For obvious reasons, Dragos indicated that further details are withheld in the public report, but made available to appropriate government sources. Dragos also sent a more comprehensive report to customers, but those details are not in scope of this report.

Reports indicate that this malware and associated payloads were likely developed by an organization with resources and interdisciplinary skills with the sole purpose of impacting ICS operations across multiple targets and systems in a way that the adversary can easily modify and customize. Based on publicly available information, no clear evidence exists in the technical data of Russian attribution at the time of this writing. Geopolitical events and active ongoing conflict impacting Ukraine may lead one to draw a conclusion on attribution, but that is a complex subject matter and is not directly relevant for the defense of industrial sites.

Capability

The capability section considered the analysis of the malware and the 2016 cyber attack on the Ukraine power system as a common evaluation due to the high confidence linkages provided within the reports. The attackers demonstrated the capability to gain a foothold into the Information Technology (IT) networks of the energy companies to establish an internal proxy listener through an attack vector that has not been publicly disclosed. The adversaries demonstrated the capability to deploy a backdoor with an additional backdoor both with the purpose to establish a C2 channel to gain access to the ICS network and install the launcher. Notably, the attackers showed expertise in ICS-specific protocols, ICS device-specific vulnerabilities, system-specific file extensions, and the ability to map an operational environment.

More concerning, the adversaries showed interest in impacting electric system components that could cause a device fault or an operational loss of view in a manner that requires a physical point of presence to re-establish functionality. The attackers' strongest capability was not in their development of tools or in their expertise, but in their capability to perform long-term operations required to learn the environment and execute a customized attack.

This report notes that the malware discovered may not be the actual mechanism for conducting the December 17, 2016, attack, even though the malware was capable of achieving the impacts. Given the high probability that the attackers leveraged the malware, the DUC will continue to evaluate the capability in this manner.

A consolidated list of the technical components detailed in the reports:

- Full protocol implementations for ICS-specific protocols with the ability to identify points and join and/or impact the communications;
- Capability of delivering exploits to a protection device requiring a physical presence to reset;

---

[15] http://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108

[16] Sandworm is the threat group iSight (FireEye) tracks that was responsible for a wide-spread campaign targeting industrial sites in the U.S. and Europe in 2014 using BlackEnergy 2 and BlackEnergy 3 malware.

- Usage of legitimate protocol functionality contained within the OLE for Process Control (OPC) standard to automatically create a configuration file and launch the malware's attack routine;
- Ability to send traffic out through an internally established proxy node or an alternate backdoor;
- Custom tools for device scanning;
- Data destruction tools targeting ICS-specific configuration and engineering files; and,
- Ability to extend the framework using additional modules, such as additional ICS specific protocols.

Motivation

In attempting to determine motivation, the evidence can become misleading in creating definitive attribution. For this reason, the SANS ICS team will not introduce all the competing hypotheses the team explored. The Dragos report stated that the Electrum group was responsible for developing and using the CrashOverride malware in the 2016 Ukraine power system cyber attack. The report linked the Electrum group and the Sandworm team, and identified the Sandworm team as the group behind the 2015 Ukraine power system cyber attack. This information led Dragos to determine that the adversary's opportunity and motivation are to be an ongoing campaign targeting multiple critical infrastructure sectors throughout Ukraine. For the 2015 and 2016 Ukraine power system attacks, no apparent financial motivations existed, and the motivation is consistent with nation-state interests during periods of geopolitical tension and conflict. Many theories exist, including that the attacks were a demonstration of force and capability or a test of an adversary capability to understand how the targets would respond.

In short, too many variables impact the team's ability to discuss attribution and motivation. Instead, this report examines the components of the attack, timeline of public reporting, lessons learned, and recommendations.

ICS Cyber Kill Chain Mapping

The ICS Cyber Kill Chain was published by SANS in 2015 (Michael Assante and Robert M. Lee) as an adaptation of the traditional cyber kill chain that Lockheed Martin analysts developed as it applied to ICS.[17] The ICS Cyber Kill Chain details the steps an adversary must move through to perform a high confidence attack on the ICS process or to cause physical damage to equipment under control in a predictable and controllable way as displayed in Figure 10.

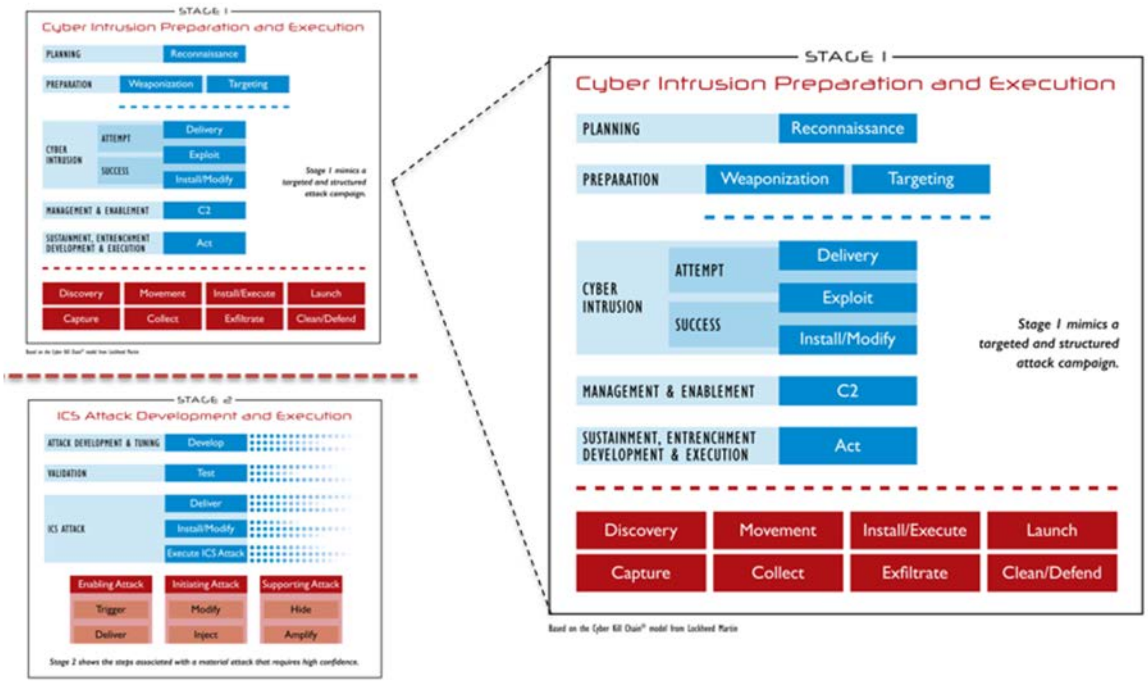


Figure 10: The ICS Cyber Kill Chain with Stage 1 Highlighted

The 2016 attack on the Ukrainian power grid showed indications of key elements of the ICS Cyber Kill Chain Phase 1 and Phase 2 based on initial reports from the impacted organization and additional reports from organizations working with the impacted company. However, the ESET and Dragos linkage of the Industroyer/CrashOverride malware to the 2016 Ukrainian power system attack is only focused on the Stage 2 portion of the ICS Cyber Kill Chain. Stage 1—how the adversary initially gained access and learned the environment—would require incident response details and not simply malware analysis.

The overall 2016 attack, however, penetrated each stage of the ICS Cyber Kill Chain as shown in Figure 11 (possible actions in white and observable actions in green). Simply completing Phase 1 would mean that the incident was a successful intrusion or breach, but not an ICS attack with resulting outages. Completion of Phase 2 demonstrates that this incident was a successful cyber attack and led to an impact on the operations of the ICS. This report discusses the steps in the two phases using currently available information.

---

[17] https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

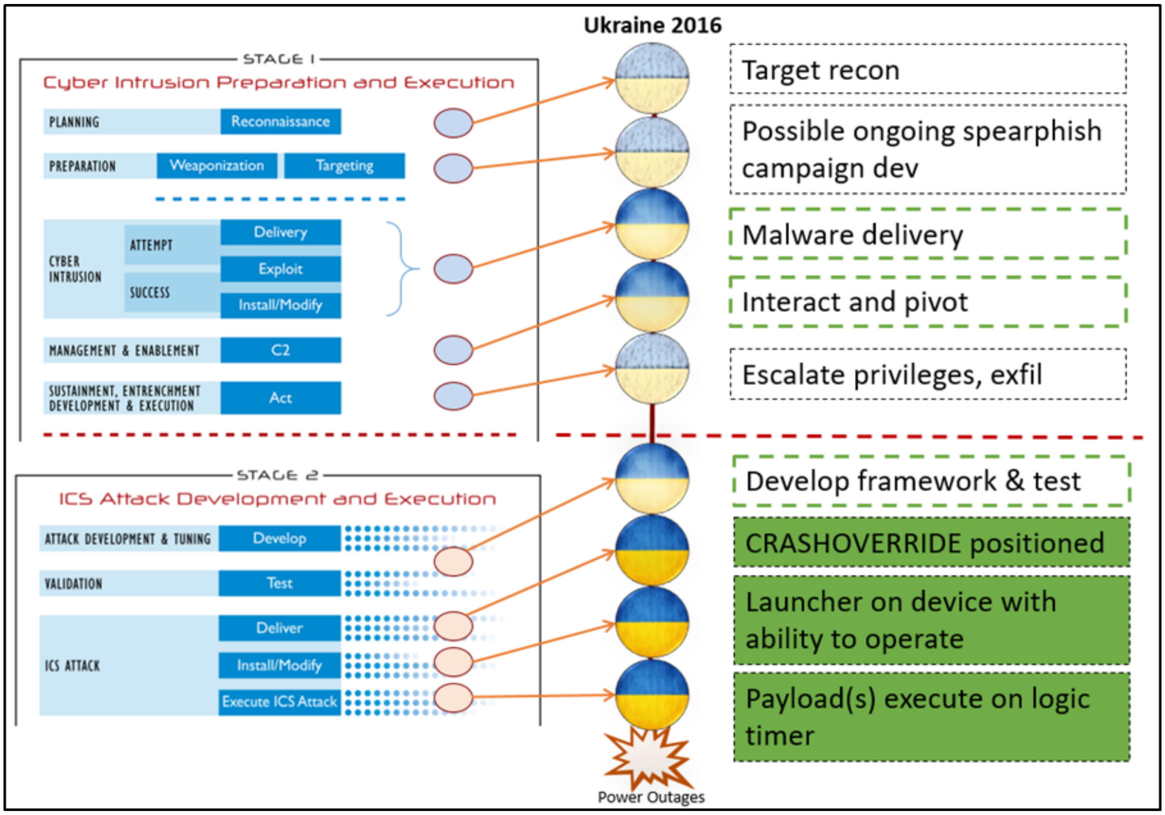


Figure 11: Mapping ICS Modular Malware to 2016 Observable Events

Community members have rightfully inquired about the Stage 1 aspects of the attack. These details are currently unknown, however, they are worth exploring for the purpose of defense recommendations. Adversaries could deliver CrashOverride through any sort of Stage 1 operations, including traditional compromises of IT networks linking to ICS networks, as was observed in the 2015 Ukraine attack.

ICS Cyber Kill Chain Mapping – Stage 1

Many cyber events covered in industry reports traditionally detail the Stage 1 activities that occurred and the data exfiltration or workstation impacts associated with the events. For an example, see the Defense Use Case[18] analysis on the Bowman Avenue Dam[19] and the Associated Press[20] report referencing U.S. energy infrastructure vulnerability to cyber attack, both reports and the events they cited were limited to purely Stage 1 activity. In this case, both the ESET and Dragos reports focus on the opposite — with the main capability of the malware analyzed mapping to the Stage 2 elements of the ICS Kill Chain.

The first step in Phase 1 is **reconnaissance**. While the reports contain no indication of specific reconnaissance components of the malware, a reference in the Dragos report links the 2016 malware to the team that it identifies as responsible for the 2015 Ukraine power system events. If these adversary groups are working together and are responsible for the attacks, then one could speculate that the Electrum group performing the second attack used or leveraged the previous Stage 1 Sandworm team's reconnaissance efforts and positioning.

---

[18] https://ics.sans.org/media/SANSICS_DUC4_Analysis_of_Attacks_on_US_Infrastructure_V1.1.pdf
[19] https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559
[20] http://bigstory.ap.org/article/c8d531ec05e0403a90e9d3ec0b8f83c2/ap-investigation-us-power-grid-vulnerable-foreign-hacks

During the 2015 Ukraine power system events, adversaries performed many Stage 1 observable actions against the targeted *oblenergos* (distribution utilities), as well as other critical infrastructure facilities. No definitive reports showed observed reconnaissance that took place prior to targeting the energy companies. However, analysis of the three impacted organizations shows that these were targets of interest due to automation in the supervisory level of the ICS that allowed remote disconnection of the substations during the attack.

Likewise in the 2016 Ukraine power system event, no reports indicated that observed reconnaissance took place prior to targeting the *Ukrenergo*; however, analysis of the targeted substation and statements by the *Ukrenergo* indicate the site was likely selected due to the high levels of automation and control system upgrades that took place at the facility. In a Wall Street Journal article, Vsevolod Kovalchuk, chief executive officer of the transmission operator in Ukraine (*Ukrenergo*) stated in reference to the December 17, 2016, attack, "Mr. Kovalchuk said he believes the latest attack was well planned because the targeted substation is one of the utility's most automated."[21] In addition, the impacted substation has a series of YouTube videos available detailing the system upgrades that have taken place.[22] While not covered in the ESET or Dragos reports, security researchers have delivered public presentations that claim the Security Service of Ukraine (SBU) has stated that the 2016 string of attacks was similar to the attack against the power utilities in 2015.[23] This is a fair statement because the attack essentially followed the same blueprint of hijacking the SCADA system and causing circuit breakers (CB) to open and damaging parts of that SCADA system. What is more likely to be different is the technique used to operate the remotely controlled CBs and the possible use of different tools to erase files, among other items.

The second step is **weaponization** or **targeting**. Targeting would normally take place when no weaponization is needed, such as accessing devices directly connected to the Internet. Analysis of the 2015 attack does not indicate that the adversaries targeted specific infrastructure prior to gaining access to the network. Instead, the adversaries weaponized Microsoft Office documents (Excel and Word) by combining BlackEnergy 3 with the documents.[24] Samples of Excel and other Office documents were recovered in the larger campaign targeting other organizations. Office documents were recovered for the specific attack being discussed against the three energy companies.[25]

In public presentations, security researchers have stated that a 2016 wave of spear phishing campaigns targeting organizations in Ukraine started in July 2016, and that, while adversaries used similar tools from the 2015 campaigns, the new attacks were more sophisticated and better organized than those conducted a year prior. The researchers also made a specific reference to continued use of BlackEnergy in the 2016 activity.

During the cyber intrusion phase of **delivery**, **exploit**, and **install**, limited direct information is available in regard to how this was accomplished; however, as an indirect link to this phase of Stage 1, the ESET and Dragos reports reference the operation of the backdoor and the existence of a configured IP address that points to a proxy server listening on port 3128. This indicates that the adversary would have had to position this proxy server during the Stage 1 delivery, exploit, and install phase. An additional backdoor attempts to communicate directly out to the C2 servers if the internal proxy cannot be contacted by use of the main backdoor.

No sufficient information exists in the reports reviewed or other public reporting to truly draw conclusions regarding the final phases of Stage 1 **C2**, and **act;** however, some analysis can be discussed. If the adversary used the malware discovered in the 2016 Ukraine power system attack, then the adversary could have used the C2 path to interact with the environment and pivot to an asset of interest that could successfully be used to achieve

---

[21] https://www.wsj.com/articles/cyberattacks-raise-alarms-for-u-s-power-grid-1483120708

[22] https://www.youtube.com/watch?v=AUoiKZBqIo0

[23] https://www.slideshare.net/MarinaKrotofil/s4-krotofil-morningsesh2017

[24] https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

[25] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

the attacker's objectives, as well as place the launcher component in the Act phase. Bridging this gap between Stage 1 and Stage 2 is complex and environment-specific; however, Figure 12 provides general concepts on how to bridge that gap, while Figure 13 describes possible adversary behaviors within an environment depending on how the adversary accessed Stage 2.

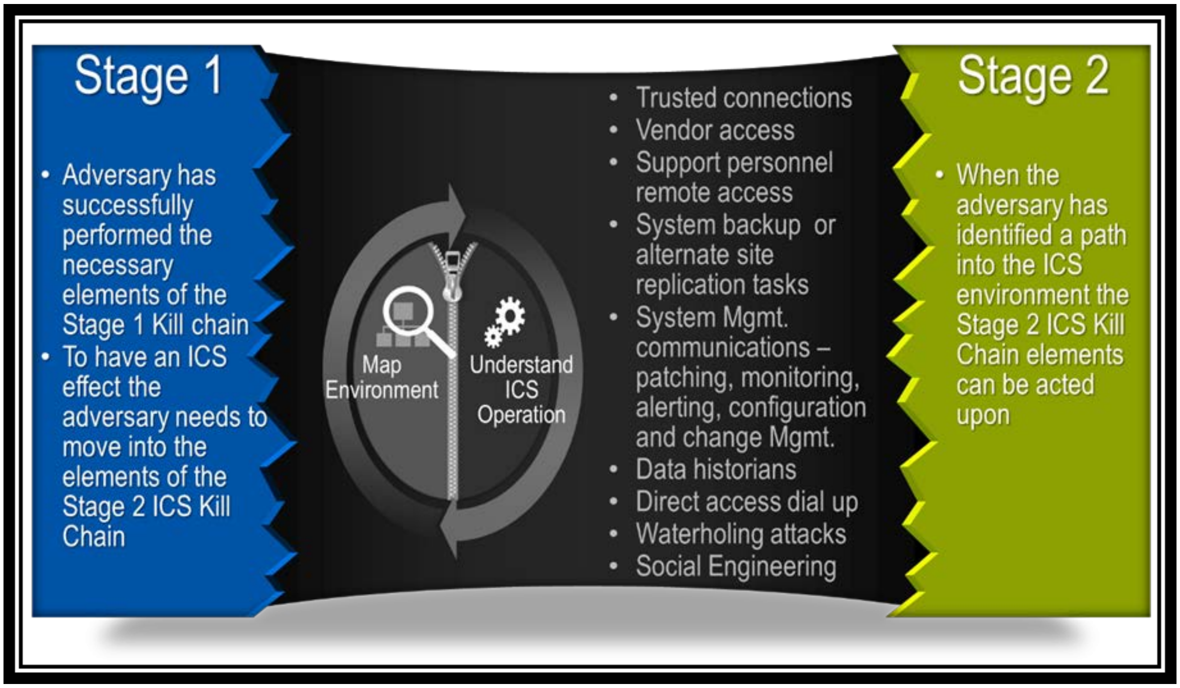

Stage 1
• Adversary has successfully performed the necessary elements of the Stage 1 Kill chain
• To have an ICS effect the adversary needs to move into the elements of the Stage 2 ICS Kill Chain
Map Environment
Understand ICS Operation
• Trusted connections
• Vendor access
• Support personnel remote access
• System backup or alternate site replication tasks
• System Mgmt. communications – patching, monitoring, alerting, configuration and change Mgmt.
• Data historians
• Direct access dial up
• Waterholing attacks
• Social Engineering
Stage 2
• When the adversary has identified a path into the ICS environment the Stage 2 ICS Kill Chain elements can be acted upon

Figure 12: Building a Bridge between Stage 1 and Stage 2

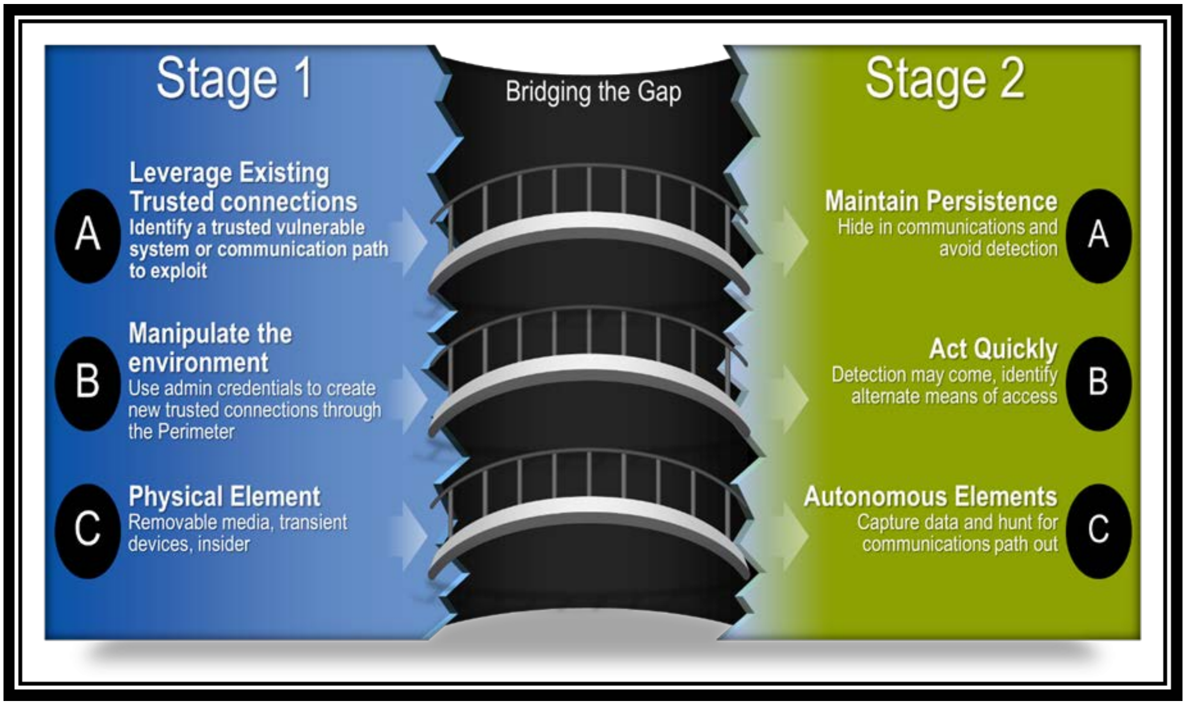

Stage 1
Bridging the Gap
Stage 2
A
Leverage Existing Trusted connections
Identify a trusted vulnerable system or communication path to exploit
B
Manipulate the environment
Use admin credentials to create new trusted connections through the Perimeter
C
Physical Element
Removable media, transient devices, insider
Maintain Persistence
Hide in communications and avoid detection
A
Act Quickly
Detection may come, identify alternate means of access
B
Autonomous Elements
Capture data and hunt for communications path out
C

Figure 13: Example Adversary Actions

Sufficient information was not available to identify if the adversary exfiltrated any information from the environment, but the adversary demonstrated capability in Stage 2 that indicates the adversary performed internal discovery and data exfiltration in the development of the ICS modular framework components needed. This reconnaissance would have included discovering field devices such as the protocols in use, ICS device types and firmware, vendor software in use to configure the wiper specific file types to target, and other system configurations and architecture specific communications path capabilities.

ICS Cyber Kill Chain Mapping – Stage 2

Throughout the following Stage 2 analysis, this report maps the electric system effects to the capabilities identified in the malware and performs the analysis as if the adversary used the malware as a test or demonstration of capability. Many of the Stage 2 phases and adversary actions discussed in this section would have similar attacker approaches and indicators even if the adversary performed the attack using a script or by sending commands direct to the field device.

In the Stage 2 **develop** phase, the adversary group likely determined how the target ICS environment looked and then created an environment that replicated similar devices and protocols to test. In creating the malware components, the adversaries obtained full protocol implementation stacks from the development community, as well as the development of an exploit package for specific protection relays. This adversary group also required a specific network scanner. While the adversary could have used many available tools to perform this function, they chose to implement their own custom tool.

Available information indicates that the current modular malware analyzed was specific to a target environment; however, the development approach used makes this approach fairly easy to modify for various targets and to avoid detection.

The SANS ICS team assesses with high confidence that, during the validation phase of Stage 2, the adversary must have **tested** its capabilities prior to deployment. The adversary likely conducted testing in an environment that allowed for the specific target configuration, protocols in use, and possibly a simulated operational environment.

During the **deliver** phase of the ICS attack Stage 2, the adversaries likely delivered the malware launcher to a position in the control system, communications, or field environment that would have allowed the execution of the launcher and had a trusted communications path to the target devices. This malware launcher delivery capability was likely accomplished through the actions outlined previously (in the Credibility section) and performed in Stage 1; however, as of the writing of this report, little observable activity is public in association with this event.

In final preparation for the attack, the adversaries could have completed the **install/modify** stage by installing module payloads necessary to operate the target environment with the appropriate configurations and launcher logic execute time.

As a final step to complete the ICS Cyber Kill Chain and to **execute the ICS attack,** the adversaries may have used the logic bomb execution timer capability of the launcher to kick off the payloads and the supporting (ICS specific data destruction) and amplifying attacks (DoS targeted relay protection devices).

In summary, Phase 2 consisted of the following attack elements:

1. **Supporting attacks**:
    a. Deletion of ICS specific configuration files
2. **Primary attack**:

   a. Malicious operation of circuit breakers

3. **Amplifying attacks**:
   a. Potential DoS to protection equipment (reports do not specify if the targeted protection equipment was installed or reachable)
   b. Wiping of SCADA human-machine interfaces (HMIs) to add confusion and delay the recovery

Implications

The discovered malware and associated payloads provide important implications and takeaways for the ICS defender community and electric industry system operators. The malware tools, associated programs, and scripts are capable of providing a path for adversaries. This path allows the adversary to deliver additional tools, discover hosts, tune payloads, schedule actions, and execute several attacks that range from misoperating power systems to denying communications and functions of the SCADA system and critical field devices. The most profound implication of this collection of capabilities is the shortening timeline needed for attackers to move from initial SCADA system access to causing impacts. Asset Owners and Operators (AOOs) must understand the true risk of this ICS modular malware as it exists and has been analyzed. AOOs should examine how this framework could be used in the future and understand the changing risk landscape to their organizations.

As AOOs consider the risk associated with this malware to their operating environments, they should consider the six primary risk areas:

- Substation communications protocols in use;
- Protection devices and firmware versions in use;
- Use of OPC protocols for control in operations environments;
- Data destruction impacts to recovery capability;
- Adversary foothold in environment without detection; and
- Adversary remote access and C2 capability to operations environment.

Figure 14 shows these six risk items and associated risk mitigation actions to consider to reduce the impact of a successful attack. Figure 15 shows an example consideration of the current risk for an example U.S. utility and some decision making criteria on what would drive increased risk assessments based on future discoveries.

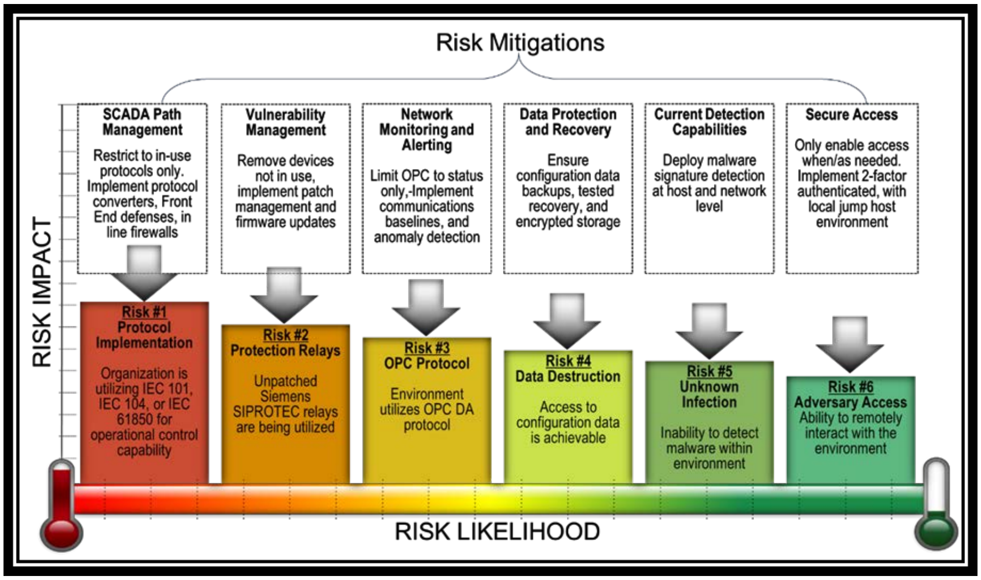
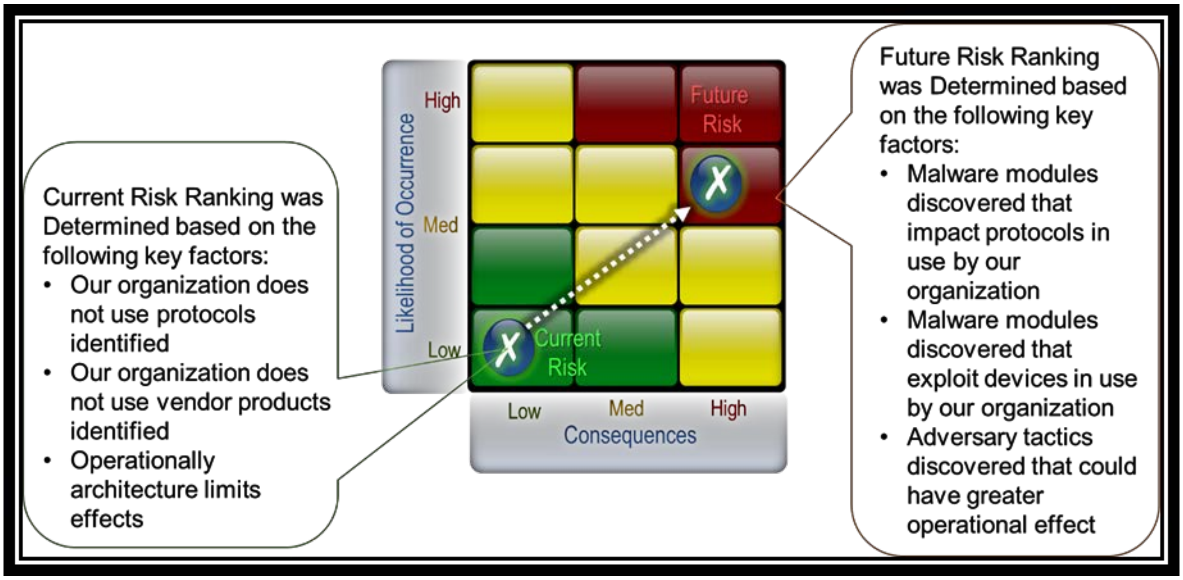

Risk Mitigations
SCADA Path Management
Restrict to in-use protocols only. Implement protocol converters, Front End defenses, in line firewalls
Vulnerability Management
Remove devices not in use, implement patch management and firmware updates
Network Monitoring and Alerting
Limit OPC to status only,-Implement communications baselines, and anomaly detection
Data Protection and Recovery
Ensure configuration data backups, tested recovery, and encrypted storage
Current Detection Capabilities
Deploy malware signature detection at host and network level
Secure Access
Only enable access when/as needed. Implement 2-factor authenticated, with local jump host environment
RISK IMPACT
Risk #1
Protocol Implementation
Organization is utilizing IEC 101, IEC 104, or IEC 61850 for operational control capability
Risk #2
Protection Relays
Unpatched Siemens SIPROTEC relays are being utilized
Risk #3
OPC Protocol
Environment utilizes OPC DA protocol
Risk #4
Data Destruction
Access to configuration data is achievable
Risk #5
Unknown Infection
Inability to detect malware within environment
Risk #6
Adversary Access
Ability to remotely interact with the environment
RISK LIKELIHOOD

Figure 14: Key Risk Item Considerations and Mitigations



Current Risk Ranking was Determined based on the following key factors:

- Our organization does not use protocols identified
- Our organization does not use vendor products identified
- Operationally architecture limits effects

Future Risk Ranking was Determined based on the following key factors:

- Malware modules discovered that impact protocols in use by our organization
- Malware modules discovered that exploit devices in use by our organization
- Adversary tactics discovered that could have greater operational effect

Figure 15: Current Risk Ranking and Assessment of Potential Risk

Defense Lessons Learned

This section focuses on the Sliding Scale of Cyber Security and identifies Passive and Active Defenses appropriate for organizations to consider in their mitigation efforts. While these cyber security items are covered in this section, another important aspect to consider is operational and engineering design components to reduce impact to electric systems. Some of the items within this section discuss electric system impacts and operational components, and for these reasons, portions will be redacted from the public report, while making the full version available only the E-ISAC portal. [26]

Passive and Active Defenses

Mitigations in the ESET and Dragos reports were reviewed and considered how an adversary may alter the next attack based on the mitigations a target will implement. This report supports many of the mitigation recommendations provided to date; however, the adversary identified in the reports likely has the ability and willingness to modify attack approaches, which is supported by the framework and modular approach to the malware analyzed. Throughout this section, the importance of electric system architecture concepts that are essential for organizations to understand as they consider defense approaches are discussed. Protection devices and cyber defenses will also be examined.

The following section explores mitigations for the attack that took place to extract defense lessons learned with a heavy focus on the capabilities present in CrashOverride. Infrastructure defenders must understand that CrashOverride is the Stage 2 capability. It could be input into the environment in a variety of Stage 1 efforts. In addition, the reliance on C2 was not a requirement for CrashOverride if the adversary used the auto-configuration aspect of the malware. This means that relying on good segmentation is not sufficient.

This report presents recommendations that could, and may in the future, disrupt this adversary's operations or reduce the impact of an attack. The cyber recommendations focus on **architecture, passive defense,** and **active defense** methodologies along the Sliding Scale of Cyber Security shown in Figure 16.[27] Electric industry recommendations are available in the E-ISAC distributed version of this DUC only.[28]

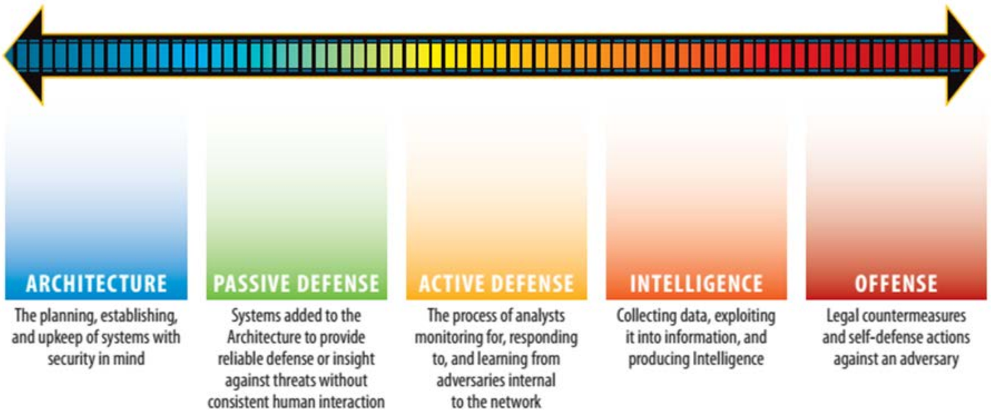

ARCHITECTURE
The planning, establishing, and upkeep of systems with security in mind
PASSIVE DEFENSE
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction
ACTIVE DEFENSE
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network
INTELLIGENCE
Collecting data, exploiting it into information, and producing Intelligence
OFFENSE
Legal countermeasures and self-defense actions against an adversary

Figure 16: The Sliding Scale of Cyber Security

---

[26] https://www.eisac.com/

[27] https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

[28] https://www.eisac.com/Account/Login

Cyber Summary Recommendations

- Architecture Recommendations
  - Properly segment networks from each other to help identify and limit the adversary's Stage 1 efforts, as well as impact ease of backdoor connectivity to C2, if leveraged.
  - Ensure that logging is enabled on devices that provide engineers remote jump host/intermediary server access to field devices and enable access logging on the field devices to the level supported.
  - Make backups of critical software installers and include a SHA256 digital hash of the installers and files.
  - Collect and vault (off the network) a backup of project files and device configuration files with appropriate digital hashes.
  - Review currently available vendor patches for protection and field communications devices, test and apply patches when operations schedules allow and prioritized based on greatest impact to system stability.
    - Siemens provided firmware update V4.25 for the EN100 card in 2015 for both the SIPROTEC 4 family of devices[29], as well as the SIPROTEC compact family of devices.[30]
  - Limit remote connections only to personnel that need them, limit the access privileges required, and use two-form authentication on the remote connections with split tunneling disabled.
  - Identify protocols in use through the field environment and ensure legacy protocol support, and that unused protocols are eliminated.
- Passive Defense Recommendations
  - Application Whitelisting can help limit adversary initial infection vectors and should be used when not too invasive to the ICS.
  - DMZs (demilitarized zones) and properly tuned firewalls between network segments will give visibility into the environment and allow defenders the time required to identify intrusions.
  - Establish a central logging and data aggregation point to allow for forensic evidence collection, and be made available to defenders.
  - Use endpoint security technologies on systems where appropriate and do not limit them to operations technology; where endpoint security technologies are not permitted, at minimum, perform host based log collection on those operations technology systems.
  - Have a method to perform intrusion detection whether it is based on anomalies, analytics, or indicators such as the SIPROTEC signatures.
    - A rule exists for the UDP port 50,000 crafted packets associated with the SIPROTEC vulnerability.
- Active Defense Recommendations
  - Train defenders to hunt for odd communications leaving the networked environment such as new IP communications and abnormal ICS protocol communications.
  - At key network traffic choke points, ensure network captures are collected, baselined, and analyzed in a manner that will identify anomalous communications.
    - Monitor all outbound (e.g., egress communications looking for suspicious connections).

---

[29] http://w3.siemens.com/smartgrid/global/en/products-systems-solutions/downloads/Pages/SIPROTEC-4-Downloads.aspx

[30] http://w3.siemens.com/smartgrid/global/en/products-systems-solutions/downloads/Pages/SIPROTEC-Compact-Downloads.aspx

- Perform network security monitoring to continuously search through the networked environment for abnormalities.
- Plan and train to incident response plans that incorporate both the IT and OT (operational technology) network personnel, and the acquisition of meaningful forensic evidence while restoring operations.
- As incident response actions begin to identify suspicious activity, disable all unnecessary remote access connections, and implement more restrictive Internet filtering, ultimately positioning the ICS in a more defendable cyber position.
- Consider Active Defense models for security operations such as the Active Cyber Defense Cycle.
- Ensure that personnel performing analysis have access to technologies, such as sandboxes, to quickly analyze incoming phishing emails or suspect files and extract IOCs to search for infected systems.
- Use backup and recovery tools to take digital images from a few of the systems in the supervisory environment such as HMIs and data historian systems every 9-12 months. This builds a baseline of activity and makes the images available for scanning with new IOCs, such as new YARA rules on emerging threats.
- Train defenders on using tools such as YARA to scan digital images and evidence collected from the environment, but do not perform the scans in the production environment itself.
- Incorporate threat hunting methodologies to proactively identify threats before incidents occur.

Electric Industry Considerations

This section of the TLP:Amber version of this DUC contains a series of nuanced electric sector specific actions, recommendations, and scenarios to consider. The TLP:Amber version of this DUC can only be obtained through the E-ISAC portal[31]. North American electric sector asset owners and operators are eligible to register and login to the E-ISAC portal to access the TLP:Amber version of the DUC.

---

[31] https://www.eisac.com/

Implications/Predictions

Discovering and analyzing the malware has broad implications: the malware may have been present more than six months prior and additional modules may exist or have been developed. The assumption is that common and open standard ICS protocols provide the building blocks for payloads like the IEC 101, IEC 104, IEC 61850, and OPC modules associated with the existing reporting. The challenge to defenders is to collapse the time available to observe positioning tools, their operation in the environment, and fine-tuning and execution. ICS defenders must consider how they would hunt for multiple copies of the tool on control system hosts and consider multiple installations with pre-set scheduled attacks. Returning a power system to an operational state may be temporary if defenders cannot identify all installations of the malware and isolate suspected hosts.

The discovered malware possessed more functionality than what was necessary to produce the December 17, 2016, outage. The time investment and resources to create a modular tool set would indicate the desire for future repeated use. Additionally, the Dragos report identified that some of the modules used in the attack were only compiled six hours before the attack, while other modules were much older. By their assessment, the framework is still under active development with research being focused on future targets. Unfortunately, no additional information is available on this at this time; however, infrastructure owners should be aware that the threat is active and displaying tradecraft that could easily be adopted and adapted by other adversary groups.

Conclusion

As the investigation and analysis of technical data continues and more information regarding this attack surfaces, this report will be updated as appropriate to maintain the most accurate and beneficial guidance document possible for ICS defenders.

Defenders must take this opportunity to conduct operational and engineering discussions as suggested in this DUC and enhance their capabilities to gain visibility in to their ICS networks and hosts. The community must learn as much as it can from real world incidents and not delay; we expect adversaries to mature their tools and enhance them with additional capabilities.

Follow NERC on Twitter:
https://twitter.com/NERC_Official

NERC website:
http://www.nerc.com

E-ISAC website:
https://www.eisac.com/

For questions or comments to the E-ISAC:
Operations@eisac.com

Follow SANS on Twitter:
https://twitter.com/SANSICS
https://twitter.com/RobertMLee
https://twitter.com/Assante_Michael

SANS library:
http://ics.sans.org/ics-library

SANS training catalog:
http://ics.sans.org/training/courses

ICS Community Forum:
https://ics-community.sans.org/signup