DRAGOS

CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack

By Joe Slowik, Dragos Inc

Abstract

Upon discovery and initial analysis in mid-2017, audiences primarily viewed CRASHOVERRIDE as a disruptive event targeting electric utility operations in Ukraine. Similar to the 2015 attack in the same area, CRASHOVERRIDE interrupted the flow of electricity by manipulating ICS equipment and delayed recovery operations to prolong the impact. However, CRASHOVERRIDE's immediate effects represent only the precursors for an attempt at a more ambitious attack than what was achieved. In addition to significantly expanded scope in power disruption, CRASHOVERRIDE differentiates itself from the 2015 event by attempting to disable protective relay devices involved in the targeted operations through a denial of service (DoS) attack. The attack as implemented failed, but the most-likely intention behind this action and its implications for electric utility operations and protection have received little attention or analysis. This paper will reexamine this phase of the CRASHOVERRIDE event and likely attacker intentions, even if actual execution failed. It will highlight how CRASHOVERRIDE attempted a different type of attack than 2015 by disrupting electric power operations only as an initial step toward setting up a protection-focused attack on transmission operations, with disabling protective gear as a final attack phase to introduce possible physical destruction via cyber means.

Table of Contents

Introduction

On its public discovery in mid-2017, some analysts called CRASHOVERRIDE[1] (also referred to as Industroyer[2]) the "biggest threat to industrial control systems since Stuxnet".[3] While concerning, the event's initial impacts resulted in a smaller effect than the 2015 Ukraine electric event in terms of number of customers impacted and for how long.[4] Technically more sophisticated than the 2015 Ukrainian power outage due to industrial control system (ICS) manipulation codified in software rather than deployed via manual interaction with systems, the seeming failure or lack of significant impact caused some to discount the severity or significance of CRASHOVERRIDE.

In terms of achieved impact and effect, CRASHOVERRIDE represents a step back from the 2015 event. Yet in terms of ambition and intention, CRASHOVERRIDE sought to attain greater and more serious impacts than 2015. Based on analysis of the various payloads, CRASHOVERRIDE attempted to create a far more widespread outage than 2015 and stage a potential destructive event as the final step in the attack sequence. Despite seemingly thorough analysis of CRASHOVERRIDE, including in public presentations at events such as Black Hat,[5] significant implications behind the event – especially its intended scope and potential outcome – remain largely ignored.

In this paper, we will explore the CRASHOVERRIDE event from a different perspective. Instead of looking at what happened at Ukrenergo station "North" in December 2016 following CRASHOVERRIDE's execution, we will explore what the attackers, identified as ELECTRUM,[6] likely sought to achieve given the design and configuration of software deployed in the victim environment. Attackers made many mistakes in designing and deploying CRASHOVERRIDE and related impact modules. However the scope and implications for this attack's intentions are cause for deep concern among electric utility operators. By exploring and understanding what CRASHOVERRIDE tried but ultimately failed to achieve, relevant ICS asset owners and operators can prepare for better instrumented and executed future attacks and prevent potentially destructive results.

CRASHOVERRIDE in Review

Several sources have reviewed the CRASHOVERRIDE event: from malware-focused analysis on the modular ICS-manipulating framework[7] to an overview of the intrusion lifecycle leading up to

---

[1] **CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations** – Dragos; **Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE** – Joe Slowik, Dragos (Virus Bulletin 2018)
[2] **Win32/Industroyer: A New Threat for Industrial Control Systems** – Anton Cherepanov, ESET
[3] **Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet** – Anton Cherepanov and Robert Lipovsky, ESET
[4] **Ukraine's Power Outage was a Cyber Attack: Ukrenergo** – Pavel Polityuk, Oleg Vukmanovic, Stephen Jewkes, Reuters; **The Ukrainian Power Grid was Hacked Again** – Kim Zetter, Motherboard; **Analysis of the Cyber Attack on the Ukrainian Power Grid** – Robert M. Lee, Michael J. Assante, and Tim Conway, SANS Institute; **Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid** – Kim Zetter, Wired
[5] Industroyer/CRASHOVERRIDE – Zero Things Cool about a Threat Group Targeting the Power Grid – Robert Lipovsky & Anton Cherepanov (EST) and Robert M. Lee, Ben Miller, and Joe Slowik (Dragos)
[6] **ELECTRUM** - Dragos
[7] **CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations** – Dragos; **Win32/Industroyer: A New Threat for Industrial Control Systems** – Anton Cherepanov, ESET

CRASHOVERRIDE's deployment and follow-on actions.[8] A high-level review of CRASHOVERRIDE's execution is provided in Figure 1. Each of these reports and their analyses largely focus on observed items following events at substation "North" in Ukrenergo. Although hewing to observed events, such analysis neglects significant aspects of what the attacker likely sought to achieve in this attack but failed to successfully execute.

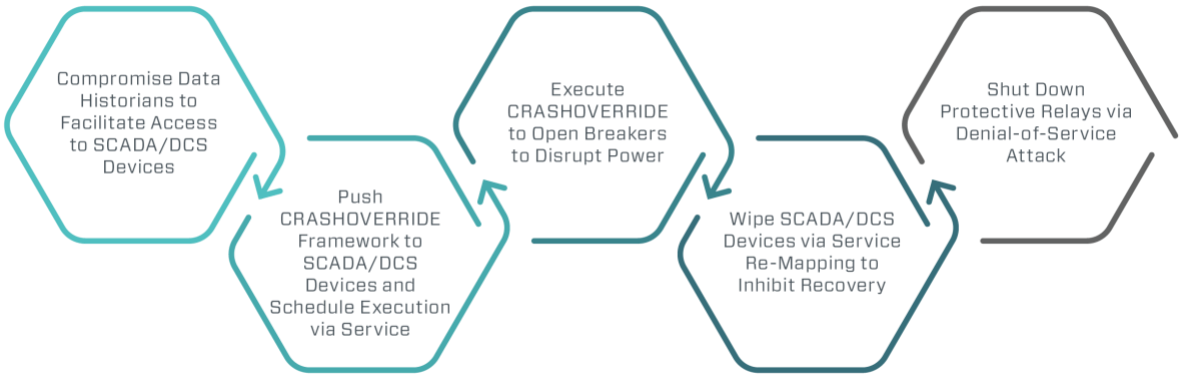

Figure 1: CRASHOVERRIDE Event Attack Flow

CRASHOVERRIDE impacted electric transmission operations resulting in an outage of approximately an hour in Kiev, Ukraine – noticeably smaller in both scale and duration than the 2015 attack.[9] While the 2015 event took place through manual manipulation of systems via compromised remote logons to control system workstations, the 2016 event leveraged the CRASHOVERRIDE framework to encode ICS manipulation within software. This aspect represents a significant development in attacker tradecraft. Encoding ICS attacks in software enables the attack to scale far better than manual system interaction. Reviewing log data and other artifacts associated with the CRASHOVERRIDE event revealed that the intended scale of the attack was far larger than 2015 but also significantly different from what attackers ultimately achieved.

CRASHOVERRIDE targeted electric transmission control systems across multiple communication protocols – IEC-101,[10] IEC-104,[11] IEC-61850,[12] and OPC-DA[13] – with a very simple yet effective objective: to change the physical state of breakers and related equipment from "closed" (allowing power to flow) to "open." There is some variation in effects in CRASHOVERRIDE. Options exist for a direct state change to the flow of power or for "strobing," meaning continuously switching between

---

[8] **Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE** – Joe Slowik, Dragos (Virus Bulletin 2018). Dragos WorldView subscribers can review a more in-depth version of this report in TR-2018-19: CRASHOVERRIDE Attack in Review.
[9] **How Do You Say Ground Hog Day in Ukrainian?** – Michael J. Assante and Tim Conway, SANS
[10] **IEC 60870-5-101** – IPcomm
[11] **IEC 60870-5-104** – IPcomm
[12] **IEC 61850: What You Need to Know about Functionality and Practical Implementation** – Dave Dolezilek, Schweitzer Engineering Laboratories, Inc.
[13] **OPC Data Access (OPC DA) Versions & Compatibility** – Matrikon

states of open and closed. However, only immediate "open" and "close" effects appear to have been used in the victim's environment.

While seemingly a simple "on-off" switch in functionality, the implementation of these standards requires more than a direct, one-step shift from one logical state to another for successful communication and state alteration. Achieving actual physical manipulation of the targeted RTU or other system requires logical messaging following discrete, required steps. An accurate understanding of the specific protocol targeted – as well as the vendor's actual implementation of the protocol – requires knowing the "statefulness" of a given protocol's communications for proper interaction.[14]

Computer science includes a notion of statefulness for programming and communication, where protocols can either be stateful or stateless. Stateful protocols are designed to record or consider preceding events in the communication stream, while stateless events can ignore or need not consider such items.[15] As an example, TCP with its handshake and session management represents a stateful protocol, whereas UDP streams are stateless in nature.

CRASHOVERRIDE's functionality is based on a semi-modular construct where different effects modules perform protocol-specific communications, usually executed from a common launcher. Based on the implementation of CRASHOVERRIDE's effects modules, the developers were either unaware of or failed to properly implement appropriate stateful communications in their software for specific ICS communication protocols. Although potentially indicative of either poor testing or understanding of the targeted systems and underlying protocols, such errors are hardly rare or unique given complex systems and varying vendor implementations of more general protocol standards.[16] One possibility for this error may be test environment. Protocol emulators in software, such as the publicly-available IEC Server project,[17] do not enforce statefulness and associated communication timeouts. Physical hardware will employ such items in line with the vendor-specific implementations of the relevant communication standard. As a result of either equipment limitations, error, or sheer ignorance, the actual receiving system in the victim environment of CRASHOVERRIDE's execution would either reject the communication as invalid given improper implementation of stateful standards, or ignore for similar reasons. The impact (or lack of effect) can be compared to an invalid TCP handshake with the resulting absence of actual communication.

This aspect of CRASHOVERRIDE is important. When reviewing intended targeting within the victim environment, the number of control systems identified for manipulation is large and more widespread than the actual outage. Based on available data from the event, at least seven OPC servers with multiple managed OPC instances each were targeted along with at least eight IEC-101 controllers and over 400 control points for IEC-104 communication.[18] Additionally, all observed instances of the IEC-61850 attack module swept the local subnet for applicable hosts and attempted to disrupt based

---

[14] **Stateful Protocol Hunting: What It IS, Why It Matters, How to Do It** – Dan Gunter and Dan Michaud-Soucy, Dragos (CS3STHLM 2018)
[15] **Protocol State** – Information and Communications Security (Google Books); **"Program State"** – Dictionary of Computer Science, Engineering, and Technology (Google Books)
[16] **Analyzing Operational Behavior of Stateful Protocol Implementations for Detecting Semantic Bugs** – Endadul Hoque, Omar Chowdhury, Sze Yiu Chau, Critina Nita-Rotaru, and Ninghui Li, 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (2017)
[17] **IEC Server** – jkl (Sourceforge)
[18] Cited figures based on non-public sources and incident artifacts made available to Dragos for analysis in 2018.

on discovery, with the number of targets essentially equal to the number of such devices on the impacted subnet. Based on this information and targeting intention, CRASHOVERRIDE attempted a widespread outage across hundreds of individual control systems, aiming for a disruptive impact that would be orders of magnitude larger than the 2015 event.

Essentially: ELECTRUM *attempted* to manipulate many systems via CRASHOVERRIDE to create a widespread electric transmission disruption. Yet across all four protocols and all related systems involved in controlling operations, the effect was relatively minimal in terms of actual outage and quickly restored due to Ukrenergo's ability to manually reclose impacted breakers. While ambitious in scope and reach, CRASHOVERRIDE's actual impact can be judged as a failure.

Yet simply stopping at ELECTRUM's failure to successfully execute a widespread transmission interruption obscures several interesting elements following attempted disruption operations. Similar to the 2015 incident, CRASHOVERRIDE deployed a wiper module to impede recovery and (in this specific case) delete configuration and related files to hamper restoration on infected SCADA systems. This portion of the attack appears to have executed successfully, and produced a situation where operators lost control and view over ICS operations in the environment. This is a non-trivial impact as it limits the flexibility of remote operations and coordination, while potentially masking subtle issues in the transmission environment given loss of remote view into operations.

The above wiper impact was then followed by an interesting action that was largely overlooked in initial analysis: an attempted denial of service attack using a publicly-known vulnerability on four Siemens SIPROTEC protective relays in the operating environment. At this point, ELECTRUM's attack sequence sought to de-energize transmission equipment, create a loss of control and loss of view impact on SCADA systems controlling this equipment, and then aimed to remove relay protection on the de-energized transmission lines. Given Ukrenergo's ability and willingness to resort to manual restoration operations, absent complete view into the ICS environment's state, CRASHOVERRIDE escalates from an immediate disruption of electric transmission to creating a potentially unstable or unsafe system state at time of manual service restoration. To analyze and understand this aspect of the 2016 Ukraine event and its significance, one must understand protective relays and their role in electric operations.

Protective Relays in Electric Utility Operations

Protective relays play a vital role in electric utility operations. Protective relays use advanced algorithms to protect transmission or generation equipment from harmful conditions. Ultimately, "the function of protective relaying is to cause the prompt removal from service of any element of a power system when it suffers a short circuit, or when it starts to operate in any abnormal manner that might cause damage or otherwise interfere with the effective operation of the rest of the system."[19] Relay locations are highlighted in the below diagram (Figure 2), relative to locations in electric generation, transmission, and distribution operations.

[19] **The Art & Science of Protective Relaying** – C. Russell Mason, GE

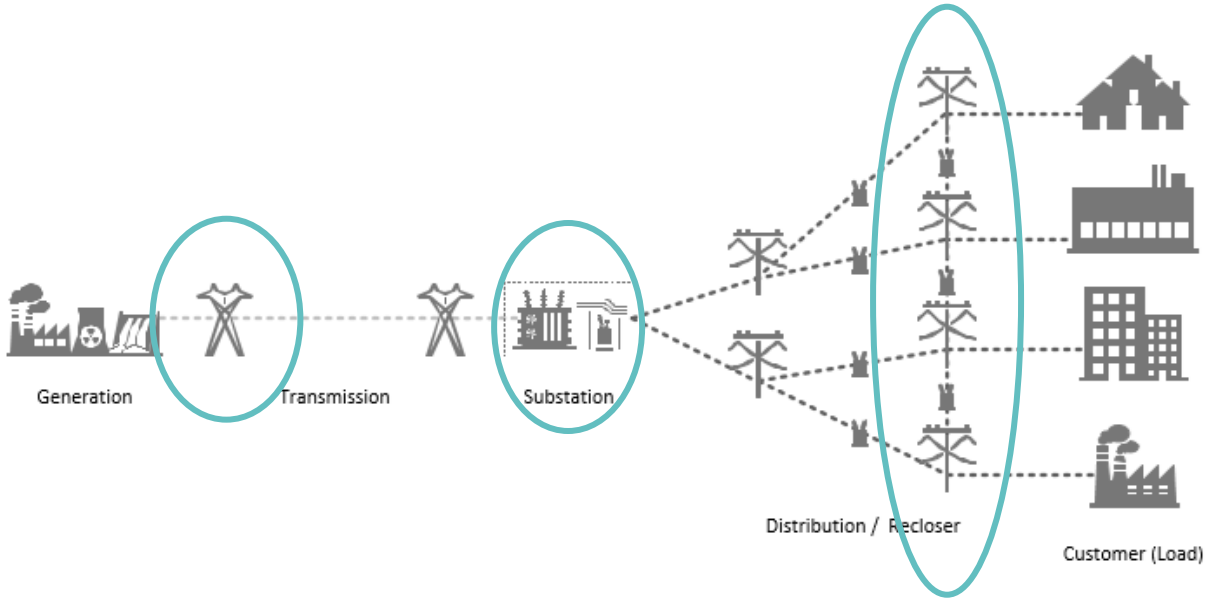

Figure 2: Overview of Protective Relay Locations Relative to Electric Operations

Protective relays work to dynamically monitor the power system and clear or mitigate faults in the system when detected. Modern digital protective relay systems perform a variety of diagnostic and monitoring functions to make this possible. They identify items from current to voltage to frequency and safeguard electric systems from anomalous, potentially destructive behavior, while providing output and feedback to end users. A high-level overview of such activity is shown in Figure 3. Key to digital relays is the ability to perform precisely the right action within incredibly small time increments to preserve the integrity of the protected system.[20]

[20] **Millisecond, Microsecond, Nanosecond: What Can We Do with More Precise Time?** - Edmund O. Schweitzer, III, David E. Whitehead, Greg Zweigle, Veselin Skendzic, and Shankar V. Achanta

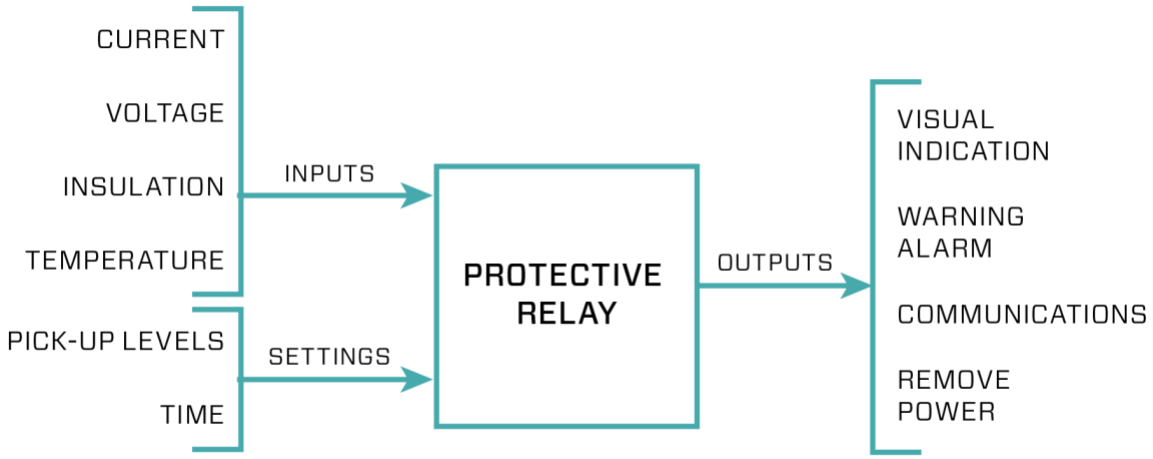

Figure 3: Protective Relay Representation[21]

Digital protective relays ensure grid stability through adverse but regularly observed, fluctuating parameters.[22] In the event of a direct, immediate event or attack, digital relays ensure resiliency by disengaging equipment from the overall, now-compromised system. Specific relay technology exists for both electric transmission (where relays protect and normalize the flow of electricity to transformers and related equipment)[23] and generation (where relays prevent potential swings in several factors, including rotation frequency).[24] Examples of protective relay applications include phase distance protection for generating assets; initiating protection in event of breaker failure; transformer and transmission system coordination to protect against overcurrent conditions; and protecting generator assets against frequency abnormalities.[25]

Coordination among protected assets and grid components is necessary to ensure system-wide stability in light of individual site protection actions.[26] While protective relays work to isolate transmission or generation from damage, such automated responses during times of electric system stress or distributed disruption can create positive-feedback loops resulting in widespread dislocation.[27] In these extreme circumstances, widespread impacts are possible, such as the US-Canada 2003 power event and the Italian blackout of 2003, irrespective of grid protection

---

[21] **What is a Protection Relay** – Littelfuse
[22] **Digital Protection for Power Systems** – A. T. Johns and S. K. Salman
[23] **Protection Relays** – Toshiba; **Transmission Line Protection Principles** – GE
[24] **Generator Protection Relay** – Schweitzer Engineering Laboratories; **Digital Generator Protection Relay** – GE
[25] **C37.102-2006 - IEEE Guide for AC Generator Protection** – IEEE Standard; **C37.91-2008 - IEEE Guide for Protecting Power Transformers** – IEEE Standard; **C37.106-2003 - IEEE Guide for Abnormal Frequency Protection for Power Generating Plants** – IEEE Standard
[26] **Power Plant and Transmission System Protection Coordination** – NERC
[27] **Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations** – US-Canada Power System Outage Task Force; **How a Smarter Grid Could Have Prevented the 2003 US Cascading Blackout** – Jeri E. Chadwick (Purdue University/Westinghouse Electric Company)

mechanisms.[28] In these cases, network effects in stressed systems result in widespread outages – which although disruptive, are preferable to the potential loss of equipment and capacity that would result from physical damage to overloaded or otherwise stressed equipment.

To highlight what happens when relays fail, the power outage impacting New York City in July 2019 originated in a distribution fault impacting substation after both primary and secondary relays failed to isolate the faulted line.[29] Improper wiring between system sensors and resident relays resulted in relays failing to respond to the fault situation.[30] In this case, failure in protective systems produced site-specific physical damage and an unplanned outage impacting thousands of consumers. Had relays functioned properly, the faulted line would have been isolated and de-energized, preserving the functionality of the rest of the substation. Ultimately, when properly controlled and implemented, protective relays ensure electric service stability and protect physical assets from a variety of natural or unnatural fluctuations.

Post-CRASHOVERRIDE Effects

After interrupting the flow of electricity in the victim environment, CRASHOVERRIDE proceeds to a combination loss of visibility- and loss of control-directed disruption. This is illustrated in Figure 4.

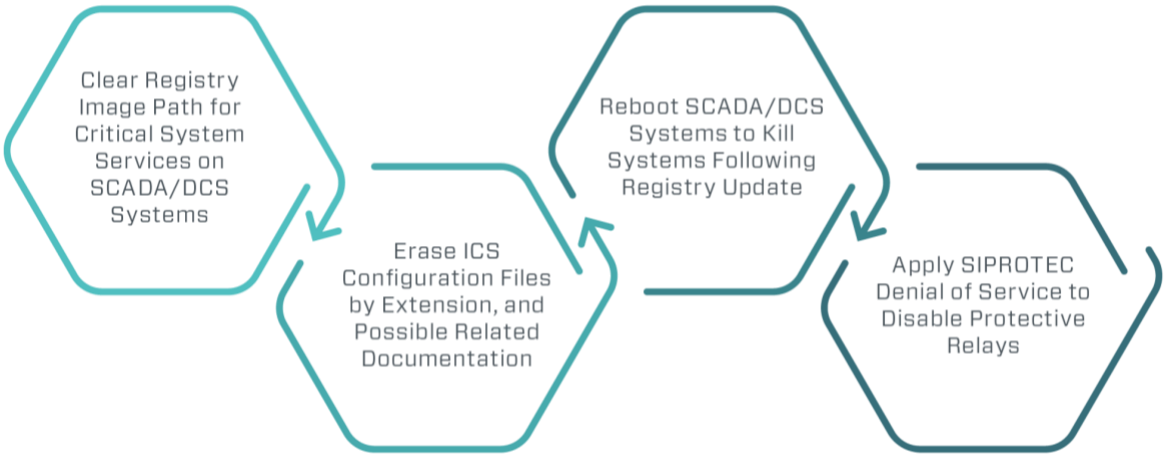

Figure 4: CRASHOVERRIDE Post-Disruption Effects

At first glance, the impact of the above sequence of events is felt primarily by service restoration and recovery – manipulating SCADA/DCS devices to inhibit reboot and control and deleting configuration

---

[28] **Relay Performance During Major System Disturbances** – Demetrios Tziouvaras (Schweitzer Engineering Laboratories); **Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations** – US-Canada Power System Outage Task Force; **Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy** – UCTE

[29] **ConEd: Failed Relay Systems, not Transmission Equipment, Caused NYC Blackout** – UtilityDive; **ConEd Starts to Shed Light on Why NYC Got Plunged Into the Dark** – Bloomberg

[30] **ConEd Ties NYC Blackout to Bad Wiring Job Done 11 Years Ago** – Bloomberg

files to deny speedy recovery. This series of events is non-trivial and tremendously disruptive, but as indicated by Ukrainian response to the 2015 event, asset owners can and showed a willingness to quickly move into manual system operations at impacted sites in order to restore impacted services as quickly as possible. What sets the 2016 event apart in intention – if not in actual impact – was the far-larger scale of disruption designed in the CRASHOVERRIDE effects modules, which as previously described aimed to cause a very large-scale interruption in transmission services across hundreds of devices.

The above widespread impact alone makes manual service restoration (in a scenario where the attack succeeds as designed) difficult given the number of devices manipulated. Yet this is only a half-way point in the overall attack logic, as the last stage of the sequence of events – functionally disabling the SIPROTEC protective relays – is most interesting from both an operational and attack impact assessment. In terms of attack progression, attackers performed a denial of service (DoS) against protective relays *after* opening system breakers and removing operator visibility into system operations through the wiper attack. Removing protection from an unenergized line at first seems nonsensical as, at this stage, there is nothing to actually protect. But the real focus of impact instead hinges on a combination of widespread transmission disruption combined with an assumption based on previous observation of Ukrainian restoration operations that finds asset owners would move to restore service as quickly as possible through manual means despite loss of visibility into actual system status.

Attacking protective relays can quickly cause severe consequences including "islanding" events related to grid self-protection actions and the potential for equipment damage due to faults absent protection.[31] However, it appears ELECTRUM in the CRASHOVERRIDE scenario (as designed) aimed to create an unsafe, unstable condition for reconnected transmission lines at the moment of physical restoration. In this scenario, manually closing breakers opens up the possibility of overcurrent scenarios absent digital protection. The vulnerability targeted in the DoS executable, CVE-2015-5374, performs a functional DoS as opposed to a network accessibility DoS.[32] Given these conditions, CRASHOVERRIDE evolves from an immediate disruption event to a delayed potential physical destruction attack. As shown in Figure 5, the disruption of transmission through remote terminal unit (RTU) manipulation is a precursor to a final, more serious stage: inhibiting protection systems so when service is restored, the target circuit is no longer safe and is subject to damage.

[31] **Anti-Islanding and Smart Grid Protection** – Stephen Evanczuk (Digi-Key Electronics)
[32] **Advisory ICSA-15-202-01 Siemens SIPROTEC Denial-of-Service Vulnerability** – US-CERT

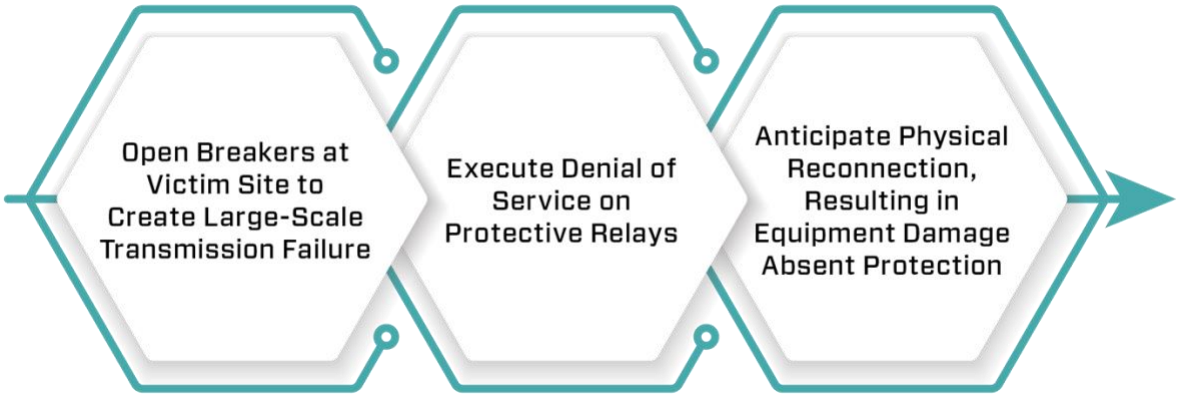

Figure 5: CRASHOVERRIDE Attack Intentions

The DoS condition places the victim SIPROTEC device in "firmware update" mode. The effect triggered is practical and useful in legitimate firmware update instances given the limited resources available to legacy SIPROTEC devices (especially for memory). However, when activated, the impacted SIPROTEC no longer performs designed protective functions – including overcurrent protection[33] – on the relevant transmission lines even if still present, powered on, and network accessible. Essentially the receiving device is placed in an inoperative holding pattern for future instructions. When triggered outside of normal or intended operations, this is a mission kill impact from the perspective of the targeted SIPROTEC relay. The SIPROTEC is still present on the network but no longer performing intended functions due to the exploit. The result is an unprotected link in electric transmission, with normal safeguards disabled.

The exploit condition is triggered by a single crafted UDP packet to UDP 50000 with the byte sequence shown in part in Figure 6. Sending this sequence will put SIPROTEC 4 and SIPROTEC Compact devices before version 4.25 into the non-functional standby mode described in the previous paragraph. Publicly-available exploit frameworks have incorporated this functionality, making it widely-accessible to immature entities, albeit against older system versions.[34]

```
11 49 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Figure 6: Siemens SIPROTEC DoS Packet Sample

[33] **Overcurrent and Feeder Protection** – Siemens
[34] **Siemens SIPROTEC 4 and SIPROTEC Compact EN100 Ethernet Module < 4.25 – Denial of Service** – Exploit Database

Although ELECTRUM properly implemented the DoS condition in a binary targeting SIPROTEC devices within the Ukrenergo network, the adversary made a coding mistake in overall communication implementation affecting the executable's functionality. Specific IP addresses – presumably for four SIPROTEC devices within the victim network – are hard-coded in the DoS binary employed in the CRASHOVERRIDE event. Yet when executed, the addresses are read backwards during communication socket creation. This is shown in Figure 7 with specific addresses obfuscated. While all devices reside on the same subnet as other control systems targeted in CRASHOVERRIDE's manipulation of transmission systems, the lack of endian awareness in socket creation results in nonsensical communications and makes the precise implementation of the SIPROTEC DoS in CRASHOVERRIDE inert.

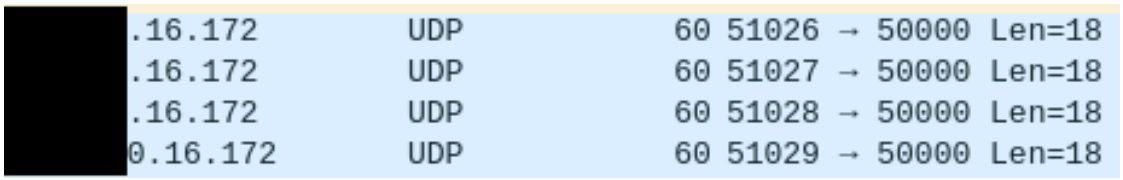

Figure 7: Packet Capture of Denial of Service Module Traffic

Implications for Protective Relay Denial of Service Attack

Assessing the intended state of events when the SIPROTEC devices were supposed to be disabled reveals worrying ambitions. It highlights CRASHOVERRIDE as a deeply serious attack, albeit one that failed in its goals due to various errors or mistakes noted earlier. Since ELECTRUM failed to disable the protective relays used at the victim site and did not manipulate as many RTUs as intended, understanding what the group was attempting to achieve is conjecture – but sufficient information exists to make informed judgment on what the group's ultimate goal was in 2016.

ELECTRUM disabled protective equipment after disconnecting breakers via logical means. Attackers then deployed measures such as the service wiping and remapping to inhibit logical recovery, while also rendering various SCADA devices non-functional eliminating accurate understanding, diagnostics, and remote operations of the transmission site. According to analysis of the 2015 Ukraine event, Ukrainian authorities possess and are willing to execute manual recovery procedures in the event of emergencies in electric utility operations. While in a state of logical loss of view, protective relays are still powered on and notionally active but the ability to ascertain their status is inhibited, if not completely removed, given the overall status of the utility's network during what was designed to be a massive transmission and control disruption event. As such, operators are placed in a situation where they attempt to restore operations to normal as quickly as possible in a degraded operational environment without having an accurate picture of that environment's current status – including the functionality of protection systems on lines about to be reconnected.

When transmission equipment is reconnected to the overall electric utility network with no protective relay in place, the range of potential outcomes is concerning, and expands the scope of impacts beyond immediate transmission disruption. The most obvious potential effect, provided ELECTRUM succeeded in its full-scale transmission interruption, is a surge when equipment is reconnected with

no protection in place. This scenario produces a possible overcurrent event on the reconnected line with the potential (depending on other backup and physical protection systems) to cause physical damage to transmission equipment. Given that CRASHOVERRIDE was designed to cause a massive transmission disruption by manipulating hundreds of devices, manual reconnection (taking place at a slower, more deliberate pace than what would be possible through normal SCADA operations) essentially connects a few lines at a time, resulting in potential overcurrent on the handful of reconnected lines during restoration. Normally, circumstances such as these would result in a fault and recovery through relay protection. But given the attack design, such protections are removed from operations allowing for potentially destructive scenarios to play out.

Of note, the above represents a most-likely ELECTRUM intention in executing the CRASHOVERRIDE attack – but it is not clear that such an attack would be successful in an actual operating environment. The presence of various system redundancies and physical protection mechanisms may have mitigated against a potential destructive scenario at the Ukrenergo site. More generally, impacts at a specific site will depend upon a litany of other factors – such as redundant relays and the presence and functionality of backup protection devices – making generalization from CRASHOVERRIDE to any transmission site difficult to impossible. However, the overall sequence of events indicates clear intentions on the part of ELECTRUM to place the targeted transmission site into an unsafe and potentially dangerous state. Given the intended (if unrealized) scale of CRASHOVERRIDE's impact to transmission operations, the potential load at time of reconnect would have been significant, and potentially amenable to a scenario resulting in physical damage to transmission equipment, producing a longer-lasting outage due to the need for repairs and replacement gear.

The combination of de-energizing transmission, eliminating process view and control, disabling protective systems, and knowing the victim's recourse to manual restoration of operations identifies a complex, multi-stage attack designed to do far more than simply interrupt the flow of electricity for a limited period of time. Instead, analyzing CRASHOVERRIDE as it was designed shifts the event from a largely logical, network-focused incident to the unique realm of cyber-induced, physical damage events so far only successfully achieved by Stuxnet. If CRASHOVERRIDE worked as ELECTRUM most likely intended, the potential outage would have been more widespread than 2015 given the number of transmission devices targeted. Additionally, the duration of the outage may have stretched to months or longer if disabling protection prior to system restoration yielded physical damage to transmission operations. While the actual efficacy of CRASHOVERRIDE – even if it had worked as intended – remains unclear given a myriad of other controls and safeguards in electric transmission, the sequence of steps executed clearly demonstrates a more complex and concerning attack than past electric service disruptions.

Lessons from CRASHOVERRIDE as a Protection Attack

Various pieces of CRASHOVERRIDE and artifacts associated with targeting suggest ELECTRUM's intentions exceeded the effects of the 2015 event, but they failed due to poor understanding or implementation of ICS communication protocols within the victim's environment. Even if all items deployed worked as intended, fundamental aspects of electric transmission and substation design may have prevented the scenario playing out as likely desired. However, focusing on ELECTRUM's failures obscures the worrying ambition behind CRASHOVERRIDE. By timing a transmission outage with both a loss of control and loss of view attack and disabling protective relays on impacted circuits,

ELECTRUM aimed for a far more significant and long-lasting effect: physical degradation or destruction of transmission equipment, with the desire to produce impacts lasting months instead of hours.

ELECTRUM failed in its attack for various reasons, but the event still provides multiple, actionable lessons to electric utility operators from generation to transmission to distribution. Operators must recognize adversaries have moved beyond switching things off and employing some mechanisms to delay recovery to targeting the fundamental protection systems underpinning electric utility operations. This element of protection-focused attack is also observed in more recent events such as TRISIS.[35] While both CRASHOVERRIDE and TRISIS failed in their execution (and may have both been prevented by other safeguards within the targeted systems), they demonstrate clear intention and willingness on the part of adversaries to expand operations in ICS environments to potential physically destructive scenarios. The implications for such attacks are significant and severe. In the rush to restore transmission in CRASHOVERRIDE, operators can inadvertently enable physical destruction if attackers successfully subvert protection mechanisms and operator visibility into protection systems.

Quickly and accurately diagnosing ICS impacts and effectively responding to disruptive events requires efforts to increase visibility, monitoring, and root cause analysis capability. In the case of CRASHOVERRIDE, identifying the combination of breaker manipulation with protective relay communication can alert asset owners that an adversary is attempting to set up the necessary preconditions for a potential destructive event. This is an example of a threat behavior analytic combining multiple observables that can be used to quickly detect, disposition, and respond to sequences of events in ICS environments.[36] In this fashion, the victim can properly grasp the scope and potential implications of the outage given the detected sequence of events, allowing for a more measured response than simply rushing to manually restore operations as quickly as possible – with the possibility of producing an unsafe operating environment.

At an even higher level, detecting or responding to CRASHOVERRIDE effectively across the scope of the ICS cyber kill chain of events necessary to actually enable and execute an attack yields even more defensive possibilities. Marrying IT-centric information highlighting ELECTRUM's penetration of the control system network with subsequent ICS-specific communication can accelerate root cause analysis of subsequent disruption events. This also provides operators with sufficient visibility and knowledge (even absent disabled SCADA equipment) to identify the event as a likely coordinated attack across multiple layers of grid operations. From this, utilities can take appropriate action and caution in responding to events and restoring operations. Furthermore, the victim will then possess knowledge on the full scope of the intrusion and subsequent attack, to ensure complete network recovery and remediation to prevent a potential re-compromise of the environment.

Lastly, asset owners and operators may discount CRASHOVERRIDE's and ELECTRUM's aims, given multiple failures in attack implementation and some fundamental misunderstandings of electric utility operations and safeguards. Yet adopting such a stance is not only misguided, but dangerous. The progression of attacks from the mostly-manual 2015 Ukraine event to the increased automation

---

[35] **TRISIS Malware** – Dragos; **Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure** – Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, and Christopher Gloyer, FireEye

[36] **Threat Analytics and Activity Groups** – Joe Slowik, Dragos; **Indicators and ICS Network Defense** – Joe Slowik, Dragos

in CRASHOVERRIDE sends a clear signal that adversaries continue to learn and evolve with each attack. CRASHOVERRIDE itself may have fallen short of its intentions, but ELECTRUM (and other adversaries) will learn from this event and adapt in future operations. CRASHOVERRIDE's shortcomings demonstrate the complexity and sophistication of cyber attacks on ICS networks to produce physical impacts – but CRASHOVERRIDE's existence clearly signals adversary intent and desire to develop such capabilities. ICS asset owners and operators must take such attempts seriously, and deploy defenses before attackers are able to deploy a fully-functional, ICS-aware attack in the future.

Conclusion

CRASHOVERRIDE was a failure in operations, especially when viewed from the perspective of actual impacts relative to the 2015 Ukraine power event. Yet further analysis of the event and its implications reveals a far more complex, nuanced, and concerning attack than its precursor. Through an attempted multi-stage manipulation of transmission operations, ICS visibility, and ultimately protection systems, ELECTRUM sought to create the preconditions for a possible physically-destructive event when the victim restored operations. While actual predictions of CRASHOVERRIDE's impact had it worked correctly is a matter of conjecture, the adversary's intent appears clear after analyzing all stages of the attack – establishing circumstances to create an unsafe, potentially destructive scenario within the victim transmission equipment.

The victim in 2016 avoided a worst-case scenario. Moving forward, electric utility operators must be aware of how adversaries executed this attack and its implications for operations. By adopting a whole-of-attack approach to reviewing what ELECTRUM tried but failed to do, ICS asset owners and operators can begin developing and deploying the required visibility, resilience, and response measures needed to cope with an attack like CRASHOVERRIDE.

Acknowledgments

As with so many things, this paper would not have been possible without the efforts and assistance of others. Principally, significant credit is due to Selena Larson, Reid Wightman, and Nick Tsamis of Dragos for content and technical review; Tim Watkins and Will Edwards of Schweitzer Engineering Laboratories (SEL) for specific help on electric power systems and protective relays; and Maggie Morganti and Mike Marshall of Oak Ridge National Laboratory (ORNL) for extended discussion on electric utility protection systems.

Resources and Works Cited

CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations – Dragos
Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Joe Slowik, Dragos (Virus Bulletin 2018). Dragos WorldView subscribers can review a more in-depth version of this report in TR-2018-19: CRASHOVERRIDE Attack in Review.
Win32/Industroyer: A New Threat for Industrial Control Systems – Anton Cherepanov, ESET
Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet – Anton Cherepanov and Robert Lipovsky, ESET
Ukraine's Power Outage was a Cyber Attack: Ukrenergo – Pavel Polityuk, Oleg Vukmanovic, Stephen Jewkes, Reuters
The Ukrainian Power Grid was Hacked Again – Kim Zetter, Motherboard

Analysis of the Cyber Attack on the Ukrainian Power Grid – Robert M. Lee, Michael J. Assante, and Tim Conway, SANS Institute
Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid – Kim Zetter, Wired
Industroyer/CRASHOVERRIDE – Zero Things Cool about a Threat Group Targeting the Power Grid – Robert Lipovsky & Anton Cherepanov (EST) and Robert M. Lee, Ben Miller, and Joe Slowik (Dragos)
ELECTRUM – Dragos
How Do You Say Ground Hog Day in Ukrainian? – Michael J. Assante and Tim Conway, SANS
IEC 60870-5-101 – IPcomm
IEC 60870-5-104 – IPcomm
IEC 61850: What You Need to Know about Functionality and Practical Implementation – Dave Dolezilek, Schweitzer Engineering Laboratories, Inc.
OPC Data Access (OPC DA) Versions & Compatibility – Matrikon
Stateful Protocol Hunting: What It IS, Why It Matters, How to Do It – Dan Gunter and Dan Michaud-Soucy, Dragos (CS3STHLM 2018)
Protocol State – Information and Communications Security (Google Books)
"Program State" – Dictionary of Computer Science, Engineering, and Technology (Google Books)
Analyzing Operational Behavior of Stateful Protocol Implementations for Detecting Semantic Bugs – Endadul Hoque, Omar Chowdhury, Sze Yiu Chau, Critina Nita-Rotaru, and Ninghui Li, 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (2017)
IEC Server – jkl (Sourceforge)
The Art & Science of Protective Relaying – C. Russell Mason, GE
Millisecond, Microsecond, Nanosecond: What Can We Do with More Precise Time? - Edmund O. Schweitzer, III, David E. Whitehead, Greg Zweigle, Veselin Skendzic, and Shankar V. Achanta
What is a Protection Relay – Littelfuse
Digital Protection for Power Systems – A. T. Johns and S. K. Salman
Protection Relays – Toshiba
Transmission Line Protection Principles – GE
Generator Protection Relay – Schweitzer Engineering Laboratories
Digital Generator Protection Relay – GE
C37.102-2006 - IEEE Guide for AC Generator Protection – IEEE Standard
C37.91-2008 - IEEE Guide for Protecting Power Transformers – IEEE Standard
C37.106-2003 - IEEE Guide for Abnormal Frequency Protection for Power Generating Plants – IEEE Standard
Power Plant and Transmission System Protection Coordination – NERC
Anti-Islanding and Smart Grid Protection – Stephen Evanczuk (Digi-Key Electronics)
Relay Performance During Major System Disturbances – Demetrios Tziouvaras (Schweitzer Engineering Laboratories)
Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations – US-Canada Power System Outage Task Force
Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy – UCTE
ConEd: Failed Relay Systems, not Transmission Equipment, Caused NYC Blackout – UtilityDive
ConEd Starts to Shed Light on Why NYC Got Plunged Into the Dark – Bloomberg
ConEd Ties NYC Blackout to Bad Wiring Job Done 11 Years Ago – Bloomberg
Advisory ICSA-15-202-01 Siemens SIPROTEC Denial-of-Service Vulnerability – US-CERT
Overcurrent and Feeder Protection – Siemens
Siemens SIPROTEC 4 and SIPROTEC Compact EN100 Ethernet Module < 4.25 – Denial of Service – Exploit Database
TRISIS Malware – Dragos
Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure – Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, and Christopher Gloyer, FireEye
Threat Analytics and Activity Groups – Joe Slowik, Dragos
Indicators and ICS Network Defense – Joe Slowik, Dragos

1745 Dorsey Rd
Hanover, MD
21076
info@dragos.com