PRECURSOR ANALYSIS REPORT: INDUSTROYER TARGETING UKRAINE ELECTRIC POWER TRANSPORT UTILITY (UKRENERGO) 2016

Cybersecurity for the Operational Technology Environment (CyOTE)

31 DECEMBER 2022

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

INL/RPT-23-72371

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

This *paper* is the product of *research* conducted by the Cybersecurity for the Operational Technology Environment (CyOTE) program and was funded by the Department of Energy Office of Cybersecurity, Energy Security and Emergency Response (DOE CESER). No updates have been made since the date of publication and no further funding has been approved.

TABLE OF CONTENTS

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: INDUSTROYER TARGETING UKRAINE ELECTRIC POWER TRANSPORT UTILITY (UKRENERGO) 2016

1. EXECUTIVE SUMMARY

The Industroyer Targeting Ukraine Electric Power Transport Utility (Ukrenergo) 2016 Precursor Analysis Report leverages publicly available information about the December 2016 cyber attack against the Ukrainian Ukrenergo electric transmission utility and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

Industroyer is a modular malware framework designed to deploy several Industrial Control System (ICS) protocol-specific attack payloads to disrupt electricity distribution. Adversaries deployed Industroyer within the target network on a Microsoft Windows endpoint capable of directly manipulating or communicating with ICS. Industroyer abuses the functionality of a targeted ICS's legitimate control system to achieve its intended impact.[1]

Adversaries likely first gained access to Ukrenergo enterprise networks in early 2016 after a successful spearphishing campaign against organizations in the electric power sector.[2] Adversaries then began capturing credentials beginning on 1 December 2016. This allowed access to the ICS environment at the Pivnichna electric transmission substation outside Kyiv through a device dual-homed on the Information Technology (IT) and ICS networks. Adversaries conducted discovery, targeting, and access to this device using information and previously captured credentials from compromised enterprise IT machines. Finally, the adversaries deployed and launched the Industroyer malware just before midnight on 17 December. By midnight, Ukrenergo had lost control of a targeted substation, resulting in electric power outages for over an hour in the city of Kyiv and the Kyiv region.[3]

Researchers and analysts identified 31 unique techniques (used in a sequence of 33 steps) utilized during the attack with a total of 846 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Twenty-nine of the identified techniques used during the Industroyer cyber attack were precursors to the triggering event. Analysis identified 548 observables associated with these precursor techniques, 353 of which were assessed to have an increased likelihood of being perceived in the 300 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

The information gathered in this report contributes to a library of observables tied to a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack. Asset owners and operators can use these products if they experience similar observables or to prepare for comparable scenarios.

2. INTRODUCTION

The Cybersecurity for the Operational Technology Environment (CyOTE) program developed capabilities for energy sector organizations to independently identify adversarial tactics and techniques within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under leadership of the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), CyOTE is a partnership with energy sector owners and operators whose goal is to tie the impacts of a cyber attack to anomalies in the OT environment to determine whether the anomalies have a malicious cyber cause.

2.1. APPLYING THE CYOTE METHODOLOGY

The CyOTE methodology, as shown in Figure 1. CyOTE Methodology, applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. The program utilizes MITRE's ATT&CK® Framework for Industrial Control Systems (ICS) as a common lexicon to assess triggering events. By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables, which could represent a faint signal of an attack requiring investigation. CyOTE can assist organizations in prioritizing their OT environment visibility investments.

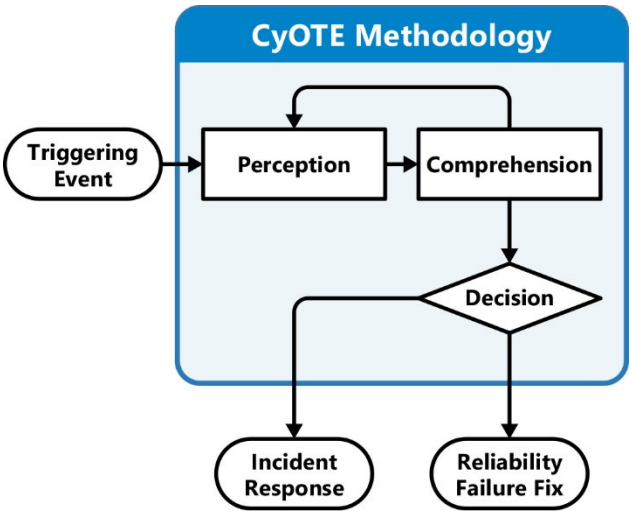


Figure 1. CyOTE Methodology

Historical case studies such as this one support continued learning through analysis of incidents that have impacted OT. This precursor analysis report is based on publicly available reports and provides examples of how key concepts in the CyOTE methodology appear in the real world, providing insights on how similar novel attacks could be detected earlier and therefore mitigated. The analysis enables OT personnel to independently identify observables associated with techniques known to be indicators of attack within OT environments. The identified observables highlight anomalous events for further investigation, which could enhance comprehension of malicious activity.

A timeline of events based on the CyOTE methodology portrays the attack-related observables associated with the precursor analysis report cyber attack. The timeline includes assessed dates, the triggering event, and comprehension of malicious activity by the organization. The point on this timeline when each technique appears is critical to the organization's ability to perceive and comprehend the associated malicious activity. Perception of techniques early in the timeline is critical, since halting those techniques will generally have greater potential to limit additional attack vectors using other techniques, defeat the cyber attack, and limit damage to operations.

Each technique has an assessed perceivability. Perceivability is a function of the number of observables and the potential for personnel to detect those observables. If a technique includes effects which personnel may detect, such as deletion or modification of system files or required user execution, then the technique would be more perceivable.

Differences in infrastructure and system configurations may present different challenges and opportunities for observable detection. For example, architecture-wide endpoint monitoring is likely to improve the perceivability of techniques which modify host files, such as the Data Destruction technique (T0809) for Inhibit Response Function and Theft of Operational Information technique (T0882) for Impact. Network monitoring and log analysis capabilities are likely to improve perceivability of techniques which create malicious network traffic, such as the Standard Application Layer Protocol technique (T0869) for Command and Control, External Remote Services technique (T0822) for Initial Access, and Connection Proxy technique (T0884) for Command and Control. Alternatively, enhancing the monitoring parameters of system files would increase the perceivability of techniques such as Data from Information Repositories technique (T0811) for Collection and the Service Stop technique (T0881) for Inhibit Response Function.

Comprehension can be further enhanced by technique artifacts created when adversaries employ certain attack techniques. The CyOTE program provides organizations with a library of observables reported in each historical case. The library can be used in conjunction with a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

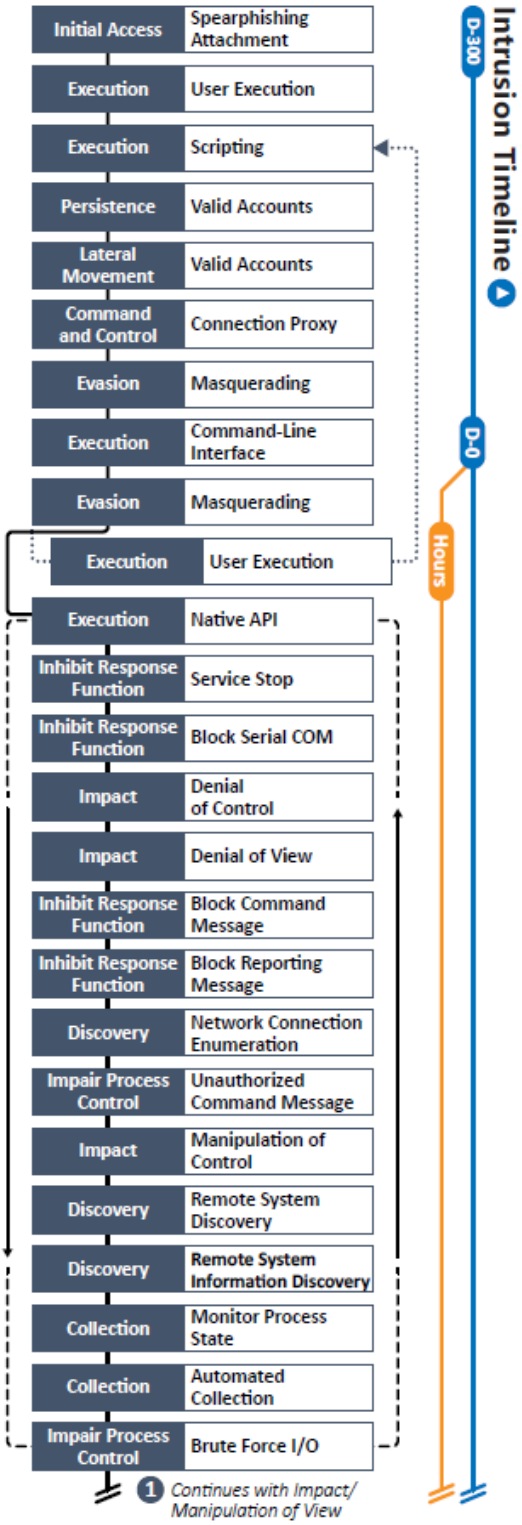
Industroyer is the first known malware specifically designed to attack an electrical grid.[4] This complex malware employs several independent Industrial Control System (ICS) payload modules implemented as dynamic link libraries (DLLs), each of which has a specific intended effect. Industroyer loads these modules through the custom launcher executable, which serves as the orchestrator for the adversaries' ICS capabilities, including discovery and impact.

The malware's modular implementation provides the framework for executing the ICS payload modules, along with provision for a data wiper module. Each Industroyer module focused on impact is tailored for a specific ICS communication protocol associated with the electric power sector.

The adversaries used techniques early in the timeline that were similar to those used in the Ukraine 2015 power grid attack that successfully targeted Ukraine's Ukrenergo electric transmission utility's IT (Information Technology) and OT (Operational Technology) networks less than a year earlier. Adversaries likely first gained access by about 3 February 2016 (D-300) after carrying out spearphishing intrusions into organizations across the Ukrainian electric power sector.[5] On the night of 17 December (D-0), the adversaries deployed and launched the Industroyer malware that impacted a single transmission level substation, resulting in electric power outages in the city of Kyiv and the Kyiv region that lasted for over an hour.[6]

A timeline of adversarial techniques is shown in Figure 2 and Figure 3. The timeline includes the estimated number of days prior to and after the triggering event. The timeline after the triggering event includes the assessed victim comprehension timeline.

Similar to the cyber attack on Ukraine's power grid in December 2015, where the KillDisk wiper was used to render victim hard drives inoperable, the adversaries deployed the Industroyer wiper module just before midnight on 17 December (D-0) to delete configuration and related files to hamper recovery and restoration of infected Supervisory Control and Data Acquisition (SCADA) systems. This caused operators to lose critical control over and view of the ICS environment, limiting their ability to coordinate and conduct remote operations of the grid and restore impacted systems.[7]



The wiper impact was accompanied by an attempted Denial-of-Service (DoS) attack using a publicly known vulnerability on four Siemens SIPROTEC protective relays in the ICS environment. At this point, the adversaries' 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 remove relay protection on the de-energized transmission lines.[8] Industroyer also used brute-force input and output traffic to cause failures within various industrial processes. These failures potentially could have resulted in excessive wear on equipment or damage to downstream equipment.

Given Ukrenergo's willingness to resort to manual restoration operations, even without a complete view into the ICS environment's state, the adversaries likely utilized Industroyer to escalate from an immediate disruption of electric transmission to creating a potentially unstable or unsafe system state at the time of manual service restoration.[9] However, the entire outage lasted just over an hour.

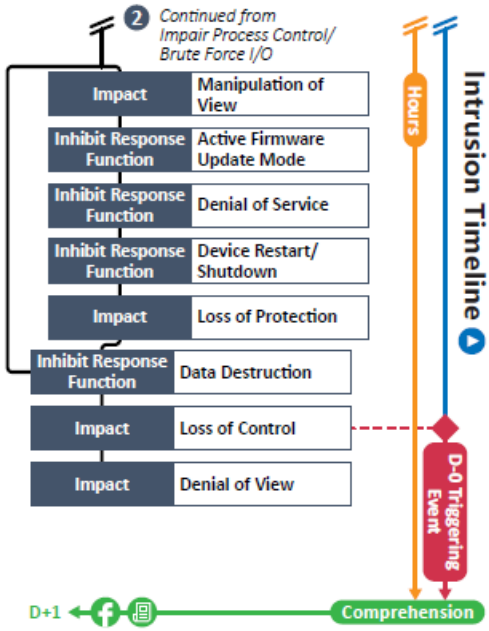


Figure 3. Intrusion Timeline (CONTD)

Analysis identified 31 techniques in a sequence and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Industroyer 2016 Cyber Attack

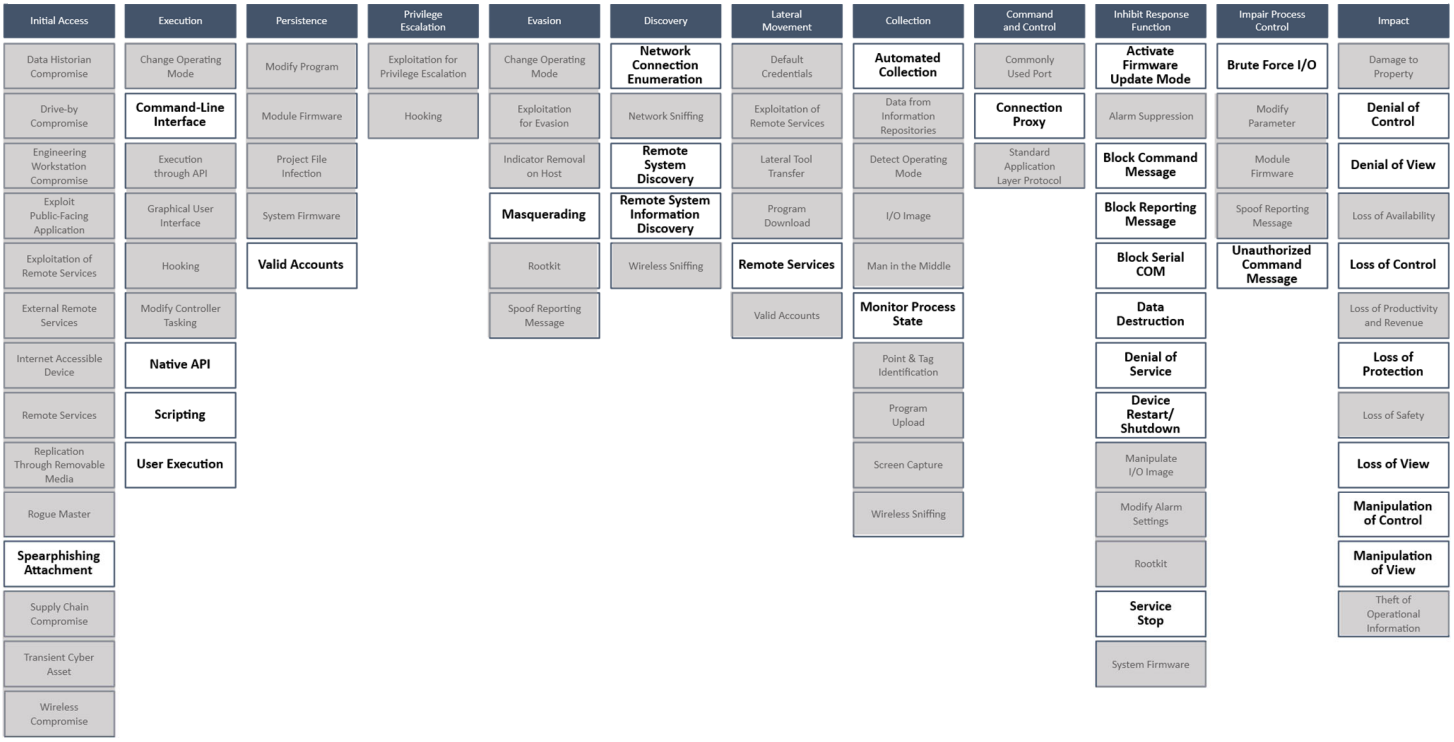


Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	**33**
Technique Observables	**743**
Precursor Techniques	**31**
Precursor Technique Observables	**644**
Highly Perceivable Precursor Technique Observable	**418**

3. OBSERVABLE AND TECHNIQUE ANALYSIS

The following analysis may assist organizations in identifying malicious cyber activity earlier and more effectively. The following techniques and observables were compiled from publicly available sources and correlated with expert analysis.

3.1. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS

The adversaries used techniques early in the timeline that were similar to those used in the 2015 attack that successfully targeted Ukrenergo IT and OT networks less than a year earlier. The adversaries likely recycled credentials captured during the 2015 attack to spoof a legitimate email account used in the spearphishing campaign in 2016. The adversaries likely used captured legitimate credentials to gain initial access to the ICS enterprise environment at the Pivnichna electric transmission substation outside of Kyiv, Ukraine. The spearphishing technique employed in this attack utilized a malicious Microsoft (MS) Office attachment that contained macros, which ran a malicious code once opened by the victim. The campaign targeted an end user on a device connected to both the IT and OT networks.[10]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have observed this technique as adversaries employed malware attached to an email and targeted a specific individual or group email address.

Two observables were identified with the use of the Spearphishing Attachment technique (T0865). This technique is important for investigation because it is often one of the first techniques an adversary will use to gain initial access to a targeted network. This technique appears first in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent adversaries from gaining initial access to the system.

Of the two observables associated with this technique, one is assessed to be highly perceivable. It is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 29 artifacts could be generated by the Spearphishing Attachment technique.
Technique Observers[a]	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

[a] Observer titles are adapted from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster. CyOTE products utilize these job categories rather than organizational titles to both support comprehensive analysis and preserve anonymity within the victim organization. A complete list of potential observers can be found in Appendix C.

3.2. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

As the end user opened the spearphishing email, they clicked on an MS Office attachment that executed an embedded macro containing malicious code. This macro loaded software that established a foothold on the IT and OT networks, most likely on a targeted device that was dual-homed (located) on both networks. The executed code made outbound calls to a remote Command and Control (C2) server operated by the adversaries.

IT Cybersecurity and OT Cybersecurity personnel may have observed this technique, as malicious code may have triggered anomalous outbound and inbound traffic on both the IT and OT networks.

A total of five observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation because it allows the malware access to the host. This technique appears early in the timeline and responding to it would effectively halt the adversaries' lateral movement. Terminating the chain of techniques at this point would prevent the malware from infecting the host, limiting operational damage in both IT and OT environments. If system backups are created after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the five observables associated with this technique, four are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 23 artifacts could be generated by the User Execution technique.
Technique Observers	IT Cybersecurity, OT Cybersecurity
Resources	Technique Detection References

3.3. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

Scripting was employed to connect the infected host to the C2 server using HTTPS and to receive commands from the adversaries. While reporting on this stage of the attack is scarce, the purpose of this scripting was most likely to establish the main backdoor using the adversaries' remote C2 server. Once the backdoor became operational, the adversaries leveraged it to gain information about the targeted field substation environment and load the Industroyer malware with proper configuration information to execute the attack. This script also created two new user accounts named "Administrator" and "System" on 1 December 2016 at 1:28 AM (D-17) and assigned them to a domain-matching local operations with delegated privileges.[11]

IT Cybersecurity and OT Cybersecurity personnel may have observed this technique, as malicious code may have triggered anomalous outbound and inbound traffic on both the IT and OT networks.

A total of 15 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because the system event logs in the active directory could have potentially notified observers of the Ukrenergo network intrusion. This technique appears early in the attack timeline and responding to it will disrupt further infection of the network. Terminating the chain of techniques at this point would limit operational damage to an attempt at malware infection. This technique modifies the host operating system files via the creation of anomalous services and modification of user accounts, resulting in the host being placed into a modified or compromised state. If system backups are created after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the 15 observables associated with this technique, 10 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 12 artifacts could be generated by the Scripting technique
Technique Observers	IT Cybersecurity, OT Cybersecurity
Resources	Technique Detection References

3.4. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

The adversaries employed the Valid Accounts technique (T0859) to build a set of login credentials starting around 1 December 2016 (D-16).[12] During this phase, they used these credentials to log in and escalate privileges on the host. These credentials eventually allowed the adversaries to move laterally across the OT environment to gain access to devices for C2 purposes. The adversaries combined this technique with other techniques to obtain access to additional systems in the ICS environment.

IT Cybersecurity and IT Staff personnel may have been able to observe the use of administrative accounts on the domain controller by monitoring authentication logs and activity timestamps.

A total of 17 observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because compromised credentials are used to bypass access controls to various resources within a network or grant an adversary increased privileges to specific systems and devices. This technique appears early in the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

Of the 17 observables associated with this technique, 15 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Cybersecurity, IT Staff
Resources	Technique Detection References

3.5. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

The adversaries performed the Valid Accounts technique (T0859) not only to establish persistence on the victim OT network by building a set of credentials during the early stages of the attack, but also to move laterally across several devices. The adversaries created two new accounts named “System” and “Administrator” that were used for login attempts at over 100 endpoints, specified by host name.[13] These accounts were used to manipulate Native API to install the launcher from which the payloads would be delivered; the Native API technique will be discussed in more detail later in the technique chain.

IT Cybersecurity, OT Staff, and OT Cybersecurity may have observed an abnormal number of logon attempts by a single account on several endpoints simultaneously, or the creation of user accounts without a person or designee assigned to them.

A total of 20 observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it modifies the host operating environment via the creation of new accounts, placing the host into a modified or compromised state. This technique appears early in the timeline and if system backups are created after this technique is executed, data recovery and disaster recovery efforts may be impaired.

Of the 20 observables associated with this technique, 15 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.6. CONNECTION PROXY TECHNIQUE (T0884) FOR COMMAND AND CONTROL

Upon execution, Industroyer attempts to connect with a hardcoded internal proxy on TCP 3128 (default Squid proxy). If established, the backdoor attempts to reach an external C2 server via the internal proxy.[14] On 12 December 2016 (D-6) a new host device appeared on the Ukrenergo OT network running Microsoft SQL Server, along with two other devices that were accessed by adversaries. These devices most likely served as data historians to query directory information and record connection information regarding specific hosts as part of network discovery while also establishing C2 connectivity as a proxy. In addition, the same password credentials were applied at over 100 endpoints, specified by host name. Finally, one of the modules, IEC 104, attempted to connect to every Internet Protocol (IP) in the subnet via broadcast address.

IT Cybersecurity and OT Cybersecurity may have observed the numerous attempts to connect to an external server from within their network. Observers may also have noticed the use of an IP address not listed within their network.

A total of 12 observables were identified with the use of the Connection Proxy technique (T0884). This technique is important for investigation because it was the means by which the adversaries were able to establish C2 within a network and launch the intended attack. This technique appears early in the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

Of the 12 observables associated with this technique, 10 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of six artifacts could be generated by the Connection Proxy technique
Technique Observers	IT Cybersecurity, OT Cybersecurity
Resources	Technique Detection References

3.7. MASQUERADING TECHNIQUE (T0849) FOR EVASION

Each payload associated with Industroyer loads DLLs and EXEs with filenames associated with common electric power sector protocols, including 101.dll, 104.dll, 61850.dll, OPCClientDemo.dll, OPC.exe, and 61850.exe.[15] By naming these files after standard communication protocols, they are meant to avoid drawing unwanted attention to their presence and actual intent.

IT Cyber Security, OT Staff, and OT Cybersecurity may have observed masquerading activity that interacted with computer systems across many types of platforms and devices within control systems environments. Observers may have also noticed these files moving laterally between systems and their extensions being changed as they moved within the OT environment.

A total of nine observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation because these seemingly harmless files were the actual payload of the attack delivered by the Industroyer launcher. This technique appears early in the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' ability to discover network connections and seize control of low-level devices, such as Remote Terminal Units (RTUs).

Of the nine observables associated with this technique, four are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 15 artifacts could be generated by the Masquerading technique
Technique Observers	IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.8. COMMAND-LINE INTERFACE TECHNIQUE (T0807) FOR EXECUTION

The adversaries performed the Command-Line Interface technique (T0807) with the Industroyer payload dynamic link library (DLL) via a command line parameter in one of the main backdoor's "execute a shell" commands. The Industroyer framework centers around the use of several independent ICS payload modules implemented as DLLs, each targeted against specific ICS communication protocols: IEC 101, IEC 104, IEC 61850, and OPC DA. Industroyer loads these modules through its custom launcher executable. The launcher, which serves as the orchestrator for the adversaries' ICS capabilities, provides the framework for executing the ICS payload modules, in addition to providing a data wiper module.[16]

IT Cybersecurity, OT Staff, and OT Cybersecurity may have observed Command-Line Interface (CLI) activity interacting with computer systems across many types of platforms and devices within control systems environments. Observers may also have noticed use of CLIs to install and run new software, including malicious tools installed over the course of an attack.

A total of 31 observables were identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation because it facilitates malicious code execution and enables subsequent deployment of follow-on payloads and components. This technique appears early in the timeline and responding to it will likely disrupt the adversary's ability to impact ICS operations. Terminating the chain of techniques at this point would limit the adversary's ability to continue the attack and thereby limit operational damage.

Of the 31 observables associated with this technique, eight are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 25 artifacts could be generated by the Command-Line Interface technique
Technique Observers	IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.9. MASQUERADING TECHNIQUE (T0849) FOR EVASION

In addition to the adversaries disguising payload module files with standard protocol names, they made a backup backdoor that executes in case the first backdoor is discovered. The additional backdoor masquerades as a Windows Notepad file containing obfuscated binary text. Once the text is de-obfuscated, the remaining code is executed and beacons out to the adversaries' C2 server.[17] While this backdoor was not used in the 2016 attack, its presence demonstrates the adversaries' ability to build redundancy into the Industroyer framework.

IT Cybersecurity, OT Staff, and OT Cybersecurity may have observed Notepad files that change extensions, located in unusual folders on the host server. They may also notice outbound traffic to external servers and obfuscated text within the files themselves.

A total of four observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation because it allows adversaries to maintain persistence on IT and OT networks, even if the initial backdoor is discovered and isolated. This technique appears early in the timeline and responding to it may prevent the adversaries from continuing their attack. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

None of the four observables associated with this technique are assessed to be highly perceivable. These observables are listed in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 15 artifacts could be generated by the Masquerading technique
Technique Observers	IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.10. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

If the additional backdoor is utilized, the de-obfuscated Notepad file would send a beacon to an external proxy.[18] The adversaries would then receive this beacon and begin re-establishing a connection to the host network by downloading and running code that establishes a backdoor connection again.

IT Cybersecurity, OT Staff, and OT Cybersecurity may have observed outbound and inbound traffic to and from a remote host located in a different country with an unfamiliar IP address, as well as a new connection request to an unknown device outside the IT and OT networks.

A total of 12 observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation because it modifies the host operating system files, resulting in the host being placed into a modified or compromised state. This technique appears early but can appear anywhere in the timeline. If system backups are created after this technique is executed, the data recovery and disaster recovery efforts will be impaired.

Of the 12 observables associated with this technique, seven are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 23 artifacts could be generated by the User Execution technique
Technique Observers	IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.11. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

The adversaries used a variety of native system commands, known utilities, and custom scripts from the core server hosts to launch the attack.[19] These native system commands combined with credential re-use were used to deploy and execute ICS impact packages. Industroyer relies on existing MS Windows built-in tools like PowerShell. With the help of these tools, additional malware is downloaded to modify the infected host system and enable the jump into the ICS network.[20] After accessing the ICS network, the Industroyer payloads are deployed onto the targeted system as a system service.[21] Each of the payload and data wiper components are standard Windows DLL files.

During this stage, the adversaries renamed the PSExec executable (ps.exe) and used multiple Visual Basic Script (VBS) and batch (BAT) scripts to facilitate file movement, system survey, and as a wrapper for PowerShell execution.[22]

IT Cybersecurity and OT Cybersecurity may have observed anomalous execution of native operating system utilities on the core server host, as well as anomalous creation of multiple services.

A total of 48 observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because the presence of an executable file command-line calling to PsExec could indicate remote execution by adversaries. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

Of the 48 observables associated with this technique, 18 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 25 artifacts could be generated by the Native API technique
Technique Observers	IT Cybersecurity, OT Cybersecurity
Resources	Technique Detection References

3.12 SERVICE STOP TECHNIQUE (T0881) FOR INHIBIT RESPONSE FUNCTION

The adversaries use Industroyer's 101 and 104 modules to interrupt services and then begin their own by blocking two serial communication (COM) ports and using a third to enable Industroyer's payloads. Additionally, the 104 module's configuration file has the built-in capability to specifically stop a service. Depending on configuration, a new communication process is started or an existing IEC 104 communications process is replaced.[23]

IT Cybersecurity, OT Staff, and OT Cybersecurity may have observed anomalous file modification and the inability to communicate successfully with a device.

A total of 45 observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation because it demonstrates the ability of the adversaries to not only interrupt a service, but to also replace it with its own while successfully communicating with a device from a remote server. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit adversaries' ability to successfully identify their intended target(s).

Of the 45 observables associated with this technique, 40 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 13 artifacts could be generated by the Service Stop technique
Technique Observers	IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.13 BLOCK SERIAL COM TECHNIQUE (T0805) FOR INHIBIT RESPONSE FUNCTION

In Industroyer's 101 module, the first COM port from the configuration file is used for actual communication and the two other COM ports are opened to prevent other processes from accessing them. Thus, the IEC 101 payload component can take over and maintain control of RTU devices. The adversaries employ this technique to prevent instructions or configurations from reaching target devices.[24]

OT Staff and OT Cybersecurity may have observed an inability to communicate with an RTU, as well as execution of anomalous commands at the same time.

A total of 10 observables were identified with the use of the Block Serial COM technique (T0805). This technique is important for investigation because it represents the adversaries' first stage of directly preventing recovery after an attack is identified. This technique appears in the middle of the timeline and responding to it may limit future impacts. Terminating the chain of techniques at this point would limit the impact of the Industroyer payloads.

Of the 10 observables associated with this technique, six are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 17 artifacts could be generated by the Block Serial COM technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.14 DENIAL OF CONTROL TECHNIQUE (T0813) FOR IMPACT

Similar to the Block Serial COM technique, components of the Industroyer payloads temporarily block serial COM channels, preventing OT Staff and OT Cybersecurity from maintaining control of affected devices.[25]

Further, Industroyer contained hidden code in hex for a pre-defined timer determining when the blackout was to take place. Commands were then sent to the circuit breakers and protection relays which not only opened circuit breaker switches but also activated a malicious launcher component.

OT Staff and OT Cybersecurity may have observed an inability to communicate with an RTU, as well as execution of anomalous commands at the same time.

A total of 17 observables were identified with the use of the Denial of Control technique (T0813). This technique is important for investigation because it can prevent personnel from interacting with process controls, causing the affected process to operate in an undesired state. This technique appears late in the timeline and responding to it may allow defenders to regain control of the system. Terminating the chain of techniques at this point would limit operational damage.

Of the 17 observables associated with this technique, 12 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of eight artifacts could be generated by the Denial of Control technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.15 DENIAL OF VIEW TECHNIQUE (T0815) FOR IMPACT

Similar to the Denial of Control technique, components of the Industroyer payloads temporarily block serial COM channels, preventing OT Staff and OT Cybersecurity from observing the status of affected devices.[26]

OT Staff and OT Cybersecurity may have observed an inability to monitor the status of affected devices.

A total of 14 observables were identified with the use of the Denial of View technique (T0815). This technique is important for investigation because it reflects the level of impact to processes and operations. This technique appears late in the timeline and responding to it will allow defenders to regain visibility into the status of the system. Terminating the chain of techniques at this point would limit operational damage.

Of the 14 observables associated with this technique, 10 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of four artifacts could be generated by the Denial of View technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.16 BLOCK COMMAND MESSAGE TECHNIQUE (T0803) FOR INHIBIT RESPONSE FUNCTION

The adversaries used the IEC 101 payload component of the Industroyer malware, which opened the first COM port from the configuration file for actual communication, while the two other COM ports were opened to prevent other processes from accessing them. The adversaries used this technique to take over and maintain control of the RTU device and prevent authorized operators from accessing the system to correct a disruption or unsafe condition.[27]

OT Staff and OT Cybersecurity may have observed an inability to communicate with an RTU, as well as anomalous commands being executed at the same time.

A total of 10 observables were identified with the use of the Block Command Message technique (T0803). This technique is important for investigation because it represents the adversaries' first stage of directly preventing recovery after an attack is identified. This technique appears in the middle of the timeline and responding to it may limit future impacts. Terminating the chain of techniques at this point would limit the impact of the Industroyer payloads.

Of the 10 observables associated with this technique, six are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of nine artifacts could be generated by the Block Command Message technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.17 BLOCK REPORTING MESSAGE TECHNIQUE (T0804) FOR INHIBIT RESPONSE FUNCTION

Using the same technical characteristics as the Block Command Message technique (T0803), the adversaries used the first COM port from the configuration file for actual communication, while the two other COM ports were opened to prevent other processes accessing them. The adversaries used this technique to take over and maintain control of the RTU device and prevent authorized operators from receiving report messages with telemetry data pertaining to the current state of equipment and the industrial process. The adversaries attempted to hide their actions from an operator using this technique.[28]

OT Staff and OT Cybersecurity may have observed an inability to communicate with an RTU, as

A total of 10 observables were identified with the use of the Block Reporting Message technique (T0804). This technique is important for investigation because it represents the adversaries' first stage of directly preventing recovery after an attack is identified. This technique appears in the middle of the timeline and responding to it may limit future impacts. Terminating the chain of techniques at this point would limit the impact of the Industroyer payloads.

Of the 10 observables associated with this technique, six are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 18 artifacts could be generated by the Block Reporting Message technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.18 NETWORK CONNECTION ENUMERATION TECHNIQUE (T0840) FOR DISCOVERY

Industroyer's 61850 module enumerates all connected network adapters to determine their TCP/IP subnet masks. Based on the network address and broadcast address for connected IPs, the module then attempts to connect to every IP in the subnet via broadcast address. Each successful attempt is then followed by Manufacturing Message Specification (MMS) Read requests from the module to ascertain whether the substation's circuit breakers are opened or closed at the time. Each successful connection and the status of each Information Object Address (IOA) is then collected and stored by the adversaries prior to deploying additional payloads.[29]

The 104 module also has the ability to enumerate network connections through a range mode that attempts to connect to specific IP addresses using the protocol described in the IEC 60870-5-104 standard. The adversaries also used a custom port scanner tool to enumerate devices.

IT Cybersecurity, OT Staff, and OT Cybersecurity may have observed significant amounts of network traffic as the module attempted to connect to every IP address on the network via broadcast connections, along with a large number of unsuccessful communication attempts to devices that do not utilize IEC 61850 and 104 protocols.

A total of 30 observables were identified with the use of the Network Connection Enumeration technique (T0840). This technique is important for investigation, because it enables additional adversarial lateral movement within the operating environment through enumeration and connection attempts. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

Of the 30 observables associated with this technique, 16 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 33 artifacts could be generated by the Network Connection Enumeration technique
Technique Observers	IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.19 UNAUTHORIZED COMMAND MESSAGE TECHNIQUE (T0855) FOR IMPAIR PROCESS CONTROL

The adversaries sent unauthorized commands to RTUs to change the state of equipment using the Industroyer protocol payloads.[30] The adversaries instructed control system assets to perform actions outside of their intended functionality, and without the logical preconditions to trigger their expected function.

OT Staff may have observed the physical movement of breakers at the substation and subsequent load loss of electricity to the power grid, while OT Cybersecurity may have noticed anomalous network traffic and execution of anomalous commands on the host network.

A total of 40 observables were identified with the use of the Unauthorized Command Message technique (T0855). This technique is important for investigation because the adversaries leveraged these command messages as the payload of the attack, with little use of actual malware. Additionally, the adversary may have leveraged these command messages to mask adversarial activity or perform unwanted manipulation of ICS components. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

Of the 40 observables associated with this technique, 23 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 16 artifacts could be generated by the Unauthorized Command Message technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.20 MANIPULATION OF CONTROL TECHNIQUE (T0831) FOR IMPACT

Industroyer toggles breakers to the open state utilizing unauthorized command messages.[31]

IT Cybersecurity, OT Staff, and OT Cybersecurity may have observed the physical state of breakers opening and closing, then remaining open indefinitely. Other observers may have noticed loss of power in the vicinity of the substation.

A total of 41 observables were identified with the use of the Manipulation of Control technique (T0831). This technique is important for investigation because adversaries may place infrastructure into indeterminate states, increasing the risk of physical damage and harm to staff. This technique appears in the middle of the timeline, and responding to it may limit disruption of electricity distribution. Terminating the chain of techniques at this point may prevent physical damage to equipment.

Of the 41 observables associated with this technique, 29 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 16 artifacts could be generated by the Manipulation of Control technique
Technique Observers	IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.21 REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

Similar to Network Connection Enumeration (T0840), the 61850 payload DLL attempts to read the configuration file, the path to which is supplied by the launcher component. The configuration file is expected to contain a list of IP addresses of devices capable of communicating via the protocol described in the IEC 61850 standard. The OPC DA module also conducts Remote System Discovery by looking for OPC items with data in the IOPCBrowseServerAddressSpace interface regarding the state of circuit breakers.[32] The module then turns those items off, essentially opening the circuit breakers, to verify that it has reached its intended target.

OT Staff may have observed the physical movement of breakers at the substation and subsequent load loss of electricity to the power grid, while OT Cybersecurity may have noticed anomalous network traffic and executed anomalous commands on the host network.

A total of 31 observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation since adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifiers on a network that is used for lateral movement or discovery techniques. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

Of the 31 observables associated with this technique, 20 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 43 artifacts could be generated by the Remote System Discovery technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.22 REMOTE SYSTEM INFORMATION DISCOVERY TECHNIQUE (T0888) FOR DISCOVERY

Once the adversaries used Industroyer's OPC DA module to discover devices, they then used the IOPCBrowseServerAddressSpace function in the OPC DA module to get detailed information about remote systems and their peripherals and looked for items with the following strings: ctlSelOn, ctlOperOn, ctlSelOff, ctlOperOff, \Pos, and stVal. The adversaries used the information they obtained to aid in targeting and shaping follow-on behaviors.[33]

OT Staff may have observed the physical movement of breakers at the substation and subsequent load loss, while OT Cybersecurity may have noticed anomalous network traffic and anomalous commands being executed on the host network.

A total of 31 observables were identified with the use of the Remote System Information Discovery technique (T0888). This technique is important for investigation because it allows an adversary to gain additional insights and information about OT components, enabling further exploitation and movement within the operating environment. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

Of the 31 observables associated with this technique, 20 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of eight artifacts could be generated by the Remote System Information Discovery technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.23 MONITOR PROCESS STATE TECHNIQUE (T0801) FOR COLLECTION

The Industroyer OPC and IEC 61850 protocol modules include the ability to send stVal requests to read the status of operational variables.[34] This allows the adversaries to track the status of each targeted breaker.

OT Staff may have observed the physical movement of breakers at the substation and subsequent load loss, while OT Cybersecurity may have noticed anomalous network traffic and execution of anomalous commands on the host network.

A total of 31 observables were identified with the use of the Monitor Process State technique (T0801). This technique is important for investigation because it demonstrates the capability to discover, identify, and manipulate OT devices in a very short time via automated sequence. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

Of the 31 observables associated with this technique, 20 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 12 artifacts could be generated by the Monitor Process State technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.24 AUTOMATED COLLECTION TECHNIQUE (T0802) FOR COLLECTION

Industroyer automatically collects OPC DA protocol object data to learn about control devices in the environment, in line with the previous three techniques discussed.[35]

OT Staff may have observed the physical movement of breakers at the substation and subsequent load loss, while OT Cybersecurity may have noticed anomalous network traffic and execution of anomalous commands on the host network.

A total of 31 observables were identified with the use of the Automated Collection technique (T0802). This technique is important for investigation because it enables data extraction, as well as persistence. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

Of the 31 observables associated with this technique, 20 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 23 artifacts could be generated by the Automated Collection technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.25 BRUTE FORCE I/O TECHNIQUE (T0806) FOR IMPAIR PROCESS CONTROL

The adversaries used the Brute Force I/O technique (T0806) to cause failures within various industrial processes. These failures could be the result of wear on equipment or damage to downstream equipment. The adversaries developed the Industroyer IEC 104 module with three modes available to perform its attack. These modes are range, shift, and sequence. The range mode operates in two stages. The first stage gathers IOAs and sends "select and execute" packets to switch the state. The second stage has an infinite loop where it will switch the state of all the previously discovered IOAs. Shift mode is similar to range mode, but instead of staying within the same range, it will add a shift value to the default range values.[36]

IT Cybersecurity, OT Staff, and OT Cybersecurity may have observed anomalous inbound network traffic and several failed attempts by a remote server to connect with devices on the OT network.

A total of 44 observables were identified with the use of the Brute Force I/O technique (T0806). This technique is important for investigation because it enables an adversary to issue unwanted commands to OT components, as well as harvest data from OT modules, potentially disabling critical functionality or enabling additional adversarial capabilities against OT components. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' ability to successfully identify their intended target(s).

Of the 44 observables associated with this technique, 29 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 19 artifacts could be generated by the Brute Force I/O technique
Technique Observers	IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.26 MANIPULATION OF VIEW TECHNIQUE (T0832) FOR IMPACT

Industroyer's OPC module can brute force values and will send out a 0x01 status, which for the target systems equates to a "Primary Variable Out of Limits," in this case preventing operators from understanding protective relay status.[37] This allowed the DoS module to function without the knowledge of the operator.

OT Staff and OT Cybersecurity may have observed anomalous files located on the host device, user logons during odd hours, and altered physical state of safety relays.

A total of 12 observables were identified with the use of the Manipulation of View technique (T0832). This technique is important for investigation because it can provide faulty information to OT Staff and Cybersecurity that could lead to ineffective defense measures. This technique appears late in the timeline and responding to it at this point may protect equipment from physical damage. Terminating the chain of techniques at this point may limit the adversaries' ability to cause physical damage to equipment.

Of the 12 observables associated with this technique, nine are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of four artifacts could be generated by the Manipulation of View technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.27 ACTIVATE FIRMWARE UPDATE MODE TECHNIQUE (T0800) FOR INHIBIT RESPONSE FUNCTION

In addition to the wiper deployed by Industroyer, the adversaries deployed a DoS module that placed the victim device into firmware update mode. While this would be a standard process under normal circumstances, the adversaries leveraged a known vulnerability that renders SIPROTEC protective relays unresponsive, requiring them to be manually rebooted. The Activate Firmware Update Mode technique was intended to prevent the protective relays from performing their designed protective functions and to leave an unprotected link in the electric transmission system by disabling the normal safeguards. However, the adversaries incorrectly configured the IP addresses to which the intended packets would be sent. Thus, this portion of the attack failed.[38]

OT Staff and OT Cybersecurity may have observed unresponsive RTUs, failure to communicate to ICS devices, opening of circuit breakers, and opening of protective relays.

A total of six observables were identified with the use of the Activate Firmware Update Mode technique (T0800). This technique is important for investigation because it enables an adversary to perform updates to device firmware, which can enable unwanted functionality, disable critical functionality, or allow for persistent unauthorized access. This technique appears very late in the timeline and responding to it may mitigate the extent of disruption and physical damage to equipment. Terminating the chain of techniques at this point would limit the adversaries' access and impact.

Of the six observables associated with this technique, five are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 14 artifacts could be generated by the Activate Firmware Update Mode technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.28 DENIAL OF SERVICE TECHNIQUE (T0814) FOR INHIBIT RESPONSE FUNCTION

Once the SIPROTEC devices are in firmware update mode, the DoS module exploits a known vulnerability that renders SIPROTEC protective relays unresponsive. At this stage, the target device stops responding to any commands until it is rebooted manually.[39] As a result, the normal safeguards are disabled, leaving an unprotected link in the electricity transmission infrastructure.[40]

OT Staff and OT Cybersecurity may have observed unresponsive RTUs, communications failure to ICS devices, opening of circuit breakers, and opening of protective relays. Additionally, OT Cybersecurity may have noticed anomalous files, such as the executable dos.exe, on the infected host.

A total of 11 observables were identified with the use of the Denial of Service technique (T0814). This technique is important for investigation because it can render devices unable to send and receive requests so they may not perform expected response functions in reaction to other events in the environment. This technique appears late in the timeline and responding to it may mitigate the extent of disruption and physical damage to equipment. Terminating the chain of techniques at this point may prevent immediate physical damage to equipment, but will not disrupt the adversaries' control of other OT systems.

Of the 11 observables associated with this technique, seven are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 14 artifacts could be generated by the Denial of Service technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.29 DEVICE RESTART/SHUTDOWN TECHNIQUE (T0816) FOR INHIBIT RESPONSE FUNCTION

Once Industroyer renders a SIPROTEC device unresponsive using the DoS module, the device must be restarted manually before it can resume operation.[41]

IT Cybersecurity, OT Staff, and OT Cybersecurity may have observed the complete shutdown of devices and anomalous timing of Activate Firmware Mode after an attack becomes apparent.

A total of nine observables were identified with the use of the Device Restart/Shutdown technique (T0816). This technique is important for investigation because it disables operation of ICS modules and can destroy evidence related to the manipulation of breakers. This technique appears late in the timeline and responding to it may mitigate the extent of disruption and physical damage to equipment. Terminating the chain of techniques at this point may prevent immediate physical damage to equipment, but will not disrupt the adversaries' control of other OT systems.

Of the nine observables associated with this technique, eight are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 18 artifacts could be generated by the Device Restart/Shutdown technique
Technique Observers	IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.30 LOSS OF PROTECTION TECHNIQUE (T0837) FOR IMPACT

The Activate Firmware Update Mode (T0800) and Denial of Service (T0814) techniques were intended to create a follow-on event after loss of power that would have caused physical damage to power distribution equipment. The adversaries' 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.[42] 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 without protection.[43]

In this scenario, manually closing breakers to restore operations after the initial stages of the attack allows the possibility of overcurrent without digital protection.[47] However, due to a programming error committed by the adversaries, this element of the attack did not execute successfully.

OT Staff and OT Cybersecurity may have observed open breakers, unresponsive RTUs, and anomalous files located on the device.

A total of 11 observables were identified with the use of the Loss of Protection technique (T0837). This technique is important for investigation because it allows for the investigation of physical damage to infrastructure. This technique appears late in the timeline and responding to it may mitigate the extent of disruption and physical damage to equipment. Terminating the chain of techniques at this point may prevent immediate physical damage to equipment, but not disrupt adversaries' control of other OT systems.

All 11 observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 14 artifacts could be generated by the Loss of Protection technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.31 DATA DESTRUCTION TECHNIQUE (T0809) FOR INHIBIT RESPONSE FUNCTION

Industroyer deploys a destructive wiper, whose files are marked with the phrase “haslo”, within a few hours of the execution of its 101, 104, 61850, and OPC DA modules. In this manner, the wiper hides the presence of the Industroyer malware after it runs. In addition, the wiper enumerates all drives on a device (except the one where it is located) and erases all files with OT-specific extensions, resulting in termination of all system processes.[44] The adversaries also destroyed data backups that were vital to recovery after the incident, forcing each affected device to be restarted manually.

OT Staff and OT Cybersecurity may have observed anomalous file names, such as haslo.dll, early on, followed by a complete system crash and all drives but one completely wiped on a device. Upon reboot, observers would notice that the system is still inoperable.

A total of 46 observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because it allows the adversaries to hide their presence in an infected network and ultimately render entire systems inoperable. This technique near the end of the timeline. This technique modifies the host operating system files via deletion of OT-specific files, placing the host into a modified or compromised state. If system backups are created after this technique is executed, data recovery and disaster recovery efforts will be impaired. Terminating the chain of techniques at this point would allow victim organizations to stop and recover from an attack before the final stages of impact occur.

Of the 46 observables associated with this technique, 41 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 27 artifacts could be generated by the Data Destruction technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.32 LOSS OF CONTROL TECHNIQUE (T0827) FOR IMPACT

Industroyer's wiper component removed the registry image path throughout the system and overwrote all files on 17 December (D-0), rendering the system unusable.[45]

OT Staff and OT Cybersecurity may have observed an inability to communicate with an RTU, as well as execution of anomalous commands at the same time.

A total of 44 observables were identified with the use of the Loss of Control technique (T0827). This technique is important for investigation because it prevents the victim from identifying and isolating the malware, giving Industroyer full control of RTUs and breakers. This technique represents the triggering event and appears near the end of the timeline, beyond the point at which a defender could take action to disrupt the attack. Terminating the chain of techniques at this point would have no impact, as the malware has already taken control of OT equipment.

Of the 44 observables associated with this technique, 42 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 13 artifacts could be generated by the Loss of Control technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.33 LOSS OF VIEW TECHNIQUE (T0829) FOR IMPACT

Similar to Loss of Control (T0827), Industroyer's wiper component removes the registry image path throughout the system and overwrites all files, rendering the system unusable.[46]

OT Staff and OT Cybersecurity may have observed an inability to monitor the status of affected devices.

A total of 44 observables were identified with the use of the Loss of View technique (T0829). This technique is important for investigation because at this point, the victim has lost all communication with OT systems and has effectively been rendered blind to what the adversaries may be doing. This technique appears at the end of the timeline, beyond the point at which a defender could take action to disrupt the attack. Terminating the chain of techniques at this point would have no impact, as the malware has already taken control of OT equipment.

Of the 44 observables associated with this technique, 42 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of four artifacts could be generated by the Loss of View technique
Technique Observers	OT Staff, OT Cybersecurity
Resources	Technique Detection References

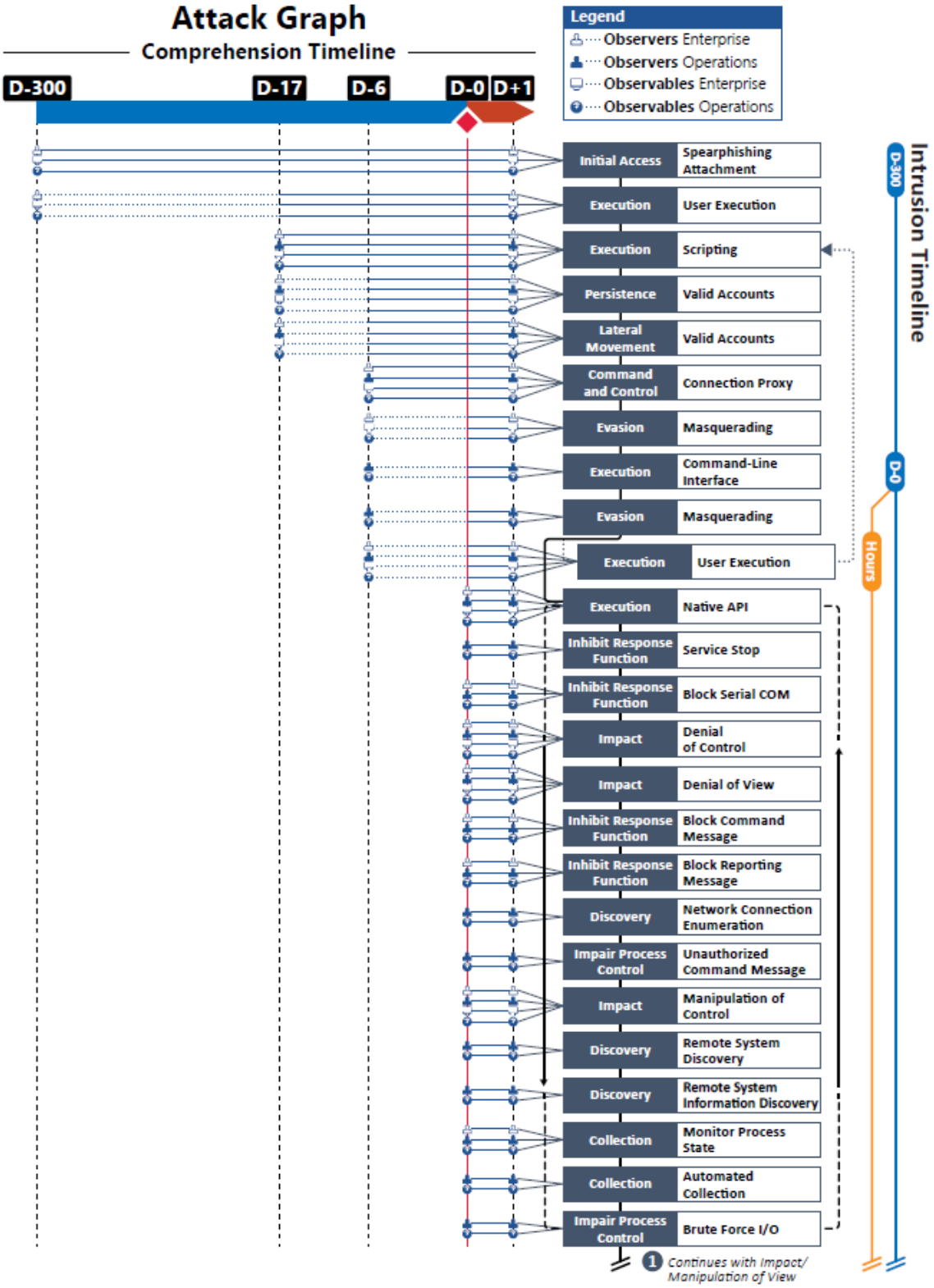


Figure 4. Attack Graph

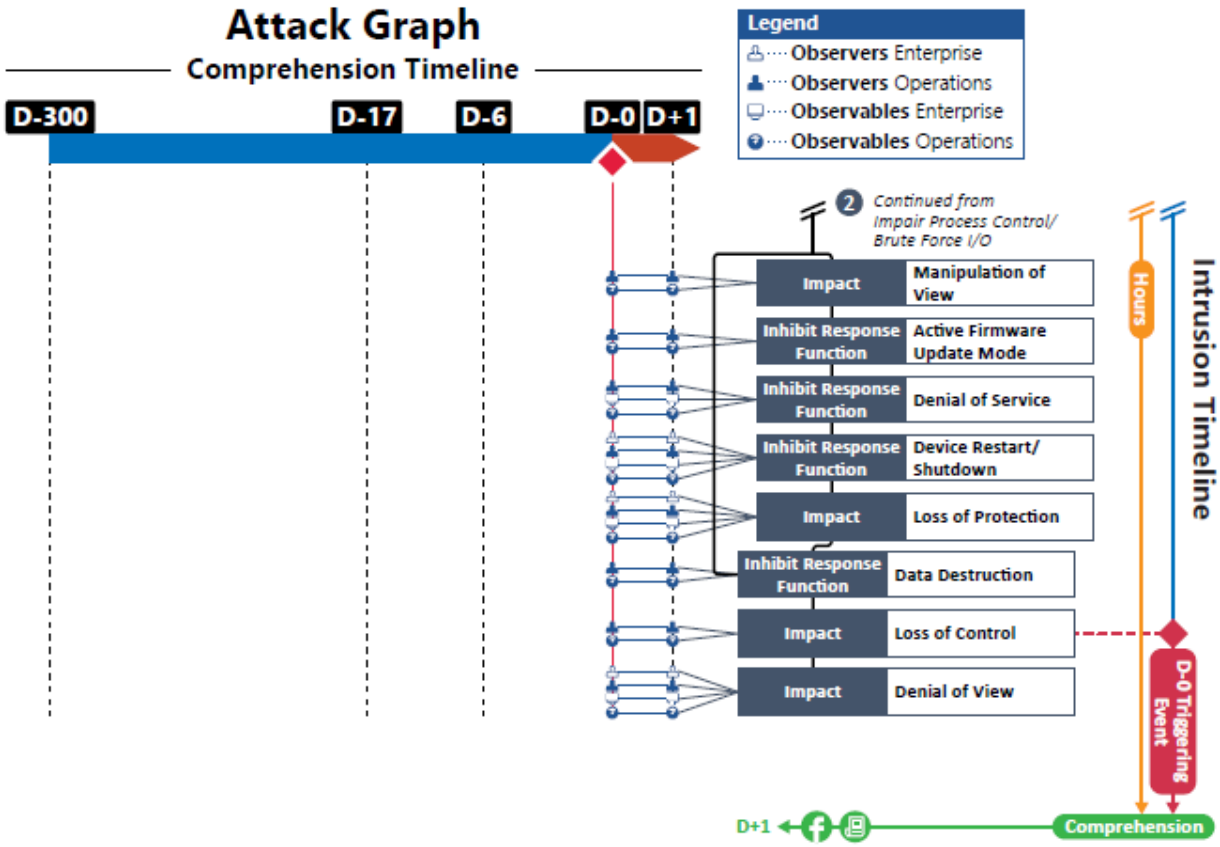


Figure 5. Attack Graph (CONTD)

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †

Observables Associated with Spearphishing Attachment Technique (T0865)	
Observable 1 †	*Anomalous Email with Attachment Received: MS Word Application Attachment: With Embedded Macro*
Observable 2	Anomalous Network Traffic Content: TCP Port 25

Observables Associated with User Execution Technique (T0863) (Section 3.2)	
Observable 1	Anomalous Email with Attachment Received: MS Word Application Attachment: With Embedded Macro
Observable 2 †	*New Process Has Been Created Windows Event Log (Windows Event ID 4688)*
Observable 3 †	*User Opens Anomalous Attachment*
Observable 4 †	*Anomalous Inbound Traffic: TCP port 139*
Observable 5 †	*Anomalous Outbound Traffic: TCP port 445*

Observables Associated with Scripting Technique (T0853)	
Observable 1 †	*Email with Anomalous MS Word Document*
Observable 2	New Process Creation: (Windows Event ID 4688)
Observable 3 †	*Anomalous Remote Desktop Application Access*
Observable 4 †	*Anomalous SMB Request: to Anomalous External IP: with Hard Coded IP*
Observable 5	Presence of Anomalous Document on Host: Anomalous MS Word Document
Observable 6 †	*Anomalous Outbound Network Traffic: TCP/UDP Port 139*
Observable 7 †	*Anomalous Outbound Network Traffic: TCP/UDP Port 445*
Observable 8 †	*Anomalous Outbound Network Traffic: TCP Port 80*
Observable 9 †	*Anomalous Inbound Network Traffic: From TCP Port 139*
Observable 10	*Anomalous Outbound Network Traffic: TCP Port 443: Download of Anomalous PowerShell Script to Host*
Observable 11	Presence of Anomalous PowerShell Script on Host
Observable 12	Execution of Downloaded PowerShell Script
Observable 13 †	*Anomalous Event Log Activity*
Observable 14 †	*Anomalous Creation of New Accounts on Network (Windows Event ID 4720)*
Observable 15 †	*Special Privileges Assigned: (Windows Event ID 4672)*

Observables Associated with Valid Accounts (T0859) (Section 3.4)	
Observable 1	Presence of Anomalous Binary on Host: Mimikatz Strings

Observables Associated with Valid Accounts (T0859) (Section 3.4)	
Observable 2 †	*Presence of Anomalous Binary on Host: mm.exe: 286c63d24fe9259bb6a758ce86e48c7f9094304ce4a32054641923a8cb4eab3c*
Observable 3 †	*Presence of Anomalous Binary on Host: ld.exe: 13a71a050d20aaad43ef78d771f22d636475b2ef8e4918731ff64d162287c480*
Observable 4	Anonymous Enumeration of User's Local Group Membership (Windows Event ID 4798)
Observable 5 †	*Anomalous Account Created (Windows Event ID 4720): "Admin"*
Observable 6 †	*Anomalous Account Created (Windows Event ID 4720): "System"*
Observable 7 †	*Special Privileges Anomalously Assigned (Windows Event ID 4672): "Admin"*
Observable 8 †	*Special Privileges Anomalously Assigned (Windows Event ID 4672): "System"*
Observable 9 †	*Anomalous Access to Administrator Credential Hashes: "Admin"*
Observable 10 †	*Anomalous Access to Administrator Credential Hashes: "System"*
Observable 11 †	*Anomalous Amount of Unsuccessful Logon attempts (Windows Event ID 4625): Over 100 Endpoints*
Observable 12 †	*Anomalous Successful Remote Logons (Windows Event ID 4624)*
Observable 13 †	*Anomalous Network Traffic: TCP Port 445*
Observable 14 †	*Anomalous Network Traffic: TCP Port 88*
Observable 15 †	*Anomalous Network Traffic: TCP Port 135*
Observable 16 †	*A Kerberos Service Ticket Was Requested (Windows Event ID 4769)*
Observable 17 †	*An Account Failed to Log On (Windows Event ID 4625)*

Observables Associated with Valid Accounts (T0859) (Section 3.5)	
Observable 1	Presence of Anomalous Binary on Host: Mimikatz Strings
Observable 2 †	*Presence of Anomalous Binary on Host: mm.exe*
Observable 3 †	*Presence of Anomalous Binary on Host: mm.exe: 286c63d24fe9259bb6a758ce86e48c7f9094304ce4a32054641923a8cb4eab3c*
Observable 4 †	*Presence of Anomalous Binary on Host: ld.exe*
Observable 5 †	*Presence of Anomalous Binary on Host: ld.exe: 13a71a050d20aaad43ef78d771f22d636475b2ef8e4918731ff64d162287c480*
Observable 6 †	*Anomalous Process on Host: mm.exe*
Observable 7 †	*Anomalous Process on Host: ld.exe*
Observable 8 †	*Anonymous Enumeration of User's Local Group Membership (Windows Event ID 4798)*
Observable 9	Anomalous Access to Administrator Credential Hashes: "Admin"
Observable 10	Anomalous Access to Administrator Credential Hashes: "System"

Observables Associated with Valid Accounts (T0859) (Section 3.5)	
Observable 11 †	*Anomalous Amount of Unsuccessful Logon attempts (Windows Event ID 4625): Over 100 Endpoints*
Observable 12 †	*Anomalous Successful Remote Logons (Windows Event ID 4624)*
Observable 13 †	*Anomalous Network Traffic: TCP Port 445*
Observable 14 †	*Anomalous Network Traffic: TCP Port 88*
Observable 15 †	*Anomalous Network Traffic: TCP Port 135*
Observable 16 †	*A Kerberos Service Ticket Was Requested (Windows Event ID 4769)*
Observable 17 †	*An Account Failed to Log On (Windows Event ID 4625)*
Observable 18 †	*Anomalous Process Creation from a Shell (Windows Event ID 4697): Anomalous Login Attempt Using Explicit Credentials (Windows Event ID 4648)*
Observable 19	Anomalous Shellcode Execution: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP>/u:<Host/Domain>\<User>/p:<Password>/t:-r cmd /c start c:\Intel\opc.exe'
Observable 20	Anomalous Shellcode Execution: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP> /u:<Host/Domain>\<User> /p:<Password> /t:-c sc config imapiservice binPath= "C:\Intel\imapi.exe C:\Intel\ imapi.dll i.ini" start= auto';

Observables Associated with Connection Proxy Technique (T0884)	
Observable 1	Anomalous Outbound Network Traffic: TCP Port 443
Observable 2 †	*Anomalous Inbound Traffic: TCP port 139: Jump Host Detection Using Netflow – Inbound Connection to a Host Immediately Followed by an Outbound Connection*
Observable 3 †	*Anomalous Creation of Network Connection: TCP 3128 (Default Squid Proxy)*
Observable 4	Anomalous Connection with Tor Client: TCP 443
Observable 5 †	*Anomalous Connection with Tor Client: TCP 9001*
Observable 6 †	*Anomalous Connection with Tor Client: TCP 9030*
Observable 7 †	*Anomalous Download of Tor Node List*
Observable 8 †	*Anomalous Network Connection: UDP 9050*
Observable 9 †	*Presence of Anomalous Network Application: Netflow Client: UDP 2055*
Observable 10 †	*Presence of Anomalous Network Application: Netflow Client: UDP 9996*
Observable 11 †	*Presence of Anomalous Network Application: Netflow Client: UDP 9997*
Observable 12 †	*Anomalous Network Connections from Network Application: Netflow Client: Over Stream Control Transmission Protocol (SCTP) Port 2904*

Observables Associated with Masquerading Technique (T0849) (Section 3.7)	
Observable 1	Anomalous Command Execution: via MSSQL xp_cmdshell Stored Procedure
Observable 2	Anomalous Time of Command Execution: 00:00-03:00 am UTC
Observable 3 †	*Anomalous File Created on Local Host: With Common System Process Name: 101.dll*
Observable 4 †	*Anomalous File Created on Local Host: With Common System Process Name: 104.dll: 7907dd95c1d36cf3dc842a1bd804f0db511a0f68f4b3d382c23a3c974a383cad*
Observable 5 †	*Anomalous File Created on Local Host: With Common System Process Name: 61850.dll: 4e7d2b269088c1575a31668d86de95fd3dde6caa88051d7ec110f7f150058789*
Observable 6 †	*Anomalous File Created on Local Host: With Common System Process Name: OPC.exe: 156bd34d713d0c8419a5da040b3c2dd48c4c6b00d8a47698e412db16b1ffac0f*
Observable 7	Anomalous Change of File Extension: From .exe to .txt
Observable 8	Anomalous Command Line Execution: "EXEC xp_cmdshell 'move C:\Delta\m32.txt C:\Delta\m32.exe"
Observable 9	Anomalous Mismatch of File Type with File Extension

Observables Associated with Command Line Interface Technique (T0807)	
Observable 1	Anomalous Network Creation: By Process Utilities: PsExec (Event ID: Event ID 4689)
Observable 2	Anomalous Network Creation: By Process Utilities: PsExec (Event ID: Event ID 7045)
Observable 3 †	*Anomalous Local Host CPU Prioritization of Processes: THREAD_PRIORITY_HIGHEST*
Observable 4 †	*Local Host CPU Prioritization of Anomalous Processes: Application Extension*
Observable 5 †	*Local Host CPU Prioritization of Anomalous Processes: Application Extension (101)*
Observable 6 †	*Local Host CPU Prioritization of Anomalous Processes: Application Extension (104)*
Observable 7 †	*Local Host CPU Prioritization of Anomalous Processes: Application Extension (OPC DA)*
Observable 8 †	*Local Host CPU Prioritization of Anomalous Processes: Application Extension (61850)*
Observable 9 †	*Local Host CPU Prioritization of Anomalous Processes: Application Extension (Wiper)*
Observable 10 †	*Local Host CPU Prioritization of Anomalous Processes: Application Extension (Backdoor)*
Observable 11	Anomalous Application Utility Attempts to Run a Module: IEC 101

Observables Associated with Command Line Interface Technique (T0807)	
Observable 12	Anomalous Application Utility Attempts to Run a Module: IEC 104
Observable 13	Anomalous Application Utility Attempts to Run a Module: 61850
Observable 14	Anomalous Application Utility Attempts to Run a Module: OPC DA
Observable 15	Anomalous Application Utility Attempts to Run a Module: "Haslo" (Wiper)
Observable 16	Anomalous Process Creation from a Shell (Windows Event ID 4697)
Observable 17	Anomalous Process Execution: Via Renamed PsExec Executable
Observable 18	Anomalous Command Line Execution: "EXEC xp_cmdshell 'move C:\Delta\m32.txt C:\Delta\m32.exe"
Observable 19	Anomalous Command Line Arguments: %LAUNCHER%.exe
Observable 20	Anomalous Command Line Arguments: %WORKING_DIRECTORY%
Observable 21	Anomalous Command Line Arguments: %PAYLOAD%.dll
Observable 22	Anomalous Command Line Arguments: %CONFIGURATION%.ini
Observable 23	Anomalous Execution of Native Operating System Utilities: sc.exe
Observable 24	Anomalous Execution of Native Operating System Utilities: rundll32.exe
Observable 25	Anomalous Execution of Native Operating System Utilities: powershell.exe
Observable 26	Anomalous Execution of Native Operating System Utilities: wscript.exe
Observable 27	Anomalous Execution of Native Operating System Utilities: regsvr32.exe
Observable 28	Anomalous Execution of Native Operating System Utilities: wmic.exe
Observable 29	Anomalous Execution of Native Operating System Utilities: wscript.exe
Observable 30	Anomalous Execution of Native Operating System Utilities: mshta.exe
Observable 31	Anomalous Execution of Native Operating System Utilities: pwsh.exe

Observables Associated with Masquerading Technique (T0849) (Section 3.9)	
Observable 1	Installation of Anomalous Host Application: Notepad: Version 5.1.2600.5512 (xpsp.080413-2105)
Observable 2	Anomalous Binary Within Host Application: Obfuscated Notepad Binary
Observable 3	Creation of Anomalous Process: Parent/Child Relationship: Deobfuscated Notepad Binary
Observable 4	Creation of New Process with Anomalous Metadata (Windows Event ID 4688)

Observables Associated with User Execution Technique (T0863) (Section 3.10)	
Observable 1	Creation of Anomalous Process: Parent/Child Relationship: Deobfuscated Notepad Binary

Observables Associated with User Execution Technique (T0863) (Section 3.10)	
Observable 2	Anomalous Binary Within Host Application: Obfuscated Notepad Binary: Creation of Anomalous Strings: RegisterPenApp
Observable 3	Anomalous Binary Within Host Application: Obfuscated Notepad Binary: Creation of Anomalous Strings: notepad.chm
Observable 4	Anomalous Binary Within Host Application: Obfuscated Notepad Binary: Creation of Anomalous Strings: hhctrl.ocx
Observable 5	Anomalous Binary Within Host Application: Obfuscated Notepad Binary: Creation of Anomalous Strings: CLSID\{ADB880A6-D8FF-11CF-9377-00AA003B7A11}\InprocServer32
Observable 6 †	*Anomalous Program Running from Notepad: csvd.exe: Presence of Anomalous Executable on Client: 61850.exe: 55e7471ad841bd8a110818760ea89af3bb456493f0798a54ce3b8e7b790afd0a*
Observable 7 †	*Attempted Connection to Anomalous Remote Host: 188.42.253.43:8820*
Observable 8 †	*Anomalous Network Traffic: Outbound Traffic: Over TCP Port 8080 [Squid Proxy]*
Observable 9 †	*Anomalous Network Traffic: Outbound Traffic: Over TCP Port 3128 [Squid Proxy]*
Observable 10 †	*Anomalous Attempted Connection to Remote Host: Over TCP Port 4444: Metasploit Service*
Observable 11 †	*Anomalous Attempted Connection to Remote Host: Over Server Message Block (SMB) TCP Port 445*
Observable 12 †	*Anomalous Network Traffic: Inbound Traffic: Over Server Message Block (SMB) TCP Port 139*

Observables Associated with Native API Technique (T0834)	
Observable 1 †	*Anomalous Rapid Authentication Attempts to Multiple Hosts: BEGIN EXEC master.dbo.sp_addlinkedserver @server = N'" & strLink & "', @srvproduct=N'SQL Server'; EXEC master.dbo.sp_addlinkedsrvlogin @rmtsrvname=N'" & strLink & "',@useself=N'False',@rmtuser=N'admin',@rmtpassword='<PASSWORD>'; END*
Observable 2	Anomalous Command Execution: via MSSQL xp_cmdshell Stored Procedure
Observable 3	Anomalous Powershell Commands: EXEC xp_cmdshell 'move C:\Delta\m32.txt C:\Delta\m32.exe
Observable 4	Anomalous Execution of Native Operating System Utilities: PsExec (ps.exe)
Observable 5	Presence of Anomalous Binaries on Local Host: svchost.exe
Observable 6	Presence of Anomalous Binaries on Local Host: cmd.exe /C
Observable 7	Execution of Anomalous Scripts on Local Host: Bat Scripts

Observables Associated with Native API Technique (T0834)	
Observable 8	Execution of Anomalous Scripts on Local Host: Bat Scripts: cscript C:\Backinfo\ufn.vbs <TargetIP> "C:\Backinfo\ImapiService.exe" "C:\Delta\svchost.exe"
Observable 9	Execution of Anomalous Scripts on Local Host: Bat Scripts: cscript C:\Backinfo\ufn.vbs <TargetIP> "C:\Backinfo\ImapiService.exe" "C:\Delta\svchost.exe": 7cc9ac6383437dd96161b93b017500a22a2c8d05f58778b9b9fce8ea73304546
Observable 10	cscript C:\Backinfo\ufn.vbs <TargetIP> "C:\Backinfo\ImapiService.exe" "C:\Delta\svchost.exe"
Observable 11	cscriptC:\Backinfo\ufn.vbs <TargetIP> "C:\Backinfo\101.dll" "C:\Delta\101.dll"
Observable 12	cscript C:\Backinfo\ufn.vbs <TargetIP> "C:\Backinfo\139.ini" "C:\Delta\101.ini"
Observable 13	cscript C:\Backinfo\ufn.vbs <TargetIP> "C:\Backinfo\haslo.dat" "C:\Delta\haslo.dat"
Observable 14	cscript C:\Backinfo\sqlc.vbs "<TargetIP>" "-c" "dir C:\Delta\"
Observable 15	cscript C:\Backinfo\ufn.vbs <TargetIP>"C:\Backinfo\ImapiService.exe" "C:\Delta\svchost.exe"
Observable 16	cscript C:\Backinfo\ufn.vbs <TargetIP> "C:\Backinfo\104.dll" "C:\Delta\104.dll"
Observable 17	cscript C:\Backinfo\ufn.vbs <TargetIP>"C:\Backinfo\140.ini" "C:\Delta\104.ini"
Observable 18	cscript C:\Backinfo\ufn.vbs <TargetIP> "C:\Backinfo\haslo.dat" "C:\Delta\haslo.dat"
Observable 19	cscript C:\Backinfo\sqlc.vbs "<TargetIP>" "-c" "dir C:\Delta\"
Observable 20	Execution of Anomalous Scripts on Local Host: VBS Scripts: "sc config"
Observable 21	Anomalous Export of Windows Operating System Library: 'Crash': 'Crash101.dll': cscriptC:\Backinfo\ufn.vbs <TargetIP> "C:\Backinfo\101.dll" "C:\Delta\101.dll"
Observable 22	Anomalous Creation of Service: sc.exe
Observable 23	Anomalous Creation of Service: runexe32.exe
Observable 24	Anomalous Creation of Service: powershell.exe
Observable 25	Anomalous Creation of Service: wscript.exe
Observable 26	Anomalous Creation of Service: regsvr32.exe
Observable 27	Anomalous Creation of Service: wmic.exe
Observable 28	Anomalous Creation of Service: mshta.exe
Observable 29	Anomalous Creation of Service: pwsh.exe
Observable 30 †	*Installation of Anomalous Service on Local Host: sc.exe*
Observable 31 †	*Installation of Anomalous Service on Local Host: rundll32.exe*
Observable 32 †	*Installation of Anomalous Service on Local Host: powershell.exe*
Observable 33 †	*Installation of Anomalous Service on Local Host: wscript.exe*

Observables Associated with Native API Technique (T0834)	
Observable 34 †	*Installation of Anomalous Service on Local Host: regsvr32.exe*
Observable 35 †	*Installation of Anomalous Service on Local Host: wmic.exe*
Observable 36 †	*Installation of Anomalous Service on Local Host: mshta.exe*
Observable 37 †	*Installation of Anomalous Service on Local Host: pwsh.exe*
Observable 38 †	*Presence of Anomalous Execution Files in Directory: sc.exe*
Observable 39 †	*Presence of Anomalous Execution Files in Directory: rundll32.exe*
Observable 40 †	*Presence of Anomalous Execution Files in Directory: powershell.exe*
Observable 41 †	*Presence of Anomalous Execution Files in Directory: wscript.exe*
Observable 42 †	*Presence of Anomalous Execution Files in Directory: regsvr32.exe*
Observable 43 †	*Presence of Anomalous Execution Files in Directory: wmic.exe*
Observable 44 †	*Presence of Anomalous Execution Files in Directory: wscript.exe*
Observable 45 †	*Presence of Anomalous Execution Files in Directory: mshta.exe*
Observable 46 †	*Presence of Anomalous Execution Files in Directory: pwsh.exe*
Observable 47	Script Execution at Anomalous Time: 17 December 2016 22:27 UTC
Observable 48	Script Execution at Anomalous Time: 20 December 2016 06:30 UTC

Observables Associated with Service Stop Technique (T0881)	
Observable 1	Anomalous Command Execution
Observable 2 †	*Anomalous File Modification*
Observable 3	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service = 0'
Observable 4	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service_name = process_01.exe'
Observable 5 †	*Termination of Standard Process: IEC 104 Protocol: D2MultiCommService.exe*
Observable 6	Anomalous Enumeration of Windows Services: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
Observable 7 †	*Anomalous Overwrite of ImagePath in Registry: SYSTEM\CurrentControlSet\Services: Overwrite with Empty String*
Observable 8 †	*Anomalous Overwrite of ImagePath in Registry: SYSTEM\CurrentControlSet\Services: Attempt to Overwrite ImagePath Twice*
Observable 9 †	*Presence of Anomalous File Content on Host: Overwrite with Random Data*
Observable 10	Anomalous Enumeration of All Drives on Device: Except Specific Drive
Observable 11 †	*Anomalous Deletion of Specific File Extensions: SYS_BASCOM.COM*
Observable 12 †	*Anomalous Deletion of Specific File Extensions: .pcmp*
Observable 13 †	*Anomalous Deletion of Specific File Extensions: .pcmi*

Observables Associated with Service Stop Technique (T0881)	
Observable 14 †	*Anomalous Deletion of Specific File Extensions: .pcmt*
Observable 15 †	*Anomalous Deletion of Specific File Extensions: .pl*
Observable 16 †	*Anomalous Deletion of Specific File Extensions: .paf*
Observable 17 †	*Anomalous Deletion of Specific File Extensions: .scl*
Observable 18 †	*Anomalous Deletion of Specific File Extensions: .cid*
Observable 19 †	*Anomalous Deletion of Specific File Extensions: .scd*
Observable 20 †	*Anomalous Deletion of Specific File Extensions: .xrf*
Observable 21 †	*Anomalous Deletion of Specific File Extensions: .v*
Observable 22 †	*Anomalous Deletion of Specific File Extensions: .trc*
Observable 23 †	*Anomalous Deletion of Specific File Extensions: .cin*
Observable 24 †	*Anomalous Deletion of Specific File Extensions: .ini*
Observable 25 †	*Anomalous Deletion of Specific File Extensions: .prj*
Observable 26 †	*Anomalous Deletion of Specific File Extensions: .mdf*
Observable 27†	*Anomalous Deletion of Specific File Extensions: .ldf*
Observable 28 †	*Anomalous Failure to Reboot Operating System (OS)*
Observable 29 †	*Anomalous Termination of System Processes: audiodg.exe*
Observable 30 †	*Anomalous Termination of System Processes: lsm.exe*
Observable 31 †	*Anomalous Termination of System Processes: svchost.exe*
Observable 32 †	*Anomalous Termination of System Processes: conhost.exe*
Observable 33 †	*Anomalous Termination of System Processes: services.exe*
Observable 34 †	*Anomalous Termination of System Processes: taskhost.exe*
Observable 35 †	*Anomalous Termination of System Processes: csrss.exe*
Observable 36 †	*Anomalous Termination of System Processes: shutdown.exe*
Observable 37 †	*Anomalous Termination of System Processes: wininit.exe*
Observable 38 †	*Anomalous Termination of System Processes: dwm.exe*
Observable 39 †	*Anomalous Termination of System Processes: smss.exe*
Observable 40 †	*Anomalous Termination of System Processes: winlogon.exe*
Observable 41 †	*Anomalous Termination of System Processes: explorer.exe*
Observable 42 †	*Anomalous Termination of System Processes: spoolss.exe*
Observable 43 †	*Anomalous Termination of System Processes: wuauclt.exe*
Observable 44 †	*Anomalous Termination of System Processes: lsass.exe*
Observable 45 †	*Anomalous Termination of System Processes: spoolsv.exe*

Observables Associated with Block Serial COM Technique (T0805)	
Observable 1 †	*Anomalous Communication Failures: From Windows Host: To Remote Terminal Unit (RTU): Multiple COM Ports Disabled*
Observable 2 †	*Presence of Anomalous File on Client: 101.dll*
Observable 3 †	*Presence of Anomalous Executable on Client: 101.exe*
Observable 4	Execution of Anomalous Executable on Client: 101.exe
Observable 5 †	*Presence of Anomalous File on Client: 104.dll: 7907dd95c1d36cf3dc842a1bd804f0db511a0f68f4b3d382c23a3c974a383cad*
Observable 6 †	*Presence of Anomalous Executable on Client: 104.exe*
Observable 7	Execution of Anomalous Executable on Client: 104.exe
Observable 8	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service = 0'
Observable 9	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service_name = process_01.exe'
Observable 10 †	*Termination of Standard Process: IEC 104 Protocol: D2MultiCommService.exe*

Observables Associated with Denial of Control Technique (T0813)	
Observable 1 †	*Presence of Anomalous File on Client: 61850.dll: 4e7d2b269088c1575a31668d86de95fd3dde6caa88051d7ec110f7f150058789*
Observable 2 †	*Presence of Anomalous Executable on Client: 61850.exe: 55e7471ad841bd8a110818760ea89af3bb456493f0798a54ce3b8e7b790afd0a*
Observable 3	Execution of Anomalous Executable on Client: 61850.exe
Observable 4 †	*Presence of Anomalous File on Client: i.ini*
Observable 5 †	*Anomalous Network Traffic: From Client to Controller: Access to Controller Firmware Functionality: Protective Relay Firmware: SIPROTEC: Inbound Traffic Intended for Anomalous IP addresses: UDP Port 50000*
Observable 6 †	*Anomalous Packet Received On Client: Access to Controller Firmware Functionality: Device Unresponsive:SIPROTEC Vulnerability: CVE-2015-5374: 0x11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E*
Observable 7 †	*Anomalous Communication Failures: From Windows Host: To Remote Terminal Unit (RTU): Multiple COM Ports Disabled*
Observable 8 †	*Presence of Anomalous Executable on Client: process_01.exe*
Observable 9 †	*Presence of Anomalous Executable on Client: process_01.exe*
Observable 10 †	*Presence of Anomalous Executable on Client: 101.exe*
Observable 11	Execution of Anomalous Executable on Client: 101.exe
Observable 12 †	*Presence of Anomalous File on Client: 104.dll: 7907dd95c1d36cf3dc842a1bd804f0db511a0f68f4b3d382c23a3c974a383cad*
Observable 13 †	*Presence of Anomalous Executable on Client: 104.exe*
Observable 14	Execution of Anomalous Executable on Client: 104.exe

Observables Associated with Denial of Control Technique (T0813)	
Observable 15	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service = 0'
Observable 16	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service_name = process_01.exe'
Observable 17 †	*Termination of Standard Process: IEC 104 Protocol: D2MultiCommService.exe*

Observables Associated with Denial of View Technique (T0815)	
Observable 1 †	*Anomalous Communication Failures: From Windows Host: To Remote Terminal Unit (RTU): Multiple COM Ports Disabled*
Observable 2 †	*Presence of Anomalous Executable on Client: process_01.exe*
Observable 3 †	*Presence of Anomalous File on Client: 101.dll*
Observable 4 †	*Presence of Anomalous Executable on Client: 101.exe*
Observable 5 †	*Presence of Anomalous File on Client: 104.dll: 7907dd95c1d36cf3dc842a1bd804f0db511a0f68f4b3d382c23a3c974a383cad*
Observable 6 †	*Presence of Anomalous Executable on Client: 104.exe*
Observable 7 †	*Presence of Anomalous Executable on Client: process_01.exe*
Observable 8	Execution of Anomalous Executable on Client: 101.exe
Observable 9	Execution of Anomalous Executable on Client: 104.exe
Observable 10 †	*Presence of Anomalous Executable on Client: process_01.exe*
Observable 11 †	*Presence of Anomalous Executable on Client: process_01.exe*
Observable 12	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service = 0'
Observable 13	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service_name = process_01.exe'
Observable 14 †	*Termination of Standard Process: IEC 104 Protocol: D2MultiCommService.exe*

Observables Associated with Block Command Message Technique (T0803)	
Observable 1 †	*Anomalous Communication Failures: From Windows Host: To Remote Terminal Unit (RTU): Multiple COM Ports Disabled*
Observable 2 †	*Presence of Anomalous File on Client: 101.dll*
Observable 3 †	*Presence of Anomalous Executable on Client: 101.exe*
Observable 4	Execution of Anomalous Executable on Client: 101.exe
Observable 5 †	*Presence of Anomalous File on Client: 104.dll: 7907dd95c1d36cf3dc842a1bd804f0db511a0f68f4b3d382c23a3c974a383cad*
Observable 6 †	*Presence of Anomalous Executable on Client: 104.exe*
Observable 7	Execution of Anomalous Executable on Client: 104.exe
Observable 8	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service = 0'

Observables Associated with Block Command Message Technique (T0803)	
Observable 9	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service_name = process_01.exe'
Observable 10 †	*Termination of Standard Process: IEC 104 Protocol: D2MultiCommService.exe*

Observables Associated with Block Reporting Message Technique (T0804)	
Observable 1 †	*Anomalous Communication Failures: From Remote Terminal Unit (RTU): To Windows Host: Multiple COM Ports Disabled*
Observable 2 †	*Presence of Anomalous File on Client: 101.dll*
Observable 3 †	*Presence of Anomalous Executable on Client: 101.exe*
Observable 4	Execution of Anomalous Executable on Client: 101.exe
Observable 5 †	*Presence of Anomalous File on Client: 104.dll: 7907dd95c1d36cf3dc842a1bd804f0db511a0f68f4b3d382c23a3c974a383cad*
Observable 6 †	*Presence of Anomalous Executable on Client: 104.exe*
Observable 7	Execution of Anomalous Executable on Client: 104.exe
Observable 8	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service = 0'
Observable 9	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service_name = process_01.exe'
Observable 10 †	*Termination of Standard Process: IEC 104 Protocol: D2MultiCommService.exe*

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 1 †	*Presence of Anomalous File on Client: 61850.dll: 4e7d2b269088c1575a31668d86de95fd3dde6caa88051d7ec110f7f150058789*
Observable 2 †	*Presence of Anomalous Executable on Client: 61850.exe: 55e7471ad841bd8a110818760ea89af3bb456493f0798a54ce3b8e7b790afd0a*
Observable 3	Execution of Anomalous Executable on Client: 61850.exe
Observable 4 †	*Presence of Anomalous File on Client: i.ini*
Observable 5 †	*Anomalous Connection Interruption: Between Client and Controller: Service Crash*
Observable 6 †	*Anomalous Network Traffic: From Client to Controller: From Workstation to ABB Sys600: Over TCP Port 102 (IEC 61850)*
Observable 7 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Failed Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 8 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Successful Network Connection: Over TCP Port 102 (IEC 61850)*

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 9	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, CF, Pos, and Model"
Observable 10	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal"
Observable 11	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal": Additional MMS Read request: "CSW, CO, Pos, Oper, but not $T"
Observable 12	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal": Additional MMS Read request: "CSW, CO, Pos, SBO, but not $T"
Observable 13	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOn"
Observable 14	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOff"
Observable 15	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "stVal"
Observable 16 †	*Anomalous Network Traffic: TCP Port 2404: Execution of anomalous script on Internet Object Address (IOAs) on Local Host*
Observable 17 †	*Anomalous Movement of Substation Breakers*
Observable 18 †	*Anomalous Network Traffic: TCP Port 80*
Observable 19	Anomalous Network Traffic: TCP Port 443
Observable 20 †	*Anomalous Network Traffic: TCP Port 3351*
Observable 21 †	*Presence of Anomalous File on Client: OPCClientDemo.dll*
Observable 22 †	*Presence of Anomalous Executable on Client: OPC.exe: 156bd34d713d0c8419a5da040b3c2dd48c4c6b00d8a47698e412db16b1ffac0f*
Observable 23	Execution of Anomalous Executable on Client: OPC.exe
Observable 24	Anomalous Command Line: OPC.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP>/u:<Host/Domain>\<User>/p:<Password>/t:-r cmd /c start c:\Intel\opc.exe'
Observable 25 †	*Presence of Anomalous File on Client: Image Mastering Application Programming Interface (imapi): imapi.dll: 12ba9887d3007b0a0713d9f1973e1176bd33eccb017b5a7dba166c7c172151e9*
Observable 26 †	*Presence of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe: 56ae7705ffcd56e74e5aecb0e43f17d510c2eaaddc7356f991c0db1daf32a641*
Observable 27	Execution of Anomalous Executable on Client: imapi.exe
Observable 28	Anomalous Command Line: imapi.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP> /u:<Host/Domain>\<User> /p:<Password>

Observables Associated with Network Connection Enumeration Technique (T0840)	
	/t:-c sc config imapiservice binPath= “C:\Intel\imapi.exe C:\Intel\ imapi.dll i.ini” start= auto’;
Observable 29 †	*Presence of Anomalous Port Scanner Tool: port.exe*
Observable 30	Execution of Anomalous Executable on Client: port.exe

Observables Associated with Unauthorized Command Message Technique (T0855)	
Observable 1 †	*Presence of Anomalous File on Client: 101.dll*
Observable 2 †	*Presence of Anomalous Executable on Client: 101.exe*
Observable 3	Execution of Anomalous Executable on Client: 101.exe
Observable 4	Anomalous Command Within Packet: C_SC_NA_1
Observable 5	Anomalous Command Within Packet: C_DC_NA_1
Observable 6 †	*Presence of Anomalous File on Client: 104.dll: 7907dd95c1d36cf3dc842a1bd804f0db511a0f68f4b3d382c23a3c974a383cad*
Observable 7 †	*Presence of Anomalous Executable on Client: 104.exe*
Observable 8	Execution of Anomalous Executable on Client: 104.exe
Observable 9	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service = 0'
Observable 10	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service_name = process_01.exe'
Observable 11 †	*Anomalous Termination of Standard Process: IEC 104 Protocol: D2MultiCommService.exe*
Observable 12	Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOn"
Observable 13	Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOff"
Observable 14	Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOn"
Observable 15	Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOff"
Observable 16	Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "stVal"
Observable 17 †	*Presence of Anomalous File on Client: 61850.dll: 4e7d2b269088c1575a31668d86de95fd3dde6caa88051d7ec110f7f150058789*
Observable 18 †	*Presence of Anomalous Executable on Client: 61850.exe: 55e7471ad841bd8a110818760ea89af3bb456493f0798a54ce3b8e7b790afd0a*
Observable 19	Execution of Anomalous Executable on Client: 61850.exe
Observable 20 †	*Presence of Anomalous File on Client: i.ini*

Observables Associated with Unauthorized Command Message Technique (T0855)	
Observable 21 †	*Anomalous Connection Interruption: Between Client and Controller: Service Crash*
Observable 22 †	*Anomalous Network Traffic: From Client to Controller: From Workstation to ABB Sys600: Over TCP Port 102 (IEC 61850)*
Observable 23 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Failed Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 24 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Successful Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 25	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOn"
Observable 26	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOff"
Observable 27	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "stVal"
Observable 28 †	*Anomalous Network Traffic: TCP Port 2404: Execution of Anomalous Script on Internet Object Address (IOAs) on Local Host*
Observable 29 †	*Presence of Anomalous File on Client: OPCClientDemo.dll*
Observable 30 †	*Presence of Anomalous Executable on Client: OPC.exe: 156bd34d713d0c8419a5da040b3c2dd48c4c6b00d8a47698e412db16b1ffac0f*
Observable 31	Execution of Anomalous Executable On Client: OPC.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP>/u:<Host/Domain>\<User>/p:<Password>/t:-r cmd /c start c:\Intel\opc.exe'
Observable 32 †	*Presence of Anomalous File on Client: Image Mastering Application Programming Interface (imapi): imapi.dll: 12ba9887d3007b0a0713d9f1973e1176bd33eccb017b5a7dba166c7c172151e9*
Observable 33 †	*Presence of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe: 56ae7705ffcd56e74e5aecb0e43f17d510c2eaaddc7356f991c0db1daf32a641*
Observable 34	Execution of Anomalous Executable On Client: imapi.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP> /u:<Host/Domain>\<User> /p:<Password> /t:-c sc config imapiservice binPath= "C:\Intel\imapi.exe C:\Intel\ imapi.dll i.ini" start= auto';
Observable 35 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOn"*
Observable 36 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOff"*
Observable 37 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOn"*

Observables Associated with Unauthorized Command Message Technique (T0855)	
Observable 38 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOff"*
Observable 39 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "stVal"*
Observable 40 †	*Anomalous Movement of Substation Breakers*

Observables Associated with Manipulation of Control Technique (T0831)	
Observable 1 †	*Presence of Anomalous File on Client: 101.dll*
Observable 2	Execution of Anomalous Executable on Client: 101.exe
Observable 3 †	*Anomalous Network Traffic: From Client to Controller: Access to Controller Firmware Functionality: Protective Relay Firmware: SIPROTEC: Inbound Traffic Intended for Anomalous IP addresses: UDP Port 50000*
Observable 4 †	*Anomalous Packet Received On Client: Access to Controller Firmware Functionality: Device Unresponsive:SIPROTEC Vulnerability: CVE-2015-5374: 0x11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E*
Observable 5 †	*Presence of Anomalous File on Client: 104.dll: 7907dd95c1d36cf3dc842a1bd804f0db511a0f68f4b3d382c23a3c974a383cad*
Observable 6 †	*Presence of Anomalous Executable on Client: process_01.exe*
Observable 7	Execution of Anomalous Executable on Client: 104.exe
Observable 8	Execution of Anomalous Executable on Client: process_01.exe
Observable 9	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service = 0'
Observable 10	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service_name = process_01.exe'
Observable 11 †	*Termination of Standard Process: IEC 104 Protocol: D2MultiCommService.exe*
Observable 12 †	*Anomalous Binary Within Configuration File*
Observable 13 †	*Anomalous Use of Remote Procedure Call (RPC): Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOn"*
Observable 14 †	*Anomalous Use of Remote Procedure Call (RPC): Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOff"*
Observable 15 †	*Anomalous Use of Remote Procedure Call (RPC): Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOn"*
Observable 16 †	*Anomalous Use of Remote Procedure Call (RPC): Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOff"*
Observable 17 †	*Anomalous Use of Remote Procedure Call (RPC): Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "stVal"*

Observables Associated with Manipulation of Control Technique (T0831)	
Observable 18 †	*Presence of Anomalous File on Client: 61850.dll: 4e7d2b269088c1575a31668d86de95fd3dde6caa88051d7ec110f7f150058789*
Observable 19 †	*Presence of Anomalous Executable on Client: 61850.exe: 55e7471ad841bd8a110818760ea89af3bb456493f0798a54ce3b8e7b790afd0a*
Observable 20	Execution of Anomalous Executable on Client: 61850.exe
Observable 21 †	*Presence of Anomalous File on Client: i.ini*
Observable 22 †	*Anomalous Network Traffic: From Client to Controller: From Workstation to ABB Sys600: Over TCP Port 102 (IEC 61850)*
Observable 23 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Failed Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 24 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Successful Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 25 †	*Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOn"*
Observable 26 †	*Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOff"*
Observable 27 †	*Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "stVal"*
Observable 28 †	*Presence of Anomalous File on Client: OPCClientDemo.dll*
Observable 29	Execution of Anomalous Executable on Client: OPC.exe
Observable 30 †	*Presence of Anomalous Script File on Client: remote.vbs*
Observable 31	Execution of Anomalous Executable On Client: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP>/u:<Host/Domain>\<User>/p:<Password>/t:-r cmd /c start c:\Intel\opc.exe'
Observable 32	Second Instance of Execution of Anomalous Executable on Client: OPC.exe
Observable 33 †	*Presence of Anomalous File on Client: Image Mastering Application Programming Interface (imapi): imapi.dll: 12ba9887d3007b0a0713d9f1973e1176bd33eccb017b5a7dba166c7c172151e9*
Observable 34 †	*Presence of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe: 56ae7705ffcd56e74e5aecb0e43f17d510c2eaaddc7356f991c0db1daf32a641*
Observable 35	Execution of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe
Observable 36	Execution of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe
Observable 37	Execution of Anomalous Executable On Client: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP> /u:<Host/Domain>\<User> /p:<Password>

Observables Associated with Manipulation of Control Technique (T0831)	
	/t:-c sc config imapiservice binPath= “C:\Intel\imapi.exe C:\Intel\ imapi.dll i.ini” start= auto’;
Observable 38 †	*Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOn"*
Observable 39 †	*Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOff"*
Observable 40 †	*Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "stVal"*
Observable 41 †	*Anomalous Movement of Substation Breakers*

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1 †	*Presence of Anomalous File on Client: 61850.dll: 4e7d2b269088c1575a31668d86de95fd3dde6caa88051d7ec110f7f150058789*
Observable 2 †	*Presence of Anomalous Executable on Client: 61850.exe: 55e7471ad841bd8a110818760ea89af3bb456493f0798a54ce3b8e7b790afd0a*
Observable 3	Execution of Anomalous Executable on Client: 61850.exe
Observable 4 †	*Presence of Anomalous File on Client: i.ini*
Observable 5 †	*Anomalous Connection Interruption: Between Client and Controller: Service Crash*
Observable 6 †	*Anomalous Network Traffic: From Client to Controller: From Workstation to ABB Sys600: Over TCP Port 102 (IEC 61850)*
Observable 7 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Failed Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 8 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Successful Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 9	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, CF, Pos, and Model"
Observable 10	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal"
Observable 11	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal": Additional MMS Read request: "CSW, CO, Pos, Oper, but not $T"
Observable 12	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal": Additional MMS Read request: "CSW, CO, Pos, SBO, but not $T"
Observable 13	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOn"

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 14	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOff"
Observable 15	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "stVal"
Observable 16 †	*Anomalous Network Traffic: TCP Port 80*
Observable 17 †	*Anomalous Network Traffic: TCP Port 3351*
Observable 18 †	*Presence of Anomalous File on Client: OPCClientDemo.dll*
Observable 19 †	*Presence of Anomalous Executable on Client: OPC.exe*
Observable 20 †	*Presence of Anomalous Executable on Client: OPC.exe: 156bd34d713d0c8419a5da040b3c2dd48c4c6b00d8a47698e412db16b1ffac0f*
Observable 21	Execution of Anomalous Executable On Client: OPC.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP>/u:<Host/Domain>\<User>/p:<Password>/t:-r cmd /c start c:\Intel\opc.exe'
Observable 22 †	*Presence of Anomalous File on Client: Image Mastering Application Programming Interface (imapi): imapi.dll: 12ba9887d3007b0a0713d9f1973e1176bd33eccb017b5a7dba166c7c172151e9*
Observable 23 †	*Presence of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe: 56ae7705ffcd56e74e5aecb0e43f17d510c2eaaddc7356f991c0db1daf32a641*
Observable 24	Execution of Anomalous Executable On Client: imapi.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP> /u:<Host/Domain>\<User> /p:<Password> /t:-c sc config imapiservice binPath= "C:\Intel\imapi.exe C:\Intel\ imapi.dll i.ini" start= auto';
Observable 25 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOn"*
Observable 26 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOff"*
Observable 27 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOn"*
Observable 28 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOff"*
Observable 29 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "stVal"*
Observable 30 †	*Presence of Anomalous Port Scanner Tool: port.exe*
Observable 31	Execution of Anomalous Executable on Client: port.exe

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 1 †	*Presence of Anomalous File on Client: 61850.dll: 4e7d2b269088c1575a31668d86de95fd3dde6caa88051d7ec110f7f150058789*
Observable 2 †	*Presence of Anomalous Executable on Client: 61850.exe: 55e7471ad841bd8a110818760ea89af3bb456493f0798a54ce3b8e7b790afd0a*
Observable 3	Execution of Anomalous Executable on Client: 61850.exe
Observable 4 †	*Presence of Anomalous File on Client: i.ini*
Observable 5 †	*Anomalous Connection Interruption: Between Client and Controller: Service Crash*
Observable 6 †	*Anomalous Network Traffic: From Client to Controller: From Workstation to ABB Sys600: Over TCP Port 102 (IEC 61850)*
Observable 7 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Failed Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 8 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Successful Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 9	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, CF, Pos, and Model"
Observable 10	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal"
Observable 11	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal": Additional MMS Read request: "CSW, CO, Pos, Oper, but not $T"
Observable 12	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal": Additional MMS Read request: "CSW, CO, Pos, SBO, but not $T"
Observable 13	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOn"
Observable 14	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOff"
Observable 15	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "stVal"
Observable 16 †	*Anomalous Network Traffic: TCP Port 80*
Observable 17 †	*Anomalous Network Traffic: TCP Port 3351*
Observable 18 †	*Presence of Anomalous File on Client: OPCClientDemo.dll*
Observable 19 †	*Presence of Anomalous Executable on Client: OPC.exe*
Observable 20 †	*Presence of Anomalous Executable on Client: OPC.exe: 156bd34d713d0c8419a5da040b3c2dd48c4c6b00d8a47698e412db16b1ffac0f*
Observable 21	Execution of Anomalous Executable On Client: OPC.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs

Observables Associated with Remote System Information Discovery Technique (T0888)	
	/s:<TargetIP>/u:<Host/Domain>\<User>/p:<Password>/t:-r cmd /c start c:\Intel\opc.exe'
Observable 22 †	*Presence of Anomalous File on Client: Image Mastering Application Programming Interface (imapi): imapi.dll: 12ba9887d3007b0a0713d9f1973e1176bd33eccb017b5a7dba166c7c172151e9*
Observable 23 †	*Presence of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe: 56ae7705ffcd56e74e5aecb0e43f17d510c2eaaddc7356f991c0db1daf32a641*
Observable 24	Execution of Anomalous Executable On Client: imapi.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP> /u:<Host/Domain>\<User> /p:<Password> /t:-c sc config imapiservice binPath= "C:\Intel\imapi.exe C:\Intel\ imapi.dll i.ini" start= auto';
Observable 25 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOn"*
Observable 26 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOff"*
Observable 27†	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOn"*
Observable 28 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOff"*
Observable 29 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "stVal"*
Observable 30 †	*Presence of Anomalous Port Scanner Tool: port.exe*
Observable 31	Execution of Anomalous Executable on Client: port.exe

Observables Associated with Monitor Process State Technique (T0801)	
Observable 1 †	*Presence of Anomalous File on Client: 61850.dll: 4e7d2b269088c1575a31668d86de95fd3dde6caa88051d7ec110f7f150058789*
Observable 2 †	*Presence of Anomalous Executable on Client: 61850.exe: 55e7471ad841bd8a110818760ea89af3bb456493f0798a54ce3b8e7b790afd0a*
Observable 3	Execution of Anomalous Executable on Client: 61850.exe
Observable 4 †	*Presence of Anomalous File on Client: i.ini*
Observable 5 †	*Anomalous Connection Interruption: Between Client and Controller: Service Crash*
Observable 6 †	*Anomalous Network Traffic: From Client to Controller: From Workstation to ABB Sys600: Over TCP Port 102 (IEC 61850)*
Observable 7 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Failed Network Connection: Over TCP Port 102 (IEC 61850)*

Observables Associated with Monitor Process State Technique (T0801)	
Observable 8 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Successful Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 9	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, CF, Pos, and Model"
Observable 10	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal"
Observable 11	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal": Additional MMS Read request: "CSW, CO, Pos, Oper, but not $T"
Observable 12	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal": Additional MMS Read request: "CSW, CO, Pos, SBO, but not $T"
Observable 13	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOn"
Observable 14	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOff"
Observable 15	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "stVal"
Observable 16 †	*Anomalous Network Traffic: TCP Port 80*
Observable 17 †	*Anomalous Network Traffic: TCP Port 3351*
Observable 18 †	*Presence of Anomalous File on Client: OPCClientDemo.dll*
Observable 19 †	*Presence of Anomalous Executable on Client: OPC.exe*
Observable 20 †	*Presence of Anomalous Executable on Client: OPC.exe: 156bd34d713d0c8419a5da040b3c2dd48c4c6b00d8a47698e412db16b1ffac0f*
Observable 21	Execution of Anomalous Executable On Client: OPC.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP>/u:<Host/Domain>\<User>/p:<Password>/t:-r cmd /c start c:\Intel\opc.exe'
Observable 22 †	*Presence of Anomalous File on Client: Image Mastering Application Programming Interface (imapi): imapi.dll: 12ba9887d3007b0a0713d9f1973e1176bd33eccb017b5a7dba166c7c172151e9*
Observable 23 †	*Presence of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe: 56ae7705ffcd56e74e5aecb0e43f17d510c2eaaddc7356f991c0db1daf32a641*
Observable 24	Execution of Anomalous Executable On Client: imapi.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP> /u:<Host/Domain>\<User> /p:<Password> /t:-c sc config imapiservice binPath= "C:\Intel\imapi.exe C:\Intel\ imapi.dll i.ini" start= auto';
Observable 25 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOn"*

Observables Associated with Monitor Process State Technique (T0801)	
Observable 26 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOff"*
Observable 27†	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOn"*
Observable 28 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOff"*
Observable 29 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "stVal"*
Observable 30 †	*Presence of Anomalous Port Scanner Tool: port.exe*
Observable 31	Execution of Anomalous Executable on Client: port.exe

Observables Associated with Automated Collection Technique (T0802)	
Observable 1 †	*Presence of Anomalous File on Client: 61850.dll: 4e7d2b269088c1575a31668d86de95fd3dde6caa88051d7ec110f7f150058789*
Observable 2 †	*Presence of Anomalous Executable on Client: 61850.exe: 55e7471ad841bd8a110818760ea89af3bb456493f0798a54ce3b8e7b790afd0a*
Observable 3	Execution of Anomalous Executable on Client: 61850.exe
Observable 4 †	*Presence of Anomalous File on Client: i.ini*
Observable 5 †	*Anomalous Connection Interruption: Between Client and Controller: Service Crash*
Observable 6 †	*Anomalous Network Traffic: From Client to Controller: From Workstation to ABB Sys600: Over TCP Port 102 (IEC 61850)*
Observable 7 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Failed Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 8 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Successful Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 9	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, CF, Pos, and Model"
Observable 10	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal"
Observable 11	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal": Additional MMS Read request: "CSW, CO, Pos, Oper, but not $T"
Observable 12	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "CSW, ST, Pos, and stVal": Additional MMS Read request: "CSW, CO, Pos, SBO, but not $T"
Observable 13	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOn"

Observables Associated with Automated Collection Technique (T0802)	
Observable 14	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOff"
Observable 15	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "stVal"
Observable 16 †	Anomalous Network Traffic: TCP Port 80
Observable 17 †	Anomalous Network Traffic: TCP Port 3351
Observable 18 †	Presence of Anomalous File on Client: OPCClientDemo.dll
Observable 19 †	Presence of Anomalous Executable on Client: OPC.exe
Observable 20 †	*Presence of Anomalous Executable on Client: OPC.exe: 156bd34d713d0c8419a5da040b3c2dd48c4c6b00d8a47698e412db16b1ffac0f*
Observable 21	Execution of Anomalous Executable On Client: OPC.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP>/u:<Host/Domain>\<User>/p:<Password>/t:-r cmd /c start c:\Intel\opc.exe'
Observable 22 †	*Presence of Anomalous File on Client: Image Mastering Application Programming Interface (imapi): imapi.dll: 12ba9887d3007b0a0713d9f1973e1176bd33eccb017b5a7dba166c7c172151e9*
Observable 23 †	*Presence of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe: 56ae7705ffcd56e74e5aecb0e43f17d510c2eaaddc7356f991c0db1daf32a641*
Observable 24	Execution of Anomalous Executable On Client: imapi.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP> /u:<Host/Domain>\<User> /p:<Password> /t:-c sc config imapiservice binPath= "C:\Intel\imapi.exe C:\Intel\ imapi.dll i.ini" start= auto';
Observable 25 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOn"*
Observable 26 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOff"*
Observable 27†	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOn"*
Observable 28 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOff"*
Observable 29 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "stVal"*
Observable 30 †	*Presence of Anomalous Port Scanner Tool: port.exe*
Observable 31	Execution of Anomalous Executable on Client: port.exe

Observables Associated with Brute Force I/O Technique (T0806)	
Observable 1 †	*Presence of Anomalous File on Client: 101.dll*

Observables Associated with Brute Force I/O Technique (T0806)	
Observable 2 †	*Presence of Anomalous Executable on Client: 101.exe*
Observable 3	Execution of Anomalous Executable on Client: 101.exe
Observable 4	Anomalous Command Within Packet
Observable 5	Anomalous Serial Traffic: From External Server to Remote Terminal Unit: Containing Command: C_SC_NA_1
Observable 6	Anomalous Serial Traffic: From External Server to Remote Terminal Unit: Containing Command: C_DC_NA_1
Observable 7 †	*Presence of Anomalous File on Client: 104.dll: 7907dd95c1d36cf3dc842a1bd804f0db511a0f68f4b3d382c23a3c974a383cad*
Observable 8 †	*Presence of Anomalous Executable on Client: 104.exe*
Observable 9	Execution of Anomalous Executable on Client: 104.exe
Observable 10 †	*Presence of Anomalous File on Client: i.ini*
Observable 11	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service = 0'
Observable 12	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service_name = process_01.exe'
Observable 13 †	*Termination of Standard Process: IEC 104 Protocol: D2MultiCommService.exe*
Observable 14 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOn"*
Observable 15 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOff"*
Observable 16 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOn"*
Observable 17 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOff"*
Observable 18 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "stVal"*
Observable 19 †	*Presence of Anomalous File on Client: 61850.dll: 4e7d2b269088c1575a31668d86de95fd3dde6caa88051d7ec110f7f150058789*
Observable 20 †	*Presence of Anomalous Executable on Client: 61850.exe: 55e7471ad841bd8a110818760ea89af3bb456493f0798a54ce3b8e7b790afd0a*
Observable 21	Execution of Anomalous Executable on Client: 61850.exe
Observable 22 †	*Presence of Anomalous File on Client: i.ini*
Observable 23 †	*Anomalous Connection Interruption*
Observable 24 †	*Anomalous Connection Interruption: Between Client and Controller: Program Crash*
Observable 25	Anomalous Network Traffic: From Client to Controller: From Workstation to ABB Sys600: Over TCP Port 102 (IEC 61850)

Observables Associated with Brute Force I/O Technique (T0806)	
Observable 26 †	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Failed Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 27†	*Anomalous Network Connection Request: Broadcast Request: From Client to Every IP Address on Network: Successful Network Connection: Over TCP Port 102 (IEC 61850)*
Observable 28	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOn"
Observable 29	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "ctlSelOff"
Observable 30	Anomalous Manufacturing Message Specification (MMS) Request: Read Request: Anomalous Function Call: "stVal"
Observable 31 †	*Anomalous Network Traffic: TCP Port 2404: Execution of anomalous script on Internet Object Address (IOAs) on Local Host*
Observable 32 †	*Presence of Anomalous File on Client: OPCClientDemo.dll*
Observable 33 †	*Presence of Anomalous Executable on Client: OPC.exe: 156bd34d713d0c8419a5da040b3c2dd48c4c6b00d8a47698e412db16b1ffac0f*
Observable 34	Execution of Anomalous Executable On Client: OPC.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP>/u:<Host/Domain>\<User>/p:<Password>/t:-r cmd /c start c:\Intel\opc.exe'
Observable 35 †	*Presence of Anomalous File on Client: Image Mastering Application Programming Interface (imapi): imapi.dll: 12ba9887d3007b0a0713d9f1973e1176bd33eccb017b5a7dba166c7c172151e9*
Observable 36 †	*Presence of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe: 56ae7705ffcd56e74e5aecb0e43f17d510c2eaaddc7356f991c0db1daf32a641*
Observable 37	Execution of Anomalous Executable on Client: imapi.exe
Observable 38	Execution of Anomalous Executable On Client: imapi.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP> /u:<Host/Domain>\<User> /p:<Password> /t:-c sc config imapiservice binPath= "C:\Intel\imapi.exe C:\Intel\ imapi.dll i.ini" start= auto';
Observable 39 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOn"*
Observable 40 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOff"*
Observable 41 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOn"*
Observable 42 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOff"*

Observables Associated with Brute Force I/O Technique (T0806)	
Observable 43 †	*Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "stVal"*
Observable 44 †	*Anomalous Movement of Substation Breakers*

Observables Associated with Manipulation of View Technique (T0832)	
Observable 1 †	*Presence of Anomalous File on Client: OPCClientDemo.dll*
Observable 2 †	*Presence of Anomalous Executable on Client: OPC.exe: 156bd34d713d0c8419a5da040b3c2dd48c4c6b00d8a47698e412db16b1ffac0f*
Observable 3	Execution of Anomalous Executable On Client: OPC.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP>/u:<Host/Domain>\<User>/p:<Password>/t:-r cmd /c start c:\Intel\opc.exe'
Observable 4 †	*Presence of Anomalous File on Client: Image Mastering Application Programming Interface (imapi): imapi.dll: 12ba9887d3007b0a0713d9f1973e1176bd33eccb017b5a7dba166c7c172151e9*
Observable 5 †	*Presence of Anomalous Executable on Client: Image Mastering Application Programming Interface (imapi): imapi.exe: 56ae7705ffcd56e74e5aecb0e43f17d510c2eaaddc7356f991c0db1daf32a641*
Observable 6	Execution of Anomalous Executable On Client: imapi.exe: EXEC xp_cmdshell 'cscript C:\Delta\remote.vbs /s:<TargetIP> /u:<Host/Domain>\<User> /p:<Password> /t:-c sc config imapiservice binPath= "C:\Intel\imapi.exe C:\Intel\ imapi.dll i.ini" start= auto';
Observable 7 †	*Anomalous Use of Remote Procedure Call (RPC): Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOn"*
Observable 8 †	*Anomalous Use of Remote Procedure Call (RPC): Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlSelOff"*
Observable 9 †	*Anomalous Use of Remote Procedure Call (RPC): Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOn"*
Observable 10 †	*Anomalous Use of Remote Procedure Call (RPC): Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "ctlOperOff"*
Observable 11 †	*Anomalous Use of Remote Procedure Call (RPC): Anomalous Interface Command on Local OPC Server: IOPCBrowseServerAddressSpace: "stVal"*
Observable 12	Anomalous Interface Command on Local OPC Server: IOPCSyncIOprotocol Function: Duplicated Value: 0x01

Observables Associated with Activate Firmware Update Mode Technique (T0800)	
Observable 1	Anomalous Network Traffic: From Client to Controller: Access to Controller Firmware Functionality: Protective Relay Firmware: SIPROTEC: Inbound Traffic Intended for Anomalous IP addresses: UDP Port 50000
Observable 2 †	*Anomalous Packet Received on Client: Access to Controller Firmware Functionality: Device Unresponsive: SIPROTEC Vulnerability: CVE-2015-5374: 0x11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E*
Observable 3 †	*Anomalous Network Traffic: Invalid IP Address Configuration*
Observable 4 †	*Presence of Anomalous Executable on Client: dos.exe: 4587ccfecc9a1ff5c5538a3475409ca1687d304bcde252077a119c436296857b*
Observable 5 †	*Presence of Anomalous Executable on Client: dos.exe*
Observable 6 †	*Control Processes in Anomalous State: Protective Relays Unresponsive*

Observables Associated with Denial of Service Technique (T0814)	
Observable 1	Anomalous Network Traffic: From Client to Controller: Access to Controller Firmware Functionality: Protective Relay Firmware: SIPROTEC: Inbound Traffic Intended for Anomalous IP addresses: UDP Port 50000
Observable 2 †	*Anomalous Packet Received On Client: Access to Controller Firmware Functionality: Device Unresponsive:SIPROTEC Vulnerability: CVE-2015-5374: 0x11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E*
Observable 3 †	*Anomalous Network Traffic: Invalid IP Address Configuration*
Observable 4 †	*Presence of Anomalous Executable on Client: process_01.exe*
Observable 5 †	*Presence of Anomalous Executable on Client: dos.exe: 4587ccfecc9a1ff5c5538a3475409ca1687d304bcde252077a119c436296857b*
Observable 6 †	*Presence of Anomalous Executable on Client: process_01.exe*
Observable 7	Execution of Anomalous Executable on Client: dos.exe
Observable 8 †	*Control Processes in Anomalous State: Safety Relays Unresponsive*
Observable 9	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service = 0'
Observable 10	Anomalous Binary Within Configuration File: 104.dll: 'stop_comm_service_name = process_01.exe'
Observable 11 †	*Termination of Standard Process: IEC 104 Protocol: D2MultiCommService.exe*

Observables Associated with Device Restart/Shutdown Technique (T0816)	
Observable 1 †	*Anomalous Shutdown of Device: Remote Terminal Unit (RTU)*
Observable 2 †	*Anomalous Network Traffic: From Client to Controller: Inbound Traffic Intended for Anomalous IP addresses: UDP Port 50000*
Observable 3	Anomalous Network Traffic: Invalid IP Address Configuration
Observable 4 †	*Presence of Anomalous Executable on Client: process_01.exe*

Observables Associated with Device Restart/Shutdown Technique (T0816)	
Observable 5 †	*Presence of Anomalous Executable on Client: dos.exe: 4587ccfecc9a1ff5c5538a3475409ca1687d304bcde252077a119c436296857b*
Observable 6 †	*Presence of Anomalous Executable on Client: dos.exe*
Observable 7 †	*Unresponsive Safety Relays*
Observable 8 †	*Anomalous Network Traffic: From Client to Controller: Access to Controller Firmware Functionality: Protective Relay Firmware: SIPROTEC: Inbound Traffic Intended for Anomalous IP addresses: UDP Port 50000*
Observable 9 †	*Anomalous Packet Received on Client: Access to Controller Firmware Functionality: Device Unresponsive:SIPROTEC Vulnerability: CVE-2015-5374: 0x11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E*

Observables Associated with Loss of Protection Technique (T0837)	
Observable 1 †	*Anomalous Interface Command on Local OPC Server: IOPCSyncIOprotocol Function: Duplicated Value: 0x01*
Observable 2 †	*Anomalous Shutdown of Device: Remote Terminal Unit (RTU)*
Observable 3 †	*Anomalous Network Traffic: From Client to Controller: Access of Firmware Functionality: Inbound Traffic Intended for Anomalous IP addresses: UDP Port 50000*
Observable 4 †	*Anomalous Network Traffic: Invalid IP Address Configuration*
Observable 5 †	*Presence of Anomalous Executable on Client: dos.exe: 4587ccfecc9a1ff5c5538a3475409ca1687d304bcde252077a119c436296857b*
Observable 6 †	*Presence of Anomalous Executable on Client: dos.exe*
Observable 7 †	*Operational Control Processes in Anomalous State: Protective Relays Unresponsive*
Observable 8 †	*Anomalous Network Traffic: From Client to Controller: Access to Controller Firmware Functionality: Protective Relay Firmware: SIPROTEC: Inbound Traffic Intended for Anomalous IP addresses: UDP Port 50000*
Observable 9 †	*Anomalous Packet Received On Client: Access to Controller Firmware Functionality: Device Unresponsive:SIPROTEC Vulnerability: CVE-2015-5374: 0x11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E*
Observable 10 †	*Anomalous Physical Damage to Substation Equipment*
Observable 11 †	*Anomalous Load Loss After System Reboot*

Observables Associated with Data Destruction Technique (T0809)	
Observable 1 †	*Presence of Anomalous File on Client: haslo.dat: 018eb62e174efdcdb3af011d34b0bf2284ed1a803718fba6edffe5bc0b446b81*
Observable 2 †	*Presence of Anomalous Executable on Client: haslo.exe: ad23c7930dae02de1ea3c6836091b5fb3c62a89bf2bcfb83b4b39ede15904910*

Observables Associated with Data Destruction Technique (T0809)	
Observable 3 †	*Local Host CPU Prioritization of Anomalous Processes: THREAD_PRIORITY_HIGHEST: Application Extension: Wiper ("Haslo")*
Observable 4	Anomalous Enumeration of Windows Services: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
Observable 5	Anomalous Overwrite of ImagePath in Registry (Windows Event ID 4657)
Observable 6	Anomalous Overwrite of ImagePath in Registry: SYSTEM\CurrentControlSet\Services
Observable 7	Anomalous Overwrite of ImagePath in Registry: SYSTEM\CurrentControlSet\Services: Overwrite with Empty String
Observable 8	Anomalous Overwrite of ImagePath in Registry: SYSTEM\CurrentControlSet\Services: Attempt to Overwrite ImagePath Twice
Observable 9 †	*Presence of Anomalous File Content on Host: Overwrite with Random Data*
Observable 10	Anomalous Enumeration of All Drives on Device: Except Specific Drive
Observable 11 †	*Anomalous Termination of All Processes (Windows Event ID 4660)*
Observable 12 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: SYS_BASCOM.COM*
Observable 13 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .pcmp*
Observable 14 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .pcmi*
Observable 15 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .pcmt*
Observable 16 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .pl*
Observable 17 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .paf*
Observable 18 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .scl*
Observable 19 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .cid*
Observable 20 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .scd*
Observable 21 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .xrf*
Observable 22 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .v*
Observable 23 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .trc*

Observables Associated with Data Destruction Technique (T0809)	
Observable 24 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .cin*
Observable 25 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .ini*
Observable 26 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .prj*
Observable 27 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .mdf*
Observable 28 †	*Anomalous Deletion of Specific Extensions: Operational Technology Specific File Extensions: .ldf*
Observable 29 †	*Anomalous Termination of System Processes: audiodg.exe*
Observable 30 †	*Anomalous Termination of System Processes: lsm.exe*
Observable 31 †	*Anomalous Termination of System Processes: svchost.exe*
Observable 32 †	*Anomalous Termination of System Processes: conhost.exe*
Observable 33 †	*Anomalous Termination of System Processes: services.exe*
Observable 34 †	*Anomalous Termination of System Processes: taskhost.exe*
Observable 35 †	*Anomalous Termination of System Processes: csrss.exe*
Observable 36 †	*Anomalous Termination of System Processes: shutdown.exe*
Observable 37 †	*Anomalous Termination of System Processes: wininit.exe*
Observable 38 †	*Anomalous Termination of System Processes: dwm.exe*
Observable 39 †	*Anomalous Termination of System Processes: smss.exe*
Observable 40 †	*Anomalous Termination of System Processes: winlogon.exe*
Observable 41 †	*Anomalous Termination of System Processes: explorer.exe*
Observable 42 †	*Anomalous Termination of System Processes: spoolss.exe*
Observable 43 †	*Anomalous Termination of System Processes: wuauclt.exe*
Observable 44 †	*Anomalous Termination of System Processes: lsass.exe*
Observable 45 †	*Anomalous Termination of System Processes: spoolsv.exe*
Observable 46 †	*System Reboot Anomalously Fails*

Observables Associated with Loss of Control Technique (T0827)	
Observable 1 †	*Local Host CPU Prioritization of Anomalous Processes: THREAD_PRIORITY_HIGHEST: Application Extension: Wiper ("Haslo")*
Observable 2 †	*Presence of Anomalous File on Client: haslo.dat: 018eb62e174efdcdb3af011d34b0bf2284ed1a803718fba6edffe5bc0b446b81*
Observable 3 †	*Presence of Anomalous Executable on Client: haslo.exe: ad23c7930dae02de1ea3c6836091b5fb3c62a89bf2bcfb83b4b39ede15904910*

Observables Associated with Loss of Control Technique (T0827)	
Observable 4	Anomalous Enumeration of Windows Services: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
Observable 5 †	*Anomalous Overwrite of ImagePath in Registry: SYSTEM\CurrentControlSet\Services: Overwrite with Empty String*
Observable 6 †	*Anomalous Overwrite of ImagePath in Registry: SYSTEM\CurrentControlSet\Services: Attempt to Overwrite ImagePath Twice*
Observable 7 †	*Presence of Anomalous File Content on Host: Overwrite with Random Data*
Observable 8	Anomalous Enumeration of All Drives on Device: Except Specific Drive
Observable 9 †	*Anomalous Termination of All Processes: Only Anomalous Process Left Running*
Observable 10 †	*Anomalous Deletion of Specific File Extensions: SYS_BASCOM.COM*
Observable 11 †	*Anomalous Deletion of Specific File Extensions: .pcmp*
Observable 12 †	*Anomalous Deletion of Specific File Extensions: .pcmi*
Observable 13 †	*Anomalous Deletion of Specific File Extensions: .pcmt*
Observable 14 †	*Anomalous Deletion of Specific File Extensions: .pl*
Observable 15 †	*Anomalous Deletion of Specific File Extensions: .paf*
Observable 16 †	*Anomalous Deletion of Specific File Extensions: .scl*
Observable 17 †	*Anomalous Deletion of Specific File Extensions: .cid*
Observable 18 †	*Anomalous Deletion of Specific File Extensions: .scd*
Observable 19 †	*Anomalous Deletion of Specific File Extensions: .xrf*
Observable 20 †	*Anomalous Deletion of Specific File Extensions: .v*
Observable 21 †	*Anomalous Deletion of Specific File Extensions: .trc*
Observable 22 †	*Anomalous Deletion of Specific File Extensions: .cin*
Observable 23 †	*Anomalous Deletion of Specific File Extensions: .ini*
Observable 24 †	*Anomalous Deletion of Specific File Extensions: .prj*
Observable 25 †	*Anomalous Deletion of Specific File Extensions: .mdf*
Observable 26 †	*Anomalous Deletion of Specific File Extensions: .ldf*
Observable 27 †	*Anomalous Termination of System Processes: audiodg.exe*
Observable 28 †	*Anomalous Termination of System Processes: lsm.exe*
Observable 29 †	*Anomalous Termination of System Processes: svchost.exe*
Observable 30 †	*Anomalous Termination of System Processes: conhost.exe*
Observable 31 †	*Anomalous Termination of System Processes: services.exe*
Observable 32 †	*Anomalous Termination of System Processes: taskhost.exe*
Observable 33 †	*Anomalous Termination of System Processes: csrss.exe*

Observables Associated with Loss of Control Technique (T0827)	
Observable 34 †	*Anomalous Termination of System Processes: shutdown.exe*
Observable 35 †	*Anomalous Termination of System Processes: wininit.exe*
Observable 36 †	*Anomalous Termination of System Processes: dwm.exe*
Observable 37 †	*Anomalous Termination of System Processes: smss.exe*
Observable 38 †	*Anomalous Termination of System Processes: winlogon.exe*
Observable 39 †	*Anomalous Termination of System Processes: explorer.exe*
Observable 40 †	*Anomalous Termination of System Processes: spoolss.exe*
Observable 41 †	*Anomalous Termination of System Processes: wuauclt.exe*
Observable 42 †	*Anomalous Termination of System Processes: lsass.exe*
Observable 43 †	*Anomalous Termination of System Processes: spoolsv.exe*
Observable 44 †	*System Reboot Anomalously Fails*

Observables Associated with Loss of View Technique (T0829)	
Observable 1 †	*Local Host CPU Prioritization of Anomalous Processes: THREAD_PRIORITY_HIGHEST: Application Extension: "Haslo" Wiper*
Observable 2 †	*Presence of Anomalous Executable on Client*
Observable 3 †	*Presence of Anomalous Executable on Client: haslo.exe: ad23c7930dae02de1ea3c6836091b5fb3c62a89bf2bcfb83b4b39ede15904910*
Observable 4	Anomalous Enumeration of Windows Services: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
Observable 5 †	*Anomalous Overwrite of ImagePath in Registry: SYSTEM\CurrentControlSet\Services: Overwrite with Empty String*
Observable 6 †	*Anomalous Overwrite of ImagePath in Registry: SYSTEM\CurrentControlSet\Services: Attempt to Overwrite ImagePath Twice*
Observable 7 †	*Presence of Anomalous File Content on Host: Content Overwritten with Random Data*
Observable 8	Anomalous Enumeration of All Drives on Device: Except Specific Drive
Observable 9 †	*Anomalous Termination of Critical Processes: Only Anomalous Process Left Running*
Observable 10 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: SYS_BASCOM.COM*
Observable 11 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .pcmp*
Observable 12 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files .pcmi*
Observable 13 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .pcmt*

Observables Associated with Loss of View Technique (T0829)	
Observable 14 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .pl*
Observable 15 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files .paf*
Observable 16 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .scl*
Observable 17 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .cid*
Observable 18 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files .scd*
Observable 19 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files:.xrf*
Observable 20 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .v*
Observable 21 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .trc*
Observable 22 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .cin*
Observable 23 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .prj*
Observable 24 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .mdf*
Observable 25 †	*Anomalous Deletion of Files: Specific Extensions: Operational Technology-Specific Files: .ldf*
Observable 26 †	*Anomalous Deletion of Files: Specific Extensions: General File: .ini*
Observable 27†	*Anomalous Termination of System Processes: audiodg.exe*
Observable 28 †	*Anomalous Termination of System Processes: lsm.exe*
Observable 29 †	*Anomalous Termination of System Processes: svchost.exe*
Observable 30 †	*Anomalous Termination of System Processes: conhost.exe*
Observable 31 †	*Anomalous Termination of System Processes: services.exe*
Observable 32 †	*Anomalous Termination of System Processes: taskhost.exe*
Observable 33 †	*Anomalous Termination of System Processes: csrss.exe*
Observable 34 †	*Anomalous Termination of System Processes: shutdown.exe*
Observable 35 †	*Anomalous Termination of System Processes: wininit.exe*
Observable 36 †	*Anomalous Termination of System Processes: dwm.exe*
Observable 37 †	*Anomalous Termination of System Processes: smss.exe*
Observable 38 †	*Anomalous Termination of System Processes: winlogon.exe*

Observables Associated with Loss of View Technique (T0829)	
Observable 39 †	*Anomalous Termination of System Processes: explorer.exe*
Observable 40 †	*Anomalous Termination of System Processes: spoolss.exe*
Observable 41 †	*Anomalous Termination of System Processes: wuauclt.exe*
Observable 42 †	*Anomalous Termination of System Processes: lsass.exe*
Observable 43 †	*Anomalous Termination of System Processes: spoolsv.exe*
Observable 44 †	*System Reboot Anomalously Fails*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Spearphishing Attachment Technique (T0865)	
Artifact 1	Mismatch MIME and Attachment File Extension
Artifact 2	Email Sender Address
Artifact 3	Email Message ID
Artifact 4	Email Receiver IP
Artifact 5	Email Receiver Name
Artifact 6	Email Receiver Domain
Artifact 7	Email Receiver Address
Artifact 8	Enable Macros Pop-up
Artifact 9	Email Application Log File
Artifact 10	Email Unified Audit Log File
Artifact 11	Email Service Name
Artifact 12	Suspicious Email Message Content
Artifact 13	Operating System Service Creation
Artifact 14	Email .PST File
Artifact 15	Email .OST File
Artifact 16	Simple Mail Transfer Protocol SMTP Traffic
Artifact 17	Mail Transfer Agent Logs
Artifact 18	Email Parent Process
Artifact 19	Mail Transfer Agent Logs
Artifact 20	Email Domain Name System DNS Traffic
Artifact 21	Email Domain Name System DNS Event
Artifact 22	File Attachment Warning Prompt
Artifact 23	Email Timestamp
Artifact 24	Email Attachment
Artifact 25	Email Attachment File Type
Artifact 26	Email Header
Artifact 27	Email Sender Name
Artifact 28	Email Sender IP Address
Artifact 29	Email Sender Domain

Artifacts Associated with User Execution Technique (T0863)	
Artifact 1	Command Execution
Artifact 2	Service Termination
Artifact 3	File Changes
Artifact 4	Increased ICMP Traffic (Network Scanning)
Artifact 5	Network Traffic Changes
Artifact 6	Application Installation
Artifact 7	Network Connection Creation
Artifact 8	Application Log Content
Artifact 9	User Account Modification
Artifact 10	File Creation
Artifact 11	Process Creation
Artifact 12	System Log
Artifact 13	Process Termination
Artifact 14	File Execution
Artifact 15	Prefetch Files
Artifact 16	Registry Modification
Artifact 17	File Modifications
Artifact 18	File Renaming
Artifact 19	System Patches Installed
Artifact 20	Files Opening
Artifact 21	File Signature Validation
Artifact 22	Installers Created
Artifact 23	Application Log

Artifacts Associated with Scripting Technique (T0853)	
Artifact 1	Startup Menu Modification
Artifact 2	OS Service Installation
Artifact 3	Registry Modifications
Artifact 4	Network Services Created
Artifact 5	External Network Connections
Artifact 6	Prefetch Files Created
Artifact 7	Executable Files
Artifact 8	System Processes Created

Artifacts Associated with Scripting Technique (T0853)	
Artifact 9	OS Timeline Event
Artifact 10	System Event Log Creation
Artifact 11	Files Dopped into Directory
Artifact 12	Windows API Event Log

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 1	Logon Session Creation
Artifact 2	User Account Creation
Artifact 3	Logon Type Entry
Artifact 4	Logon Timestamp
Artifact 5	Failed Logons Event
Artifact 6	Successful Logon Event
Artifact 7	System Logs
Artifact 8	Default Credential Use
Artifact 9	Authentication Creation
Artifact 10	Prefetch Files Created After Execution
Artifact 11	Logons
Artifact 12	Application Log
Artifact 13	Domain Permission Requests
Artifact 14	Permission Elevation Requests
Artifact 15	Application Use Times
Artifact 16	Configuration Changes

Artifacts Associated with Connection Proxy Technique (T0884)	
Artifact 1	Unexpected Application Communication to Network Proxy Port in Command Line Output (netstat)
Artifact 2	Unexpected Process Usage of Network Proxy Port Observed via Memory
Artifact 3	Unexpected Process Usage of Network Proxy Port Observed via OS Logs
Artifact 4	Unexpected Process Usage of Network Proxy Port Observed via firewall logs
Artifact 5	Unexpected Host Communicating with Network Proxy Port on Industrial Asset
Artifact 6	Unusual Network or Host Communications Identified in Network Proxy Log

Artifacts Associated with Masquerading Technique (T0849)	
Artifact 1	Command-Line Execution
Artifact 2	Additional Functionality in Applications
Artifact 3	Applications Causing Unintended Actions
Artifact 4	Leetspeak File Creation
Artifact 5	File Modification
Artifact 6	Process Metadata Changes
Artifact 7	Common Application with Non-Native Child Processes
Artifact 8	Scheduled Job Metadata
Artifact 9	Services Metadata
Artifact 10	Service Creation
Artifact 11	Scheduled Job Modification
Artifact 12	Additional File Directories Created
Artifact 13	File Creation with Common Name
Artifact 14	Leetspeak User Metadata
Artifact 15	Warez Application Use

Artifacts Associated with Command-Line Interface Technique (T0807)	
Artifact 1	Command Execution
Artifact 2	Application Log
Artifact 3	HTTP Traffic
Artifact 4	Telnet Traffic
Artifact 5	SSH Traffic
Artifact 6	VNC Traffic Port
Artifact 7	Process Creation
Artifact 8	Remote Connections
Artifact 9	Process Ending
Artifact 10	Script Execution
Artifact 11	User Account Logon
Artifact 12	User Account Privilege Change
Artifact 13	Logon Event
Artifact 14	Event Log Type
Artifact 15	Event Log Type
Artifact 16	Failed Logon Event

Artifacts Associated with Command-Line Interface Technique (T0807)	
Artifact 17	Command-Line Memory Data
Artifact 18	cmd.exe Application Execution
Artifact 19	RDP Traffic
Artifact 20	Industrial Application Execution
Artifact 21	POWERSHELL Cmdlet Application Execution
Artifact 22	Event ID 4103 POWERSHELL Command
Artifact 23	Event ID 4688 Command-Line Execution
Artifact 24	NTUSER Application Execution Entries
Artifact 25	External Network Connection

Artifacts Associated with Native API Technique (T0834)	
Artifact 1	Industrial Network Traffic
Artifact 2	Industrial Protocol Command Packet
Artifact 3	Device Reads
Artifact 4	Device I/O Image Table Manipulated
Artifact 5	Device Failure
Artifact 6	Alter Process Logic
Artifact 7	Device Performance Degradation
Artifact 8	Device Memory Modification
Artifact 9	Device Alarm
Artifact 10	Device Live Data Changes
Artifact 11	System Calls
Artifact 12	Alert Generated
Artifact 13	Memory Corruption
Artifact 14	Host Device Failure
Artifact 15	Blue Screen
Artifact 16	Performance Degradation
Artifact 17	SYSMON Events Created
Artifact 18	Services Initiated
Artifact 19	Processes Initiated
Artifact 20	Files Created
Artifact 21	Imports Hash Changed
Artifact 22	.dll Modifications

Artifacts Associated with Native API Technique (T0834)	
Artifact 23	System Resource Usage Management Changes
Artifact 24	Command Execution
Artifact 25	Configuration Change

Artifacts Associated with Service Stop Technique (T0881)	
Artifact 1	Internal System Logs
Artifact 2	Alarm Event
Artifact 3	OS API Call
Artifact 4	Application Error Messages
Artifact 5	Process Error Messages
Artifact 6	Application Service Stop
Artifact 7	Registry Change HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES
Artifact 8	OS Service Crash
Artifact 9	System Event Logs
Artifact 10	Application Event Logs
Artifact 11	System Resource Usage Manager Application Usage Change
Artifact 12	Command Line System Argument
Artifact 13	Process Failure

Artifacts Associated with Block Serial COM Technique (T0805)	
Artifact 1	Converter Protocol Denied
Artifact 2	Protocol Network Error
Artifact 3	Network Routing Failure
Artifact 4	Application Log Events
Artifact 5	Failed Connections
Artifact 6	Process Shutdown
Artifact 7	Physically Removed Connections
Artifact 8	Failed Command Input
Artifact 9	Failed Report Output
Artifact 10	Open TCP Session on Converter
Artifact 11	IP Address
Artifact 12	MAC Address

Artifacts Associated with Block Serial COM Technique (T0805)	
Artifact 13	External Network Connection
Artifact 14	Local Network Connections
Artifact 15	Serial Devices failure
Artifact 16	Reconfiguration of Device Unit ID
Artifact 17	Converter Update Notices

Artifacts Associated with Denial of Control Technique (T0813)	
Artifact 1	Network Ports Closed
Artifact 2	Input Failure
Artifact 3	Process Nonresponsive
Artifact 4	Network Ports Opened
Artifact 5	Serial Communication Failure
Artifact 6	Process Reboot
Artifact 7	Process Failure
Artifact 8	Increased Network Packet Delivery

Artifacts Associated with Denial of View Technique (T0815)	
Artifact 1	Application Logic Hooks or Modifications Might Prevent Proper Reporting to/from an Industrial Application
Artifact 2	File System Modification Artifacts Might Be Associated with The Denial of View Might Be Present on Disk
Artifact 3	Blocking Communications Paths and Channels (Comms, Network Infrastructure, Host Packet Routing) Might Occur via an OS or Device Modification
Artifact 4	Masked Reconfiguration of Alarm Thresholds or Other Configuration Settings Might Result in Unexpected Lack of Situational Awareness

Artifacts Associated with Block Command Message Technique (T0803)	
Artifact 1	New Network Connections Created
Artifact 2	Supervisory Application Log Event
Artifact 3	Supervisory Application Log Failure
Artifact 4	Application Processes Terminated
Artifact 5	Operational Data Mismatch Process Physical State
Artifact 6	Historian Data Missing

Artifacts Associated with Block Command Message Technique (T0803)	
Artifact 7	Historian Data Query Failure
Artifact 8	Operational Database Event Alarms
Artifact 9	Input failed to change operations device

Artifacts Associated with Block Reporting Message Technique (T0804)	
Artifact 1	Application Modification
Artifact 2	Physical Process Changes Without Data Received
Artifact 3	Conflicting Device Status Reports
Artifact 4	I/O Values Mismatched with Process Current State
Artifact 5	Delayed Operational Process Status Change
Artifact 6	Application Log Event Absent
Artifact 7	Historian Database Missing Data
Artifact 8	I/O Server Nonresponsive
Artifact 9	Real-time Operational Data Missing
Artifact 10	Supervisory Application Logs Mismatch Current State
Artifact 11	Process Status Modification
Artifact 12	Network Traffic Changes
Artifact 13	Network Connections Creation
Artifact 14	Operational Device Failure
Artifact 15	Operational Database Data Modification
Artifact 16	Operational Database Configuration Change
Artifact 17	Operational Process Termination
Artifact 18	Operational Process Alarm Failures

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 1	Common Network Traffic
Artifact 2	Polling Network Traffic from Abnormal IP Sender Addresses
Artifact 3	NetBIOS Name Services Port 137
Artifact 4	LDAP Port 389
Artifact 5	Active Directory Calls
Artifact 6	Email Server Calls
Artifact 7	SMTP Port 25 Traffic

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 8	DNS Lookup Queries
Artifact 9	ARP Scans
Artifact 10	TCP Connect Scan
Artifact 11	TCP SYN Scans
Artifact 12	Industrial Network Traffic
Artifact 13	TCP FIN Scans
Artifact 14	TCP Reverse Ident Scan
Artifact 15	TCP XMAS Scan
Artifact 16	TCP ACK Scan
Artifact 17	VNC Port 5900 Calls
Artifact 18	Protocol Content Enumeration
Artifact 19	Protocol Header Enumeration
Artifact 20	Recurring Protocol SYN Traffic
Artifact 21	Sequential Protocol SYN Traffic
Artifact 22	Statistical Anomalies in Network Traffic
Artifact 23	Echo Port 8 Traffic
Artifact 24	Device Failure
Artifact 25	Device Reboot
Artifact 26	Bandwidth Degradation
Artifact 27	Host Recent Connection Logs
Artifact 28	ICMP Port 7 Traffic
Artifact 29	SNMP Port 162 Traffic
Artifact 30	SNMP Port 161 Traffic
Artifact 31	Command Line Dialog Box Open
Artifact 32	Operating System Queries
Artifact 33	DNS Port 53 Zone Transfers

Artifacts Associated with Unauthorized Command Message Technique (T0855)	
Artifact 1	MAC Addresses
Artifact 2	Application Level I/O Manipulation
Artifact 3	Process Alarm Event
Artifact 4	Process Alarm
Artifact 5	Operational Data Created

Artifacts Associated with Unauthorized Command Message Technique (T0855)	
Artifact 6	OS Level I/O Manipulation
Artifact 7	IP Addresses
Artifact 8	Operational Application Log
Artifact 9	Process Logic Change
Artifact 10	Protocol Specific Command Packet
Artifact 11	Machine State Change
Artifact 12	Process Restart
Artifact 13	Process Failure
Artifact 14	Network Resets
Artifact 15	Protocol Metadata Change
Artifact 16	Process Timing Change

Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 1	Controller Set Point Change
Artifact 2	Event Log Creation
Artifact 3	Process Restart
Artifact 4	Process Shutdown
Artifact 5	Process State Change
Artifact 6	Process Initiated
Artifact 7	Controller Tag Change
Artifact 8	Controller Parameter Change
Artifact 9	I/O Modification
Artifact 10	Operational Data Modification
Artifact 11	Application File Modification
Artifact 12	Application Log Event
Artifact 13	Command Execution
Artifact 14	HMI Input Manipulation
Artifact 15	Altered Command Sequences
Artifact 16	Engineering Workstation Mouse Movement

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 1	Protocol Header Enumeration

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 2	Protocol Content Enumeration
Artifact 3	VNC Port 5900 Calls
Artifact 4	TCP ACK Scan
Artifact 5	TCP XMAS Scan
Artifact 6	Recurring Protocol SYN Traffic
Artifact 7	TCP FIN Scans
Artifact 8	Device Failure
Artifact 9	TCP Reverse Ident Scan
Artifact 10	Sequential Protocol SYN Traffic
Artifact 11	Scans Over Industrial Network Ports with Target IPS
Artifact 12	Industrial Network Traffic Content Containing Logical Identifiers
Artifact 13	SMTP Port 25 Traffic
Artifact 14	Device Reboot
Artifact 15	Bandwidth Degradation
Artifact 16	Host Recent Connection Logs
Artifact 17	IEC 101 Traffic to Serial Devices
Artifact 18	IEC 102
Artifact 19	IEC 104
Artifact 20	OPC Network Traffic
Artifact 21	Statistical Anomalies in Network Traffic
Artifact 22	DNS Port 53 Zone Transfers
Artifact 23	Industrial Network Traffic
Artifact 24	Common Network Traffic
Artifact 25	IEC 103 Traffic (For North America)
Artifact 26	IEC 61850 MMS
Artifact 27	Controller Proprietary Traffic
Artifact 28	Echo Type 8 Traffic
Artifact 29	ICMP Type 7 Traffic
Artifact 30	SNMP Port 162 Traffic
Artifact 31	SNMP Port 161 Traffic
Artifact 32	ARP Scans
Artifact 33	Operating System Queries
Artifact 34	TCP SYN Scans

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 35	Industrial Network Traffic Content About Hostnames
Artifact 36	Polling Network Traffic from Unauthorized IP Sender Addresses
Artifact 37	NETBIOS Name Services Port
Artifact 38	LDAP Port
Artifact 39	Active Directory Calls
Artifact 40	Email Server Calls
Artifact 41	DNS Lookup Queries
Artifact 42	TCP Connect Scan
Artifact 43	Command-Line Dialog Box Open

Artifacts Associated with Remote System Information Discovery Technique (T0888)	
Artifact 1	Unexpected Recon Associated Library Calls
Artifact 2	Unexpected Standard Protocol Usage
Artifact 3	Unexpected Recon Associated Command Line Options (Ping Sweep, netstat, etc.)
Artifact 4	Unexpected Recon Associated Child Processes (Ping Sweep, netstat, etc.)
Artifact 5	Exfiltration of Host, Network, and/or System Architecture or Configuration Data
Artifact 6	Compromise and Exfiltration of Data from Asset Information Datastores or Applications
Artifact 7	Unexpected Industrial Protocol Usage
Artifact 8	Unexpected Industrial Application Usage

Artifacts Associated with Monitor Process State Technique (T0801)	
Artifact 1	Network Read Request
Artifact 2	OPC Read Requests
Artifact 3	Local memory read requests
Artifact 4	Database Read Request
Artifact 5	External Network connections
Artifact 6	Internal Network Connections
Artifact 7	IP Addresses
Artifact 8	MAC Addresses
Artifact 9	Operational data exfiltration
Artifact 10	User Account Creation

Artifacts Associated with Monitor Process State Technique (T0801)	
Artifact 11	User Account Privilege Change
Artifact 12	SQL Read Requests

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 1	POWERSHELL Command Arguments
Artifact 2	External Network Connections
Artifact 3	SQL Read Requests
Artifact 4	User Account Creation
Artifact 5	Operational Data Exfiltration
Artifact 6	MAC Addresses
Artifact 7	IP Addresses
Artifact 8	Internal Network Connections
Artifact 9	Command Execution
Artifact 10	File Execution
Artifact 11	Local Memory Read Requests
Artifact 12	Command-Line Arguments
Artifact 13	Network Read Request
Artifact 14	Native Tool Use
Artifact 15	Service Log
Artifact 16	Application Log
Artifact 17	File Transfer
Artifact 18	SMB Traffic Port
Artifact 19	User Account Logs
Artifact 20	User Account Privilege Change
Artifact 21	Database Read Request
Artifact 22	OPC Read Requests
Artifact 23	File Creation

Artifacts Associated with Brute Force I/O Technique (T0806)	
Artifact 1	Application Log
Artifact 2	Network Bandwidth Degradation
Artifact 3	Select Packets Sent

Artifacts Associated with Brute Force I/O Technique (T0806)	
Artifact 4	Execute Packets Sent
Artifact 5	Process Specific Protocol Mode Change
Artifact 6	Network Session Creation
Artifact 7	External Network Connections
Artifact 8	Internal Network Connections
Artifact 9	Sequential Read Requests
Artifact 10	Operational Database Performance Degrades
Artifact 11	Low Network Resource Warning
Artifact 12	User Logon
Artifact 13	Change in Process State
Artifact 14	Device Failure
Artifact 15	IP Addresses
Artifact 16	MAC Addresses
Artifact 17	Command Packets
Artifact 18	Set Point Changes
Artifact 19	Device Polling Rate Increase

Artifacts Associated with Manipulation of View Technique (T0832)	
Artifact 1	Modification of Application Libraries or Dependencies
Artifact 2	Compromise and Manipulation of Data Storage Locations Used to Produce or Present Information to Operators
Artifact 3	A Rogue Proxy, Gateway, or Network Device in The Path of The Industrial Communications Could Manipulate Traffic
Artifact 4	Modification of Operating System or The Installation of a Filter Driver Could Lead to Manipulations of Packet at The Kernel Level

Artifacts Associated with Activate Firmware Update Mode Technique (T0800)	
Artifact 1	Firmware Update Dialog Box
Artifact 2	Input Command Failure
Artifact 3	Device Metadata Firmware Version Changes
Artifact 4	Device Flash Counter Changed
Artifact 5	Controller State Change
Artifact 6	Application Log Event

Artifacts Associated with Activate Firmware Update Mode Technique (T0800)	
Artifact 7	Process Malfunction
Artifact 8	Device Alarm
Artifact 9	Firmware Protocol Traffic
Artifact 10	File Download
Artifact 11	Byte Quantities Increase to Controllers
Artifact 12	IP Addresses
Artifact 13	MAC Address
Artifact 14	Controller Configuration Change

Artifacts Associated with Denial of Service Technique (T0814)	
Artifact 1	MAC Addresses
Artifact 2	ICMP Echo Port 7 Traffic Increase
Artifact 3	Application Failure
Artifact 4	Operational Data Corruption
Artifact 5	Application Log
Artifact 6	External Network Connections
Artifact 7	IP Addresses
Artifact 8	Network Traffic Connection Increase
Artifact 9	Services Failure
Artifact 10	Ransom Notice
Artifact 11	Low Resources Warning
Artifact 12	Increase Industrial Protocol Exceptions
Artifact 13	TDS Traffic Increase Port
Artifact 14	Process Performance Degrades

Artifacts Associated with Device Restart/Shutdown Technique (T0816)	
Artifact 1	Application Modification
Artifact 2	Physical Process Changes Without Data Received
Artifact 3	Conflicting Device Status Reports
Artifact 4	I/O Values Mismatched with Process Current State
Artifact 5	Delayed Operational Process Status Change
Artifact 6	Application Log Event Absent

Artifacts Associated with Device Restart/Shutdown Technique (T0816)	
Artifact 7	Historian Database Missing Data
Artifact 8	I/O Server Nonresponsive
Artifact 9	Real-time Operational Data Missing
Artifact 10	Supervisory Application Logs Mismatch Current State
Artifact 11	Process Status Modification
Artifact 12	Network Traffic Changes
Artifact 13	Network Connections Creation
Artifact 14	Operational Device Failure
Artifact 15	Operational Database Data Modification
Artifact 16	Operational Database Configuration Change
Artifact 17	Operational Process Termination
Artifact 18	Operational Process Alarm Failures

Artifacts Associated with Loss of Protection Technique (T0837)	
Artifact 1	Application Log
Artifact 2	TDS Traffic Increase Port
Artifact 3	Increase Industrial Protocol Exceptions
Artifact 4	Low Resources Warning
Artifact 5	Ransom Notice
Artifact 6	Service Failure
Artifact 7	Network Traffic Connection Increase
Artifact 8	IP Addresses
Artifact 9	MAC Addresses
Artifact 10	External Network Connections
Artifact 11	Process Performance Degrades
Artifact 12	Operational Data Corruption
Artifact 13	Application Failure
Artifact 14	ICMP Echo Port 7 Traffic Increase

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 1	Command Line Arguments
Artifact 2	Files Moved to Recycle Bin

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 3	Missing Files
Artifact 4	Host System Reboot Failure
Artifact 5	Process Logic Failure
Artifact 6	Event Log Creation
Artifact 7	System Call
Artifact 8	System Application Interruption
Artifact 9	Device Failure
Artifact 10	Recovery Attempt Failure
Artifact 11	TFTP Port
Artifact 12	SFTP Port
Artifact 13	Memory Corruption
Artifact 14	Use of File Transfer Protocols
Artifact 15	SCP Port
Artifact 16	File Encryptions
Artifact 17	Non-Native Files
Artifact 18	External Network Connections
Artifact 19	Transient Device Connections
Artifact 20	Program Execution
Artifact 21	Telnet Port
Artifact 22	FTPS Port
Artifact 23	HTTP Port
Artifact 24	HTTPS Port
Artifact 25	Local Network Connections
Artifact 26	FTP Port
Artifact 27	SMB Port

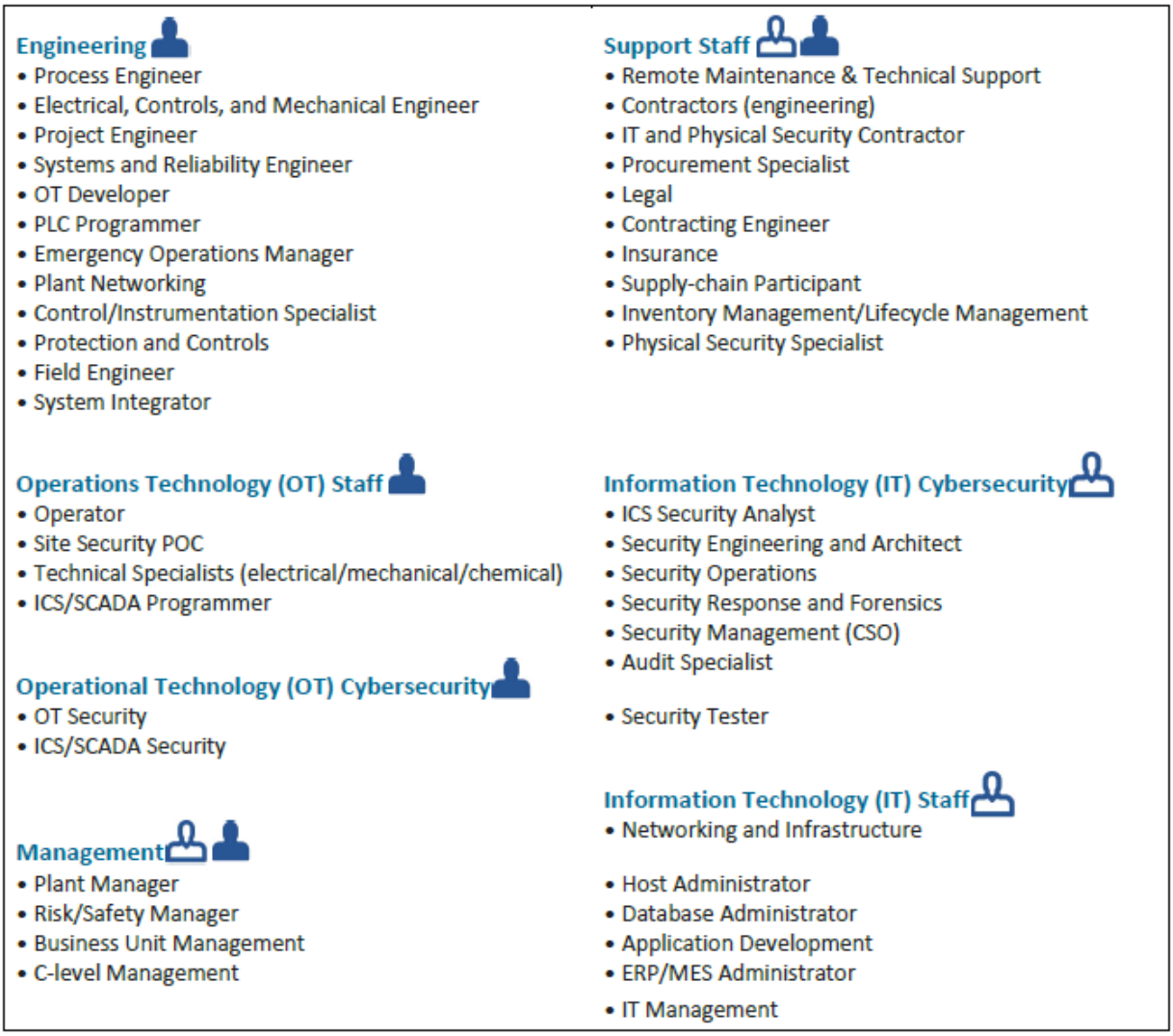
Artifacts Associated with Loss of Control Technique (T0827)	
Artifact 1	Failed Input Commands
Artifact 2	Repeated Maintenance Reports
Artifact 3	Process Failure
Artifact 4	Unresponsive I/O Conditions
Artifact 5	Network Connection Loss
Artifact 6	Process Environment Changes

Artifacts Associated with Loss of Control Technique (T0827)	
Artifact 7	Runaway Conditions
Artifact 8	Service Request Increases
Artifact 9	Set Point Failure
Artifact 10	Configuration Change
Artifact 11	Machine State Change
Artifact 12	Process Alarms
Artifact 13	Device Failure

Artifacts Associated with Loss of View Technique (T0829)	
Artifact 1	Blocking Communications Paths and Channels (Comms, Network Infrastructure, Host Packet Routing) Might Occur via an OS or Device Modification
Artifact 2	Masked Reconfiguration of Alarm Thresholds or Other Configuration Settings Might Result in Unexpected Lack of Situational Awareness
Artifact 3	File System Modification Artifacts Might Be Associated with The Loss of View Attack Might Be Present on Disk
Artifact 4	Application Logic Hooks or Modifications Might Prevent Proper Reporting to/from an Industrial Application

APPENDIX C: OBSERVERS

This is a collection of standardized potential observers that work in operational technology organizations. It has been slightly modified by the CyOTE team from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster to communicate the categories of potential observers during cyber events.



REFERENCES

[1] [Virus Bulletin | Joe Slowik | "VB2018 Paper: Anatomy of an Attack: Detecting and Defeating CRASHOVERIDE" | https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/ | 2018 | Accessed on 4 April 2022 | The source is publicly available information and does not contain classification markings]

[2] [Recorded Future | Monica Todros |"CRASHOVERRIDE: The Malware that Attacks Power Grids" | https://inlbox.app.box.com/file/1021198671254 | 10 January 2018 | Accessed on 23 March 2022 | The source is publicly available information and does not contain classification markings]

[3] [Dragos | Joe Slowik | "INDUSTROYER: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack" | https://www.dragos.com/wp-content/uploads/INDUSTROYER.pdf | 15 August 2019 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[4] [Virus Bulletin | Joe Slowik | "VB2018 Paper: Anatomy of an Attack: Detecting and Defeating CRASHOVERIDE" | https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/ | 2018 | Accessed on 4 April 2022 | The source is publicly available information and does not contain classification markings]

[5] [Dragos | Joe Slowik | "Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE" | https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf | 12 October 2018 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[6] [Dragos | Joe Slowik | "INDUSTROYER: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack" | https://www.dragos.com/wp-content/uploads/INDUSTROYER.pdf | 15 August 2019 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[7] [Virus Bulletin | Joe Slowik | "VB2018 Paper: Anatomy of an Attack: Detecting and Defeating CRASHOVERIDE" | https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/ | 2018 | Accessed on 4 April 2022 | The source is publicly available information and does not contain classification markings]

[8] [MITRE | Michael McFail, Jordan Hanna, and Daniel Rebori-Carretero | "Detection Engineering in Industrial Control Systems – Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study" | https://www.mitre.org/sites/default/files/publications/pr-22-0094-detection-engineering-in-industrial-control-systems-ukraine-2016-attack-case-study.pdf | December 2021 | Accessed on 2 June 2022 | The source is publicly available information and does not contain classification markings]

[9] [Dragos | Joe Slowik | "INDUSTROYER: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack" | https://www.dragos.com/wp-content/uploads/INDUSTROYER.pdf | 15 August 2019 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[10] [Dragos | Joe Slowik | "Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE" | https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf | 12 October 2018 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[11] [Virus Bulletin | Joe Slowik | "VB2018 Paper: Anatomy of an Attack: Detecting and Defeating CRASHOVERIDE" | https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/ | 2018 | Accessed on 4 April 2022 | The source is publicly available information and does not contain classification markings]

[12] [Dragos | Joe Slowik | “Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE” | https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf | 12 October 2018 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[13] [Dragos | Joe Slowik | “Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE” | https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf | 12 October 2018 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[14] [MITRE | Michael McFail, Jordan Hanna, and Daniel Rebori-Carretero | “Detection Engineering in Industrial Control Systems – Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study” | https://www.mitre.org/sites/default/files/publications/pr-22-0094-detection-engineering-in-industrial-control-systems-ukraine-2016-attack-case-study.pdf | December 2021 | Accessed on 2 June 2022 | The source is publicly available information and does not contain classification markings]

[15] [ESET | Anton Cherepanov | “Industroyer: Biggest threat to industrial control systems since Stuxnet” | https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet | 12 June 2017 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[16] [ESET | Anton Cherepanov | “Industroyer: Biggest threat to industrial control systems since Stuxnet” | https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet | 12 June 2017 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[17] [ESET | Anton Cherepanov | “Industroyer: Biggest threat to industrial control systems since Stuxnet” | https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet | 12 June 2017 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[18] [Virus Bulletin | Joe Slowik | “VB2018 Paper: Anatomy of an Attack: Detecting and Defeating CRASHOVERIDE” | https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/ | 2018 | Accessed on 4 April 2022 | The source is publicly available information and does not contain classification markings]

[19] [Virus Bulletin | Joe Slowik | “VB2018 Paper: Anatomy of an Attack: Detecting and Defeating CRASHOVERIDE” | https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/ | 2018 | Accessed on 4 April 2022 | The source is publicly available information and does not contain classification markings]

[20] [MITRE | Michael McFail, Jordan Hanna, and Daniel Rebori-Carretero | “Detection Engineering in Industrial Control Systems – Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study” | https://www.mitre.org/sites/default/files/publications/pr-22-0094-detection-engineering-in-industrial-control-systems-ukraine-2016-attack-case-study.pdf | December 2021 | Accessed on 2 June 2022 | The source is publicly available information and does not contain classification markings]

[21] [MITRE | Michael McFail, Jordan Hanna, and Daniel Rebori-Carretero | “Detection Engineering in Industrial Control Systems – Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study” | https://www.mitre.org/sites/default/files/publications/pr-22-0094-detection-engineering-in-industrial-control-systems-ukraine-2016-attack-case-study.pdf | December 2021 | Accessed on 2 June 2022 | The source is publicly available information and does not contain classification markings]

[22] [Virus Bulletin | Joe Slowik | “VB2018 Paper: Anatomy of an Attack: Detecting and Defeating CRASHOVERIDE” | https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/ | 2018 | Accessed on 4 April 2022 | The source is publicly available information and does not contain classification markings]

[23] [Virus Bulletin | Joe Slowik | "VB2018 Paper: Anatomy of an Attack: Detecting and Defeating CRASHOVERIDE" | https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/ | 2018 | Accessed on 4 April 2022 | The source is publicly available information and does not contain classification markings]

[24] [MITRE | MITRE Corporation and Joe Slowik | "Software: Industroyer, CRASHOVERRIDE" | https://collaborate.mitre.org/attackics/index.php/Software/S0001 | 14 March 2022 | Accessed 5 April 2022 | The source is publicly available information and does not contain classification markings]

[25] [Dragos | Joe Slowik | "Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE" | https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf | 12 October 2018 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[26] [Dragos | Joe Slowik | "Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE" | https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf | 12 October 2018 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[27] [MITRE | Michael McFail, Jordan Hanna, and Daniel Rebori-Carretero | "Detection Engineering in Industrial Control Systems – Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study" | https://www.mitre.org/sites/default/files/publications/pr-22-0094-detection-engineering-in-industrial-control-systems-ukraine-2016-attack-case-study.pdf | December 2021 | Accessed on 2 June 2022 | The source is publicly available information and does not contain classification markings]

[28] [MITRE | MITRE Corporation and Joe Slowik | "Software: Industroyer, CRASHOVERRIDE" | https://collaborate.mitre.org/attackics/index.php/Software/S0001 | 14 March 2022 | Accessed 5 April 2022 | The source is publicly available information and does not contain classification markings]

[29] [ESET | Anton Cherepanov | "Industroyer: Biggest threat to industrial control systems since Stuxnet" | https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet | 12 June 2017 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[30] [Dragos | Joe Slowik | "Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE" | https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf | 12 October 2018 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[31] [MITRE | MITRE Corporation and Joe Slowik | "Software: Industroyer, CRASHOVERRIDE" | https://collaborate.mitre.org/attackics/index.php/Software/S0001 | 14 March 2022 | Accessed 5 April 2022 | The source is publicly available information and does not contain classification markings]

[32] [ESET | Anton Cherepanov | "Industroyer: Biggest threat to industrial control systems since Stuxnet" | https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet | 12 June 2017 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[33] [ESET | Anton Cherepanov | "Industroyer: Biggest threat to industrial control systems since Stuxnet" | https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet | 12 June 2017 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[34] [MITRE | MITRE Corporation and Joe Slowik | "Software: Industroyer, CRASHOVERRIDE" | https://collaborate.mitre.org/attackics/index.php/Software/S0001 | 14 March 2022 | Accessed 5 April 2022 | The source is publicly available information and does not contain classification markings]

[35] [MITRE | MITRE Corporation and Joe Slowik | "Software: Industroyer, CRASHOVERRIDE" | https://collaborate.mitre.org/attackics/index.php/Software/S0001 | 14 March 2022 | Accessed 5 April 2022 | The source is publicly available information and does not contain classification markings]

[36] [MITRE | MITRE Corporation and Joe Slowik | “Software: Industroyer, CRASHOVERRIDE” | https://collaborate.mitre.org/attackics/index.php/Software/S0001 | 14 March 2022 | Accessed 5 April 2022 | The source is publicly available information and does not contain classification markings]

[37] [MITRE | MITRE Corporation and Joe Slowik | “Software: Industroyer, CRASHOVERRIDE” | https://collaborate.mitre.org/attackics/index.php/Software/S0001 | 14 March 2022 | Accessed 5 April 2022 | The source is publicly available information and does not contain classification markings]

[38] [Dragos | Joe Slowik | “INDUSTROYER: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack” | https://www.dragos.com/wp-content/uploads/INDUSTROYER.pdf | 15 August 2019 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[39] [ESET | Anton Cherepanov | “Industroyer: Biggest threat to industrial control systems since Stuxnet” | https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet | 12 June 2017 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[40] [Dragos | Joe Slowik | “INDUSTROYER: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack” | https://www.dragos.com/wp-content/uploads/INDUSTROYER.pdf | 15 August 2019 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[41] [MITRE | MITRE Corporation and Joe Slowik | “Software: Industroyer, CRASHOVERRIDE” | https://collaborate.mitre.org/attackics/index.php/Software/S0001 | 14 March 2022 | Accessed 5 April 2022

[42] [Dragos | Joe Slowik | “INDUSTROYER: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack” | https://www.dragos.com/wp-content/uploads/INDUSTROYER.pdf | 15 August 2019 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[43] [Dragos | Joe Slowik | “INDUSTROYER: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack” | https://www.dragos.com/wp-content/uploads/INDUSTROYER.pdf | 15 August 2019 | Accessed on 3 June 2022 | The source is publicly available information and does not contain classification markings]

[44] [Virus Bulletin | Joe Slowik | “VB2018 Paper: Anatomy of an Attack: Detecting and Defeating CRASHOVERIDE” | https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/ | 2018 | Accessed on 4 April 2022 | The source is publicly available information and does not contain classification markings]

[45] [MITRE | MITRE Corporation and Joe Slowik | “Software: Industroyer, CRASHOVERRIDE” | https://collaborate.mitre.org/attackics/index.php/Software/S0001 | 14 March 2022 | Accessed 5 April 2022 | The source is publicly available information and does not contain classification markings]

[46] [MITRE | MITRE Corporation and Joe Slowik | “Software: Industroyer, CRASHOVERRIDE” | https://collaborate.mitre.org/attackics/index.php/Software/S0001 | 14 March 2022 | Accessed 5 April 2022 | The source is publicly available information and does not contain classification markings]