PRECURSOR ANALYSIS REPORT: INDUSTROYER2 AND WIPER MALWARE TARGETING UKRAINIAN ENERGY PROVIDER 2022

Cybersecurity for the Operational Technology Environment (CyOTE)

31 MARCH 2023

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-23-71546

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: INDUSTROYER2 AND WIPER MALWARE TARGETING UKRAINIAN ENERGY PROVIDER 2022

1. EXECUTIVE SUMMARY

The Industroyer2 and Wiper Malware Targeting Ukrainian Energy Provider 2022 Precursor Analysis Report leverages publicly available information about the attack 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.

An adversary attempted to cause a blackout in Ukraine in April 2022 by using the Industroyer2 malware against a regional Ukrainian energy provider. The adversary targeted eight high-voltage electrical substations and utilized the malware in tandem with disk wipers for Windows, Linux, and Solaris operating systems in an attempt to make response and recovery efforts more difficult. The adversary reused a piece of the original Industroyer malware designed to open circuit breakers and de-energize target substations.

The adversary gained initial access to the victim's enterprise network through unknown means in February 2022 and was able to perform reconnaissance, pivot to the operations network, and reside in the system for at least 51 days. This gave the adversary a detailed understanding of the environment and allowed them to customize the Industroyer2 malware to the victim's operations network. However, defenders detected and stopped the attack before the adversary could achieve their intended impact. Had the Industroyer2 attack been successful, it could have caused a blackout for more than two million people during the early stages of Russia's invasion of Ukraine.

Researchers and analysts identified 22 unique techniques (used in a sequence of 31 steps) utilized during the attack with a total of 297 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-three of the identified techniques used during the Industroyer2 cyber attack were precursors to the triggering event. Analysis identified 224 observables associated with these precursor techniques, 122 of which were assessed to have an increased likelihood of being perceived in the 51 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.

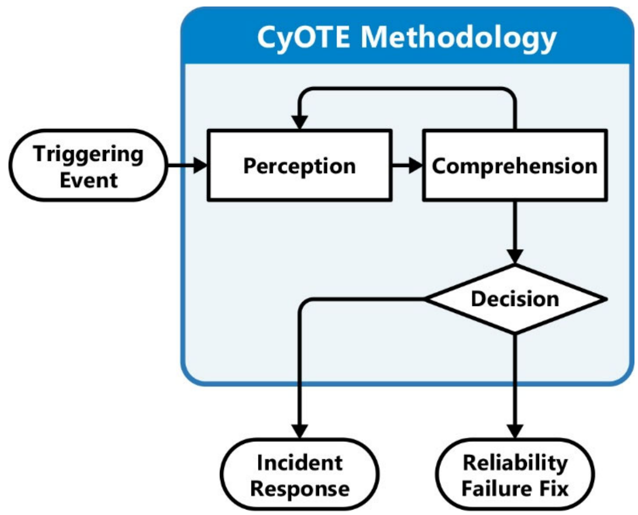

Figure 1. CyOTE Methodology

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

An adversary attempted and failed to cause a blackout in Ukraine using Industroyer2, a variant of the well-known ICS-capable malware Industroyer, on 8 April 2022 (D-0) during the early stages of Russia's invasion of Ukraine.[1] The adversary targeted specific high-voltage electrical substations operated by a regional Ukrainian energy provider and used disk wipers for Windows, Linux, and Solaris operating systems in tandem with Industroyer2 to hamper recovery efforts.[2] The Computer Emergency Response Team of Ukraine (CERT-UA) and Slovakian cybersecurity company ESET publicly reported the cyber attack on 12 April.[3,4]

A prompt and coordinated response by defenders at the targeted energy company, CERT-UA, and ESET, thwarted the attack. Had Industroyer2 been successful, it could have caused a blackout for more than two million people in Ukraine.[5]

A timeline of adversarial techniques is shown in Figure 2. 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.[a]

How the adversary gained initial access to the Ukrainian energy provider's enterprise network, conducted reconnaissance, and pivoted to the operations network is not known. In terms of tactics, the adversary would have also had to maintain persistence and escalate their privileges in the target environments to gain a foothold from which they could launch their attack. For the purposes of this report, CyOTE analysts used general terms and techniques to describe how the adversary gained initial access, performed reconnaissance, and moved laterally.

The adversary gained initial access to the Ukrainian energy provider's enterprise network by at least 17 February 2022 (D-51), likely via a device connected to the internet, such as a corporate workstation.[6] Between the date of initial access and 8 April 2022 (D-0), the adversary performed reconnaissance to gain a thorough understanding of the victim's networks. Details embedded in the Industroyer2 malware configurations demonstrate they collected information about eight targeted substations, including Internet Protocol (IP)

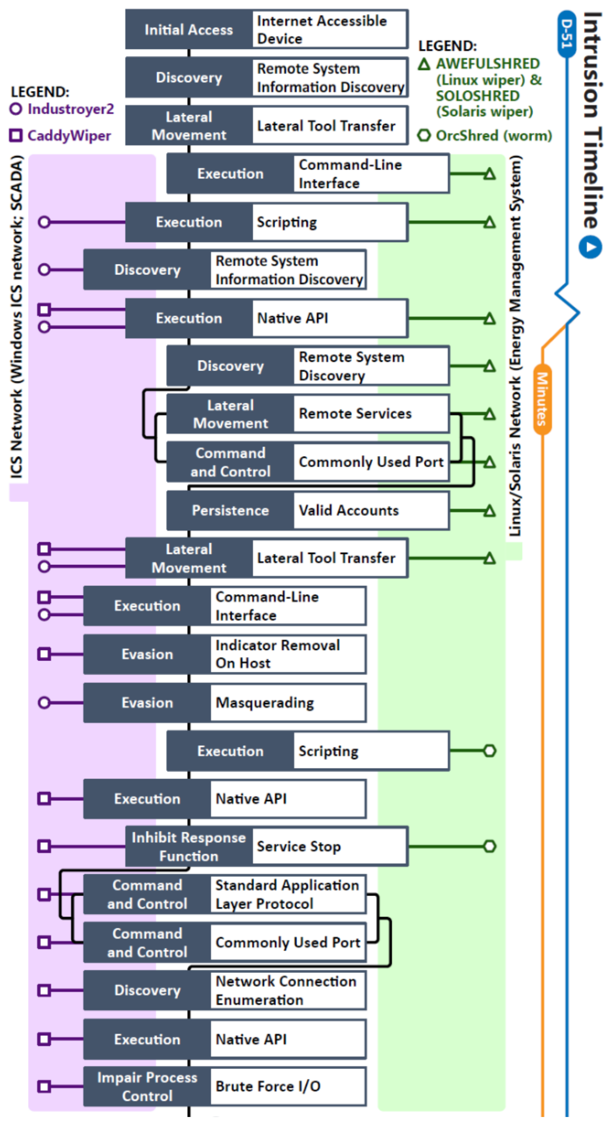

Figure 2. Intrusion Timeline

[a] "M" corresponds to minutes prior to (M-) or after (M+) the triggering event; "D" events correspond to days prior to or after; and "H" events correspond to hours prior to or after.

addresses and specific values used during communication via the International Electrotechnical Commission (IEC) 60870-5-104 (IEC-104) protocol.[7,8,b]

At some point between 17 February (D-51) and 8 April (D-0), the adversary gained access to the victim's operational technology (OT) network. In parallel with the deployment of Industroyer2 in the supervisory control and data acquisition (SCADA) segment of the operations network, the adversary deployed a new version of the CaddyWiper destructive malware on at least two Windows machines on 8 April at 3:58 PM local Ukraine time (M-72).[9] The adversary likely used CaddyWiper to slow down recovery efforts and prevent operators from regaining control of the affected ICS consoles. Had it executed as the adversary intended, it would have made the targeted systems inoperable and unrecoverable.[10]

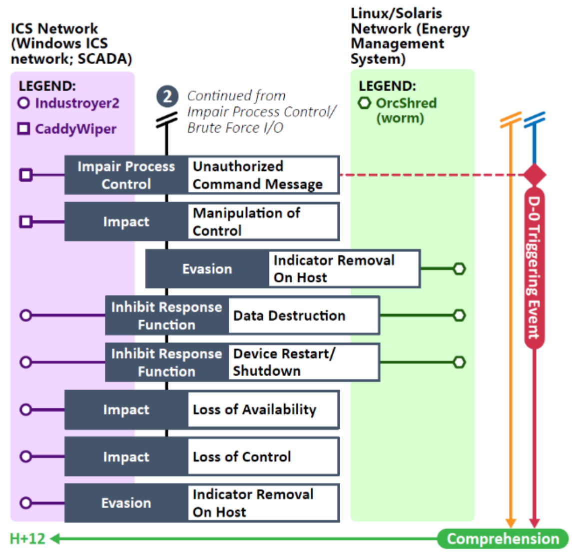

Figure 3. Intrusion Timeline (CONTD.)

At the same time (M-72), likely in the energy management system (EMS) segment of the operations network, the adversary deployed the OrcShred self-propagating malware to spread the SOLOSHRED and AWFULSHRED data wiping malware.[11] SOLOSHRED targeted server equipment with Solaris operating systems, while AWFULSHRED targeted similar equipment with Linux operating systems.[12]

On 8 April at 4:02 PM (M-68), the adversary created a scheduled task to launch Industroyer2 at 5:10 PM (D-0) on a control station. It is likely the victim comprehended they were under attack just before the malware sent unauthorized command messages to target systems, allowing the victim's responders to stop it. The adversary also scheduled CaddyWiper to execute on the same machine at 5:20 PM (M+10) to erase traces of Industroyer2.[13] Twelve hours after they comprehended and stopped the attack (H+12), responders reached their preliminary conclusions and developed indicators of compromise.[14]

Analysis of Industroyer2 indicates the adversary designed the malware to open circuit breakers, which would effectively cut power from the eight targeted substations.[15] Had the attack executed as the adversary intended, it could have left more than 2 million Ukrainians in the dark for an unknown amount of time during the early stages of Russia's invasion of Ukraine.

Analysis identified 22 unique techniques (used in a sequence of 31 steps) 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.

[b] IEC-104 is a SCADA protocol primarily used to monitor and control electricity transmission and distribution systems.

Table 1. Techniques Used in the Industroyer2 and Wiper Malware Targeting Ukrainian Energy Provider 2022

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	**Network Connection Enumeration**	Default Credentials	Automated Collection	**Commonly Used Port**	Activate Firmware Update Mode	**Brute Force I/O**	Damage to Property
Drive-by Compromise	**Command-Line Interface**	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		**Indicator Removal on Host**	**Remote System Discovery**	**Lateral Tool Transfer**	Detect Operating Mode	**Standard Application Layer Protocol**	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		**Masquerading**	**Remote System Information Discovery**	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	**Loss of Availability**
Exploitation of Remote Services	Hooking	**Valid Accounts**		Rootkit	Wireless Sniffing	**Remote Services**	Man in the Middle		Block Serial COM	**Unauthorized Command Message**	**Loss of Control**
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		**Data Destruction**		Loss of Productivity and Revenue
Internet Accessible Device	**Native API**						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	**Scripting**						Program Upload		**Device Restart/ Shutdown**		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		**Manipulation of Control**
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									**Service Stop**		Theft of Operational Information
Transient Cyber Asset									System Firmware		
Wireless Compromise											

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	**31**
Technique Observables	**297**
Precursor Techniques	**23**
Precursor Technique Observables	**224**
Highly Perceivable Precursor Technique Observable	**122**

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. INTERNET ACCESSIBLE DEVICE TECHNIQUE (T0883) FOR INITIAL ACCESS

As of this writing, how the adversary initially compromised the victim company's enterprise network is unknown.[16] For the purposes of this report, CyOTE analysts used a likely scenario in which the adversary gained initial access through an Internet accessible device, such as a corporate workstation. The initial compromise likely occurred on or before 17 February 2022.[17]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalies in compromised enterprise systems.

A total of two observables were identified with the use of the Internet Accessible Device technique (T0883). This technique is important for investigation because it is a common means by which an adversary can gain remote access to a victim's system. This technique appears at the beginning of the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent operational damage.

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 **(See Appendix B)**	A total of 23 artifacts could be generated by the Internet Accessible Device technique
Technique Observers[c]	IT Staff, IT Cybersecurity

[c] 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. REMOTE SYSTEM INFORMATION DISCOVERY TECHNIQUE (T0888) FOR DISCOVERY

Based on details embedded in the Industroyer2 malware configurations, the adversary conducted internal network reconnaissance of the victim's environments to identify specific devices and how to access them.[d] The adversary configured the Industroyer2 malware to target devices across specific subnets, indicating success in discovering and penetrating surrounding networks to gain a robust understanding of the victim environment.[18]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network activity indicating adversarial behavior.

A total of four observables were identified with the use of the Remote System Information Discovery technique (T0888). This technique is important for investigation because adversaries may use the information they gather to aid in targeting and shaping follow-on operational objectives. This technique appears at the beginning of the timeline and responding to it will inhibit the adversary's ability to scope subsequent technique usage. Terminating the chain of techniques at this point would prevent operational damage.

Of the four observables associated with this technique, none are assessed to be highly perceivable. Observables are listed in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 8 artifacts could be generated by the Remote System Information Discovery technique
Technique Observers	IT Staff, IT Cybersecurity

[d] At the time of writing, the means by which the adversary conducted reconnaissance is unknown.

3.3. LATERAL TOOL TRANSFER TECHNIQUE (T0867) FOR LATERAL MOVEMENT

The adversary transferred the Industroyer2, CaddyWiper, Linux, and Solaris malware to the OT network using unknown means to stage the malwares for future execution.[19] CyOTE analysts assess Industroyer2 and CaddyWiper were deployed in the SCADA segment of the victim's operations network and the Linux and Solaris wipers were deployed in the EMS network segment.

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe anomalous network traffic from the enterprise network to the operations network.

A total of 15 observables were identified with the use of the Lateral Tool Transfer technique (T0867). This technique is important for investigation because it is a means by which adversaries may transfer tools or other files from one system to another to stage for use over the course of an operation. This technique appears near the beginning of the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent operational damage.

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 **(See Appendix B)**	A total of 22 artifacts could be generated by the Lateral Tool Transfer technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

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

After moving laterally to the operations network, the adversary launched OrcShred to begin the spread of the Linux and Solaris wipers. The OrcShred worm contains a set of command-line arguments which query cron jobs[e] and the current OS release name and version of target hosts. Based on this, the worm determines if the host operating system is Solaris-based or running a variant of Linux. If the target host is Solaris- or Linux-based, OrcShred then runs another script to propagate the worm to additional hosts. After verifying that the propagation script has successfully executed, OrcShred will execute additional command-line instructions that remove log entries to hide evidence of worm propagation and execution.[20,21]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe command-line execution or utility usage.

A total of 15 observables were identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation because adversaries may use it to install and run malicious tools over the course of an operation. This technique appears early in the timeline and responding to it will effectively halt all future events associated with the Linux and Solaris wipers. Terminating the chain of techniques at this point would prevent operational damage associated with these wipers.

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 **(See Appendix B)**	A total of 25 artifacts could be generated by the Command-Line Interface technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

[e] Cron jobs are equivalent to scheduled tasks on UNIX-like operating systems.

3.5. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

The adversary used several scripts in both the SCADA and EMS network segments of the operations zone during the Industroyer2 attack. Prior to scheduling the execution of Industroyer2 and the accompanying data wipers, the adversary used the POWERGAP PowerShell script (link.ps1) to enumerate information about the centralized management and configuration of the targeted environments.[22] Additionally, the OrcShred worm is a UNIX Bash script with the file name sc.sh.[23]

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe the anomalous script and host activity on the domain controller.

A total of 22 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because adversaries may use scripting languages to execute arbitrary code in the target environment. This technique appears early in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent operational damage.

Of the 22 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 **(See Appendix B)**	A total of 12 artifacts could be generated by the Scripting technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity

3.6. REMOTE SYSTEM INFORMATION DISCOVERY TECHNIQUE (T0888) FOR DISCOVERY

The POWERGAP script discovers Group Policy Objects (GPO) using the Active Directory Service Interface (ADSI) in order to add a group policy and create a scheduled task on the targeted hosts.[24,25] The adversary implemented the centralized distribution and launch of CaddyWiper and likely Industroyer2 via this GPO.[26]

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe the anomalous script and host activity on the domain controller.

A total of five observables were identified with the use of the Remote System Information Discovery technique (T0888). This technique is important for investigation because the adversary may use it to aid in targeting and to tailor management actions such as lateral movement. This technique appears early in the timeline and responding to it will effectively halt all future events in the SCADA network segment. Terminating the chain of techniques at this point would prevent the spread of Industroyer2 and CaddyWiper.

Of the five 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 **(See Appendix B)**	A total of 8 artifacts could be generated by the Remote System Information Discovery technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity

3.7. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

The adversary leveraged Windows Application Program Interfaces (APIs) to create scheduled tasks via GPO to schedule the execution of CaddyWiper and Industroyer2 in the SCADA network segment of the operations network.[27] The adversary scheduled CaddyWiper to execute on one Windows machine on 8 April at 3:58 PM. At 4:02 PM, the adversary created the scheduled task that would have executed Industroyer2 on a control station with access to the eight targeted substations at 5:10 PM. The adversary scheduled a second instance of CaddyWiper on this control station to execute 10 minutes after Industroyer2 at 5:20 PM.[28]

In coordination with the deployment of Industroyer2 and CaddyWiper, the adversary leveraged UNIX APIs to create a cron job to schedule the execution of the SOLOSHRED and AWFULSHRED data wipers at 3:58 PM in the EMS network segment.[29]

To perform these actions, the adversary had to have access to the domain controller in the victim environment.

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous executables on hosts and anomalous network traffic.

A total of 15 observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because adversaries may attempt to leverage APIs for communication between control software and hardware. This technique appears early in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent the adversary from scheduling the execution of their malware, preventing operational damage.

Of the 15 observables associated with this technique, 11 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (**See Appendix B**)	A total of 25 artifacts could be generated by the Native API technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.8. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

OrcShred utilizes a scheduled cron job to propagate over the network from the system it is loaded on by looking at the results of ip route or ifconfig -a UNIX API calls. The worm always assumes a class C network (/24)[f] is reachable for each IP address it collects.[30]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous host and network activity.

A total of 13 observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation because adversaries may attempt to get a list of other systems by logical identifiers on a network that may be used for subsequent techniques. This technique appears early in the timeline and responding to it will effectively halt all future events in the EMS network segment. Terminating the chain of techniques at this point would prevent operational damage associated with the Linux and Solaris wipers.

Of the 13 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 (See Appendix B)	A total of 43 artifacts could be generated by the Remote System Discovery technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

[f] Class C network addresses are used in small private local area network (LAN) internet protocol (IP) ranges as opposed to public IP networks. Class C networks use a default subnet mask of 255.255.255.0 and have 192.X.X.X-223.X.X.X in their first octet. The /24 notation denotes the Classless Inter-Domain Routing (CIDR) Notation. This means that that the self-propagating component of the malware would only reach one network segment and the potential 254 available hosts in that segment.

3.9. REMOTE SERVICES TECHNIQUE (T0886) FOR LATERAL MOVEMENT

OrcShred then tries to connect to all hosts in the class C networks it discovered in the previous technique using the Secure Shell (SSH) protocol.[31]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous host and network activity.

A total of 13 observables were identified with the use of the Remote Services technique (T0886). This technique is important for investigation because adversaries may use it to move between assets and network segments. This technique appears early in the timeline and responding to it will effectively halt all future events in the EMS network segment. Terminating the chain of techniques at this point would prevent operational damage associated with the Linux and Solaris wipers.

Of the 13 observables associated with this technique, three are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 24 artifacts could be generated by the Remote Services technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.10. COMMONLY USED PORT TECHNIQUE (T0885) FOR COMMAND AND CONTROL

OrcShred attempts to connect to the hosts using SSH over TCP Ports 22, 2468, 24687, and 522.[32] TCP Port 22 is the default port for SSH. The other ports are non-standard ports for this protocol.

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous network traffic.

A total of 13 observables were identified with the use of the Commonly Used Port technique (T0885). This technique is important for investigation because adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend in with normal network activity. This technique appears early in the timeline and responding to it will effectively halt all future events in the EMS network segment. Terminating the chain of techniques at this point would prevent operational damage associated with the Linux and Solaris wipers.

Of the 13 observables associated with this technique, three are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 5 artifacts could be generated by the Commonly Used Port technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.11. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

Once OrcShred finds a reachable SSH server, it tries credentials from a list provided with the malicious script. The adversary likely collected credentials prior to the attack to enable the spread of the Linux and Solaris wipers.[33]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe anomalous network traffic and logon attempts.

A total of 12 observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because compromised credentials may be used to bypass access controls within the network and may be used for persistent access to remote systems. This technique appears early in the timeline and responding to it will effectively halt all future events in the EMS network segment. Terminating the chain of techniques at this point would prevent operational damage associated with the Linux and Solaris wipers.

Of the 12 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 **(See Appendix B)**	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.12. LATERAL TOOL TRANSFER TECHNIQUE (T0867) FOR LATERAL MOVEMENT

The SSH server copies AWFULSHRED to other internal Linux-based targets and SOLOSHRED to Solaris-based targets if the target servers are not already compromised by OrcShred.[34]

The addition of the scheduled task via GPO during the previous Native API technique (T0834) provides for the download of the CaddyWiper file wiping components from the domain controller to the targeted systems.[35] A scheduled task also propagates Industroyer2 from the domain controller to the target Windows host.[36] Once on the Windows host, Industroyer2 targeted eight specific substations.

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous network traffic from the domain controller and anomalous executable on the target hosts.

A total of 28 observables were identified with the use of the Lateral Tool Transfer technique (T0867). This technique is important for investigation because adversaries may transfer tools or other files from one system to another to move laterally into more sensitive systems. This technique appears early in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent the malware from being placed on systems where it could execute.

Of the 28 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 **(See Appendix B)**	A total of 22 artifacts could be generated by the Lateral Tool Transfer technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

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

The Industroyer2 executable supports two command-line flags, -t and -o. The adversary can use the -o flag to produce a log file or output its progress to the console window and the -t flag to perform a delayed execution.[37,38] It is unclear whether the adversary used these functions during the attack.

CaddyWiper depends on the ArguePatch (peremoga.exe) loader to decrypt itself.[39] This patched binary loads encrypted shellcode, TailJump (pa.pay), from a file and decrypts it with a key. ArguePatch and TailJump are both executed via command-line arguments.[40]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous executables and command line arguments on the compromised hosts.

A total of four observables were identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation because adversaries may use command-line interfaces to install and run malicious tools over the course of an operation. This technique appears near the middle of the timeline and responding to it could halt all future events associated with the Industroyer2 and CaddyWiper malware. Terminating the chain of techniques at this point would likely prevent the malware from executing.

All four 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 **(See Appendix B)**	A total of 25 artifacts could be generated by the Command-Line Interface technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.14. INDICATOR REMOVAL ON HOST TECHNIQUE (T0872) FOR EVASION

If the adversary uses the -o flag to produce a log file or output progress to the console window, Industroyer2 writes various error codes rather than meaningful text messages. This is likely an obfuscation attempt by the adversary to make analysis more difficult.[41]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the presence of the anomalous log file on the compromised host.

One observable was identified with the use of the Indicator Removal on Host technique (T0872). This technique is important for investigation because adversaries may try to remove indicators of their presence on a system in an effort to cover their tracks. This technique appears near the middle of the timeline and responding to it could halt all future events associated with the Industroyer2 malware. Terminating the chain of techniques at this point could prevent the malware from executing.

The observable associated with this technique is assessed to be highly perceivable. It is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 23 artifacts could be generated by the Indicator Removal on Host technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.15. MASQUERADING TECHNIQUE (T0849) FOR EVASION

CaddyWiper uses the ArguePatch loader, a patched version of a legitimate component of software company Hex-Rays Interactive Disassembler (IDA) Pro disassembly and debugger software, specifically the remote IDA debugger server win32_remote.exe. IDA Pro is primarily used for software reverse engineering and malware analysis and therefore is not likely to be present in an OT environment.[42] It is unclear why the adversary used a patched version of this software as the CaddyWiper loader. However, using this technique may reduce scrutiny by responders during or after an incident.

IT Cybersecurity, OT Cybersecurity, and Support Staff personnel may have been able to observe the presence of anomalous executable files in the operations network.

A total of four observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation because adversaries may use it to disguise a malicious application or executable as another file to avoid operator and engineer suspicion. This technique appears in the middle of the timeline and responding to it will effectively halt all future events associated with CaddyWiper. Terminating the chain of techniques at this point would prevent the spread of the wiper.

All four 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 **(See Appendix B)**	A total of 15 artifacts could be generated by the Masquerading technique
Technique Observers	IT Cybersecurity, OT Cybersecurity, Support Staff

3.16. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

After OrcShred copies AWFULSHRED (wobf.sh) to Linux-based targets and SOLOSHRED (wsol.sh) to Solaris-based targets using the Lateral Tool Transfer technique (T0867), the wipers begin scripted routines. Both wipers are Bash scripts intended to disable infrastructure elements such as server equipment.[43]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the execution of the anomalous scripts and host activity they created.

A total of 12 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because adversaries may use scripting languages to execute arbitrary code in the target environment. This technique appears in the middle of the timeline and responding to it will effectively halt all future events in the EMS network segment. Terminating the chain of techniques at this point would prevent operational damage associated with the Linux and Solaris wipers.

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 **(See Appendix B)**	A total of 12 artifacts could be generated by the Scripting technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.17. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

Before connecting to targeted devices at the eight transmission substations, Industroyer2 attempted to terminate two legitimate processes responsible for IEC-104 service communication between the control station and remote stations by using the native Windows API function TerminateProcess.[44] The malware then uses the native Windows API function MoveFileA to rename the original executables to prevent automatic restart of the legitimate processes.[45]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous execution of native Windows APIs.

A total of two observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because adversaries may directly interact with native OS APIs to access system functions. This technique appears in the middle of the timeline and responding to it will effectively halt all future events associated with the Industroyer2 malware. Terminating the chain of techniques at this point would prevent Industroyer2 from connecting to targeted substation devices.

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 **(See Appendix B)**	A total of 25 artifacts could be generated by the Native API technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.18. SERVICE STOP TECHNIQUE (T0881) FOR INHIBIT RESPONSE FUNCTION

Industroyer2 attempts to terminate two processes, PServiceControl.exe and PService_PDD.exe. It then renames the executables by appending the .MZ file extension to prevent them from relaunching.[46] As mentioned in the previous technique, these processes provide the service that allows for IEC-104 communication with transmission substations.[47] Terminating the PService_PDD.exe service interrupts any existing communication with IEC-104 servers, which usually support only one active connection at a time. Once existing connections are interrupted, Industroyer2 can connect to its targets.[48]

The Linux and Solaris wipers also utilize the Service Stop technique (T0881) during their scripted routines. Depending on the size of the full disk, it may take hours to be completely erased. To render the system inoperable faster, AWFULSHRED first tries to disable HTTP and SSH services. The wiper disables these services using systemctl. To ensure services are not reenabled, the malware deletes the system unit file responsible for loading the service.[49]

Similar to the Linux variant, SOLOSHRED searches through all services to stop and disable them if they contain the keyword ssh, http, apache, ora_, or oracle because these services are commonly used by applications used in control systems. Wiping them would prevent the victim's operators from retaking control of the substations and rolling back Industroyer2's impacts. SOLOSHRED uses either systemctl or svcadm to stop the services, depending on what is available.[50]

IT Cybersecurity, OT Cybersecurity, and OT Staff personnel may have been able to observe the anomalous stoppage of services.

A total of 26 observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation because stopping critical services can inhibit response to an incident or aid in the adversary's overall objectives to cause damage to an environment. This technique appears near the middle of the timeline and responding to it will halt all future events associated with the Industroyer2 malware and the Linux and Solaris wipers. Terminating the chain of techniques at this point would prevent the malware from connecting to targeted substation devices and the wipers from impacting the EMS network.

Of the 26 observables associated with this technique, 24 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 13 artifacts could be generated by the Service Stop technique
Technique Observers	IT Cybersecurity, OT Cybersecurity, OT Staff

3.19. STANDARD APPLICATION LAYER PROTOCOL TECHNIQUE (T0869) FOR COMMAND AND CONTROL

After terminating and renaming PServiceControl.exe and PService_PPD.exe, Industroyer2 begins connecting to target substations over IEC-104.[51] For each hardcoded substation address and embedded configuration entry, Industroyer2 creates a network thread that implements IEC-104 communication with the targeted controlled systems.[52] IEC-104 uses the Application Protocol Data Unit (APDU) transmission specification which can be composed of either an Application Protocol Control Information (APCI) frame or an APCI header and a subsequent Application Service Data Unit (ASDU) frame.[53] This message structure carries application data sent between stations. The ASDU transmits an Information Object Address (IOA), which is used to interact with switches and breakers in a station. During normal operations, a controller can send an APDU frame with an ASDU that contains specific IOA commands to change the state of stations and substations.[54]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe anomalous network traffic from the controlling station to the controlled station.

A total of two observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation because adversaries may use standard protocols to disguise their actions as benign network traffic or to interact with devices within the compromised network. This technique appears in the latter half of the timeline and responding to it will effectively halt all future events associated with the Industroyer2 malware. Terminating the chain of techniques at this point would prevent the malware from communicating with its targets.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 12 artifacts could be generated by the Standard Application Layer technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.20. COMMONLY USED PORT TECHNIQUE (T0885) FOR COMMAND AND CONTROL

Industroyer2 used the Commonly Used Port technique (T0885) in tandem with the Standard Application Layer Protocol technique (T0869) to communicate with the eight hardcoded RTU IP addresses using IEC-104 over Transmission Control Protocol (TCP) Port 2404. Port 2404 is the standard port used by the IEC-104 protocol.[55]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous network traffic from the controlling station to the controlled stations.

A total of two observables were identified with the use of the Commonly Used Port technique (T0885). This technique is important for investigation because adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend in with normal network activity. This technique appears in the latter half of the timeline and responding to it will effectively halt all future events associated with the Industroyer2 malware. Terminating the chain of techniques at this point would prevent the malware from communicating with its targets.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 5 artifacts could be generated by the Commonly Used Port technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.21. NETWORK CONNECTION ENUMERATION TECHNIQUE (T0840) FOR DISCOVERY

With IEC-104 network connections enabled, Industroyer2 sends control function messages contained within an APCI frame. The malware first sends a Test Frame (TESTFR ACT) to the targeted RTUs to verify an established connection. If one exists, the RTU responds with a corresponding TESTFR CON to confirm the connection.[56] During normal operations, IEC-104 uses TESTFR frames between controlling stations and controlled stations to periodically check the status of a connection and detect communication problems.[57]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous network traffic between the RTUs and infected controlling station.

A total of three observables were identified with the use of the Network Connection Enumeration technique (T0840). This technique is important for investigation because adversaries may use it to discover information about device communication patterns and to inspect the state of network connections. This technique appears in the latter half of the timeline and responding to it will effectively halt all future events associated with the Industroyer2 malware. Terminating the chain of techniques at this point would prevent the malware from sending malicious commands to the targeted RTUs.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 33 artifacts could be generated by the Network Connection Enumeration technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.22. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

After a targeted RTU confirms an active connection, Industroyer2 opens a data transfer channel with the remote station using a native control message type of Start Data Transfer (STARTDT). Data transfer is not enabled on an active connection between a control station and remote station by default. The malware therefore sends a STARTDT ACT message to activate a data transfer channel and the RTU responds with a STARTDT CON to confirm a successful activation.[58]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous network traffic between the RTUs and infected controlling station.

A total of five observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because adversaries may directly interact with native OS APIs to access system functions. This technique appears in the latter half of the timeline and responding to it will effectively halt all future events associated with the Industroyer2 malware. Terminating the chain of techniques at this point would prevent the malware from sending malicious data to targeted substations.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 25 artifacts could be generated by the Native API technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

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

In addition to hardcoded station addresses, Industroyer2 contained IOA configurations embedded in the binary. Industroyer2 manipulates a selected list of IOAs, which control outputs for power line switches or circuit breakers in a RTU or relay configuration.[59,60] For each targeted RTU in a configuration entry, the malware iterates through corresponding ASDU data entries, crafts specified telegrams (ASDU messages), and sends them to the RTU to change the state of specific IOAs to ON or OFF.[61] The fact that the malware changed specific outputs, rather than randomly turning outputs ON or OFF, indicates the adversary had technical knowledge of the specific substations being targeted.[62]

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe anomalous network traffic from the controlling station to the controlled stations.

A total of six observables were identified with the use of the Brute Force I/O technique (T0806). This technique is important for investigation because adversaries may change I/O point values to manipulate a process function. This technique appears in the latter half of the timeline and responding to it will effectively halt all future events associated with the Industroyer2 malware. Terminating the chain of techniques at this point would prevent the malware from sending unauthorized commands to targeted devices.

All six of the 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 (See Appendix B)	A total of 19 artifacts could be generated by the Brute Force I/O technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.24. UNAUTHORIZED COMMAND MESSAGE TECHNIQUE (T0855) FOR IMPAIR PROCESS CONTROL

Activation of data transfer during the Native API technique (T0834) enables Industroyer2 to directly interact with electrical utility equipment and send commands to substation devices that control the flow of power.[63] As mentioned in the previous technique, the malware utilizes an ASDU frame to send commands to the remote station. ASDU messages are a set of application functions defined by IEC-104 to monitor and control remote stations.[64] Industroyer2 first sends an interrogation command (C_IC_NA_1). It then sends Single Command (C_SC_NA_1) or Double Command (C_DC_NA_1) activation messages, depending on each IOA's configuration.[65] These are the commands that modify the target's IOA to either ON or OFF.

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe anomalous network traffic from the controlling station to the controlled stations**.**

A total of six observables were identified with the use of the Unauthorized Command Message technique (T0855). This technique is important for investigation because adversaries may send unauthorized command messages to instruct control system assets to perform actions outside their intended functionality.

At this point, the victim successfully detected the Industroyer2 attack while it was in progress and stopped it before the adversary could trigger an effect. However, due to a lack of publicly available information, it is unknown at which point in the attack timeline detection occurred. For the purposes of this report, CyOTE analysts assumed that the victim comprehended they were under attack at this point in the timeline, which represents the triggering event for this attack. Responding to it prevented Industroyer2 from sending unauthorized command messages that would have cut power from the eight targeted substations.

All six of the 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 (See Appendix B)	A total of 16 artifacts could be generated by the Unauthorized Command Message technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.25. MANIPULATION OF CONTROL TECHNIQUE (T0831) FOR IMPACT

Industroyer2 manipulates the state of targeted RTUs by sending the command messages described in the previous technique. Based on the command types, the targeted IOAs likely control circuit breakers, which operators use to disconnect power from an electric utility substation. The adversary designed the malware to open circuit breakers, which would have cut power from the eight targeted substations.[66] Had Industroyer2 executed as intended, it could have caused a blackout for more than two million people in Ukraine.[67]

IT Cybersecurity and OT Staff personnel may have been able to observe the anomalous network traffic from the controlling station to controlled stations. OT Staff and Engineering personnel may have been able to observe the open circuit breakers. These personnel, along with IT Staff, Support Staff, and Management personnel would have been able to observe the blackout that would have been caused by power being disconnected from the eight targeted substations.

A total of seven observables were identified with the use of the Manipulation of Control technique (T0831). This technique is important for investigation because adversaries may manipulate process control within the industrial environment to cause physical impacts. This technique would have appeared near the end of the timeline. However, defenders were able to successfully detect and stop the attack before the circuit breakers in the targeted substations could be opened.

All seven 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 (See Appendix B)	A total of 16 artifacts could be generated by the Manipulation of Control technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management

3.26. INDICATOR REMOVAL ON HOST TECHNIQUE (T0872) FOR EVASION

The adversary likely timed the destructive actions of the Solaris and Linux wipers in the EMS network to occur around the same time as the Industroyer2 malware's impact would have occurred.

AWFULSHRED and SOLOSHRED remove files from /boot, /home, and /var/log before destroying the full drives. This makes the system inoperable faster, deletes user data, and likely removes incriminating logs.[68]

The victim successfully detected the attack while it was in progress and stopped it before the wipers could begin destroying data. As mentioned in the Unauthorized Command Message technique (T0855) section, it is unknown at which point in the attack timeline this occurred. For the purposes of this report, it is assumed the victim detected the Linux and Solaris wipers in the EMS network at this point in the timeline and prevented the malware from wiping data on the targeted systems.

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the anomalous deletion of data on hosts.

A total of 13 observables were identified with the use of the Indicator Removal on Host technique (T0872). This technique is important for investigation because adversaries may try to remove indicators of their presence on a system in an effort to cover their tracks. This technique would have appeared near the end of the timeline. However, defenders stopped the attack in progress and prevented the adversary from achieving their intended impact.

Of the 13 observables associated with this technique, 11 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 23 artifacts could be generated by the Indicator Removal on Host technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.27. DATA DESTRUCTION TECHNIQUE (T0809) FOR INHIBIT RESPONSE FUNCTION

The adversary attempted to use CaddyWiper to destroy as much data on the targeted devices as quickly as possible. Once TailJump decrypts into CaddyWiper, the malware calls the Windows API DeviceIoControl and a zeroed InputBuffer for all physical disks from \.\\PHYSICALDRIVE0 to \.\\PHYSICALDRIVE9. This erases the Master Boot Record and GUID partition table.[69] It also wipes all contents in C:\Users and all attached disks from D:\ to Z:\. CaddyWiper accomplishes this by zero-filling all affected destinations.[70] The adversary intended for CaddyWiper to launch on one unspecified Windows machine at 3:58 PM and at 5:20 PM on the machine where Industroyer2 was deployed.[71]

If the targeted Linux and Solaris systems were set to local time, the adversary would schedule the AWFULSHRED and SOLOSHRED wipers to execute at the same time as the first scheduled instance of CaddyWiper to destroy all data. Ultimately, the Linux wiper could destroy all contents of the disks attached to the system by using the shred or dd if=/dev/random commands. If multiple disks are attached, the malware removes data in parallel to speed up the process.[72]

The Solaris wiper begins file destruction by deleting databases. Using the shred and rm commands, it removes all files and directories contained in environment variables starting with “ORA”. Shred ensures data recovery, without a backup, is not possible. The script then iterates over disks connected to the system found in /dev/dsk, ignoring partitions and working only on full disks. For each of them, SOLOSHRED overwrites the full contents using shred. As with the Linux variant, the wiper minimizes the time required to perform the wipe by erasing all disks in parallel. Lastly, SOLOSHRED self-destructs.[73]

IT Staff, IT Cybersecurity, OT Cybersecurity, and OT Staff personnel may have been able to observe the destruction of data on targeted hosts. However, in this case the defenders were able to catch the wiper malware before it could fully execute and cause its intended impact.[74]

A total of 18 observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because adversaries may use it to disrupt response functions from occurring as expected or to destroy data backups that are vital to recovery after an incident. This technique would have appeared near the end of the timeline. However, defenders stopped the attack in progress and prevented the adversary from achieving their intended impact.

Of the 18 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 **(See Appendix B)**	A total of 27 artifacts could be generated by the Data Destruction technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity, OT Staff

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

If CaddyWiper executed as intended and wiped the disks on targeted devices, the affected systems would have inevitably crashed and been unable to reboot.[75]

AWFULSHRED's last action, had it executed as intended, would have been to force a reboot using the Linux kernel-level command *SysRq*. The operating system would not boot once the malware overloaded the host drives with random data.[76]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel would have been able to observe the anomalous shutdown of hosts and associated blue screen error on Windows devices.

A total of five observables were identified with the use of the Device Restart/Shutdown technique (T0816). This technique is important for investigation because unexpected restart or shutdown of control system devices may prevent operators from performing required response functions, potentially negatively impacting physical processes. This technique would have appeared near the end of the timeline. However, defenders stopped the attack in progress and prevented the adversary from destroying critical systems.

All five 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 **(See Appendix B)**	A total of 17 artifacts could be generated by the Device Restart/Shutdown technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management

3.29. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

The main purpose of CaddyWiper is to erase user data and partition information from attached disks, making the system inoperable and unrecoverable. Similarly, the Solaris and Linux wipers would have disabled several infrastructure elements, including server equipment.[77] Had the adversary been successful, the targeted systems would no longer have been available to the operators.

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel would have been able to observe the loss of availability of the targeted systems.

A total of eight observables were identified with the use of the Loss of Availability technique (T0826). This technique is important for investigation because adversaries may use malware to delete data on critical systems, disrupting essential processes for recovery. This technique would have appeared near the end of the timeline. However, defenders stopped the attack in progress and prevented the adversary from achieving their intended impact.

Of the eight 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 **(See Appendix B)**	A total of 8 artifacts could be generated by the Loss of Availability technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management

3.30. LOSS OF CONTROL TECHNIQUE (T0827) FOR IMPACT

The adversary likely deployed CaddyWiper to slow the victim's recovery process and prevent operators at the energy company from regaining control of the Windows consoles the malware targeted in the SCADA segment of the operations network.[78]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel would have been able to observe the loss of control of devices targeted by CaddyWiper.

A total of eight observables were identified with the use of the Loss of Control technique (T0827). This technique is important for investigation because adversaries may seek to achieve a sustained loss of control or runaway condition in which operators cannot issue any commands. This technique would have appeared near the end of the timeline. However, defenders stopped the attack in progress and prevented the adversary from achieving their intended impact.

Of the eight 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 **(See Appendix B)**	A total of 13 artifacts could be generated by the Loss of Control technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management

3.31. INDICATOR REMOVAL ON HOST TECHNIQUE (T0872) FOR EVASION

The adversary scheduled CaddyWiper to execute at 5:20 PM, 10 minutes after Industroyer2, on the same machine, likely to avoid discovery in a post-event analysis.[79]

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe the destruction of data on the targeted host.

A total of eight observables were identified with the use of the Indicator Removal on Host technique (T0872). This technique is important for investigation because adversaries may attempt to remove indicators of their presence on a system in an effort to cover their tracks. This technique would have appeared at the end of the timeline. However, defenders stopped the attack in progress and prevented the adversary from achieving their intended impact.

Of the eight 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 (See Appendix B)	A total of 23 artifacts could be generated by the Indicator Removal on Host technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity

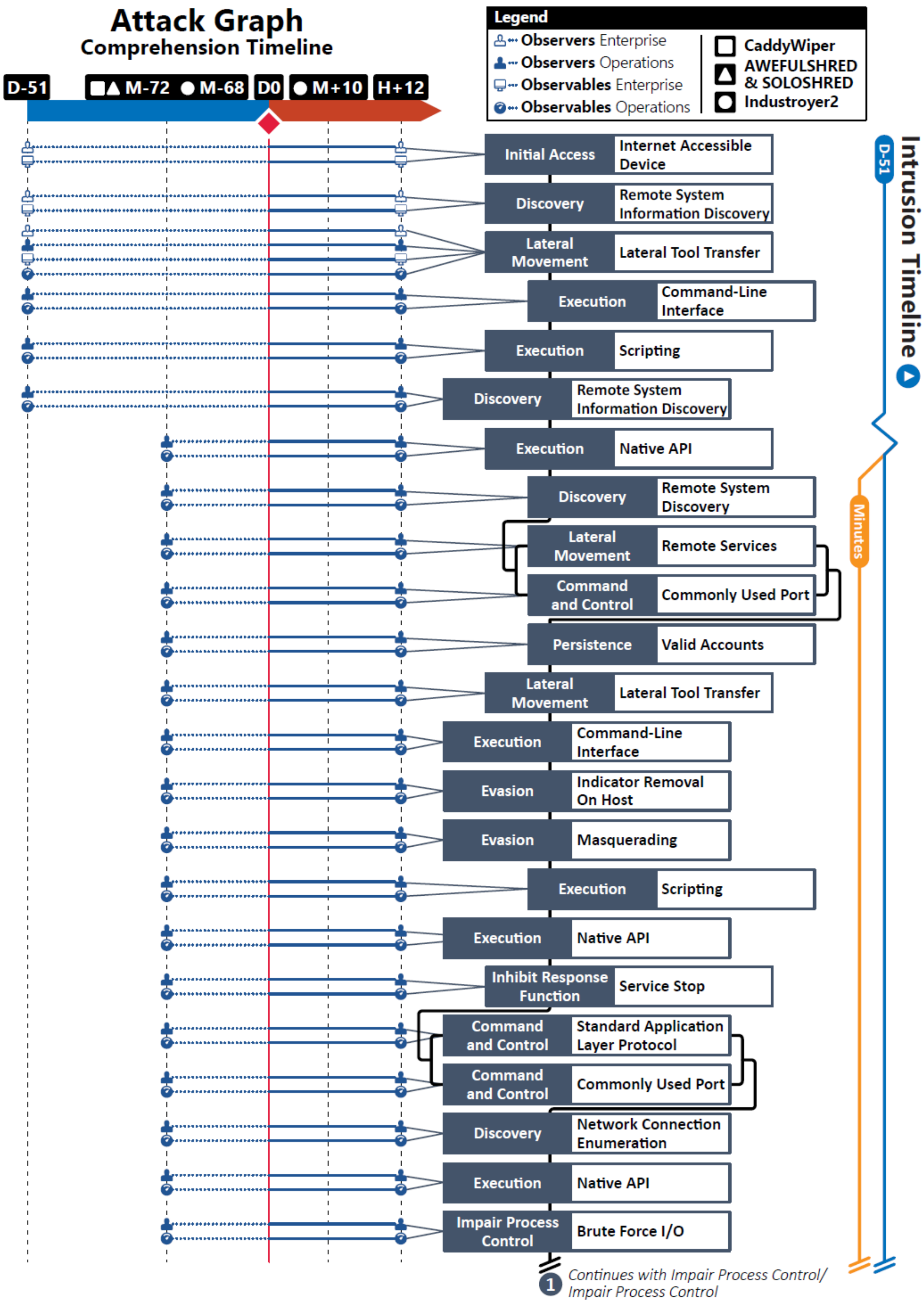

Figure 4. Attack Graph

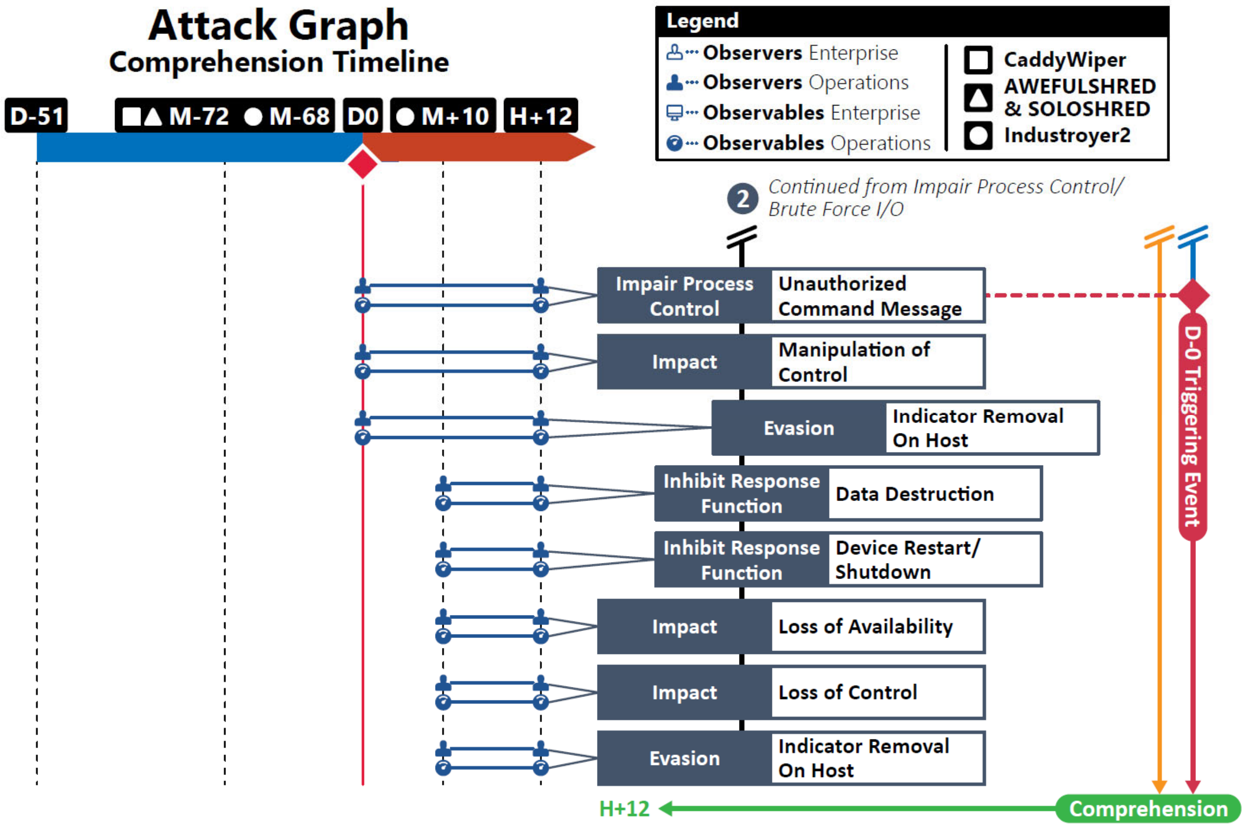

Figure 5. Attack Graph (CONTD.)

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †

Observables Associated with Internet Accessible Device Technique (T0883)	
Observable 1 †	*Anomalous Network Traffic: From External Remote Host to Local Host*
Observable 2	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Network Bandwidth Utilization

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 1	Anomalous Network Traffic: From External Remote Host to Local Host: Over Transmission Control Protocol (TCP) Ports 1-1024
Observable 2	Anomalous Network Traffic: From External Remote Host to Local Host: Over Transmission Control Protocol (TCP) Ports 2404-2406
Observable 3	Anomalous Network Traffic: From Local Host to External Remote Host: Over Transmission Control Protocol (TCP) Ports 1-1024
Observable 4	Anomalous Network Traffic: From Local Host to External Remote Host: Over Transmission Control Protocol (TCP) Ports 2404-2406

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22*
Observable 2 †	*Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468*
Observable 3 †	*Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687*
Observable 4 †	*Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522*
Observable 5 †	*Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22*
Observable 6 †	*Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468*
Observable 7 †	*Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687*
Observable 8 †	*Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522*
Observable 9	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Lightweight Directory Access Protocol (LDAP) TCP Port 389
Observable 10	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Remote Procedure Call (RPC) TCP Port 135

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 11	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Server Message Block (SMB) TCP Port 445
Observable 12	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Server Message Block (SMB) TCP Port 445: Distributed over Distributed File System (DFS)
Observable 13	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Network Bandwidth Utilization
Observable 14 †	*Presence of Anomalous Executable on Host: Windows Workstations in Operations Environment*
Observable 15 †	*Presence of Anomalous Script on Host: UNIX Bash Script*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 1 †	*Presence of Anomalous Script on Host: UNIX Bash Script: sc.sh: with MD5 Hash fbe32784c073e341fc57d175a913905c*
Observable 2 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): Crontab*
Observable 3	Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): Find
Observable 4	Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): Cat
Observable 5 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): rm*
Observable 6 †	*Anomalous Command Line: "crontab -l /var/log/tasks"*
Observable 7	Anomalous Command Line: "find /etc -name os-release > /var/log/res"
Observable 8	Anomalous Command Line: "cat /var/log/res"
Observable 9	Anomalous Command Line: "cat /etc/os-release | grep ID=solaris; echo $? > /var/log/res"
Observable 10 †	*Anomalous Command Line: "echo "58 17 /bin/bash /var/log/wsol.sh & disown" >> /var/log/tasks"*
Observable 11 †	*Anomalous Command Line: "echo "58 17 *** /bin/bash /var/log/wobf.sh & disown" >> /var/log/tasks"*
Observable 12 †	*Anomalous Command Line: "58 17 * * /bin/bash /var/log/wobf.sh & disown" >> /var/log/tasks"*
Observable 13 †	*Anomalous Command Line: "crontab /var/log/tasks"*
Observable 14 †	*Anomalous Command Line: "rm -f /var/log/tasks"*
Observable 15 †	*Anomalous Command Line: "rm -f /var/log/res"*

Observables Associated with Scripting Technique (T0853)	
Observable 1 †	*Presence of Anomalous Script on Host: UNIX Bash Script: sc.sh: with MD5 Hash fbe32784c073e341fc57d175a913905c*
Observable 2 †	*Presence of Anomalous Script on Host: Domain Controller: PowerShell Script: C:\Windows\Temp\link.ps1: With SHA-1 Hash 0090CB4DE31D2D3BCA55FD4A36859921B5FC5DAE*
Observable 3 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): Crontab*
Observable 4	Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): Find
Observable 5	Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): Cat
Observable 6 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): rm*
Observable 7	Anomalous Host Activity: Interrogation of Domain Group Policy Objects (GPOs)
Observable 8	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Central Processing Unit (CPU) Utilization
Observable 9 †	*Presence of Anomalous Executable on Host: Windows workstations in Operations Environment: peremoga.exe*
Observable 10 †	*Anomalous Command Line: "crontab -l /var/log/tasks"*
Observable 11	Anomalous Command Line: "find /etc -name os-release > /var/log/res"
Observable 12	Anomalous Command Line: "cat /var/log/res"
Observable 13	Anomalous Command Line: "cat /etc/os-release | grep ID=solaris; echo $? > /var/log/res"
Observable 14 †	*Anomalous Command Line: "echo "58 17 /bin/bash /var/log/wsol.sh & disown" >> /var/log/tasks"*
Observable 15 †	*Anomalous Command Line: "echo "58 17 *** /bin/bash /var/log/wobf.sh & disown" >> /var/log/tasks"*
Observable 16 †	*Anomalous Command Line: "58 17 * * /bin/bash /var/log/wobf.sh & disown" >> /var/log/tasks"*
Observable 17 †	*Anomalous Command Line: "crontab /var/log/tasks"*
Observable 18 †	*Anomalous Command Line: "rm -f /var/log/tasks"*
Observable 19 †	*Anomalous Command Line: "rm -f /var/log/res"*
Observable 20	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Lightweight Directory Access Protocol (LDAP) TCP Port 389
Observable 21	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Remote Procedure Call (RPC) TCP Port 135
Observable 22	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Server Message Block (SMB) TCP Port 445

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 1 †	*Presence of Anomalous Script on Host: Domain Controller: PowerShell Script: C:\Windows\Temp\link.ps1: With SHA-1 Hash 0090CB4DE31D2D3BCA55FD4A36859921B5FC5DAE*
Observable 2	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Lightweight Directory Access Protocol (LDAP) TCP Port 389
Observable 3	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Remote Procedure Call (RPC) TCP Port 135
Observable 4	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Server Message Block (SMB) TCP Port 445
Observable 5	Anomalous Host Activity: Interrogation of Domain Group Policy Objects (GPOs)

Observables Associated with Native API Technique (T0834)	
Observable 1 †	*Presence of Anomalous Executable on Host: Engineering Workstation Running Windows: 108_100.exe*
Observable 2 †	*Presence of Anomalous Executable on Host: Engineering Workstation Running Windows: zrada.exe*
Observable 3 †	*A Scheduled Task Was Created (Windows Event ID 4698): Creation of Anomalous Scheduled Task on Host: Engineering Workstation Running Windows*
Observable 4 †	*Presence of Anomalous Script on Host: Domain Controller: PowerShell Script: C:\Windows\Temp\link.ps1: With SHA-1 Hash 0090CB4DE31D2D3BCA55FD4A36859921B5FC5DAE*
Observable 5	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Lightweight Directory Access Protocol (LDAP) TCP Port 389
Observable 6	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Remote Procedure Call (RPC) TCP Port 135
Observable 7 †	*Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Server Message Block (SMB) TCP Port 445: Distributed over Distributed File System (DFS): Containing Executable: 108_100.exe*
Observable 8 †	*Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Server Message Block (SMB) TCP Port 445: Distributed over Distributed File System (DFS): Containing Executable: zrada.exe*
Observable 9 †	*Execution of Anomalous Executable on Host: Engineering Workstation Running Windows: 108_100.exe*
Observable 10 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): Crontab*
Observable 11	Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): Find
Observable 12	Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): Cat

Observables Associated with Native API Technique (T0834)	
Observable 13 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): rm*
Observable 14 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): iproute*
Observable 15 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): ipconfig*

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1 †	*Presence of Anomalous Script on Host: UNIX Bash Script: sc.sh: with MD5 Hash fbe32784c073e341fc57d175a913905c*
Observable 2 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wsol.sh: With MD-5 hash 97ad7f3ed815c0528b070941be903d07*
Observable 3 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wobf.sh: with MD-5 hash 73561d9a331c1d8a334ec48dfd94db99*
Observable 4 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): iproute*
Observable 5 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): ipconfig*
Observable 6	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22
Observable 7	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468
Observable 8	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687
Observable 9	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522
Observable 10	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22
Observable 11	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468
Observable 12	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687
Observable 13	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522

Observables Associated with Remote Services Technique (T0886)	
Observable 1 †	*Presence of Anomalous Script on Host: UNIX Bash Script: sc.sh: with MD5 Hash fbe32784c073e341fc57d175a913905c*

Observables Associated with Remote Services Technique (T0886)	
Observable 2 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wsol.sh: With MD-5 Hash 97ad7f3ed815c0528b070941be903d07*
Observable 3 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wobf.sh: with MD-5 Hash 73561d9a331c1d8a334ec48dfd94db99*
Observable 4	Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): iproute
Observable 5	Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): ipconfig
Observable 6	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22
Observable 7	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468
Observable 8	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687
Observable 9	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522
Observable 10	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22
Observable 11	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468
Observable 12	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687
Observable 13	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 1 †	*Presence of Anomalous Script on Host: UNIX Bash Script: sc.sh: with MD5 Hash fbe32784c073e341fc57d175a913905c*
Observable 2 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wsol.sh: With MD-5 Hash 97ad7f3ed815c0528b070941be903d07*
Observable 3 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wobf.sh: with MD-5 Hash 73561d9a331c1d8a334ec48dfd94db99*
Observable 4	Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): iproute
Observable 5	Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): ipconfig
Observable 6	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22
Observable 7	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 8	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687
Observable 9	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522
Observable 10	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22
Observable 11	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468
Observable 12	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687
Observable 13	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22
Observable 2	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468
Observable 3	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687
Observable 4	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522
Observable 5	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22
Observable 6	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468
Observable 7	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687
Observable 8	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522
Observable 9 †	*Anomalous Host Activity: Successful Logon from External Host: Anomalous Timestamp*
Observable 10 †	*Anomalous Host Activity: Successful Logon from External Host: Anomalous Remote IP Address*
Observable 11 †	*Anomalous Host Activity: Increase in Failed Login Attempts: Anomalous Timestamp*
Observable 12 †	*Anomalous Host Activity: Increase in Failed Login Attempts: Anomalous Remote IP Address*

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 1	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Lightweight Directory Access Protocol (LDAP) TCP Port 389
Observable 2	Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Remote Procedure Call (RPC) TCP Port 135
Observable 3 †	*Anomalous Network Traffic: From Domain Controller to Windows Host on Domain: Over Server Message Block (SMB) TCP Port 445: Distributed over Distributed File System (DFS): Containing Executable: 108_100.exe*
Observable 4	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22
Observable 5	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468
Observable 6	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687
Observable 7	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522
Observable 8	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C network (/24): Over Secure Copy Protocol (SCP) TCP Port 22
Observable 9	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C network (/24): Over Secure Copy Protocol (SCP) TCP Port 2468
Observable 10	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C network (/24): Over Secure Copy Protocol (SCP) TCP Port 24687
Observable 11	Anomalous Network Traffic: From Local Host to Linux Hosts: Over Class-C network (/24): Over Secure Copy Protocol (SCP) TCP Port 522
Observable 12	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 22
Observable 13	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 2468
Observable 14	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 24687
Observable 15	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Shell (SSH) TCP Port 522
Observable 16	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Copy Protocol (SCP) TCP Port 22
Observable 17	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Copy Protocol (SCP) TCP Port 2468
Observable 18	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Copy Protocol (SCP) TCP Port 24687
Observable 19	Anomalous Network Traffic: From Local Host to Solaris Hosts: Over Class-C Network (/24): Over Secure Copy Protocol (SCP) TCP Port 522

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 20 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): scp*
Observable 21 †	*Presence of Anomalous Script on Host: UNIX Bash Script: sc.sh*
Observable 22 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wsol.sh*
Observable 23 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wobf.sh*
Observable 24 †	*Presence of Anomalous Executable on Host: Engineering Workstation Running Windows: 108_100.exe*
Observable 25 †	*Presence of Anomalous Executable on Host: Windows Workstations in Operations Environment: zrada.exe*
Observable 26 †	*Presence of Anomalous Executable on Host: Windows Workstations in Operations Environment: peremoga.exe*
Observable 27 †	*Presence of Anomalous Executable on Host: Windows Workstations in Operations Environment: vatt.exe*
Observable 28 †	*Presence of Anomalous Script on Host: Windows Workstations in Operations Environment: PowerShell Script: C:\Windows\Temp\link.ps1: With SHA-1 Hash 0090CB4DE31D2D3BCA55FD4A36859921B5FC5DAE*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 1 †	*Presence of Anomalous Executable on Host: Engineering Workstation Running Windows: 108_100.exe: Command-Line Contents cmd /c C:\Dell\108_100.exe -o "C:\dell\108 100.log"*
Observable 2 †	*Presence of Anomalous Executable on Host: Windows Workstations in Operations Environment: peremoga.exe: With MD-5 hash 9EC8468DD4A81B0B35C499B31E67375E*
Observable 3 †	*Presence of Anomalous File on Host: Engineering Workstation Running Windows: C:\dell\108 100.log*
Observable 4 †	*Anomalous Command Line: C:\Users\user\Desktop\peremoga.exe*

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 1 †	*Presence of Anomalous File on Host: Engineering Workstation Running Windows: C:\dell\108 100.log*

Observables Associated with Masquerading Technique (T0849)	
Observable 1 †	*Presence of Anomalous Executable on Host: Windows Workstations in Operations Environment: zrada.exe*
Observable 2 †	*Presence of Anomalous Executable on Host: Windows Workstations in Operations Environment: peremoga.exe*

Observables Associated with Masquerading Technique (T0849)	
Observable 3 †	*Presence of Anomalous Executable on Host: Windows Workstations in Operations Environment: vatt.exe*
Observable 4 †	*Presence of Anomalous Executable on Host: Windows Workstations in Operations Environment: win32_remote.exe*

Observables Associated with Scripting Technique (T0853)	
Observable 1 †	*Presence of Anomalous Script on Host: UNIX Bash Script: sc.sh*
Observable 2 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wsol.sh*
Observable 3 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wobf.sh*
Observable 4 †	*Execution of Anomalous Script on Host: UNIX Bash Script: sc.sh*
Observable 5 †	*Execution of Anomalous Script on Host: UNIX Bash Script: /var/log/wsol.sh*
Observable 6 †	*Execution of Anomalous Script on Host: UNIX Bash Script: /var/log/wobf.sh*
Observable 7	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Central Processing Unit (CPU) Utilization
Observable 8	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity
Observable 9 †	*Anomalous Host Activity: Anomalous Enumeration of Local Disks*
Observable 10 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Random Bytes: On Local Disk*
Observable 11 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): shred*
Observable 12 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): dd*

Observables Associated with Native API Technique (T0834)	
Observable 1 †	*Anomalous Execution of Native Operating System (OS) Application Programming Interface (API): Windows API: TerminateProcess*
Observable 2	Anomalous Execution of Native Operating System (OS) Application Programming Interface (API): Windows API: MoveFileA

Observables Associated with Service Stop Technique (T0881)	
Observable 1 †	*A Process has Exited (Windows Event ID 4689): Anomalous Host Activity: Legitimate Process Anomalously Stopped: PServiceControl.exe*
Observable 2 †	*A Process has Exited (Windows Event ID 4689): Anomalous Host Activity: Legitimate Process Anomalously Stopped: Pservice_PPD.exe*
Observable 3 †	*Presence of Anomalous File on Host: Engineering Workstation Running Windows: PServiceControl.exe.MZ*

Observables Associated with Service Stop Technique (T0881)	
Observable 4 †	*Presence of Anomalous File on Host: Engineering Workstation Running Windows: Pservice_PPD.exe.MZ*
Observable 5 †	*Presence of Anomalous Script on Host: UNIX Bash Script: sc.sh*
Observable 6 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wsol.sh*
Observable 7 †	*Presence of Anomalous Script on Host: UNIX Bash Script: /var/log/wobf.sh*
Observable 8 †	*Execution of Anomalous Script on Host: UNIX Bash Script: sc.sh*
Observable 9 †	*Execution of Anomalous Script on Host: UNIX Bash Script: /var/log/wsol.sh*
Observable 10 †	*Execution of Anomalous Script on Host: UNIX Bash Script: /var/log/wobf.sh*
Observable 11	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Central Processing Unit (CPU) Utilization
Observable 12	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity
Observable 13 †	*Anomalous Host Activity: Anomalous Enumeration of Local Disks*
Observable 14 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Random Bytes: On Local Disk*
Observable 15 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): shred*
Observable 16 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): dd*
Observable 17 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): systemctl*
Observable 18 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): svcadm*
Observable 19 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): ps*
Observable 20 †	*Anomalous Host Activity: Linux Service Disabled: Hypertext Transfer Protocol (HTTP) Daemon*
Observable 21 †	*Anomalous Host Activity: Linux Service Disabled: Secure Shell (SSH) Daemon*
Observable 22 †	*Anomalous Host Activity: Solaris Service Disabled: Services Containing String "HTTP"*
Observable 23 †	*Anomalous Host Activity: Solaris Service Disabled: Services Containing String "SSH"*
Observable 24 †	*Anomalous Host Activity: Solaris Service Disabled: Services Containing String "Apache"*
Observable 25 †	*Anomalous Host Activity: Solaris Service Disabled: Services Containing String "ora_"*
Observable 26 †	*Anomalous Host Activity: Solaris Service Disabled: Services Containing String "oracle"*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1	Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404
Observable 2	Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 1	Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404
Observable 2	Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 1	Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing a TESTFR ACT Control Function Message
Observable 2	Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing a TESTFR ACT Control Function Message
Observable 3	Anomalous Network Traffic: from Controlled Stations to Engineering Workstation: Over IEC-104 TCP Port 2404: Containing TESTFR CON Control Function Messages

Observables Associated with Native API Technique (T0834)	
Observable 1	Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing a STARTDT ACT Control Function Message
Observable 2	Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing a STARTDT ACT Control Function Message
Observable 3	Anomalous Network Traffic: from Controlled Stations to Engineering Workstation: Over IEC-104 TCP Port 2404: Containing STARTDT CON Control Function Messages
Observable 4 †	*Presence of Anomalous Binary on Host: 108_100.exe: With MD5 hash 3229e8c4150b5e43f836643ec9428865*

Observables Associated with Native API Technique (T0834)	
Observable 5 †	*Execution of Anomalous Binary on Host: 108_100.exe: With MD5 Hash 3229e8c4150b5e43f836643ec9428865*

Observables Associated with Brute Force I/O Technique (T0806)	
Observable 1 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing Interrogation Command (C_IC_NA_1)*
Observable 2 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing Single Command Activation Messages (C_SC_NA_1 act)*
Observable 3 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing Double Command Activation Messages (C_DC_NA_1 act)*
Observable 4 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing Interrogation Command (C_IC_NA_1)*
Observable 5 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing Single Command Activation Messages (C_SC_NA_1 act)*
Observable 6 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing Double Command Activation Messages (C_DC_NA_1 act)*

Observables Associated with Unauthorized Command Message Technique (T0855)	
Observable 1 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing Interrogation Command (C_IC_NA_1)*
Observable 2 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing Single Command Activation Messages (C_SC_NA_1 act)*
Observable 3 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing Double Command Activation Messages (C_DC_NA_1 act)*
Observable 4 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing Interrogation Command (C_IC_NA_1)*

Observables Associated with Unauthorized Command Message Technique (T0855)	
Observable 5 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing Single Command Activation Messages (C_SC_NA_1 act)*
Observable 6 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing Double Command Activation Messages (C_DC_NA_1 act)*

Observables Associated with Manipulation of Control Technique (T0831)	
Observable 1 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing Interrogation Command (C_IC_NA_1)*
Observable 2 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing Single Command Activation Messages (C_SC_NA_1 act)*
Observable 3 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 192.x.x.x: Over IEC-104 TCP Port 2404: Containing Double Command Activation Messages (C_DC_NA_1 act)*
Observable 4 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing Interrogation Command (C_IC_NA_1)*
Observable 5 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing Single Command Activation Messages (C_SC_NA_1 act)*
Observable 6 †	*Anomalous Network Traffic: from Engineering Workstation to Controlled Station: To Eight Specific Hosts: With Private IP Address: IP Address 10.x.x.x: Over IEC-104 TCP Port 2404: Containing Double Command Activation Messages (C_DC_NA_1 act)*
Observable 7 †	*Anomalous Host Activity: Controlled Process in Anomalous State: Circuit Breakers Open: Power Disconnected from Substation*

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 1	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Central Processing Unit (CPU) Utilization
Observable 2	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity
Observable 3 †	*Anomalous Host Activity: On Linux Host: Anomalous Deletion of Data: from /boot*

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 4 †	*Anomalous Host Activity: On Linux Host: Anomalous Deletion of Data: from /home*
Observable 5 †	*Anomalous Host Activity: On Linux Host: Anomalous Deletion of Data: from /var/log*
Observable 6 †	*Anomalous Host Activity: On Linux Host: Anomalous Deletion of Data: From local drive*
Observable 7 †	*Anomalous Host Activity: On Solaris Host: Anomalous Deletion of Data: from /boot*
Observable 8 †	*Anomalous Host Activity: On Solaris Host: Anomalous Deletion of Data: from /home*
Observable 9 †	*Anomalous Host Activity: On Solaris Host: Anomalous Deletion of Data: from /var/log*
Observable 10 †	*Anomalous Host Activity: On Solaris Host: Anomalous Deletion of Data: from local drive*
Observable 11 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): shred*
Observable 12 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): rm*
Observable 13 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): dd*

Observables Associated with Data Destruction Technique (T0809)	
Observable 1 †	*Presence of Anomalous Binary on Host: CaddyWiper Binary*
Observable 2 †	*Anomalous Execution of Native Operation System (OS) Application Programming Interface (API): Windows API: DeviceIoControl*
Observable 3	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Central Processing Unit (CPU) utilization
Observable 4	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity
Observable 5 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within C:\Users*
Observable 6 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within All Direct Attached Storage Containers*
Observable 7 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within Physical Disks: \\.\\PHYSICALDRIVE0 to \\.\\PHYSICALDRIVE9*
Observable 8 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within Master Boot Record (MBR)*
Observable 9 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within GUID Partition Table (GPT)*

Observables Associated with Data Destruction Technique (T0809)	
Observable 10 †	*Anomalous Host Activity: Anomalous Enumeration of Local Disks*
Observable 11 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Random Bytes: On Local Disk*
Observable 12 †	*Anomalous Host Activity: On Linux Host: Anomalous Deletion of Data: From Attached Disks*
Observable 13 †	*Anomalous Host Activity: On Solaris Host: Anomalous Deletion of Data: From Directories Starting with the String "ORA"*
Observable 14 †	*Anomalous Host Activity: On Solaris Host: Anomalous Deletion of Data: Of Files Starting with the String "ORA"*
Observable 15 †	*Anomalous Host Activity: On Solaris Host: Anomalous Deletion of Data: From Attached Disks*
Observable 16 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): shred*
Observable 17 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): rm*
Observable 18 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): dd*

Observables Associated with Device Restart/Shutdown Technique (T0816)	
Observable 1 †	*Anomalous Host Activity: Windows is Shutting Down (Event ID 4609): Inability to Reboot*
Observable 2 †	*Anomalous Host Activity: Windows is Shutting Down (Event ID 4609): Missing Boot Loader*
Observable 3 †	*Anomalous Host Activity: Anomalous Stop Error (Blue Screen Error)*
Observable 4 †	*Anomalous Host Activity: Host Reboots: Reboot Fails*
Observable 5 †	*Anomalous Host Activity: Usage of UNIX Application Programming Interface (API): SysRq*

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1	Anomalous Execution of Native Operating System (OS) Application Programming Interface (API): Windows API: DeviceIoControl
Observable 2	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Central Processing Unit (CPU) utilization
Observable 3	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity
Observable 4 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within C:\Users*

Observables Associated with Loss of Availability Technique (T0826)	
Observable 5 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within All Direct Attached Storage Containers*
Observable 6 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within Physical Disks: \\.\\PHYSICALDRIVE0 to \\.\\PHYSICALDRIVE9*
Observable 7 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within Master Boot Record (MBR)*
Observable 8 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within GUID Partition Table (GPT)*

Observables Associated with Loss of Control Technique (T0827)	
Observable 1	Anomalous Execution of Native Operating System (OS) Application Programming Interface (API): Windows API: DeviceIoControl
Observable 2	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Central Processing Unit (CPU) utilization
Observable 3	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity
Observable 4 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within C:\Users*
Observable 5 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within All Direct Attached Storage Containers*
Observable 6 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within Physical Disks: \\.\\PHYSICALDRIVE0 to \\.\\PHYSICALDRIVE9*
Observable 7 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within Master Boot Record (MBR)*
Observable 8 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within GUID Partition Table (GPT)*

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 1	Anomalous Execution of Native Operating System (OS) Application Programming Interface (API): Windows API: DeviceIoControl
Observable 2	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Central Processing Unit (CPU) utilization
Observable 3	Anomalous Host Activity: Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity
Observable 4 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within C:\Users*

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 5 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within All Direct Attached Storage Containers*
Observable 6 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within Physical Disks: \\.\\PHYSICALDRIVE0 to \\.\\PHYSICALDRIVE9*
Observable 7 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within Master Boot Record (MBR)*
Observable 8 †	*Anomalous Host Activity: Anomalous Modification of Data: Overwriting Existing Data with Null Bytes: Within GUID Partition Table (GPT)*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Internet Accessible Device Technique (T0883)	
Artifact 1	Host Registry Entries
Artifact 2	HTTPS Traffic
Artifact 3	Suspicious Connections in Proxy Logs
Artifact 4	Timestamps
Artifact 5	Virtual Private Network (VPN) Logoff Events
Artifact 6	Suspicious Connections in Firewall Logs
Artifact 7	VPN Logon Events
Artifact 8	Service Access Point) SAP Traffic
Artifact 9	Host Registry Entries HKEY_LOCAL_MACHINE\SYSTEM
Artifact 10	SQL Traffic
Artifact 11	Host Information in External Data Store or Website (SHODAN)
Artifact 12	HTTP 80
Artifact 13	Virtual Network Computing (VNC) Traffic Port 5800
Artifact 14	Dialog Boxes Opened on Human-Machine Interface (HMI)
Artifact 15	Application Authentication Events
Artifact 16	Internet Address in Memory Socket Data
Artifact 17	Remote Logins in OS Logs (Windows Event)
Artifact 18	Operational Database Connection to External Addresses
Artifact 19	Industrial Traffic from Internet Address
Artifact 20	Standard Traffic from Internet Address
Artifact 21	Internet Address in Application Logs
Artifact 22	Internet Address in OS Logs
Artifact 23	Internet Address in Command Line Record Data (netstat)

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 Lateral Tool Transfer Technique (T0867)	
Artifact 1	Remote Network Traffic
Artifact 2	File Metadata Changes
Artifact 3	User Information Changes
Artifact 4	Process Creation
Artifact 5	System Resource Usage Management Events
Artifact 6	Data Sent from One Location to Another
Artifact 7	Data Received from One Location to Another
Artifact 8	SQL Commands
Artifact 9	SQL Create Commands
Artifact 10	SQL Insert Commands
Artifact 11	Command Prompt Dialog Box Open
Artifact 12	SMB Traffic
Artifact 13	.dll Injection into File Directory
Artifact 14	.dll Execution
Artifact 15	Common Network Traffic
Artifact 16	Command Execution
Artifact 17	Industrial Network Traffic
Artifact 18	File Creation
Artifact 19	File Modification
Artifact 20	File Deletion
Artifact 21	File Location Change
Artifact 22	POWERSHELL Dialog Box Open

Artifacts Associated with Command-Line Interface Technique (T0807)	
Artifact 1	Command Execution
Artifact 2	Application Log
Artifact 3	HTTP Traffic
Artifact 4	Telnet Traffic

Artifacts Associated with Command-Line Interface Technique (T0807)	
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
Artifact 17	Command Line Memory Data
Artifact 18	cmd.exe Application Execution
Artifact 19	Remote Desktop Protocol (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 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
Artifact 9	OS Timeline Event
Artifact 10	System Event Log Creation

Artifacts Associated with Scripting Technique (T0853)	
Artifact 11	Files Dopped into Directory
Artifact 12	Windows API Event Log

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 Native API Technique (T0834)	
Artifact 1	Alert Generated
Artifact 2	System Resource Usage Management Changes
Artifact 3	.dll Modifications
Artifact 4	Imports Hash Changed
Artifact 5	Files Created
Artifact 6	Processes Initiated
Artifact 7	Services Initiated
Artifact 8	SYSMON Events Created
Artifact 9	Performance Degradation
Artifact 10	Blue Screen
Artifact 11	Configuration Change
Artifact 12	Command Execution
Artifact 13	Industrial Protocol Command Packet
Artifact 14	Host Device Failure
Artifact 15	Industrial Network Traffic
Artifact 16	Device Reads
Artifact 17	Device I/O Image Table Manipulated

Artifacts Associated with Native API Technique (T0834)	
Artifact 18	Device Failure
Artifact 19	Systems Calls
Artifact 20	Device Performance Degradation
Artifact 21	Device Memory Modification
Artifact 22	Device Alarm
Artifact 23	Device Live Data Changes
Artifact 24	Alter Process Logic
Artifact 25	Memory Corruption

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 1	Protocol Header Enumeration
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	Simple Mail Transfer Protocol (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	Open Platform Communications (OPC) Network Traffic
Artifact 21	Statistical Anomalies in Network Traffic
Artifact 22	Domain Name System (DNS) Port 53 Zone Transfers
Artifact 23	Industrial Network Traffic

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 24	Common Network Traffic
Artifact 25	IEC-103 Traffic (For North America)
Artifact 26	IEC-61850 Manufacturing Message Simplification (MMS)
Artifact 27	Controller Proprietary Traffic
Artifact 28	Echo Type 8 Traffic
Artifact 29	Internet Control Message Protocol (ICMP) Type 7 Traffic
Artifact 30	Simple Network Management Protocol (SNMP) Port 162 Traffic
Artifact 31	SNMP Port 161 Traffic
Artifact 32	Address Resolution Protocol (ARP) Scans
Artifact 33	Operating System Queries
Artifact 34	TCP SYN Scans
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 Services Technique (T0886)	
Artifact 1	Mouse Movement
Artifact 2	Authentication Logs
Artifact 3	Network Traffic Content Creation
Artifact 4	Remote Session Creation Timestamp
Artifact 5	Process Creation
Artifact 6	VNC Traffic
Artifact 7	SMB Traffic
Artifact 8	SSH Traffic
Artifact 9	MSSQL Traffic Port 1433
Artifact 10	File Movement
Artifact 11	Desktop Prompt Windows Created

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 12	Graphical User Interface (GUI) Modifications
Artifact 13	System Log Event
Artifact 14	RDP Traffic
Artifact 15	Application Log
Artifact 16	Session Cache
Artifact 17	Unexpected
Artifact 18	Registry Connection Change
Artifact 19	Registry Changes
Artifact 20	Logoff Event
Artifact 21	Logoff
Artifact 22	Logon Event
Artifact 23	Remote Client Connection
Artifact 24	Data File Size in Network Content

Artifacts Associated with Commonly Used Port Technique (T0885)	
Artifact 1	Unexpected Process Usage of Common Port Observed via Firewall Logs
Artifact 2	Unexpected Process Usage of Common Port Observed via OS Commands (netstat)
Artifact 3	Unexpected Process Usage of Common Port Observed via Memory
Artifact 4	Unexpected Process Usage of Common Port Observed via OS Logs
Artifact 5	Unexpected Host Communicating with Common Port on Industrial Asset

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

Artifacts Associated with Valid Accounts Technique (T0859)	
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 Lateral Tool Transfer Technique (T0867)	
Artifact 1	Remote Network Traffic
Artifact 2	File Metadata Changes
Artifact 3	User Information Changes
Artifact 4	Process Creation
Artifact 5	System Resource Usage Management Events
Artifact 6	Data Sent from One Location to Another
Artifact 7	Data Received from One Location to Another
Artifact 8	SQL Commands
Artifact 9	SQL Create Commands
Artifact 10	SQL Insert Commands
Artifact 11	Command Prompt Dialog Box Open
Artifact 12	SMB Traffic
Artifact 13	.dll Injection into File Directory
Artifact 14	.dll Execution
Artifact 15	Common Network Traffic
Artifact 16	Command Execution
Artifact 17	Industrial Network Traffic
Artifact 18	File Creation
Artifact 19	File Modification
Artifact 20	File Deletion
Artifact 21	File Location Change
Artifact 22	POWERSHELL Dialog Box Open

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
Artifact 17	Command Line Memory Data
Artifact 18	cmd.exe Application Execution
Artifact 19	Remote Desktop Protocol (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 Indicator Removal on Host Technique (T0872)	
Artifact 1	HMI Dialog Box Open
Artifact 2	API System Calls
Artifact 3	HMI Interface Manipulation
Artifact 4	Process Creation
Artifact 5	Command Execution
Artifact 6	File Creation

Artifacts Associated with Indicator Removal on Host Technique (T0872)	
Artifact 7	HMI Dialog Box Close
Artifact 8	User Logon Event
Artifact 9	Windows Registry Key Modification
Artifact 10	Windows Registry Key Deletion
Artifact 11	User Logoff Event
Artifact 12	HMI Screen Changes
Artifact 13	Missing Log Events
Artifact 14	Unexpected Reboots
Artifact 15	Windows Security Log 1102 for Cleared Events
Artifact 16	File Deletion
Artifact 17	File Modification
Artifact 18	Sdelete Executable Loaded
Artifact 19	Sdelete Executable Executed
Artifact 20	File Metadata Changes
Artifact 21	Timestamp Inconsistencies
Artifact 22	User Authentication
Artifact 23	Memory Writes

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 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
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 Native API Technique (T0834)	
Artifact 1	Alert Generated
Artifact 2	System Resource Usage Management Changes
Artifact 3	.dll Modifications
Artifact 4	Imports Hash Changed
Artifact 5	Files Created
Artifact 6	Processes Initiated
Artifact 7	Services Initiated
Artifact 8	SYSMON Events Created
Artifact 9	Performance Degradation
Artifact 10	Blue Screen
Artifact 11	Configuration Change
Artifact 12	Command Execution
Artifact 13	Industrial Protocol Command Packet
Artifact 14	Host Device Failure
Artifact 15	Industrial Network Traffic
Artifact 16	Device Reads

Artifacts Associated with Native API Technique (T0834)	
Artifact 17	Device I/O Image Table Manipulated
Artifact 18	Device Failure
Artifact 19	Systems Calls
Artifact 20	Device Performance Degradation
Artifact 21	Device Memory Modification
Artifact 22	Device Alarm
Artifact 23	Device Live Data Changes
Artifact 24	Alter Process Logic
Artifact 25	Memory Corruption

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 Standard Application Layer Protocol Technique (T0869)	
Artifact 1	SMB Traffic Port
Artifact 2	Network Connection Times
Artifact 3	External IP Addresses
Artifact 4	External Network Connections
Artifact 5	DNS Autonomous System Number
Artifact 6	Increase in the Number of External Connections

Artifacts Associated with Standard Application Layer Protocol Technique (T0869)	
Artifact 7	RDP Traffic Port
Artifact 8	HTTP Traffic Port
Artifact 9	DNS Traffic Port
Artifact 10	HTTP Post Request
Artifact 11	HTTPS Traffic Port
Artifact 12	Network Content Metadata

Artifacts Associated with Commonly Used Port Technique (T0885)	
Artifact 1	Unexpected Process Usage of Common Port Observed via Firewall Logs
Artifact 2	Unexpected Process Usage of Common Port Observed via OS Commands (netstat)
Artifact 3	Unexpected Process Usage of Common Port Observed via Memory
Artifact 4	Unexpected Process Usage of Common Port Observed via OS Logs
Artifact 5	Unexpected Host Communicating with Common Port on Industrial Asset

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 1	Device Failure
Artifact 2	Protocol Header Enumeration
Artifact 3	Protocol Content Enumeration
Artifact 4	Sequential Protocol SYN Traffic
Artifact 5	Statistical Anomalies in Network Traffic
Artifact 6	Echo Port 8 Traffic
Artifact 7	DNS Port 53 Zone Transfers
Artifact 8	Device Reboot
Artifact 9	Bandwidth Degradation
Artifact 10	Host Recent Connection Logs
Artifact 11	ICMP Port 7 Traffic
Artifact 12	SNMP Port 162 Traffic
Artifact 13	SNMP Port 161 Traffic
Artifact 14	Command Line Dialog Box Open
Artifact 15	VNC Port 5900 Calls
Artifact 16	Operating System Queries
Artifact 17	Email Server Calls

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 18	Recurring Protocol SYN Traffic
Artifact 19	TCP ACK Scan
Artifact 20	Common Network Traffic
Artifact 21	Polling Network Traffic from Abnormal IP Sender Addresses
Artifact 22	NETBIOS Name Services Port
Artifact 23	Active Directory Calls
Artifact 24	SMTP Port 25 Traffic
Artifact 25	DNS Lookup Queries
Artifact 26	ARP Scans
Artifact 27	TCP Connect Scan
Artifact 28	TCP SYN Scans
Artifact 29	Industrial Network Traffic
Artifact 30	TCP FIN Scans
Artifact 31	TCP Reverse Ident Scan
Artifact 32	TCP XMAS Scan
Artifact 33	LDAP Port

Artifacts Associated with Native API Technique (T0834)	
Artifact 1	Alert Generated
Artifact 2	System Resource Usage Management Changes
Artifact 3	.dll Modifications
Artifact 4	Imports Hash Changed
Artifact 5	Files Created
Artifact 6	Processes Initiated
Artifact 7	Services Initiated
Artifact 8	SYSMON Events Created
Artifact 9	Performance Degradation
Artifact 10	Blue Screen
Artifact 11	Configuration Change
Artifact 12	Command Execution
Artifact 13	Industrial Protocol Command Packet
Artifact 14	Host Device Failure
Artifact 15	Industrial Network Traffic

Artifacts Associated with Native API Technique (T0834)	
Artifact 16	Device Reads
Artifact 17	Device I/O Image Table Manipulated
Artifact 18	Device Failure
Artifact 19	Systems Calls
Artifact 20	Device Performance Degradation
Artifact 21	Device Memory Modification
Artifact 22	Device Alarm
Artifact 23	Device Live Data Changes
Artifact 24	Alter Process Logic
Artifact 25	Memory Corruption

Artifacts Associated with Brute Force I/O Technique (T0806)	
Artifact 1	User Logon
Artifact 2	Execute Packets Sent
Artifact 3	Process Specific Protocol Mode Change
Artifact 4	Network Session Creation
Artifact 5	External Network Connections
Artifact 6	Internal Network Connections
Artifact 7	Sequential Read Requests
Artifact 8	Network Bandwidth Degradation
Artifact 9	Low Network Resource Warning
Artifact 10	Application Log
Artifact 11	Change in Process State
Artifact 12	Device Failure
Artifact 13	IP Addresses
Artifact 14	MAC Addresses
Artifact 15	Command Packets
Artifact 16	Set Point Changes
Artifact 17	Device Polling Rate Increase
Artifact 18	Operational Database Performance Degrades
Artifact 19	Select Packets Sent

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
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

Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 16	Engineering Workstation Mouse Movement

Artifacts Associated with Indicator Removal on Host Technique (T0872)	
Artifact 1	HMI Dialog Box Open
Artifact 2	API System Calls
Artifact 3	HMI Interface Manipulation
Artifact 4	Process Creation
Artifact 5	Command Execution
Artifact 6	File Creation
Artifact 7	HMI Dialog Box Close
Artifact 8	User Logon Event
Artifact 9	Windows Registry Key Modification
Artifact 10	Windows Registry Key Deletion
Artifact 11	User Logoff Event
Artifact 12	HMI Screen Changes
Artifact 13	Missing Log Events
Artifact 14	Unexpected Reboots
Artifact 15	Windows Security Log 1102 for Cleared Events
Artifact 16	File Deletion
Artifact 17	File Modification
Artifact 18	Sdelete Executable Loaded
Artifact 19	Sdelete Executable Executed
Artifact 20	File Metadata Changes
Artifact 21	Timestamp Inconsistencies
Artifact 22	User Authentication
Artifact 23	Memory Writes

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 1	Command Line Arguments
Artifact 2	Files Moved to Recycle Bin
Artifact 3	Missing Files
Artifact 4	Host System Reboot Failure

Artifacts Associated with Data Destruction Technique (T0809)	
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	Trivial File Transfer Protocol (TFTP) Port
Artifact 12	Secure File Transfer Protocol (SFTP) Port
Artifact 13	Memory Corruption
Artifact 14	Use of File Transfer Protocols
Artifact 15	Secure Copy Protocol (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 Device Restart/Shutdown Technique (T0816)	
Artifact 1	Logon Events
Artifact 2	Process Alarm
Artifact 3	Memory Corruption
Artifact 4	Unauthorized Input
Artifact 5	Command Prompt Opened
Artifact 6	Hardware Failure
Artifact 7	Logoff Events
Artifact 8	Local Network Connections

Artifacts Associated with Device Restart/Shutdown Technique (T0816)	
Artifact 9	Significant Operational Data Changes
Artifact 10	Blue Screen
Artifact 11	Reboot Screen
Artifact 12	Network Command Packets
Artifact 13	Loss of Network Connection
Artifact 14	Process Environmental Changes
Artifact 15	Process Failure
Artifact 16	Process Application Event
Artifact 17	External Network Connections

Artifacts Associated with Loss of Availability Technique (T0826)	
Artifact 1	Process Failure Due to Loss of Required Network or System Dependency
Artifact 2	Unexplained Loss of User Data
Artifact 3	Changes in Network Routing or Usage of Redundant Control System Network Connection Due to Failed Network Path
Artifact 4	Significant Reduction or Increase in Network Traffic Due to Malware Propagation of Disappearance of Services
Artifact 5	Significant Logged Usage of Native Crypto Functions or Presence of Import of Crypto Functions in Binaries
Artifact 6	Operator or User Discovery of Encrypted or Inoperable Systems
Artifact 7	File System Modification Artifacts Might Be Associated with The Loss of Availability Might Be Present on Disk
Artifact 8	Unexplained Loss of Application Data

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
Artifact 7	Runaway Conditions
Artifact 8	Service Request Increases
Artifact 9	Set Point Failure

Artifacts Associated with Loss of Control Technique (T0827)	
Artifact 10	Configuration Change
Artifact 11	Machine State Change
Artifact 12	Process Alarms
Artifact 13	Device Failure

Artifacts Associated with Indicator Removal on Host Technique (T0872)	
Artifact 1	HMI Dialog Box Open
Artifact 2	API System Calls
Artifact 3	HMI Interface Manipulation
Artifact 4	Process Creation
Artifact 5	Command Execution
Artifact 6	File Creation
Artifact 7	HMI Dialog Box Close
Artifact 8	User Logon Event
Artifact 9	Windows Registry Key Modification
Artifact 10	Windows Registry Key Deletion
Artifact 11	User Logoff Event
Artifact 12	HMI Screen Changes
Artifact 13	Missing Log Events
Artifact 14	Unexpected Reboots
Artifact 15	Windows Security Log 1102 for Cleared Events
Artifact 16	File Deletion
Artifact 17	File Modification
Artifact 18	Sdelete Executable Loaded
Artifact 19	Sdelete Executable Executed
Artifact 20	File Metadata Changes
Artifact 21	Timestamp Inconsistencies
Artifact 22	User Authentication
Artifact 23	Memory Writes

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.

Engineering
- Process Engineer
- Electrical, Controls, and Mechanical Engineer
- Project Engineer
- Systems and Reliability Engineer
- OT Developer
- PLC Programmer
- Emergency Operations Manager
- Plant Networking
- Control/Instrumentation Specialist
- Protection and Controls
- Field Engineer
- System Integrator

Operations Technology (OT) Staff
- Operator
- Site Security POC
- Technical Specialists (electrical/mechanical/chemical)
- ICS/SCADA Programmer

Operational Technology (OT) Cybersecurity
- OT Security
- ICS/SCADA Security

Management
- Plant Manager
- Risk/Safety Manager
- Business Unit Management
- C-level Management

Support Staff
- Remote Maintenance & Technical Support
- Contractors (engineering)
- IT and Physical Security Contractor
- Procurement Specialist
- Legal
- Contracting Engineer
- Insurance
- Supply-chain Participant
- Inventory Management/Lifecycle Management
- Physical Security Specialist

Information Technology (IT) Cybersecurity
- ICS Security Analyst
- Security Engineering and Architect
- Security Operations
- Security Response and Forensics
- Security Management (CSO)
- Audit Specialist
- Security Tester

Information Technology (IT) Staff
- Networking and Infrastructure
- Host Administrator
- Database Administrator
- Application Development
- ERP/MES Administrator
- IT Management

REFERENCES

[1] [Computer Emergency Response Team of Ukraine | “Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435)” | https://cert.gov.ua/article/39518 |12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[2] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[3] [Computer Emergency Response Team of Ukraine | “Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435)” | https://cert.gov.ua/article/39518 |12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[4] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[5] [TechTarget | Rob Wright | “Industroyer2: How Ukraine avoided another blackout attack” | https://www.techtarget.com/searchsecurity/news/252523694/Industroyer2-How-Ukraine-avoided-another-blackout-attack |10 August 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[6] [Youtube | Black Hat | Anton Cherepanov and Robert Lipovsky | “Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again” | https://www.youtube.com/watch?v=xC9iM5wVedQ | 28 November 2022 | Accessed on 6 December 2022 | The source is publicly available information and does not contain classification markings]

[7] [Mandiant | Daniel Kapellmann, Raymond Leong, and others | “INDUSTROYER.V2: Old Malware Learns New Tricks” | https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks | 2 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[8] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[9] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[10] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[11] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[12] [Computer Emergency Response Team of Ukraine | “Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware INDUSTROYER2 and CADDYWIPER (CERT-

UA#4435)" | https://cert.gov.ua/article/39518 |12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[13] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[14] [Youtube | Black Hat | Anton Cherepanov and Robert Lipovsky | "Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again" | https://www.youtube.com/watch?v=xC9iM5wVedQ | 28 November 2022 | Accessed on 6 December 2022 | The source is publicly available information and does not contain classification markings]

[15] [Netresec | Erik Hjelmvik | "Industroyer2 IEC-104 Analysis" | https://www.netresec.com/?page=Blog&month=2022-04&post=Industroyer2-IEC-104-Analysis | 25 April 2022 | Accessed on 1 December 2022 | The source is publicly available information and does not contain classification markings]

[16] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[17] [Youtube | Black Hat | Anton Cherepanov and Robert Lipovsky | "Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again" | https://www.youtube.com/watch?v=xC9iM5wVedQ | 28 November 2022 | Accessed on 6 December 2022 | The source is publicly available information and does not contain classification markings]

[18] [Mandiant | Daniel Kapellmann, Raymond Leong, and others | "INDUSTROYER.V2: Old Malware Learns New Tricks" | https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks | 2 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[19] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[20] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[21] [Computer Emergency Response Team of Ukraine | "Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435)" | https://cert.gov.ua/article/39518 |12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[22] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[23] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[24] [Computer Emergency Response Team of Ukraine | "Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware INDUSTROYER2 and CADDYWIPER (CERT-

UA#4435)” | https://cert.gov.ua/article/39518 |12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[25] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[26] [Computer Emergency Response Team of Ukraine | “Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435)” | https://cert.gov.ua/article/39518 |12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[27] [Youtube | Black Hat | Anton Cherepanov and Robert Lipovsky | “Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again” | https://www.youtube.com/watch?v=xC9iM5wVedQ | 28 November 2022 | Accessed on 6 December 2022 | The source is publicly available information and does not contain classification markings

[28] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[29] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[30] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[31] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[32] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[33] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[34] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[35] [Computer Emergency Response Team of Ukraine | “Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435)” | https://cert.gov.ua/article/39518 |12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[36] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed

on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[37] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[38] [Nozomi Networks | Giannis Tsaraias and Ivan Speziale | “Industroyer vs. Industroyer2: Evolution of the IEC 104 Component” | https://www.nozominetworks.com/downloads/US/Nozomi-Networks-WP-Industroyer2.pdf | 27 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[39] [Vedere Labs | “Industroyer2 and Incontroller” | https://www.forescout.com/resources/industroyer2-and-incontroller-report/ | 13 August 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[40] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[41] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[42] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[43] [Computer Emergency Response Team of Ukraine | “Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435)” | https://cert.gov.ua/article/39518 |12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[44] [Trustwave | Pawel Knapczyk | “Overview of the Cyber Weapons Used in the Ukraine - Russia War” | https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/ | 18 August 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[45] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[46] [Mandiant | Daniel Kapellmann, Raymond Leong, and others | “INDUSTROYER.V2: Old Malware Learns New Tricks” | https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks | 2 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[47] [Trustwave | Pawel Knapczyk | “Overview of the Cyber Weapons Used in the Ukraine - Russia War” | https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/ | 18 August 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[48] [Vedere Labs | “Industroyer2 and Incontroller” | https://www.forescout.com/resources/industroyer2-and-incontroller-report/ | 13 August 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[49] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[50] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[51] [Nozomi Networks | Giannis Tsaraias and Ivan Speziale | "Industroyer vs. Industroyer2: Evolution of the IEC 104 Component" | https://www.nozominetworks.com/downloads/US/Nozomi-Networks-WP-Industroyer2.pdf | 27 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[52] [Mandiant | Daniel Kapellmann, Raymond Leong, and others | "INDUSTROYER.V2: Old Malware Learns New Tricks" | https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks | 2 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[53] [Mandiant | Daniel Kapellmann, Raymond Leong, and others | "INDUSTROYER.V2: Old Malware Learns New Tricks" | https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks | 2 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[54] [Blackberry | "Threat Thursday: Malware Rebooted - How Industroyer2 Takes Aim at Ukraine Infrastructure" | https://blogs.blackberry.com/en/2022/05/threat-thursday-malware-rebooted-how-industroyer2-takes-aim-at-ukraine-infrastructure | 12 May 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[55] [Netresec | Erik Hjelmvik | "Industroyer2 IEC-104 Analysis" | https://www.netresec.com/?page=Blog&month=2022-04&post=Industroyer2-IEC-104-Analysis | 25 April 2022 | Accessed on 1 December 2022 | The source is publicly available information and does not contain classification markings]

[56] [Mandiant | Daniel Kapellmann, Raymond Leong, and others | "INDUSTROYER.V2: Old Malware Learns New Tricks" | https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks | 2 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[57] [Nozomi Networks | Giannis Tsaraias and Ivan Speziale | "Industroyer vs. Industroyer2: Evolution of the IEC 104 Component" | https://www.nozominetworks.com/downloads/US/Nozomi-Networks-WP-Industroyer2.pdf | 27 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[58] [Mandiant | Daniel Kapellmann, Raymond Leong, and others | "INDUSTROYER.V2: Old Malware Learns New Tricks" | https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks | 2 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[59] [Mandiant | Daniel Kapellmann, Raymond Leong, and others | "INDUSTROYER.V2: Old Malware Learns New Tricks" | https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks | 2 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[60] [Netresec | Erik Hjelmvik | "Industroyer2 IEC-104 Analysis" | https://www.netresec.com/?page=Blog&month=2022-04&post=Industroyer2-IEC-104-Analysis | 25 April 2022 | Accessed on 1 December 2022 | The source is publicly available information and does not contain classification markings]

[61] [Mandiant | Daniel Kapellmann, Raymond Leong, and others | "INDUSTROYER.V2: Old Malware Learns New Tricks" | https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks | 2 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[62] [Netresec | Erik Hjelmvik | "Industroyer2 IEC-104 Analysis" | https://www.netresec.com/?page=Blog&month=2022-04&post=Industroyer2-IEC-104-Analysis | 25 April 2022 | Accessed on 1 December 2022 | The source is publicly available information and does not contain classification markings]

[63] [Wired | Andy Greenberg | "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine" | Russia's Sandworm hackers attempted a third blackout in Ukraine | Ars Technica | 12 April 2022 | Accessed on 25 January 2023 | The source is publicly available information and does not contain classification markings]

[64] [Mandiant | Daniel Kapellmann, Raymond Leong, and others | "INDUSTROYER.V2: Old Malware Learns New Tricks" | https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks | 2 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[65] [Nozomi Networks | "Industroyer2: Nozomi Networks Labs Analyzes the IEC 104 Payload" | https://www.nozominetworks.com/blog/industroyer2-nozomi-networks-labs-analyzes-the-iec-104-payload/ | 27 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[66] [Netresec | Erik Hjelmvik | "Industroyer2 IEC-104 Analysis" | https://www.netresec.com/?page=Blog&month=2022-04&post=Industroyer2-IEC-104-Analysis | 25 April 2022 | Accessed on 1 December 2022 | The source is publicly available information and does not contain classification markings]

[67] [TechTarget | Rob Wright | "Industroyer2: How Ukraine avoided another blackout attack" | https://www.techtarget.com/searchsecurity/news/252523694/Industroyer2-How-Ukraine-avoided-another-blackout-attack |10 August 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[68] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[69] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[70] [Securonix | Den Iuzvyk and Tim Peck | "Securonix Threat Labs Initial Coverage Advisory: Industroyer2/CaddyWiper Targeting Ukrainian Power Grid – Detailed Analysis" | https://www.securonix.com/blog/industroyer2-caddywiper-targeting-ukrainian-power-grid/ | 13 August 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[71] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[72] [WeLiveSecurity | "Industroyer2: Industroyer reloaded" | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed

on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[73] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[74] [Computer Emergency Response Team of Ukraine | “Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435)” | https://cert.gov.ua/article/39518 |12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[75] [Securonix | Den Iuzvyk and Tim Peck | “Securonix Threat Labs Initial Coverage Advisory: Industroyer2/CaddyWiper Targeting Ukrainian Power Grid – Detailed Analysis” | https://www.securonix.com/blog/industroyer2-caddywiper-targeting-ukrainian-power-grid/ | 13 August 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[76] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[77] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[78] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[79] [WeLiveSecurity | “Industroyer2: Industroyer reloaded” | https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ | 12 April 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]