PRECURSOR ANALYSIS REPORT: UKRAINE ENERGY SECTOR CYBER ATTACK 2015

Cybersecurity for the Operational Technology Environment (CyOTE)

30 JUNE 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-69464

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: UKRAINE ENERGY SECTOR CYBER ATTACK 2015

1. EXECUTIVE SUMMARY

The Ukraine Energy Sector Cyber Attack 2015 Precursor Analysis Report leverages publicly available information about the cyber attack mounted against Ukraine's energy sector in December 2015 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.

Ukraine was the victim of a highly sophisticated and coordinated cyber attack on 23 December 2015 that compromised three power distribution utilities, known as oblenergos, and allowed the adversaries to open the breakers at over 50 electrical substations. The attack caused a loss of power to approximately 225,000 customers for several hours.[1]

The groundwork for the attack was laid as far back as May 2014, when spearphishing campaigns likely provided adversaries with initial access to the oblenergos' networks.[2] The adversaries employed an extensive array of malware and techniques in the course of their campaign: BlackEnergy, sshbear, and Kryptic malware; compromise of Virtual Private Networks (VPN) connected to a Distribution Management System (DMS) and Human-Machine Interface (HMI); and a Telephonic Denial-of-Service (TDoS) attack and adversary-scheduled outage of the Uninterruptable Power Supply (UPS) for a Private Branch Exchange (PBX) telephone system that served the oblenergos, which seriously degraded the ability of responders to communicate after the attack was triggered. While the impact on communications temporarily degraded the oblenergos' situational awareness after operators took the Supervisory Control and Data Acquisition (SCADA) systems offline, they were able to restore power in six hours by sending engineers to manually control the substations.[3]

The adversary was able to control the victims' systems and disrupt their response without causing excessive damage to either the SCADA systems or the electrical power grid itself. The main elements that were effectively destroyed were Serial-to-Ethernet converters rendered inoperable by a malicious firmware update and hard drives destroyed with KillDisk, which targeted the Master Boot Record (MBR) of victim machines, destroying just enough data to render systems inoperable during the attack.

Even though the attack did not result in catastrophic damage to the grid infrastructure, the oblenergos were operating the substations manually over two months later, still unable to remotely operate the substation breakers.[4]

Researchers and analysts identified 21 techniques likely utilized during the attack with a total of 86 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 stakeholders perceive and investigate observables accompanying the attack techniques prior to the triggering event, earlier comprehension of malicious activity can take place. Ten of the identified techniques used during the Ukraine 2015 cyber attack were precursors to the triggering event. Case study analysts identified 48 observables associated with precursor techniques. CyOTE researchers assessed 34 observables

to have an increased likelihood of perception during the 575 days preceding the triggering event.

The information gathered in this report contributes to a library of observables tied to a repository of artifacts, data sources, and technique detection references 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.

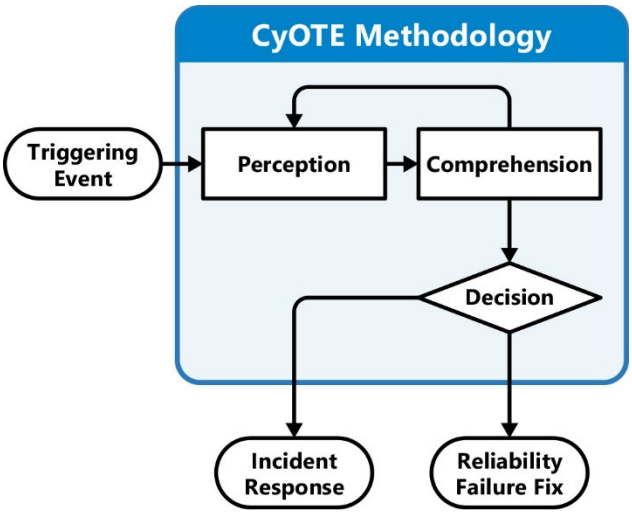


Figure 1. CyOTE Methodology

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 case study's 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 to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

Three Ukrainian power distribution utilities, known as oblenergos, were the victims of a cyber attack on 23 December 2015 (D-0) that resulted in a loss of power for approximately 225,000 customers.[5]

Spearphishing campaigns likely provided the adversaries with initial access as far back as May 2014 (D-575).[6] Using harvested credentials, the adversaries launched a coordinated attack to open breakers at over 50 substations across the three oblenergos, causing an outage that lasted six hours.[7]

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.

At about 3:30 PM on 23 December 2015 (D-0), operators at Chernivistioblenergo noticed the cursors on their Human-Machine Interfaces (HMIs) moving on the screen (phantom mouse) to open their substation breakers.[8,9] At roughly the same time, adversaries attacked Kievoblenergo by sending commands via a rogue client directly to the Distribution Management System (DMS) to open breakers.[10,11] Approximately 30 minutes later at Prykarpattyoblenergo, adversaries used the phantom mouse again to open that utility's substation breakers. The three victims had little time to respond once the adversaries triggered these attacks.

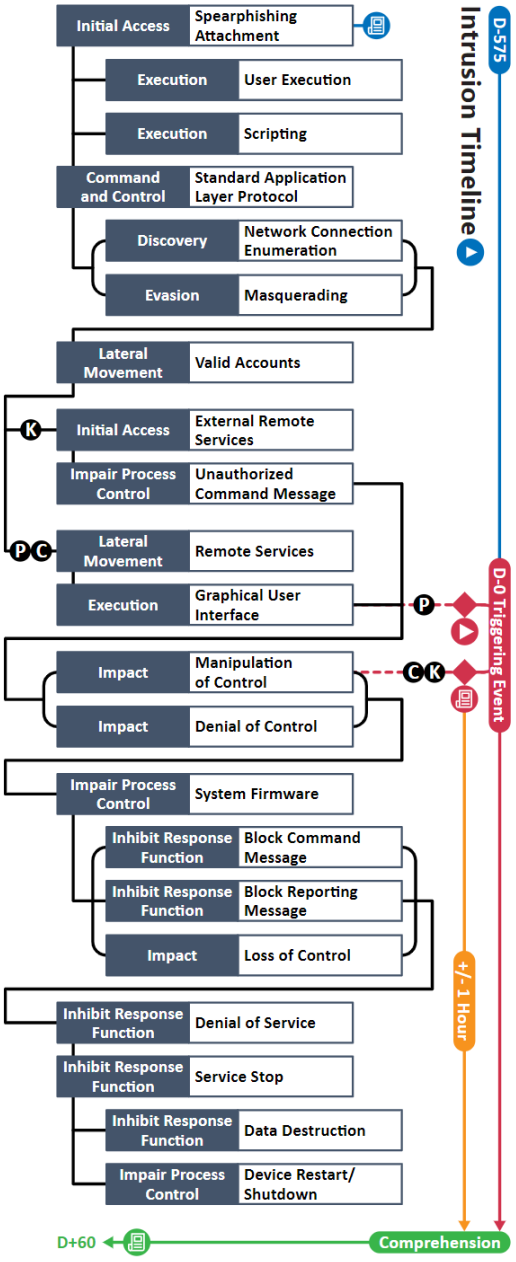


Figure 2. Intrusion Timeline

Adversaries also anticipated and impaired the oblenergos' ability to respond to the outage. The adversaries overwrote firmware on the Serial-to-Ethernet converters that enabled control center operators to remotely control breakers (H-0 through H+1), forcing engineers into the field to take manual control of the substations. A coordinated Telephonic Denial-of-Service (TDoS) attack disabled Kievoblenergo's call center for three hours (H+3), preventing communication with customers. The adversaries also impacted key data centers and phone systems by scheduling Uninterruptable Power Supply (UPS) systems to go offline prior to the attack.[12] Finally, a wiper deleted the Master Boot Record (MBR) of systems that remained online, including those tied to finance and human resources, rendering them useless and further adding to the chaos.

Full comprehension of the attack did not occur until two months later (D+60), when the Department of Homeland Security (DHS) issued a formal report on the event.[13]

Analysts and researchers identified 21 techniques in a sequence and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Ukraine Energy Sector Cyber Attack 2015

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
Wireless Compromise									**System Firmware**		

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	21
Technique Observables	86
Precursor Techniques	10
Precursor Technique Observables	48
Highly Perceivable Precursor Technique Observable	34

3. OBSERVABLE AND TECHNIQUE ANALYSIS

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

3.1. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS

Adversaries used the Spearphishing Attachment technique (T0865) for Initial Access to communications networks of multiple companies within the Ukrainian energy sector. Adversaries sent malicious Word/Excel docs with embedded Object Linking and Embedding (OLE) objects.[14] Malicious document names included, Додаток1.xls, $RR143TB.doc, and associated components such as vba_macro.exe.[15] If a victim downloaded and executed such attachments, these attachments would generate anomalous network connections or downloads over HTTP(S).

Adversaries conducted multiple phishing campaigns against the Ukrainian energy sector leading up to the December 2015 attack.[16,17,18] On 12 May 2014, Prykarpattyaoblenergo received an email as part of a campaign targeting Ukraine's State Administration of Railway Transport. At the end of March 2015, an oblenergo in Western Ukraine was the target of a phishing attack.[19] The spearphishing campaigns included forged sender addresses that appeared to impersonate at least two Ukrainian government entities, the Ukrainian Ministry of Energy and the Supreme Council of Ukraine.[20,21,22]

Kryptic and Dropbear backdoors were discovered on hosts in Prykarpattyaoblenergo and Chernivistioblenergo, respectively, and along with BlackEnergy 2/3—a highly modular trojan—are additional possible access vectors for the December 2015 attack.[23,24]

In addition, spearphishing attachments used in a subsequent attack in January 2016 initiated a download of a GCat binary compiled by PyInstaller.[25] When executed, this binary sends unusual Simple Mail Transfer Protocol (SMTP) traffic to Google or another webmail provider. File signatures extracted from network traffic or host data provide additional observables for BlackEnergy 2/3 or GCat.

Considering the prevalence of spearphishing attacks against Ukrainian targets, particularly in the energy sector, CyOTE analysts assess that spearphishing was a likely access vector for the December 2015 attack against the three oblenergos.

Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe these reported pieces of evidence.

A total of seven observables were identified with the use of the Spearphishing Attachment technique (T0865). This technique is important for investigation because it presents perceivable effects that, if identified and investigated earlier, could have reduced comprehension time by as much as 19 months. 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 likely prevent adversaries from accessing internal networks and delivering malicious payloads.

Of the seven 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 30 artifacts could be generated by the Spearphishing Attachment technique
Technique Observers[a]	Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

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

3.2. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

Adversary malware employed the User Execution technique (T0863) for Execution by sending victims malicious Microsoft Office documents. Targeted victims would likely notice suspicious emails with spoofed sender addresses and attachments that prompt users to enable macros when downloaded. Once opened, these Word and Excel documents would spawn suspicious child processes associated with command prompt processes or network communications. As a result, HTTP or Server Message Block (SMB) protocols may contain known malicious signatures for Command and Control (C2) or malware propagation.

Victims of spearphishing campaigns likely provided one vector for initial access leading to the December 2015 power outages. Email recipients would have been prompted to download and open weaponized Microsoft Office files.[26] For example, the May 2014 spearphishing attack that affected Prykarpattyaoblenergo employed a Portable Executable (PE) file disguised as a Microsoft Word document.[27] In another example, the March 2015 phishing attack targeted grid operators in Western Ukraine via a weaponized Microsoft Excel file Додаток1.xls.[28] BlackEnergy malware, if it was being employed, would install once the email recipients enabled the malicious macros on their workstation.

Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel who monitor enterprise and operational networks, as well as endpoint devices, may have been able to observe the reported pieces of evidence. IT Cybersecurity, and IT Staff would likely observe communications with external IP addresses via HTTP traffic, as well as malicious signatures associated with embedded scripts within Microsoft Office documents.[29] It is important to note, however, that identifying Indicators of Compromise (IoC) is not enough to stop infection. For example, in the May 2014 spearphishing campaign the executable PE file was detected by 16 of 52 antivirus products, but still resulted in an infection.[30]

A total of three observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation because it allows malware access to the host. User execution is a common technique that adversaries regularly use to execute payloads within a victim's environment for follow-on activities, such as reconnaissance or deployment of additional malicious software. This technique appears early in the timeline and responding to it would effectively halt the adversaries' initial access. Terminating the chain of technique at this point would prevent the malware from infecting the host, eliminating the possibility of operational damage in both the IT and OT environments.

Of the three observables associated with this technique, all 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 23 artifacts could be generated by the User Execution technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

3.3. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

Malicious Microsoft Office documents containing OLE (or another scripting object) execute and install malware on the victim workstation as part of the Scripting technique (T0853) for Execution. Child processes of these malicious MS Office documents then generate network traffic for C2 and scan the victim network. Malicious macros written in Visual Basic for Applications (VBA) install plugins on the email recipient's workstation containing libraries for keylogging, network scanning, taking screenshots, or stealing passwords.[31]

Files specific to the 2015 campaign included Додаток1.xls, $RR143TB.doc, VBA_macro.exe, CPLEXE.EXE (original name), MS-IME (internal name), virus_04.exe, vba_macro, icshextobin.exe, BlackEnergy.exe, and 1.exe.[32,33,34]

This technique would very likely have occurred immediately following the User Execution technique in Section 3.2 and, by inference, likely occurred sometime between May 2014 and March 2015. Execution of this technique would provide data from reconnaissance of the victim networks that would be used in later stages of the attack.

Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel who monitor enterprise and operational networks, as well as endpoint devices, may have been able to observe the reported pieces of evidence. These observers would likely observe an increase in network traffic as well as the execution of specific services on endpoints.

A total of three observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because it allows the adversary to conduct malicious actions in a victim's environment, often establishing an initial foothold. This technique appears early in the timeline and responding to it will likely halt further adversary activity within the victim's environment. Terminating the chain of techniques at this point would limit malicious activity in the victim's environment, as well as avert future events such as manipulation of control and data destruction.

Of the three observables associated with this technique, all 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 12 artifacts could be generated by the Scripting technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

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

The Standard Application Layer Protocol technique (T0869) was used for Command and Control. The C2 traffic resulted in anomalous outbound network connections or downloads over HTTP(S).[35] This traffic was associated with a parent process for a malicious Microsoft Office document containing OLE or another scripting object. Communications to a C2 server also made an HTTP request directly to an IP with no associated Domain Name System (DNS) request.[36] If GCat, a backdoor trojan, was used, one could observe SMTP connections to unusual or unexpected mail services. In addition, C2 servers can encrypt some HTTP communications with the RC4 algorithm.[37]

As early as May 2014 and as late as December 2015, the BlackEnergy malware deployed to victim networks likely established a remote connection with a C2 server via HTTP POST requests to download additional malware plugins.[38] These plugins, described in Section 3.3, could be used to collect information about the victim networks.[39,40]

Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff personnel could perceive these reported pieces of evidence.

A total of four observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation because defenders within the victim's environments may be able to identify which internal host(s) is communicating with anomalous external domains. Defenders could deny anomalous external communications after they identify hosts that have established connections. This technique appears early in the timeline and responding to it will degrade adversarial external C2 communications as well as adversarial control over victim operating assets. Terminating the chain of techniques at this point would end the adversaries' ability to exfiltrate sensitive information.

Of the four 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 12 artifacts could be generated by the Standard Application Layer Protocol technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

3.5. NETWORK CONNECTION ENUMERATION TECHNIQUE (T0840) FOR DISCOVERY

Adversary malware employed the Network Connection Enumeration technique (T0840) for Discovery. Infected systems likely generated network traffic associated with scanning behavior including sequential ports, high destination to source port communication ratio, and high quantity of partial connections. The technique may also be associated with anomalous use of the MS Sysinternals PsExec tool.

Using malware such as BlackEnergy 3, the adversaries could map the network and scan hosts for open ports using modules such as scan.dll.[41,42] This activity could have occurred as early as May 2014 at Prykarpattyaoblenergo and as late as December 2015 for the other victims. The three oblenergos used different DM), so adversaries needed to gather information to understand each of them.[43,44] Once BlackEnergy operators obtained valid credentials, they could move to other computers via PsExec and the vs.dll module.[45] In the October 2015 attacks against Ukrainian media outlets, adversaries utilized this approach, which may have been used in December against the three oblenergos to enumerate and establish access to victim systems.[46]

OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel monitoring operational networks and endpoint devices may have been able to observe these reported pieces of evidence.

A total of three observables were identified with the use of the Network Connection Enumeration technique (T0840) for Discovery. This technique is important for investigation because it generates observable remote-to-internal network traffic across multiple network segments. Additionally, this technique can be used to catalogue systems within victim networks. This technique appears early in the sequence of techniques and responding to it will delay the adversary's ability to discover shared resources with internet facing devices. Terminating the chain of techniques at this point would prevent the adversary from gaining awareness of targeted IT and OT systems.

Of the three observables associated with this technique, all 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 33 artifacts could be generated by the Network Connection Enumeration technique
Technique Observers	OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

3.6. MASQUERADING TECHNIQUE (T0849) FOR EVASION

The Masquerading technique (T0849) was used for Evasion. Adversaries began scanning the network with the BlackEnergy component scan.dl but then switched to the more effective nmap tool. This evidence suggests that adversaries had time to adapt their approach to conducting reconnaissance on victim networks.

Adversaries disguised the nmap tool as the svchost.exe executable in the directory C:\Windows\Temp\Syslog, while the legitimate svchost.exe is in C:\Windows\System32\.[47] The illegitimate svchost.exe could be unsigned, have an invalid signature, have an unusual publisher signature, or a valid signature but invalid or unknown file hash. Defenders may observe unusual library imports and exports or application files within the operating system.

IT Cybersecurity and IT Staff personnel may have been able to observe the reported pieces of evidence.

A total of six observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation because the adversary purposely disguises files so staff may not suspect malicious applications or executables. This technique appears early in the attack timeline and responding to it would enhance detection of adversarial activity. This technique modifies the host operating system files via the manipulation of system configuration settings and associated system registry entries, placing the host into a modified or compromised state. This technique also generates network traffic, a potential source of investigation for defenders.

Of the six 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 14 artifacts could be generated by the Masquerading technique
Technique Observers	IT Cybersecurity, IT Staff

3.7. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

Adversaries employed the Valid Accounts technique (T0859) for Lateral Movement by gathering valid credentials to establish pathways into the control environments of the oblenergos on 23 December 2015.[48,49] At 4:10 PM OT Staff responded to outages at one oblenergo by disabling an HMI administrator account, only to have the adversaries switch to another HMI account to continue the attack.[50] Pathways that enabled this capability included credentials for the Virtual Private Network (VPN) used to access the control network remotely and likely the Remote Desktop Protocol (RDP) service to access the Windows Domain Controller. Adversaries created additional unauthorized domain accounts in at least one instance.[51] These credentials could have been harvested through BlackEnergy 3 plugins to log keystrokes, through compromise of the domain or by using mimikatz to retrieve Windows account passwords/hashes.[52]

Suspicious or unusual logins to domain-joined assets observed in the Domain Controller or target machine's Windows Event Logs' Security Log and likely indicated anomalous use of valid accounts. SMB traffic associated with a user account that can invoke PsExec also indicates potential use of this technique to propagate across the network.[53] By default, PsExec creates a new service, named PSEXESVC, on the remote system that can be detected via Windows new service creation logs, Event ID 7045 and 4697. Unusual user account logins, particularly those associated with admin accounts across network services such as SMB, also indicate the Valid Accounts technique. As the BlackEnergy malware propagates, suspicious files such as ps.dll, ss.dll, and kl.dll are moved over SMB or other admin shares.[54]

OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe the reported pieces of evidence through an investigation.

A total of eight observables were identified for the Valid Accounts technique (T0859). This technique is important for investigation because compromised credentials may be used to bypass access controls to various resources within a network or grant an adversary increased privileges to specific systems and devices. This technique appears early in the timeline and responding to it will limit persistence via gathering of legitimate credentials and access to protected systems. Terminating the chain of techniques at this point would limit access to the victim's operating environment.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

3.8. EXTERNAL REMOTE SERVICES TECHNIQUE (T0822) FOR INITIAL ACCESS

The External Remote Services technique (T0822) was used for Initial Access. Adversaries gained access to oblenergo control networks as early as May 2014 with persistent access continuing through at least 23 December 2015 by using existing remote access tools similar to RDP and radmin.[55] Credentials for VPN access to oblenergo Supervisory Control and Data Acquisition (SCADA) networks were likely obtained from Windows Domain Controllers, allowing the adversaries to interact directly with DMS clients, and the VPNs from the business network into the SCADA networks appeared to lack Two Factor Authentication (2FA).[56] Adversaries were then able to access the SCADA systems for Chernivistioblenergo, Kievoblenergo, and Prykarpattyaoblenergo at approximately 3:30 PM, 3:35 PM, and 4:06 PM, respectively, on 23 December.[57,58]

As a result of this technique, VPN application logs likely showed anomalous account activity and VPN logon session metadata likely showed the use of a compromised account. Further, host logs contained unusual process data associated with remote access tools such as radmin.[59] These remote access connections could trigger network Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alerts (e.g., snort rules).

OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel monitoring operational networks and endpoint devices may have been able to observe the reported pieces of evidence through an investigation.

A total of four observables were identified with the use of the External Remote Services technique (T0822). This technique is important for investigation because it allowed the adversary to gain initial access to victim operating environments. 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 gaining initial access to the system.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 26 artifacts could be generated by the External Remote Services technique
Technique Observers	IT Staff, OT Staff, IT Cybersecurity, OT Cybersecurity

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

The Unauthorized Command Message technique (T0855) was used to Impair Process Control. One expression of this technique is to use anomalous VPN connections to access a key business application. In this case study, adversaries used a DMS client application to issue commands directly to a DMS server in the rogue client approach employed at Kyivoblenergo.[60] Even with the phantom mouse technique, operator HMIs reflected unauthorized process change inputs via the radmin log. Other observables associated with this technique in an operational environment include PCAP files showing unauthorized instructions sent to field controllers, and alarms due to changes in the operational database or device configurations. This SCADA hijack approach was employed at Kievoblenergo, whereas the phantom mouse in the previous section was used at Prykarpattyaoblenergo and Chernivtsioblenergo.[61] Therefore, CyOTE analysts assess that this technique occurred at approximately 3:35 PM on 23 December 2015.

Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe the reported pieces of evidence through an investigation.

A total of five observables were identified with the use of the Unauthorized Command Message technique (T0855). This technique is important for investigation because it is the mechanism by which adversaries can instruct operational systems to perform actions outside of their intended functionality. This technique appears in the middle of the timeline and responding to it will prevent the adversary from performing any actions that may cause an impact to physical processes. Terminating the chain of techniques at this point would limit operational damage.

Of the five 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 16 artifacts could be generated by the Unauthorized Command Message technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

3.10. REMOTE SERVICES TECHNIQUE (T0886) FOR INITIAL ACCESS

The Remote Services technique (T0886) was used for Initial Access. Adversaries began to access legitimate remote services following credential harvesting using RDP from admin accounts to access the domain controller. At least one oblenergo' s firewall allowed adversaries to remote admin out of the environment with a capability native to the victim systems.[62] This access was used just before attack execution on the afternoon of 23 December.[63] The phantom mouse phenomenon, where breakers were opened via HMIs, was enabled via RDP.[64]

Observables associated with this technique include increased RDP traffic to or from unusual or unexpected hosts. IT and OT personnel could very likely observe RDP connections in network traffic or host logs. Logs may reveal unexpected usage of administrator accounts for RDP sessions, as well as changes to the time-of-day access patterns. In addition, logs of affected hosts may contain unusual process data in host logs; unexpected radmin connections may trigger network IDS/IPS alerts. Finally, users of affected hosts might observe commands being entered or unexpected mouse movements.

Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe the reported pieces of evidence through an investigation.

A total of six observables were identified with the use of the Remote Services technique (T0886). This technique is important for investigation because it is used by adversaries to laterally move through a victim's environment, allowing for further malicious activity. This technique appears in the middle of the timeline and responding to it may halt future activity. Terminating the chain of techniques at this point would limit adversary activity in the victim's environment.

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

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

3.11. GRAPHICAL USER INTERFACE TECHNIQUE (T0823) FOR EXECUTION

The Graphical User Interface technique (T0823) was used for Execution. This technique is referred to as the phantom mouse. At Prykarpattyaoblenergo and Chernivistioblenergo, remote admin tools at the OS level were employed to open breakers.[65] Adversaries took control of employee workstations and opened breakers across the managed substations between 15:30 and 16:30 local time.[66] Adversaries targeting the first oblenergo started to open circuit breakers at 15:30 and the cyber attack lasted approximately 60 minutes.[67] OT Staff noticed the phantom mouse and took a video as it was happening in real-time, and were unable to use their mouse and keyboard to interfere with the attack.[68,69]

Victims of this technique would likely notice mouse movements on the screen, unauthorized inputs, and a potential inability to utilize the mouse or keyboard. If access to the GUI is enabled via RDP, additional observables would include an increase in RDP traffic associated with remote GUI sessions. Such RDP traffic may also originate from a new or unusual source host, occur at an odd time, or be via a session with an unusual or unexpected user.

Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe the reported pieces of evidence through an investigation. Operations zone stakeholders would likely have noticed the phantom mouse movements, and IT Staff and IT Cybersecurity might observe anomalous RDP traffic.

A total of seven observables were identified with the use of the Graphical User Interface technique (T0823). This technique is important for investigation because adversaries may gain access to a machine and enhance their execution capabilities. Additionally, this technique may be apparent to observers, allowing for enhanced detection of adversarial actions. This technique appears later in the attack and represents the triggering event, as it is the point at which the victim noticed mouse cursor movement. Terminating the chain of techniques at this point would limit operational damage as the adversary would not have direct access to equipment that controls substation equipment.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 58 artifacts could be generated by the Graphical User Interface technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

3.12. MANIPULATION OF CONTROL TECHNIQUE (T0831) FOR IMPACT

Adversaries employed the Manipulation of Control technique (T0831) for Impact. Observables associated with an Impact tactic depend upon the business process supported by the Operations Zone. Within the energy sector, substation breakers physically changing positions indicate manipulation of control over the electrical power topology.[70,71] Secondly, unanticipated command traffic to control operational assets are a general observable for this technique that is sector agnostic.

In the case of the December 2015 attack against Ukraine, attackers manipulated physical control processes by sending valid commands to open substation breakers managed by the victim oblenergos. Over a period of approximately 60 minutes, attackers were able to open breakers in at least 57 substations, resulting in widespread power outages.[72] For Prykarpattyaoblenergo, attackers took between 20 and 30 minutes to inflict an outage.[73]

Engineering and OT Staff personnel may have been able to observe anomalous device activity and command messages during the attack.

A total of two observables were identified with the Manipulation of Control technique (T0831). This technique is important for investigation because adversaries can manipulate physical process controls within the OT environment, potentially causing service interruptions. This technique appears late in the attack sequence and responding to it will delay the adversary's coordinated activities to cause interruption to controlled processes. Terminating the chain of techniques at this point would limit operational damage, as the adversary would not be able to manipulate operational systems.

Of the two observables associated with this technique, both 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	Engineering, OT Staff

3.13. DENIAL OF CONTROL TECHNIQUE (T0813) FOR IMPACT

The Denial of Control technique (T0813) was used for Impact. Adversaries modified user passwords to hamper the ability of the victims to recover and then, during the attack, took control of workstations and locked out operators.[74,75,76,77] Observables include the inability to control input devices (keyboard, mouse, etc.) to a system.

Engineering, OT Staff, and OT Cybersecurity personnel may have been able to observe the reported pieces of evidence during an attack.

A total of two observables were identified with the use of the Denial of Control technique (T0813). This technique is important for investigation because it can prevent operators and engineers from interacting with process controls causing the affected process to operate in an undesired state. This technique appears late in the timeline and responding to it will allow defenders to regain control of the system. Terminating the chain of techniques at this point would limit 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 8 artifacts could be generated by the Denial of Control technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity

3.14. SYSTEM FIRMWARE TECHNIQUE (T0857) FOR INHIBIT RESPONSE FUNCTION

Adversaries used the System Firmware technique (T0857) to inhibit the response function. After opening breakers, the adversaries updated firmware for Serial-to-Ethernet communications devices, rendering them inoperable.[78,79,80] As a result, Engineers at the affected oblenergos were unable to open breakers to restore power remotely. Instead, Engineers took SCADA systems offline and went to manual mode to restore power, traveling to distribution substations to manually open and close breakers. The oblenergos were still operating breakers manually over two months after the attack.[81]

Observables associated with this technique include an unauthorized modification made to device firmware, which rendered field devices inoperable. At least 16 substations were disconnected from the control network using the malicious firmware updates. Data transfers directly to field devices, either at an unexpected time or of an unusual size, may be associated with implementations of this technique.

Engineering, OT Staff, and OT Cybersecurity personnel may have been able to observe the reported pieces of evidence during an attack.

A total of four observables were associated with the use of the System Firmware technique (T0857). This technique is important for investigation because it enables adversaries to interrupt service as well as damage physical equipment. This technique appears late in the timeline, and responding to it will prevent adversaries from interrupting services. Terminating the chain of techniques at this point would limit adversarial capabilities related to Operational Technology equipment manipulation.

Of the four 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 16 artifacts could be generated by the Module Firmware technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity

3.15. BLOCK COMMAND MESSAGE TECHNIQUE (T0803) FOR INHIBIT RESPONSE FUNCTION

The Block Command Message technique (T0803) was used for Inhibit Response Function. During the Ukraine 2015 attack, adversaries severed communications between oblenergo control centers and field devices in substations using two main approaches; the elements of this technique are very similar to those for the Block Reporting Message technique (T0804) in Section 3.16.

First, Engineers at impacted workstations could observe SCADA commands to open breakers being issued but were unable to use their mouse and keyboard to interfere with the attack.[82,83,84] Second, adversaries updated and corrupted the firmware of Serial-to-Ethernet converters. Once corrupted, these devices would have to be physically replaced to enable breakers to be opened and closed remotely.

When command messages are blocked by corrupting a converter, the following three observables may occur. First, a large file transfer to a converter typically doesn't occur in an OT environment. Second, if the protocol used to upload the malicious firmware is supported by passive network monitoring deep packet inspection, then the firmware upload might be detected and/or extracted. Third, command messages that depend on corrupted protocol converters will not reach source or destination assets.

Engineering and OT Staff personnel monitoring operational networks and end devices may have been able to observe a lack of response to commands even after control of the network was restored.[85]

A total of three observables were associated with the use of the Block Command Message technique (T0803). This technique is important for investigation because adversaries can block legitimate commands issued to industrial equipment. This technique appears late in the attack sequence and responding to it will limit the interruption of control. Terminating the chain of techniques at this point would prevent adversaries from blocking victims' access to operational equipment, as well as limit the interruption of services to customers.

Of the three 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 9 artifacts could be generated by the Block Command Message technique
Technique Observers	Engineering, OT Staff

3.16. BLOCK REPORTING MESSAGE TECHNIQUE (T0804) FOR INHIBIT RESPONSE FUNCTION

The Block Reporting Message technique (T0804), associated with the adversary's corruption of Serial-to-Ethernet converters, was used to Inhibit Response Function. Reporting messages that depend on corrupted protocol converters will not reach source or destination assets, resulting in message time-outs and non-responsive assets.

During the Ukraine 2015 attack, adversaries severed communications between oblenergo control centers and field devices in substations by updating and corrupting the firmware of Serial-to-Ethernet converters.[86,87,88,89,90] Operators would have to physically replace these converters to restore communications between field devices and the control center.

Engineering and OT Staff personnel monitoring operational networks and end devices may have been able to observe unresponsive commands even after control of the network was restored.[91]

One observable was identified with the Block Reporting Message technique (T0804). This technique is important for investigation because adversaries can mask changes they have made to operational equipment, preventing detection. This technique appears late in the attack sequence and responding to it will temporarily delay the adversary's activity. Terminating the chain of techniques at this point would delay the adversary but would not prevent impacts to the OT environment.

The one 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 18 artifacts could be generated by the Block Reporting Message technique
Technique Observers	Engineering, OT Staff

3.17. LOSS OF CONTROL TECHNIQUE (T0827) FOR INHIBIT RESPONSE FUNCTION

Adversaries used the Loss of Control Technique (T0827) to Inhibit Response Function. Although this technique may apply to a variety of systems, observables associated with the Ukraine 2015 attack include inaccessible systems, systems not booting, and error messages or application crashes due to missing critical files. Binaries extracted from network traffic or a host that match KillDisk file signatures in Yara or other signature tools provide an additional observable.

On 23 December, adversaries implemented the Loss of Control Technique with a variant of KillDisk featuring a timer, scheduling outages to UPS systems, and uploading firmware to disable Serial-to-Ethernet converters at substations.[92] The overall result was a loss of system control for enterprise systems such as finance and human resources via KillDisk, a loss of telephone connectivity at Prykarpattyaoblenergo via scheduling UPS outages, and a loss of SCADA so severe that operators took those systems offline.[93]

Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, and IT Staff personnel may have been able to observe the reported pieces of evidence.

A total of four observables were identified with the use of the Loss of Control technique (T0827). This technique is important for investigation because it prevents owners and operators from issuing commands to equipment. This technique also presents noticeable effects, particularly unresponsive equipment. This technique appears late in the timeline, and terminating the chain of techniques at this point would limit the adversary's ability to impact additional operational systems, as well as reduce impact severity and recovery time.

Of the four observables associated with this technique, all 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 13 artifacts could be generated by the Loss of Control technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff

3.18. DENIAL OF SERVICE TECHNIQUE (T0814) FOR INHIBIT RESPONSE FUNCTION

The Denial-of-Service technique (T0814) was used for Inhibit Response Function. Several observables are associated with a TDoS attack, which was employed during the Ukraine 2015 attack. During a TDoS, calls flood a targeted call center, resulting in a large wait queue. The volume of phone calls may result in high utilization of telephone infrastructure, denying users the ability to dial an impacted phone number, or the infrastructure itself may fail.

During the Ukraine 2015 attack, adversaries launched a TDoS attack on call centers to disrupt operations and restoration efforts of Prykarpattyaoblenergo and Kievoblenergo. Kievoblenergo was unable to receive calls about the location of outages due to a flood of bogus, automated telephone calls from foreign phone numbers. This degraded its ability to respond quickly because the oblenergo had no situational awareness without inputs from the HMIs and was unable to receive calls from customers about where outages had occurred. The TDoS attack compounded the effect on the oblenergos' response capability after adversaries took the SCADA systems offline.[94] The adversaries further degraded communications through a scheduled UPS outage (see Section 3.21) that impacted a telephony communications server at one oblenergo.[95]

Engineering, OT Staff, IT Cybersecurity, and IT Staff personnel may have been able to observe the reported pieces of evidence associated with this technique.

A total of five observables were identified with the use of the Denial-of-Service technique (T0814). This technique is important for investigation because it enables adversaries to impact operational environments and limit the ability of responders to mitigate operational impacts. This technique appears late in the timeline, and responding to it will limit the impact to operational systems outside of the initial access vector. Terminating the chain of techniques at this point would protect external systems and networks from damage.

Of the five observables associated with this technique, all 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 14 artifacts could be generated by Denial-of-Service technique
Technique Observers	Engineering, OT Staff, IT Cybersecurity, IT Staff

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

The Service Stop technique (T0881) was used for Inhibit Response Function. During the Ukraine 2015 attack, adversary behavior targeting oblenergo systems stopped critical functions in the cyber and physical domains.[96] In the physical domain, attackers stopped electrical service for an estimated 225,000 customers by taking offline multiple substations across three oblenergos. Adversaries targeted Serial-to-Ethernet converters, rendering them unrecoverable by the manufacturer, to deny operators the ability to open and close substation breakers remotely.[97,98]

In addition, using KillDisk, adversaries overwrote the MBRs of multiple machines in enterprise and operational environments, impacting a variety of business functions.[99] Filenames such as svchost.exe, tsk.exe, crab.exe, and virus_ololo.dat are correlated with the implementation of this technique in the Ukraine 2015 attack.

Stopped network services might result in an increase in failed network connections observed in network traffic (e.g., TCP RST). In addition, inoperable systems might result in an increase in network messages associated with an unknown or unavailable host (e.g., ICMP host unreachable). Due to unavailable systems, operators might notice that process functions are not working as expected or that systems cannot be accessed.

Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe the reported pieces of evidence during an investigation.

A total of four observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation because it prevents victims from delivering products or services. This technique appears late in the timeline, and it modifies the host operating system files, via the manipulation of host services and modification of registry files, resulting in the host being placed into a modified or compromised state. Terminating the chain of techniques at this point would limit the theft of operational information and potential business interruptions.

Of the four observables associated with this technique, all 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 13 artifacts could be generated by the Service Stop technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

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

Adversary malware used the Data Destruction technique (T0809) for Inhibit Response Function. This technique inhibits recovery attempts made by the victim through deletion of critical OS files. In general, effects of this technique include file signatures from files extracted from network data or recovered from an endpoint that contains KillDisk signature matches. Users might be unable to login to victim systems and systems might crash or throw error messages.

During the Ukraine 2015 attack, adversaries used a specific variant of Win32/Killdisk.NBB.[100] This variant included a command line argument for a time delay, the ability to delete Windows Event Logs, and a targeted list of document extensions.[101] Targets were mainly enterprise networks and included servers and hosts used by management, human resources, and finance staff; some Remote Terminal Units (RTUs) in the OT environment were also impacted.[102]

Engineering, OT Staff, OT Cybersecurity, IT Staff, and IT Cybersecurity personnel may have been able to observe the reported pieces of evidence.

A total of five observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because it is the mechanism by which Disttrack destroys data and incapacitates systems. This attack appears near the end of the timeline, and responding to it would allow defenders to limit data loss. Terminating the chain of techniques at this point would limit the destruction of data and resultant business interruptions.

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 27 artifacts could be generated by the Data Destruction technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Staff, IT Cybersecurity

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

The Device Restart/Shutdown technique (T0816) was used for Inhibit Response Function. Devices are unavailable while restarting or after shutting down. These systems remained inaccessible and did not respond even if restarted after their MBRs were deleted. System log entries denoting system shutdown will be present on the host until deleted and will be visible if central logging is enabled.

During the Ukraine 2015 attack, adversaries inhibited the oblenergos' response following the power outage by scheduling outages to systems infected with KillDisk malware and compromised UPS systems that could provide backup power.[103] When KillDisk runs, after targeting the MBR on a device it restarts the host, rendering it inoperable.[104] UPS outages were scheduled using remote management interfaces before the first breakers were opened.[105]

As with the TDoS attack, this technique may have been an alternative approach to deny telephone communications to Prykarpattyaoblenergo, where the UPS of the Private Branch Exchange (PBX) was shut down.[106,107] Additional impacts included the backup power to oblenergo control centers.[108]

Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, and IT Staff personnel may have been able to observe the reported pieces of evidence.

A total of three observables were identified with the use of the Device Restart/Shutdown technique (T0816). This technique is important for investigation because unexpected shutdowns and restarts prevent operators from performing required response functions. This technique appears at the end of the timeline, beyond the point at which a defender could take action to disrupt the attack.

Of the three observables associated with this technique, all 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 17 artifacts could be generated by the Device Restart/Shutdown technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff

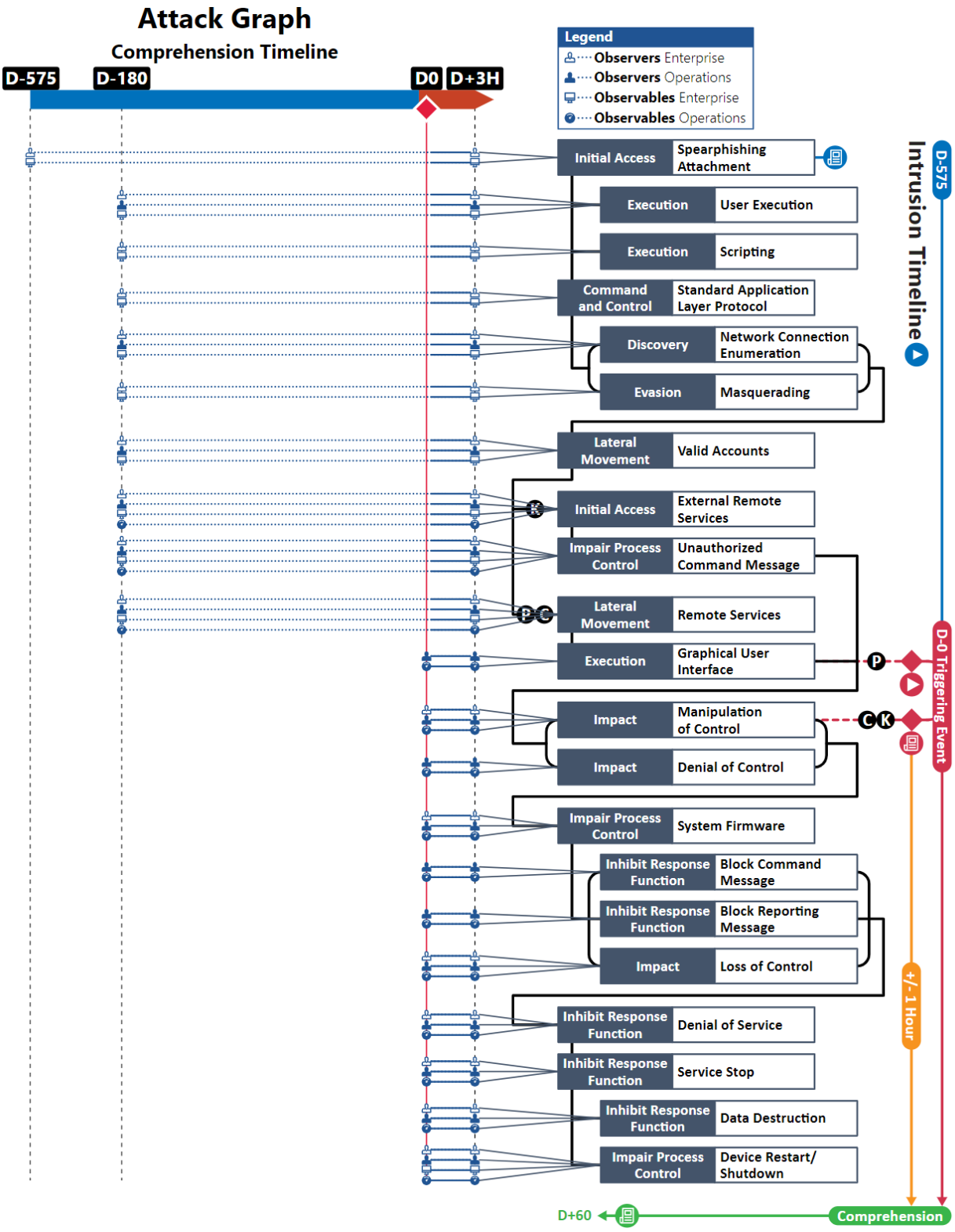


Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †.

Observables Associated with Spearphishing Attachment technique (T0865) for Initial Access	
Observable 1	Anomalous Outbound Network Connections/Downloads Over HTTP(S)
Observable 2 †	*Object Linking and Embedding (OLE) Objects in Malicious Word/Excel Docs*
Observable 3 †	*Додатюк1.xls and Associated Components: "vba_macro.exe". In Some Cases, Associated Components Included a Dropper Installer "DropbearRun.vbs"*
Observable 4 †	*$RR143TB.doc and Associated Components: "vba_macro.exe". In Some Cases, Associated Components Included a Dropper Installer "DropbearRun.vbs"*
Observable 5	Download Of PyInstaller Compiled GCat Binary
Observable 6 †	*Unusual SMTP Traffic to Google or Other Web Mail Provider. If the User Primarily Uses a Browser to Access Email, GCat Will Generate Unusual SMTP*
Observable 7 †	*File Signatures in Files Extracted from Network Traffic or Host Data Matching BlackEnergy or GCat Signatures (Example: Yara)*

Observables Associated with User Execution technique (T0863) for Execution	
Observable 1 †	*Office Documents (Word, Excel) Associated with Network Communications, Command Prompt Processes or Other Suspicious Child Process*
Observable 2 †	*HTTP or SMB Protocols Containing Known Malicious Signatures for C2 or Malware Propagation. This Might Be Seen in Network Signatures or File Signatures Associated with Extracted Files*
Observable 3 †	*Suspicious Emails with Spoofed Sender Addresses and Attachments that Prompt Users to Enable Macros When Downloaded*

Observables Associated with Scripting Technique (T0853)	
Observable 1 †	*Office Document (Word, Excel) Containing OLE or Other Scripting Object Such as "DropbearRun.vbs"*
Observable 2 †	*Network Traffic Associated with Microsoft Office (Word, Excel) Processes*
Observable 3 †	*Filenames Specific To 2015 Campaign Included Додатюк1.xls, $RR143TB.doc, VBA_macro.exe, CPLEXE.EXE (Original Name), MS-IME (Internal Name), virus_04.exe, vba_macro, icshextobin.exe, BlackEnergy.exe, 1.exe*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1 †	*Anomalous Outbound Network Connections/Downloads Over HTTP(S)*
Observable 2 †	*Microsoft Office Document (Word, Excel) Containing OLE or Other Scripting Object as Parent Process Associated to HTTP Comms to External IP*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 3	HTTP Request to IP Directly with No Associated DNS Request. This May Include an HTTP POST Request with the Following Fields: Id=[bot_id_sha1]&bid=[base64_encoded_build_id]&nm=[x]&cn=[y]&num=[z]
Observable 4 †	*SMTP Connections to Unusual or Unexpected Mail Services*

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 1 †	*Network Traffic with Scanning Behavior (Sequential Ports, High Destination to Source Port Communication Ratio, High Quantity of Partial Connections) Might Be Noted from Unusual Systems*
Observable 2 †	*Filenames specific to the 2015 Campaign Included: VS.dll, SCAN.dll, DC.dll, BS.dll*
Observable 3 †	*Anomalous Use of MS Sysinternals PsExec Tool*

Observables Associated with Masquerading Technique (T0849)	
Observable 1	Executable with Common Name Outside of Expected Folder. In this Event, the Malicious svchost.exe Malware File Was Located at C:\Windows\Temp\Syslog\ While the Legitimate svchost.exe Is Stored at C:\Windows\System32\
Observable 2 †	*Unsigned or Invalid Signature on Operating System or Application File*
Observable 3 †	*Unusual Publisher Signature on Operating System or Application File*
Observable 4	Valid Signature but Invalid or Unknown File Hash on Operating System or Application File
Observable 5	Unusual Imports or Exports on Operating System or Application File
Observable 6	Scanner Tool Executable Renamed to svchost.exe

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1 †	*Suspicious or Unusual Interactive Successful Logins to Domain-Joined Assets Observed in the Domain Controller or Target Machine's Windows Event Logs Security Log (Event 4624)*
Observable 2 †	*Suspicious or Unusual Interactive Unsuccessful Logins to Domain-Joined Assets Observed in the Domain Controller or Target Machine's Windows Event Logs Security Log (Event 4625)*
Observable 3 †	*SMB Traffic Associated with PsExec User Account Compromised. This Might Be Done with Either Elevated or User Level Accounts*
Observable 4 †	*Unusual User Account Logins, Particularly Admin Accounts Across Network Services Such as SMB*
Observable 5 †	*PsExec Process Artifacts on Destination System Associated with PSEXESVC.Exe*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 6	Movement of Suspicious Files Over SMB or Other Admin Shares
Observable 7 †	*Filenames Specific to the 2015 Campaign Included: PS.dll, SI.dll, KI.dll*
Observable 8 †	*Event ID 7045 and 4697*

Observables Associated with External Remote Services Technique (T0822)	
Observable 1 †	*VPN Application Logs Show Anomalous Account Activity*
Observable 2 †	*VPN Logon Session Metadata Shows Use of Compromised Acct*
Observable 3	Unusual Radmin Associated Process Data in Host Logs
Observable 4 †	*Network IDS/IPS Alerts Associated with Radmin Connections (Example: Snort Rule)*

Observables Associated with Unauthorized Command Message Technique (T0855)	
Observable 1	Anomalous VPN Connections
Observable 2 †	*DMS Client Application Issuing Commands Directly to DMS Server (Kievoblenergo)*
Observable 3 †	*HMI Reflects Unauthorized Process Change Inputs via radmin (Prykarpattya, Chernivtsi)*
Observable 4	PCAP Shows Unauthorized Instructions Sent to Field Controllers
Observable 5 †	*Operational Database Device/Process Alarm Triggered by Event*

Observables Associated with Remote Services Technique (T0886)	
Observable 1 †	*Increased RDP Traffic to Or from Unusual or Unexpected Hosts Observed in Network Traffic or Host Logs Details*
Observable 2	Unexpected Usage of Administrator Accounts for RDP Sessions
Observable 3 †	*Unusual Changes to Time-Of-Day RDP Access Patterns Observed in Network Traffic*
Observable 4 †	*Unusual radmin Associated Process Data in Host Logs*
Observable 5 †	*Network IDS/IPS Alerts Associated with Radmin Connections (Example: Snort Rule)*
Observable 6 †	*Users Observe Commands Being Entered and Mouse Being Moved*

Observables Associated with Graphical User Interface Technique (T0823)	
Observable 1 †	*Mouse Movement on Screen*
Observable 2 †	*HMI Reflects Unauthorized Change Inputs*

Observables Associated with Graphical User Interface Technique (T0823)	
Observable 3	Increase in RDP Traffic Associated with Remote GUI Sessions
Observable 4 †	*RDP Traffic from New or Unusual Source Host*
Observable 5 †	*RDP Traffic at Odd Hours*
Observable 6 †	*RDP Sessions from Unusual or Unexpected User*
Observable 7 †	*Inability of Users to Utilize Mouse or Keyboard*

Observables Associated with Manipulation of Control Technique (T0831)	
Observable 1 †	*Breakers Physically Changing Positions*
Observable 2 †	*Network Command Traffic Shows Unauthorized Commands Sent to Breakers*

Observables Associated with Denial of Control Technique (T0813)	
Observable 1 †	*Inability to Control Input Devices (Keyboard, Mouse, etc.) to System*
Observable 2	Modified User Passwords to Hamper Recovery Ability

Observables Associated with System Firmware Technique (T0857)	
Observable 1 †	*Unauthorized Modification Made to Device Firmware*
Observable 2	Large File or Data Transfer Directly to Convertor
Observable 3 †	*Bricked Device Due to Unsuccessful Firmware Update*
Observable 4	Control Center Systems Unable to Connect to Substation Devices

Observables Associated with Block Command Message Technique (T0803)	
Observable 1 †	*File Transfer Destined to Converter. This Doesn't Typically Occur in OT Environment*
Observable 2 †	*Firmware Upload Can Be Extracted if the Protocol Used is Supported by Passive Network Monitoring Deep Packet Inspection*
Observable 3 †	*Non-Responsive Assets and Command Message Time-Outs (as Command Messages that Depend on Corrupted Protocol Converters Will not Reach Source or Destination Assets)*

Observables Associated with Block Reporting Message Technique (T0804)	
Observable 1 †	*Non-Responsive Assets and Reporting Message Time-Outs (as Reporting Messages that Depend on Corrupted Protocol Converters Will not Reach Source or Destination Assets)*

Observables Associated with Loss of Control Technique (T0827)	
Observable 1 †	*Extraction of Binary That Matches KillDisk File Signatures in Yara or Other File Signature Tools from Extracted Files from Network Traffic or From a Host*
Observable 2 †	*Systems Remotely Inaccessible/Non-Responding*
Observable 3 †	*System Does not Boot*
Observable 4 †	*Error Messages or Application Crashes Associated with Missing Critical Files*

Observables Associated with Denial of Service Technique (T0814)	
Observable 1 †	*Flood of Calls to Operator Telephone Call Center*
Observable 2 †	*High Call Center Wait Queue*
Observable 3 †	*Inability to Dial Impacted Phone Number*
Observable 4 †	*High Utilization or Failure of Telephone Infrastructure*
Observable 5 †	*Unavailability of Telephone Services*

Observables Associated with Service Stop Technique (T0881)	
Observable 1 †	*Stopped Services Might Result in an Increase in Failed Network Connections Observed in Network Traffic (TCP Resets, etc.)*
Observable 2 †	*Inoperable Systems Might Result in an Increase in ICMP Host Unreachable or Other Network Messages Associated with an Unknown or Unavailable Host*
Observable 3 †	*Operators Might Notice That Process Functions Are not Working as Expected or That Systems Cannot Be Accessed*
Observable 4 †	*Filenames Specific to the 2015 Campaign Malware Included: svchost.exe, tsk.exe, danger, Ukranian.bin.exe, crab.exe, ololo.exe, ololo 2.exe, ololo.txt, trololo.exe, 123.txt, virus_ololo.dat*

Observables Associated with Data Destruction Technique (T0809)	
Observable 1	File Signatures from Files Extracted from Network Data or Recovered from an Endpoint Might Contain KillDisk Signature Matches (Example Yara)
Observable 2 †	*Users Unable to Login to Systems*
Observable 3 †	*Systems Crash or Throw Error Messages*
Observable 4	Absence of System Log Data
Observable 5	Absence of MBR Data

Observables Associated with Device Restart/Shutdown Technique (T0816)	
Observable 1 †	*Inability to Access Remote Services on Device Impacted by Restart/Shutdown Attack*

Observables Associated with Device Restart/Shutdown Technique (T0816)	
Observable 2 †	*Systems Inaccessible/Non-Responding*
Observable 3 †	*System Log Entries Denoting System Was Restarted / Shutdown*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Spearphishing Attachment Technique (T0865) for Initial Access	
Artifact 1	Mismatch MIME and Attachment File Extension
Artifact 2	Email Sender Address
Artifact 3	Email Message
Artifact 4	Email Receiver
Artifact 5	Email Receiver Name
Artifact 6	Email Receiver Domain
Artifact 7	Email Receiver Address
Artifact 8	Enable Macros Pop-Up
Artifact 9	Email Application Log File
Artifact 10	Email Unified Audit Log File
Artifact 11	Email Service Name
Artifact 12	Suspicious Email Message Content
Artifact 13	Operating System Service Creation
Artifact 14	Email .pst File
Artifact 15	Email .ost File
Artifact 16	Simple Mail Transfer Protocol (SMTP) Traffic
Artifact 17	Mail Transfer Agent Logs
Artifact 18	Email Parent Process
Artifact 19	Mail Transfer Agent Logs
Artifact 20	Email Parent Process
Artifact 21	Email Domain Name System (DNS) Traffic
Artifact 22	Email Domain Name System (DNS) Event
Artifact 23	File Attachment Warning Prompt
Artifact 24	Email Timestamp
Artifact 25	Email Attachment
Artifact 26	Email Attachment File Type
Artifact 27	Email Header
Artifact 28	Email Sender Name
Artifact 29	Email Sender IP Address
Artifact 30	Email Sender Domain

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

Artifacts Associated with Scripting Technique (T0853) for Execution	
Artifact 1	Files Dropped into Directory
Artifact 2	System Event Log Creation
Artifact 3	OS Timeline Event
Artifact 4	Startup Menu Modification
Artifact 5	System Processes Created
Artifact 6	Windows API Event Log
Artifact 7	Executable Files
Artifact 8	Prefetch Files Created

Artifacts Associated with Scripting Technique (T0853) for Execution	
Artifact 9	External Network Connections
Artifact 10	Network Services Created
Artifact 11	Registry Modifications
Artifact 12	OS Service Installation

Artifacts Associated with Standard Application Layer Protocol Technique (T0869)	
Artifact 1	External Network Connections
Artifact 2	DNS Autonomous System Number
Artifact 3	Increase In the Number of External Connections
Artifact 4	Network Content Metadata
Artifact 5	Network Connection Times
Artifact 6	HTTP Traffic Port
Artifact 7	DNS Traffic Port
Artifact 8	SMB Traffic Port
Artifact 9	HTTPS Traffic Port
Artifact 10	RDP Traffic Port
Artifact 11	HTTP Post Request
Artifact 12	External IP Addresses

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 1	Common Network Traffic
Artifact 2	Polling Network Traffic from Abnormal IP Sender Addresses
Artifact 3	NETBIOS Name Services Port
Artifact 4	LDAP Port
Artifact 5	Active Directory Calls
Artifact 6	Email Server Calls
Artifact 7	SMTP Port 25 Traffic
Artifact 8	DNS Lookup Queries
Artifact 9	ARP Scans
Artifact 10	TCP Connect Scan
Artifact 11	TCP SYN Scans
Artifact 12	Industrial Network Traffic

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

Artifacts Associated with Masquerading Technique (T0849)	
Artifact 1	File Creation with Common Name
Artifact 2	Additional File Directories Created
Artifact 3	Scheduled Job Modification
Artifact 4	Service Creation
Artifact 5	Services Metadata
Artifact 6	Leetspeak User Metadata
Artifact 7	Common Application with Non-Native Child Processes
Artifact 8	Process Metadata Changes
Artifact 9	Command Line Execution
Artifact 10	File Modification

Artifacts Associated with Masquerading Technique (T0849)	
Artifact 11	Warez Application Use
Artifact 12	Leetspeak File Creation
Artifact 13	Applications Causing Unintended Actions
Artifact 14	Additional Functionality in Applications

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

Artifacts Associated with External Remote Services Technique (T0822)	
Artifact 1	Remote Services Protocols
Artifact 2	VPN Connections
Artifact 3	Remote Vendor Connections
Artifact 4	Session Authentication
Artifact 5	Failed Logons Event
Artifact 6	Session Timestamp
Artifact 7	Logon Event Type
Artifact 8	Remote Session Key

Artifacts Associated with External Remote Services Technique (T0822)	
Artifact 9	System Registry Network Interfaces
Artifact 10	Remote Services Logon
Artifact 11	TLS Certificate
Artifact 12	Session Logoff Event
Artifact 13	Domain Controller Log
Artifact 14	User Account Name
Artifact 15	User Client Address
Artifact 16	Security Account Manager Registry Entries
Artifact 17	Dialog Box Pop-Up
Artifact 18	Mouse Movement
Artifact 19	Command Prompt Window Opened
Artifact 20	Security Account Manager Registry Password Hashes
Artifact 21	External IP Address
Artifact 22	User Account Creation
Artifact 23	User Privileges Change
Artifact 24	Blocked Incoming Connections Event
Artifact 25	Blocked Incoming Packet Event
Artifact 26	Encrypted Network Traffic

Artifacts Associated with Unauthorized Command Message Technique (T0855)	
Artifact 1	Protocol Specific Command Packet
Artifact 2	Machine State Change
Artifact 3	Process Restart
Artifact 4	Process Failure
Artifact 5	Network Resets
Artifact 6	Protocol Metadata Change
Artifact 7	Process Timing Change
Artifact 8	Process Logic Change
Artifact 9	MAC Addresses
Artifact 10	IP Addresses
Artifact 11	Operational Application Log
Artifact 12	Operational Data Created
Artifact 13	Process Alarm

Artifacts Associated with Unauthorized Command Message Technique (T0855)	
Artifact 14	Process Alarm Event
Artifact 15	Application Level I/O Manipulation
Artifact 16	OS Level I/O Manipulation

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 1	Remote Client Connection
Artifact 2	Logon Event
Artifact 3	Logoff
Artifact 4	Logoff Event
Artifact 5	Registry Changes
Artifact 6	Registry Connection Change
Artifact 7	Mouse Movement
Artifact 8	Unexpected
Artifact 9	Desktop Prompt Windows Created
Artifact 10	Session Cache
Artifact 11	Application Log
Artifact 12	RDP Traffic
Artifact 13	System Log Event
Artifact 14	Authentication Logs
Artifact 15	GUI Modifications
Artifact 16	Data File Size In Network Content
Artifact 17	File Movement
Artifact 18	MSSQL Traffic 1433 Port
Artifact 19	SSH Traffic
Artifact 20	SMB Traffic
Artifact 21	VNC Traffic
Artifact 22	Process Creation
Artifact 23	Remote Session Creation Timestamp
Artifact 24	Network Traffic Content Creation

Artifacts Associated with Graphical User Interface Technique (T0823)	
Artifact 1	Remote Services Protocols

Artifacts Associated with Graphical User Interface Technique (T0823)	
Artifact 2	VPN Connections
Artifact 3	Remote Vendor Connections
Artifact 4	Session Authentication
Artifact 5	Failed Logons Event
Artifact 6	Session Timestamp
Artifact 7	Logon Event Type
Artifact 8	Remote Session Key
Artifact 9	System Registry Network Interfaces
Artifact 10	Remote Services Logon
Artifact 11	TLS Certificate
Artifact 12	Session Logoff Event
Artifact 13	Domain Controller Log
Artifact 14	User Account Name
Artifact 15	User Client Address
Artifact 16	Security Account Manager Registry Entries
Artifact 17	Dialog Box Pop-Up
Artifact 18	Mouse Movement
Artifact 19	Command Prompt Window Opened
Artifact 20	Security Account Manager Registry Password Hashes
Artifact 21	External IP Address
Artifact 22	User Account Creation
Artifact 23	User Privileges Change
Artifact 24	Blocked Incoming Connections Event
Artifact 25	Blocked Incoming Packet Event
Artifact 26	Encrypted Network Traffic
Artifact 27	External MAC Address
Artifact 28	Event Log Creation
Artifact 29	Logon Event
Artifact 30	SMB Port
Artifact 31	RDP Port
Artifact 32	SSH Port
Artifact 33	Mouse Movement
Artifact 34	Cursor Movement

Artifacts Associated with Graphical User Interface Technique (T0823)	
Artifact 35	Keyboard Entries
Artifact 36	Application Execution via Input Devices
Artifact 37	Prefetch Files Created
Artifact 38	VNC Connections
Artifact 39	RDP Connections
Artifact 40	Program Executions
Artifact 41	Code Injections
Artifact 42	Host-Screen Adjustments
Artifact 43	Screen Resolution Changes
Artifact 44	SSH Connections
Artifact 45	Process Creations
Artifact 46	Service Creation
Artifact 47	Service Modification
Artifact 48	Process Input Changes
Artifact 49	JUMPLIST Creation
Artifact 50	SHELLBAG Creation
Artifact 51	System Resource Use Management Changes
Artifact 52	Network Connection Durations
Artifact 53	Changes in Bytes Sent and Received
Artifact 54	Increase CPU Cycles
Artifact 55	Host System Crash
Artifact 56	Application Usage Increase
Artifact 57	Network Bandwidth Changes
Artifact 58	Remote Client Execution

Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 1	HMI Input Manipulation
Artifact 2	Command Execution
Artifact 3	Event Log Creation
Artifact 4	Application Log Event
Artifact 5	Altered Command Sequences
Artifact 6	Application File Modification
Artifact 7	Operational Data Modification

Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 8	I/O Modification
Artifact 9	Engineering Workstation Mouse Movement
Artifact 10	Controller Set Point Change
Artifact 11	Controller Parameter Change
Artifact 12	Controller Tag Change
Artifact 13	Process State Change
Artifact 14	Process Shutdown
Artifact 15	Process Restart
Artifact 16	Process Initiated

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

Artifacts Associated with System Firmware Technique (T0857)	
Artifact 1	Firmware Update Request
Artifact 2	Device Restart
Artifact 3	Device Shutdown
Artifact 4	Protection Relay Modification
Artifact 5	Protection Relay Status Change
Artifact 6	User Account Creation
Artifact 7	Administrator Account Use
Artifact 8	Device Authentication Event
Artifact 9	Network Traffic
Artifact 10	Operations Device Failure
Artifact 11	External Network Connections to Operational Devices

Artifacts Associated with System Firmware Technique (T0857)	
Artifact 12	External Network Exchange of Data
Artifact 13	I/O Server Modifications
Artifact 14	Device Status Change
Artifact 15	Device Tag Manipulation
Artifact 16	Code Execution

Artifacts Associated with Block Command Message Technique (T0803)	
Artifact 1	New Network Connections Created
Artifact 2	Supervisory Application Log Event
Artifact 3	Supervisory Application Log Failure
Artifact 4	Application Processes Terminated
Artifact 5	Operational Data Mismatch Process Physical State
Artifact 6	Historian Data Missing
Artifact 7	Historian Data Query Failure
Artifact 8	Operational Database Event Alarms
Artifact 9	Input Failed to Change Operations Device

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

Artifacts Associated with Block Reporting Message Technique (T0804)	
Artifact 15	Operational Database Data Modification
Artifact 16	Operational Database Configuration Change
Artifact 17	Operational Process Termination
Artifact 18	Operational Process Alarm Failures

Artifacts Associated with Loss of Control Technique (T0827)	
Artifact 1	Process Alarms
Artifact 2	Machine State Change
Artifact 3	Configuration Change
Artifact 4	Set Point Failure
Artifact 5	Service Request Increases
Artifact 6	Runaway Conditions
Artifact 7	Failed Input Commands
Artifact 8	Process Environment Changes
Artifact 9	Device Failure
Artifact 10	Network Connection Loss
Artifact 11	Unresponsive I/O Conditions
Artifact 12	Process Failure
Artifact 13	Repeated Maintenance Reports

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

Artifacts Associated with Denial of Service Technique (T0814)	
Artifact 12	Operational Data Corruption
Artifact 13	Application Failure
Artifact 14	ICMP Echo Port 7 Traffic Increase

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

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 1	Program Execution
Artifact 2	Telnet Port
Artifact 3	SFTP Port
Artifact 4	FTPS Port
Artifact 5	SMB Port
Artifact 6	HTTP Port
Artifact 7	HTTPS Port
Artifact 8	Command Line Arguments
Artifact 9	SCP Port
Artifact 10	Memory Corruption
Artifact 11	Files Moved to Recycle Bin
Artifact 12	Non-Native Files

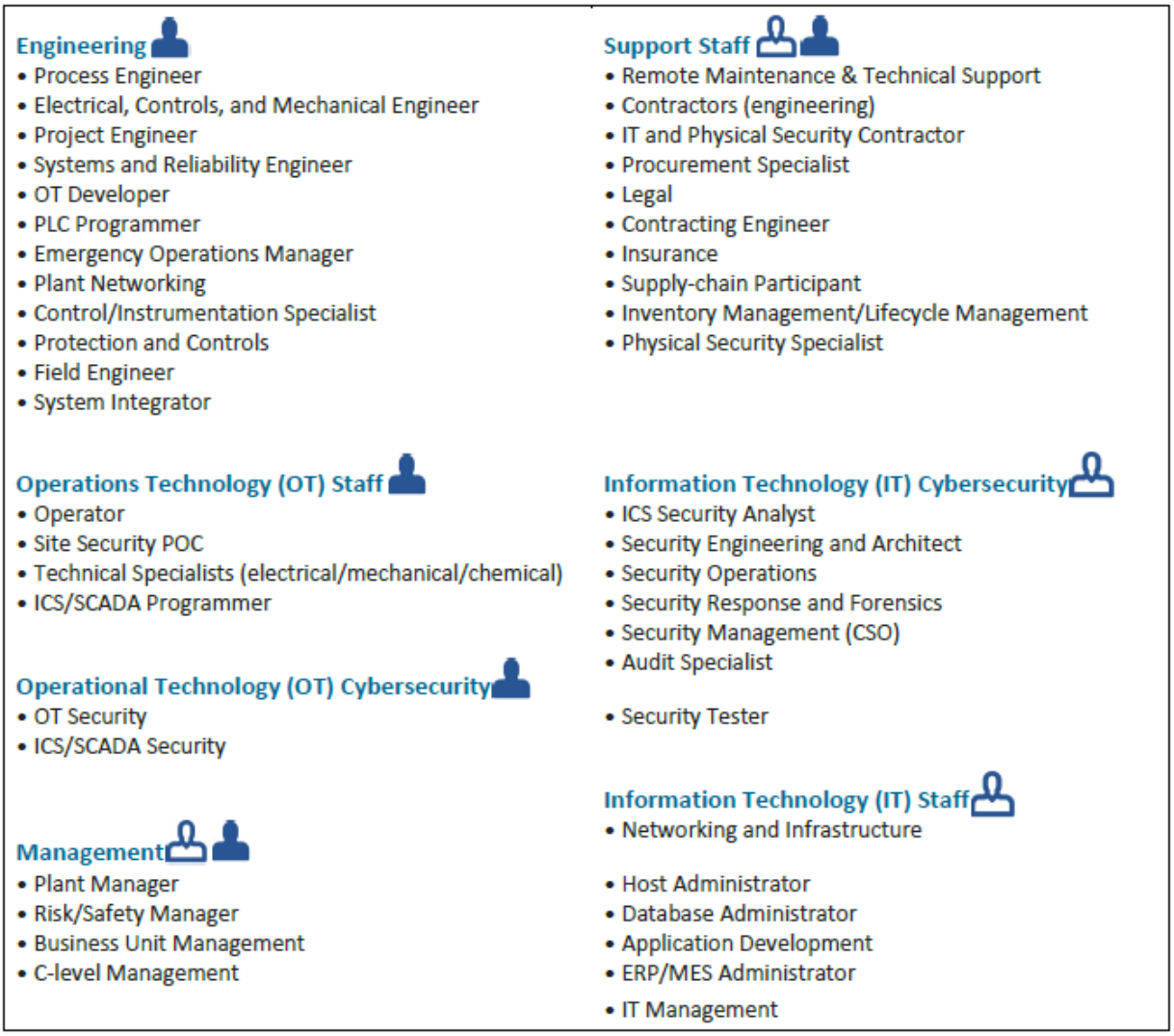
Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 13	Transient Device Connections
Artifact 14	External Network Connections
Artifact 15	Local Network Connections
Artifact 16	Host System Reboot Failure
Artifact 17	Process Logic Failure
Artifact 18	Event Log Creation
Artifact 19	System Call
Artifact 20	System Application Interruption
Artifact 21	Device Failure
Artifact 22	Recovery Attempt Failure
Artifact 23	File Encryptions
Artifact 24	Missing Files
Artifact 25	Use of File Transfer Protocols
Artifact 26	FTP Port
Artifact 27	TFTP Port

Artifacts Associated with Device Restart/Shutdown Technique (T0816)	
Artifact 1	Process Application Event
Artifact 2	Process Environmental Changes
Artifact 3	Loss of Network Connection
Artifact 4	Network Command Packets
Artifact 5	Reboot Screen
Artifact 6	Blue Screen
Artifact 7	Significant Operational Data Changes
Artifact 8	Logon Events
Artifact 9	Logoff Events
Artifact 10	Process Failure
Artifact 11	Hardware Failure
Artifact 12	Command Prompt Opened
Artifact 13	Unauthorized Input
Artifact 14	Memory Corruption
Artifact 15	Process Alarm
Artifact 16	External Network Connections

Artifacts Associated with Device Restart/Shutdown Technique (T0816)	
Artifact 17	Local Network Connections

APPENDIX C: OBSERVERS

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



REFERENCES

[1] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[2] [CysCentrum | CysCentrum | “Cyber Threat BlackEnergy 2/3. History of Attacks on Critical IT Infrastructure in Ukraine” | https://cys-centrum.com/ru/news/black_energy_2_3 | 16 January 2016 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[3] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[4] [WIRED | Kim Zetter | “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid” | https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ | 3 March 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[5] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[6] [CysCentrum | CysCentrum | “Cyber Threat BlackEnergy 2/3. History of Attacks on Critical IT Infrastructure in Ukraine” | https://cys-centrum.com/ru/news/black_energy_2_3 | 16 January 2016 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[7] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[8] [WIRED | Andy Greenberg | “Watch Hackers Take Over the Mouse of a Power-Grid Computer in Ukraine” | https://www.wired.com/story/video-hackers-take-over-power-grid-computer-mouse/ | 20 June 2017 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[9] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[10] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[11] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[12] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[13] [DHS | “IR-ALERT-H-16-056-01 Cyber attack Against Ukrainian Critical Infrastructure” | https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01 | 25 February 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[14] [Ministry of Energy and Coal Mining of Ukraine | “The Ministry of Energy and Coal Industry intends to form a group with the participation of representatives of all energy companies within the Ministry’s management to study the possibilities of preventing unauthorized interference in the operation of energy networks” | https://mpe.kmu.gov.ua/minugol/control/uk/publish/article;jsessionid=CE1C739AA046FF6BA00FE8E8A4D857F3.app1?art_id=245086886&cat_id=35109 | 2 December 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[15] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[16] [Ministry of Energy and Coal Mining of Ukraine | “The Ministry of Energy and Coal Industry intends to form a group with the participation of representatives of all energy companies within the Ministry’s management to study the possibilities of preventing unauthorized interference in the operation of energy networks” | https://mpe.kmu.gov.ua/minugol/control/uk/publish/article;jsessionid=CE1C739AA046FF6BA00FE8E8A4D857F3.app1?art_id=245086886&cat_id=35109 | 2 December 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[17] [VirusBulletin | Anton Cherepanov, Robert Lipovsky | “VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks” | https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber-attacks/ | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[18] [FireEye | “Cyber Attacks on the Ukrainian Grid: What You Should Know” | https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[19] [CysCentrum | “Cyber Threat BlackEnergy 2/3. History of Attacks on Critical IT Infrastructure in Ukraine” | https://cys-centrum.com/ru/news/black_energy_2_3 | 16 January 2016 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[20] [VirusBulletin | Anton Cherepanov, Robert Lipovsky | “VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks” | https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber-attacks/ | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[21] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[22] [Army Cyber Institute | Michael Assante | “Analysis of the Attack on the Ukrainian Power Grid” | https://www.youtube.com/watch?v=cs1V4KY5j8Y | 31 May 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[23] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[24] [DHS | “IR-ALERT-H-16-056-01 Cyber-Attack Against Ukrainian Critical Infrastructure” | https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01 | 25 February 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[25] [DHS | “IR-ALERT-H-16-056-01 Cyber-Attack Against Ukrainian Critical Infrastructure” | https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01 | 25 February 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[26] [SentinelOne | Udi Shamir | “Analyzing a New Variant of BlackEnergy 3” | https://www.sentinelone.com/wp-content/uploads/2017/06/BlackEnergy3_WP_012716_1c.pdf | June 2017 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[27] [CysCentrum | CysCentrum | “Cyber Threat BlackEnergy 2/3. History of Attacks on Critical IT Infrastructure in Ukraine” | https://cys-centrum.com/ru/news/black_energy_2_3 | 16 January 2016 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[28] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[29] [DHS | “ICS-ALERT 14-281-01E Ongoing Sophisticated Malware Campaign Compromising ICS” | https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-14-281-01B | 10 December 2014 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[30] [CysCentrum | CysCentrum | “Cyber Threat BlackEnergy 2/3. History of Attacks on Critical IT Infrastructure in Ukraine” | https://cys-centrum.com/ru/news/black_energy_2_3 | 16 January 2016 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[31] [VirusBulletin | Anton Cherepanov, Robert Lipovsky | “VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks” | https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber-attacks/ | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[32] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[33] [DHS | “ICS-ALERT 14-281-01E Ongoing Sophisticated Malware Campaign Compromising ICS” | https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-14-281-01B | 10 December 2014 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[34] [ESET WeLiveSecurity | Anton Cherepanov | “BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry” | BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry | WeLiveSecurity | 3 January 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[35] [E-ISAC and SANS | Robert M. Lee, Michael J. Assante, Tim Conway | “Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case” | https://isij.eu/article/analysis-cyber-attack-ukrainian-power-grid-defense-use-case | 18 March 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[36] [ESET WeLiveSecurity | Anton Cherepanov | “BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry” | https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/ | 3 January 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[37] [VirusBulletin | Anton Cherepanov, Robert Lipovsky | “VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks” | https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber-attacks/ | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[38] [F-Secure | “BlackEnergy & Quedagh” | https://blog.f-secure.com/wp-content/uploads/2019/10/BlackEnergy_Quedagh.pdf | October 2019 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[39] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[40] [SentinelOne | Udi Shamir | “Analyzing a New Variant of BlackEnergy 3” | https://www.sentinelone.com/wp-content/uploads/2017/06/BlackEnergy3_WP_012716_1c.pdf | June 2017 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[41] [DHS | “IR-ALERT-H-16-056-01 Cyber-attack Against Ukrainian Critical Infrastructure” | https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01 | 25 February 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[42] [VirusBulletin | Anton Cherepanov, Robert Lipovsky | “VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks” | https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber attacks/ | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[43] [CysCentrum | CysCentrum | “Cyber Threat BlackEnergy 2/3. History of Attacks on Critical IT Infrastructure in Ukraine” | https://cys-centrum.com/ru/news/black_energy_2_3 | 16 January 2016 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[44] [E-ISAC and SANS | Robert M. Lee, Michael J. Assante, Tim Conway | “Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case” | https://isij.eu/article/analysis-cyber attack-ukrainian-power-grid-defense-use-case | 18 March 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[45] [VirusBulletin | Anton Cherepanov, Robert Lipovsky | “VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks” | https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber attacks/ | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[46] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[47] [VirusBulletin | Anton Cherepanov, Robert Lipovsky | “VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks” | https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber attacks/ | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[48] [Journal of Cybersecurity | Peter Maynard, Kieran McLaughlin, Sakir Sezer | “Decomposition and sequential – AND analysis of known cyber attacks on critical infrastructure control systems” | https://doi.org/10.1093/cybsec/tyaa020 | 15 December 2020 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[49] [Software and Systems Modeling | Wenjun Xiong and others | “Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix” | https://doi.org/10.1007/s10270-021-00898-7 | 18 June 2021 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[50] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[51] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[52] [VirusBulletin | Anton Cherepanov, Robert Lipovsky | “VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks” | https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber attacks/ | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[53] [VirusBulletin | Anton Cherepanov, Robert Lipovsky | “VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks” | https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber attacks/ | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[54] [VirusBulletin | Anton Cherepanov, Robert Lipovsky | “VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks” | https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber attacks/ | 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[55] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[56] [E-ISAC and SANS | Robert M. Lee, Michael J. Assante, Tim Conway | “Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case” | https://isij.eu/article/analysis-cyber attack-ukrainian-power-grid-defense-use-case | 18 March 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[57] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[58] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[59] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[60] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[61] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[62] [E-ISAC and SANS | Robert M. Lee, Michael J. Assante, Tim Conway | “Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case” | https://isij.eu/article/analysis-cyber attack-ukrainian-power-grid-defense-use-case | 18 March 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[63] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[64] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[65] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[66] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[67] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[68] [WIRED | Andy Greenberg | “Watch Hackers Take Over the Mouse of a Power-Grid Computer in Ukraine” | https://www.wired.com/story/video-hackers-take-over-power-grid-computer-mouse/ | 20 June 2017 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[69] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[70] [WIRED | Kim Zetter | “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid” | https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ | 3 March 2016

| Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[71] [Ministry of Energy and Coal Mining of Ukraine | “The Ministry of Energy and Coal Industry intends to form a group with the participation of representatives of all energy companies within the Ministry’s management to study the possibilities of preventing unauthorized interference in the operation of energy networks” | https://mpe.kmu.gov.ua/minugol/control/uk/publish/article;jsessionid=CE1C739AA046FF6BA00FE8E8A4D857F3.app1?art_id=245086886&cat_id=35109 | 2 December 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[72] [WIRED | Kim Zetter | “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid” | https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ | 3 March 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[73] [Army Cyber Institute | Michael Assante | “Analysis of the Attack on the Ukrainian Power Grid” | https://www.youtube.com/watch?v=cs1V4KY5j8Y | 31 May 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[74] [E-ISAC and SANS | Robert M. Lee, Michael J. Assante, Tim Conway | “Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case” | https://isij.eu/article/analysis-cyber attack-ukrainian-power-grid-defense-use-case | 18 March 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[75] [TripWire | Guest Authors | “Attacks to Critical Infrastructure Are Real, & They Can be Incredibly Easy” | https://www.tripwire.com/state-of-security/ics-security/attacks-critical-infrastructure-real-can-incredibly-easy/ | 20 December 2017 | Accessed on 7 June 2022 | The Source is publicly available information and does not contain classification markings]

[76] [DHS | “IR-ALERT-H-16-056-01 Cyber-attack Against Ukrainian Critical Infrastructure” | https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01 | 25 February 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[77] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[78] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[79] [DHS | “IR-ALERT-H-16-056-01 Cyber-attack Against Ukrainian Critical Infrastructure” | https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01 | 25 February 2016 | Accessed on 1 November 2021 |This source is publicly available information and does not contain classification markings]

[80] [E-ISAC and SANS | Robert M. Lee, Michael J. Assante, Tim Conway | “Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case” | https://isij.eu/article/analysis-cyber attack-ukrainian-power-grid-defense-use-case | 18 March 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[81] [WIRED | Kim Zetter | “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid” | https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ | 3 March 2016

| Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[82] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[83] [IEEE | Gaoqi Liang and others | “The 2015 Ukraine Blackout: Implications for False Data Injection Attacks” | https://doi.org/10.1109/TPWRS.2016.2631891 | 22 November 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[84] [E-ISAC and SANS | Robert M. Lee, Michael J. Assante, Tim Conway | “Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case” | https://isij.eu/article/analysis-cyber attack-ukrainian-power-grid-defense-use-case | 18 March 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[85] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[86] [IEEE | Gaoqi Liang and others | “The 2015 Ukraine Blackout: Implications for False Data Injection Attacks” | https://doi.org/10.1109/TPWRS.2016.2631891 | 22 November 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[87] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[88] [DHS | “IR-ALERT-H-16-056-01 Cyber-attack Against Ukrainian Critical Infrastructure” | https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01 | 25 February 2016 | Accessed on 1 November 2021 |This source is publicly available information and does not contain classification markings]

[89] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[90] [E-ISAC and SANS | Robert M. Lee, Michael J. Assante, Tim Conway | “Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case” | https://isij.eu/article/analysis-cyber attack-ukrainian-power-grid-defense-use-case | 18 March 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[91] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[92] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[93] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 |

Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[94] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[95] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[96] [ESET WeLiveSecurity | Robert Lipovsky, Anton Cherepanov | “BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry” | https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/ | 4 January 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[97] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[98] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[99] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[100] [TrendMicro | Jennifer Gumban | “Trend Micro, TROJ_KILLDISK.X” | https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TROJ_KILLDISK.X/ | 28 January 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[101] [CysCentrum | CysCentrum | “Cyber Threat BlackEnergy 2/3. History of Attacks on Critical IT Infrastructure in Ukraine” | https://cys-centrum.com/ru/news/black_energy_2_3 | 16 January 2016 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[102] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[103] [Software and Systems Modeling | Wenjun Xiong and others | “Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix” | https://doi.org/10.1007/s10270-021-00898-7 | 18 June 2021 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[104] [Booz Allen Hamilton | Jake Styczynski, Nate Beach-Westmoreland | “When the Lights Went Out” | https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-

went-out.pdf | September 2016 | Accessed on 7 June 2022 | The source is publicly available information and does not contain classification markings]

[105] [E-ISAC and SANS | Robert M. Lee, Michael J. Assante, Tim Conway | “Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case” | https://isij.eu/article/analysis-cyber attack-ukrainian-power-grid-defense-use-case | 18 March 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]

[106] [INL CyberStrike | “CyberStrike Presentation” | https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:fc96744e-eea0-45ba-8be3-4f2636db394e | 2020 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[107] [IEEE | David E. Whitehead, and others | “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies” | https://ieeexplore.ieee.org/document/8090056 | 2 November 2017 | Accessed on 6 June 2022 | This source is publicly available information and does not contain classification markings]

[108] [E-ISAC and SANS | Robert M. Lee, Michael J. Assante, Tim Conway | “Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case” | https://isij.eu/article/analysis-cyber attack-ukrainian-power-grid-defense-use-case | 18 March 2016 | Accessed on 7 June 2022 | This source is publicly available information and does not contain classification markings]