DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

PRECURSOR ANALYSIS REPORT: CYBER ATTACK ON THYSSENKRUPP BLAST FURNACE 2014

Cybersecurity for the Operational Technology Environment (CyOTE)

31 DECEMBER 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

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

TABLE OF CONTENTS

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: CYBER ATTACK ON THYSSENKRUPP BLAST FURNACE 2014

1. EXECUTIVE SUMMARY

The Cyber Attack on Thyssenkrupp Blast Furnace 2014 Precursor Analysis Report leverages publicly available information about the Thyssenkrupp Steel Mill cyber attack and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

In December 2014, the German Government's Federal Office for Information Security (BSI) released a report detailing a cyber attack on a German steel mill that occurred earlier that year, though exact dates and details of the attack were not revealed. While the report did not specify the name of the company, multiple sources identified the victim as one of Europe's largest steel manufacturers, Thyssenkrupp AG.[1,2] Further, Thyssenkrupp announced on 16 May of that year that Europe's largest blast furnace, "Schwelgern 2," located at its facility in Duisburg, Germany, would be offline for several weeks for repairs and upgrades,[3] suggesting Schwelgern 2 was likely the target of the attack.

The attack began in early 2014, when adversaries infiltrated the victim steel mill's Information Technology (IT) network via a spearphishing campaign, then worked their way into the Operational Technology (OT) environment, where they executed software that caused denial of service, denial of control, and eventually a loss of control. This led to the blast furnace shutting down without proper safety procedures, resulting in catastrophic physical damage. No lives were lost in the incident, but ThyssenKrupp suffered $4 million in damage to the blast furnace and an additional $6 million in lost revenue.[5]

The adversaries required specialized knowledge and expertise in steel production, which enabled them to compromise a variety of internal systems and components across both IT and OT networks. The attack also demonstrated detailed knowledge of the industrial control systems (ICS) and production processes being used. This combination resulted in one of the earliest known publicly reported cybersecurity incidents resulting in physical damage to ICS equipment.

Researchers and analysts identified 19 unique techniques (used in a sequence of 20 steps) utilized during the attack with a total of 454 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Fifteen of the identified techniques used during the Thyssenkrupp cyber attack were precursors to the triggering event. Analysis identified 369 observables associated with these precursor techniques, 316 of which were assessed to have an increased likelihood of being perceived in the 120 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

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

2. INTRODUCTION

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

2.1. APPLYING THE CYOTE METHODOLOGY

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

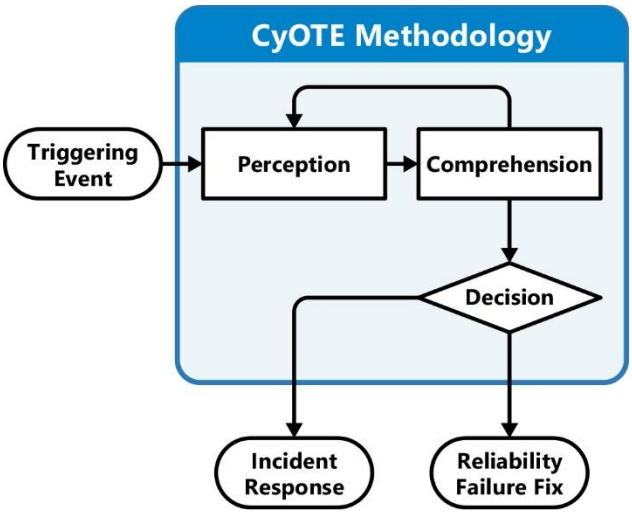


Figure 1. CyOTE Methodology

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

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

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

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

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

2.2. BACKGROUND ON THE ATTACK

In early 2014, adversaries infiltrated a ThyssenKrupp steel mill, located in Duisburg, Germany, through its Information Technology (IT) network before pivoting to the Operational Technology (OT) environment.

CyOTE analysts and researchers assess that the initial access was via spearphishing and drive-by compromise sometime between 15 January (D-120) and 30 April (D-16). Operators interacted with links and attachments that ran malicious code sometime between 15 January (D-120) and 30 April (D-16), but most likely around 14 February (D-91).[a]

After obtaining initial access, Havex malware was installed on local IT hosts. Havex is used primarily for theft of operational data during espionage campaigns and utilizes active scanning across multiple industrial network protocols.

Havex established a remote connection to the adversaries' command and control (C2) server, which enabled system reconnaissance through discovery and enumeration of devices connected to control system workstations. The adversaries used valid credentials to move laterally through the network and collected information from operational systems, such as the blast furnace controls. These events likely happened over the course of at least three months (D-91 to D-0).

A timeline of adversarial techniques is shown in **Error! Reference source not found.**. 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.

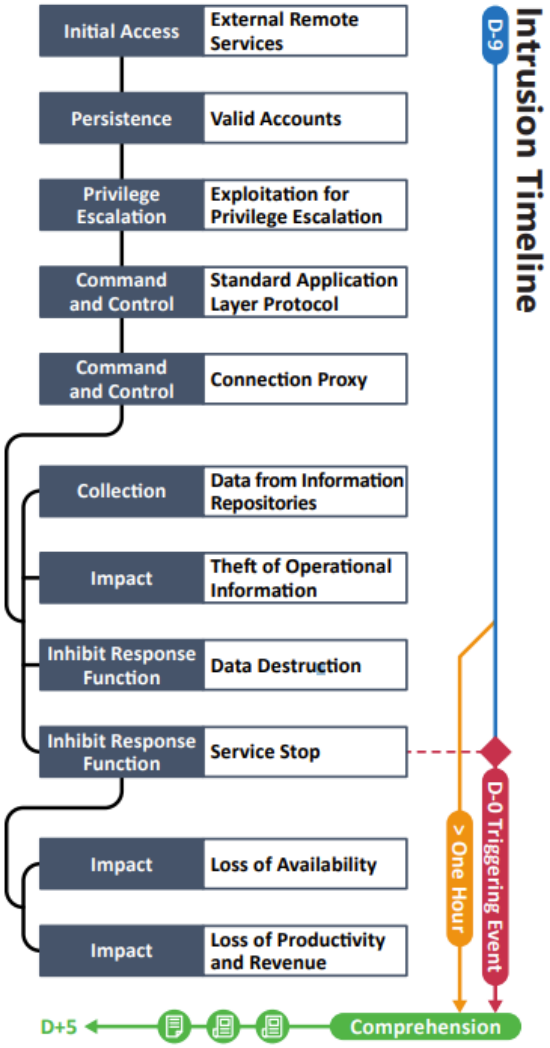


Figure 2. Intrusion Timeline

Havex's active scanning likely caused a denial of service (DoS) to the mill's OT systems. The blast furnace was 21 years old in 2014, and the OT systems were not designed to handle repeated network scanning from malware like Havex, which likely resulted in a loss of control and loss of safety during the attack. The loss of control led to the furnace overheating beyond its standard temperature (2,000° F), resulting in what BSI described as "massive damage" to the mill.[8] Thyssenkrupp announced on 16 May at 03:36 AM (Berlin Time) (D-0) that Europe's largest blast furnace, "Schwelgern 2", located at its facility in Duisburg, Germany, would be offline for several weeks for necessary repairs and upgrades.

[a] Cybersecurity researchers assessed that versions 40 through 44 of Havex malware were active during this time, and the list of targeted victims included a German manufacturer.[7] Further details on Havex can be found in the *Havex Malware in a U.S. Manufacturing Facility 2014 Precursor Analysis Report*.

This chain of events ultimately incurred $4 million in repair costs and another $6 million in lost revenue after the announced shutdown on 16 May (D-0).[9] ThyssenKrupp returned the blast furnace to service on 20 October (D+157), with the first public report on the cyber attack emerging on 18 December (D+216).

Analysis identified 20 unique techniques in a sequence and timeframe likely used by adversaries during this cyber attack (**Error! Reference source not found.** 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Thyssenkrupp Blast Furnace 2014 Cyber Attack

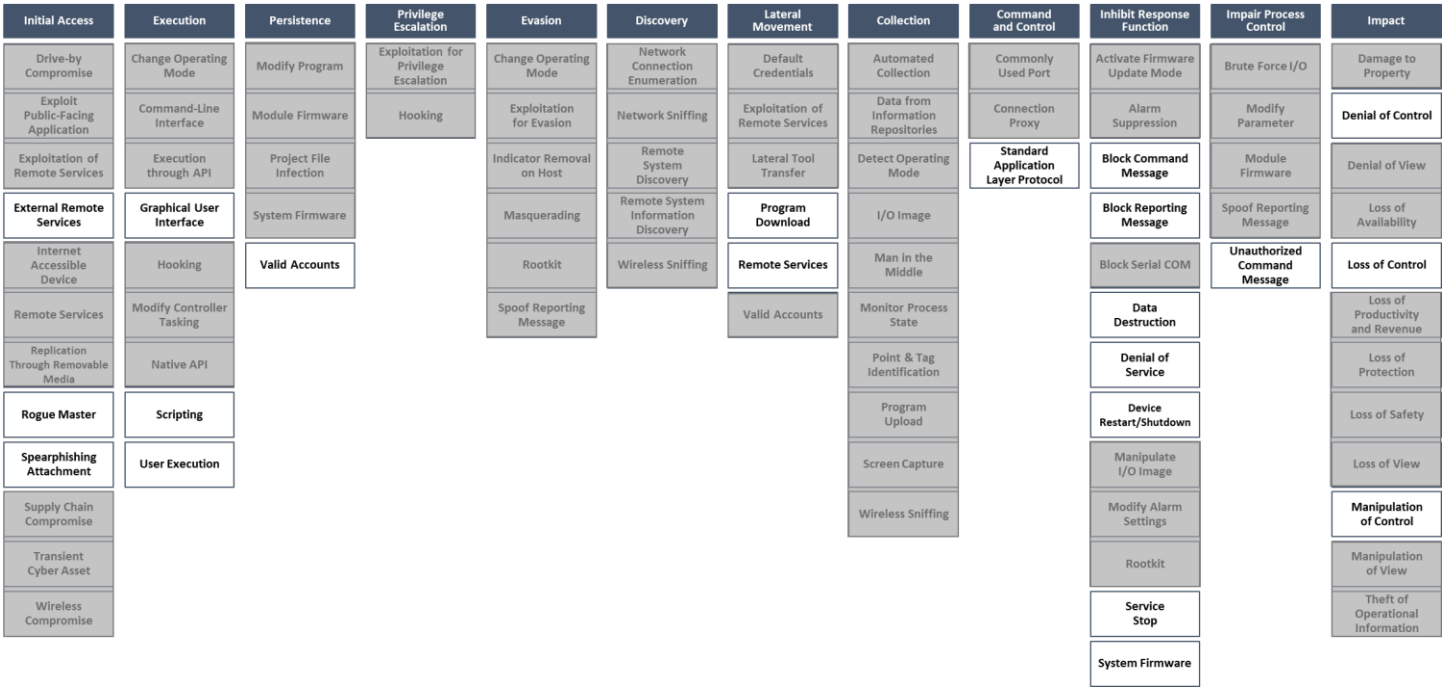


Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	**20**
Technique Observables	**454**
Precursor Techniques	**15**
Precursor Technique Observables	**369**
Highly Perceivable Precursor Technique Observable	**316**

3. OBSERVABLE AND TECHNIQUE ANALYSIS

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

3.1. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS

The adversaries used an extensive spearphishing campaign which targeted multiple members of the mill's OT staff. The spearphishing emails appeared to be from users internal to the organization and enticed the recipients to interact with the anomalous email messages. The adversaries utilized this spearphishing campaign to gather victim credentials, including enterprise usernames and passwords.[10]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe the spearphishing campaign that included both spam emails and emails from trusted sender addresses.

A total of 11 observables were identified with the use of the Spearphishing Attachment technique (T0865). This technique is important for investigation because it is often one of the first techniques an adversary uses to gain initial access to a target environment. This technique appears early in the timeline and responding to it will eliminate an additional initial access vector. Terminating the chain of techniques at this point would limit adversaries' ability to access other internal systems.

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

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

[b] 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. DRIVE-BY COMPROMISE TECHNIQUE (T0817) FOR INITIAL ACCESS

The adversaries also utilized drive-by compromises to spread and install the malware in targeted environments.[12] The adversaries employed anomalous links within spam emails and several exploit kits to redirect the user's browser session to a second website that hosted the Havex payload.[13] Once the user's browser visited the compromised site, the victim's machine downloaded and executed Havex malware automatically. The adversary targeted and infected websites of interest to the victims, which increased the likelihood a victim would interact with the compromised site.[14]

IT Cybersecurity, IT Staff, OT Cybersecurity, OT Staff, Support Staff, and Engineering personnel may have been able to observe the email requiring security credentials after the users interacted with an object.

A total of 36 observables were identified with the use of the Drive-By Compromise technique (T0817). This technique is important for investigation because it provides the malware access to the host. This technique appears early in the timeline and responding to it would effectively halt the adversaries' initial access and persistence. Terminating the chain of technique at this point would prevent the malware from infecting the host, limiting operational damage in both the IT and OT environments.

Of the 36 observables associated with this technique, 35 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 24 artifacts could be generated by the Drive-By Compromise technique
Technique Observers	IT Cybersecurity, IT Staff, OT Cybersecurity, OT Staff, Support Staff, Engineering
Resources	Technique Detection References

3.3. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

The spearphishing emails targeted various users associated with blast furnace operations, enticing recipients to click on either an object, such as a Uniform Research Locator (URL) or an attachment, such as a PDF or Microsoft Office document. Once the user clicked on the object, it established a network connection with an anomalous external client. The external client then prompted the user via the internal client to input their credentials in a web-based application.

By interacting with the malicious email, the end user triggered the download and installation of Havex malware onto a host. The sequence followed an end user interacting with malicious email attachments in spearphishing emails, visiting a compromised website in a browser, and installing a trojan-infected update from an Original Equipment Manufacturer (OEM).[11]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe the email requiring security credentials after the users interacted with an object.

A total of 37 observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation because it allows the malware access to the host. 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' lateral movement. 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 37 observables associated with this technique, 30 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

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

The adversaries used the Standard Application Layer Protocol technique (T0869) to establish communications between the victim's environment and external servers over Hypertext Transfer Protocol (HTTP). The victim's internal host then communicated over Object Linking and Embedding (OLE) for Process Control (OPC) to discover, enumerate, and communicate with ICS controls in the blast furnace OT environment.[15,16]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity may have been able to observe anomalous network connections over HTTP or Simple Mail Transfer Protocol (SMTP), or Domain Name System (DNS) requests to anomalous external URLs.

A total of 43 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 continues throughout the rest of the attack sequence and responding to it will degrade adversarial external C2 communications. Terminating the chain of techniques at this point would end the adversaries' ability to exfiltrate sensitive information.

Of the 43 observables associated with this technique, 39 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.5. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

The spearphishing emails and social engineering techniques provided the adversaries with opportunities to collect valid credentials from employees in the OT environment.[17] Once a victim clicked on the URL or malicious attachment, it executed code that gathered credentials, allowing adversaries to have continued access to control systems that relied on OPC communications to control and monitor the blast furnace.

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe an increased number of logins with multiple accounts not associated with known legitimate user activity. These observers would be able to follow up with users to ensure anomalous account usage reflected their actual behavior. Valid account usage by adversaries is difficult to perceive without observers auditing account usage.

A total of 11 observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it is the primary mechanism by which the adversary propagates through the network toward more critical systems. This activity is typically seen in the transition from the early stage to middle stage in the chain of techniques and identifying this technique will limit the adversaries' continued presences on hosts throughout the network.

Of the 11 observables associated with this technique, 10 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

Please see Appendix A for the list of observables.

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

3.6. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

Havex writes itself to the host in the %AppData%, %TEMP%, or %System32% directories and creates an auto-start registry key.[24] This step establishes persistence for the adversary on the host even after the system reboots.

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

A total of 31 observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because changes to the native system could indicate remote execution of an adversary. This technique appears early and continues to the late stages because it occurs any time the malware is written to a host; responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access.

Of the 31 observables associated with this technique, 29 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.7. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

To gain insight into the target's environment, Havex malware utilized network scanning capabilities through the remote system discovery (T0846) technique. Havex can identify networked assets in the Local Area Network (LAN) using Windows Network (Wnet) calls.[18,19] The malware helped adversaries discover assets that rely on OPC for communications from control system endpoints to the supervisory workstation. The Havex modules included capabilities to target systems over ISO-TAP/Siemens S7Com, Modbus, Measuresoft ScadaPRO Monitoring, 7-Technologies Interactive Graphical Scada System (IGSS), WellinTech KingSCADA Monitoring, Ethernet Industrial Protocol (IP), Cisco OS Common Industrial Protocol (CIP) Messaging, Rockwell Automation ControlLogix Messaging, Remote Procedure Call (RPC), and OPC protocols. Outputs of this baseline scanning activity determine what types of assets the Havex malware will scan for next and are discussed in subsequent technique sections.

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe anomalous network connections from internal hosts to other internal hosts, in both the IT and OT environments. The protocols used for discovering various targeting hosts would come from hosts that do not normally request connections from one other.

A total of 28 observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation because if the defenders can prevent the adversary from collecting system information then the adversary will have to use more complicated techniques to understand the victim's network. This technique appears in the middle and late stage of the timeline and responding to it will help identify and scope which hosts the adversaries have infected and which hosts they are targeting. In so doing, defenders may be able to prevent continual scanning and contain infected hosts. If the defenders identify and contain this activity, they could degrade the adversaries' ability to discover hosts, remotely connect, or collect operational information from compromised machines. Terminating the chain of techniques at this point would limit the adversaries' ability to identify systems with operational information.

Of the 28 observables associated with this technique, 21 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

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

After mapping the victim's general network topography, Havex malware scans hard-coded ports commonly used in OT environments, such as TCP/IP Ports 102 (Siemens S7), 502 (Schneider Electric), and 44818 (Rockwell Automation).[20] Havex also scans for Microsoft Distributed Component Object Model (COM/DCOM) interfaces.[21,22] If Havex receives a response to its COM/DCOM requests, then the malware requests specific system information such as Unique System ID, OS Version, Username, Computer Name, Country, Language, Current IP Address, list of drives, default browser, running processes, proxy settings, user agent, email names, Basic Input/Output System (BIOS) version and date, and a list of files and folders from Desktop, My Documents, Program Files Folder, and Root Directories on all drives.[23]

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

A total of 27 observables were identified with the use of the Remote System Information Discovery technique (T0888). This technique is important for investigation because it provides adversaries detailed information about target devices, allowing them to attack with enhanced specificity. This technique appears near the middle of the timeline and responding to it will prevent adversaries from properly identifying intended target devices. Terminating the chain of techniques at this point would limit data exfiltration and possibly operational damage.

Of the 27 observables associated with this technique, 22 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 8 artifacts could be generated by the Remote System Information Discovery technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity
Resources	Technique Detection References

3.9. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

The adversaries collected credential information using Havex modules on compromised, legitimate websites and exported these credentials to C2 servers.[25] Adversaries used harvested credentials to move progressively from the company's IT network to the blast furnace OT network.[26]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe an increase in logons of user accounts moving from system to system across enterprise and operations environments.

A total of 24 observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it is the primary mechanism by which the adversary propagates through multiple networks. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit adversarial movement through the OT network.

Of the 24 observables associated with this technique, 21 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.10. POINT AND TAG IDENTIFICATION TECHNIQUE (T0861) FOR COLLECTION

After determining if a networked asset responds to COM/DCOM traffic, Havex collects information specific to OPC assets and control system Point and Tag information. OPC allows Windows-based software to interact across numerous proprietary vendor protocols, simplifying inter-device communications within modern industrial environments. OPC assets use labels known as “points” and “tags” to reference various aspects of an OPC server or client. “Points” include values such as inputs, outputs, and other process-specific values and “tags” are labels given to various points for operator convenience. The malware targets control system attributes such as server state, class identification, tag name, type, access, and identification number.[27]

OT Staff, OT Cybersecurity, Support Staff, and Engineering personnel may have been able to observe unusual scanning from previous techniques, as well as anomalous OPC traffic. OPC Data Access (DA) is documented to run on TCP Port 135 but there are other ephemeral port configurations depending on facility requirements.

A total of 16 observables were identified with the use of the Point and Tag Identification technique (T0861). This technique is important for investigation because if the defender is aware of this collection, they can comprehend which system(s) adversaries are targeting. This OPC access and control system Point and Tag information would be key to an adversary for either industrial espionage or as preparation for more tailored malicious cyber activity against that facility. This technique appears in the middle of the timeline and responding to it will effectively halt future events. Terminating the chain of techniques at this point would prevent further collection of operational data.

All 16 observables are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 53 artifacts could be generated by the Point and Tag Identification technique
Technique Observers	OT Staff, OT Cybersecurity, Support Staff, Engineering
Resources	Technique Detection References

3.11. AUTOMATED COLLECTION TECHNIQUE (T0802) FOR COLLECTION

Once the adversaries mapped the victim's network and enumerated OPC assets, the malware then automatically collected data as it compiled the results, encrypted the data, and sent it to a C2 server. Havex outputs the scan results into a .txt file with the name of the OPC asset it identifies, such as OPCServer[random].txt.dat, encrypts the .txt file in the %TEMP% directory, then sends the output to an external C2 server.[28,29,30]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe the presence of anomalous text files in the %TEMP% directory with device-specific information, as well as anomalous outbound traffic to external servers.

A total of 20 observables were identified with the use of the Automated Collection technique (T0802). This technique is important for investigation because it provides adversaries detailed information about target devices, allowing them to attack with enhanced specificity. This technique appears near the middle of the timeline and responding to it will prevent adversaries from properly identifying intended target devices. Terminating the chain of techniques at this point would limit data exfiltration and possibly operational damage.

Of the 20 observables associated with this technique, 18 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

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

Havex infection led to multiple OPC platforms crashing, likely due to Havex's OPC scanning capabilities. [31,32] The blast furnace the control systems were 21 years old in 2014 and were not designed to handle repeated network scanning from malware like Havex. In such cases, a temporary unintended DoS effect could cause a denial of control incident for assets reliant on OPC for operation and control.[32]

OT Staff, OT Cybersecurity, Support Staff and Engineering personnel may have been able to observe OPC clients or servers behaving anomalously or not functioning properly when in use.

A total of 33 observables were identified with the use of the Denial of Service technique (T0814). This technique is important for investigation because abnormal behavior of OPC clients or servers could indicate disruption of those OT devices. This technique appears in the middle of the attack and terminating the chain of techniques at this point would limit the adversaries' ability to cause operational damage, even if unintended, with the malware.

All 33 observables are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.13. COMMONLY USED PORTS TECHNIQUE (T0885) FOR COMMAND AND CONTROL

For C2 traffic, Havex uses HTTP over TCP/IP Port 80 to communicate with C2 servers.[34]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel would likely be able to observe C2 traffic, especially if Havex is attempting to communicate from a properly segmented production environment.

A total of 10 observables were identified with the use of the Commonly Used Ports technique (T0885). This technique is important for investigation each time it appears throughout the attack timeline, as it allows defenders a greater opportunity to detect network activity between the malware and its C2 infrastructure. This technique is usually established early in the timeline and continues throughout the late stages of the attack. Terminating the attack chain here could either identify malicious activity in a victim's environment or prevent the malware from exfiltrating operational information to a C2 server.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 5 artifacts could be generated by the Commonly Used Ports technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.14. THEFT OF OPERATIONAL INFORMATION TECHNIQUE (T0882) FOR IMPACT

After the automated reconnaissance is complete, Havex exfiltrates the output of its activities to an external C2 server. In addition to mapping network infrastructure and identifying OPC assets, Havex malware can also harvest credentials from applications such as email clients and web browsers used in enterprise environments. Havex outputs the results of its reconnaissance module into a .txt file, and then encrypts the .txt file into YuleLog Data Format (.yls), which helps ensure a casual observer would not know the true purpose of the file.[35]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe anomalous file extensions, such as .yls, located in the %TEMP% directory, as well as outbound network traffic to an unknown external server.

A total of 19 observables were identified with the use of the Theft of Operational Information technique (T0882). This technique is important for investigation because it is a critical point at which adversaries obtain sensitive data that enables malicious behaviors through the end of the timeline. This technique appears mid-timeline and responding to it will prevent denial and loss of control to OT devices. Terminating the chain of techniques at this point would safeguard sensitive data and preserve the ability of OT devices to operate normally.

Of the 19 observables associated with this technique, 15 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 4 artifacts could be generated by the Theft of Operational Information technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

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

Havex wipes files from disk to avoid detection after conducting its reconnaissance on an infected host. The malware writes files to disk in the %TEMP%, %System32%, and %AppData% directories, and deletes the files once the output of its automated reconnaissance is sent to a C2 server.[36]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe anomalous outbound network traffic, system event logs listing details of that traffic, and the erasure of data.

A total of 22 observables were identified with the use of the Indicator Removal on Host technique (T0872). This technique, which may be difficult to detect, is important for investigation because it helps conceal the presence of adversaries on an infected network. This technique appears late in the timeline and its use would conceal the presence of adversaries on host systems. Missing files associated with external network connections would support a decision to investigate adversarial behavior.

Of the 22 observables associated with this technique, 15 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.16. DENIAL OF CONTROL TECHNIQUE (T0812) FOR IMPACT

As a result of the DoS on assets that were reliant on OPC (as described in 3.12 Denial of Service Technique (T0814)), operators were not able to control assets in the blast furnace OT environment.

OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe anomalous network traffic between hosts and loss of control to the ICS Programmable Logic Controllers (PLC), alarm Safety Instrumented Systems (SIS), and Human Machine Interfaces (HMI).

A total of 34 observables were identified with the use of the Denial of Control technique (T0812). This technique is important for investigation because it is the first technique that limits the operators' ability to ensure the safety and reliability of critical OT systems. This technique appears late in the timeline and represents the triggering event for this case study, as there are no preventative measures the victim could take at this point. To prevent catastrophic failure, operators would have to bypass the disabled OT devices.

All 34 observables are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.17. LOSS OF CONTROL TECHNIQUE (T0827) FOR IMPACT

As a result of the triggering event, operators lost their ability to control OPC reliant assets in the blast furnace OT environment. Blast furnaces are intended to run continuously over the course of decades, and loss of control systems, even if only temporary, can cause a significant impact to planned operations and safety.[37] Loss of control likely resulted in an uncontrolled shutdown of the steel mill's blast furnace.

OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe anomalous network traffic between hosts and loss of control to the PLCs, SISs, and HMIs.

A total of 34 observables were identified with the use of the Loss of Control technique (T0827). This technique is important for investigation because it prevents victim organizations from controlling further damage to the affected physical systems. This technique appears late in the timeline, after the triggering event. Successfully returning the systems to normal operations is the only way to prevent further damage or loss.

All 34 observables are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.18. LOSS OF SAFETY TECHNIQUE (T0880) FOR IMPACT

As the Havex malware caused the loss of control to proliferate throughout the steel mill's OT environment, safety shutdown controls became unavailable.[38] Steel manufacturers rarely shut down blast furnaces and the process includes steps to both schedule and confirm a shutdown before starting the process. A safe "blowdown" procedure gradually cools down the furnace, without recharging, before it can be considered as safely shut down.[39] In this case, the blowdown process failed to initiate, and is likely what led to a loss of control and loss of safety during the attack.[40]

OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe system alarms and pressure build-up in sensors and gauges as the furnace failed to shut down properly.

A total of 11 observables were identified with the use of the Loss of Safety technique (T0880). This technique is important for investigation because the malware not only disrupted normal operations of the plant, but also prevented implementation of the safety procedures intended to safely shut down the blast furnace. This technique appears late in the timeline and responding to it may prevent further physical damage. Terminating the chain of techniques at this point would minimize physical damage to equipment and prevent potential loss of life.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 3 artifacts could be generated by the Loss of Safety technique
Technique Observers	OT Staff, OT Cybersecurity, Engineering
Resources	Technique Detection References

3.19. DAMAGE TO PROPERTY TECHNIQUE (T0879) FOR IMPACT

According to BSI, the attack left the blast furnace in an "undefined state" with "massive damage" to the furnace and ICS systems.[41]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe the physical damage.

A total of three observables were identified with the use of the Damage to Property technique (T0879). This technique is important for investigation because adversarial behavior not only causes reliability failures, but physical damage, as well. If the victim does not comprehend that the adversary is causing the damage, additional associated losses might be incurred. This technique appears at the end of the timeline and responding to it may mitigate recovery costs and loss of revenue. Terminating the chain of techniques at this point would only limit the future impact on OT infrastructure and systems remaining under control.

All three observables assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 18 artifacts could be generated by the Damage to Property technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management
Resources	Technique Detection References

3.20. LOSS OF PRODUCTIVITY AND REVENUE TECHNIQUE (T0828) FOR IMPACT

Beyond the physical damage sustained by the blast furnace, the steel mill suffered financial losses from the cost of repair and lost revenues while the furnace was inoperable. The estimated cost of repair for the blast furnace and ICS equipment was roughly $4 million, and Thyssenkrupp's lost revenue and productivity totaled another $6 million.[42]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe loss of revenue and productivity while repairs were taking place.

A total of four observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation because it reveals the financial exposure to cyber-physical adversarial behavior. If adversarial behavior is not identified as a contributing cause, continued adversarial behavior may cause additional physical and financial impacts to the victim. This technique appears at the end of the timeline and responding to it will include efforts to regain operational functionality and resume normal operation.

All four observables are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 5 artifacts could be generated by the Loss of Productivity and Revenue technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management
Resources	Technique Detection References

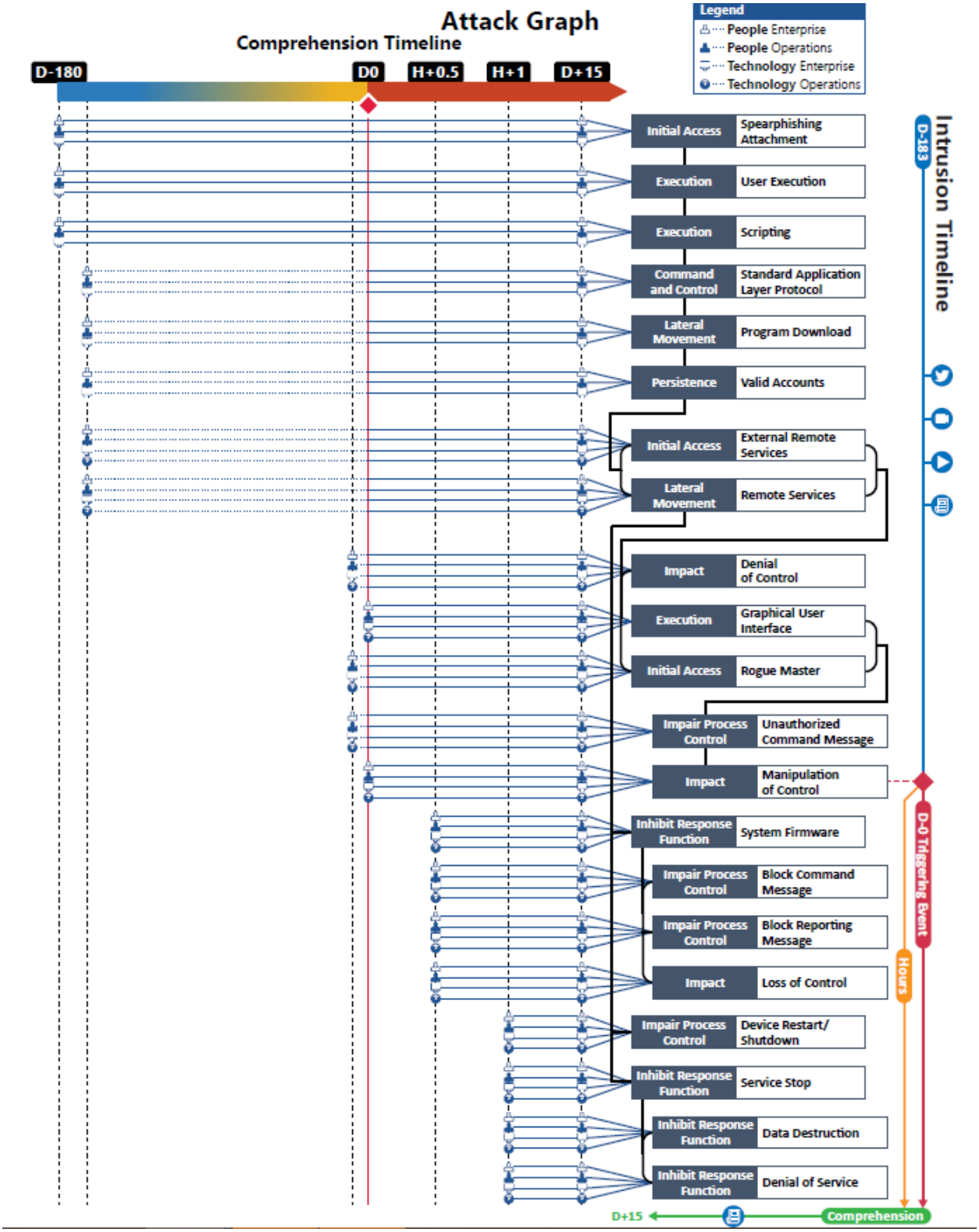


Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †.

Observables Associated with Spearphishing Technique (T0865)	
Observable 1 †	Anomalous Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80
Observable 2	Anomalous Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 3	Presence of Anomalous Email: Attachment Containing Anomalous Code from Trusted Source: Portable Document Format (.pdf) from Steel Manufacturing Partners
Observable 4	Presence of Anomalous Email: Attachment Containing Anomalous Code from Trusted Source: Extensible Markup Language (.xml) From Steel Manufacturing Partners
Observable 5	Presence of Anomalous Email: Attachment Containing Anomalous Code from Trusted Source: Extensible Markup Language Data Package (.xdp) from Steel Manufacturing Partners
Observable 6	Presence of Anomalous Email: Attachment Containing Anomalous Code from Trusted Source: From Domain Outside of Network: Gmail.com
Observable 7 †	Presence of Anomalous Email: SPAM Email with Anomalous Universal Resource Locator (URL): http://adultfriendfrance.com/wp-includes/pomo/src.php
Observable 8 †	Presence of Anomalous Email: SPAM Email with Anomalous Universal Resource Locator (URL): http://adultfrienditaly.com/wp-includes/pomo/src.php
Observable 9 †	Presence of Anomalous Email: SPAM Email with Anomalous Universal Resource Locator (URL): http://disney.freesexycomics.com/
Observable 10	Presence of Anomalous Email: Anomalous Subject Line Content: "The Account"
Observable 11	Presence of Anomalous Email: Anomalous Subject Line Content: "Settlement of Delivery Problem"

Observables Associated with Drive-by Compromise Technique (T0817)	
Observable 1 †	Anomalous Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80
Observable 2	Anomalous Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 3 †	Presence of Anomalous Email on Local Host: SPAM Email with Anomalous Universal Resource Locator (URL): http://adultfriendfrance.com/wp-includes/pomo/src.php
Observable 4 †	Presence of Anomalous Email on Local Host: SPAM Email with Anomalous Universal Resource Locator (URL): http://adultfrienditaly.com/wp-includes/pomo/src.php
Observable 5 †	Presence of Anomalous Email on Local Host: SPAM Email with Anomalous Universal Resource Locator (URL): http://disney.freesexycomics.com/

Observables Associated with Drive-by Compromise Technique (T0817)	
Observable 6 †	User Interaction with Anomalous Email: Selects Anomalous Universal Resource Locator (URL): http://adultfriendfrance.com/wp-includes/pomo/src.php
Observable 7 †	User Interaction with Anomalous Email: Selects Anomalous Universal Resource Locator (URL): http://adultfrienditaly.com/wp-includes/pomo/src.php
Observable 8 †	User Interaction with Anomalous Email: Selects Anomalous Universal Resource Locator (URL): http://disney.freesexycomics.com/
Observable 9 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://adultfriendfrance.com/wp-includes/pomo/src.php
Observable 10 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://adultfriendfrance.com/wp-includes/pomo/src.php: Over Hypertext Transfer Protocol (HTTP) TCP Port 80
Observable 11 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://adultfrienditaly.com/wp-includes/pomo/src.php
Observable 12 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://adultfrienditaly.com/wp-includes/pomo/src.php: Over Hypertext Transfer Protocol (HTTP) TCP Port 80
Observable 13 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://disney.freesexycomics.com/
Observable 14 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://disney.freesexycomics.com/: Over Hypertext Transfer Protocol (HTTP) TCP Port 80
Observable 15 †	Anomalous Network Traffic: Bi-directional Traffic Over Hypertext Transfer Protocol (HTTP) TCP 80 From External Internet Protocol (IP) Address: 91.239.206
Observable 16 †	Anomalous Network Traffic: Bi-directional Traffic Over Hypertext Transfer Protocol (HTTP) TCP 80 From External Internet Protocol (IP) Address: 23.253.126.58
Observable 17 †	Anomalous Network Traffic: Bi-directional Traffic Over Hypertext Transfer Protocol (HTTP) TCP 80 From External Internet Protocol (IP) Address: 104.239.157.210
Observable 18 †	Anomalous Network Traffic: Bi-directional Traffic Over Hypertext Transfer Protocol (HTTP) TCP 80 From External Internet Protocol (IP) Address: 85.17.156.37
Observable 19 †	Anomalous Network Traffic: From Local Host to External Server: Over Domain Name System (DNS) UDP/TCP Port 53: Request for Anomalous Domain: Yell[.]ge
Observable 20 †	Anomalous Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: GET Request from Domain: http://Yell[.]ge/blogs/wp-content/plugins

Observables Associated with Drive-by Compromise Technique (T0817)	
	/buddypress/bp-settings/bpsettings-src.php?id=18554534288436177420090FD80-c8a7af419640516616c342b13efab&v1=043&v2=170393861&q=45474bca5c3a10c8e94e56543c2bd
Observable 21 †	*Anomalous Network Traffic: From External Web Server to Local Host: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: POST Response from Domain: <html> <head> <mega httpequiv='CACHE-CONTROL' content='NO-CACHE'></head><body>Nodata!<!--havexQlpoOTFBWS<additionaldata removed>llwg==havex--></body></head>*
Observable 22 †	*Anomalous Network Traffic: From External Web Server to Local Host: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: POST Response from Domain: Comment Tags within HTTP Request/Response: <!--havex (encrypted code) havex-->*
Observable 23 †	Presence of Anomalous Binary on Host: mbcheck.dll: <username>\%TEMP%\mbCHECK.dll
Observable 24 †	Presence of Anomalous Binary on Host: TMprovider.dll: <username>\%TEMP%\TmProvider.dll
Observable 25 †	Presence of Anomalous Binary on Host: TMPprovider038.dll: %SYSTEM32%\TMPprovider038.dll
Observable 26 †	Presence of Anomalous Binary on Host: TMPprovider038.dll: %ALLUSERSAPPDATA%\TMPprovider038.dll
Observable 27 †	Presence of Anomalous Binary on Host: qln.dbx: <username>\%TEMP%\qln.dbx
Observable 28 †	Presence of Anomalous Binary on Host: setup.exe: %TEMP%\setup.exe
Observable 29 †	Presence of Anomalous Binary on Host: egrabitsetup.exe
Observable 30 †	Presence of Anomalous Binary on Host: svcprocess043.dll: %SYSTEM32%\svcprocess043.dll
Observable 31 †	Presence of Anomalous Binary on Host: svcprocess043.dll: %ALLUSERAPPDATA%\svcprocess043.dll
Observable 32 †	Presence of Anomalous Binary on Host: setup_1.0.1.exe: <username>\%TEMP%\setup_1.0.1.exe
Observable 33 †	Presence of Anomalous Binary on Host: setup_1.0.1.dll: <username>\%TEMP%\setup_1.0.1.dll
Observable 34 †	Presence of Anomalous Binary on Host: SwissrangerSetup1.0.14.706.exe
Observable 35 †	Presence of Anomalous Binary on Host: tmp687.dll: %TEMP%\tmp687.dll
Observable 36 †	Presence of Anomalous Binary on Host: sydmain.dll: %APPDATA%\sydmain.dll

Observables Associated with User Execution Technique (T0863)	
Observable 1 †	Anomalous Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80

Observables Associated with User Execution Technique (T0863)	
Observable 2	Anomalous Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 3	User Interaction with Anomalous Email: Opens Attachment Containing Anomalous Code from Trusted Source: Portable Document Format (.pdf) Attachment from Steel Manufacturing Partners
Observable 4	User Interaction with Anomalous Email: Opens Attachment Containing Anomalous Code from Trusted Source: Extensible Markup Language (.xml) Attachment from Steel Manufacturing Partners
Observable 5	User Interaction with Anomalous Email: Opens Attachment Containing Anomalous Code from Trusted Source: Extensible Markup Language Data Package (.xdp) Attachment from Steel Manufacturing Partners
Observable 6	Anomalous Attachment Executes Embedded Function on Local Host: Portable Document Format (.pdf) from Steel Manufacturing Partners Executes Macros
Observable 7	Anomalous Attachment Executes Embedded Function on Local Host: Extensible Markup Language (.xml) From Steel Manufacturing Partners
Observable 8	Anomalous Attachment Executes Embedded Function on Local Host: Extensible Markup Language Data Package (.xdp) from Steel Manufacturing Partners
Observable 9 †	User Interaction with Anomalous Email: Selects Anomalous Universal Resource Locator (URL): http://adultfriendfrance.com/wp-includes/pomo/src.php
Observable 10 †	User Interaction with Anomalous Email: Selects Anomalous Universal Resource Locator (URL): http://adultfrienditaly.com/wp-includes/pomo/src.php
Observable 11 †	User Interaction with Anomalous Email: Selects Anomalous Universal Resource Locator (URL): http://disney.freesexycomics.com/
Observable 12 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://adultfriendfrance.com/wp-includes/pomo/src.php
Observable 13 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://adultfriendfrance.com/wp-includes/pomo/src.php: Over Hypertext Transfer Protocol (HTTP) TCP Port 80
Observable 14 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://adultfrienditaly.com/wp-includes/pomo/src.php
Observable 15 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://adultfrienditaly.com/wp-includes/pomo/src.php: Over Hypertext Transfer Protocol (HTTP) TCP Port 80
Observable 16 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://disney.freesexycomics.com/
Observable 17 †	Anomalous Network Traffic: Outbound from Local Host to Anomalous External IP Address Associated with Universal Resource Locator (URL): http://disney.freesexycomics.com/: Over Hypertext Transfer Protocol (HTTP) TCP Port 80

Observables Associated with User Execution Technique (T0863)	
Observable 18 †	Presence of Anomalous Binary on Host: mbcheck.dll: <username>\%TEMP%\mbCHECK.dll
Observable 19 †	Presence of Anomalous Binary on Host: mbcheck.exe: <username>\%TEMP%\mbCHECK.exe
Observable 20 †	Presence of Anomalous Binary on Host: TMprovider.dll: <username>\%TEMP%\TmProvider.dll
Observable 21 †	Presence of Anomalous Binary on Host: TMPprovider038.dll: %SYSTEM32%\TMPprovider038.dll
Observable 22 †	Presence of Anomalous Binary on Host: TMPprovider038.dll: %ALLUSERSAPPDATA%\TMPprovider038.dll
Observable 23 †	Presence of Anomalous Binary on Host: qln.dbx: <username>\%TEMP%\qln.dbx
Observable 24 †	Presence of Anomalous Binary on Host: setup.exe: %TEMP%\setup.exe
Observable 25 †	Presence of Anomalous Binary on Host: egrabitsetup.exe
Observable 26 †	Presence of Anomalous Binary on Host: svcprocess043.dll: %SYSTEM32%\svcprocess043.dll
Observable 27 †	Presence of Anomalous Binary on Host: svcprocess043.dll: %ALLUSERAPPDATA%\svcprocess043.dll
Observable 28 †	Presence of Anomalous Binary on Host: setup_1.0.1.exe: <username>\%TEMP%\setup_1.0.1.exe
Observable 29 †	Presence of Anomalous Binary on Host: setup_1.0.1.dll: <username>\%TEMP%\setup_1.0.1.dll
Observable 30 †	Presence of Anomalous Binary on Host: tmp687.dll: %TEMP%\tmp687.dll
Observable 31 †	Presence of Anomalous Binary on Host: sydmain.dll: %APPDATA%\sydmain.dll
Observable 32 †	Execution of Anomalous Executable on Host: mbcheck.exe
Observable 33 †	Execution of Anomalous Executable on Host: ecatchersetup.exe
Observable 34 †	Execution of Anomalous Executable on Host: egrabitsetup.exe
Observable 35 †	Execution of Anomalous Executable on Host: setup_1.0.1.exe
Observable 36 †	Anomalous Process Spawned on Host: From Email Attachment
Observable 37 †	Anomalous Process Spawned on Host: From Universal Resource Locator (URL) Link in Email

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1 †	*Anomalous Host Activity: Successful Logon from External Host: Valid User Account Windows Event ID (4624)*
Observable 2	Anomalous Call to Windows API on Multiple Local Hosts: recursive_WNetEnumResourceW
Observable 3 †	*Presence of Anomalous Binary on Host: mbcheck.dll: <username>\%TEMP%\mbCHECK.dll*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 4 †	*Presence of Anomalous Binary on Host: mbcheck.exe: <username>\%TEMP%\mbCHECK.exe*
Observable 5 †	*Presence of Anomalous Binary on Host: TMprovider.dll: <username>\%TEMP%\TmProvider.dll*
Observable 6 †	*Presence of Anomalous Binary on Host: TMPprovider038.dll: %SYSTEM32%\TMPprovider038.dll*
Observable 7 †	*Presence of Anomalous Binary on Host: TMPprovider038.dll: %ALLUSERSAPPDATA%\TMPprovider038.dll*
Observable 8 †	Presence of Anomalous Binary on Host: qln.dbx: <username>\%TEMP%\qln.dbx
Observable 9 †	*Presence of Anomalous Binary on Host: setup.exe: %TEMP%\setup.exe*
Observable 10 †	*Presence of Anomalous Binary on Host: egrabitsetup.exe*
Observable 11 †	*Presence of Anomalous Binary on Host: svcprocess043.dll: %SYSTEM32%\svcprocess043.dll*
Observable 12 †	*Presence of Anomalous Binary on Host: svcprocess043.dll: %ALLUSERAPPDATA%\svcprocess043.dll*
Observable 13 †	*Presence of Anomalous Binary on Host: setup_1.0.1.exe: <username>\%TEMP%\setup_1.0.1.exe*
Observable 14 †	*Presence of Anomalous Binary on Host: setup_1.0.1.dll: <username>\%TEMP%\setup_1.0.1.dll*
Observable 15 †	*Presence of Anomalous Binary on Host: SwissrangerSetup1.0.14.706.exe*
Observable 16 †	*Presence of Anomalous Binary on Host: tmp687.dll: %TEMP%\tmp687.dll*
Observable 17 †	*Presence of Anomalous Binary on Host: sydmain.dll: %APPDATA%\sydmain.dll*
Observable 18 †	*Execution of Anomalous Executable on Host: mbcheck.exe*
Observable 19 †	*Execution of Anomalous Executable on Host: ecatchersetup.exe*
Observable 20 †	*Execution of Anomalous Executable on Host: egrabitsetup.exe*
Observable 21 †	*Execution of Anomalous Executable on Host: setup_1.0.1.exe*
Observable 22 †	*Creation of Anomalous Process on Host: Rundll32: mbcheck.dll Loaded*
Observable 23 †	*Anomalous Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80*
Observable 24	Anomalous Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 25	Anomalous Network Traffic: From External Remote Host to Local Host: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: SYN Request
Observable 26	Anomalous Network Traffic: From External Remote Host to Local Host: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443: SYN Request
Observable 27 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 28 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: ISO-TAP/Siemens S7Com TCP Port 102*
Observable 29 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Modbus TCP Port 502*
Observable 30 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Measuresoft ScadaPRO Monitoring TCP Port 11234*
Observable 31 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: 7-Technologies Interactive Graphical Scada System (IGSS) TCP Port 12401*
Observable 32 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: GE Proficy Server License Manager TCP Port 12401*
Observable 33 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: WellinTech KingSCADA Monitoring TCP Port 12401*
Observable 34 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Ethernet Industrial Protocol (IP) TCP Port 44818*
Observable 35 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Cisco OS Common Industrial Protocol (CIP) Messaging TCP Port 44819*
Observable 36 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Rockwell Automation ControlLogix Messaging TCP Port 44820*
Observable 37 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135*
Observable 38 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Component Object Model (COM) Connections*
Observable 39 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Distributed Component Object Model (DCOM) Connections*
Observable 40 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) Connections*
Observable 41 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA)*
Observable 42 †	*Anomalous Network Traffic: From Local Routers to Internal Hosts: Over Common Networking Protocol for Mapping Dynamic Internet Protocol (IP) Addresses: Address Resolution Protocol (ARP) SYN Requests*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 43 †	*Anomalous Network Traffic: From Local Routers to Internal Hosts: Over Common Networking Protocol for Mapping Dynamic Internet Protocol (IP) Addresses: Address Resolution Protocol (ARP) SYN ACK Requests*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1 †	*Anomalous Outbound Network Traffic: From Local Host to External Host: Over Hypertext Transfer Protocol (HTTP) TCP Port 80*
Observable 2	Anomalous Outbound Network Traffic: From Local Host to External Host: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 3 †	*Anomalous Outbound Network Traffic: From Local Host to External Host: Over NetBIOS/Server Message Block (SMB) TCP Port 139*
Observable 4 †	*Anomalous Outbound Network Traffic: From Local Host to External Host: Over NetBIOS/Server Message Block (SMB) TCP Port 445*
Observable 5 †	*Anomalous Outbound Network Traffic: Connection Request from Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 139*
Observable 6 †	*Anomalous Outbound Network Traffic: Connection Established from Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 445*
Observable 7 †	*Anomalous Host Activity: Successful Logon with Valid User Account on Local Host from External Remote Host (Windows Event ID 4624 Type 10)*
Observable 8 †	*Anomalous Host Activity: Creation of Autostart Registry Key on Host: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run*
Observable 9 †	*Anomalous Host Activity: Creation of Autostart Registry Key on Host: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce*
Observable 10 †	*Anomalous Host Activity: Creation of Autostart Registry Key on Host: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run*
Observable 11 †	*Anomalous Host Activity: Creation of Autostart Registry Key on Host: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce*

Observables Associated with Native API Technique (T0834)	
Observable 1 †	*Anomalous Outbound Network Traffic: From Local Host to External Host: Over Hypertext Transfer Protocol (HTTP) TCP Port 80*
Observable 2	Anomalous Outbound Network Traffic: From Local Host to External Host: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 3 †	*Anomalous Outbound Network Traffic: From Local Host to External Host: Over NetBIOS/Server Message Block (SMB) TCP Port 139*
Observable 4 †	*Anomalous Outbound Network Traffic: From Local Host to External Host: Over NetBIOS/Server Message Block (SMB) TCP Port 445*

Observables Associated with Native API Technique (T0834)	
Observable 5 †	*Anomalous Network Traffic: Connection Request from Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 139*
Observable 6 †	*Anomalous Network Traffic: Connection Establish from Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 445*
Observable 7 †	*Anomalous Host Activity: Successful Logon with Valid User Account on Local Host from External Remote Host (Windows Event ID 4624 Type 10)*
Observable 8 †	*Presence of Anomalous Binary on Host: mbcheck.dll: <username>\%TEMP%\mbCHECK.dll*
Observable 9 †	*Presence of Anomalous Binary on Host: mbcheck.exe: <username>\%TEMP%\mbCHECK.exe*
Observable 10 †	*Presence of Anomalous Binary on Host: TMprovider.dll: <username>\%TEMP%\TmProvider.dll*
Observable 11 †	*Presence of Anomalous Binary on Host: TMPprovider038.dll: %SYSTEM32%\TMPprovider038.dll*
Observable 12 †	*Presence of Anomalous Binary on Host: TMPprovider038.dll: %ALLUSERSAPPDATA%\TMPprovider038.dll*
Observable 13 †	*Presence of Anomalous Binary on Host: qln.dbx: <username>\%TEMP%\qln.dbx*
Observable 14 †	*Presence of Anomalous Binary on Host: setup.exe: %TEMP%\setup.exe*
Observable 15 †	*Presence of Anomalous Binary on Host: egrabitsetup.exe*
Observable 16 †	*Presence of Anomalous Binary on Host: svcprocess043.dll: %SYSTEM32%\svcprocess043.dll*
Observable 17 †	*Presence of Anomalous Binary on Host: svcprocess043.dll: %ALLUSERAPPDATA%\svcprocess043.dll*
Observable 18 †	*Presence of Anomalous Binary on Host: setup_1.0.1.exe: <username>\%TEMP%\setup_1.0.1.exe*
Observable 19 †	*Presence of Anomalous Binary on Host: setup_1.0.1.dll: <username>\%TEMP%\setup_1.0.1.dll*
Observable 20 †	*Presence of Anomalous Binary on Host: SwissrangerSetup1.0.14.706.exe*
Observable 21 †	*Presence of Anomalous Binary on Host: tmp687.dll: %TEMP%\tmp687.dll*
Observable 22 †	*Presence of Anomalous Binary on Host: sydmain.dll: %APPDATA%\sydmain.dll*
Observable 23 †	*Execution of Anomalous Binary on Host: mbcheck.exe: Located at File Path <C:\DOCUME~1\<USER>~1/LOCALS~1\Temp\mbcheck.exe C\DOCUME~1\<USER>~1\LOCALS~1\Temp\mbcheck.exe" ">*
Observable 24 †	*Execution of Anomalous Binary on Host: setup.exe*
Observable 25 †	*Execution of Anomalous Binary on Host: egrabitsetup.exe*
Observable 26 †	*Execution of Anomalous Binary on Host: setup_1.0.1.exe*
Observable 27 †	*Creation of Anomalous Process on Host: Rundll32: mbcheck.dll Loaded*
Observable 28	Execution of Anomalous Encoded Native API Call: Recursive_WNetEnumResourceW

Observables Associated with Native API Technique (T0834)	
Observable 29 †	*Anomalous Command Line: Anomalous Modification of Registry Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run load (REG_SZ): With Parameters: %SYSTEM32%\rundll32.exe "%APPDATA%\sydmain.dll",AGTwLoad*
Observable 30 †	*Anomalous Command Line: Anomalous Modification of Registry Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run TmProvider (REG_SZ): With Parameters: rundll32 "%ALLUSERAPPDATA%\TMPprovider038.dll",RunDllEntry*
Observable 31 †	*Anomalous Command Line: Anomalous Modification of Registry Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run TmProvider (REG_SZ): With Parameters: rundll32 "%SYSTEM32%\TMPprovider038.dll",RunDllEntry*

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: ISO-TAP/Siemens S7Com TCP Port 102*
Observable 2 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Modbus TCP Port 502*
Observable 3 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Measuresoft ScadaPRO Monitoring TCP Port 11234*
Observable 4 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: 7-Technologies Interactive Graphical Scada System (IGSS) TCP Port 12401*
Observable 5 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: GE Proficy Server License Manager TCP Port 12401*
Observable 6 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: WellinTech King SCADA Monitoring TCP Port 12401*
Observable 7 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Ethernet Industrial Protocol (IP) TCP Port 44818*
Observable 8 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Cisco OS Common Industrial Protocol (CIP) Messaging TCP Port 44819*
Observable 9 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Rockwell Automation ControlLogix Messaging TCP Port 44820*
Observable 10 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Component Object Model (COM) Connections*

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 11 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Distributed Component Object Model (DCOM) Connections*
Observable 12 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) Connections*
Observable 13 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA)*
Observable 14 †	*Anomalous Network Traffic: From Local Routers to Internal Hosts: Over Common Networking Protocol for Mapping Dynamic Internet Protocol (IP) Addresses: Address Resolution Protocol (ARP) SYN Requests*
Observable 15 †	*Anomalous Network Traffic: From Local Routers to Internal Hosts: Over Common Networking Protocol for Mapping Dynamic Internet Protocol (IP) Addresses: Address Resolution Protocol (ARP) SYN ACK Requests*
Observable 16 †	*Anomalous Call to Windows API on Multiple Local Hosts: recursive_WNetEnumResourceW*
Observable 17	Anomalous Access to Component Object Model (COM) Objects on Multiple Local Hosts: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA) Servers: IID_IOPCServerList2
Observable 18	Anomalous Access to Component Object Model (COM) Objects on Multiple Local Hosts: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA) Servers: CLSID_OPCServerList
Observable 19	Anomalous Access to Component Object Model (COM) Objects on Multiple Local Hosts: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA) Servers: IID_IOPCServerList2: An Attempt was Made to Access an Object (Windows Event ID 4663)
Observable 20	Anomalous Access to Component Object Model (COM) Objects on Multiple Local Hosts: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA) Servers: CLSID_OPCServerList: An Attempt was Made to Access an Object (Windows Event ID 4663)
Observable 21 †	*Presence of Anomalous File on Host: tracedscn.yls: %TEMP%\~tracedscn.yls*
Observable 22 †	*Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: GET Request*
Observable 23	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: POST Response: Containing Encrypted Files: <encryptedfile>.yls (Operational Data)
Observable 24	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443: GET Request
Observable 25	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443: POST Response: Containing Encrypted Files: <encryptedfile>.yls (Operational Data)

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 26 †	*Deletion of Anomalous File on Host: .yls*
Observable 27 †	*Deletion of Anomalous File on Host: .dat*
Observable 28 †	*Deletion of Anomalous File on Host: .tmp: containing enterprise address book*

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: ISO-TAP/Siemens S7Com TCP Port 102*
Observable 2 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Modbus TCP Port 502*
Observable 3 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Measuresoft ScadaPRO Monitoring TCP Port 11234*
Observable 4 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: 7-Technologies Interactive Graphical Scada System (IGSS) TCP Port 12401*
Observable 5 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: GE Proficy Server License Manager TCP Port 12401*
Observable 6 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: WellinTech KingSCADA Monitoring TCP Port 12401*
Observable 7 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Ethernet Industrial Protocol (IP) TCP Port 44818*
Observable 8 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Cisco OS Common Industrial Protocol (CIP) Messaging TCP Port 44819*
Observable 9 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Rockwell Automation ControlLogix Messaging TCP Port 44820*
Observable 10 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Component Object Model (COM) Connections*
Observable 11 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Distributed Component Object Model (DCOM) Connections*
Observable 12 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) Connections*
Observable 13 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC)*

Observables Associated with Remote System Information Discovery Technique (T0888)	
	TCP Port 135: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA)
Observable 14 †	*Anomalous Network Traffic: From Local Routers to Internal Hosts: Over Common Networking Protocol for Mapping Dynamic Internet Protocol (IP) Addresses: Address Resolution Protocol (ARP) SYN Requests*
Observable 15 †	*Anomalous Network Traffic: From Local Routers to Internal Hosts: Over Common Networking Protocol for Mapping Dynamic Internet Protocol (IP) Addresses: Address Resolution Protocol (ARP) SYN ACK Requests*
Observable 16	Anomalous Call to Windows API on Multiple Local Hosts: recursive_WNetEnumResourceW
Observable 17	Anomalous Access to Component Object Model (COM) Objects on Multiple Local Hosts: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA) Servers: IID_IOPCServerList2: An Attempt was Made to Access an Object (Windows Event ID 4663)
Observable 18	Anomalous Access to Component Object Model (COM) Objects on Multiple Local Hosts: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA) Servers: CLSID_OPCServerList: An Attempt was Made to Access an Object (Windows Event ID 4663)
Observable 19 †	*Presence of Anomalous File on Host: tracedscn.yls: %TEMP%\~tracedscn.yls*
Observable 20 †	*Creation of Anomalous Temporary Files on Host: <filename>.tmp: Contents Include Enterprise Address Book*
Observable 21 †	*Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: GET Request*
Observable 22	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: POST Response: Containing Encrypted Files: <encryptedfile>.yls (Operational Data)
Observable 23	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443: POST Response: Containing Encrypted Files: <encryptedfile>.yls (Operational Data)
Observable 24 †	*Deletion of Anomalous File on Host: .yls*
Observable 25 †	*Deletion of Anomalous File on Host: .dat*
Observable 26 †	*Deletion of Anomalous File on Host: .tmp*
Observable 27 †	*Deletion of Anomalous File on Host: .tmp: containing enterprise address book*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Anomalous Outbound Network Traffic: From Local Host to External Remote Host: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: Containing Encrypted Files: <encryptedfile>.yls (Operational Data)
Observable 2	Anomalous Outbound Network Traffic: From Local Host to External Remote Host: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 3 †	*Anomalous Outbound Network Traffic: From Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 139*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 4 †	*Anomalous Outbound Network Traffic: From Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 445*
Observable 5 †	*Anomalous Outbound Network Traffic: Connection Request from Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 139*
Observable 6 †	*Anomalous Outbound Network Traffic: Connection Established from Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 445*
Observable 7 †	*Anomalous Host Activity: Successful Logon with Valid User Account on Local Host from External Remote Host (Windows Event ID 4624 Type 10)*
Observable 8 †	*Anomalous Host Activity: Creation of Autostart Registry Key on Host: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run*
Observable 9 †	*Anomalous Host Activity: Creation of Autostart Registry Key on Host: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce*
Observable 10 †	*Anomalous Host Activity: Creation of Autostart Registry Key on Host: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run*
Observable 11 †	*Anomalous Host Activity: Creation of Autostart Registry Key on Host: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce*
Observable 12 †	*Anomalous Outbound Network Traffic: From Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 139*
Observable 13 †	*Anomalous Outbound Network Traffic: From Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 445*
Observable 14 †	*Anomalous Outbound Network Traffic: Connection Request from Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 139*
Observable 15 †	*Anomalous Outbound Network Traffic: Connection Established from Local Host to External Remote Host: Over NetBIOS/Server Message Block (SMB) TCP Port 445*
Observable 16 †	*Anomalous Host Activity: Successful Logon with Valid User Account on Local Host from External Remote Host (Windows Event ID 4624 Type 10)*
Observable 17 †	*Anomalous Network Activity: Connection Request from Local Host to Local Remote Host: Over NetBIOS/Server Message Block (SMB) TCP 139*
Observable 18 †	*Anomalous Network Activity: Connection Request from Local Host to Local Remote Host: Over NetBIOS/Server Message Block (SMB) TCP 445*
Observable 19 †	*Anomalous Host Activity: Successful Logon with Valid User Account on Local Host from Local Remote Host (Windows Event ID 4624 Type 10)*
Observable 20	Anomalous Host Activity: Presence of Encrypted YuleLog Data Files on Host: Containing Encrypted Outputs: <encryptedscanoutput>.yls: %TEMP%\[seq_no].yls
Observable 21 †	*Anomalous Uniform Resource Locator (URL): rapidecharge.gigfa.com*
Observable 22 †	*Anomalous Domain Name System (DNS) Request: rapidecharge.gigfa.com*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 23 †	*Anomalous Domain Name System (DNS) Request: sinfulcelebs.freesexycomics.com*
Observable 24 †	*Anomalous Domain Name System (DNS) Request: rapidecharge.gigfa.com*

Observables Associated with Point and Tag Identification Technique (T0861)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Emphemeral Network Ports and Protocols: TCP Ports 1024-65535*
Observable 2 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: ISO-TAP/Siemens S7Com TCP Port 102*
Observable 3 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Modbus TCP Port 502*
Observable 4 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Measuresoft ScadaPRO Monitoring TCP Port 11234*
Observable 5 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: 7-Technologies Interactive Graphical Scada System (IGSS) TCP Port 12401*
Observable 6 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: GE Proficy Server License Manager TCP Port 12401*
Observable 7 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: WellinTech KingSCADA Monitoring TCP Port 12401*
Observable 8 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Ethernet Industrial Protocol (IP) TCP Port 44818*
Observable 9 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Cisco OS Common Industrial Protocol (CIP) Messaging TCP Port 44819*
Observable 10 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Rockwell Automation ControlLogix Messaging TCP Port 44820*
Observable 11 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Component Object Model (COM) Connections*
Observable 12 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Distributed Component Object Model (DCOM) Connections*
Observable 13 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) Connections*

Observables Associated with Point and Tag Identification Technique (T0861)	
Observable 14 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA)*
Observable 15 †	*Anomalous Network Traffic: From Local Routers to Internal Hosts: Over Common Networking Protocol for Mapping Dynamic Internet Protocol (IP) Addresses: Address Resolution Protocol (ARP) SYN Requests*
Observable 16 †	*Anomalous Network Traffic: From Local Routers to Internal Hosts: Over Common Networking Protocol for Mapping Dynamic Internet Protocol (IP) Addresses: Address Resolution Protocol (ARP) SYN ACK Requests*

Observables Associated with Automated Collection Technique (T0802)	
Observable 1 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Ephemeral Network Ports and Protocols: TCP Ports 1024-65535*
Observable 2 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Industrial Application Networking Protocol: ISO-TAP/Siemens S7Com TCP Port 102*
Observable 3 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Industrial Application Networking Protocol: Modbus TCP Port 502*
Observable 4 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Industrial Application Networking Protocol: Measuresoft ScadaPRO Monitoring TCP Port 11234*
Observable 5 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Industrial Application Networking Protocol: 7-Technologies Interactive Graphical Scada System (IGSS) TCP Port 12401*
Observable 6 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Industrial Application Networking Protocol: GE Proficy Server License Manager TCP Port 12401*
Observable 7 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Industrial Application Networking Protocol: WellinTech KingSCADA Monitoring TCP Port 12401*
Observable 8 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Industrial Application Networking Protocol: Ethernet Industrial Protocol (IP) TCP Port 44818*
Observable 9 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Industrial Application Networking Protocol: Cisco OS Common Industrial Protocol (CIP) Messaging TCP Port 44819*
Observable 10 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Industrial Application Networking Protocol: Rockwell Automation ControlLogix Messaging TCP Port 44820*
Observable 11 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Component Object Model (COM) Connections*
Observable 12 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Distributed Component Object Model (DCOM) Connections*

Observables Associated with Automated Collection Technique (T0802)	
Observable 13 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) Connections*
Observable 14 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Common Remote Client to Server Protocol: Remote Procedure Call (RPC) TCP Port 135: Object Linking and Embedding (OLE) for Process Control (OPC) Data Access (DA)*
Observable 15 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Common Networking Protocol for Mapping Dynamic Internet Protocol (IP) Addresses: Address Resolution Protocol (ARP) SYN Requests*
Observable 16 †	*Anomalous Network Traffic: Internal Hosts to Single Host: Over Common Networking Protocol for Mapping Dynamic Internet Protocol (IP) Addresses: Address Resolution Protocol (ARP) SYN ACK Requests*
Observable 17 †	*Presence of Anomalous File on Host: tracedscn.yls: %TEMP%\~tracedscn.yls*
Observable 18	Anomalous Host Activity: Presence of Text Files on Host: Containing Network Scan Outputs: <scanoutput>.txt
Observable 19	Anomalous Host Activity: Presence of Encrypted YuleLog Data Files on Host: Containing Encrypted Outputs: <encryptedscanoutput>.yls
Observable 20 †	*Anomalous Host Activity: Creation of Autostart Registry Key on Host (Windows Event ID 4657)*

Observables Associated with Denial of Service Technique (T0814)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: ISO-TAP/Siemens S7Com TCP Port 102*
Observable 2 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Modbus TCP Port 502*
Observable 3 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Measuresoft ScadaPRO Monitoring TCP Port 11234*
Observable 4 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: 7-Technologies Interactive Graphical Scada System (IGSS) TCP Port 12401*
Observable 5 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: GE Proficy Server License Manager TCP Port 12401*
Observable 6 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: WellinTech KingSCADA Monitoring TCP Port 12401*
Observable 7 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Ethernet Industrial Protocol (IP) TCP Port 44818*

Observables Associated with Denial of Service Technique (T0814)	
Observable 8 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Cisco OS Common Industrial Protocol (CIP) Messaging TCP Port 44819*
Observable 9 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Rockwell Automation ControlLogix Messaging TCP Port 44820*
Observable 10 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Programmable Logic Controller (PLC): Burden Control*
Observable 11 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Programmable Logic Controller (PLC): Burden Distribution*
Observable 12 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Programmable Logic Controller (PLC): Mass and Energy Balance*
Observable 13 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Programmable Logic Controller (PLC): Kinetic Process Model*
Observable 14 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Programmable Logic Controller (PLC): Hot-Blast System*
Observable 15 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Burden Control*
Observable 16 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Burden Distribution*
Observable 17 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Mass and Energy Balance*
Observable 18 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Kinetic Process Model*
Observable 19 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Hot-Blast System*
Observable 20 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Human Machine Interface (HMI): Burden Control*
Observable 21 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Human Machine Interface (HMI): Burden Distribution*
Observable 22 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Human Machine Interface (HMI): Mass and Energy Balance*
Observable 23 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Human Machine Interface (HMI): Kinetic Process Model*
Observable 24 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Human Machine Interface (HMI): Hot-Blast System*
Observable 25 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Programmable Logic Controller (PLC) : Siemens Step 7*
Observable 26 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Programmable Logic Controller (PLC) : Rockwell Automation ControlLogix*

Observables Associated with Denial of Service Technique (T0814)	
Observable 27 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Industrial Network Router: Cisco*
Observable 28 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Industrial Network Switch: Cisco*
Observable 29 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Supervisory and Data Acquisition Workstation: Measuresoft Workstation*
Observable 30 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Supervisory and Data Acquisition Workstation: 7-Technologies Interactive Graphical Scada System (IGSS)*
Observable 31 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Supervisory and Data Acquisition Workstation: WellinTechn KingSCADA System*
Observable 32 †	*Anomalous Host Activity: Temporary Loss of Service: Industrial Control System Device: Industrial Data Historian: GE Proficy Server*
Observable 33 †	*Failure of Commands to Reach Control Systems: Supervisory Control System*

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 1 †	*Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: GET Request*
Observable 2 †	*Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: POST Response: Containing Encrypted Files: <encryptedfile>.yls (Operational Data)*
Observable 3	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443: GET Request
Observable 4	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443: POST Response: Containing Encrypted Files: <encryptedfile>.yls (Operational Data)
Observable 5 †	*Anomalous Outbound Network Traffic: From Local Host to External Remote Server: Over NetBIOS and Server Message Block (SMB) TCP Port 139*
Observable 6 †	*Anomalous Outbound Network Traffic: From Local Host to External Remote Server: Over NetBIOS and Server Message Block (SMB) TCP Port 445*
Observable 7 †	*Anomalous Network Connection Request from External Remote Server*
Observable 8 †	*Anomalous Login Attempt on Local Host from Remote Server: Failure: Windows Event ID (4625)*
Observable 9 †	*Anomalous Login Attempt on Local Host from Remote Server: Success: Windows Event ID (4624 Type 10)*
Observable 10 †	*Creation of Anomalous File on Host: .tmp: containing enterprise address book*

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 1 †	*Anomalous Outbound Network Traffic: From Local Host to External Web Server*
Observable 2 †	*Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80*
Observable 3	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 4 †	*Anomalous Outbound Network Traffic: From Local Host to External Remote Server: Over NetBIOS and Server Message Block (SMB) TCP Port 139*
Observable 5 †	*Anomalous Outbound Network Traffic: From Local Host to External Remote Server: Over NetBIOS and Server Message Block (SMB) TCP Port 445*
Observable 6 †	*Anomalous Network Connection Request from External Remote Server*
Observable 7 †	*Anomalous Login Attempt on Local Host from Remote Server*
Observable 8 †	*Anomalous Login Attempt on Local Host from Remote Server: Windows Event ID (4624 Type 10)*
Observable 9 †	*Creation of Anomalous Temporary Files on Host: <filename>.tmp: Contents Include Enterprise Address Book*
Observable 10 †	*Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: GET Request*
Observable 11	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: POST Response: Containing Encrypted Files: <encryptedfile>.yls (Operational Data)
Observable 12	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443: GET Request
Observable 13	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443: POST Response: Containing Encrypted Files: <encryptedfile>.yls (Operational Data)
Observable 14 †	*Creation of Anomalous File on Host: <filename>.tmp*
Observable 15 †	*Presence of Anomalous File on Host: tracedscn.yls: %TEMP%\~tracedscn.yls*
Observable 16 †	*Deletion of Anomalous File on Host: .yls*
Observable 17 †	*Deletion of Anomalous File on Host: .dat*
Observable 18 †	*Deletion of Anomalous File on Host: .tmp*
Observable 19 †	*Deletion of Anomalous File on Host: .tmp: containing enterprise address book*

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 1 †	*Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol (HTTP) TCP Port 80*
Observable 2	Anomalous Outbound Network Traffic: From Local Host to External Web Server: Over Hypertext Transfer Protocol Secure (HTTPS) TCP Port 443

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 3 †	*Anomalous Outbound Network Traffic: From Local Host to External Remote Server: Over NetBIOS and Server Message Block (SMB) TCP Port 139*
Observable 4 †	*Anomalous Outbound Network Traffic: From Local Host to External Remote Server: Over NetBIOS and Server Message Block (SMB) TCP Port 445*
Observable 5	Creation of Anomalous File on Host: <filename>.tmp (Containing Enterprise Address Book): Found in various Directories: %TEMP%
Observable 6 †	*Creation of Anomalous File on Host: <filename>.tmp (Containing Enterprise Address Book): Found in various Directories: %Appdata%*
Observable 7 †	*Creation of Anomalous File on Host: <filename>.tmp (Containing Enterprise Address Book): Found in various Directories: %System32%*
Observable 8	Creation of Anomalous File on Host: <filename>.yls (Containing Encrypted Operational Data): Found in various Directories: %TEMP%
Observable 9 †	*Creation of Anomalous File on Host: <filename>.yls (Containing Encrypted Operational Data): Found in various Directories: %Appdata%*
Observable 10 †	*Creation of Anomalous File on Host: <filename>.yls (Containing Encrypted Operational Data): Found in various Directories: %System32%*
Observable 11	Creation of Anomalous File on Host: <filename>.dat (Containing Operational Data): Found in various Directories: %TEMP%
Observable 12 †	*Creation of Anomalous File on Host: <filename>.dat (Containing Operational Data): Found in various Directories: %Appdata%*
Observable 13 †	*Creation of Anomalous File on Host: <filename>.dat (Containing Operational Data): Found in various Directories: %System32%*
Observable 14	Deletion of Anomalous File on Host: <filename>.tmp (Containing Enterprise Address Book): Found in various Directories: %TEMP%
Observable 15 †	*Deletion of Anomalous File on Host: <filename>.tmp (Containing Enterprise Address Book): Found in various Directories: %Appdata%*
Observable 16 †	*Deletion of Anomalous File on Host: <filename>.tmp (Containing Enterprise Address Book): Found in various Directories: %System32%*
Observable 17	Deletion of Anomalous File on Host: <filename>.yls (Containing Encrypted Operational Data): Found in various Directories: %TEMP%
Observable 18 †	*Deletion of Anomalous File on Host: <filename>.yls (Containing Encrypted Operational Data): Found in various Directories: %Appdata%*
Observable 19 †	*Deletion of Anomalous File on Host: <filename>.yls (Containing Encrypted Operational Data): Found in various Directories: %System32%*
Observable 20	Deletion of Anomalous File on Host: <filename>.dat (Containing Operational Data): Found in various Directories: %TEMP%
Observable 21 †	*Deletion of Anomalous File on Host: <filename>.dat (Containing Operational Data): Found in various Directories: %Appdata%*
Observable 22 †	*Deletion of Anomalous File on Host: <filename>.dat (Containing Operational Data): Found in various Directories: %System32%*

Observables Associated with Denial of Control Technique (T0813)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: ISO-TAP/Siemens S7Com TCP Port 102*
Observable 2 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Modbus TCP Port 502*
Observable 3 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Measuresoft ScadaPRO Monitoring TCP Port 11234*
Observable 4 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: 7-Technologies Interactive Graphical Scada System (IGSS) TCP Port 12401*
Observable 5 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: GE Proficy Server License Manager TCP Port 12401*
Observable 6 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: WellinTech KingSCADA Monitoring TCP Port 12401*
Observable 7 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Ethernet Industrial Protocol (IP) TCP Port 44818*
Observable 8 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Cisco OS Common Industrial Protocol (CIP) Messaging TCP Port 44819*
Observable 9 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Rockwell Automation ControlLogix Messaging TCP Port 44820*
Observable 10 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Burden Control*
Observable 11 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Burden Distribution*
Observable 12 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Mass and Energy Balance*
Observable 13 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Kinetic Process Model*
Observable 14 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Hot-Blast System*
Observable 15 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Burden Control*
Observable 16 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Burden Distribution*
Observable 17 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Mass and Energy Balance*
Observable 18 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Kinetic Process Model*

Observables Associated with Denial of Control Technique (T0813)	
Observable 19 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Hot-Blast System*
Observable 20 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Human Machine Interface (HMI): Burden Control*
Observable 21 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Human Machine Interface (HMI): Burden Distribution*
Observable 22 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Human Machine Interface (HMI): Mass and Energy Balance*
Observable 23 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Human Machine Interface (HMI): Kinetic Process Model*
Observable 24 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Human Machine Interface (HMI): Hot-Blast System*
Observable 25 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC) : Siemens Step 7*
Observable 26 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Rockwell Automation ControlLogix*
Observable 27 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Industrial Network Router: Cisco*
Observable 28 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Industrial Network Switch: Cisco*
Observable 29 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Supervisory and Data Acquisition Workstation: Measuresoft Workstation*
Observable 30 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Supervisory and Data Acquisition Workstation: 7-Technologies Interactive Graphical Scada System (IGSS)*
Observable 31 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Supervisory and Data Acquisition Workstation: WellinTechn KingSCADA System*
Observable 32 †	*Anomalous Host Activity: Temporary Loss of Control: Industrial Control System Device: Industrial Data Historian: GE Proficy Server*
Observable 33 †	*Loss of Access to Control System: Supervisory Control System*
Observable 34 †	*Failure of Commands to Reach Control Systems: Supervisory Control System*

Observables Associated with Loss of Control Technique (T0827)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: ISO-TAP/Siemens S7Com TCP Port 102*
Observable 2 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Modbus TCP Port 502*

Observables Associated with Loss of Control Technique (T0827)	
Observable 3 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Measuresoft ScadaPRO Monitoring TCP Port 11234*
Observable 4 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: 7-Technologies Interactive Graphical Scada System (IGSS) TCP Port 12401*
Observable 5 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: GE Proficy Server License Manager TCP Port 12401*
Observable 6 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: WellinTech KingSCADA Monitoring TCP Port 12401*
Observable 7 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Ethernet Industrial Protocol (IP) TCP Port 44818*
Observable 8 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Cisco OS Common Industrial Protocol (CIP) Messaging TCP Port 44819*
Observable 9 †	*Anomalous Network Traffic: From Local Host to Other Internal Hosts: Over Industrial Application Networking Protocol: Rockwell Automation ControlLogix Messaging TCP Port 44820*
Observable 10 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Burden Control*
Observable 11 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Burden Distribution*
Observable 12 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Mass and Energy Balance*
Observable 13 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Kinetic Process Model*
Observable 14 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Hot-Blast System*
Observable 15 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Burden Control*
Observable 16 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Burden Distribution*
Observable 17 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Mass and Energy Balance*
Observable 18 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Kinetic Process Model*
Observable 19 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Hot-Blast System*
Observable 20 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Human Machine Interface (HMI): Burden Control*

Observables Associated with Loss of Control Technique (T0827)	
Observable 21 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Human Machine Interface (HMI): Burden Distribution*
Observable 22 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Human Machine Interface (HMI): Mass and Energy Balance*
Observable 23 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Human Machine Interface (HMI): Kinetic Process Model*
Observable 24 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Human Machine Interface (HMI): Hot-Blast System*
Observable 25 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Siemens Step 7*
Observable 26 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Programmable Logic Controller (PLC): Rockwell Automation ControlLogix*
Observable 27 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Industrial Network Router: Cisco*
Observable 28 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Industrial Network Switch: Cisco*
Observable 29 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Supervisory and Data Acquisition Workstation: Measuresoft Workstation*
Observable 30 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Supervisory and Data Acquisition Workstation: 7-Technologies Interactive Graphical Scada System (IGSS)*
Observable 31 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Supervisory and Data Acquisition Workstation: WellinTechn KingSCADA System*
Observable 32 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Industrial Data Historian: GE Proficy Server*
Observable 33 †	*Loss of Access to Control System: Supervisory Control System*
Observable 34 †	*Failure of Commands to Reach Control Systems: Supervisory Control System*

Observables Associated with Loss of Safety Technique (T0880)	
Observable 1 †	*Anomalous Host Activity: Industrial Systems Unresponsive: System Override Inoperable*
Observable 2 †	*Anomalous Host Activity: Industrial Systems Unresponsive: Safety System Inoperable: Blow-Down Process Failure*
Observable 3 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Burden Control*
Observable 4 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Burden Distribution*
Observable 5 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Mass and Energy Balance*

Observables Associated with Loss of Safety Technique (T0880)	
Observable 6 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Kinetic Process Model*
Observable 7 †	*Anomalous Host Activity: Sustained Loss of Control: Industrial Control System Device: Alarm Safety Instrumented Systems (SIS): Hot-Blast System*
Observable 8 †	*Anomalous Environmental Factors: In the Operational Environment: Uncontrolled Molten Metal Escaping from Blast Furnace: Heat Damage to Surrounding Structure: Structural Integrity Compromised*
Observable 9 †	*Anomalous Environmental Factors: In the Operational Environment: Threat to Human Life: Fire Hazard*
Observable 10 †	*Anomalous Environmental Factors: In the Operational Environment: Threat to Human Life: Smoke Inhalation*
Observable 11 †	*Anomalous Environmental Factors: In the Operational Environment: Threat to Human Life: Collapse of Physical Structure(s)*

Observables Associated with Damage to Property Technique (T0879)	
Observable 1 †	*Anomalous Environmental Factors: In the Operational Environment: Uncontrolled Molten Metal Escaping from Blast Furnace*
Observable 2 †	*Anomalous Environmental Factors: In the Operational Environment: Physical Damage: Blast Furnace Inoperable*
Observable 3 †	*Anomalous Environmental Factors: In the Operational Environment: Physical Damage: Plant Facility and Equipment Damaged or Destroyed*

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1 †	*Anomalous Loss of Revenue: $6,000,000*
Observable 2 †	*Anomalous Loss of Revenue: Recovery Cost Incurred: $4,000,000*
Observable 3 †	*Anomalous Loss of Productivity: Reduced Production of Pig Iron*
Observable 4 †	*Anomalous Loss of Productivity: Delays in Planned Outage Cycle: 30 Additional Days in the Outage Cycle*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Spearphishing Attachment Technique (T0865)	
Artifact 1	Email .ost File
Artifact 2	Mismatch MIME and Attachment File Extension
Artifact 3	Email Sender Address
Artifact 4	Email Message
Artifact 5	Email Receiver
Artifact 6	Email Receiver Name
Artifact 7	Email Receiver Domain
Artifact 8	Email Receiver Address
Artifact 9	Enable Macros Pop-Up
Artifact 10	Email Application Log File
Artifact 11	Email Unified Audit Log File
Artifact 12	Email Service Name
Artifact 13	Suspicious Email Message Content
Artifact 14	Email Sender Domain
Artifact 15	Email .pst File
Artifact 16	Email Sender IP Address
Artifact 17	Simple Mail Transfer Protocol SMTP Traffic
Artifact 18	Mail Transfer Agent Logs
Artifact 19	Email Parent Process
Artifact 20	Mail Transfer Agent Logs
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	Operating System Service Creation

Artifacts Associated with Drive-By Compromise Technique (T0817)	
Artifact 1	Application Log

Artifacts Associated with Drive-By Compromise Technique (T0817)	
Artifact 2	cmd.exe Application Start
Artifact 3	Dialog Boxes Open
Artifact 4	POWERSHELL Cmdlet Open
Artifact 5	POWERSHELL Log Creation
Artifact 6	Source IP Address
Artifact 7	Destination IP Address
Artifact 8	File Creation
Artifact 9	Memory Evidence
Artifact 10	Disk Read
Artifact 11	Disk Write
Artifact 12	TLS Certificates
Artifact 13	Website
Artifact 14	Industrial Application Process
Artifact 15	Industrial Application Disk Write
Artifact 16	Prefetch Files
Artifact 17	.lnk Files
Artifact 18	HTTP Traffic
Artifact 19	DNS Traffic
Artifact 20	HTTPS Traffic
Artifact 21	SMB Traffic
Artifact 22	Process Creation
Artifact 23	Process Ending
Artifact 24	Child Processes Created
Artifact 25	Application Log
Artifact 26	cmd.exe Application Start

Artifacts Associated with User Execution Technique (T0863)	
Artifact 1	Command Execution
Artifact 2	Service Termination
Artifact 3	File Changes
Artifact 4	Increased ICMP Traffic (Network Scanning)
Artifact 5	Network Traffic Changes
Artifact 6	Application Installation
Artifact 7	Network Connection Creation

Artifacts Associated with User Execution Technique (T0863)	
Artifact 8	Application Log Content
Artifact 9	User Account Modification
Artifact 10	File Creation
Artifact 11	Process Creation
Artifact 12	System Log
Artifact 13	Process Termination
Artifact 14	File Execution
Artifact 15	Prefetch Files
Artifact 16	Registry Modification
Artifact 17	File Modifications
Artifact 18	File Renaming
Artifact 19	System Patches Installed
Artifact 20	Files Opening
Artifact 21	File Signature Validation
Artifact 22	Installers Created
Artifact 23	Application Log

Artifacts Associated with 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 Valid Accounts Technique (T0859)	
Artifact 1	Logon Session Creation

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

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

Artifacts Associated with Indicator Removal on Host Technique (T0872)	
Artifact 18	Sdelete Executable Loaded
Artifact 19	Sdelete Executable Executed
Artifact 20	File Metadata Changes
Artifact 21	Timestamp Inconsistencies
Artifact 22	User Authentication
Artifact 23	Memory Writes

Artifacts Associated with Native API Technique (T0834)	
Artifact 1	Industrial Network Traffic
Artifact 2	Industrial Protocol Command Packet
Artifact 3	Device Reads
Artifact 4	Device I/O Image Table Manipulated
Artifact 5	Device Failure
Artifact 6	Alter Process Logic
Artifact 7	Device Performance Degradation
Artifact 8	Device Memory Modification
Artifact 9	Device Alarm
Artifact 10	Device Live Data Changes
Artifact 11	System Calls
Artifact 12	Alert Generated
Artifact 13	Memory Corruption
Artifact 14	Host Device Failure
Artifact 15	Blue Screen
Artifact 16	Performance Degradation
Artifact 17	SYSMON Events Created
Artifact 18	Services Initiated
Artifact 19	Processes Initiated
Artifact 20	Files Created
Artifact 21	Imports Hash Changed
Artifact 22	.dll Modifications
Artifact 23	System Resource Usage Management Changes
Artifact 24	Command Execution
Artifact 25	Configuration Change

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 1	Protocol Header Enumeration
Artifact 2	Protocol Content Enumeration
Artifact 3	VNC Port 5900 Calls
Artifact 4	TCP ACK Scan
Artifact 5	TCP XMAS Scan
Artifact 6	Recurring Protocol SYN Traffic
Artifact 7	TCP FIN Scans
Artifact 8	Device Failure
Artifact 9	TCP Reverse Ident Scan
Artifact 10	Sequential Protocol SYN Traffic
Artifact 11	Scans Over Industrial Network Ports with Target IPS
Artifact 12	Industrial Network Traffic Content Containing Logical Identifiers
Artifact 13	SMTP Port 25 Traffic
Artifact 14	Device Reboot
Artifact 15	Bandwidth Degradation
Artifact 16	Host Recent Connection Logs
Artifact 17	IEC 101 Traffic to Serial Devices
Artifact 18	IEC 102
Artifact 19	IEC 104
Artifact 20	OPC Network Traffic
Artifact 21	Statistical Anomalies in Network Traffic
Artifact 22	DNS Port 53 Zone Transfers
Artifact 23	Industrial Network Traffic
Artifact 24	Common Network Traffic
Artifact 25	IEC 103 Traffic (For North America)
Artifact 26	IEC 61850 MMS and
Artifact 27	Controller Proprietary Traffic
Artifact 28	Echo Type 8 Traffic
Artifact 29	ICMP Type 7 Traffic
Artifact 30	SNMP Port 162 Traffic
Artifact 31	SNMP Port 161 Traffic
Artifact 32	ARP Scans
Artifact 33	Operating System Queries
Artifact 34	TCP SYN Scans
Artifact 35	Industrial Network Traffic Content About Hostnames

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

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

Artifacts Associated with Point & Tag Identification Technique (T0861)	
Artifact 1	Destination IP Address
Artifact 2	Static Source IP Address
Artifact 3	Ping Echo Port
Artifact 4	HTTP Port
Artifact 5	LLDP Requests
Artifact 6	DNS Queries Traffic Port
Artifact 7	SNMP Port
Artifact 8	Unscheduled Firmware Updates
Artifact 9	Network Discover Protocols
Artifact 10	Source IP Address
Artifact 11	Usage of Default Account
Artifact 12	Mismatched Software Hashes
Artifact 13	SMB Port

Artifacts Associated with Point & Tag Identification Technique (T0861)	
Artifact 14	Usage of Vendor Maintenance Account
Artifact 15	Domain Name
Artifact 16	Domain Registrant Data
Artifact 17	Domain IP Resolution
Artifact 18	Domain Autonomous System Number
Artifact 19	Additional Hardware Inserted on Devices
Artifact 20	Device Failure
Artifact 21	Device Incompatibility Issues
Artifact 22	Hardware Tampering Evidence
Artifact 23	Hardware Failed Site Acceptance Test
Artifact 24	Physical Defects to Hardware
Artifact 25	Control Server Logon
Artifact 26	Hardware Serial Number Missing
Artifact 27	Point and Tag Data Exfiltration
Artifact 28	Database Logon Event
Artifact 29	MAC Address
Artifact 30	Industrial Network Traffic
Artifact 31	Control Server Logoff
Artifact 32	Application Logs
Artifact 33	Application Manipulation
Artifact 34	Application User Event
Artifact 35	Application Copy
Artifact 36	Host System Registry Modification
Artifact 37	User Registry Changes
Artifact 38	Memory Location Changes
Artifact 39	Common Network Traffic
Artifact 40	Data Historian Writes
Artifact 41	Data Historian Logon Event
Artifact 42	Control Server Reads
Artifact 43	Application Reads
Artifact 44	Database Reads
Artifact 45	OPC Requests
Artifact 46	Data Historian Reads
Artifact 47	External Point and Tag Read Requests Over Network Trust Boundaries
Artifact 48	Database Vendor Specific Protocol Request

Artifacts Associated with Point & Tag Identification Technique (T0861)	
Artifact 49	SQL Network Traffic
Artifact 50	.dll Hooking
Artifact 51	.dll Creation
Artifact 52	Network Traffic Content Focused on Point and Tag Reads
Artifact 53	.dll Execution

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

Artifacts Associated with Commonly Used Port Technique (T0885)	
Artifact 1	Unexpected Process Usage of Common Port Observed via Firewall Logs
Artifact 2	Unexpected Process Usage of Common Port Observed via OS Commands (netstat)

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

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

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

Artifacts Associated with Theft of Operational Information Technique (T0882)	
Artifact 1	Exfiltration of Endpoint Host Data (Spreadsheets, Diagrams, Documents, Configurations, etc.) via Standard Protocols
Artifact 2	Exfiltration from Database via Standard Queries
Artifact 3	Exfiltration of Endpoint Host Data (Spreadsheets, Diagrams, Documents, Configurations, etc.) via Industrial Protocols
Artifact 4	Exfiltration of Operational Info via Phishing

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

Artifacts Associated with Loss of Safety Technique (T0880)	
Artifact 1	Malicious Firmware Update to a Safety System
Artifact 2	Loss of Control of a Safety System
Artifact 3	Loss of Access to a Safety System

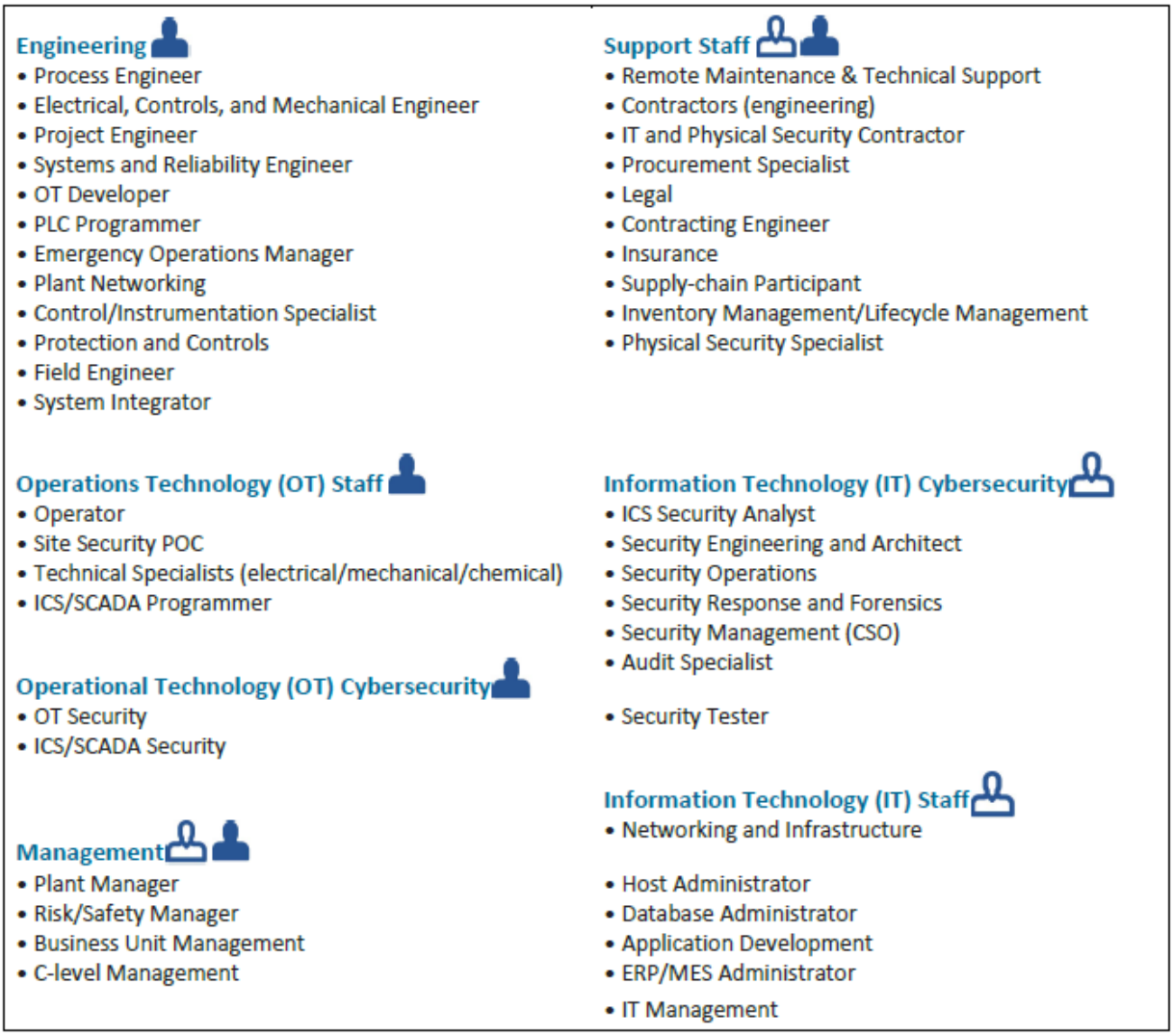
Artifacts Associated with Damage to Property Technique (T0879)	
Artifact 1	Pressure Relief
Artifact 2	Reduction In Traffic Volume to Device
Artifact 3	Frequent Maintenance Failures
Artifact 4	Damage to Property Due to Equipment Degradation
Artifact 5	Damage to Property Due to Malicious Network Traffic
Artifact 6	Breakers Closing and Opening Rapidly
Artifact 7	Safety Systems Engaged

Artifacts Associated with Damage to Property Technique (T0879)	
Artifact 8	Increase In Connecting Errors to Device
Artifact 9	Loud Vibrations
Artifact 10	Liquid Spills
Artifact 11	Damage to Property Due to Equipment Malfunction
Artifact 12	Catastrophic Failure
Artifact 13	Surges In Power
Artifact 14	Ladder Logic Configuration Changes
Artifact 15	Industrial Network Traffic
Artifact 16	Smoke
Artifact 17	Process Trip
Artifact 18	Alarms

Artifacts Associated with Loss of Productivity and Revenue Technique (T0828)	
Artifact 1	Loss of Confidence in a Safety System Due to Unreliability Might Result in a Risk Management Driven Shutdown of a Plant
Artifact 2	Wormable or Other Highly Propagating Malware Might Result in The Shutdown of a Plant to Prevent Ransomware or Other Destructive Attacks
Artifact 3	Extortion Attempts Might Lead to Reduced Operations Due to Potential Presence of Malicious Attackers
Artifact 4	Loss of Control of Critical Systems Due to Ransomware or Loss of Confidence Might Lead to a Degraded Productivity or Revenue Operating State
Artifact 5	File System Modification Artifacts Might Be Associated with The Loss of Productivity and Revenue Attack Might Be Present on Disk

APPENDIX C: OBSERVERS

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



REFERENCES

[1] [Bloomberg | Michael Riley and Jordan Robertson | "Cyberspace Becomes Second Front in Russia's Clash With NATO" | https://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato | 14 October 2015 | Accessed on 14 October 2022 | The source is publicly available information and does not contain classification markings]

[2] [George Mason University | Craig Wiener | "Penetrate, Exploit, Disrupt, Destroy: The Rise Of Computer Network Operations as a Major Military Innovation" | http://mars.gmu.edu/handle/1920/10613 | 2016 | Accessed on 14 October 2022 | The source is publicly available information and does not contain classification markings]

[3] [ThyssenKrupp | "First Campaign Ends after 21 Years: Europe's Biggest Blast Furnace To Be Modernized" |https://www.thyssenkrupp.com/en/newsroom/press-releases/first-campaign-ends-after-21-years--europe-s-biggest-blast-furnace-to-be-modernized-3303.html | 16 May 2014 | Accessed on 14 October 2022 | The source is publicly available information and does not contain classification markings]

[4] [ThyssenKrupp | "Europe's Biggest Blast Furnace Relit: "Schwelgern 2" Producing Iron Again" | https://www.thyssenkrupp-steel.com/en/newsroom/press-releases/europes-biggest-blast-furnace-relit-schwelgern-2-producing-iron-again.html | 20 October 2014 | Accessed on 14 October 2022 | The source is publicly available information and does not contain classification markings]

[5][Capitol Technology University | Scott Buchanan | "Cyber-Attacks To Industrial Control Systems Since Stuxnet" | https://www.proquest.com/openview/4be679a2dcfa686903463391d5dde19b/ 1?pq-origsite=gscholar&cbl=18750&diss=y%20 |10 April 2022 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[6][Federal Office for Information Security (BSI) | "The State of IT Security in Germany 2014" | https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3 | November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[7] [Kaspersky Lab | "Energetic Bear – Crouching Yeti" | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf | 14 July 2014 | Accessed on 29 November 2022 | The source is publicly available information and does not contain classification markings]

[8] [Federal Office for Information Security (BSI) | "The State of IT Security in Germany 2014" | https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3 | November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[9] [Capitol Technology University | Scott Buchanan | "Cyber-Attacks To Industrial Control Systems Since Stuxnet" | https://www.proquest.com/openview/4be679a2dcfa686903463391d5dde19b/ 1?pq-origsite=gscholar&cbl=18750&diss=y%20 |10 April 2022 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[10] [Federal Office for Information Security (BSI) | "The State of IT Security in Germany 2014" | https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3 | November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[11] [Gigamon | Joe Slowik | "The Baffling Berserk Bear: A Decade's Activity Targeting Critical Infrastructure" | https://vblocalhost.com/uploads/VB2021-Slowik.pdf | 7 October 2021 | Accessed on 3 May 2022 | The source is publicly available information and does not contain classification markings]

[12] [Broadcom |A L Johnson | "Dragonfly: Western Energy Companies Under Sabotage Threat" | https://community.broadcom.com/symantecenterprise/viewdocument/dragonfly-western-energy-companies?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments | 30 June

2014 | Accessed on 15 November 2022 | The source is publicly available information and does not contain classification markings]

[13] [Gigamon | Joe Slowik | "The Baffling Berserk Bear: A Decade's Activity Targeting Critical Infrastructure" | https://vblocalhost.com/uploads/VB2021-Slowik.pdf / | 7 October 2021 | Accessed on 3 May 2022 | The source is publicly available information and does not contain classification markings]

[14] [F-Secure Labs | "Havex Hunts for ICS/SCADA Systems" | https://archive.f-secure.com/weblog/archives/00002718.html | 23 June 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

[15] [Gigamon | Joe Slowik | "The Baffling Berserk Bear: A Decade's Activity Targeting Critical Infrastructure" | https://vblocalhost.com/uploads/VB2021-Slowik.pdf / | 7 October 2021 | Accessed on 3 May 2022 | The source is publicly available information and does not contain classification markings]

[16] [F-Secure Labs | "Havex Hunts for ICS/SCADA Systems" | https://archive.f-secure.com/weblog/archives/00002718.html | 23 June 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

[17] [Federal Office for Information Security (BSI) | "The State of IT Security in Germany 2014" | https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation%20/IT-Security-Situation-in-Germany-2014.pdf?blob=publicationFile&v=3|November2021 | November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[18] [Wired | Kim Zetter | "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever" | https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ | 8 January 2015 | Accessed on 14 October 2022 | The source is publicly available information and does not contain classification markings]

[19] [MITRE | "Backdoor.Oldrea" | https://attack.mitre.org/software/S0093/ | 12 October 2022 | Accessed on 15 November 2022 | The source is publicly available information and does not contain classification markings]

[20] [Gigamon | Joe Slowik | "The Baffling Berserk Bear: A Decade's Activity Targeting Critical Infrastructure" | https://vblocalhost.com/uploads/VB2021-Slowik.pdf / | 7 October 2021 | Accessed on 3 May 2022 | The source is publicly available information and does not contain classification markings]

[21] [F-Secure Labs | "Havex Hunts for ICS/SCADA Systems" | https://archive.f-secure.com/weblog/archives/00002718.html | 23 June 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

[22] [Belden | Joel Langill | "Defending Against the Dragonfly Cyber Security Attacks" | https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en | 22 October 2014 | Accessed on 17 November 2022 | The source is publicly available information and does not contain classification markings]

[23] [Kaspersky Lab | "Energetic Bear – Crouching Yeti" | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf | 14 July 2014 | Accessed on 29 November 2022 | The source is publicly available information and does not contain classification markings]

[24] [Gigamon | Joe Slowik | "The Baffling Berserk Bear: A Decade's Activity Targeting Critical Infrastructure" | https://vblocalhost.com/uploads/VB2021-Slowik.pdf / | 7 October 2021 | Accessed on 3 May 2022 | The source is publicly available information and does not contain classification markings]

[25] [MITRE | "Backdoor.Oldrea" | https://attack.mitre.org/software/S0093/ | 12 October 2022 | Accessed on 15 November 2022 | The source is publicly available information and does not contain classification markings]

[26] [Federal Office for Information Security (BSI) | "The State of IT Security in Germany 2014" | https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3 | November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[27] [MITRE | “Backdoor.Oldrea” | https://attack.mitre.org/software/S0093/ | 12 October 2022 | Accessed on 15 November 2022 | The source is publicly available information and does not contain classification markings]

[28] [Gigamon | Joe Slowik | "The Baffling Berserk Bear: A Decade's Activity Targeting Critical Infrastructure" | https://vblocalhost.com/uploads/VB2021-Slowik.pdf / | 7 October 2021 | Accessed on 3 May 2022 | The source is publicly available information and does not contain classification markings]

[29] [Belden | Joel Langill | “Defending Against the Dragonfly Cyber Security Attacks” | https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en | 22 October 2014 | Accessed on 17 November 2022 | The source is publicly available information and does not contain classification markings]

[30] [Broadcom | A L Johnson | “Dragonfly: Western Energy Companies Under Sabotage Threat” | https://community.broadcom.com/symantecenterprise/viewdocument/dragonfly-western-energy-companies?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments | 30 June 2014 | Accessed on 15 November 2022 | The source is publicly available information and does not contain classification markings]

[31] [Belden | Joel Langill | “Defending Against the Dragonfly Cyber Security Attacks” | https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en | 22 October 2014 | Accessed on 17 November 2022 | The source is publicly available information and does not contain classification markings]

[32] [Gigamon | Joe Slowik | "The Baffling Berserk Bear: A Decade's Activity Targeting Critical Infrastructure" | https://vblocalhost.com/uploads/VB2021-Slowik.pdf / | 7 October 2021 | Accessed on 3 May 2022 | The source is publicly available information and does not contain classification markings]

[33] [MITRE | “Backdoor.Oldrea” | https://attack.mitre.org/software/S0093/ | 12 October 2022 | Accessed on 15 November 2022 | The source is publicly available information and does not contain classification markings]

[34] [Broadcom | A L Johnson | “Dragonfly: Western Energy Companies Under Sabotage Threat” | https://community.broadcom.com/symantecenterprise/viewdocument/dragonfly-western-energy-companies?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments | 30 June 2014 | Accessed on 15 November 2022 | The source is publicly available information and does not contain classification markings]

[35] [Belden | Joel Langill | “Defending Against the Dragonfly Cyber Security Attacks” | https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en | 22 October 2014 | Accessed on 17 November 2022 | The source is publicly available information and does not contain classification markings]

[36] [MITRE | “Backdoor.Oldrea” | https://attack.mitre.org/software/S0093/ | 12 October 2022 | Accessed on 15 November 2022 | The source is publicly available information and does not contain classification markings]

[37] [Dover Microsystems | “German Steel Mill Attack” | https://www.dovermicrosystems.com/case-study/german-steel-mill-cyberattack/ | 2022 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[38] [Federal Office for Information Security (BSI) | “The State of IT Security in Germany 2014” | https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3 | November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[39] [Dover Microsystems | “German Steel Mill Attack” | https://www.dovermicrosystems.com/case-study/german-steel-mill-cyberattack/ | 2022 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[40] [Dover Microsystems | “German Steel Mill Attack” | https://www.dovermicrosystems.com/case-study/german-steel-mill-cyberattack/ | 2022 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[41] [Federal Office for Information Security (BSI) | "The State of IT Security in Germany 2014" | https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3 | November 2021 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[42] [Capitol Technology University | Scott Buchanan | "Cyber-Attacks To Industrial Control Systems Since Stuxnet" | https://www.proquest.com/openview/4be679a2dcfa686903463391d5dde19b/ 1?pq-origsite=gscholar&cbl=18750&diss=y%20 |10 April 2022 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]