CASE STUDY: TRITON MALWARE ATTACK AGAINST PETRO RABIGH

Cybersecurity for the Operational Technology Environment (CyOTE)

30 JUNE 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-67981

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

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

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

TABLE OF CONTENTS

FIGURES

TABLES

CASE STUDY: TRITON MALWARE ATTACK AGAINST PETRO RABIGH

1. EXECUTIVE SUMMARY

The Triton Malware Attack Against Petro Rabigh Case Study leverages publicly available information about the cyber attack on Saudi Arabia-based Rabigh Refining & Petrochemical Company (Petro Rabigh) 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.

Adversaries gained initial access to the Information Technology (IT) network of Petro Rabigh by May 2017, at least 90 days before initiating the Triton malware attack. On 2 June, the implanted Triton malware accidently shut down one Safety Instrumented System (SIS) controller that resulted in a halt in refinery operations. Refinery engineers determined the shutdown was a mechanical error and the refinery resumed operations after seven days.

Without victim comprehension of the shutdown being caused by a cyber attack, adversaries had another two months of unimpeded access to the network, during which they tested executables multiple times.

On 4 August, the adversaries triggered the malware, causing six of Petro Rabigh's Triconex SIS controllers to initiate a safety shutdown. While the attack did not cause physical damage, it again disrupted the refinery's industrial processes and halted operations. Petro Rabigh was inoperable for another 10 days and lost approximately $938,000 in revenue.[1] Though no catastrophic impact occurred either time, Dragos believes the way the adversaries targeted the six controllers potentially could have caused major physical damage and loss of human life.[2]

Researchers and analysts identified 20 techniques utilized during the attack with a total of 46 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, the victim may achieve earlier comprehension of malicious activity. Seventeen of the identified techniques used during the Petro Rabigh cyber attack were precursors to the triggering event. Case study analysis identified 41 observables associated with these precursor techniques, 14 of which were assessed to have an increased likelihood of being perceived in the 90 days preceding the execution of the malware. The response and comprehension time could have been reduced to less than 10 days if these observables had been identified earlier.

The information gathered in this case study contributes to a library of observables tied to a repository of artifacts, data sources, technique detection capabilities, and procedural recipes 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 asset owners and operators (AOOs) 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, 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 AOOs in prioritizing their OT environment visibility investments.

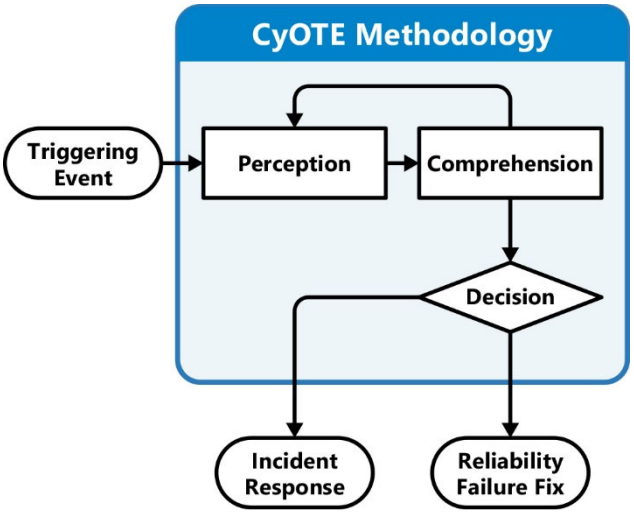


Figure 1. CyOTE Methodology

Case studies such as this one support continued learning through analysis of historical incidents that have impacted OT. This case study 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 AOOs to independently identify observables associated with techniques known to be indicators of attack within OT environments. The identified observables highlight anomalous events for further investigation, which could enhance comprehension of malicious activity.

A timeline of events based on the CyOTE methodology portrays the attack-related observables associated with the case study's cyber attack. The timeline includes assessed dates, the triggering event, and comprehension of malicious activity by the AOO. The point on this timeline when each technique appears is critical to the AOO'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 AOOs to detect those observables. If a technique includes

effects which AOOs 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 AOOs with a library of observables reported in each historical case. The library can be used in conjunction with a repository of artifacts, data sources, technique detection capabilities, and procedural recipes to support the comprehension of indicators of attack.

A Bayesian network was developed to quantify the risk associated with combinations of observables and artifacts. The Bayesian network models expert belief systems about adversary behavior by defining probabilistic relationships between observables and potential adversary behavior. The likelihood of malicious behavior is updated as each piece of new evidence is introduced through perception of more observables. The model's purpose is to enhance the process of comprehending adversary behavior given the perception of observables and subsequent collection of artifacts during an investigation. Section 4 demonstrates the overall likelihood of adversary behavior.

2.2. BACKGROUND ON THE ATTACK

Adversaries gained initial access to the Information Technology (IT) network of the Saudi Petro Rabigh refinery by May 2017, at least 90 days (D-90) before initiating the attack.

At 7:43 PM on 4 August (D-0), the adversaries activated the Triton malware they implanted in the target networks, causing six Schneider Electric Triconex Safety Instrumented System (SIS) controllers to initiate a safety shutdown. As a result, the refinery equipment was shut down for 10 days, prompting asset owners to begin an investigation.[3] During the investigation, responders determined the SIS controllers had initiated a safe shutdown after the application code between redundant processing units failed a validation check.[4]

Saudi Aramco responded to the incident, though the researchers did not fully understand the Triton malware until much later. Petro Rabigh officials announced the outage was resolved on 14 August (D+10).[5] Full comprehension of the attack did not occur until November (D+90), when Dragos released their analysis of the Triton malware used in this ICS-tailored attack.[6]

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

The adversaries gained unauthorized access to the company's IT networks through a poorly configured firewall no later than May 2017.[7] Specific indicators for intrusion, such as formatting logs, execution of files, and gaining access to an SIS engineering workstation, began around 23 May (D-73). [8] From then until the attack was initiated, the adversaries focused their efforts on gaining access to the Operational Technology (OT) network by utilizing tools to enable network reconnaissance, lateral movement, and persistent presence in the target environment.[9]

Adversaries accidently shut down one Triconex system on 2 June, initiating an investigation by company engineers. However, Petro Rabigh staff brought systems back online after a week, as Schneider Electric engineers attributed the attack to a mechanical failure.[10]

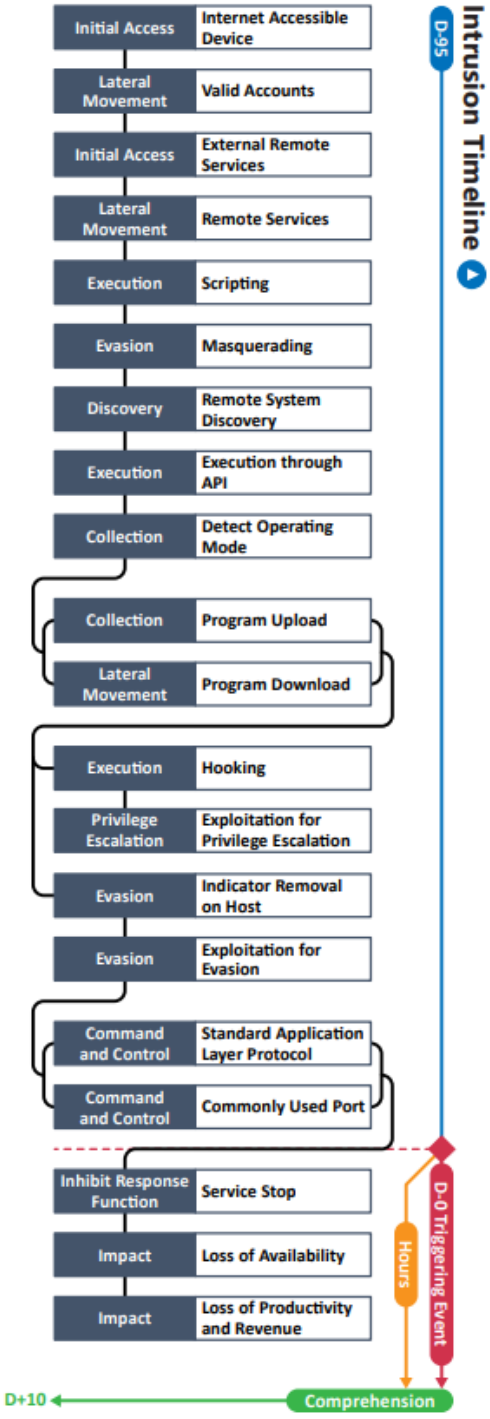


Figure 2. Intrusion Timeline

The triggering event on 4 August (D-0) occurred when the main processor for the burner management system caused a redundancy alarm, forcing six infected Triconex systems to start

the safety shutdown protocol.[11] This resulted in a disruption of the refinery's industrial processes and a complete shutdown of the facility. Though no catastrophic physical disaster occurred either time, commercial analysts believe the way adversaries targeted the six controllers could have caused major damage and loss of human life.[12]

Incident responders arrived shortly after the shutdown, but operations did not resume until 14 August (D+10), resulting in an estimated $938,000 in lost revenue.

Analysis identified 20 techniques in a sequence and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework version 3.2.

Table 1. Techniques Used in the Triton Cyber Attack

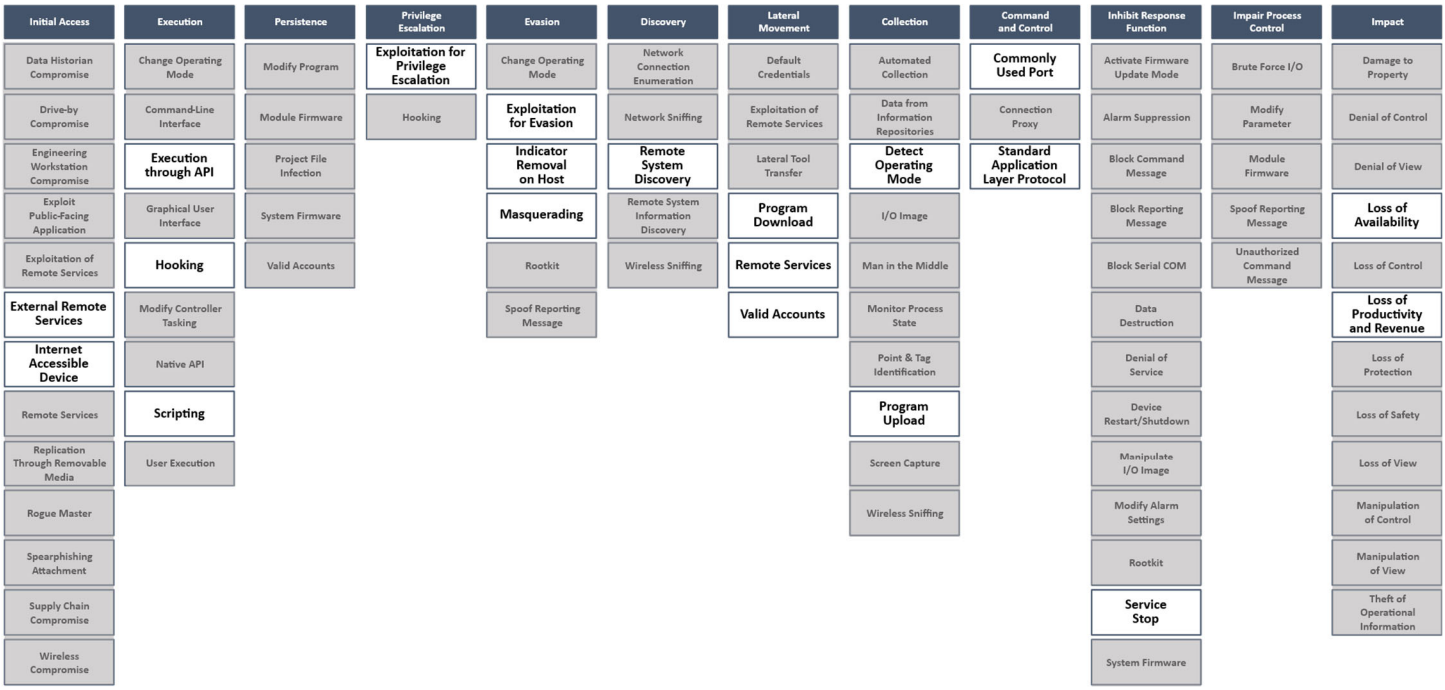


Table 2. Case Study Quantitative Summary

Case Study Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	20
Technique Observables	46
Precursor Techniques	17
Precursor Technique Observables	41
Highly Perceivable Precursor Technique Observable	14

3. OBSERVABLE AND TECHNIQUE ANALYSIS

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

3.1. INTERNET ACCESSIBLE DEVICE TECHNIQUE (T0883) FOR INITIAL ACCESS

Adversaries were able to gain initial remote access to the system by utilizing a poorly configured firewall directly exposed to the Internet, suggesting the use of the Internet Accessible Device technique (T0883). The adversaries pivoted from the Internet-accessible IT systems to the OT networks that hosted Schneider Electric safety systems. They employed credential harvesting tools such as Mimikatz, SecHack, a Cryptcat-based backdoor, a PLINK-based backdoor, and WebShell.[13]

IT Staff and IT Cybersecurity personnel may have been able to observe the usage of attack tools, though adversaries used multiple techniques to hide their activities, cover their tracks, and deter forensic examination of their tools and activities.[14]

A total of five observables were identified with the use of the Internet Accessible Device technique (T0883). This technique is important for investigation as it may allow adversaries to move directly into a control system network. This technique appears early in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent adversaries from accessing the SIS equipment, thus preventing an operational shutdown.

Of the five observables associated with this technique, one is assessed to be highly perceivable (Mimikatz Traffic). Please see Appendix A for the list of observables.

Please see Figure 3 for comprehension of the Internet Accessible Device technique using the risk model.[a] Given the five identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

[a] See Appendix D for a detailed walkthrough of how the risk model supports comprehension using a sample technique

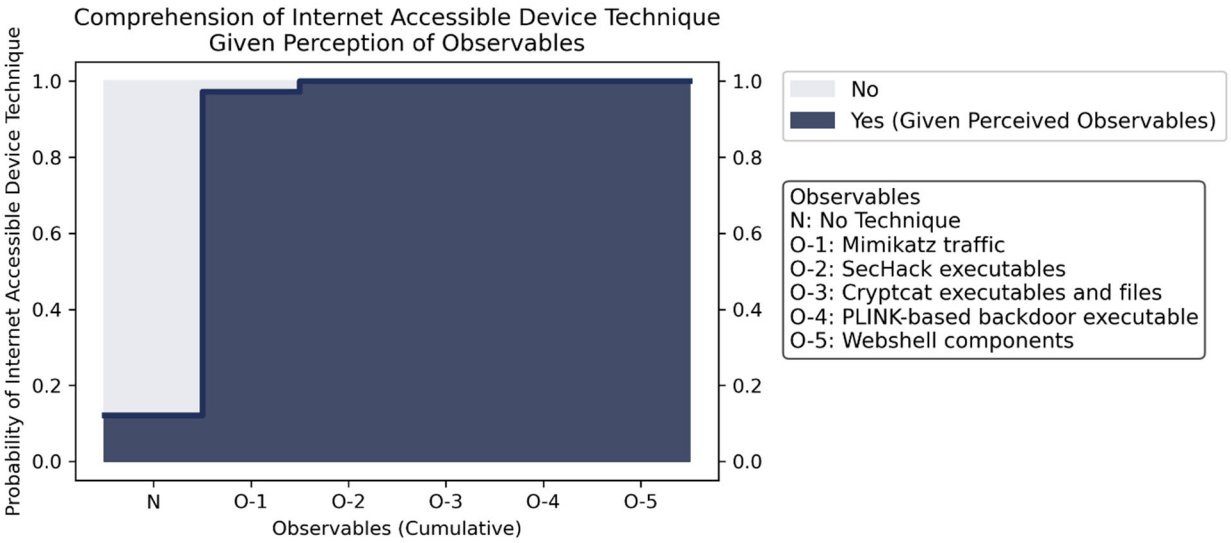


Figure 3: Internet Accessible Device Technique (T0883) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 23 artifacts could be generated by the Internet Accessible Device technique
Technique Observers[b]	IT Staff, IT Cybersecurity

[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. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

Around 29 May, adversaries used a historian server and stolen administrator login credentials to remotely access an engineering workstation that was part of the refinery's distributed control system (DCS).[15] Administrator credentials were stolen using tools introduced in the previous technique, Mimikatz and SecHack.[16] This unauthorized access increased adversary privileges to connected SIS devices, including the Tristation Engineering Workstation and Triconex controllers.

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe the use of the Valid Accounts technique (T0859) if proper account login notification parameters had been set.

A total of two observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because compromised credentials may be used to bypass access controls to various resources within a network or grant an adversary increased privileges to specific systems and devices. This technique typically appears early in the timeline and responding to it will effectively limit access to protected systems. Terminating the chain of techniques at this point would protect SIS devices from unauthorized access.

Of the two observables associated with this technique, one is assessed to be highly perceivable (Mimikatz Traffic). Please see Appendix A for the list of observables.

Please see Figure 4 for comprehension of the Valid Accounts technique using the risk model. Given the two identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

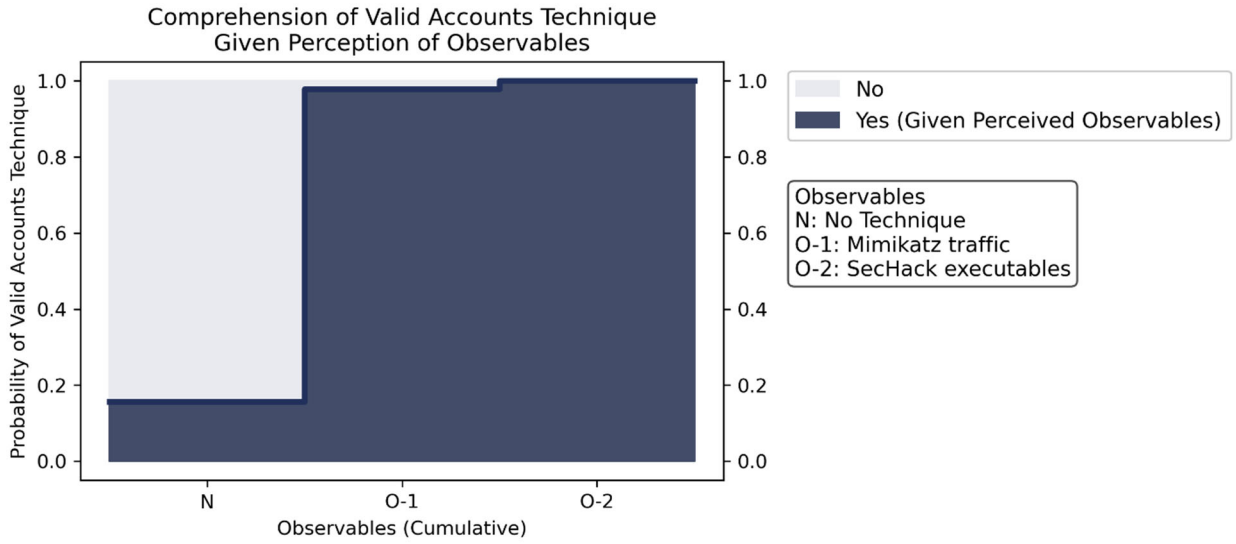


Figure 4: Valid Accounts Technique (T0859) Risk Assessment

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

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

Adversaries pivoted to the OT network by using the External Remote Services technique (T0822). The refinery's perimeter virtual private network (VPN) was compromised and infiltrated during off-hour times to reduce the chance of being observed during higher-risk activities.[17,18] As a result, adversaries compromised the poorly configured demilitarized zone (DMZ), despite apparent proper architecture implementation of a firewall to separate IT and OT networks.[19]

During initial access, adversaries accessed Triconex SIS log files and sought to disable the company's cybersecurity systems.[20]

OT Cybersecurity, IT Cybersecurity, and IT Staff may be able to observe VPN logon anomalies or unauthorized VPN access.

A total of two observables were identified with the use of the External Remote Services technique (T0822). This technique is important for investigation because it allows adversaries to proliferate to the OT network, granting administration of control networks from outside the system. This technique appears early in the timeline and terminating the chain of techniques at this point would prevent adversaries from gaining access to internal operational networks and delivering malicious payloads.

The two observables associated with this technique are both assessed to be highly perceivable (Unauthorized VPN Access; VPN Logon Anomalies). Please see Appendix A for the list of observables.

Please see Figure 5 for comprehension of the External Remote Services technique using the risk model. Given the two identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

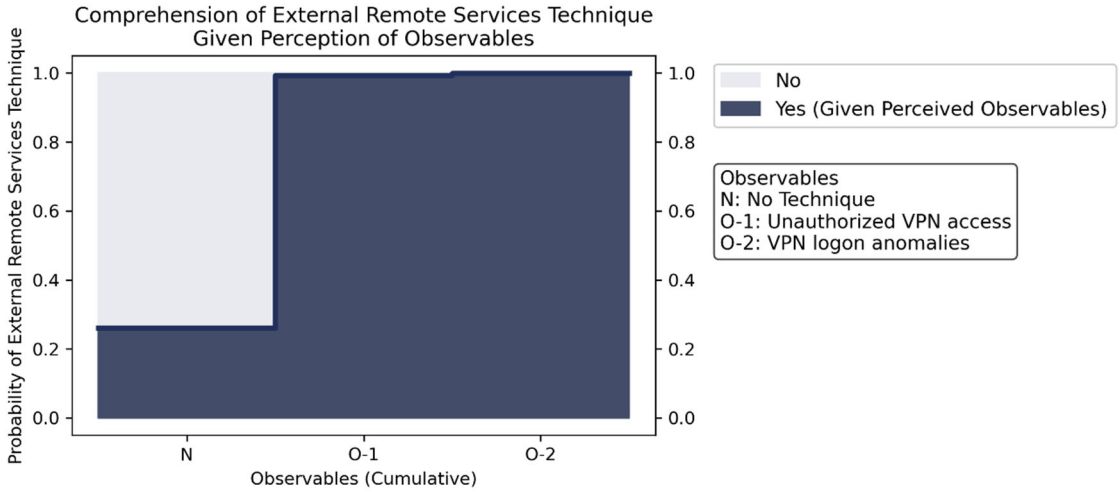


Figure 5: External Remote Services Technique (T0822) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 56 artifacts could be generated by the External Remote Services technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

3.4. REMOTE SERVICES TECHNIQUE (T0886) FOR LATERAL MOVEMENT

With access to IT and OT networks, windows event logs showed adversaries had accessed the plant's SIS engineering workstations via the remote desktop protocol (RDP).[21] As part of this technique, adversaries routinely used standard tools that would hide activity by mimicking legitimate administrator activities with heavy use of RDP and PsExec/WinRM, or relying on encrypted SSH-based tunnels to transfer tools and for remote command/program execution.[22] With RDP connections, a back door utilizing tools from Internet Accessible Device technique (T0883) was installed on the SIS engineering workstation on 29 May, allowing an unauthorized user to gain access to the same workstation in the future.[23]

OT Cybersecurity, IT Cybersecurity, and IT Staff could observe associated traffic within the DMZ, including Remote Procedure Protocol (RPC), Windows Management Instrumentation (WMI), and SSH.

A total of seven observables were identified with the use of the Remote Services technique (T0886). This technique is important for investigation as it allows adversaries to move between assets and network segments, resulting in the ability to configure systems. This technique appears early on the attack timeline and terminating the chain of techniques at this point would have limited the adversaries to initial access points, resulting in a halt of attack execution.

Of the seven observables associated with this technique, one is assessed to be highly perceivable (Use of Windows Task Scheduler to Execute Programs). Please see Appendix A for the list of observables.

Please see Figure 6 for comprehension of the Remote Services technique using the risk model. Given the seven identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

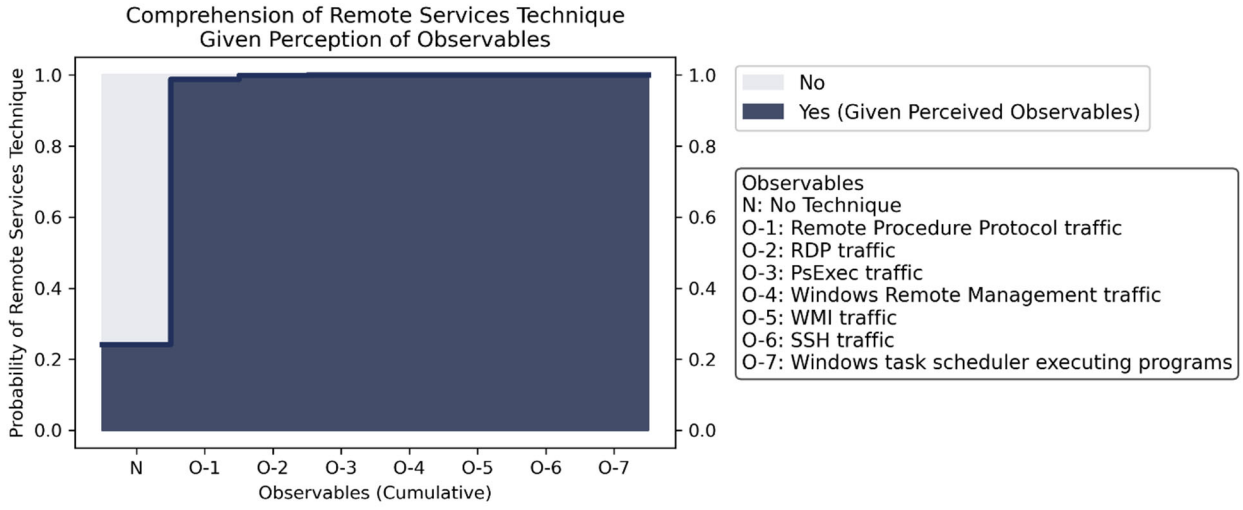


Figure 6: Remote Services Technique (T0886) Risk Assessment

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

3.5. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

After access was gained to the SIS engineering workstation, adversaries executed Triton malware through the main HatMan (Py2EXE) Python script.[24] The adversaries' first step after access is to execute the main HatMan Python script, which is script_test.py compiled into trilog.exe. This trilog.exe script leverages a custom implementation of the internal proprietary TriStation protocol (library.zip).[25]

Once a script is installed, adversaries can access the controller to gather information about the system state.[26] On 2 June, a package of software applications on a SIS device connected to an engineering workstation, enabling the deployment of an earlier Triton malware version. Within minutes of the malware installation, the Triconex SIS controller detected a fault, causing an unintended emergency shutdown of the refinery for a week.[27]

OT Staff, Engineering, OT Cybersecurity, and IT Cybersecurity staff could have observed the use of the Scripting technique (T0853) had the first emergency shutdown on 2 June resulted in an investigation; however, engineering staff brought systems back online without a thorough cybersecurity investigation.

A total of three observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because scripting can be abused by adversaries to execute code in the target environment. Terminating the chain of techniques at this point would have prevented the 4 August shutdown.

The three observables associated with this technique are not assessed to be highly perceivable. Please see Appendix A for the list of observables.

Please see Figure 7 for comprehension of the Scripting technique using the risk model. Given the three identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

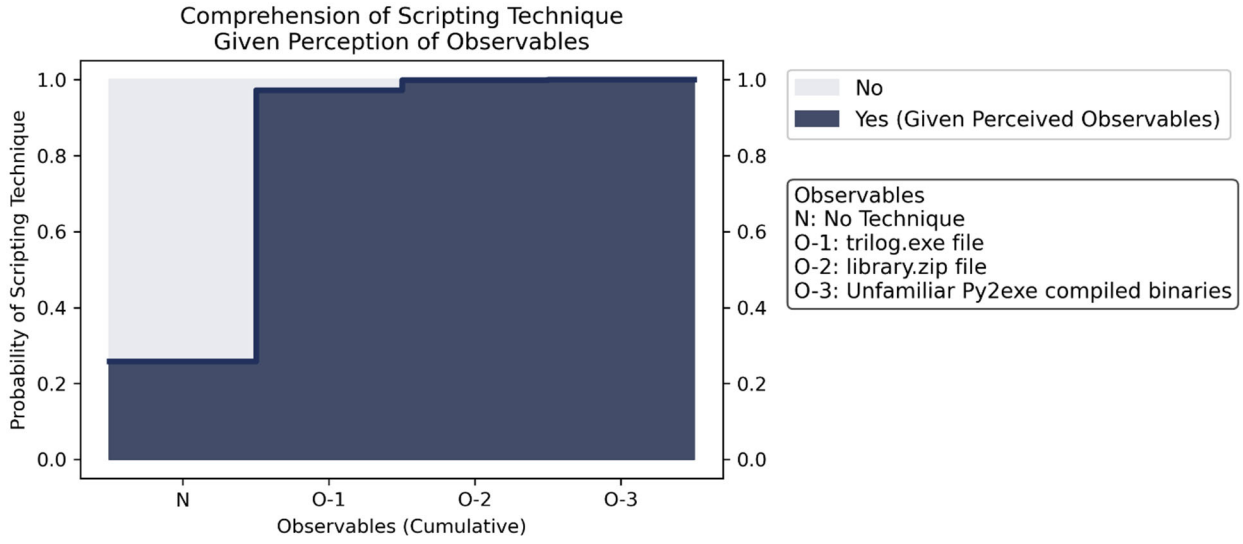


Figure 7: Scripting Technique (T0853) Risk Assessment

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

3.6. MASQUERADING TECHNIQUE (T0849) FOR EVASION

The Triton malware, trilog.exe, masquerades as the legitimate Triconex Trilog application. Adversaries used multiple staging folders and opted to use directories used infrequently by legitimate users or processes. By renaming the tools, it is difficult to identify the malware's purpose, even if it was deleted from the disk through residual artifacts (e.g., ShimCache entries or WMI Recently Used Apps).[28]

IT Cybersecurity or OT Cybersecurity staff may have observed this technique if there was a process implemented to alert staff of the unauthorized creation of files.

A total of five observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation as adversaries purposely disguise files so staff may not suspect malicious applications or executables. Operators and engineers may not notice the presence of the underlying malicious content and ultimately run files masquerading as legitimate files. This technique appears further along the attack timeline and responding to it would allow staff to inhibit the execution of malicious files. Terminating the chain of techniques at this point would limit adversaries to reconnaissance activity.

The five observables associated with this technique are not assessed to be highly perceivable. Please see Appendix A for the list of observables.

Please see Figure 8 for comprehension of the Masquerading technique using the risk model. Given the five identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

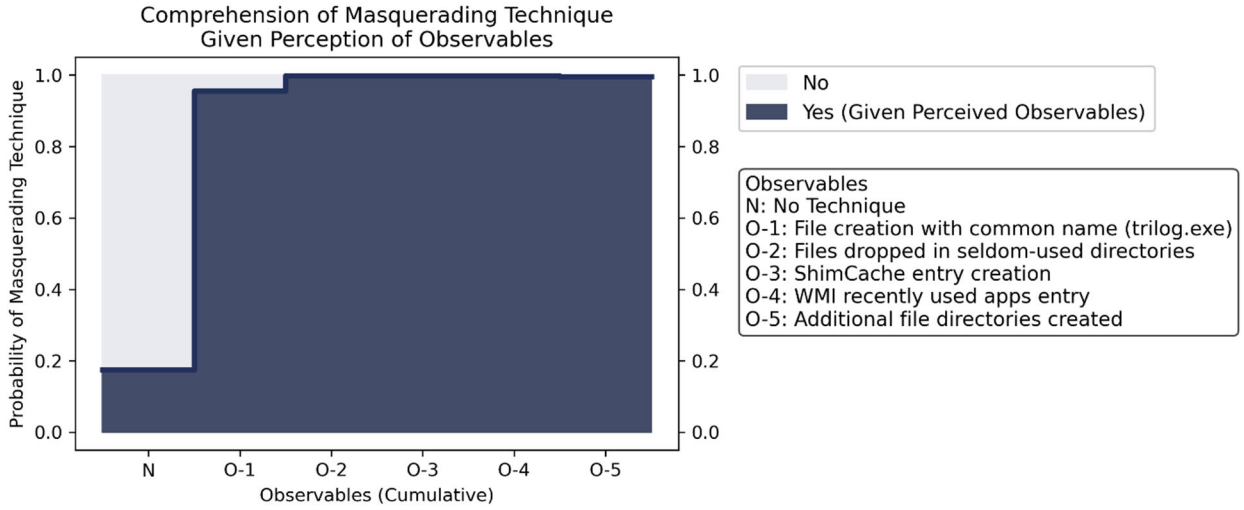


Figure 8: Masquerading Technique (T0849) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 15 artifacts could be generated by the Masquerading technique
Technique Observers	IT Cybersecurity, OT Cybersecurity

3.7. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

Triton malware uses a Python script capable of auto detecting Triconex controllers on the network by sending a specific UDP broadcast packet over Port 1502. The ability to auto scan a network is an application of the Remote System Discovery technique (T0846). This function was not used in the accidental shutdown triggered on 2 June.[29]

With the use of the Remote System Discovery technique (T0846), Engineering, OT Cybersecurity, and IT Cybersecurity could observe IP addresses present on Port 1502.

One observable was identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation since adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifiers on a network that may be used for lateral movement or discovery techniques.

The one observable associated with this technique is not assessed to be highly perceivable. Please see Appendix A for the list of observables.

Please see Figure 9 for comprehension of the Remote System Discovery technique using the risk model. Given the one identified observable, the adversary's use of this technique is very likely. Two diagnostic artifacts for the risk model were selected from the set of 43 artifacts to enhance comprehension of the technique. Given the observable and artifacts, the adversary's use of this technique is almost certain.

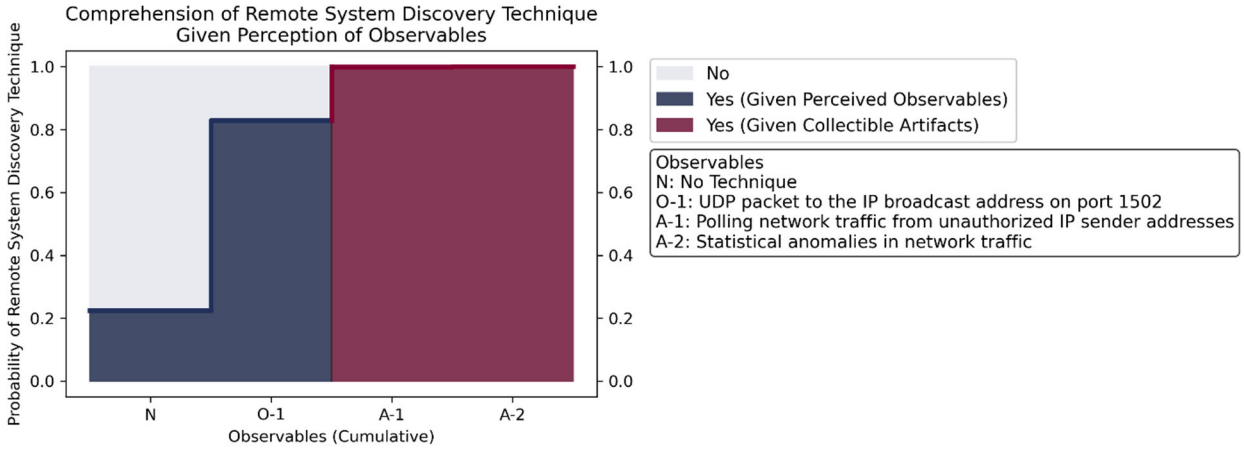


Figure 9: Remote System Discovery Technique (T0846) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 43 artifacts could be generated by the Remote System Discovery technique
Technique Observers	Engineering, OT Cybersecurity, IT Cybersecurity

3.8. EXECUTION THROUGH API TECHNIQUE (T0871) FOR EXECUTION

Triton malware leverages the Execution Through API technique (T0871) by using a reconstructed TriStation protocol within its framework to trigger application program interfaces (API) related to program download, program allocation, and program changes.[30]

The Triton malware framework allows the SIS workstation to interact with a Tricon controller via the unauthenticated TriStation protocol over Ethernet. The malware is capable of reading and writing control programs and data, running and halting a program, and retrieving status information.[31]

Engineering, OT Cybersecurity, and IT Cybersecurity staff may have observed activity related to the Execution Through API technique (T0871).

A total of two observables were identified with the use of the Execution Through API technique (T0871). This technique is important for investigation as adversaries may attempt to leverage APIs used for communication between control software and hardware. This technique appears later in the attack timeline and responding to it will limit the available communication methods between assets.

The two observables associated with this technique are assessed to be highly perceivable (Increase in UDP Pings and Connection Requests Compared to Baseline for TriStation Traffic; Network Traffic Between SIS Workstation and Controller During Off-Hours). Please see Appendix A for the list of observables.

Please see Figure 10 for comprehension of the Execution Through API technique using the risk model. Given the two identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

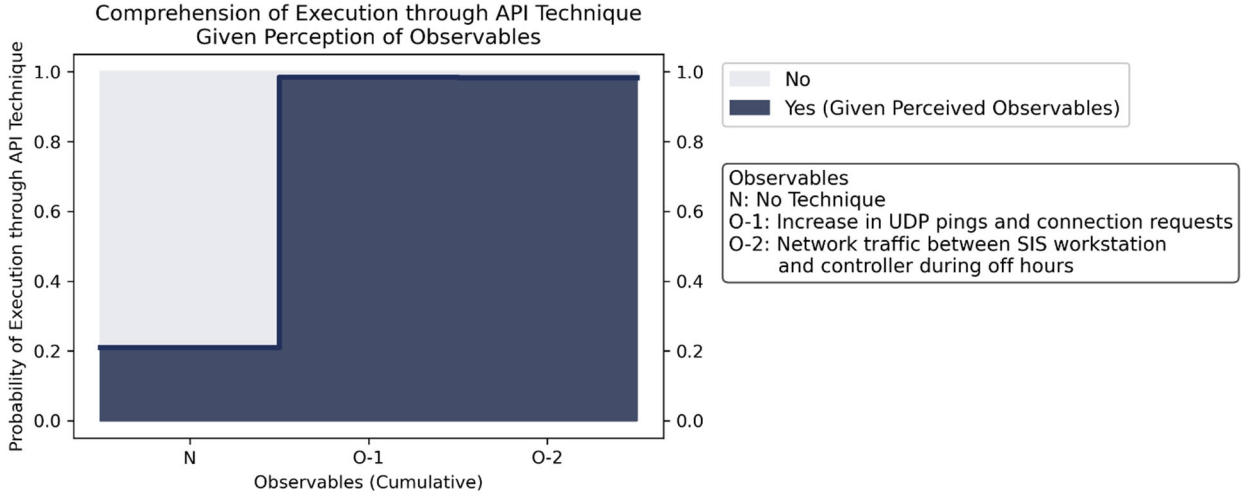


Figure 10: Execution through API Technique (T0871) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 19 artifacts could be generated by the Execution through API technique
Technique Observers	Engineering, OT Cybersecurity, IT Cybersecurity

3.9. DETECT OPERATING MODE TECHNIQUE (T0868) FOR COLLECTION

For collection, the Triton malware script connects to a Tricon Communication Module (TCM) to determine if the controller could be compromised. More specifically, an instance of trilog.exe was invoked separately for each target controller. Once invoked, trilog.exe determined if a controller could be compromised by reading the configuration information exposed by the TriStation protocol.[32]

OT Cybersecurity and IT Cybersecurity personnel may be able to observe the traffic associated with this technique.

Two observables were identified with the use of the Detect Operating Mode technique (T0868). This technique is important for investigation because it allows adversaries to gather information on a programmable logic controller (PLC) or controller's current operating mode. The difference in operating modes dictates what change or maintenance functions can be manipulated. This technique appears relatively late in the attack timeline, after access to identified assets is achieved, and responding to it will restrict adversaries' knowledge and ability to reprogram the PLC.

Of the two observables associated with this technique, one is assessed to be highly perceivable (Traffic from Script to TCM). Please see Appendix A for the list of observables.

Please see Figure 11 for comprehension of the Detect Operating Mode technique using the risk model. Given the two identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

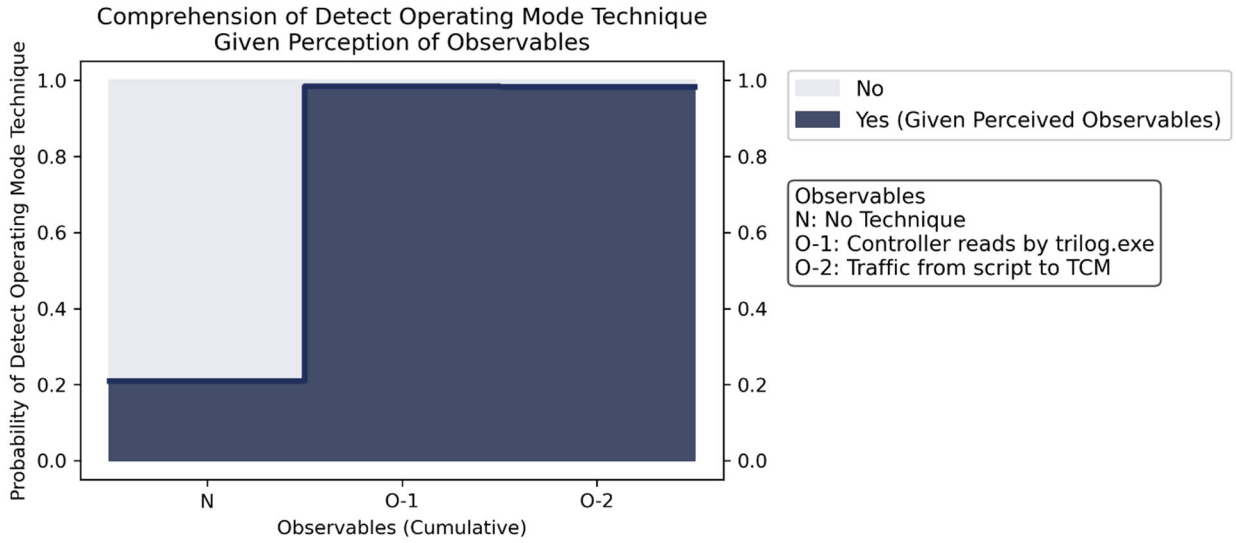


Figure 11: Detect Operating Mode Technique (T0868) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 8 artifacts could be generated by the Detect Operating Mode technique
Technique Observers	OT Cybersecurity, IT Cybersecurity

3.10. PROGRAM UPLOAD TECHNIQUE (T0845) FOR COLLECTION

The Program Upload technique (T0845) and the Program Download technique (T0843) (see Section 3.11) were utilized to deploy the payload.[33] Triton malware calls SafeAppendProgramMod to transfer its payloads to the Triconex controller, which includes performing a program upload. The Python function in the Triton malware counts the number of programs and functions on the controller and tries to retrieve the final program in the program list. If this retrieval is successful, execution continues with attempts to allocate or write the program slot using "download changes."[34]

OT Staff, Engineering, OT Cybersecurity, and IT Cybersecurity could observe abnormal activity in the event logs if the logs are configured appropriately.

One observable was identified with the use of the Program Upload technique (T0845). This technique is important for investigation, as uploading a program allows adversaries to acquire and study the underlying logic of a PLC. This technique appears close to the triggering event and responding to it will prevent the software from uploading to workstations, jump boxes, or an interfacing device. Terminating the chain of techniques at this point would prevent the malicious files from executing.

The one observable associated with this technique is assessed to be highly perceivable (Application Event Log of the SafeAppendProgramMod Transferring Data to Tricon). Please see Appendix A for the list of observables.

Please see Figure 12 for comprehension of the Program Upload technique using the risk model. Given the one identified observable, the adversary's use of this technique is very likely. Three diagnostic artifacts were selected for the risk model from the set of 14 artifacts to enhance comprehension of the technique. Given the observable and artifacts, the adversary's use of this technique is almost certain.

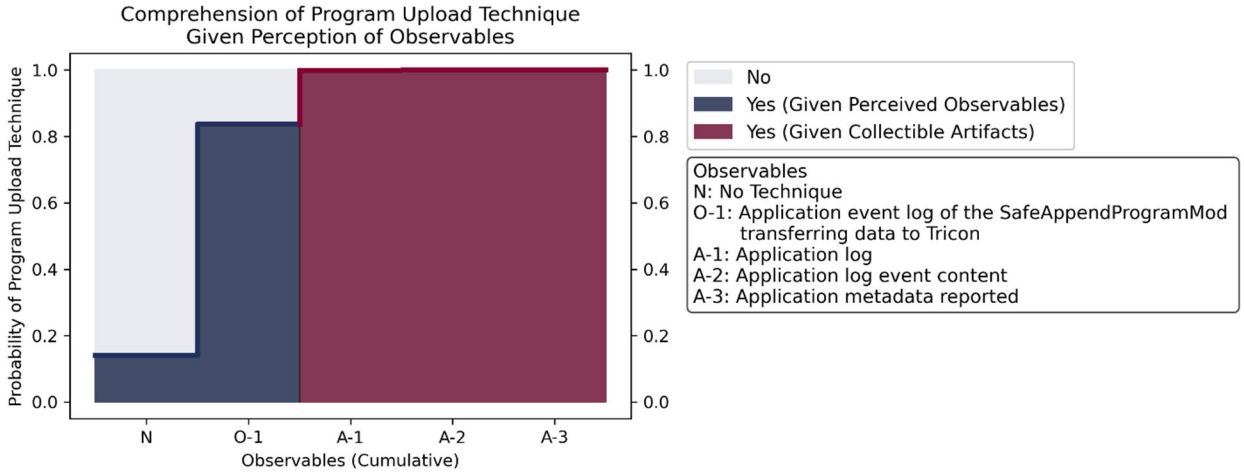


Figure 12: Program Upload Technique (T0845) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 14 artifacts could be generated by the Program Upload technique
Technique Observers	OT Staff, Engineering, OT Cybersecurity, IT Cybersecurity

3.11. PROGRAM DOWNLOAD TECHNIQUE (T0843) FOR LATERAL MOVEMENT

After verification of PROGRAM mode on the Triconex controller, the script downloads a small PowerPC program (PresetStatus), allowing trilog.exe to encode two payload files (inject.bin and imain.bin). Then, as payload files are passed to the communication libraries to be appended using Program Download technique (T0843), the malware sets a control value in the Triconex controller program memory and execution table. Once this program has finished running, the script checks whether the injector is successful.[35] During this check, operators saw safety alarms from the controllers appear on the screen but dismissed them, as procedures indicated the alarms only needed to be acknowledged once per day.[36]

Variations of program downloads allow a controller to continue running during the transfer and reconfiguration process without interruption to process control. However, a stop state is sometimes necessary before starting a full program download. Adversaries may avoid downloading to prevent disruption of the physical processes, while Detect Operating Mode (T0868) or Change Operating Mode (T0858) techniques may be used to ensure the controller is in the proper mode to accept a program download.

OT Staff, Engineering, OT Cybersecurity, and IT Cybersecurity could observe the program state of the controller and safety alarm notifications.

Three observables were identified with the use of the Program Download technique (T0843). This technique is important for investigation since this technique allows adversaries to transfer a user program to a controller. This technique appears later in the timeline and responding to it will prevent malicious payloads from propagating to controllers.

Of the three observables associated with this technique, two are assessed to be highly perceivable (Controller in Program State; Safety Alarms Notifying Operators that Controllers were in Program Mode). Please see Appendix A for the list of observables.

Please see Figure 13 for comprehension of the Program Download technique using the risk model. Given the three identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

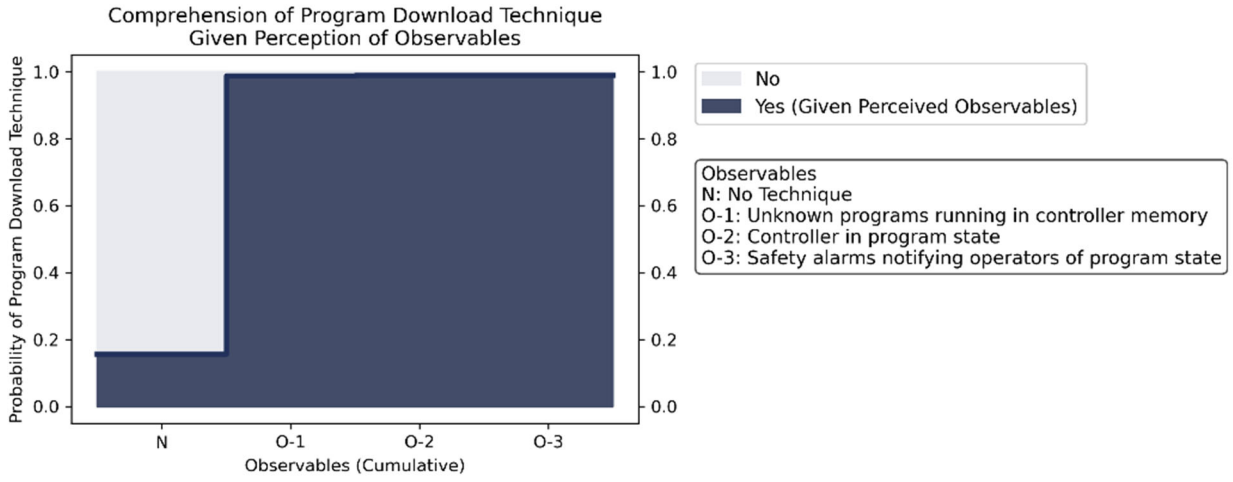


Figure 13: Program Download Technique (T0843) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 19 artifacts could be generated by the Program Download technique
Technique Observers	OT Staff, Engineering, OT Cybersecurity, IT Cybersecurity

3.12. EXPLOITATION FOR PRIVILEGE ESCALATION TECHNIQUE (T0890) FOR PRIVILEGE ESCALATION

Once the injector (inject.bin) verifies the controller can be compromised through several tests, the injector uses vulnerabilities discussed in ICS Advisory ICSA-18-107-02 to misinform or control the SIS equipment. The vulnerability affects Tricon firmware Versions 10.0 to 10.4 by allowing an insecurely written system call to be exploited to achieve an arbitrary 2-byte write primitive, resulting in escalated supervisor privileges. Using the exploit to enable supervisor privileges, the machine state register (MSR) disables instruction and data caching, allowing the rest of the code to function.[37]

OT Cybersecurity and IT Cybersecurity personnel could observe execution of the injector file.

One observable was identified with the use of the Exploitation for Privilege Escalation technique (T0890). This technique is important for investigation as it is common for adversaries to exploit software vulnerabilities in an attempt to elevate privileges via executable adversary-controlled code. While not the case with the attack on Petro Rabigh, this technique typically appears early in an attack, as adversaries may be operating within a lower privileged process when initially gaining access to a system. Terminating the chain of techniques at this point would prevent access to certain resources on a system, such as the control panel of Triconex controllers.

The one observable associated with this technique is not assessed to be highly perceivable. Please see Appendix A for the list of observables.

Please see Figure 14 for comprehension of the Exploitation for Privilege Escalation technique using the risk model. Given the one identified observable, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observable is highly diagnostic.

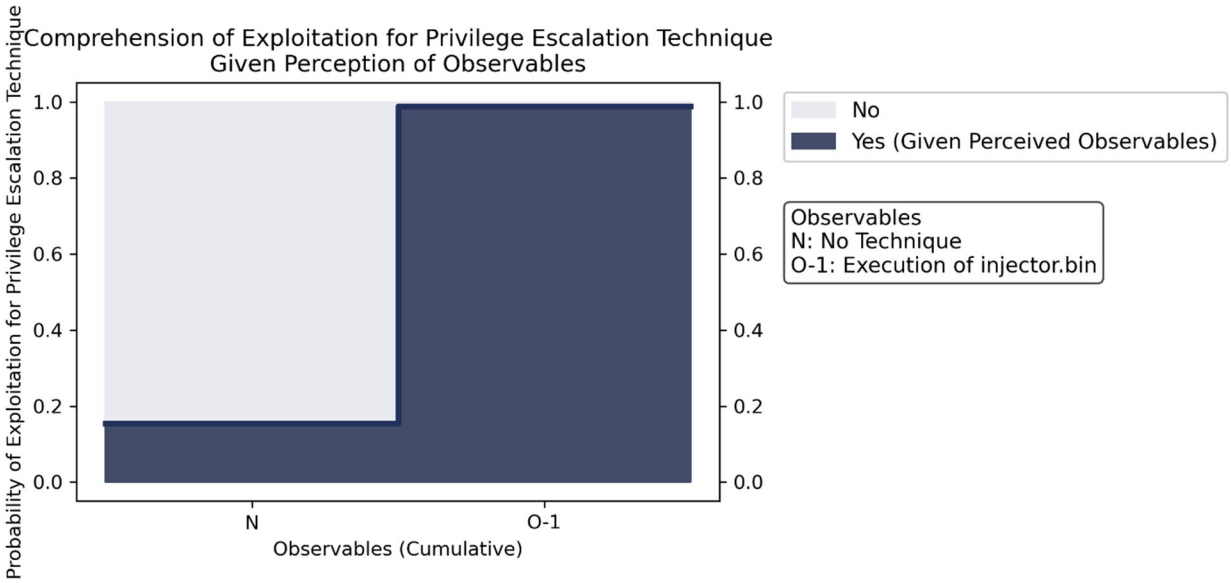


Figure 14: Exploitation for Privilege Escalation Technique (T0890) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 15 artifacts could be generated by the Exploitation for Privilege Escalation technique
Technique Observers	OT Cybersecurity, IT Cybersecurity

3.13. HOOKING TECHNIQUE (T0874) FOR EXECUTION

If the injector is successful in escalating privileges, the Hooking technique (T0874) is used to modify the address of the handler for a specific TriStation protocol command, resulting in execution of the payload upon receiving the command. The implant (imain.bin) then copies to an area within the in-memory firmware region. Afterward, the implant patches a specific network command to initiate the malicious code being called, rather than the default behavior. If these checks are successful, the imain.bin shellcode relocates and the function pointer of the TriStation command changes to the address of the relocated imain.bin, resulting in execution of the prior normal handler.

Triton malware was designed to run in device memory as a fileless malware; Triton would be removed if the controller was rebooted. At this point, the controller has been fully compromised.[38]

OT Cybersecurity and IT Cybersecurity personnel may be able to observe the shellcode that would be present on SIS controllers.

One observable was identified with the use of the Hooking technique (T0874). Terminating the chain of techniques at this point would prevent full compromise of the controller.

The one observable associated with this technique is assessed to be highly perceivable (Shellcode Present on SIS Controllers). Please see Appendix A for the list of observables.

Please see Figure 15 for comprehension of the Hooking technique using the risk model. Given the one identified observable, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observable is highly diagnostic.

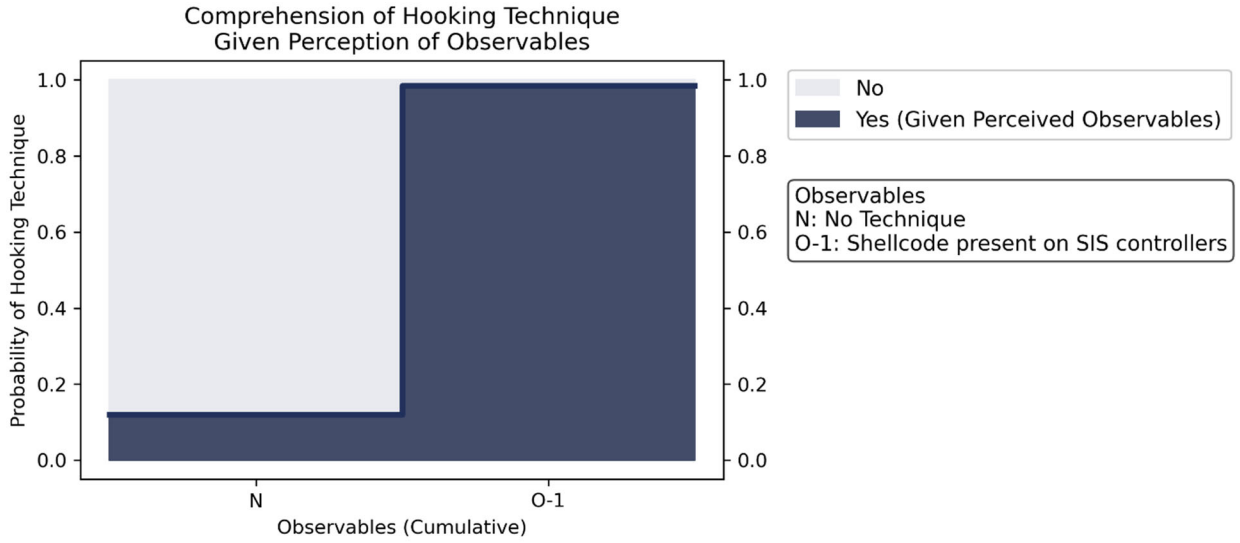


Figure 15: Hooking Technique (T0874) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 11 artifacts could be generated by the Hooking technique
Technique Observers	OT Cybersecurity, IT Cybersecurity

3.14. EXPLOITATION FOR EVASION TECHNIQUE (T0820) FOR EVASION

The Triton malware injection program exploits a vulnerability in the device firmware to disable the firmware RAM/ROM consistency check for the Exploitation for Evasion technique (T0820). Triconex systems include continuous means of detection, including checksums for firmware and program integrity, memory reference integrity, and configuration. Therefore, no fault will be generated by the controller when the firmware does not match the loaded ROM image.[39]

At this level of firmware, the perceivability of this technique's two observables is extremely low for OT Cybersecurity and IT Cybersecurity staff, although the vendor could potentially notify the end user of a vulnerability in the product.

The Exploitation for Evasion technique (T0820) is important for investigation as security features can be disabled or circumvented by exploiting vulnerabilities that may exist in software. Without patching this consistency check, the injector could write the payload into the firmware region or modify the jump table without faulting the device.[40] Please see Appendix A for the list of observables.

Please see Figure 16 for comprehension of the Exploitation for Evasion technique using the risk model. Given the two identified observables, the adversary's use of this technique is almost certain. Two artifacts were selected for the risk model from the set of 30 artifacts to enhance comprehension of the technique because the observables have extremely low perceivability. Given the observables and artifacts, the adversary's use of this technique is almost certain.

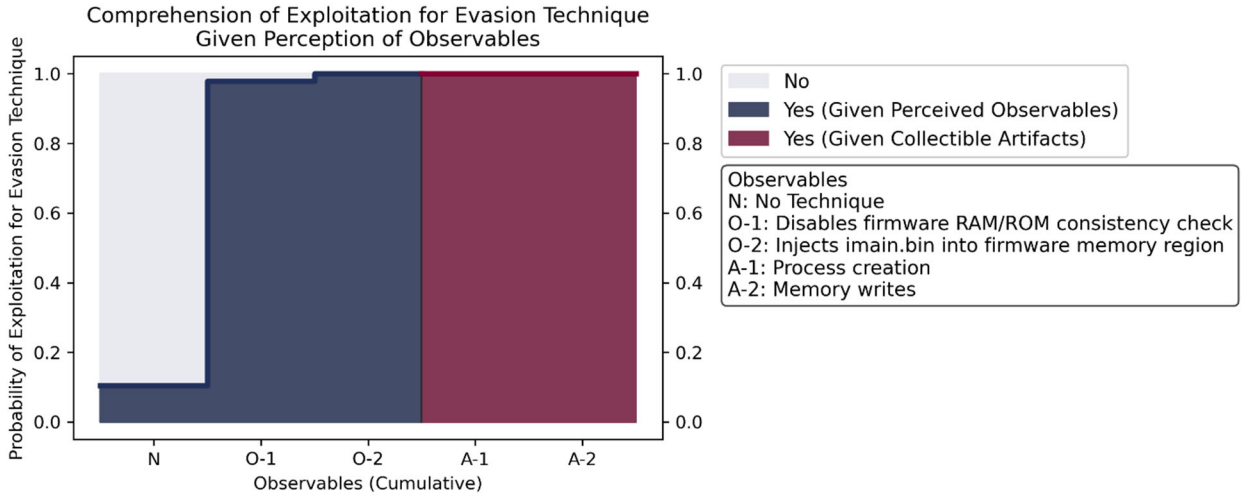


Figure 16: Exploitation for Evasion Technique (T0820) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 30 artifacts could be generated by the Exploitation for Evasion technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Support Staff

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

After the payload files are inserted into the Triconex controller memory, the script initiates a countdown to periodically check the status of the controller. If an error is detected, the communication library's method SafeAppendProgramMod attempts to reset the controller to the previous state using a TriStation protocol command. If this attempt fails, then trilog.exe attempts to write a small dummy program to memory to evade forensics, implementing the use of the Indicator Removal on Host technique (T0872).[41]

It is highly unlikely that observers, particularly OT Cybersecurity and IT Cybersecurity, would be able to detect this activity unless the attack was terminated at some earlier point in the chain, after which errant behavior of an affected controller might be identified.

A total of three observables were identified with the use of the Indicator Removal on Host technique (T0872). This technique appears later in an attack timeline and inhibits tracking of the adversaries' presence on a system by overwriting, deleting, or otherwise covering up evidence of malicious activity.

The three observables associated with this technique are not assessed to be highly perceivable. Please see Appendix A for the list of observables.

Please see Figure 17 for comprehension of the Indicator Removal on Host technique using the risk model. Given the three identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

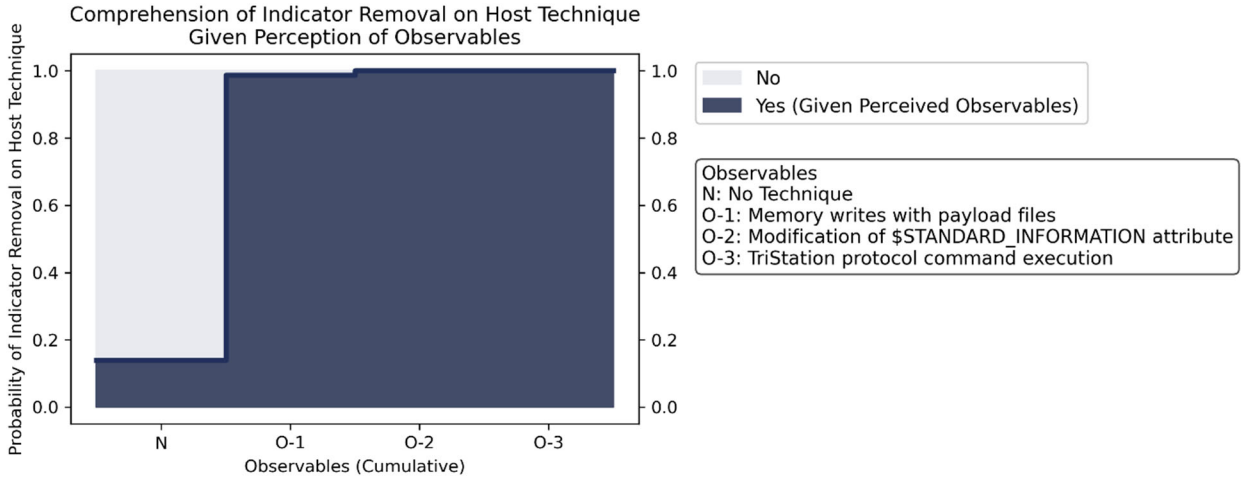


Figure 17: Indicator Removal on Host Technique (T0872) Risk Assessment

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

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

The Standard Application Layer Protocol technique (T0869) and the Commonly Used Port technique (T0885) are utilized simultaneously in this attack chain. Triton malware can communicate utilizing the TriStation "get main processor diagnostic data" command to look for a crafted packet body from which it extracts a command value and its arguments. The Python modules then expose a set of methods to interact with the compromised safety controller, regardless of the key switch position.[42]

OT Cybersecurity and IT Cybersecurity staff may observe larger than expected packets being sent to the controllers.

One highly perceivable observable (Larger than Expected Packets Sent to Controllers) was identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation as adversaries use it to disguise actions as benign network traffic. This technique appears late in the timeline, close to the triggering event, and responding to it would terminate the attack. Please see Appendix A for the list of observables.

Please see Figure 18 for comprehension of the Standard Application Layer Protocol technique using the risk model. Given the one identified observable, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observable is highly diagnostic.

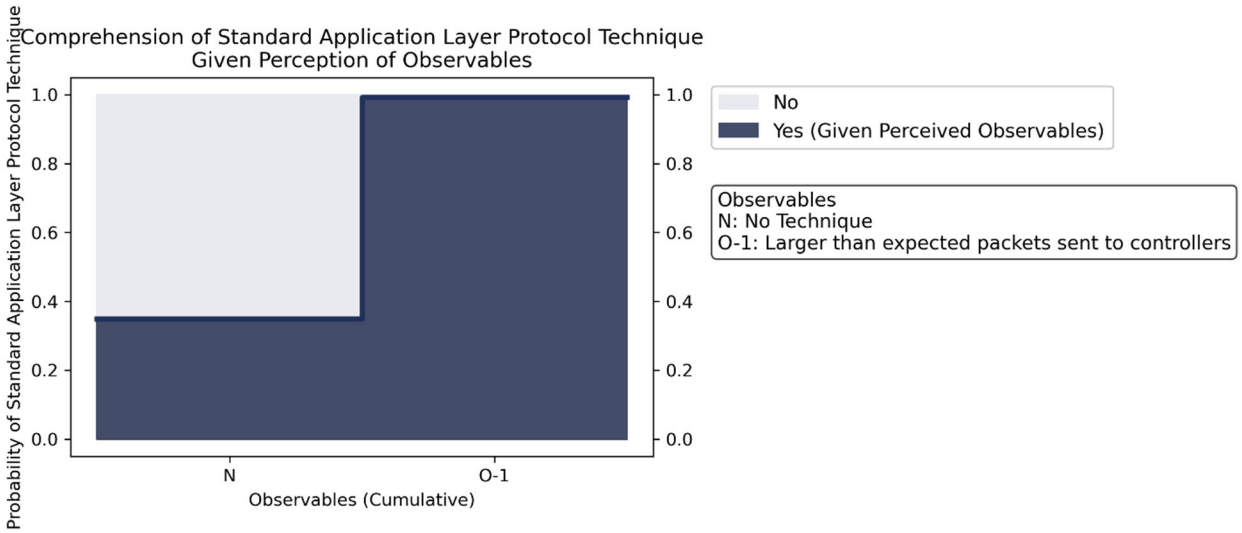


Figure 18: Standard Application Layer Protocol Technique (T0869) Risk Assessment

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

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

In association with the Standard Application Layer Protocol technique (T0869), adversaries used the Commonly Used Port technique (T0885) by employing TriStation's default UDP Port 1502 to communicate with various devices.[43] Employment of this normal port disguises the malware communication as common network traffic.

If monitoring network traffic, OT Cybersecurity and IT Cybersecurity personnel may observe unusual TriStation communication over UDP Port 1502.

One observable was identified with the use of the Commonly Used Port technique (T0885). This technique is important for investigation as adversaries may communicate over a commonly used port to bypass firewalls or network detection systems. This technique appears relatively late and is closely tied to the triggering event; responding to it will terminate the attack chain. Terminating the chain of techniques at this point would allow personnel to investigate unusual network traffic, terminating the attack.

The one observable associated with this technique is assessed to be highly perceivable (Network Traffic – Unusual TriStation Communication over UDP Port 1502). Please see Appendix A for the list of observables.

Please see Figure 19 for comprehension of the Commonly Used Port technique using the risk model. Given the one identified observable, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observable is highly diagnostic.

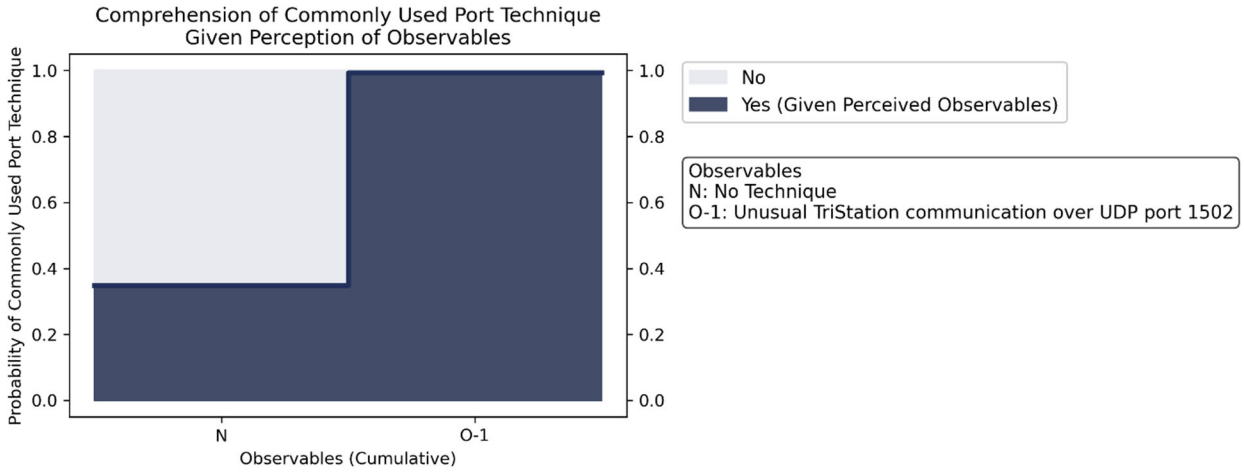


Figure 19: Commonly Used Port Technique (T0885) Risk Assessment

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

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

At 7:43 PM on 4 August, adversaries installed an updated version of the Triton malware on one controller, placing the physical key in “program” mode. Within several hours, the malware was copied across other SIS controllers before initiating the Service Stop technique (T0881). The Triton malware caused a fault detected by a Triconex SIS safety feature, triggering a second emergency shut down of the refinery.[44]

Engineering and OT Staff should be able to observe the emergency shut down system initiation.

One observable was identified with the use of the Service Stop technique (T0881). This technique is important for investigation as sometimes adversaries conduct a service stop to render services unavailable to legitimate users, possibly to conduct data destruction. In this case, this technique was the triggering event.

The one observable associated with this technique is assessed to be highly perceivable (Emergency Shut down System Initiated). Please see Appendix A for the list of observables.

Please see Figure 20 for comprehension of the Service Stop technique using the risk model. Given the one identified observable, the adversary’s use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observable is highly diagnostic.

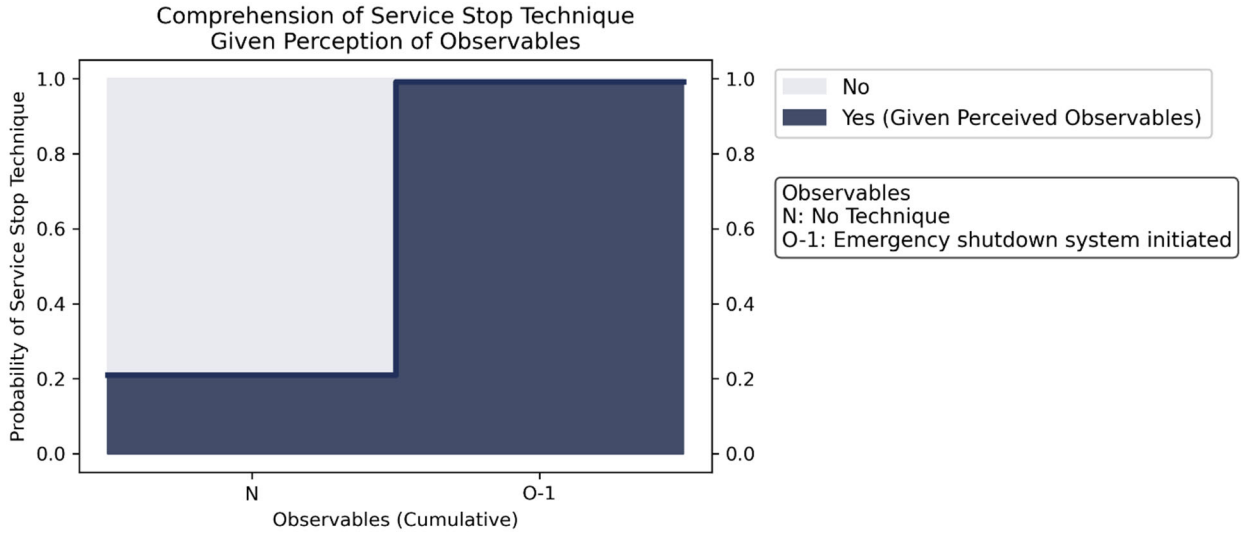


Figure 20: Service Stop Technique (T0881) Risk Assessment

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

3.19. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

The Loss of Availability technique (T0826) occurred as the emergency shutdown systems brought part of the Petro Rabigh refinery complex offline to prevent a gas release and deadly explosion.[45]

All personnel on-site and off-site would observe this event.

One observable was identified with the use of the Loss of Availability technique (T0826). This technique is important for investigation as it prevents owners and operators from delivering products or services. This technique appears after the triggering event.

The one observable associated with this technique is assessed to be highly perceivable (Emergency Shut down System Initiated). Please see Appendix A for the list of observables.

Please see Figure 21 for comprehension of the Loss of Availability technique using the risk model. Given the one identified observable, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observable is highly diagnostic.

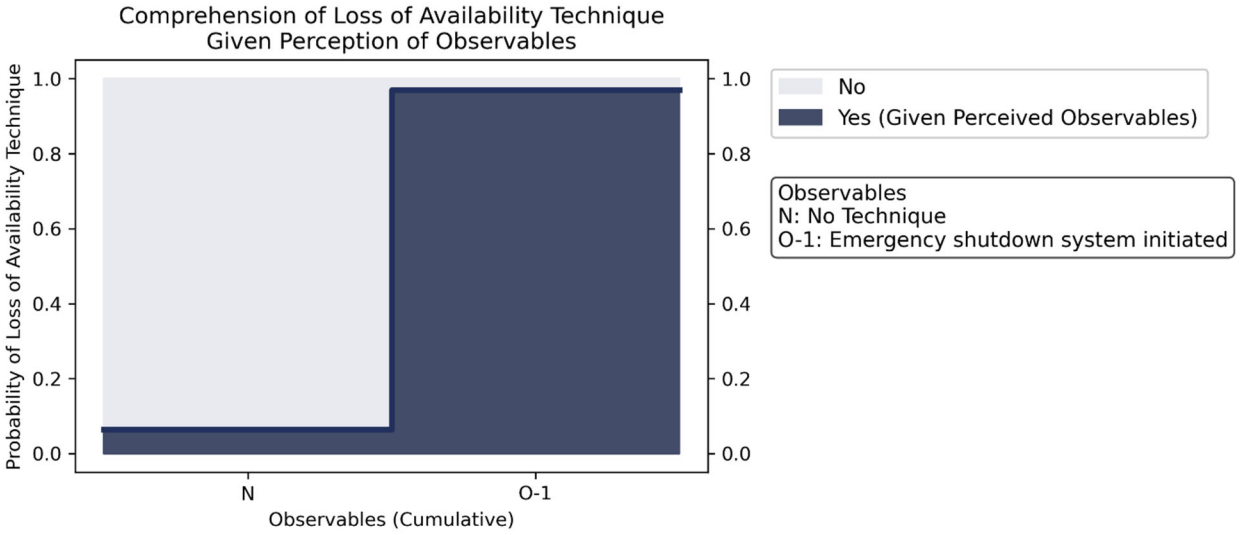


Figure 21: Loss of Availability Technique (T0826) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 8 artifacts could be generated by the Loss of Availability technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff

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

The refinery operations halted for ten days as incident responders investigated the shutdown, resulting in the Loss of Productivity and Revenue technique (T0828).[46] The ten-day shutdown resulted in the refinery losing an estimated $938,000 in revenue.[47]

Two observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation as it may present an impact for the end-users or consumers of products and services.

The two observables associated with this technique are assessed to be highly perceivable (Loss of 10 Days of Productivity; Approximately $938,000 in Lost Revenue). Please see Appendix A for the list of observables.

Please see Figure 22 for comprehension of the Loss of Productivity and Revenue technique using the risk model. Given the two identified observables, the adversary's use of this technique is almost certain. No artifacts are included for the risk model for this technique because the observables are highly diagnostic.

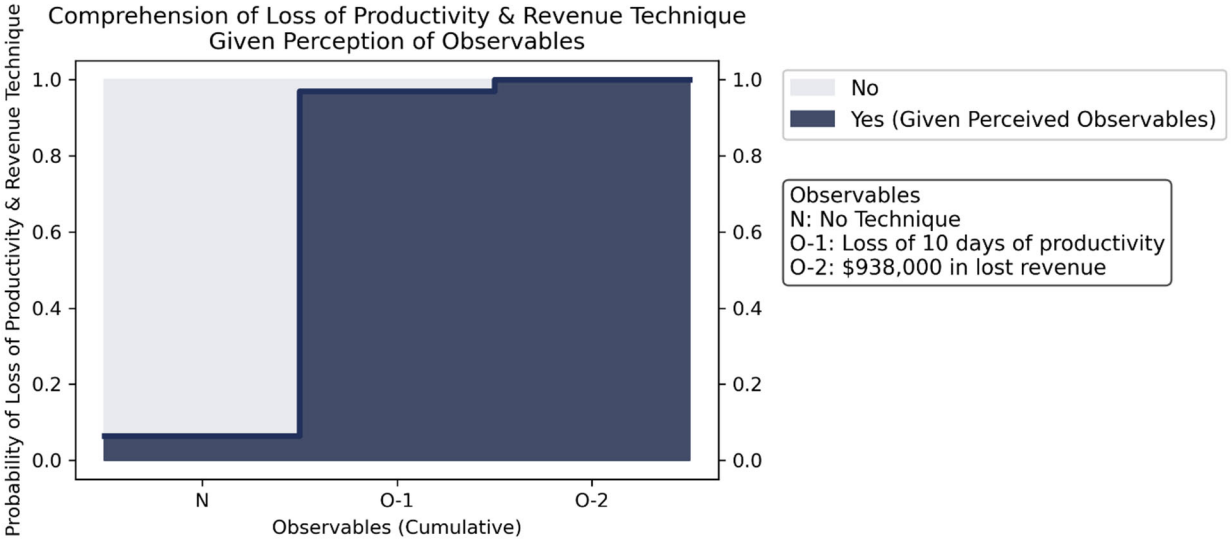


Figure 22: Loss of Productivity and Revenue Technique (T0828) Risk Assessment

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 5 artifacts could be generated by the Loss of Productivity and Revenue technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff

4. LIKELIHOOD OF ADVERSARY BEHAVIOR BY ATTACK STAGE

An adversary's campaign can be characterized by four phases of behavior: early, middle, late, and impact. In the early phase, the adversary obtains limited privileges and access to the network, and has partial visibility of the network with a basic user presence. The Initial Access, Evasion, Discovery, and Collection MITRE ATT&CK® for ICS tactics are commonly associated with early adversary behavior. In the middle phase, the adversary attempts to escalate privilege and access to the network and expand visibility of the network with capabilities common to power users. The Persistence, Privilege Escalation, Lateral Movement and Command and Control MITRE ATT&CK® for ICS tactics are commonly associated with adversary behavior during the middle phase of the campaign. In the late phase, the adversary often obtains elevated privileges on the network and is able to cause an impact to the asset. The Execution, Inhibit Response Function, and Impair Process Control MITRE ATT&CK® for ICS tactics are commonly associated with late adversary behavior. Finally, in the impact phase the adversary is actively impacting the asset.

Click the switches on the CyOTE Attack Chain Model Estimator in Figure 23 to see a representative visualization of the likelihood of ongoing adversary behavior in each phase based on the perceived observables and collectible artifacts. The heads-up display highlights the accumulation of techniques across the MITRE ATT&CK® for ICS framework. The first row of gauges shows the likelihood of adversary behavior given only the perceived observables reported for this case study in Appendix A. The second row shows the likelihood of adversary behavior given the perceived observables and the collectible artifacts identified by the CyOTE artifact repository in Appendix B. The effect of transitioning from perception to collection can be seen by comparing the two rows of gauges.

Group 1 consists of the techniques from Internet Accessible Device through Remote Services. This group contains techniques from two tactics associated with the early and middle phases of adversary behavior. Given the observables identified for these techniques, early adversary behavior is very likely. At this stage, middle adversary behavior is likely, while late and impact behaviors are unlikely. Artifacts were not included for these techniques because the observables in this group were highly diagnostic.

Group 2 consists of all previous techniques and the techniques from Scripting through Program Upload. The additional techniques in this group belong to four tactics, all of which are associated with both the early and middle phases of adversary behavior. Given the observables identified for these techniques, early behavior remains very likely, and middle behavior remains likely, however each phase does have a greater probability relative to Group 1. For this group, late behavior is likely, and the chances of impact behavior are roughly even. Artifacts were included for two techniques with less diagnostic observables. The inclusion of artifacts resulted in an increase in the probability of adversary behavior of about 1% for the middle, late, and impact phases. The difference between the two rows of gauges is small because most observables were diagnostic.

Group 3 consists of all previous techniques and the techniques from Program Download through Exploitation for Evasion. The additional techniques in this group belong to four tactics associated with the early and middle phases of adversary behavior. Given the observables identified for these techniques, early and middle adversary behavior is almost certain, late behavior is very likely, and impact behavior is likely. The difference between the two rows of gauges is minimal because of the introduction of additional diagnostic observables.

Finally, Group 4 consists of all previous techniques and the techniques from Standard Application Layer Protocol though Loss of Productivity and Revenue. This group includes the triggering event

– Service Stop. The additional techniques in this group belong to tactics typical of the late and impact behavior phases. Given the observables identified for these techniques, all phases of adversary behavior are almost certain.

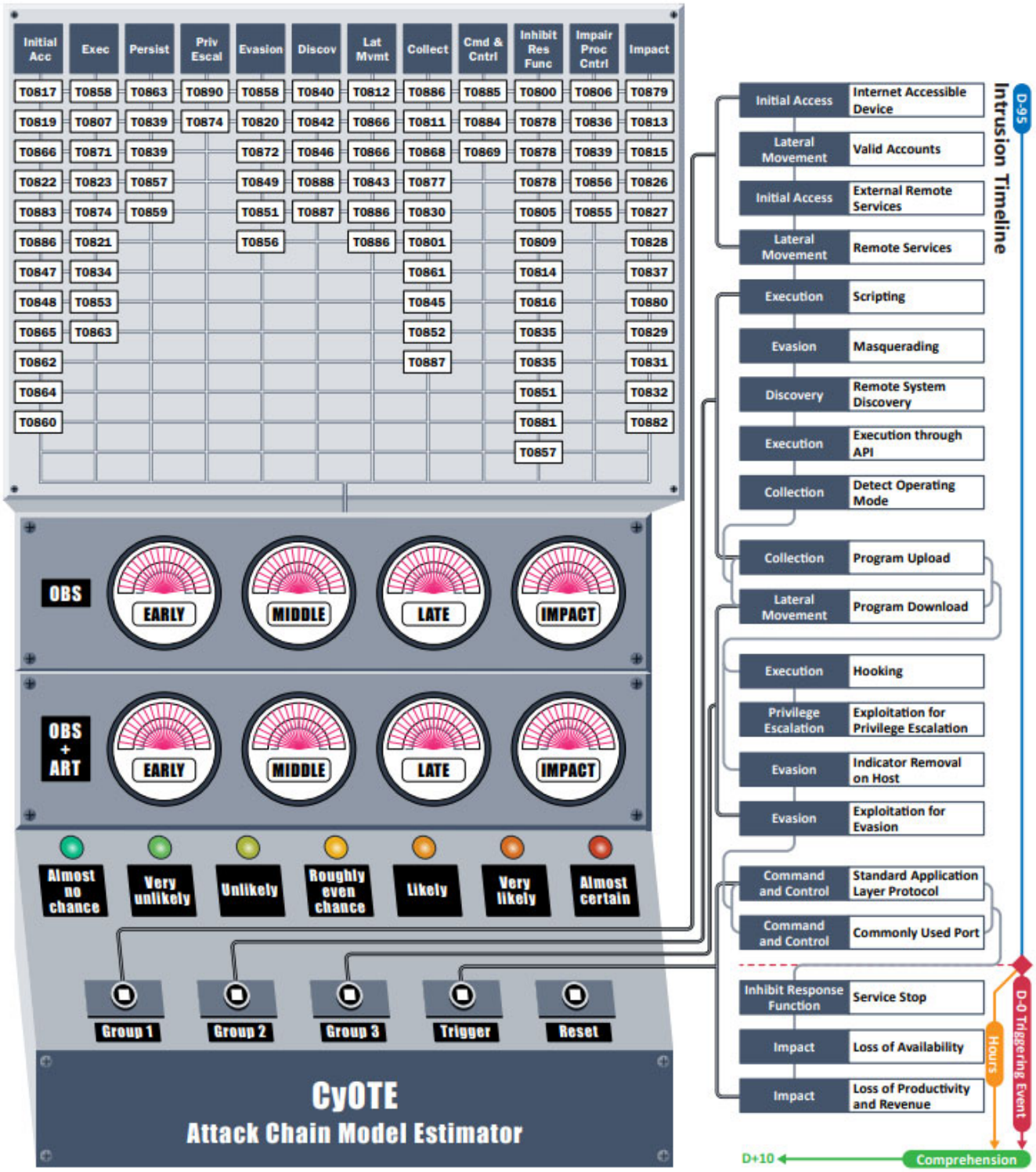


Figure 23. Interactive CyOTE Attack Chain Model Estimator

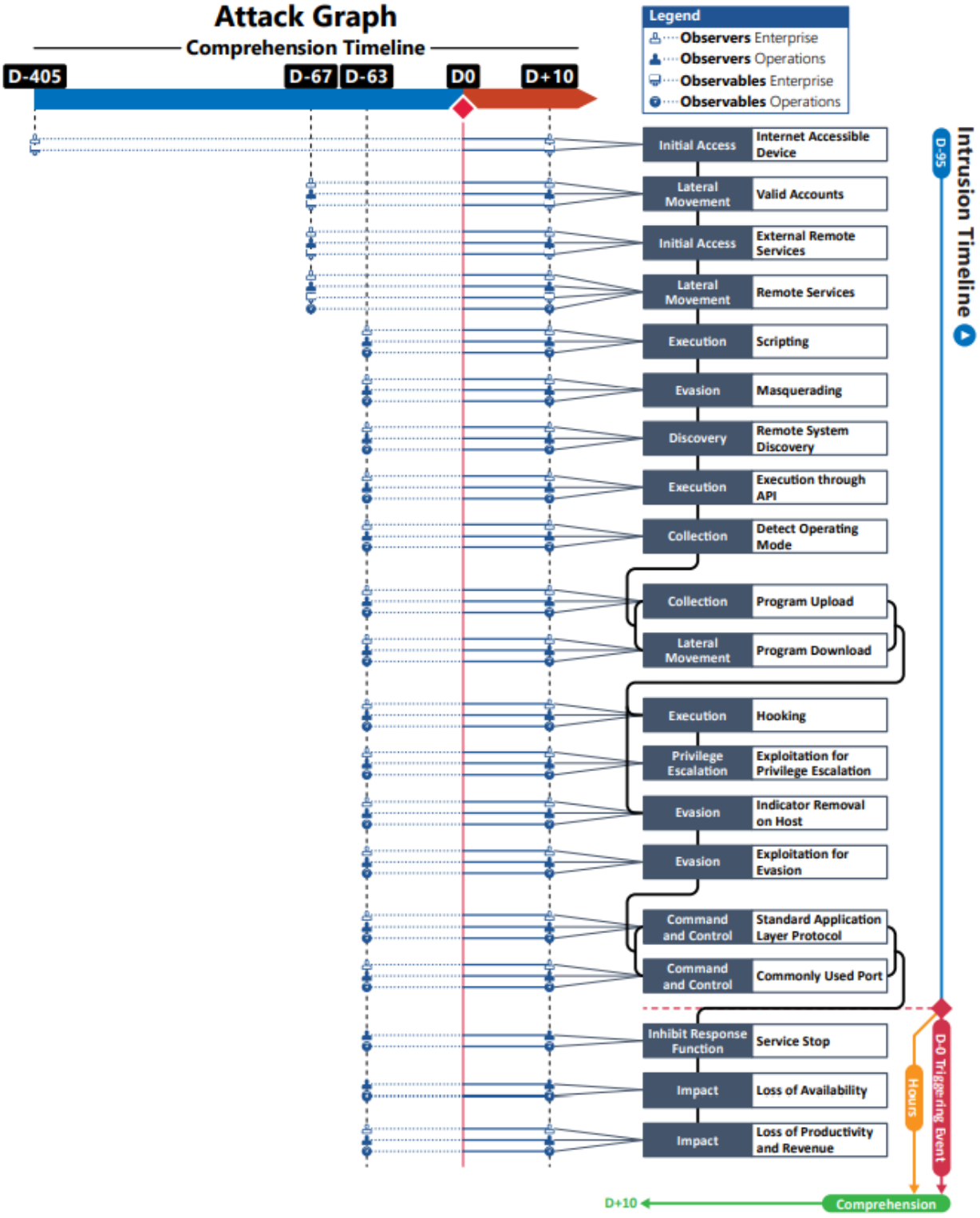


Figure 24. Triton Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

The observables listed here were associated or believed to be associated with the use of Triton malware on Petro Rabigh.

Observables Associated with Internet Accessible Device Technique (T0883)	
Observable 1	Mimikatz Traffic
Observable 2	SecHack Executables
Observable 3	Cryptcat-Based Executables and Files
Observable 4	PLINK-Based Backdoor Executable
Observable 5	Webshell Components

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Mimikatz Traffic
Observable 2	SecHack Executables

Observables Associated with External Remote Services Technique (T0822)	
Observable 1	Unauthorized VPN Access
Observable 2	VPN Logon Anomalies

Observables Associated with Remote Services Technique (T0886)	
Observable 1	Windows Task Scheduler
Observable 2	RDP Traffic
Observable 3	PsExec Traffic
Observable 4	Windows Remote Management (WinRM) Traffic
Observable 5	SSH Traffic
Observable 6	Remote Procedure Protocol (RPC)
Observable 7	Windows Management Instrumentation (WMI) Traffic

Observables Associated with Scripting Technique (T0853)	
Observable 1	Py2EXE Complied Binaries
Observable 2	Trilog.exe File
Observable 3	Library.zip File

Observables Associated with Masquerading Technique (T0849)	
Observable 1	File Creation with Common Name Trilog.exe
Observable 2	File Drop
Observable 3	File Directories Creation
Observable 4	ShimCache Entry Creation
Observable 5	WMI Recently Used Apps Entry

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1	UDP Broadcast Packet on Port 1502

Observables Associated with Execution through API Technique (T0871)	
Observable 1	Increase of API Pings and Connection Requests
Observable 2	Network Traffic between SIS Workstation and Controller

Observables Associated with Detect Operating Mode Technique (T0868)	
Observable 1	Traffic from Script to TCM
Observable 2	Controller Read by Trilog.exe

Observables Associated with Program Upload Technique (T0845)	
Observable 1	Application Event Log of SafeAppendProgramMod

Observables Associated with Program Download Technique (T0843)	
Observable 1	Controller in Program State
Observable 2	Unknown Programs in Controllers' Memory (PresetStatus)
Observable 3	Safety Alarms Notifying Program State

Observables Associated with Exploitation for Privilege Escalation Technique (T0890)	
Observable 1	Execution of Injector File

Observables Associated with Hooking Technique (T0874)	
Observable 1	Shellcode on SIS Controllers

Observables Associated with Exploitation for Evasion Technique (T0820)	
Observable 1	Disables a Firmware RAM/ROM
Observable 2	Injects Payload

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 1	TriStation Protocol Command Script Execution
Observable 2	Modification of SafeAppendProgramMod Attributes
Observable 3	Memory Writes with Malicious Payload Files

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1	Packets Sent to Controllers

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 1	TriStation Communication over UDP Port 1502

Observables Associated with Service Stop Technique (T0881)	
Observable 1	Emergency Shut down

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1	Emergency Shut down

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1	Loss of 10 Days of Productivity
Observable 2	Approximately $938,000 Lost in Revenue

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Internet Accessible Device Technique (T0883)	
Artifact 1	Remote Logins in OS logs (Windows Event 4624)
Artifact 2	Internet Address in Memory Socket Data
Artifact 3	Application Authentication Events
Artifact 4	Dialog Boxes Opened on HMI or EWS
Artifact 5	VNC Traffic Port 5800 or 5900
Artifact 6	HTTP 80
Artifact 7	HTTPS Traffic 443
Artifact 8	SQL Traffic 1433
Artifact 9	Operational Database Connection to External Addresses
Artifact 10	SAP Traffic 3200, 3300
Artifact 11	VPN Logon Events
Artifact 12	Suspicious Connections in Firewall Logs
Artifact 13	VPN Logoff events
Artifact 14	Timestamps
Artifact 15	Host Registry Entries HKEY_CURRENT_USER
Artifact 16	Host Registry Entries HKEY_LOCAL_MACHINE\System
Artifact 17	Suspicious Connections in Proxy Logs
Artifact 18	Host Information in External Data Store or Website (shodan)
Artifact 19	Industrial Traffic from Internet Address
Artifact 20	Standard Traffic from Internet Address
Artifact 21	Internet Address in Application Logs
Artifact 22	Internet Address in OS Logs
Artifact 23	Internet address in command line record data (netstat)

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 1	Logons
Artifact 2	Default Credential Use
Artifact 3	Application Log
Artifact 4	Domain Permission Requests
Artifact 5	Permission Elevation Requests
Artifact 6	Application Use Times

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 7	Configuration Changes
Artifact 8	Prefetch Files Created After Execution
Artifact 9	Logon Session Creation
Artifact 10	User Account Creation
Artifact 11	Authentication Creation
Artifact 12	System Logs
Artifact 13	Successful Logon Event ID 4624
Artifact 14	Failed Logons Event ID 4625
Artifact 15	Logon Timestamp
Artifact 16	Logon Type Entry

Artifacts Associated with External Remote Services Technique (T0822)	
Artifact 1	Failed Logons Event ID 4625
Artifact 2	Session Timestamp
Artifact 3	Logon Event Type 3
Artifact 4	Logon Event Type 10
Artifact 5	Logon Event Type 11
Artifact 6	Remote Session Key
Artifact 7	System Registry Network Interfaces
Artifact 8	Remote Services Logon
Artifact 9	Remote Services Logon
Artifact 10	Session Logoff Event ID 4634/4647
Artifact 11	Domain Controller Log
Artifact 12	User Account Name
Artifact 13	User Client Address
Artifact 14	Security Account Manager Registry Entries
Artifact 15	Dialog Box pop-up
Artifact 16	Mouse Movement
Artifact 17	Command Prompt Window Opened
Artifact 18	Security Account Manager Registry Password Hashes
Artifact 19	External IP Address
Artifact 20	External IP Address
Artifact 21	User Privileges Change

Artifacts Associated with External Remote Services Technique (T0822)	
Artifact 22	Blocked Incoming Connections Event ID 5031
Artifact 23	Blocked Incoming Packet Event ID 5152
Artifact 24	Encrypted Network Traffic
Artifact 25	Mouse Movement
Artifact 26	Cursor Movement
Artifact 27	Keyboard entries
Artifact 28	Application Execution via Input Devices
Artifact 29	Prefetch Files Created
Artifact 30	External MAC Address
Artifact 31	External MAC Address
Artifact 32	RDP Connections
Artifact 33	Program Executions
Artifact 34	Code Injections
Artifact 35	Host-Screen Adjustments
Artifact 36	Screen Resolution Changes
Artifact 37	SSH Connections
Artifact 38	Process Creation
Artifact 39	Service Creation
Artifact 40	Service Modification
Artifact 41	Event Log Creation
Artifact 42	Event Log Creation
Artifact 43	Jumplist Creation
Artifact 44	Shellbag Creation
Artifact 45	System Resource Use Management Changes
Artifact 46	Network Connection Durations
Artifact 47	Changes in Bytes Sent and Received
Artifact 48	Increase CPU Cycles
Artifact 49	Host System Crash
Artifact 50	Application Usage Increase
Artifact 51	Network Bandwidth Changes
Artifact 52	Logon Event ID 4624
Artifact 53	Logon Event ID 4624
Artifact 54	SMB Port 445

Artifacts Associated with External Remote Services Technique (T0822)	
Artifact 55	RDP Port 3389
Artifact 56	SSH Port 22

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 1	Remote Client Connection
Artifact 2	Logon Event
Artifact 3	Logoff
Artifact 4	Logoff Event
Artifact 5	Registry Changes
Artifact 6	Registry Connection Change
Artifact 7	Mouse Movement
Artifact 8	Unexpected I/O
Artifact 9	Desktop Prompt Windows Created
Artifact 10	Session Cache
Artifact 11	Application Log
Artifact 12	RDP Traffic 3389
Artifact 13	System Log Event
Artifact 14	Authentication Logs
Artifact 15	GUI Modifications
Artifact 16	Data File Size in Network Content
Artifact 17	File Movement
Artifact 18	MSSQL Traffic Port 1433
Artifact 19	SSH Traffic Port 22
Artifact 20	SMB Traffic Ports 139, 445
Artifact 21	VNC Traffic Ports 5800, 5900
Artifact 22	Process Creation
Artifact 23	Remote Session Creation Timestamp
Artifact 24	Network Traffic Content Creation

Artifacts Associated with Scripting Technique (T0853)	
Artifact 1	Files Dropped into Directory
Artifact 2	System Event Log Creation

Artifacts Associated with Scripting Technique (T0853)	
Artifact 3	OS Timeline Event
Artifact 4	Startup Menu Modification
Artifact 5	System Processes Created
Artifact 6	Windows API Event Log
Artifact 7	Executable Files
Artifact 8	Prefetch Files Created
Artifact 9	External Network Connections
Artifact 10	Network Services Created
Artifact 11	Registry Modifications
Artifact 12	OS Service Installation

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

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 1	Common Network Traffic
Artifact 2	IEC 103 Traffic (for North America)
Artifact 3	IEC 61850 MMS and GOOSE

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 4	Controller Proprietary Traffic
Artifact 5	Echo Type 8 Traffic
Artifact 6	ICMP Type 7 Traffic
Artifact 7	SNMP Port 162 Traffic
Artifact 8	SNMP Port 161 Traffic
Artifact 9	Command Line Dialog Box Open
Artifact 10	Operating System Queries
Artifact 11	DNS Port 53 Zone Transfers
Artifact 12	Industrial Network Traffic Content about Hostnames
Artifact 13	Polling Network Traffic from Unauthorized IP Sender Addresses
Artifact 14	NetBIOS Name Services Port 137
Artifact 15	LDAP Port 389
Artifact 16	Active Directory Calls
Artifact 17	Email Server Calls
Artifact 18	SMTP Port 25 Traffic
Artifact 19	DNS Lookup Queries
Artifact 20	ARP Scans
Artifact 21	TCP Connect Scan
Artifact 22	TCP SYN Scans
Artifact 23	Scans Over Industrial Network Ports with Target IPs
Artifact 24	TCP FIN Scans
Artifact 25	TCP Reverse Ident Scan
Artifact 26	TCP XMAS Scan
Artifact 27	TCP ACK Scan
Artifact 28	VNC Port 5900 Calls
Artifact 29	Protocol Content Enumeration
Artifact 30	Protocol Header Enumeration
Artifact 31	Recurring Protocol SYN Traffic
Artifact 32	Sequential Protocol SYN Traffic
Artifact 33	Statistical Anomalies In Network Traffic
Artifact 34	Industrial Network Traffic Content Containing Logical Identifiers
Artifact 35	Device Failure
Artifact 36	Device Reboot

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 37	Bandwidth Degradation
Artifact 38	Host Recent Connection Logs
Artifact 39	Industrial Network Traffic
Artifact 40	OPC Network Traffic
Artifact 41	IEC 104
Artifact 42	IEC 102
Artifact 43	IEC 101 Traffic to Serial Devices

Artifacts Associated with Execution through API Technique (T0871)	
Artifact 1	Process Failure
Artifact 2	Reboot
Artifact 3	Module Load
Artifact 4	Control Logic Change
Artifact 5	Timestamps Associated with Activity
Artifact 6	IP Addresses from Network Traffic
Artifact 7	API Log Event (if Enabled)
Artifact 8	SCADA Protocol Network Traffic
Artifact 9	Data Sent with Large File Size
Artifact 10	Data Received with Large File Size
Artifact 11	Network Traffic with Command Execution Content
Artifact 12	State Change in the Process
Artifact 13	Function Execution
Artifact 14	Common Network Traffic
Artifact 15	Industrial Network Traffic
Artifact 16	Vendor Specific Network Traffic
Artifact 17	Remote Connections
Artifact 18	Controller Failure
Artifact 19	Controller Configuration Change

Artifacts Associated with Detect Operating Mode Technique (T0868)	
Artifact 1	Industrial Network Traffic
Artifact 2	Remote Network traffic

Artifacts Associated with Detect Operating Mode Technique (T0868)	
Artifact 3	Vendor Specific Protocol Traffic
Artifact 4	Controller Reads
Artifact 5	Controller Writes
Artifact 6	Engineering Workstation Project File Reads
Artifact 7	HMI End Point Connections with Operating Mode Content
Artifact 8	External Operating Mode Read Requests Over Network Trust Boundaries

Artifacts Associated with Program Upload Technique (T0845)	
Artifact 1	Common Network Traffic Protocols
Artifact 2	Application Dialog Box Open
Artifact 3	Logon Event
Artifact 4	Logoff Event
Artifact 5	Application Authentication Event
Artifact 6	Application Metadata Reported
Artifact 7	Industrial Network Traffic
Artifact 8	Product Specific Protocols
Artifact 9	Data Sent to Unknown IP Addresses
Artifact 10	Controller Sending Data to New IP Address
Artifact 11	Application Log
Artifact 12	Application Log Event Content
Artifact 13	Large Data File Transfers
Artifact 14	Vendor Software Used at Strange Time

Artifacts Associated with Program Download Technique (T0843)	
Artifact 1	Controller in Stop State
Artifact 2	Operational Process Restart
Artifact 3	Operational Database Data Modification
Artifact 4	Device Alert
Artifact 5	Device Alarm
Artifact 6	Controller Application Log Event
Artifact 7	Supervisory Workstation Program Download Popup
Artifact 8	Controller Application Log Type

Artifacts Associated with Program Download Technique (T0843)	
Artifact 9	Controller Application Log Timestamp
Artifact 10	Controller Network Connections via Management Protocol
Artifact 11	Controller Connection to External Website
Artifact 12	Controller in Program State
Artifact 13	Controller Connected to External Networks
Artifact 14	Network Traffic Creation
Artifact 15	Network Metadata
Artifact 16	External Domain Connection
Artifact 17	External IP Address
Artifact 18	Controller State Change
Artifact 19	Operational Process Shut down

Artifacts Associated with Exploitation for Privilege Escalation Technique (T0890)	
Artifact 1	Network Traffic Associated with Privilege Escalation Vulnerabilities (CVE-2014-4076: Sent a Specially Crafted TCP Packet To \\.\\ TCP Device Through DeviceIoControl Function)
Artifact 2	Unusual Process Activity (Thread Suspension of Everything Except Thread Running in a Process Other Than Exploit Thread for CVE-2016-7255)
Artifact 3	Sysmon Event 8: CreateRemoteThread Process Injection Detected
Artifact 4	Unusual Command Line History Associated with Known CVE Techniques (CVE-2019-5736: Privilege Escalation Is Visible Via Unusual Command Line Commands)
Artifact 5	Suspicious File Write to System Directory Followed by Privileged Execution of File
Artifact 6	Execution of a Suspicious File in the System32 or Windows Directory at Privileged Level
Artifact 7	Unusual or Unexpected Kerberos Ticket Requests (CVE-2014-6423)
Artifact 8	Suspicious Files Written to Disk
Artifact 9	Suspicious Program Running Under SYSTEM or Other Elevated Account
Artifact 10	Driver loaded (Sysmon Event ID 6)
Artifact 11	Network Traffic Matching Vulnerability (snort, suricata)
Artifact 12	Abnormal Reads/Writes Between Processes
Artifact 13	Unusual Command Line Arguments to Application (lolbins)
Artifact 14	Artifacts Associated with Known Privilege Escalation CVEs (Privilege Escalation Hard-Coded Debug File Path for APT28 Malware Included Reference to CVE-2014-4076 Privilege Escalation CVE)

Artifacts Associated with Exploitation for Privilege Escalation Technique (T0890)	
Artifact 15	Unusual or Unexpected Child Process Running at Elevated Privileges

Artifacts Associated with Hooking Technique (T0874)	
Artifact 1	.dll Execution
Artifact 2	Files Closed
Artifact 3	Process Performance Mismatched with User Interface at HMI or EWS
Artifact 4	File Modification
Artifact 5	Module Load
Artifact 6	Privilege Escalation Header
Artifact 7	Memory Writes
Artifact 8	Executable And Linkable Format (ELF) Binaries
Artifact 9	Mismatch Parent to Child Processes
Artifact 10	Mismatch Between Memory Resources (Dll, Files, Sockets) and Disk Resources
Artifact 11	Files Open

Artifacts Associated with Exploitation for Evasion Technique (T0820)	
Artifact 1	File Creation
Artifact 2	Internal Sender IP Address
Artifact 3	Destination Address
Artifact 4	MAC Address
Artifact 5	Firmware Version Modification
Artifact 6	OS Version Modification
Artifact 7	Kernel Error
Artifact 8	RDP Traffic Port 3389
Artifact 9	VNC Traffic Port 5900
Artifact 10	SSH Traffic Port 22
Artifact 11	Telnet Traffic
Artifact 12	Process Creation
Artifact 13	TFTP Port 69
Artifact 14	FTP Port 21
Artifact 15	FTPS Port 990
Artifact 16	HTTPS Port 443

Artifacts Associated with Exploitation for Evasion Technique (T0820)	
Artifact 17	External Industrial Protocol Connections
Artifact 18	Web Proxy Logs
Artifact 19	SMB Traffic
Artifact 20	Industrial Protocol Traffic
Artifact 21	HTTP Traffic
Artifact 22	Memory writes
Artifact 23	Disk Writes
Artifact 24	Application Log
Artifact 25	Firewall Log
Artifact 26	External Sender IP Address
Artifact 27	Software Vulnerability CVE
Artifact 28	Zero-Day Announcement
Artifact 29	Protocol Vulnerability
Artifact 30	Pip Use

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

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

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 80
Artifact 7	DNS Traffic Port 53
Artifact 8	SMB Traffic Port 445
Artifact 9	HTTPS Traffic Port 443
Artifact 10	RDP Traffic Port 3389
Artifact 11	HTTP Post Request
Artifact 12	External IP Addresses

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

Artifacts Associated with Service Stop Technique (T0881)	
Artifact 1	Process Failure
Artifact 2	Alarm Event
Artifact 3	Internal System Logs

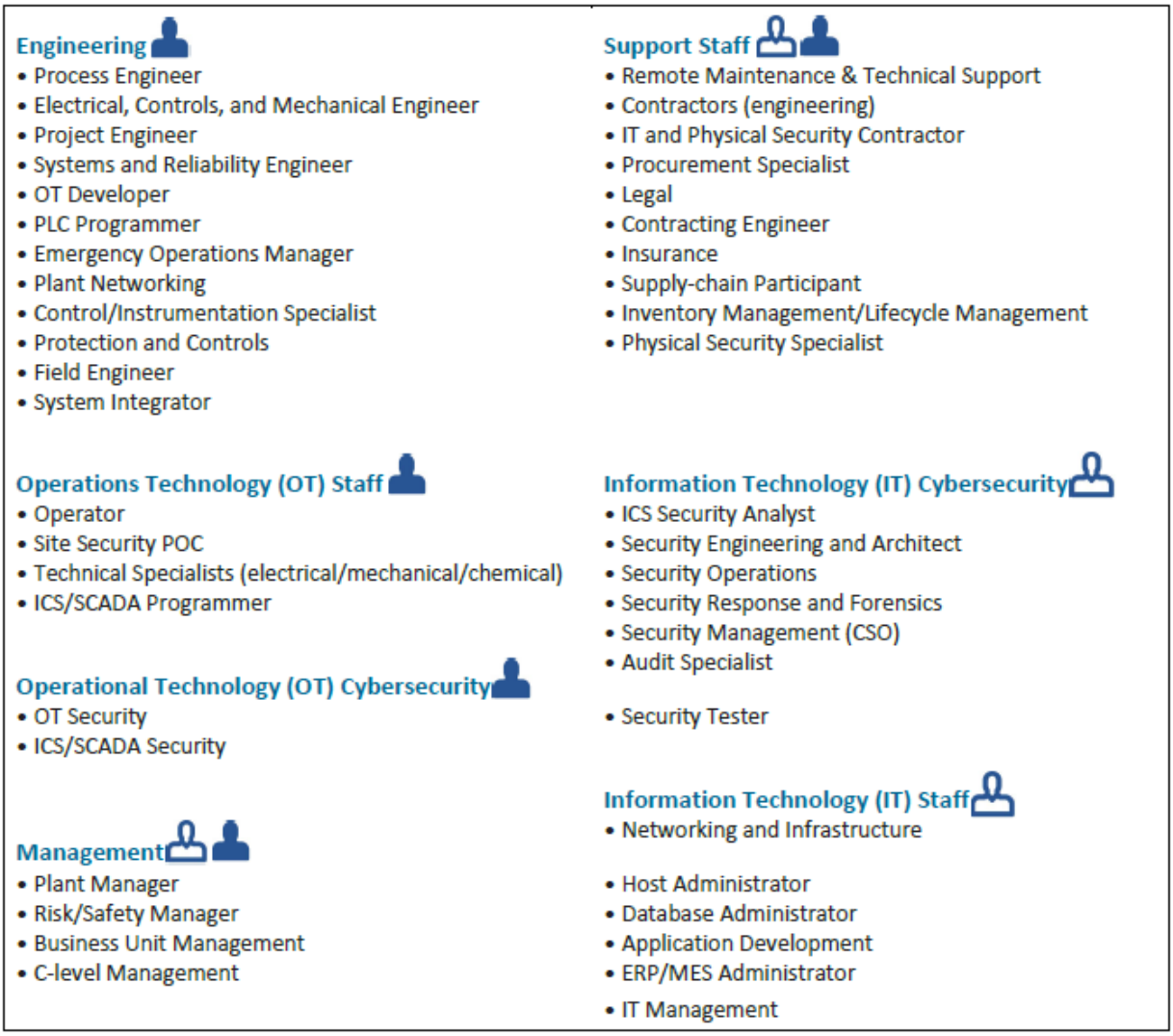
Artifacts Associated with Service Stop Technique (T0881)	
Artifact 4	Application Error Messages
Artifact 5	Process Error Messages
Artifact 6	Application Service Stop
Artifact 7	OS Service Crash
Artifact 8	System Event Logs
Artifact 9	Application Event Logs
Artifact 10	OS API Call
Artifact 11	Command Line System Argument
Artifact 12	System Resource Usage Manager Application Usage Change
Artifact 13	Registry Change HKLM\System\CurrentControlSet\Services

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

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 Shut Down of a Plant to Prevent Ransomware or Other Destructive Attacks
Artifact 3	Extortion Attempts Might Lead to Reduced Operations Due to Potential Presence of Adversaries
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 OT organizations. It has been slightly modified by the CyOTE team from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster to communicate the categories of potential observers during cyber events.



APPENDIX D: TECHNIQUE COMPREHENSION

Click on observables and artifacts in Figure 25 to see the change in probability of the Valid Accounts technique (T0859) being used given evidence (observables or artifacts) related to adversary behavior. Observable O-1 provides a significant increase in the likelihood of the Valid Accounts technique to a roughly even chance of 48%. Observables O-2 and O-3 provide a small increase in the technique likelihood by raising it to 51%. Therefore, additional evidence must be obtained to comprehend whether the adversary is implementing the Valid Accounts technique. If an observer perceives an anomaly and evaluates it as a triggering event, the AOO can obtain additional evidence of adversary behavior by collecting artifacts. Figure 25 shows an observer perceiving observables O-1, O-2, and O-3 (triggering event) and collecting artifacts A-1 and A-2, resulting in almost certain use of the Valid Accounts technique. Collecting artifact A-1 raises the likelihood of the Valid Accounts technique from 51% to 95%, and the additional collection of A-2 raises the likelihood to 99%.

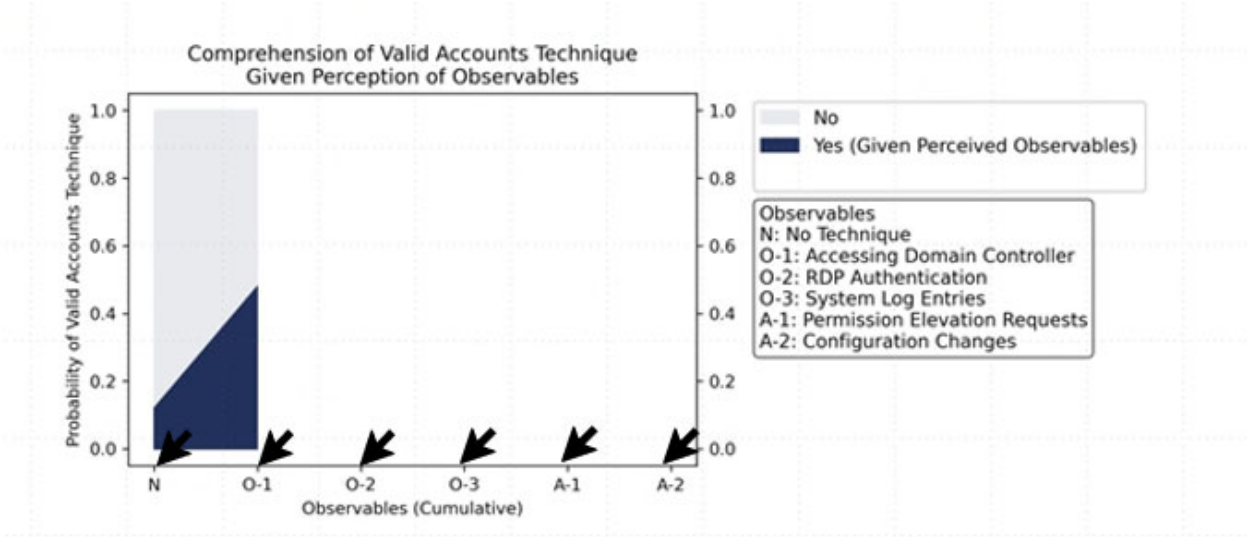


Figure 25: Interactive Sample Risk Assessment

REFERENCES

[1] [Rabigh Refining and Petrochemical Company | “Unaudited Condensed Interim Financial Information For The Three-Month And Year Ended December 31, 2017 And Report On Review Of Interim Financial Information” | https://www.petrorabigh.com/Financial%20Statements%20Documents/Rabigh%20Refining%20%20Petrochemical%20Co%20FS-Q4%202017%20English.pdf | 4 February 2018 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[2] [DARKReading | Kelly Jackson Higgins | “Triton/Trisis Attack Was More Widespread than Publicly Known” | https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known | 16 January 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[3] [E&E News | Black Sobczak | “The inside story of the world’s most dangerous malware” | https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/ | 3 July 2019 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[4] [Mandiant | Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer | “Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure” | https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton | 14 December 2017 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[5] [E&E News | Black Sobczak | “The inside story of the world’s most dangerous malware” | https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/ | 3 July 2019 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[6] [Dragos | Robert M. Lee | “TRISIS: Analyzing Safety System Targeting Malware” | https://www.dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/ | 14 December 2017 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[7] [Department of Justice | “Holding a Criminal Term” | https://www.justice.gov/opa/press-release/file/1486831/download | 29 June 2021 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[8] [Department of Justice | “Holding a Criminal Term” | https://www.justice.gov/opa/press-release/file/1486831/download | 29 June 2021 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[9] [Mandiant | Steve Miller, and others| “TRITON Actor TTP Profile, Custom Attack Tools, Detections and ATT&CK Mapping” | https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections | 10 April 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[10] [DARKReading | Kelly Jackson Higgins | “Triton/Trisis Attack Was More Widespread than Publicly Known” | https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known | 16 January 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[11] [DARKReading | Kelly Jackson Higgins | “Triton/Trisis Attack Was More Widespread than Publicly Known” | https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known | 16 January 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[12] [DARKReading | Kelly Jackson Higgins | “Triton/Trisis Attack Was More Widespread than Publicly Known” | https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known | 16 January 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[13] [E&E News | Black Sobczak | “The inside story of the world’s most dangerous malware” | https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/ | 3 July 2019 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[14] [Mandiant | Steve Miller, and others| “TRITON Actor TTP Profile, Custom Attack Tools, Detections and ATT&CK Mapping” | https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections | 10 April 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[15] [Department of Justice | “Holding a Criminal Term” | https://www.justice.gov/opa/press-release/file/1486831/download | 29 June 2021 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[16] [DARKReading | Kelly Jackson Higgins | “Triton/Trisis Attack Was More Widespread than Publicly Known” | https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known | 16 January 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[17] [Mandiant | Steve Miller, and others| “TRITON Actor TTP Profile, Custom Attack Tools, Detections and ATT&CK Mapping” | https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections | 10 April 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[18] [DARKReading | Kelly Jackson Higgins | “Triton/Trisis Attack Was More Widespread than Publicly Known” | https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known | 16 January 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[19] [Fortinet | “Securing OT Systems in the Face of Rapid Threat Evolution” | https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-securing-ot-systems-in-the-face-of-rapid-threat-evolution.pdf | 24 February 2021 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[20] [Department of Justice | “Holding a Criminal Term” | https://www.justice.gov/opa/press-release/file/1486831/download | 29 June 2021 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[21] [Mandiant | Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer | “Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure” | https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton | 14 December 2017 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[22] [Mandiant | Steve Miller, and others | “TRITON Actor TTP Profile, Custom Attack Tools, Detections and ATT&CK Mapping” | https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections | 10 April 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[23] [Department of Justice | “Holding a Criminal Term” | https://www.justice.gov/opa/press-release/file/1486831/download | 29 June 2021 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[24] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-

Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[25] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[26] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[27] [Department of Justice | “Holding a Criminal Term” | https://www.justice.gov/opa/press-release/file/1486831/download | 29 June 2021 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[28] [Mandiant | Steve Miller, and others | “TRITON Actor TTP Profile, Custom Attack Tools, Detections and ATT&CK Mapping” | https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections | 10 April 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[29] [Midnight Blue Labs | Jos Wetzels, Calo Meijer, Wouter Bokslag | “Analyzing the TRITON Industrial Malware” | https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware | 16 January 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[30] [MITRE ATT&CK | “Execution through API” | https://collaborate.mitre.org/attackics/index.php/Technique/T0871 | 20 October 2021 | Accessed 4 May 2022 | The source is publicly available information and does not contain classification markings]

[31] [Midnight Blue Labs | Jos Wetzels, Calo Meijer, Wouter Bokslag | “Analyzing the TRITON Industrial Malware” | https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware | 16 January 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[32] [Mandiant | Blake Johnson, and others | “Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure” | https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton | 14 December 2017 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[33] [Schneider Electric | “Security Notification – EcoStruxure Triconex Tricon V3” | https://www.se.com/us/en/download/document/SEVD-2017-347-01/ | 14 December 2017 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[34] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[35] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[36] [YouTube | S4 Events | Julian Gutmanis | “Triton – A Report from the Trenches” | https://www.youtube.com/watch?v=XwSJ8hloGvY | 11 March 2019 | Accessed 3 March 2022 | Source is publicly available information and does not contain classification markings]

[37] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-

Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[38] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[39] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[40] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[41] [Mandiant | Steve Miller, and others| “TRITON Actor TTP Profile, Custom Attack Tools, Detections and ATT&CK Mapping” | https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections | 10 April 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[42] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[43] [Cybersecurity & Infrastructure Security Agency | “MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)” | https://www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B | 27 February 2019 | Accessed 3 March 2022 | The source is publicly available information and does not contain classification markings]

[44] [Department of Justice | “Holding a Criminal Term” | https://www.justice.gov/opa/press-release/file/1486831/download | 29 June 2021 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[45][E&E News | Black Sobczak | “The inside story of the world’s most dangerous malware” | https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/ | 3 July 2019 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[46] [E&E News | Black Sobczak | “The inside story of the world’s most dangerous malware” | https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/ | 3 July 2019 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]

[47] [Rabigh Refining and Petrochemical Company | “Unaudited Condensed Interim Financial Information For The Three-Month And Year Ended December 31, 2017 And Report On Review Of Interim Financial Information” | https://www.petrorabigh.com/Financial%20Statements%20Documents/Rabigh%20Refining%20%20Petrochemical%20Co%20FS-Q4%202017%20English.pdf | 4 February 2018 | Accessed 14 March 2022 | The source is publicly available information and does not contain classification markings]