## DISCLAIMER

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


# PRECURSOR ANALYSIS REPORT: DOPPELPAYMER RANSOMWARE ATTACK ON PETROLEOS MEXICANOS (PEMEX) 2019

Cybersecurity for the Operational Technology Environment (CyOTE)

**31 DECEMBER 2022**

CyOTE Cybersecurity for the Operational Technology Environment

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

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

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

# TABLE OF CONTENTS



## FIGURES



## TABLES

# PRECURSOR ANALYSIS REPORT: DOPPELPAYMER RANSOMWARE ATTACK ON PETROLEOS MEXICANOS (PEMEX) 2019

## 1. EXECUTIVE SUMMARY

The DoppelPaymer Ransomware Attack on Petroleos Mexicanos (PEMEX) 2019 Precursor Analysis Report leverages publicly available information about the PEMEX cyber attack and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

The 2019 DoppelPaymer ransomware attack on PEMEX, Mexico's nationalized petroleum corporation, highlights a unique threat that ransomware and cybercriminal extortion poses to Operational Technology (OT) environments in critical infrastructure. The incident began with an employee downloading commodity malware that allowed adversaries to gain initial access to PEMEX's enterprise environment. After conducting privilege escalation, tool ingress, and data exfiltration, the adversaries deployed DoppelPaymer ransomware throughout the PEMEX enterprise environment, resulting in the company having to take dozens of systems offline for at least several days. Although PEMEX stated that their operations were not affected, the data exfiltrated from PEMEX was made available for download on DoppelPaymer's leak site, as well as on other illicit criminal forums. This stolen data included not only company information, but also sensitive OT-specific configuration data. This incident showcases how cybercriminal exfiltration and posting of sensitive OT architecture documentation can pose security concerns for the targeted organization for years due to the long lifespan of OT assets and architectures.

Researchers and analysts identified 18 unique techniques utilized during the attack with a total of 190 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Fifteen of the identified techniques used during the DoppelPaymer ransomware attack were precursors to the triggering event. Analysis identified 163 observables associated with these precursor techniques, 34 of which were assessed to have an increased likelihood of being perceived in the 60 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

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

# 2. INTRODUCTION

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

## 2.1. APPLYING THE CYOTE METHODOLOGY

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

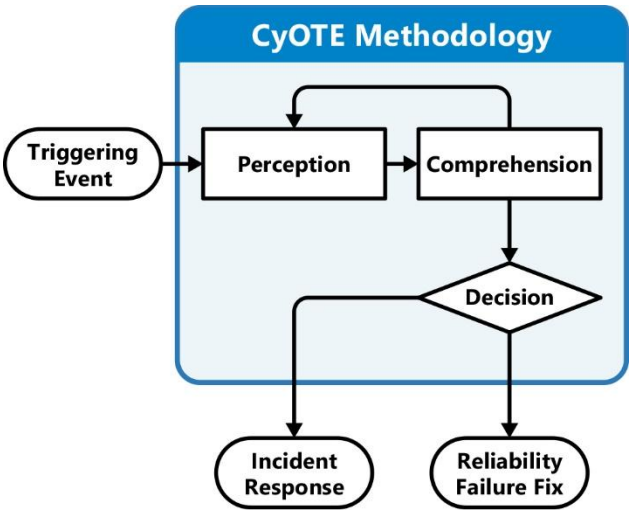



***Figure 1. CyOTE Methodology***

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

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

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

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

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

## 2.2. BACKGROUND ON THE ATTACK

The 2019 DoppelPaymer ransomware attack on Petroleos Mexicanos (PEMEX), Mexico's nationalized petroleum company, began with an employee downloading commodity malware that is often used for initial access, such as Emotet or Dridex, likely sometime in early September 2019 (D-60).[1,a] During the same period adversaries may have also used the FakeUpdates malware framework, a drive-by compromise masquerading as a browser update, to gain initial access.

After achieving initial access and profiling the victim environment, the adversaries proceeded to escalate privileges, exfiltrate data, and move additional tools and payloads into the PEMEX network. Adversaries eventually deployed the DoppelPaymer ransomware on 10 November (D-0).[2] Numerous PEMEX enterprise systems displayed a ransom note demanding payment of 565 Bitcoin (then equivalent to $4,899,295.80 USD).[3] Although PEMEX stated that OT systems were unaffected by the ransomware incident, public reporting indicated that PEMEX employees were not able to access their enterprise systems for days after the attack. Further, the data exfiltrated from PEMEX was available for download on DoppelPaymer's leak site, as well as on other illicit criminal forums. This stolen data included not only company information, but also sensitive OT-specific configuration data.

A timeline of adversarial techniques is shown in **Error! Reference source not found.**. The timeline includes the estimated number of days prior to and after the triggering event. The timeline after the triggering event includes the assessed victim comprehension timeline.

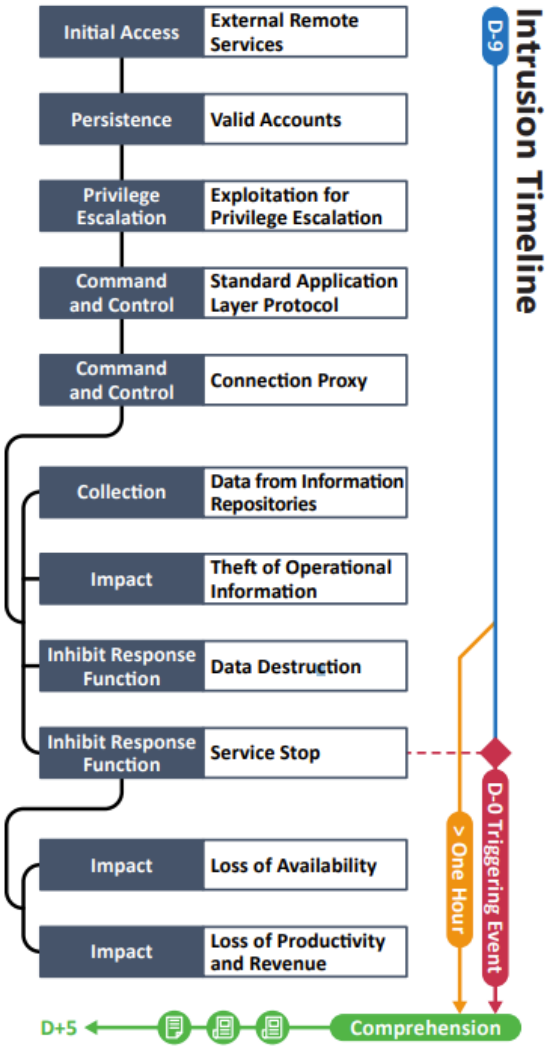



*Figure 2. Intrusion Timeline*

After gaining initial access sometime in early September 2019, the adversaries proceeded to escalate privileges, move laterally, and exfiltrate data from PEMEX from D-60 until around D-1.The exfiltration of sensitive OT environment documentation is a significant concern: according to cybersecurity firm Mandiant, one in every seven critical infrastructure ransomware incidents involves the leak of sensitive OT data.[4] Such data stored in the enterprise environment may be subject to inadvertent exfiltration by a ransomware group(s) as part of their strategy to pressure the victim into paying a ransom. The attack on PEMEX involved several groups of cybercriminal adversaries, including initial access brokers, botnet masters, and ransomware operators.

[a] IBM stated the average time from initial access to ransom demand for DoppelPaymer attacks in 2019 was over two months.

Analysis identified 18 unique techniques in a sequence and timeframe likely used by adversaries during this cyber attack (**Error! Reference source not found.** 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

***Table 1. Techniques Used in the DoppelPaymer Ransomware Attack on PEMEX in 2019***

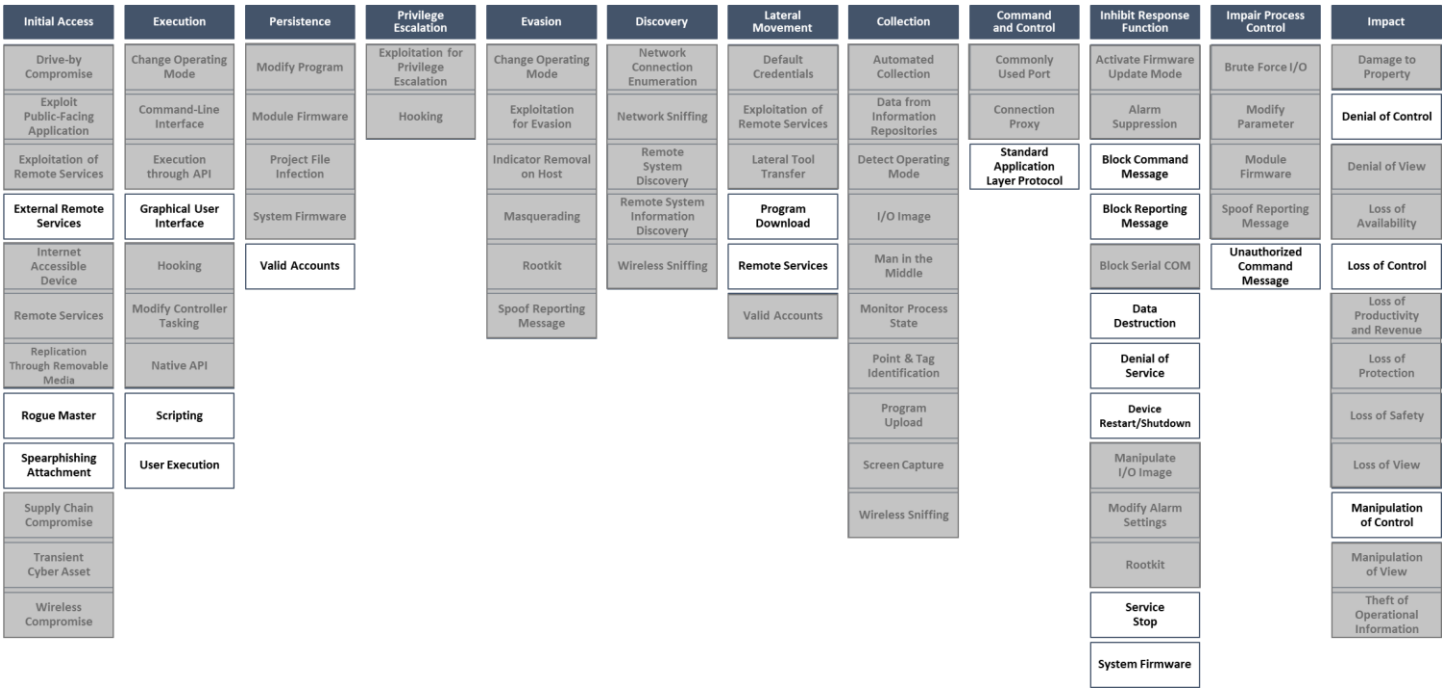



***Table 2. Precursor Analysis Report Quantitative Summary***

| Precursor Analysis Report Quantitative Summary | Totals |
|---|---|
| **MITRE ATT&CK® for ICS Techniques** | **18** |
| **Technique Observables** | **190** |
| **Precursor Techniques** | **15** |
| **Precursor Technique Observables** | **163** |
| **Highly Perceivable Precursor Technique Observable** | **34** |

# 3. OBSERVABLE AND TECHNIQUE ANALYSIS

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

## 3.1. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS

Adversaries likely used malicious spearphishing attachment campaigns to facilitate the download and execution of Emotet, Dridex, or both. Emotet and Dridex are banking trojans that often act as initial access vectors for ransomware groups. Ransomware groups buy access from botnet operators and then conduct further malicious activity in a victim's environment, including ransomware deployment.[5] Adversaries who control banking trojans such as Emotet and Dridex regularly make use of Microsoft Office documents in malicious spam campaigns, with common email themes like finance or payroll to bait the end-user into interacting with the malicious attachment.[6] In some cases, the Dridex malware is embedded in the document itself, not requiring an external resource to install the initial payload.[7]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe initial malicious email attachments before interacting with them. It is unclear in the case of PEMEX who may have initially interacted with the malicious attachment, but any individual with a company email is susceptible to this tactic.

A total of seven observables were identified with the use of the Spearphishing Attachment technique (T0865). This technique is important for investigation because it is a common method for adversaries to gain initial access into victim environments. This technique appears early in the timeline and responding to it will likely halt future events. Terminating the chain of techniques at this point would limit initial access vectors into the victim environment.

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

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

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

## 3.2. DRIVE-BY COMPROMISE TECHNIQUE (T0817) FOR INITIAL ACCESS

Adversaries may have also leveraged the Drive-by Compromise technique (T0817) to gain initial access into the PEMEX enterprise network. Dridex operators may have made use of a malware framework known as FakeUpdates or SocGhoulish during of the compromise. FakeUpdates was observed downloading Dridex in October and November of 2019, several weeks before the attack on PEMEX.[8] FakeUpdates, as the name implies, is malware that masquerades as Google Chrome, FireFox, Opera, or Internet Explorer browser updates that redirect a user to a malicious site and prompts them to download a "browser update." Because FakeUpdates makes use of Search Engine Optimization (SEO) poisoning, it is likely a PEMEX employee used a browser to search for a targeted subject and then interacted with a malicious URL indexed by that search result. Once installed, FakeUpdates can then download other malware payloads such as Dridex. After the compromised site redirects the victim user, the user is prompted to download the malware, often written in Hypertext Markup Language (HTML), JavaScript (.js), or a ZIP file containing a JavaScript file.[9]

IT Staff, IT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe compromised websites prompting them to download a file masquerading as a browser update, as well as the downloading of files onto the host.

A total of seven observables were identified with the use of the Drive-by Compromise technique (T0817). This technique is important for investigation because it results in the download of malicious software into a victim's enterprise environment. This technique appears early in the timeline and responding to it will likely prevent initial access. Terminating the chain of techniques at this point may limit further adversary activity in the victim environment and prevent the theft of operational information.

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

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

## 3.3. USER EXECUTION TECHNIQUE (T0836) FOR EXECUTION

Adversaries leveraged one or more unwitting victim employees to deploy first stage malware such as Emotet, Dridex, or FakeUpdates via the User Execution technique (T0836). Victims are prompted to enable malicious Macros in Microsoft Office documents that load either Dridex or Emotet malware onto the victim's host machine. These documents prompt the victim to enable macros, which then execute embedded code in the document that reaches out to an external resource to download a malware payload. External resources like compromised third-party websites often host an initial payload of Emotet, Dridex, or other malware. Dridex is also capable of being loaded directly into memory from malicious Office documents, negating the need for outbound network communications for an initial download.[10] Victim users may also have downloaded the FakeUpdates malware framework, believing it to be a legitimate browser update.

IT Staff, IT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe the malicious Office Documents or the faux browser update prompts that downloaded FakeUpdates.

A total of 13 observables were identified with the use of the User Execution technique (T0836). This technique is important for investigation because it is one of the most common gateways cyber adversaries utilize to gain initial access. This technique appears early in the timeline and responding to it will likely halt all future adversary activity in the victim's environment. Terminating the chain of techniques at this point would effectively halt all further adversary activity and limit impact to business operations.

Of the 13 observables associated with this technique, none are assessed to be highly perceivable. They are listed in Appendix A.

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

## 3.4. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

The adversaries made use of the Scripting technique (T0853) throughout the course of the PEMEX intrusion. Malicious documents that download Emotet or Dridex often abuse Visual Basic for Applications (VBA) when an end-user enables Macros to either download a malware payload or load malicious code directly into memory. Additionally, the FakeUpdates malware has been observed using both JavaScript and Hypertext Markup Language (HTML) files to install the initial module that masquerades as a browser update inside of a .ZIP file.[11]

IT Staff and IT Cybersecurity personnel may have been able to observe malicious documents and prompts for a fake browser update associated with malware utilizing this technique**.**

A total of 20 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because it allows the adversary to conduct malicious actions in a victim's environment, often facilitating initial access or lateral movement. This technique appears relatively early in the timeline and responding to it will likely halt further adversary activity within the victim's environment. Terminating the chain of techniques at this point would limit malicious activity in the victim's environment, as well as avert future events such as theft of operational information and manipulation of view.

Of the 20 observables associated with this technique, none are assessed to be highly perceivable. They are listed in Appendix A.

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

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

The adversaries used several standard application layer protocols throughout the intrusion for command and control (C2), tool ingress, and data exfiltration. Malware like Emotet, Dridex, and FakeUpdates use HTTP and HTTPS for routine C2 communications, as well as for fetching other payloads from external resources. Additionally, adversaries almost certainly used File Transfer Protocol (FTP) and Secure File Transfer Protocol (SFTP) to move additional tools and malware payloads into PEMEX's environment, as well as to exfiltrate company data later listed on the DoppelPaymer leak site.

IT Staff and IT Cybersecurity personnel may have been able to observe C2 traffic associated with Emotet, Dridex, and FakeUpdates. Furthermore, IT Staff and IT cybersecurity may have been able to observe the data exfiltration traffic, which in the case of the PEMEX attack may have lasted several weeks due to the volume of data involved.

A total of 10 observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation as prolonged anomalous network traffic is a strong indication of adversary activity. This technique appears throughout the timeline and responding to it will alert defenders to malicious activity within their environment. Terminating the chain of techniques at this point would likely halt any further adversary activity if defenders took steps to block the malicious network traffic.

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

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

## 3.6. COMMONLY USED PORT TECHNIQUE (T0855) FOR COMMAND AND CONTROL

The adversaries employed commonly used ports throughout the intrusion for C2, tool ingress, and data exfiltration. Emotet and Dridex commonly use TCP Ports 80, 443, and 8080 for C2, although both also have been observed using non-standard ports. FakeUpdates also regularly makes use of Ports 80 and 443 for download and C2. Adversaries likely used Ports 21 and 22 for data exfiltration while using Rclone or Mega, which are utilities designed for data transfer and cloud storage, respectively.

IT Staff and IT Cybersecurity personnel may have been able to observe the anomalous traffic to and from C2 servers, as well as outbound data exfiltration traffic at odd hours.

A total of 10 observables were identified with the use of the Commonly Used Port technique (T0855). This technique is important for investigation as port usage is an indicator of adversary activity in the victim's environment. This technique appears throughout the timeline and responding to it may halt future activity. Terminating the chain of techniques at this point would limit adversary activity in the victim's environment and prevent communication with malware already present.

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

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

## 3.7. REMOTE SERVICES TECHNIQUE (T0886) FOR LATERAL MOVEMENT

The adversaries likely employed the Remote Services technique (T0886) to facilitate lateral movement within the PEMEX enterprise environment. Financially motivated cyber threat actors often abuse native remote services, such as Server Message Block (SMB) or Remote Desktop Protocol (RDP), with valid accounts to conduct further reconnaissance and lateral movement. This often leads to critical assets such as domain controllers being compromised and then used as a springboard for enterprise-wide deployment of ransomware.

IT Staff and IT Cybersecurity personnel may have been able to observe the anomalous network traffic related to the SMB or RDP protocols at irregular hours.

A total of four observables were identified with the use of the Remote Services technique (T0886). This technique is important for investigation as it is often leveraged to facilitate lateral movement in a victim's environment, allowing for further malicious activity. This technique appears throughout the timeline and responding to it may halt future activity. Terminating the chain of techniques at this point would limit adversary activity in the victim's environment and prevent communication with installed malware that acts as a foothold in a victim's environment.

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

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** | A total of 24 artifacts could be generated by the Remote Services technique |
| **Technique Observers** | IT Staff, IT Cybersecurity |
| **Resources** | Technique Detection References |

## 3.8. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

Financially motivated adversaries often make use of stolen credentials for valid accounts that precursor malware, such as Dridex, can harvest from web browsers and email clients on infected hosts. The adversaries may have used stolen credentials from an initial commodity malware infection for further discovery and lateral movement in the victim's environment.

IT Staff and IT Cybersecurity personnel may have been able to observe logons from valid user credentials at anomalous hours.

A total of six observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because adversaries often use stolen credentials to help facilitate lateral movement in a victim's environment. This technique appears early in the timeline and responding to it will limit an adversary's ability to persist or move laterally in a victim's environment via bypassing access controls. Terminating the chain of techniques at this point would partially limit an adversary's presence in the environment, as these credentials may have been harvested by malware still present in the system.

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

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

## 3.9. LATERAL TOOL TRANSFER TECHNIQUE (T0867) FOR LATERAL MOVEMENT

Adversaries utilized the Lateral Tool Transfer technique (T0867) throughout the intrusion. Upon gaining initial access, adversaries may have used Ebanking malware such as Emotet to download and execute Dridex within the PEMEX enterprise environment, allowing a separate group of adversaries access. From there, the adversaries proceeded to deploy additional tools, such as Mimikatz, Koadic, and PoshC2 to help elevate privileges and move laterally, between 30 minutes and two hours after initial Dridex execution.[12] The adversaries likely also transferred data exfiltration tools, such as Rclone or Mega, into the victim's environment. These tools are used to steal sensitive company data from victims over a period of several weeks to facilitate double extortion, a popular tactic ransomware adversaries use to strong-arm victims into paying ransoms to avoid legal penalties due to violation of data privacy laws.

IT Staff and IT cybersecurity personnel may have been able to observe the presence of anomalous files as well as the anomalous network traffic associated with the download of additional tools and payloads.

A total of 22 observables were identified with the use of the Lateral Tool Transfer technique (T0867). This technique is important for investigation because it indicates adversaries are moving additional tools and payloads into the victim environment to perform further malicious activity. This technique appears throughout the timeline and responding to it will limit further adversary activity. Terminating the chain of techniques at this point would prevent ransomware deployment and data exfiltration from the enterprise environment.

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

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** | A total of 22 artifacts could be generated by the Lateral Tool Transfer technique |
| **Technique Observers** | IT Staff, IT Cybersecurity |
| **Resources** | Technique Detection References |

## 3.10. COMMAND-LINE INTERFACE TECHNIQUE (T0807) FOR EXECUTION

Adversaries utilized the Command-Line Interface technique (T0807) throughout the timeline. This technique most likely would have been associated with the adversaries executing PowerShell commands, Active Directory (AD) reconnaissance commands, or using Command-Line Interface (CLI)-based tools to exfiltrate data. DoppelPaymer is designed to execute only after a specific command-line argument is provided to hamper analysis and reverse engineering of the malware.

IT Staff and IT Cybersecurity personnel may have been able to observe various command-line executions associated with PowerShell, AD reconnaissance, or data exfiltration tools.

A total of 16 observables were identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation because it often is associated with adversaries executing malicious payloads within the victim's environment or conducting reconnaissance. This technique appears throughout the timeline and responding to it may prevent the adversaries from deploying or executing the ransomware. Terminating the chain of techniques at this point would prevent prolonged data exfiltration.

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

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

## 3.11. THEFT OF OPERATIONAL INFORMATION TECHNIQUE (T0882) FOR IMPACT

A common tactic that ransomware operators use is known as “double extortion,” which entails exfiltrating victim data prior to deploying the ransomware payload, and then threatening to post the stolen data to pressure the victim into paying a ransom.[13] The adversaries often use tools such as Mega and Rclone, which employ FTP asnd SFTP, to accomplish large-scale data exfiltration up to several weeks prior to ransomware deployment. The time required to exfiltrate large volumes of data provides a considerable window of opportunity for energy sector and other critical infrastructure organizations to identify this activity.

IT Staff and IT Cybersecurity personnel may have been able to observe prolonged network traffic to an external server associated with data exfiltration.

A total of 17 observables were identified with the use of the Theft of Operational Information technique (T0882). This technique is important for investigation because theft of operational data jeopardizes not only business practices but the security of the OT environment. This technique appears late in the timeline and responding to it will prevent the adversaries from exfiltrating data from the enterprise and OT environments. Terminating the chain of techniques at this point would limit operational damage and the loss of sensitive OT documentation.

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

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

## 3.12. MASQUERADING TECHNIQUE (T0849) FOR EVASION

DoppelPaymer ransomware makes use of stolen signed software certificates to evade signature-based detection engines and ensure stealthy execution. DoppelPaymer uses stolen software certificates and attempts to masquerade as the "SpotLife WebAlbum Service Plugin" developed by Logitech.[14]

IT Cybersecurity personnel are unlikely to have observed the stolen software certificates masquerading as Logitech plugins due to the extremely common use of Logitech-associated certificates.

One observable was identified with the use of the Masquerading technique (T0849). This technique is important for investigation because it circumvents critical security tools that can alert a victim of malicious cyber activity. This technique appears late in the timeline and responding to it will likely halt the execution of the malware, although this is unlikely given the brief time from disabling services to ransomware execution. Terminating the chain of techniques at this point would halt the deployment of the ransomware.

The one observable associated with this technique is not assessed to be highly perceivable. It is listed in Appendix A.

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

## 3.13. SERVICE STOP TECHNIQUE (T0881) FOR INHIBIT RESPONSE FUNCTION

DoppelPaymer attempts to disable various processes once executed in the victim's environment. The ransomware makes use of Process Hacker to identify and terminate any listed processes hardcoded in its configuration.[15] Any blacklisted processes are identified via DoppelPaymer using Process Hacker to check the CRC32 hash of the specific process. If a process hash matches to a blacklisted hash, DoppelPaymer then leverages Process Hacker to open a handle to that process and kill it.[16] These processes include common Windows security applications, as well as commercial anti-virus products.

IT Cybersecurity personnel may have been able to observe the malfunctioning or nonfunctioning of Windows security programs or the execution of DoppelPaymer. However, this would be after the deployment and execution of DoppelPaymer throughout the enterprise environment, so any observer attempts to halt execution at this point are unlikely to succeed.

A total of 14 observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation because it disables critical security tools that can alert a victim to malicious cyber activity. This technique appears late in the timeline and responding to it would likely halt final execution of the ransomware, although it is highly unlikely defenders would have sufficient time to act. Terminating the chain of techniques at this point would limit operational damage.

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

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

## 3.14. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

Commodity malware often makes use of the Native API technique (T0834) to help evade behavior-based antivirus engines and interactions with the Windows OS. DoppelPaymer uses the Native API technique (T0834) while halting and disabling security tools before execution via the ZwTerminateProcess Application Programming Interface (API) call.[17] DoppelPaymer also uses the NtCreateFile and ZwDeleteFile API calls.

IT Cybersecurity personnel may have been able to observe execution of Native Windows OS APIs via behavior-based detection engines.

A total of 14 observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because adversaries often use native APIs in malware to avoid behavior-based antivirus engines. This technique appears late in the timeline and responding to it may halt execution of the malware, although it is highly unlikely defenders would have sufficient time to act. Terminating the chain of techniques at this point would potentially halt the execution of DoppelPaymer.

Of the 14 observables associated with this technique, none are assessed to be highly perceivable. They are listed in Appendix A.

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

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

DoppelPaymer changes user passwords before forcing a system restart into safe mode to prevent users from accessing the system. The ransomware will then change the notice text that appears before Windows proceeds to the login screen. Use of this technique may have "[affected] the operation of less than 5% of personal computer equipment," as PEMEX reported in an official announcement.[18]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe anomalous host shutdowns and restarts.

A total of two observables were identified with the use of the Device Restart/Shutdown technique (T0816). This technique is important for investigation because anomalous shutdowns often are part of the final stage of an enterprise-wide ransomware attack. Anomalous shutdowns may also indicate a reliability incident with malfunctioning equipment. This technique appears late in the timeline and responding to it may halt the execution and spread of DoppelPaymer. Terminating the chain of techniques at this point could halt the execution of the ransomware, although it is highly unlikely defenders would have sufficient time to act.

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

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** | A total of 17 artifacts could be generated by the Device Restart/Shutdown technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management |
| **Resources** | Technique Detection References |

## 3.16. DATA DESTRUCTION TECHNIQUE (T0809) FOR INHIBIT RESPONSE FUNCTION

Upon execution of DoppelPaymer, the malware encrypts and appends any targeted file extensions with the .doppeled file extension. This effectively renders any targeted files unusable by end-users. Infected hosts would also display a ransom note on enterprise systems informing users that their files were encrypted, and the only way to decrypt them was to pay the ransom.

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management likely observed files with the .doppeled file extension and were unable to access common file types.

A total of 17 observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because it renders files crucial to business and other enterprise operations unusable. This technique appears late in the timeline and responding to it at this point in the timeline is unlikely to minimize the impact of DoppelPaymer ransomware deployment.

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

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

## 3.17. MANIPULATION OF VIEW TECHNIQUE (T0832) FOR IMPACT

Upon execution of DoppelPaymer, the malware would encrypt any targeted file extensions with the .doppeled extension and display a ransom note on enterprise systems informing users that their files were encrypted and the only way to decrypt them was to pay the ransom.

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management likely observed the ransom note on infected hosts in the enterprise environment.

A total of seven observables were identified with the use of the Manipulation of View technique (T0832). This technique is important for investigation because it prevents the organization from viewing the state of – and prevents users from interacting with – any compromised systems. This technique appears late in the timeline and represents the triggering event for the attack on PEMEX. Responding to it would include efforts to regain operational functionality and resume normal operation. Terminating the chain of techniques at this point would not limit destruction or business impacts.

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

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** | A total of 5 artifacts could be generated by the Manipulation of View technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management |
| **Resources** | Technique Detection References |

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

Although PEMEX released an official statement saying that fewer than 5% of their computers had been affected and the core company functions had not been impacted, PEMEX employees indicated that "entire floors of computers were wiped out" employees had to use old machines to "half-way work".[19,20] PEMEX also was forced to resort to manual billing operations, hindering business and payroll functions. Although the DoppelPaymer attack did not affect core PEMEX functions such as fuel production or supply operations, the impact of an enterprise-centric ransomware attack can impact normal business and supply chain operations.

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel likely observed the switch to manual business and payroll operations due to multiple hosts being rendered unusable by the DoppelPaymer ransomware.

A total of three observables were identified with the use of the Loss of Productivity technique (T0828). This technique is important for investigation to determine the extent of potential damage to systems and business losses. This technique appears after the triggering event and occurs beyond the point at which the victim could limit the impact of the attack.

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

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

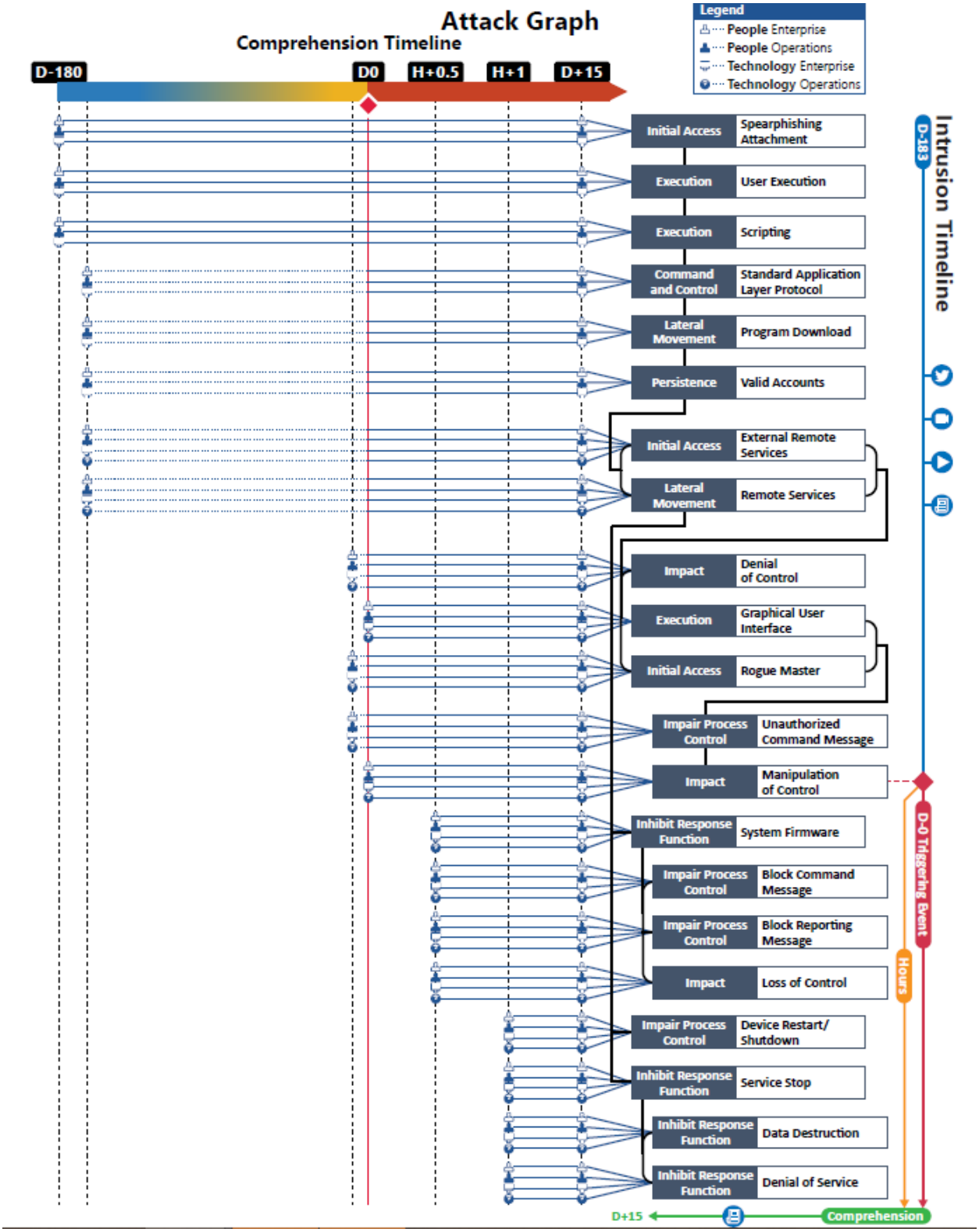



***Figure 3. Attack Graph***

# APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †.

| Observables Associated with Spearphishing Attachment Technique (T0865) | |
|---|---|
| **Observable 1** | Presence of Anomalous Email Containing an Attachment: Office Document: Word Document |
| **Observable 2** | Presence of Anomalous Email Containing an Attachment: Office Document: Excel Document |
| **Observable 3** | Presence of Anomalous Email Containing an Attachment: Office Document: PDF Document |
| **Observable 4** | Presence of Anomalous Email Containing an Attachment: JAR File |
| **Observable 5** | Anomalous Network Traffic: Outbound: HTTP: Over TCP Port 80: HTTP GET Request |
| **Observable 6** | Anomalous Network Traffic: Outbound: HTTPS: Over TCP Port 443: HTTPS Get Request |
| **Observable 7** | Anomalous Prompt to Enable Macros |

| Observables Associated with Drive-By Compromise Technique (T0817) | |
|---|---|
| **Observable 1** | User Interaction with Anomalous Browser Update: Hypertext Markup Language File |
| **Observable 2** | User Interaction with Anomalous Browser Update: JavaScript File |
| **Observable 3** | User Interaction with Anomalous Browser Update: Compressed File: ZIP File |
| **Observable 4** | Anomalous Network Traffic: Inbound: HTTP: Over TCP Port 80: HTTP GET Request |
| **Observable 5** | Anomalous Network Traffic: Inbound: HTTPS: Over TCP Port 443: HTTP GET Request |
| **Observable 6** | Anomalous Network Traffic: Outbound: HTTPS: Over TCP Port 443: HTTP GET Request |
| **Observable 7** | Anomalous Network Traffic: Outbound: HTTPS: Over TCP Port 80: HTTP GET Request |

| Observables Associated with User Execution Technique (T0836) | |
|---|---|
| **Observable 1** | User Interaction with Anomalous Browser Update: Hypertext Markup Language File |
| **Observable 2** | User Interaction with Anomalous Browser Update: JavaScript File |
| **Observable 3** | User Interaction with Anomalous Browser Update: Compressed File: ZIP File |
| **Observable 4** | User Interaction with Anomalous Email: Opens Attachment: Containing Macros: Excel Document |
| **Observable 5** | User Interaction with Anomalous Email: Opens Attachment: Containing Macros: Word Document |

| Observables Associated with User Execution Technique (T0836) | |
|---|---|
| **Observable 6** | User Interaction with Anomalous Email: Opens Attachment: Containing Macros: PDF |
| **Observable 7** | User Interaction with Anomalous Email: Opens Attachment: JAR |
| **Observable 8** | Anomalous Network Traffic: Inbound: HTTP: Over TCP Port 80: HTTP GET Request |
| **Observable 9** | Anomalous Network Traffic: Inbound: HTTPS: Over TCP Port 443: HTTP GET Request |
| **Observable 10** | Anomalous Network Traffic: Outbound: HTTPS: Over TCP Port 443: HTTP GET Request |
| **Observable 11** | Anomalous Network Traffic: Outbound: HTTPS: Over TCP Port 80: HTTP GET Request |
| **Observable 12** | Presence of Anomalous Binary on Host: C:\Users\<username>\Desktop\p1q135no.exe |
| **Observable 13** | Presence of Anomalous Binary on Host: C:\Users\<username>\Desktop\DoppelPaymer.exe |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| **Observable 1** | Anomalous Script Execution on Local Host: PowerShell |
| **Observable 2** | Anomalous Script Execution on Local Host: Visual Basic for Applications (VBA) |
| **Observable 3** | Anomalous Script Execution on Local Host: JavaScript |
| **Observable 4** | Anomalous Script Execution on Local Host: Hypertext Markup Language (HTML) |
| **Observable 5** | Anomalous Network Traffic: Inbound from External IP to Local Host: HTTP: Over TCP Port 80: HTTP GET Request |
| **Observable 6** | Anomalous Network Traffic: Inbound from External IP to Local Host: HTTPS: Over TCP Port 443: HTTP GET Request |
| **Observable 7** | Anomalous Network Traffic: Outbound from Local Host to External IP: Over Hypertext Transfer Protocol Secure TCP Port 443: HTTP GET Request |
| **Observable 8** | Anomalous Network Traffic: Outbound: HTTP: Over TCP Port 80: HTTP GET Request |
| **Observable 9** | UAC Window Pops Up |
| **Observable 10** | Presence of Anomalous Binary on Host |
| **Observable 11** | Presence of Anomalous Binary on Host: C:\Users\<username>\Desktop\p1q135no.exe |
| **Observable 12** | Presence of Anomalous Binary on Host: C:\Users\<username>\Desktop\DoppelPaymer.exe |
| **Observable 13** | Presence of Anomalous Binary on Host: Signed Executable: Spoofed signature: Logitech Plug-In: SpotLife WebAlbum Service Plugin |
| **Observable 14** | Presence of Anomalous File on Host: Anomalous Alternative Data Stream (ADS): In %AppData% |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| **Observable 15** | Anomalous Command-Line: 'C:\Users\<USER>\AppData\Roaming\<random>:<random> QWD5MRg95gUEfGVSvUGBY84h C:\Users\gratemin\Desktop\p1q135no.exe' |
| **Observable 16** | Anomalous Command Line: C:\Windows\system32\takeown.exe /F <service_name> |
| **Observable 17** | Anomalous Command Line: C:\Windows\system32\icacls.exe <service_name> /reset |
| **Observable 18** | Execution of Anomalous Binary on Host: C:\Users\<username>\Desktop\p1q135no.exe |
| **Observable 19** | Execution of Anomalous Binary on Host: Locator.exe |
| **Observable 20** | Creation of Anomalous Service on Host: RPC Locator: Locator.exe |

| Observables Associated with Standard Application Layer Protocol Technique (T0869) | |
|---|---|
| **Observable 1** | Anomalous Network Traffic: From Local Host to External IP: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: HTTP GET Request |
| **Observable 2** | Anomalous Network Traffic: From Local Host to External IP: Over Hypertext Transfer Secure Protocol (HTTPS) TCP Port 443: HTTPS GET Request |
| **Observable 3 †** | *Anomalous Network Traffic: From Local Host to External IP: Over File Transfer Protocol (FTP) TCP Port 22* |
| **Observable 4 †** | *Anomalous Network Traffic: From Local Host to External IP: Over Secure File Transfer Protocol (SFTP) TCP Port 23* |
| **Observable 5** | Anomalous Network Traffic: From External IP to Local Host: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: HTTP POST Request |
| **Observable 6** | Anomalous Network Traffic: From External IP to Local Host: Over Hypertext Transfer Secure Protocol (HTTPS) TCP Port 443: HTTPS POST Request |
| **Observable 7** | Anomalous Network Traffic: From External IP to Local Host: Over File Transfer Protocol (FTP) TCP Port 22 |
| **Observable 8** | Anomalous Network Traffic: From External IP to Local Host: Over Secure File Transfer Protocol (SFTP) TCP Port 23 |
| **Observable 9 †** | *Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) TCP Port 445* |
| **Observable 10 †** | *Anomalous Network Traffic: From External IP to Local Host: Over Remote Desktop Protocol (RDP) TCP Port 3389* |

| Observables Associated with Commonly Used Port Technique (T0855) | |
|---|---|
| **Observable 1** | Anomalous Network Traffic: From Local Host to External IP: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: HTTP GET Request |
| **Observable 2** | Anomalous Network Traffic: From Local Host to External IP: Over Hypertext Transfer Secure Protocol (HTTPS) TCP Port 443: HTTPS GET Request |
| **Observable 3 †** | *Anomalous Network Traffic: From Local Host to External IP: Over File Transfer Protocol (FTP) TCP Port 22* |

| Observables Associated with Commonly Used Port Technique (T0855) | |
|---|---|
| **Observable 4 †** | *Anomalous Network Traffic: From Local Host to External IP: Over Secure File Transfer Protocol (SFTP) TCP Port 23* |
| **Observable 5** | Anomalous Network Traffic: From External IP to Local Host: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: HTTP POST Request |
| **Observable 6** | Anomalous Network Traffic: From External IP to Local Host: Over Hypertext Transfer Secure Protocol (HTTPS) TCP Port 443: HTTPS POST Request |
| **Observable 7** | Anomalous Network Traffic: From External IP to Local Host: Over File Transfer Protocol (FTP) TCP Port 22 |
| **Observable 8** | Anomalous Network Traffic: From External IP to Local Host: Over Secure File Transfer Protocol (SFTP) TCP Port 23 |
| **Observable 9 †** | *Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) TCP Port 445* |
| **Observable 10 †** | *Anomalous Network Traffic: From External IP to Local Host: Over Remote Desktop Protocol (RDP) TCP Port 3389* |

| Observables Associated with Remote Services Technique (T0886) | |
|---|---|
| **Observable 1 †** | *Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) TCP Port 445* |
| **Observable 2 †** | *Anomalous Network Traffic: From External IP to Local Host: Over Remote Desktop Protocol (RDP) TCP Port 3389* |
| **Observable 3** | Anomalous Host Activity: Successful Logon From External Host: Valid User Account Windows Event ID (4624): Anomalous timestamp |
| **Observable 4** | Anomalous Host Activity: Successful Logon From External Host: Valid User Account Windows Event ID (4624): Anomalous remote IP |

| Observables Associated with Valid Accounts Technique (T0859) | |
|---|---|
| **Observable 1 †** | *Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) TCP Port 445* |
| **Observable 2 †** | *Anomalous Network Traffic: From External IP to Local Host: Over Remote Desktop Protocol (RDP) TCP Port 3389* |
| **Observable 3** | Anomalous Host Activity: Successful Logon From External Host: An Account Was Successfully Logged On (Windows Event ID 4624): Anomalous Timestamp |
| **Observable 4** | Anomalous Host Activity: Successful Logon From External Host: An Account Was Successfully Logged On (Windows Event ID 4624): Anomalous Remote IP |
| **Observable 5** | Anomalous Host Activity: Increase in Failed Login Attempts: An Account Failed To Log On (Windows Event ID 4625): Anomalous Timestamp |
| **Observable 6** | Anomalous Host Activity: Increase in Failed Login Attempts: An Account Failed To Log On (Windows Event ID 4625): Anomalous Remote IP |

| Observables Associated with Lateral Tool Transfer Technique (T0867) | |
|---|---|
| **Observable 1** | Anomalous Network Traffic: From Local Host to External IP: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: HTTP GET Request |
| **Observable 2** | Anomalous Network Traffic: From Local Host to External IP: Over Hypertext Transfer Secure Protocol (HTTPS) TCP Port 443: HTTPS GET Request |
| **Observable 3 †** | *Anomalous Network Traffic: From Local Host to External IP: Over File Transfer Protocol (FTP) TCP Port 22* |
| **Observable 4 †** | *Anomalous Network Traffic: From Local Host to External IP: Over Secure File Transfer Protocol (SFTP) TCP Port 23* |
| **Observable 5** | Anomalous Network Traffic: From Local Host to External IP: Via Rclone Application |
| **Observable 6 †** | *Anomalous Network Traffic: From Local Host to External IP: Over TCP Port 445* |
| **Observable 7** | Anomalous Network Traffic: From External IP to Local Host: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: HTTP POST Request |
| **Observable 8** | Anomalous Network Traffic: From External IP to Local Host: Over Hypertext Transfer Secure Protocol (HTTPS) TCP Port 443: HTTPS POST Request |
| **Observable 9 †** | *Anomalous Network Traffic: From External IP to Local Host: Over File Transfer Protocol (FTP) TCP Port 22* |
| **Observable 10 †** | *Anomalous Network Traffic: From External IP to Local Host: Over Secure File Transfer Protocol (SFTP) TCP Port 23* |
| **Observable 11 †** | *Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) TCP Port 445* |
| **Observable 12 †** | *Anomalous Command Line: rclone copy <source:sourcepath> <dest:destpath>* |
| **Observable 13 †** | *Anomalous Command Line: mega-export -a <Local Host File Path> <Remote Host File Path>* |
| **Observable 14** | Anomalous Command Line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| **Observable 15** | Anomalous Binary on Local Host: rclone.exe |
| **Observable 16** | Anomalous Binary on Local Host: MEGAcmdShell.exe |
| **Observable 17** | Anomalous Binary on Local Host: empire.exe |
| **Observable 18** | Anomalous Binary on Local Host: koadic.exe |
| **Observable 19** | Execution of Anomalous Binary on Host: rclone.exe |
| **Observable 20** | Execution of Anomalous Binary on Host: MEGAcmdShell.exe |
| **Observable 21** | Execution of Anomalous Binary on Host: empire.exe |
| **Observable 22** | Execution of Anomalous Binary on Host: koadic.exe |

| Observables Associated with Command-Line Interface Technique (T0807) | |
|---|---|
| **Observable 1** | Anomalous Network Traffic: From Local Host to External IP: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: HTTP GET Request |

| Observables Associated with Command-Line Interface Technique (T0807) | |
|---|---|
| **Observable 2** | Anomalous Network Traffic: From Local Host to External IP: Over Hypertext Transfer Secure Protocol (HTTPS) TCP Port 443: HTTPS GET Request |
| **Observable 3 †** | *Anomalous Network Traffic: From Local Host to External IP: Over File Transfer Protocol (FTP) TCP Port 22* |
| **Observable 4 †** | *Anomalous Network Traffic: From Local Host to External IP: Over Secure File Transfer Protocol (SFTP) TCP Port 23* |
| **Observable 5** | Anomalous Network Traffic: From Local Host to External IP: Via Rclone application |
| **Observable 6** | Anomalous Network Traffic: From Local Host to External IP: Over TCP Port 445 |
| **Observable 7 †** | *Anomalous Command Line: rclone.exe copy <source:sourcepath> <dest:destpath>* |
| **Observable 8 †** | *Anomalous Command Line: MEGAcmdShell.exe mega-export -a <Local Host File Path> <Remote Host File Path>* |
| **Observable 9** | Anomalous Command Line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| **Observable 10** | Anomalous Binary on Local Host: MEGAcmdShell.exe |
| **Observable 11** | Anomalous Binary on Local Host: empire.exe |
| **Observable 12** | Anomalous Binary on Local Host: koadic.exe |
| **Observable 13** | Execution of Anomalous Binary on Host: rclone.exe |
| **Observable 14** | Execution of Anomalous Binary on Host: MEGAcmdShell.exe |
| **Observable 15** | Execution of Anomalous Binary on Host: empire.exe |
| **Observable 16** | Execution of Anomalous Binary on Host: koadic.exe |

| Observables Associated with Theft of Operational Information Technique (T0882) | |
|---|---|
| **Observable 1** | Anomalous Network Traffic: From Local Host to External IP: Over Hypertext Transfer Protocol (HTTP) TCP Port 80: HTTP GET Request |
| **Observable 2** | Anomalous Network Traffic: From Local Host to External IP: Over Hypertext Transfer Secure Protocol (HTTPS) TCP Port 443: HTTPS GET Request |
| **Observable 3 †** | *Anomalous Network Traffic: From Local Host to External IP: Over File Transfer Protocol (FTP) TCP Port 22* |
| **Observable 4 †** | *Anomalous Network Traffic: From Local Host to External IP: Over Secure File Transfer Protocol (SFTP) TCP Port 23* |
| **Observable 5** | Anomalous Network Traffic: From Local Host to External IP: Via Rclone application |
| **Observable 6 †** | *Anomalous Network Traffic: From Local Host to External IP: Over TCP Port 445* |
| **Observable 7 †** | *Anomalous Command Line: rclone.exe copy <source:sourcepath> <dest:destpath>* |

| Observables Associated with Theft of Operational Information Technique (T0882) | |
|---|---|
| **Observable 8 †** | *Anomalous Command Line: MEGAcmdShell.exe mega-export -a <Local Host File Path> <Remote Host File Path>* |
| **Observable 9** | Anomalous Command Line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| **Observable 10** | Anomalous Binary on Local Host: rclone.exe |
| **Observable 11** | Anomalous Binary on Local Host: MEGAcmdShell.exe |
| **Observable 12** | Anomalous Binary on Local Host: empire.exe |
| **Observable 13** | Anomalous Binary on Local Host: koadic.exe |
| **Observable 14** | Execution of Anomalous Binary on Host: rclone.exe |
| **Observable 15** | Execution of Anomalous Binary on Host: MEGAcmdShell.exe |
| **Observable 16** | Execution of Anomalous Binary on Host: empire.exe |
| **Observable 17** | Execution of Anomalous Binary on Host: koadic.exe |

| Observables Associated with Masquerading Technique (T0849) | |
|---|---|
| **Observable 1** | Presence of Anomalous Binary on Host: Signed Executable: Spoofed signature: Logitech Plug-In: SpotLife WebAlbum Service Plugin |

| Observables Associated with Service Stop Technique (T0881) | |
|---|---|
| **Observable 1** | Anomalous Command Line: C:\Windows\system32\takeown.exe /F <service_name> |
| **Observable 2** | Anomalous Command Line: C:\Windows\system32\icacls.exe <service_name> /reset |
| **Observable 3 †** | *Anomalous Host Activity: Windows Service Disabled: Windows Security Services* |
| **Observable 4** | Anomalous Host Activity: Windows Service Disabled: Email Services |
| **Observable 5** | Anomalous Host Activity: Windows Service Disabled: Backup Services |
| **Observable 6** | Anomalous Host Activity: Windows Service Disabled: Database Services |
| **Observable 7 †** | *Anomalous Host Activity: Windows Service Disabled: AntiVirus Services* |
| **Observable 8** | Anomalous Host Activity: Windows Process Terminated (Event ID 4689) |
| **Observable 9 †** | *Anomalous Host Activity: Windows Process Terminated: Windows Security Service Processes* |
| **Observable 10** | Anomalous Host Activity: Windows Process Terminated: Email Service Processes |
| **Observable 11** | Anomalous Host Activity: Windows Process Terminated: Backup Service Processes |
| **Observable 12** | Anomalous Host Activity: Windows Process Terminated: Database Service Processes |

| Observables Associated with Service Stop Technique (T0881) | |
|---|---|
| **Observable 13 †** | *Anomalous Host Activity: Windows Process Terminated: AntiVirus Service Processes* |
| **Observable 14** | Presence of Anomalous Binary on Local Host: kprocesshacker.sys |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| **Observable 1** | Anomalous Execution of Native OS API: Windows API: ZwTerminateProcess |
| **Observable 2** | Anomalous Execution of Native OS API: Windows API: NtCreateFile |
| **Observable 3** | Anomalous Execution of Native OS API: Windows API: ZwDeleteFile |
| **Observable 4** | Presence of Anomalous Binary on Host: C:\Users\<username>\Desktop\p1q135no.exe |
| **Observable 5** | Presence of Anomalous Binary on Host: C:\Users\<username>\Desktop\DoppelPaymer.exe |
| **Observable 6** | Presence of Anomalous Binary on Host: kprocesshacker.sys |
| **Observable 7** | Execution of Anomalous Binary on Host: C:\Users\<username>\Desktop\p1q135no.exe |
| **Observable 8** | Execution of Anomalous Binary on Host: Locator.exe |
| **Observable 9** | Execution of Anomalous Binary on Host: kprocesshacker.sys |
| **Observable 10** | Anomalous Execution of Binary on Host: ntdll.dll |
| **Observable 11** | Anomalous Execution of Binary on Host: kernel32.dll |
| **Observable 12** | Anomalous Execution of Binary on Host: advapi32.dll |
| **Observable 13** | Anomalous Execution of Binary on Host: shlwapi.dll |
| **Observable 14** | Anomalous Execution of Binary on Host: crypt32.dll |

| Observables Associated with Device Stop/Device Restart Technique (T0816) | |
|---|---|
| **Observable 1** | Anomalous Host Activity: Host reboots (Event ID 4609) |
| **Observable 2 †** | *Anomalous Host Activity: Host reboots: Reboots into Safe Mode: Displays Anomalous Text on Reboot* |

| Observables Associated with Data Destruction Technique (T0809) | |
|---|---|
| **Observable 1** | Anomalous Increase in System Resource Utilization: Increase in CPU Utilization |
| **Observable 2** | Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity |
| **Observable 3** | Anomalous Increase in System Resource Utilization: Increase in Network Activity |
| **Observable 4** | Anomalous Command Line: C:\Windows\system32\vssadmin.exe Delete Shadows /All /Quiet |

| Observables Associated with Data Destruction Technique (T0809) | |
|---|---|
| **Observable 5** | Anomalous Command Line: C:\Windows\system32\diskshadow.exe /s C:\Users\User\Appdata\Local\Temp\<random>.tmp |
| **Observable 6** | Anomalous Command Line: C:\Windows\system32\takeown.exe /F <file> |
| **Observable 7** | Anomalous Command Line: C:\Windows\system32\icacls.exe <file> /reset |
| **Observable 8** | Anomalous deletion of data: Deletion of Windows Shadow Volume |
| **Observable 9 †** | *Anomalous Modification of Files: .doppeled Appended to Filenames* |
| **Observable 10 †** | *Anomalous Modification of Files: Files Encrypted on Host* |
| **Observable 11 †** | *Presence of Anomalous File: Anomalous File on Desktop: Howtodecrypt.txt* |
| **Observable 12 †** | *Presence of Anomalous File: Anomalous File on Desktop: Howtodecrypt.txt: File Contains TOR Link* |
| **Observable 13 †** | *Presence of Anomalous File: Anomalous File on Desktop: Howtodecrypt.txt: File Contains @protonmail.com Email Address* |
| **Observable 14** | Presence of Anomalous File: <random>.tmp file in %TEMP% folder |
| **Observable 15** | Presence of Anomalous File: Unencrypted System Volume Information |
| **Observable 16** | Presence of Anomalous File: Unencrypted $RECYCLE.BIN |
| **Observable 17** | Presence of Anomalous File: Unencrypted WebCache |

| Observables Associated with Manipulation of View Technique (T0832) | |
|---|---|
| **Observable 1 †** | *Anomalous Modification of Files: .doppeled Appended to Filenames* |
| **Observable 2 †** | *Anomalous Modification of Files: Files Encrypted on Host* |
| **Observable 3 †** | *Presence of Anomalous File: Anomalous File on Desktop: Howtodecrypt.txt* |
| **Observable 4 †** | *Presence of Anomalous File: Anomalous File on Desktop: Howtodecrypt.txt: File Contains TOR Link* |
| **Observable 5 †** | *Presence of Anomalous File: Anomalous File on Desktop: Howtodecrypt.txt: File Contains @protonmail.com Email Address* |
| **Observable 6** | Anomalous Host Activity: Host Reboots (Event ID 4609) |
| **Observable 7** | Anomalous Host Activity: Host Reboots: Reboots into Safe Mode: Displays Anomalous Text on Reboot |

| Observables Associated with Loss of Productivity and Revenue Technique (T0882) | |
|---|---|
| **Observable 1 †** | *Anomalous Loss of Productivity: Business Processes Inaccessible: Enterprise Functionality* |
| **Observable 2 †** | *Anomalous Loss of Productivity: Business Processes Inaccessible: Standard Business Operations* |
| **Observable 3 †** | *Anomalous Loss of Productivity: Business Processes Inaccessible: Billing* |

# APPENDIX B: ARTIFACTS LIBRARY

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

| Artifacts Associated with Drive-by Compromise Technique (T0817) | |
|---|---|
| **Artifact 1** | Destination IP Address |
| **Artifact 2** | Industrial Application Disk Write |

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

| Artifacts Associated with User Execution Technique (T0863) | |
|---|---|
| **Artifact 1** | Command Execution |
| **Artifact 2** | Service Termination |
| **Artifact 3** | File Changes |
| **Artifact 4** | Increased ICMP Traffic (Network Scanning) |
| **Artifact 5** | Network Traffic Changes |
| **Artifact 6** | Application Installation |
| **Artifact 7** | Network Connection Creation |
| **Artifact 8** | Application Log Content |
| **Artifact 9** | User Account Modification |
| **Artifact 10** | File Creation |

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

| Artifacts Associated with Scripting Technique (T0853) | |
|---|---|
| **Artifact 1** | Startup Menu Modification |
| **Artifact 2** | OS Service Installation |
| **Artifact 3** | Registry Modifications |
| **Artifact 4** | Network Services Created |
| **Artifact 5** | External Network Connections |
| **Artifact 6** | Prefetch Files Created |
| **Artifact 7** | Executable Files |
| **Artifact 8** | System Processes Created |
| **Artifact 9** | OS Timeline Event |
| **Artifact 10** | System Event Log Creation |
| **Artifact 11** | Files Dopped into Directory |
| **Artifact 12** | Windows Api Event Log |

| Artifacts Associated with Standard Application Layer Protocol Technique (T0869) | |
|---|---|
| **Artifact 1** | SMB Traffic Port |
| **Artifact 2** | Network Connection Times |
| **Artifact 3** | External IP Addresses |
| **Artifact 4** | External Network Connections |
| **Artifact 5** | DNS Autonomous System Number |

| Artifacts Associated with Standard Application Layer Protocol Technique (T0869) | |
|---|---|
| **Artifact 6** | Increase in the Number of External Connections |
| **Artifact 7** | RDP Traffic Port |
| **Artifact 8** | HTTP Traffic Port |
| **Artifact 9** | DNS Traffic Port |
| **Artifact 10** | HTTP Post Request |
| **Artifact 11** | HTTPS Traffic Port |
| **Artifact 12** | Network Content Metadata |

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

| Artifacts Associated with Remote Services Technique (T0886) | |
|---|---|
| **Artifact 1** | Mouse Movement |
| **Artifact 2** | Authentication Logs |
| **Artifact 3** | Network Traffic Content Creation |
| **Artifact 4** | Remote Session Creation Timestamp |
| **Artifact 5** | Process Creation |
| **Artifact 6** | VNC Traffic |
| **Artifact 7** | SMB Traffic |
| **Artifact 8** | SSH Traffic |
| **Artifact 9** | MSSQL Traffic 1433 Port |
| **Artifact 10** | File Movement |
| **Artifact 11** | Desktop Prompt Windows Created |
| **Artifact 12** | GUI Modifications |
| **Artifact 13** | System Log Event |
| **Artifact 14** | RDP Traffic |
| **Artifact 15** | Application Log |
| **Artifact 16** | Session Cache |
| **Artifact 17** | Unexpected |
| **Artifact 18** | Registry Connection Change |

| Artifacts Associated with Remote Services Technique (T0886) | |
|---|---|
| **Artifact 19** | Registry Changes |
| **Artifact 20** | Logoff Event |
| **Artifact 21** | Logoff |
| **Artifact 22** | Logon Event |
| **Artifact 23** | Remote Client Connection |
| **Artifact 24** | Data File Size In Network Content |

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

| Artifacts Associated with Lateral Tool Transfer Technique (T0867) | |
|---|---|
| **Artifact 1** | Remote Network Traffic |
| **Artifact 2** | File Metadata Changes |
| **Artifact 3** | User Information Changes |
| **Artifact 4** | Process Creation |
| **Artifact 5** | System Resource Usage Management Events |
| **Artifact 6** | Data Sent from One Location to Another |
| **Artifact 7** | Data Received from One Location to Another |
| **Artifact 8** | SQL Commands |

| Artifacts Associated with Lateral Tool Transfer Technique (T0867) | |
|---|---|
| **Artifact 9** | SQL Create Commands |
| **Artifact 10** | SQL Insert Commands |
| **Artifact 11** | Command Prompt Dialog Box Open |
| **Artifact 12** | SMB Traffic |
| **Artifact 13** | .dll Injection into File Directory |
| **Artifact 14** | .dll Execution |
| **Artifact 15** | Common Network Traffic |
| **Artifact 16** | Command Execution |
| **Artifact 17** | Industrial Network Traffic |
| **Artifact 18** | File Creation |
| **Artifact 19** | File Modification |
| **Artifact 20** | File Deletion |
| **Artifact 21** | File Location Change |
| **Artifact 22** | POWERSHELL Dialog Box Open |

| Artifacts Associated with Command-Line Interface Technique (T0807) | |
|---|---|
| **Artifact 1** | Command Execution |
| **Artifact 2** | Application Log |
| **Artifact 3** | HTTP Traffic |
| **Artifact 4** | Telnet Traffic |
| **Artifact 5** | SSH Traffic |
| **Artifact 6** | VNC Traffic Port |
| **Artifact 7** | Process Creation |
| **Artifact 8** | Remote Connections |
| **Artifact 9** | Process Ending |
| **Artifact 10** | Script Execution |
| **Artifact 11** | User Account Logon |
| **Artifact 12** | User Account Privilege Change |
| **Artifact 13** | Logon Event |
| **Artifact 14** | Event Log Type |
| **Artifact 15** | Event Log Type |
| **Artifact 16** | Failed Logon Event |
| **Artifact 17** | Command-Line Memory Data |
| **Artifact 18** | cmd.exe Application Execution |

| Artifacts Associated with Command-Line Interface Technique (T0807) | |
|---|---|
| **Artifact 19** | RDP Traffic |
| **Artifact 20** | Industrial Application Execution |
| **Artifact 21** | POWERSHELL Cmdlet Application Execution |
| **Artifact 22** | Event ID 4103 POWERSHELL Command |
| **Artifact 23** | Event ID 4688 Command-Line Execution |
| **Artifact 24** | NTUSER Application Execution Entries |
| **Artifact 25** | External Network Connection |

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

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

| Artifacts Associated with Service Stop Technique (T0881) | |
|---|---|
| **Artifact 1** | Internal System Logs |

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

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

| Artifacts Associated with Native API Technique (T0834) | |
|---|---|
| **Artifact 21** | Device Memory Modification |
| **Artifact 22** | Device Alarm |
| **Artifact 23** | Device Live Data Changes |
| **Artifact 24** | Alter Process Logic |
| **Artifact 25** | Memory Corruption |

| Artifacts Associated with Device Restart/Shutdown Technique (T0816) | |
|---|---|
| **Artifact 1** | Logon Events |
| **Artifact 2** | Process Alarm |
| **Artifact 3** | Memory Corruption |
| **Artifact 4** | Unauthorized Input |
| **Artifact 5** | Command Prompt Opened |
| **Artifact 6** | Hardware Failure |
| **Artifact 7** | Logoff Events |
| **Artifact 8** | Local Network Connections |
| **Artifact 9** | Significant Operational Data Changes |
| **Artifact 10** | Blue Screen |
| **Artifact 11** | Reboot Screen |
| **Artifact 12** | Network Command Packets |
| **Artifact 13** | Loss of Network Connection |
| **Artifact 14** | Process Environmental Changes |
| **Artifact 15** | Process Failure |
| **Artifact 16** | Process Application Event |
| **Artifact 17** | External Network Connections |

| Artifacts Associated with Data Destruction Technique (T0809) | |
|---|---|
| **Artifact 1** | Command-Line Arguments |
| **Artifact 2** | Files Moved to Recycle Bin |
| **Artifact 3** | Missing Files |
| **Artifact 4** | Host System Reboot Failure |
| **Artifact 5** | Process Logic Failure |
| **Artifact 6** | Event Log Creation |
| **Artifact 7** | System Call |
| **Artifact 8** | System Application Interruption |

| Artifacts Associated with Data Destruction Technique (T0809) | |
|---|---|
| **Artifact 9** | Device Failure |
| **Artifact 10** | Recovery Attempt Failure |
| **Artifact 11** | TFTP Port |
| **Artifact 12** | SFTP Port |
| **Artifact 13** | Memory Corruption |
| **Artifact 14** | Use of File Transfer Protocols |
| **Artifact 15** | SCP Port |
| **Artifact 16** | File Encryptions |
| **Artifact 17** | Non-Native Files |
| **Artifact 18** | External Network Connections |
| **Artifact 19** | Transient Device Connections |
| **Artifact 20** | Program Execution |
| **Artifact 21** | Telnet Port |
| **Artifact 22** | FTPS Port |
| **Artifact 23** | HTTP Port |
| **Artifact 24** | HTTPS Port |
| **Artifact 25** | Local Network Connections |
| **Artifact 26** | FTP Port |
| **Artifact 27** | SMB Port |

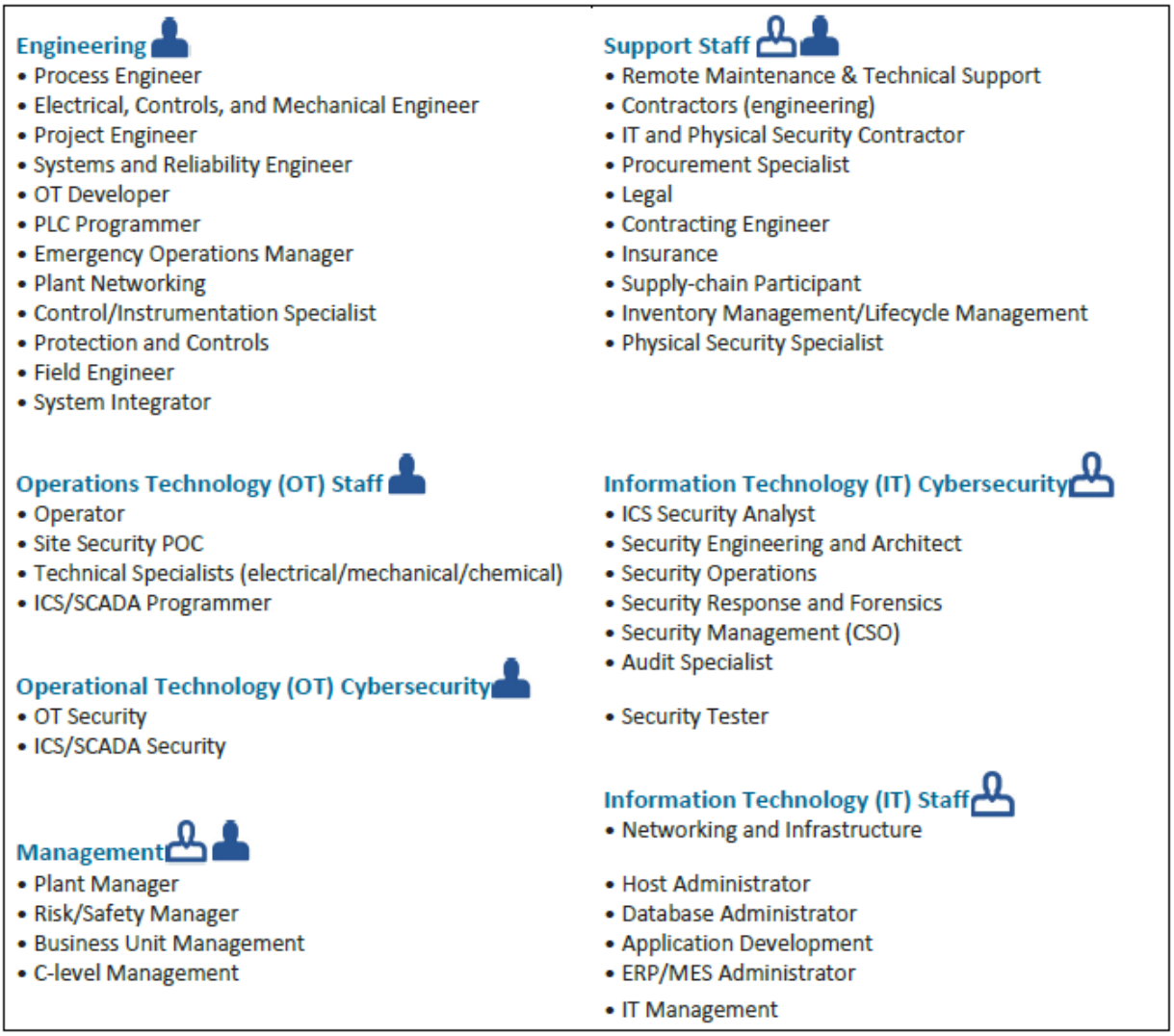
| Artifacts Associated with Manipulation of View Technique (T0832) | |
|---|---|
| **Artifact 1** | Modification of Operating System or the Installation of a Filter Driver Could Lead to Manipulations of Packet at the Kernel Level |
| **Artifact 2** | File System Modification Artifacts Might Be Associated with the Manipulation of View Attack Might Be Present on Disk |
| **Artifact 3** | A Rogue Proxy, Gateway, or Network Device in the Path of the Industrial Communications Could Manipulate Traffic |
| **Artifact 4** | Compromise and Manipulation of Data Storage Locations Used to Produce or Present Information to Operators |
| **Artifact 5** | Modification of Application Libraries or Dependencies as Seen with STUXNET DLL Hooking |

| Artifacts Associated with Loss of Productivity and Revenue Technique (T0828) | |
|---|---|
| **Artifact 1** | Loss of Confidence in a Safety System Due to Unreliability Might Result in a Risk Management Driven Shutdown of a Plant |
| **Artifact 2** | Wormable or Other Highly Propagating Malware Might Result in the Shutdown of a Plant to Prevent Ransomware or Other Destructive Attacks |

| Artifacts Associated with Loss of Productivity and Revenue Technique (T0828) | |
|---|---|
| **Artifact 3** | Extortion Attempts Might Lead to Reduced Operations Due to Potential Presence of Malicious Attackers |
| **Artifact 4** | Loss of Control of Critical Systems Due to Ransomware or Loss of Confidence Might Lead to a Degraded Productivity or Revenue Operating State |
| **Artifact 5** | File System Modification Artifacts Might Be Associated with the Loss of Productivity and Revenue Attack Might Be Present On Disk |

# APPENDIX C: OBSERVERS

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



# REFERENCES

[1] [Bleeping Computer | Lawrence Abrams | "Mexico's Pemex Oil Suffers Ransomware Attack, $4.9 Million Demanded" | https://www.bleepingcomputer.com/news/security/mexicos-pemex-oil-suffers-ransomware-attack-49-million-demanded/ | 21 April 2021 | Accessed on 5 September 2022 | The source is publicly available information and does not contain classification markings]

[2] [Reuters | Adriana Barrera | "Ransomware attack on Mexico's Pemex halts work, threatens to cripple computers" | https://www.reuters.com/article/us-mexico-pemex/ransomware-attack-at-mexicos-pemex-halts-work-threatens-to-cripple-computers-idUSKBN1XM041 | 11 November 2019 | Accessed on 5 October 2022 | The source is publicly available information and does not contain classification markings]

[3] [Bleeping Computer | Lawrence Abrams | "Mexico's Pemex Oil Suffers Ransomware Attack, $4.9 Million Demanded" | https://www.bleepingcomputer.com/news/security/mexicos-pemex-oil-suffers-ransomware-attack-49-million-demanded/ | 21 April 2021 | Accessed on 5 September 2022 | The source is publicly available information and does not contain classification markings]

[4] [Mandiant | Kappellman Zafra, and others | "1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information" | https://www.mandiant.com/resources/blog/ransomware-extortion-ot-docs | 31 January 2022 | Accessed on 1 September 2022 | The source is publicly available information and does not contain classification markings]

[5][CERT-FR | "The Malware-as-a-Service Emotet" | https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-003.pdf | 12 February 2021 | Accessed on 15 September 2022 | The source is publicly available information and does not contain classification markings]

[6] [Cybersecurity and Infrastructure Security Agency | "Alert (AA19-339A Dridex Malware" | https://www.cisa.gov/uscert/ncas/alerts/aa19-339a | 5 December 2019 | Accessed on 22 August 2022 | The source is publicly available information and does not contain classification markings]

[7] [U.S. Department of Health and Human Services | "HC3 Intelligence Briefing Dridex Malware" | https://www.aha.org/system/files/media/file/2020/06/hc3-cyber-threat-briefing-tlp-white-dridex%20malware-6-25-2020.pdf | 5 June 2020 | Accessed on 1 October 2022 | The source is publicly available information and does not contain classification markings]

[8] [CERT-FR | "The Malware Dridex: Origins and Uses" | https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf | 17 July 2020 | Accessed on 15 September 2022 | The source is publicly available information and does not contain classification markings]

[9] [Mandiant | Abdo, and others | "Head Fake: Tackling Disruptive Ransomware Attacks" | https://www.mandiant.com/resources/blog/head-fake-tackling-disruptive-ransomware-attacks | 1 October 2019 | Accessed on 15 September 2022 | The source is publicly available information and does not contain classification markings]

[10] [Department of Health and Human Services | "HC3 Intelligence Briefing Dridex Malware" | https://www.aha.org/system/files/media/file/2020/06/hc3-cyber-threat-briefing-tlp-white-dridex%20malware-6-25-2020.pdf | 5 June 2020 | Accessed on 1 October 2022 | The source is publicly available information and does not contain classification markings]

[11] [Sucuri | Denis Sinegubko| "SocGhoulish: 5+ Years of Massive Website Infections" | https://blog.sucuri.net/2022/06/analysis-massive-ndsw-ndsx-malware-campaign.html | 16 August 2022 | Accessed on 1 October 2022 | The source is publicly available information and does not contain classification markings]

[12] [Mandiant | Abdo, and others | "Head Fake: Tackling Disruptive Ransomware Attacks" | https://www.mandiant.com/resources/blog/head-fake-tackling-disruptive-ransomware-attacks | 1 October 2019 | Accessed on 15 September 2022 | The source is publicly available information and does not contain classification markings]

[13] [Trend Micro| Agcaoilli, and others | "Ransomware Double Extortion and Beyond" | https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-

extortion-and-beyond-revil-clop-and-conti | December 2021 | Accessed on 10 November 2022 | The source is publicly available information and does not contain classification markings]

[14] [Acronis | "Threat Analysis: DoppelPaymer Ransomware" | https://www.acronis.com/en-us/cyber-protection-center/posts/doppelpaymer-ransomware/ | 4 June 2021 | Accessed on 10 November 2022 | The source is publicly available information and does not contain classification markings]

[15] [CrowdStrike | Shaun Hurley | "Critical Hit: How DoppelPaymer Hunts and Kills Windows Processes" | https://www.crowdstrike.com/blog/how-doppelpaymer-hunts-and-kills-windows-processes/ | 7 December 2021 | Accessed on 15 September 2022 | The source is publicly available information and does not contain classification markings]

[16] [CrowdStrike | Shaun Hurley | "Critical Hit: How DoppelPaymer Hunts and Kills Windows Processes" | https://www.crowdstrike.com/blog/how-doppelpaymer-hunts-and-kills-windows-processes/ | 7 December 2021 | Accessed on 15 September 2022 | The source is publicly available information and does not contain classification markings]

[17] Department of Health and Human Services | "HC3 Intelligence Briefing Dridex Malware" | https://www.aha.org/system/files/media/file/2020/06/hc3-cyber-threat-briefing-tlp-white-dridex%20malware-6-25-2020.pdf | 5 June 2020 | Accessed on 1 October 2022 | The source is publicly available information and does not contain classification markings]

[18] [PEMEX | "Pemex opera con normalidad" | 11 November 2019 | Accessed on 17 December 2022 | https://www.pemex.com/saladeprensa/boletines_nacionales/Paginas/2019-47_nacional.aspx | The source is publicly available information and does not contain classification markings]

[19] [Bleeping Computer | Lawrence Abrams | "Mexico's Pemex Oil Suffers Ransomware Attack, $4.9 Million Demanded" | https://www.bleepingcomputer.com/news/security/mexicos-pemex-oil-suffers-ransomware-attack-49-million-demanded/ | 21 April 2021 | Accessed on 5 September 2022 | The source is publicly available information and does not contain classification markings]

[20] [Reuters | "Mexican minister says Pemex oil firm unaffected by cyberattack, workers disagree" | https://www.reuters.com/article/us-mexico-pemex/mexican-minister-says-pemex-oil-firm-unaffected-by-cyberattack-workers-disagree-idUSKBN1XP02D | 21 April 2021 | Accessed on 22 August 2022 | The source is publicly available information and does not contain classification markings]