PRECURSOR ANALYSIS REPORT: NIGHT DRAGON CAMPAIGN (2007 TO 2011) TARGETING A U.S.-BASED OIL AND GAS FIRM

Cybersecurity for the Operational Technology Environment (CyOTE)

30 SEPTEMBER 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-69761

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

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

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

TABLE OF CONTENTS

FIGURES

TABLES

PRECURSOR ANALYSIS: NIGHT DRAGON CAMPAIGN (2007 TO 2011) TARGETING A U.S.-BASED OIL AND GAS FIRM

1. EXECUTIVE SUMMARY

The Night Dragon Campaign (2007 to 2011) Targeting a U.S.-based Oil and Gas Firm Precursor Analysis Report leverages publicly available information about the Night Dragon malware campaign and catalogs anomalous observables for each employed technique. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

In February 2011, commercial analysts announced the discovery of a series of coordinated attacks—designated Night Dragon—against global oil, energy, and petrochemical companies. The campaign targeted at least five and possibly as many as 12 multinational energy and oil firms. The attacks likely began sometime in 2007, and industry began monitoring them in November 2009. Night Dragon activity occurred in the Americas, Europe, and Asia. Adversaries used a coordinated combination of techniques including spearphishing and remote administration tools to target and exfiltrate sensitive data. The adversaries targeted information concerning operational technology, field exploration, financial documentation, and contractual bids for oil and gas assets. Damages from Night Dragon were potentially in the hundreds of millions of dollars.

This case study will illustrate an attack sequence against a notional U.S.-based oil and gas firm from the evidence and behavior exhibited during the Night Dragon cyber attacks that occurred between 2007 and 2011.

Researchers and analysts identified 19 unique techniques (used in a sequence of 24 steps) utilized during the attack with a total of 182 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Twenty-three of the identified techniques used during the notional Night Dragon cyber attack were precursors to the triggering event. Case study analysis identified 170 observables associated with these precursor techniques, 105 of which were assessed to have an increased likelihood of being perceived in the roughly three years 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. Organizations 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.

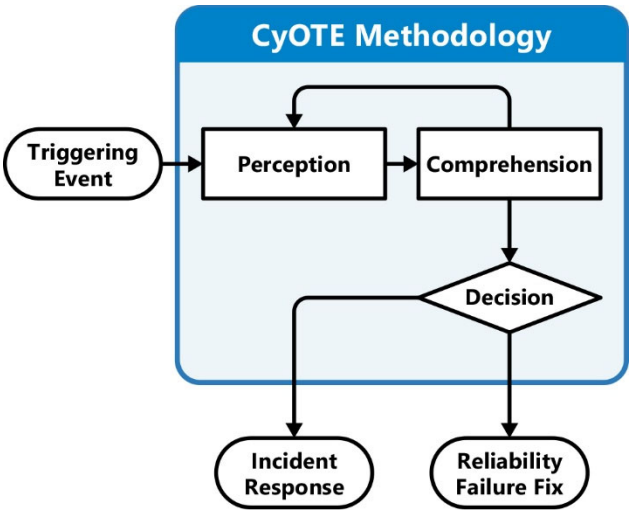


Figure 1. CyOTE Methodology

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

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

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

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

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

2.2. BACKGROUND ON THE ATTACK

This precursor analysis report attempts to reproduce an attack sequence against a notional U.S.-based oil and gas firm from available evidence and adversarial behavior exhibited during the Night Dragon campaign.

Night Dragon was a series of coordinated cyber attacks against global oil, energy, and petrochemical companies that occurred between 2007 and 2011. The campaign targeted at least five multinational firms with some reports suggesting that it impacted an additional seven.[1,2] Adversaries targeted files about operational oil and gas field production systems and financial documents related to field exploration and bidding, and exfiltrated the data from compromised hosts or via extranet servers. Adversaries also copied files to, and downloaded them from, company web servers and in certain cases also collected data from supervisory control and data acquisition (SCADA) systems.[3] While the damage caused by the Night Dragon attacks is difficult to estimate because it occurred over several years, the stolen proprietary information was worth millions of dollars and likely caused losses beyond regulatory penalties and lost revenue, potentially totaling hundreds of millions of dollars.[4]

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

The Night Dragon attacks began with Structured Query Language (SQL) injection exploits against corporate, Internet-facing web servers roughly three years before the triggering event (Y-3).[5] The compromised web servers were used to stage attacks on internal targets while adversaries harvested account credentials to enable further infiltration to internal desktops and servers.[6,7]

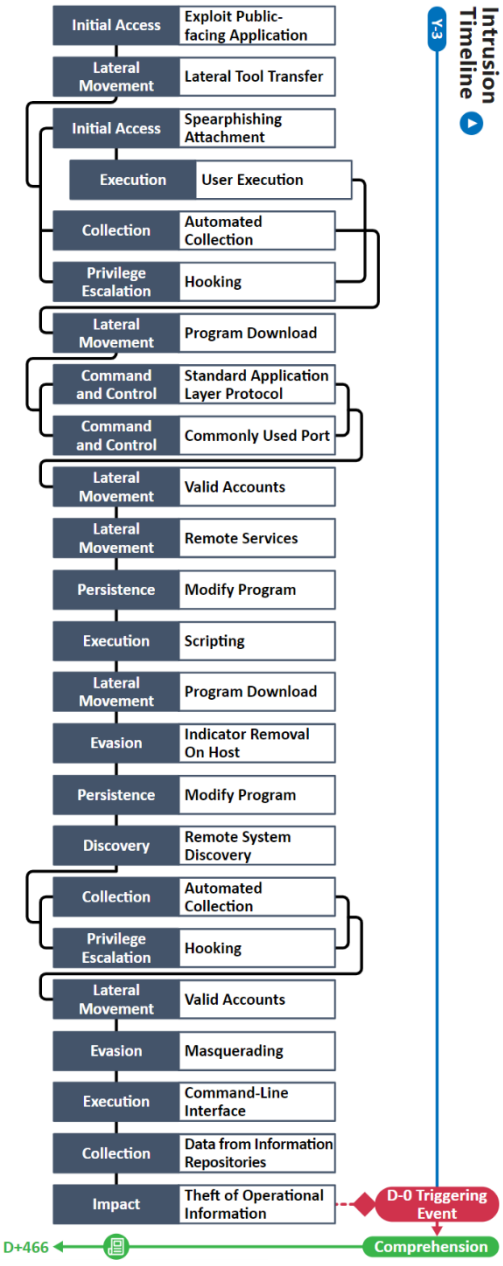


Figure 2. Intrusion Timeline

Adversaries gained additional internal access through spearphishing attacks on remote VPN-connected workers, then established command and control (C2) servers and remote access trojans (RAT) as they moved laterally throughout the network.[8]

Although the attack did not result in sabotage, the adversaries were able to extract email archives from executive accounts and operational information, including industrial control systems (ICS) data.[9] This theft of operational information was the triggering event (D-0) and, for the purposes of this case study, is assessed to have occurred on 1 November 2009.

The intended use of the stolen data is unknown and could have been for a variety of purposes. While adversaries did not cause physical impact to the ICS of the target companies, they could use the exfiltrated operational control system data in a later, more targeted attack. Full comprehension of the attack is assessed to have occurred on 10 February 2011 (D+466), when commercial researchers published a report on the attack.[10]

Analysis identified 19 unique techniques (used in a sequence of 24 steps) in a sequence and timeframe likely used by adversaries during this cyber attack (Table 1. Techniques Used in the Night Dragon Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Night Dragon Campaign

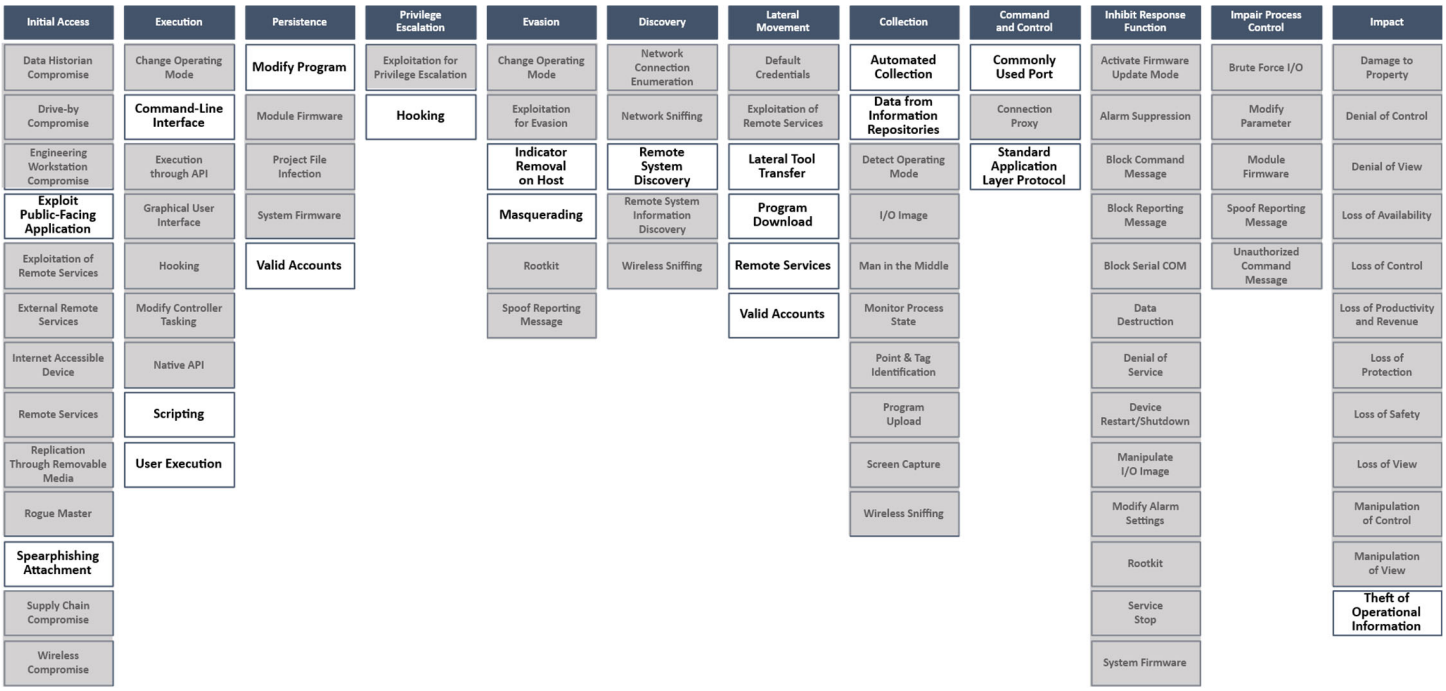


Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	24
Technique Observables	182
Precursor Techniques	23
Precursor Technique Observables	170
Highly Perceivable Precursor Technique Observables	105

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. EXPLOIT PUBLIC-FACING APPLICATION TECHNIQUE (T0819) FOR INITIAL ACCESS

Starting in 2007, adversaries gained initial access to company web servers by compromising perimeter security controls through SQL injection exploits.[11] This initial step of the attack targeted the company's public-facing web sites where adversaries attempted to force backend databases to reply to commands that should be blocked.[12] SQL injection attacks can return sensitive information, allow for remote command execution, and set the stage for subsequent attack techniques. In the case of Night Dragon, the adversaries' goal was to obtain a persistent backdoor into the victim organization's systems, leading to long-term compromise that would go unnoticed for an extended period. To achieve this, adversaries crafted Hypertext Transfer Protocol (HTTP) GET requests to inject commands into SQL servers to gain system-level access.[13] Once adversaries compromised web servers, they used them to stage attacks on internal targets.[14]

IT Staff and IT Cybersecurity personnel may have been able to observe network traffic associated with this technique which could contain malformed or anomalous HTTP and SQL objects.

A total of eight observables were identified with the use of the Exploit Public-Facing Application technique (T0819). This technique is important for investigation because it produces anomalous network traffic when compared to a system baseline. Additionally, it generates server log entries and database errors that IT Staff and IT Cybersecurity personnel can monitor. This technique appears first in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent adversaries from staging subsequent attacks on internal targets, limiting the possibility of lateral movement within the system.

All eight observables are assessed to be highly perceivable. They are italicized and marked † in **Error! Reference source not found.Error! Reference source not found.** Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 55 artifacts could be generated by the Exploit Public-Facing Application technique
Technique Observers[a]	IT Staff, IT Cybersecurity

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

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

Once adversaries compromised web servers via SQL injection, they used the Lateral Tool Transfer technique to place various commonly available malware and hacking tools on the servers. These tools were used to pivot into the company's intranet and gave adversaries access to sensitive desktops and internal servers. The malware included hacking tools widely available online such as ASPXSpy, WebShell, and reduh. WebShell and ASPXSpy are backdoor payloads that allow adversaries to bypass firewall rules and subsequently use reduh to tunnel TCP traffic through compromised web servers. Adversaries used these tools to harvest local and Active Directory (AD) account credentials, access network computers, and plant additional RATs that connect with remote C2 addresses,[15] as discussed in later sections.

IT Staff and IT Cybersecurity personnel may have been able to observe files on web servers that the tools above may have left behind or utilized for running. They also may have been able to observe host system log entries containing evidence of tool transfers.

A total of three observables were identified with the use of the Lateral Tool Transfer technique (T0867). This technique is important for investigation because it presents noticeable effects, such as generation of host system event logs. This technique appears early in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent adversaries from staging tools on web servers to access additional, more sensitive systems.

Of the three observables associated with this technique, two are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found. Error! Reference source not found.Error! Reference source not found.**Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 22 artifacts could be generated by the Lateral Tool Transfer technique
Technique Observers	IT Staff, IT Cybersecurity

3.3. AUTOMATED COLLECTION TECHNIQUE (T0802) FOR COLLECTION

Once the adversaries transferred the necessary tools and had complete control of the targeted internal system, they used password collecting and pass-the-hash tools to obtain further authenticated access to sensitive internal servers. Adversaries dumped account hashes with gsecdump and used the password recovery tool Cain & Abel to crack the hashes. They also used WinlogonHack to intercept Windows logon requests and hijack usernames and passwords.[16] As the adversaries targeted ever more sensitive infrastructures, they continued to install RATs and malware as they went.[17]

IT Staff and IT Cybersecurity personnel may have been able to observe various event IDs (EID) using System Monitor (Sysmon) or within Windows security logs related to gsecdump. Additionally, resource utilization would have increased.

A total of 18 observables were identified with the use of the Automated Collection technique (T0802). This technique is important for investigation because it presents noticeable effects, such as generation of system event logs and increased resource utilization. This technique appears early in the timeline and responding to it will effectively halt adversary access to more sensitive systems. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the 18 observables associated with this technique, 11 are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found. Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.**Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 23 artifacts could be generated by the Automated Collection technique
Technique Observers	IT Staff, IT Cybersecurity

3.4. HOOKING TECHNIQUE (T0874) FOR PRIVILEGE ESCALATION

At the same time adversaries used Automated Collection Technique (T0802) for Collection tools, they utilized Hookmsgina for additional password and username collection.[18] This tool hooks the legitimate Microsoft Graphical Identification and Authentication DLL (msgina.dll) and dumps the username, domain, password, and old password (in the event of a password change logout) to a text file on the victim host.[19]

IT Staff and IT Cybersecurity personnel may have been able to observe the Hookmsgina DLL running on compromised systems.

Four observables were identified with the use of the Hooking technique (T0874). This technique is important for investigation because it generates an anomalous DLL. This technique appears early in the timeline and responding to it will limit the adversaries' collection of account credentials. Terminating the chain of techniques at this point would limit authenticated account access and privilege escalation.

Of the four observables associated with this technique, one is assessed to be highly perceivable. It is italicized and marked † in**Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

3.5. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS

In parallel with the compromise of web servers, adversaries used spearphishing email attacks as an additional initial access vector. The spearphishing emails targeted remote, virtual private network (VPN)-connected workers to gain additional internal access.[20] The emails contained a link to an infected web server that, when clicked, compromised the corporate VPN account to obtain access to the company intranet.[21,22]

Support Staff and Management may have been able to recognize the malicious emails if they vetted them thoroughly through either autonomous or manual means. Spearphishing emails present an early perception opportunity for organizations as there are several cognitive processes that end-users can learn to determine if an email is suspicious, even without interacting with it.

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

All four observables are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 29 artifacts could be generated by the Spearphishing Attachment technique
Technique Observers	Support Staff, Management

3.6. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

After a user receives a spearphishing email, they must interact with the malicious link it contains. The user clicks the malicious link, accessing the compromised website and enabling the compromise of the host as discussed in the Program Download Technique (T0843) for Lateral Movement section.[23]

Support Staff and Management personnel may have been able to recognize their interaction with the malicious link by observing redirection to an anomalous website. IT Staff and IT Cybersecurity personnel may have been able to observe the network traffic associated with the malicious links that directed users to anomalous websites.

A total of four observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation because it presents noticeable effects, such as network traffic to anomalous websites. This technique appears early in the timeline and responding to it will effectively halt adversarial lateral movement. Terminating the chain of techniques at this point would limit access to internal systems.

All four observables are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found. Error! Reference source not found.Error! Reference source not found.** Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 23 artifacts could be generated by the User Execution technique
Technique Observers	Support Staff, Management, IT Staff, IT Cybersecurity

3.7. PROGRAM DOWNLOAD TECHNIQUE (T0843) FOR LATERAL MOVEMENT

The victim user unknowingly downloaded the zwShell RAT after clicking the malicious link in the spearphishing email and accessing the compromised website.[b] The RAT then sends account and host configuration information to a C2 server,[24] eventually giving adversaries the ability to control the compromised host remotely.

IT Staff and IT Cybersecurity personnel may have been able to observe downloads of unauthorized DLLs or executables as well as anomalous HTTP(S) traffic.

A total of six observables were identified with the use of the Program Download technique (T0843). This technique is important for investigation because it presents noticeable effects, such as generation of anomalous network traffic and Event Viewer log entries. This technique appears early in the timeline and responding to it will effectively halt the adversaries' ability to move laterally within the system. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the six observables associated with this technique, four are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

[b] Information regarding zwShell functionality begins in the Remote Services Technique (T0886) for Lateral Movement section.

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

Adversaries used standard application layer protocols such as HTTP and Simple Mail Transfer Protocol (SMTP) for C2 communications. The zwShell backdoor uses a unique host beacon and server response protocol. Each communication packet between the compromised host and C2 server is signed with a plain text signature of “hW$.” at the byte offset 0x42 within the TCP packet. The backdoor beacons approximately every five seconds. Once the server acknowledges the connection by sending a synchronize-acknowledgement (SYN-ACK) message, the backdoor sends the password to the server in clear text. The backdoor sends “keep-alive” (ACK) messages to the C2 server while the backdoor and server have an active connection. The adversaries used a dynamic Domain Name System (DNS) Internet name services account to relay C2 communications or temporarily associate DNS addresses with remote servers. The primary domains adversaries used for C2 traffic included is-a-chef.com, thruhere.net, officeon-the.net, and selfip.com.[25]

IT Staff and IT Cybersecurity may have been able to observe anomalous network connections over HTTP and SMTP as well as DNS requests to anomalous URLs.

A total of nine observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation because it presents noticeable anomalous network traffic. This technique appears early in the timeline and responding to it will effectively halt C2 capability. Terminating the chain of techniques at this point would terminate the adversaries’ ability to exfiltrate sensitive information.

Of the nine observables associated with this technique, eight are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

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

At the same time adversaries used the Standard Application Layer Protocol technique (T0869), the C2 infrastructure communicated over common ports. Although the backdoor primarily communicates over TCP port 80 (HTTP) and 25 (SMTP), the adversary can configure it to communicate over any determined TCP port.[26]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network connections over commonly used ports.

A total of two observables were identified with the use of the Commonly Used Port technique (T0885). This technique is important for investigation because it generates anomalous network traffic. This technique appears early in the timeline and responding to it will effectively halt C2 capability. Terminating the chain of techniques at this point would terminate the adversaries' ability to exfiltrate sensitive information.

Both observables are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

3.10. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

After adversaries collected usernames and passwords using the Automated Collection (T0802) and Hooking (T0874) techniques, they used these credentials to compromise valid local administrator and AD administrator accounts to move laterally in the victim's system.[27] Additionally, adversaries used the valid corporate VPN accounts of remote worker laptops they gained access to via the Spearphishing Attachment (T0865), User Execution (T0863), and Program Download (T0843) techniques to move laterally to the victim company's intranet.[28] Adversaries used common host administration techniques by primarily leveraging standard administrative credentials.[29]

IT Staff and IT Cybersecurity personnel may have been able to observe the use of administrative accounts on the domain controller by monitoring authentication logs and activity timestamps.

A total of six observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it presents noticeable effects, such as authentication log entries and potentially anomalous time and location logins. This technique appears early in the timeline and responding to it will limit lateral movement. Terminating the chain of techniques at this point would limit the adversaries' access to sensitive information.

Of the six observables associated with this technique, five are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

3.11. REMOTE SERVICES TECHNIQUE (T0886) FOR LATERAL MOVEMENT

Adversaries leveraged compromised valid accounts to deploy the zwShell RAT on dozens of machines within the victim company, and zwShell was the primary C2 application that controlled the infected machines. Adversaries used this RAT to generate unique Trojan variants and initiate beacon connections via a custom protocol.[30] The Trojan dropper, a delivery mechanism for malware, was a packaged executable customized to the victim that included the DLL file and configuration settings for installing the backdoor on the remote system.[31] The dropper can be run from any directory and was copied over network shares to the compromised computer. The adversary then executed it with PsExec or via Remote Desktop Protocol (RDP). In some cases, they used an "AT.job" or "SchTasks" entry to execute the dropper over the network on a remote machine.[32] Thus, related Windows Security Event logs would provide useful information concerning compromised AD accounts.[33]

IT Staff and IT Cybersecurity personnel may have been able to observe Windows Security Event logs containing useful information concerning compromised AD accounts and PsExec and RDP sessions. Personnel can review the logs with Windows Event Log Manager.

A total of 25 observables were identified with the use of the Remote Services technique (T0886). This technique is important for investigation because it presents noticeable effects, such as valuable forensic information generated in system event logs. This technique appears toward the middle of the timeline and responding to it will limit the adversaries' ability to remotely access and control victim machines. Terminating the chain of techniques at this point would limit the exfiltration of sensitive data directly from infected machines.

Of the 25 observables associated with this technique, 15 are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

3.12. MODIFY PROGRAM TECHNIQUE (T0889) FOR PERSISTENCE

After adversaries execute the customized dropper via the Remote Services technique (T0886), the dropper creates a temporary file that is reflected in Windows update logs. This is because the dropper modifies the Windows Registry by creating a "netsvcs" key under HKLM\system\<controlset>\services\. Accordingly, the kilobyte (KB) log files contain the date of the backdoor installation. The backdoor DLL itself also identifies this temporary file, the name of which usually consists of some alphanumeric combination that includes "gzg" (i.e., xgt0gzg).[34] When the dropper runs, it drops two DLLs, Startup.dll and Connect.dll. The Trojan installer creates a service named "Crypthost" to run the dropped component Startup.dll as a service. When Startup.dll runs, it loads and runs an export from the component Connect.dll named "PluginExecute."[35] The RAT then launches as a persistent Windows service and immediately sends a beacon on the configured port to the designated C2 server and waits for instructions.[36]

IT Staff and IT Cybersecurity personnel may have been able to observe the Windows Registry data modification and anomalous persistent Windows services running.

A total of 10 observables were identified with the use of the Modify Program technique (T0889). This technique is important for investigation because it presents noticeable effects, such as entries in the Windows update logs. This technique appears toward the middle of the timeline and responding to it will effectively halt adversaries from gaining full control of remote machines. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the 10 observables associated with this technique, six are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

3.13. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

As described in the Modify Program technique (T0889), the backdoor payload, running as CryptHost, attempted to connect to a remote server on the configured TCP port, generally port 25 or 80. It then loaded and ran the export PluginExecute from the Connect.dll component. The export supports numerous commands that the server may return, including:[37]

CMD_SET_REM
CMD_File_FIND
CMD_File_Managers
CMD_RESET_HOST
CMD_Screen_Managers
CMD_CLOSE_HOST
CMD_UNINSTALL_HOST
SHELL_CMD
CMD_REGEDIT
SERVICE_ENUM
PROCESS_ENUM
PLUGIN_INSTALL
CMD_VIDEO
CMD_KEYBOARD.

The server initiated these commands by starting associated plugin DLLs described in the Program Download technique (T0843) section.

IT Staff and IT Cybersecurity personnel may have been able to observe an anomalous export running on the host.

A total of four observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because it generates an anomalous export running on the host. This technique appears in the middle of the timeline and responding to it will effectively halt adversaries from gaining full control of remote machines. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the four observables associated with this technique, none are assessed to be highly perceivable. They are listed in**Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

3.14. PROGRAM DOWNLOAD TECHNIQUE (T0843) FOR LATERAL MOVEMENT

Connect.dll created the temporary file HostID.DAT, sent it to the C2 server, then downloaded and configured associated plugin DLLs including PluginFile.dll, PluginScreen.dll, PluginCmd.dll, PluginKeyboard.dll, PluginProcess.dll, PluginService.dll, and PluginRegedit.dll. Startup.dll then operated the service under a Windows Registry key. The DLL identifies the service key as HKLM\Software\RAT. This DLL is usually located in the %System%\System32 directory. The Windows Registry ServiceDLL key indicates the path to the backdoor DLL.[38]

IT Staff and IT Cybersecurity personnel may have been able to observe the temporary file creation or configuration of anomalous plugin DLLs.

A total of 18 observables were identified with the use of the Program Download technique (T0843). This technique is important for investigation because it presents noticeable effects, such as file creation and DLL downloads. This technique appears in the middle of the timeline and responding to it will effectively prevent adversaries from gaining full control of remote machines. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the 18 observables associated with this technique, one is assessed to be highly perceivable. It is italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

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

The Program Download technique (T0843) completed the creation of the backdoor service on the victim host. The Trojan dropper then automatically deleted itself and the temporary file was deleted when the system rebooted. The Windows Update logs contained an entry in the C:\Windows directory with the date, time, path, and name of the temporary file.[39] If a backdoor has already been configured on the system, the dropper installation fails.[40]

IT Staff and IT Cybersecurity personnel may have been able to observe the entry of the temporary file in the Windows Update logs.

Two observables were identified with the use of the Indicator Removal on Host technique (T0872). This technique is important for investigation because it presents noticeable effects, such as generation of update logs. This technique appears in the middle of the timeline and responding to it will alert personnel to the existence of a remote compromise. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Both observables are assessed to be highly perceivable. They are italicized and marked † in **Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.**Appendix A.

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

3.16. MODIFY PROGRAM TECHNIQUE (T0889) FOR PERSISTENCE

Adversaries had been using the victim company's compromised web servers as C2 servers. At this point in the timeline, they disabled Microsoft Internet Explorer proxy settings via the Registry Editor which allowed direct communication from infected machines to the Internet.[41]

IT Staff and IT Cybersecurity may have been able to observe this Registry modification.

A total of two observables were identified with the use of the Modify Program technique (T0889). This technique is important for investigation because it presents noticeable effects, such as changes to the Windows Registry. This technique appears in the final third of the timeline and responding to it will effectively halt C2 capability. Terminating the chain of techniques at this point would terminate the adversaries' ability to exfiltrate sensitive information.

Both observables are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

3.17. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

At this point, adversaries have established C2 connectivity. When an adversary launches zwShell, it presents a fake crash error dialogue box to them that contains a hidden text entry field. The adversary enters the special password and launches the tool. Adversaries likely used this obfuscation method to confuse investigators about the true purpose of the zwShell executable. Once the adversary bypasses the error and launches zwShell, it allows them to create a custom Trojan by selecting the Server menu or to launch the C2 server by clicking Start and entering the port to listen for traffic with the password used by backdoor DLLs. Once launched, zwShell begins to listen for incoming compromised client connections and displays them to the adversary. Adversaries can launch as many instances of the zwShell application as desired, as long as each listen on a different port, or for traffic with different passwords used by the backdoor DLLs.[42] Adversaries can now monitor multiple networks of compromised computers.

As was the case in the Standard Application Layer Protocol Technique (T0869) for Command and Control, IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network connections over HTTP and SMTP as well as DNS requests to anomalous URLs.

A total of nine observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation because it presents noticeable anomalous network traffic. This technique appears in the last third of the timeline and responding to it will effectively halt the adversaries' ability to discover and remotely connect to compromised machines. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the nine observables associated with this technique, eight are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

3.18. AUTOMATED COLLECTION TECHNIQUE (T0802) FOR COLLECTION

As described near the beginning of the timeline, adversaries used the Automated Collection technique (T0802) to collect credentials primarily focused on web servers and AD. At this point in the timeline, adversaries used the same technique and tools such as gsecdump, Cain & Abel, and WinlogonHack to gain additional access to sensitive internal desktops as they made their way across the network.[43]

As was the case in the first instance of this technique, IT Staff and IT Cybersecurity personnel may have been able to observe various EIDs using System Monitor (Sysmon) or within Windows security logs related to gsecdump. Resource utilization also would have increased.

A total of 18 observables were identified with the use of the Automated Collection technique (T0802). This technique is important for investigation because it presents noticeable effects, such as generation of system event logs and increased resource utilization. This technique appears late in the timeline and responding to it will limit adversaries' access to sensitive internal desktops. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the 18 observables associated with this technique, 11 are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 23 artifacts could be generated by the Automated Collection technique
Technique Observers	IT Staff, Cybersecurity

3.19. HOOKING TECHNIQUE (T0874) FOR PRIVILIGE ESCALATION

As described near the beginning of the timeline, adversaries used the Hooking technique (T0874) at the same time as the Automated Collection technique (T0802) for additional AD and server password and username collection. At this point in the timeline, adversaries again used the Hookmsgina tool, but this time to collect additional internal desktop credentials.[44]

As was the case in the first instance of this technique, IT Staff and IT Cybersecurity personnel may have been able to observe the existence of the Hookmsgina DLL running on compromised hosts.

A total of four observables were identified with the use of the Hooking technique (T0874). This technique is important for investigation because it generates an anomalous DLL. This technique appears late in the timeline and responding to it will limit adversaries' access to sensitive internal desktops. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the four observables associated with this technique, one is assessed to be highly perceivable. It is italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

3.20. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

Adversaries once again used the Valid Accounts technique (T0859) at this point in the timeline, leveraging the internal desktop usernames and passwords they collected via the Automated Collection (T0802) and Hooking (T0874) techniques. In this step, however, adversaries used the credentials they collected for persistence rather than lateral movement.[45]

As with the first instance of this technique, IT Staff and IT Cybersecurity personnel may have been able to observe the use of administrative accounts on the domain controller by monitoring authentication logs and activity timestamps.

A total of six observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it presents noticeable effects, such as authentication log entries and potentially anomalous time and location logins. This technique appears late in the timeline and responding to it will limit the adversaries' persistence in the network. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the six observables associated with this technique, five are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

3.21. MASQUERADING TECHNIQUE (T0849) FOR EVASION

When a victim device is fully compromised, it connects to the adversaries' zwShell interface. The adversaries' graphical user interface shows the client's IP address, PC name, name of the logged-in user, and information about the machine's operating system, including the major patch levels. The adversaries copy CMD.EXE to the compromised host in the C:\Windows\Temp directory with the filename svchost.exe. This copy is an unmodified version of the Microsoft Windows command shell executable.[46]

IT Staff and IT Cybersecurity personnel may have been able to observe the anomalous file in the Windows\Temp folder.

A total of two observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation because it presents noticeable effects, such as changes to Windows directories. This technique appears late in the timeline and responding to it will limit the adversaries' access to sensitive information. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Both observables are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

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

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

Once adversaries copy CMD.EXE to the compromised host, they can then launch a remote command-line shell to execute commands directly on the victim's machine. The Registry can also be viewed and edited in a user interface similar to the Windows Registry editor.[47]

IT Staff and IT Cybersecurity personnel may have been able to observe changes to the C:\Windows\Temp directory.

A total of three observables were identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation because it presents noticeable effects, such as additions to the Windows directory. This technique appears near the end of the timeline and responding to it will limit the adversaries' ability to interact with remote machines. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the three observables associated with this technique, two are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 25 artifacts could be generated by the Command-Line Interface technique
Technique Observers	IT Staff, IT Cybersecurity

3.23. DATA FROM INFORMATION REPOSITORIES TECHNIQUE (T0811) FOR COLLECTION

Once adversaries had full access to a compromised host via the zwShell RAT, they proceeded to connect to various machines and exfiltrated email archives and other sensitive documents. Browsing the client file system was a fully interactive process. Adversaries could delete, rename, copy, download, and upload individual files and folders to the remote machine.[48] They targeted systems belonging to executives for the emails and files they exfiltrated.[49]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous commands embedded in network traffic, because zwShell sends all traffic unencrypted. They may also have been able to observe zwShell accessing local files.

A total of three observables were identified with the use of the Data from Information Repositories technique (T0811). This technique is important for investigation because it presents noticeable effects, such as anomalous network traffic. This technique appears near the end of the timeline and responding to it will effectively halt the adversaries' ability to exfiltrate information. Terminating the chain of techniques at this point would limit extraction of proprietary information.

Of the three observables associated with this technique, one is assessed to be highly perceivable. It is italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 35 artifacts could be generated by the Data from Information Repositories technique
Technique Observers	IT Staff, IT Cybersecurity

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

Adversaries exfiltrated files primarily via HTTP over port 80 and SMTP over port 25 from compromised hosts or via extranet servers. The files focused on operational oil and gas field production systems and financial documents related to field exploration and bidding. In some cases, they copied and downloaded files from company web servers. In other cases, adversaries collected data from SCADA systems.[50] Specific types of information adversaries targeted included market intelligence reports, computerized topographical maps that showed locations of potential oil reserves, and architectural plans for oil and gas pipelines.[51,52,53]

Though not publicly calculated, some sources claim that the damage from these attacks may have potentially been in the hundreds of millions of dollars as sensitive data theft can be highly damaging beyond regulatory penalties and lost revenue.[54,55] The Night Dragon campaign did not result in impacts related to loss of availability or physical damage to processes.

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe the exfiltration of data to the adversaries' C2 network.

A total of 12 observables were identified with the use of the Theft of Operational Information technique (T0882). This technique is important for investigation because it represents the triggering event in this case study. It is the stage at which victim information is exfiltrated that adversaries could use for either industrial espionage or a later, more targeted attack. This technique appears at the end of the timeline, beyond the point at which a defender could take action to disrupt the attack. Terminating the chain of techniques at this point would safeguard sensitive data.

All 12 observables are assessed to be highly perceivable. They are italicized and marked † in**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.** Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of four artifacts could be generated by the Theft of Operational Information technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity

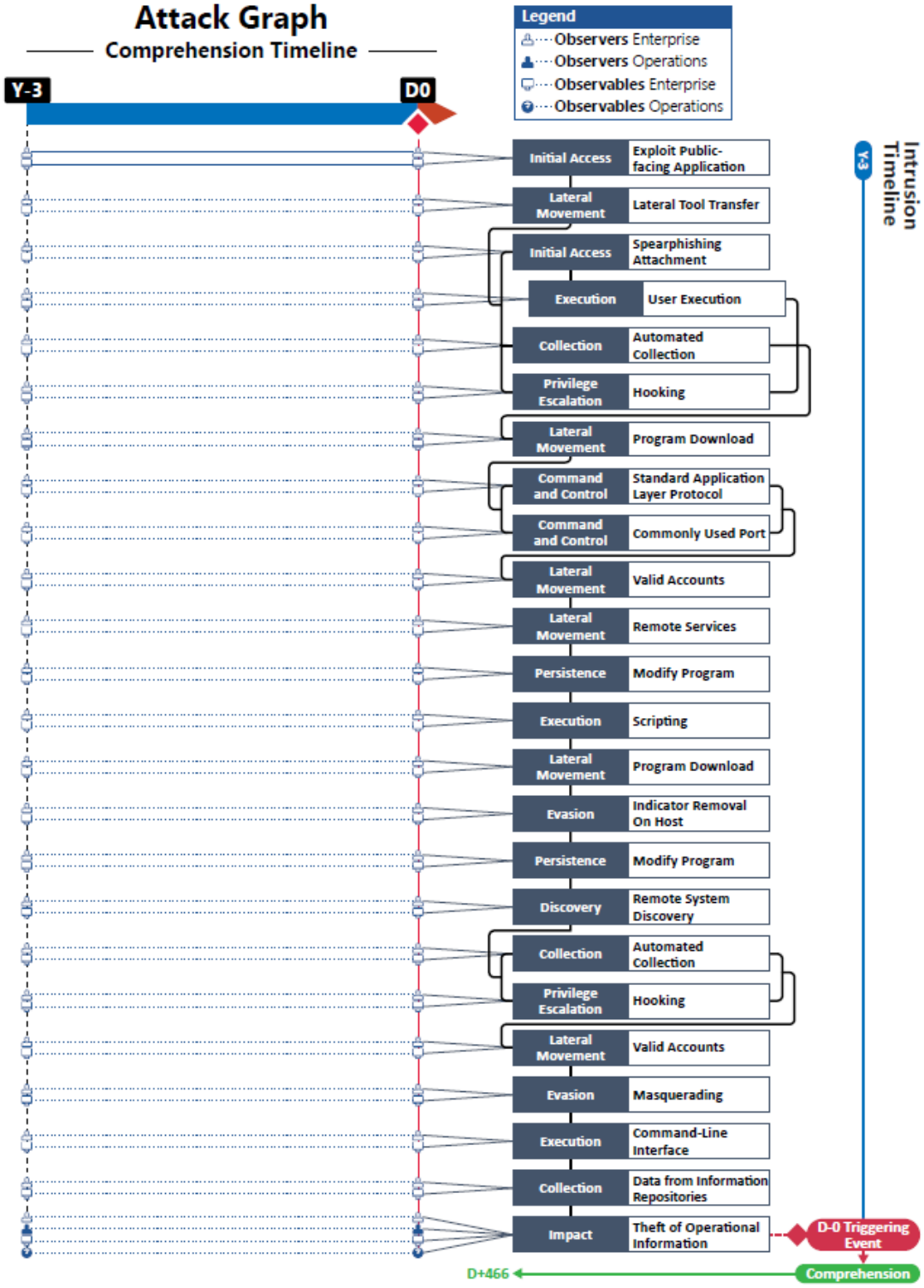


Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Observables Associated with Exploit Public-Facing Application Technique (T0819)	
Observable 1 †	*Malformed SQL Queries*
Observable 2 †	*Anomalous SQL Fragments*
Observable 3 †	*Log Files (Associated with SQL Server or Webapp)*
Observable 4 †	*Malformed HTTP Headers*
Observable 5 †	*Unusually High Number of HTTP GET Requests*
Observable 6 †	*Anomalous HTTP Requests*
Observable 7 †	*Increase in Anomalous Traffic*
Observable 8 †	*Increase in Host Resource Utilization*

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 1 †	*ASPXSpy1.0.aspx WebShell Running on Web Server*
Observable 2	Reduh: PHP, ASP, JSP, or JS File on Web Server
Observable 3 †	*Host System Log Entries*

Observables Associated with Automated Collection Technique (T0802)	
Observable 1 †	*Gsecdump.exe on Host (gsecdump Must Exist on Disk at Specified Location)*
Observable 2	Sysmon EID 1 (Process Creation) Associated with gsecdump
Observable 3	Sysmon EID 5 (Process Terminated) Associated with gsecdump
Observable 4	Sysmon EID 10 (Process Accessed) Associated with gsecdump
Observable 5	Sysmon EID 11 (File Created) Associated with gsecdump
Observable 6 †	*Windows Security Log EID 4656 (Handle to Object Was Requested) Associated with gsecdump*
Observable 7 †	*Windows Security Log EID 4658 (Handle to Object Closed) Associated with gsecdump*
Observable 8 †	*Windows Security Log EID 4663 (Attempt Made to Access Object) Associated with gsecdump*
Observable 9 †	*Windows Security Log EID 4688 (Process Create) Associated with gsecdump*
Observable 10 †	*Windows Security Log EID 4689 (Process Exited) Associated with gsecdump*
Observable 11	Command-Line Arguments Using gsecdump (#{gsecdump_exe})
Observable 12 †	*Cain & Abel: Increased Resource Utilization Shown in System Resource Utilization Monitor*
Observable 13	Cain & Abel: Access of SAM File by Anomalous Process

Observables Associated with Automated Collection Technique (T0802)	
Observable 14	Cain & Abel Application Running as a Process
Observable 15 †	*WinlogonHack: Existence of Install.bat*
Observable 16 †	*WinlogonHack: Existence of Readlog.bat*
Observable 17 †	*WinlogonHack: Existence of Uninstall.bat*
Observable 18 †	*WinlogonHack: Existence of %systemroot%\system32\wminotify.dll*

Observables Associated with Hooking Technique (T0874)	
Observable 1 †	*Existence of Hookmsgina.dll*
Observable 2	Execution of Hookmsgina.dll
Observable 3	Collection of User Credentials from Internal Host
Observable 4	Creation of .txt File with Credential Information

Observables Associated with Spearphishing Attachment Technique (T0865)	
Observable 1 †	*Emails Designed to Trick End Users into Clicking on a Malicious Link*
Observable 2 †	*DNS Requests for Anomalous Websites Over Port 53*
Observable 3 †	*HTTP Traffic to Anomalous Websites Over Port 80*
Observable 4 †	*HTTPS Traffic to Anomalous Websites Over Port 443*

Observables Associated with User Execution Technique (T0863)	
Observable 1 †	*User Interaction with Malicious Link*
Observable 2 †	*DNS Requests for Anomalous Websites Over Port 53*
Observable 3 †	*HTTP Traffic to Anomalous Websites Over Port 80*
Observable 4 †	*HTTPS Traffic to Anomalous Websites Over Port 443*

Observables Associated with Program Download Technique (T0843)	
Observable 1	zwShell Downloaded
Observable 2	Anomalous DLLs/EXEs Downloaded
Observable 3 †	*Anomalous HTTP Traffic Over Port 80*
Observable 4 †	*Anomalous HTTPS Traffic Over Port 443*
Observable 5 †	*Windows Event ID 4688 (A New Process Has Been Created)*
Observable 6 †	*Windows Event ID 4689 (A Process Has Exited)*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1 †	*Anomalous HTTP Connection from Internal Host to External IP Over Port 80*
Observable 2 †	*Anomalous SMTP Connections from Internal Host to External IP Over Port 25*
Observable 3	HTTP Packets Signed with Plain Text Signature of "Hw$."
Observable 4 †	*5-second Interval Beacons*
Observable 5 †	*Periodic TCP Keep-Alive (ACK) Packets*
Observable 6 †	*DNS Requests to is-a-chef.com Over UDP Port 53*
Observable 7 †	*DNS Requests to thruhere.net Over UDP Port 53*
Observable 8 †	*DNS Requests to office-on-the.net Over UDP Port 53*
Observable 9 †	*DNS Requests to selfip.com Over UDP Port 53*

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 1 †	*Anomalous Outbound Network Connections Over TCP Port 80 (HTTP)*
Observable 2 †	*Anomalous Connections Over TCP Port 25 (SMTP)*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Usage of Administrative Accounts on Domain Controller
Observable 2 †	*Admin Authentication Log on Domain Controller (Event ID 4648 (Explicit Credentials Were Used)*
Observable 3 †	*Domain Controller Activity Timestamp*
Observable 4 †	*VPN Authentication Log*
Observable 5 †	*VPN Activity Timestamp*
Observable 6 †	*Anomalous Logins (Time and Location)*

Observables Associated with Remote Services Technique (T0886)	
Observable 1	zwShell.exe 093640a69c8eafbc60343bf9cd1d3ad3
Observable 2	zwShell.exe 85df6b3e2c1a4c6ce20fc8080e0b53e9
Observable 3	Shell.exe 093640a69c8eafbc60343bf9cd1d3ad3
Observable 4	PsExec: Sysmon EID 1 (Process Creation)
Observable 5	PsExec: Sysmon EID 3 (Network Connection Detected)
Observable 6	PsExec: Sysmon EID 5 (Process Terminated)
Observable 7	PsExec: Sysmon EID 10 (Process Accessed)
Observable 8	PsExec: Sysmon EID 11 (File Created)
Observable 9	PsExec: Sysmon EID 12 (Registry Object Added/Deleted)

Observables Associated with Remote Services Technique (T0886)	
Observable 10	PsExec: Sysmon EID 13 (Registry Value Set)
Observable 11 †	*Psexec: Windows Security Log EID 4660 (Object Deleted)*
Observable 12 †	*Psexec: Windows Security Log EID 4656/4663 (Handle to an Object Was Requested)*
Observable 13 †	*Psexec: Windows Security Log EID 4674 (Sensitive Privilege Use)*
Observable 14 †	*Psexec: Windows Security Log EID 4688 (Process Creation)*
Observable 15 †	*Psexec: Windows Security Log EID 4689 (Process Termination)*
Observable 16 †	*Psexec: Windows Security Log EID 5140 (File Sharing)*
Observable 17 †	*Psexec: Windows Security Log EID 5145 (Detailed File Share)*
Observable 18 †	*Psexec: Windows Security Log EID 5156 (Filtering Platform Connection)*
Observable 19 †	*Psexec: Windows Security Log EID 7036 (Service Control Manager)*
Observable 20 †	*Psexec: Windows Security Log EID 7045/4697 (Service Installed on System)*
Observable 21 †	*RDP Session Traffic Over TCP Port 3389*
Observable 22 †	*Windows Security Event Logs Concerning Compromised AD Accounts*
Observable 23 †	*AT.job Entry*
Observable 24 †	*Schtasks: Event ID 4698 (A Scheduled Task Was Created)*
Observable 25 †	*Schtasks: Event ID 4699 (A Scheduled Task Was Deleted)*

Observables Associated with Modify Program Technique (T0889)	
Observable 1 †	*Dropper Creates Temporary File in KB*.log Files in C:\Windows Folder*
Observable 2 †	*Windows Registry Modified to Create a netsvcs Key Under HKLM\system\<controlset>\services*
Observable 3 †	*File Name with Alphanumeric Combination Containing "gzg"*
Observable 4	Startup.dll Created in the %System%\System32 or %System%\SysWow64 Directory
Observable 5	Startup.dll A6CBA73405C77FEDEAF4722AD7D35D60 Created in the %System%\System32 or %System%\SysWow64 Directory
Observable 6	Connect.dll Created in the %System%\System32 or %System%\SysWow64 Directory
Observable 7	Connect.dll 6E31CCA77255F9CDE228A2DB9E2A3855 Created in the %System%\System32 or %System%\SysWow64 Directory
Observable 8 †	*Windows Event ID 7045 (A New Service Was Installed in the System: CryptHost)*
Observable 9 †	*Anomalous Persistent Windows Service Running*
Observable 10 †	*Windows Event Log ID 4667 (Registry Value Was Modified)*

Observables Associated with Scripting Technique (T0853)	
Observable 1	PluginExecute Export Running
Observable 2	Increased Resource Utilization Shown in System Resource Utilization Monitor
Observable 3	Network Traffic Associated with Connect.dll Over TCP Port 25
Observable 4	Network Traffic Associated with Connect.dll Over TCP Port 80

Observables Associated with Program Download Technique (T0843)	
Observable 1 †	*Temporary File Created: HostID.DAT*
Observable 2	Network Traffic Associated with Connect.dll Over TCP Port 25
Observable 3	Network Traffic Associated with Connect.dll Over TCP Port 80
Observable 4	PluginFile.dll Downloaded
Observable 5	PluginFile.dll Configured
Observable 6	PluginScreen.dll Downloaded
Observable 7	PluginScreen.dll Configured
Observable 8	PluginCmd.dll Downloaded
Observable 9	PluginCmd.dll Configured
Observable 10	PluginKeyboard.dll Downloaded
Observable 11	PluginKeyboard.dll Configured
Observable 12	PluginProcess.dll Downloaded
Observable 13	PluginProcess.dll Configured
Observable 14	PluginService.dll Downloaded
Observable 15	PluginService.dll Configured
Observable 16	PluginRegedit.dll Downloaded
Observable 17	PluginRegedit.dll Configured
Observable 18	Execution of %System%\System32\connect.dll

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 1 †	*Entry Created in the Windows Update Logs (KB****.log)*
Observable 2 †	*Entry Created in the C:\Windows Directory with the Date, Time, Path, and Name of the Temporary File (KB****.log)*

Observables Associated with Modify Program Technique (T0889)	
Observable 1 †	*Microsoft Internet Proxy Settings Disabled*
Observable 2 †	*Windows Event Log ID 4667 (Registry Value Was Modified)*

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1 †	*Anomalous HTTP Connection from Internal Host to External IP Over Port 80*
Observable 2 †	*Anomalous SMTP Connections from Internal Host to External IP Over Port 25*
Observable 3	HTTP Packets Signed with Plain Text Signature Of “Hw$.”
Observable 4 †	*5-second Interval Beacons*
Observable 5 †	*Periodic TCP Keep-Alive (ACK) Packets*
Observable 6 †	*DNS Requests to is-a-chef.com Over UDP Port 53*
Observable 7 †	*DNS Requests to thruhere.net Over UDP Port 53*
Observable 8 †	*DNS Requests to office-on-the.net Over UDP Port 53*
Observable 9 †	*DNS Requests to selfip.com Over UDP Port 53*

Observables Associated with Automated Collection Technique (T0802)	
Observable 1 †	*Gsecdump.exe on Host (gsecdump Must Exist on Disk at Specified Location)*
Observable 2	Sysmon EID 1 (Process Creation) Associated with gsecdump
Observable 3	Sysmon EID 5 (Process Terminated) Associated with gsecdump
Observable 4	Sysmon EID 10 (Process Accessed) Associated with gsecdump
Observable 5	Sysmon EID 11 (File Created) Associated with gsecdump
Observable 6 †	*Windows Security Log EID 4656 (Handle to Object Was Requested) Associated with gsecdump*
Observable 7 †	*Windows Security Log EID 4658 (Handle to Object Closed) Associated with gsecdump*
Observable 8 †	*Windows Security Log EID 4663 (Attempt Made to Access Object) Associated with gsecdump*
Observable 9 †	*Windows Security Log EID 4688 (Process Create) Associated with gsecdump*
Observable 10 †	*Windows Security Log EID 4689 (Process Exited) Associated with gsecdump*
Observable 11	Command-Line Arguments Using gsecdump (#{gsecdump_exe})
Observable 12 †	*Cain & Abel: Increased Resource Utilization*
Observable 13	Cain & Abel: Access of SAM File by Anomalous Process
Observable 14	Cain & Abel Application Running as a Process
Observable 15 †	*WinlogonHack: Existence of Install.bat*
Observable 16 †	*WinlogonHack: Existence of Readlog.bat*
Observable 17 †	*WinlogonHack: Existence of Uninstall.bat*
Observable 18 †	*WinlogonHack: Existence of %systemroot%\system32\wminotify.dll*

Observables Associated with Hooking Technique (T0874)	
Observable 1 †	*Existence of Hookmsgina.dll*
Observable 2	Execution of Hookmsgina.dll
Observable 3	Collection of User Credentials from Internal Host
Observable 4	Creation of .txt File with Credential Information

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Usage of Administrator Accounts on Domain Controller
Observable 2 †	*Admin Authentication Log on Domain Controller (Event ID 4648 (Explicit Credentials Were Used)*
Observable 3 †	*Anomalous Logins (Time and Location)*
Observable 4 †	*Event Viewer Login Events*
Observable 5 †	*Event ID 4624 (An Account Was Successfully Logged On)*
Observable 6 †	*Event ID 4625 (An Account Failed to Log On)*

Observables Associated with Masquerading Technique (T0849)	
Observable 1 †	*CMD.EXE Copied to the C:\Windows\Temp Directory*
Observable 2 †	*CMD.EXE Renamed to svchost.exe*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 1	Windows Security Log EID 4688 (A New Process Has Been Created)
Observable 2 †	*Anomalous Command Execution*
Observable 3 †	*Windows Event Log ID 4667 (Registry Value Was Modified)*

Observables Associated with Data from Information Repositories Technique (T0811)	
Observable 1	Anomalous Commands Embedded in Network Traffic
Observable 2 †	*zwShell.exe Sending and Receiving Network Traffic*
Observable 3	RAT (zwShell) Accessing Local Files

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 1 †	*Movement of Data from Compromised Hosts to Anomalous External Server Over HTTP Port 80*
Observable 2 †	*Movement of Data from Compromised Hosts to Anomalous External Server Over SMTP Port 25*

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 3 †	*Movement of Data from Extranet Server to Anomalous External Server Over HTTP Port 80*
Observable 4 †	*Movement of Data from Extranet Server to Anomalous External Server Over SMTP Port 25*
Observable 5 †	*Movement of Data from Company Web Servers to Anomalous External Server Over HTTP Port 80*
Observable 6 †	*Movement of Data from Company Web Servers to Anomalous External Server Over SMTP Port 25*
Observable 7 †	*Movement of Data from SCADA Systems to Anomalous External Server Over HTTP Port 80*
Observable 8 †	*Movement of Data from SCADA Systems to Anomalous External Server Over SMTP Port 25*
Observable 9 †	*Movement of Market Intelligence Reports from Internal Location to External Location*
Observable 10 †	*Movement of Topographical Maps from Internal Location to External Location*
Observable 11 †	*Movement of Architectural Plans from Internal Location to External Location*
Observable 12 †	*Movement of Operational Technology Information from Internal Location to External Location*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Exploit Public-Facing Application Technique (T0819)	
Artifact 1	Logon Security Event
Artifact 2	Logon Timestamp
Artifact 3	Process Failure
Artifact 4	Process State Change
Artifact 5	Operational Data Modification
Artifact 6	Operational Data Corruption
Artifact 7	OPC COM Objects
Artifact 8	Remote Connections
Artifact 9	External Network Connections
Artifact 10	Logon Event
Artifact 11	Prefetch
Artifact 12	Logon Event
Artifact 13	Administrator Logon
Artifact 14	External Network Connections
Artifact 15	Remote Connections
Artifact 16	Ransom Note
Artifact 17	Logon Timestamp After Hours
Artifact 18	MAC Address
Artifact 19	IP Address
Artifact 20	Process Ending
Artifact 21	HTTP Traffic Port
Artifact 22	External Industrial Protocol Connections
Artifact 23	Web Server Log
Artifact 24	VNC Traffic Port
Artifact 25	SSH Traffic Port
Artifact 26	Logon Security Event
Artifact 27	Telnet Traffic
Artifact 28	Increase Number of Logon Attempts
Artifact 29	TFTP Port
Artifact 30	FTP Port
Artifact 31	Application Failure
Artifact 32	HTTPS Port

Artifacts Associated with Exploit Public-Facing Application Technique (T0819)	
Artifact 33	User Account
Artifact 34	Web Proxy Logs
Artifact 35	Application Log
Artifact 36	Process Creation
Artifact 37	Process Ending
Artifact 38	Source IP Address
Artifact 39	MAC Address
Artifact 40	Firewall Logs
Artifact 41	TLS Certificate
Artifact 42	.lnk Files
Artifact 43	FTPS Port
Artifact 44	Logon Alert for Default Password
Artifact 45	Process Creation
Artifact 46	Vendor Jump Host Logon
Artifact 47	Configuration Alert for Default Password
Artifact 48	Remote Connections
Artifact 49	RDP Traffic Port
Artifact 50	VNC Traffic Port
Artifact 51	SSH Traffic Port
Artifact 52	Telnet Traffic
Artifact 53	HTTP Traffic
Artifact 54	Application Log
Artifact 55	RDP Traffic Port

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 Automated Collection Technique (T0802)	
Artifact 1	POWERSHELL Command Arguments
Artifact 2	External Network Connections
Artifact 3	SQL Read Requests
Artifact 4	User Account Creation
Artifact 5	Operational Data Exfiltration
Artifact 6	MAC Addresses
Artifact 7	IP Addresses
Artifact 8	Internal Network Connections
Artifact 9	Command Execution
Artifact 10	File Execution
Artifact 11	Local Memory Read Requests
Artifact 12	Command-Line Arguments
Artifact 13	Network Read Request
Artifact 14	Native Tool Use
Artifact 15	Service Log
Artifact 16	Application Log
Artifact 17	File Transfer

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 18	SMB Traffic Port
Artifact 19	User Account Logs
Artifact 20	User Account Privilege Change
Artifact 21	Database Read Request
Artifact 22	OPC Read Requests
Artifact 23	File Creation

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

Artifacts Associated with Spearphishing Attachment Technique (T0865)	
Artifact 1	Email .ost File
Artifact 2	Mismatch MIME and Attachment File Extension
Artifact 3	Email Sender Address
Artifact 4	Email Message
Artifact 5	Email Receiver
Artifact 6	Email Receiver Name
Artifact 7	Email Receiver Domain
Artifact 8	Email Receiver Address
Artifact 9	Enable Macros Pop-Up
Artifact 10	Email Application Log File
Artifact 11	Email Unified Audit Log File

Artifacts Associated with Spearphishing Attachment Technique (T0865)	
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 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
Artifact 11	Process Creation
Artifact 12	System Log
Artifact 13	Process Termination

Artifacts Associated with User Execution Technique (T0863)	
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 Program Download Technique (T0843)	
Artifact 1	Controller State Change
Artifact 2	Controller Connection to External Website
Artifact 3	Controller In Stop State
Artifact 4	Controller Connected to External Networks
Artifact 5	Network Traffic Creation
Artifact 6	Network Metadata
Artifact 7	External IP Address
Artifact 8	Controller Network Connections via Management Protocol
Artifact 9	Operational Process Shutdown
Artifact 10	External Domain Connection
Artifact 11	Operational Process Restart
Artifact 12	Controller Application Log Type
Artifact 13	Supervisory Workstation Program Download Popup
Artifact 14	Controller Application Log Event
Artifact 15	Device Alarm
Artifact 16	Device Alert
Artifact 17	Operational Database Data Modification
Artifact 18	Controller Application Log Timestamp
Artifact 19	Controller In Program State

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

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

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 1	Logon Session Creation
Artifact 2	User Account Creation
Artifact 3	Logon Type Entry
Artifact 4	Logon Timestamp
Artifact 5	Failed Logons Event
Artifact 6	Successful Logon Event
Artifact 7	System Logs
Artifact 8	Default Credential Use
Artifact 9	Authentication Creation
Artifact 10	Prefetch Files Created After Execution

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 11	Logons
Artifact 12	Application Log
Artifact 13	Domain Permission Requests
Artifact 14	Permission Elevation Requests
Artifact 15	Application Use Times
Artifact 16	Configuration Changes

Artifacts Associated with 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
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 Modify Program Technique (T0889)	
Artifact 1	Unexpected Program Download Observed on Network
Artifact 2	Modification to Application Responsible for Program Downloads
Artifact 3	Unexpected Modification to Program organizational Units on a Device

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 Program Download Technique (T0843)	
Artifact 1	Controller State Change
Artifact 2	Controller Connection to External Website
Artifact 3	Controller In Stop State
Artifact 4	Controller Connected to External Networks
Artifact 5	Network Traffic Creation
Artifact 6	Network Metadata
Artifact 7	External IP Address
Artifact 8	Controller Network Connections via Management Protocol
Artifact 9	Operational Process Shutdown
Artifact 10	External Domain Connection
Artifact 11	Operational Process Restart
Artifact 12	Controller Application Log Type
Artifact 13	Supervisory Workstation Program Download Popup

Artifacts Associated with Program Download Technique (T0843)	
Artifact 14	Controller Application Log Event
Artifact 15	Device Alarm
Artifact 16	Device Alert
Artifact 17	Operational Database Data Modification
Artifact 18	Controller Application Log Timestamp
Artifact 19	Controller In Program State

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

Artifacts Associated with Modify Program Technique (T0889)	
Artifact 1	Unexpected Program Download Observed on Network
Artifact 2	Modification to Application Responsible for Program Downloads
Artifact 3	Unexpected Modification to Program organizational Units on a Device

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

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 29	ICMP Type 7 Traffic
Artifact 30	SNMP Port 162 Traffic
Artifact 31	SNMP Port 161 Traffic
Artifact 32	ARP Scans
Artifact 33	Operating System Queries
Artifact 34	TCP SYN Scans
Artifact 35	Industrial Network Traffic Content About Hostnames
Artifact 36	Polling Network Traffic from Unauthorized IP Sender Addresses
Artifact 37	NETBIOS Name Services Port
Artifact 38	LDAP Port
Artifact 39	Active Directory Calls
Artifact 40	Email Server Calls
Artifact 41	DNS Lookup Queries
Artifact 42	TCP Connect Scan
Artifact 43	Command-Line Dialog Box Open

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 1	POWERSHELL Command Arguments
Artifact 2	External Network Connections
Artifact 3	SQL Read Requests
Artifact 4	User Account Creation
Artifact 5	Operational Data Exfiltration
Artifact 6	MAC Addresses
Artifact 7	IP Addresses
Artifact 8	Internal Network Connections
Artifact 9	Command Execution
Artifact 10	File Execution
Artifact 11	Local Memory Read Requests
Artifact 12	Command-Line Arguments
Artifact 13	Network Read Request
Artifact 14	Native Tool Use
Artifact 15	Service Log
Artifact 16	Application Log

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 17	File Transfer
Artifact 18	SMB Traffic Port
Artifact 19	User Account Logs
Artifact 20	User Account Privilege Change
Artifact 21	Database Read Request
Artifact 22	OPC Read Requests
Artifact 23	File Creation

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

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 1	Logon Session Creation
Artifact 2	User Account Creation
Artifact 3	Logon Type Entry
Artifact 4	Logon Timestamp
Artifact 5	Failed Logons Event
Artifact 6	Successful Logon Event
Artifact 7	System Logs
Artifact 8	Default Credential Use
Artifact 9	Authentication Creation
Artifact 10	Prefetch Files Created After Execution

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 11	Logons
Artifact 12	Application Log
Artifact 13	Domain Permission Requests
Artifact 14	Permission Elevation Requests
Artifact 15	Application Use Times
Artifact 16	Configuration Changes

Artifacts Associated with 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 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

Artifacts Associated with Command-Line Interface Technique (T0807)	
Artifact 8	Remote Connections
Artifact 9	Process Ending
Artifact 10	Script Execution
Artifact 11	User Account Logon
Artifact 12	User Account Privilege Change
Artifact 13	Logon Event
Artifact 14	Event Log Type
Artifact 15	Event Log Type
Artifact 16	Failed Logon Event
Artifact 17	Command-Line Memory Data
Artifact 18	cmd.exe Application Execution
Artifact 19	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

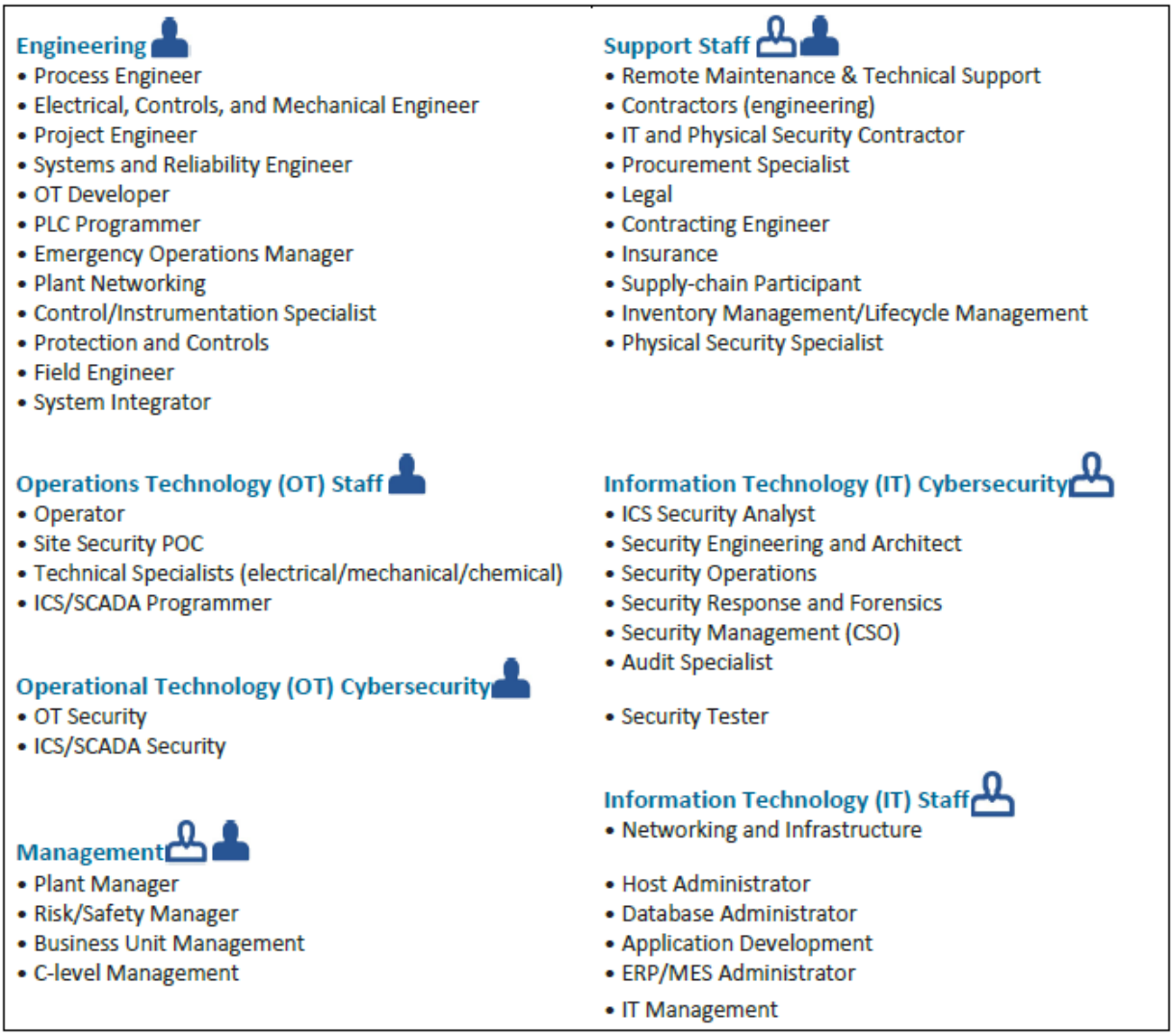
Artifacts Associated with Data from Information Repositories Technique (T0811)	
Artifact 1	SFTP Traffic Port
Artifact 2	Share Drive Access
Artifact 3	Operational Database Logons
Artifact 4	Engineering Workstation Application Log
Artifact 5	HTTP Traffic Port
Artifact 6	HTTPS Traffic Port
Artifact 7	FTPS Traffic Port
Artifact 8	File Access
Artifact 9	Telnet Traffic Port
Artifact 10	File Modification
Artifact 11	FTP Traffic Port
Artifact 12	VNC Traffic Port
Artifact 13	RDP Traffic Port

Artifacts Associated with Data from Information Repositories Technique (T0811)	
Artifact 14	Authentication Success
Artifact 15	Authentication Attempts
Artifact 16	MSSQL Traffic
Artifact 17	Traffic Timestamps
Artifact 18	SMB Traffic
Artifact 19	Project File Modification
Artifact 20	Data Bytes Sent
Artifact 21	User Session Creation
Artifact 22	Application Logon
Artifact 23	TDS Port
Artifact 24	Operational Database Data Modification
Artifact 25	Design Documentation Manipulation
Artifact 26	Authentication Failure
Artifact 27	Personnel List Files Accessed
Artifact 28	Jump Host Credentials Accessed
Artifact 29	Vendor Documentation Accessed
Artifact 30	Remote Procedure Calls
Artifact 31	Recent Search List
Artifact 32	MRU List Change
Artifact 33	Design Documentation Access
Artifact 34	Database Request
Artifact 35	SSH Traffic Port

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 Information via Phishing

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] [The Register | John Leyden | "'Chinese Cyberspies' target energy giants" | https://www.theregister.com/2011/02/10/night_dragon_cyberespionage/ | 10 February 2011 | Accessed 10 May 2022 | The source is publicly available information and does not contain classification markings]

[2] [The Hamilton Spectator | "Exxon, Shell, BP hacked via Chinese servers" | https://www.thespec.com/business/2011/02/23/exxon-shell-bp-hacked-via-chinese-servers.html | 28 February 2020 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[3] [McAfee | "Global Energy Cyberattacks: 'Night Dragon'" | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[4] [U.S. House of Representatives | "Examining The Cyber Threat To Critical Infrastructure and The American Economy: Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security" | https://www.govinfo.gov/content/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf | 16 March 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[5] [PCWorld | Jeremy Kirk | "Night Dragon' Attacks from China Strike Energy Companies" | https://www.pcworld.com/article/494731/article-1776.html | 10 February 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[6] [U.S. House of Representatives | "Examining The Cyber Threat To Critical Infrastructure and The American Economy: Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security" | https://www.govinfo.gov/content/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf | 16 March 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[7] [McAfee | "Global Energy Cyberattacks: 'Night Dragon'" | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[8] [U.S. House of Representatives | "Examining The Cyber Threat To Critical Infrastructure and The American Economy: Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security" | https://www.govinfo.gov/content/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf | 16 March 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[9] [Center for Education and Research in Information Assurance and Security of Purdue University | K. Kambic, and others | "Crude Faux: An analysis of cyber conflict within the oil & gas industries" | https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2013-9.pdf | 23 October 2013 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[10] [McAfee | "Global Energy Cyberattacks: 'Night Dragon'" | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[11] [McAfee | "Global Energy Cyberattacks: 'Night Dragon'" | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Gl

obal%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[12] [PCWorld | Jeremy Kirk | “Night Dragon’ Attacks from China Strike Energy Companies” | https://www.pcworld.com/article/494731/article-1776.html | 10 February 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[13] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[14] [U.S. House of Representatives | “Examining The Cyber Threat To Critical Infrastructure and The American Economy: Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security” | https://www.govinfo.gov/content/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf | 16 March 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[15] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[16] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[17] [U.S. House of Representatives | “Examining The Cyber Threat To Critical Infrastructure and The American Economy: Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security” | https://www.govinfo.gov/content/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf | 16 March 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[18] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[19] [Mandiant | “Mandiant M-Trends an Evolving Threat” | https://personal.utdallas.edu/~muratk/courses/dbsec12f_files/trend-report.pdf | 2012 | Accessed 18 July 2022 | The source is publicly available information and does not contain classification markings]

[20] [U.S. House of Representatives | “Examining The Cyber Threat To Critical Infrastructure and The American Economy: Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security” | https://www.govinfo.gov/content/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf | 16 March 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[21] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[22] [Center for Education and Research in Information Assurance and Security of Purdue University | K. Kambic, and others | “Crude Faux: An analysis of cyber conflict within the oil & gas industries”

| https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2013-9.pdf | 23 October 2013 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[23] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[24] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[25] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[26] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[27] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[28] [Center for Education and Research in Information Assurance and Security of Purdue University | K. Kambic, and others | “Crude Faux: An analysis of cyber conflict within the oil & gas industries” | https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2013-9.pdf | 23 October 2013 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[29] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[30] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[31] [Cybersecurity & Infrastructure Security Agency | “ICS Advisory (ICSA-11-041-01A) McAfee Night Dragon Report (Update A)” | https://www.cisa.gov/uscert/ics/advisories/ICSA-11-041-01A | 11 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[32] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[33] [Cybersecurity & Infrastructure Security Agency | “ICS Advisory (ICSA-11-041-01A) McAfee Night Dragon Report (Update A)” | https://www.cisa.gov/uscert/ics/advisories/ICSA-11-041-01A | 11 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[34] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Gl

obal%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[35] [Microsoft | “TrojanDropper:Win32/Redsip.A” | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanDropper%3AWin32%2FRedsip.A | 12 May 2010 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[36] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[37] [Microsoft | “Backdoor:Win32/Redsip.A!dll” | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor%3AWin32%2FRedsip.A!dll | 12 May 2010 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[38] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[39] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[40] [Cybersecurity & Infrastructure Security Agency | “ICS Advisory (ICSA-11-041-01A) McAfee Night Dragon Report (Update A)” | https://www.cisa.gov/uscert/ics/advisories/ICSA-11-041-01A | 11 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[41] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[42] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[43] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[44] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[45] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[46] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[47] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[48] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[49] [U.S. House of Representatives | “Examining The Cyber Threat To Critical Infrastructure and The American Economy: Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security” | https://www.govinfo.gov/content/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf | 16 March 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[50] [McAfee | “Global Energy Cyberattacks: ‘Night Dragon’” | https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf | 10 February 2011 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[51] [Center for Education and Research in Information Assurance and Security of Purdue University | K. Kambic, and others | “Crude Faux: An analysis of cyber conflict within the oil & gas industries” | https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2013-9.pdf | 23 October 2013 | Accessed 25 April 2022 | The source is publicly available information and does not contain classification markings]

[52] [The Hamilton Spectator | “Exxon, Shell, BP hacked via Chinese servers” | https://www.thespec.com/business/2011/02/23/exxon-shell-bp-hacked-via-chinese-servers.html | 28 February 2020 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[53] [U.S. House of Representatives | “Examining The Cyber Threat To Critical Infrastructure and The American Economy: Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security” | https://www.govinfo.gov/content/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf | 16 March 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[54] [CSO Online | Ann Bednarz | “Inside Cisco Global Security Operations” | https://www.csoonline.com/article/2129555/inside-cisco-global-security-operations.html | 12 September 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[55] [U.S. House of Representatives | “Examining The Cyber Threat To Critical Infrastructure and The American Economy: Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security” | https://www.govinfo.gov/content/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf | 16 March 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]