PRECURSOR ANALYSIS REPORT: HAVEX MALWARE IN A U.S. MANUFACTURING FACILITY 2014

Cybersecurity for the Operational Technology Environment (CyOTE)

30 JUNE 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-69481

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: USE OF HAVEX AGAINST A U.S. MANUFACTURING FACILITY IN 2014

1. EXECUTIVE SUMMARY

The Use of Havex Against a U.S. Manufacturing Facility in 2014 precursor analysis report leverages publicly available information about the Havex remote access trojan (RAT) and catalogs anomalous observables for each technique employed in the attacks. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

Havex, also referred to as Backdoor.Oldrea, PEACEPIPE, and Fertger, was a modular RAT used in the Dragonfly 1.0 cyberespionage campaign conducted by a Russian state-sponsored adversary from 2013 to 2014. Havex was targeted against multiple sectors such as energy, manufacturing, pharmaceutical, and others throughout the campaign.

Among its reconnaissance capabilities, Havex could scan industrial environments for assets using Open Platform Communications (OPC), an interoperability protocol popular in operational technology (OT) environments. This capability to scan for OPC assets is unique, particularly since Havex is one of the earliest pieces of malware that could specifically scan for industrial protocols. OPC is an interoperability protocol in wide use among multiple industries, and malware like Havex could be used to steal operational information, which could also result in unforeseen reliability issues. Havex also scanned TCP/IP network ports commonly used in OT environments, demonstrating a targeted approach by the adversary.

This report will illustrate the deployment of Havex against a U.S.-based manufacturing facility using OPC during the Dragonfly 1.0 campaign.

Researchers and analysts identified 14 techniques utilized during the attack with a total of 48 observables using the MITRE ATT&CK® for Industrial Control Systems framework. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity

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

2. INTRODUCTION

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

2.1. APPLYING THE CYOTE METHODOLOGY

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

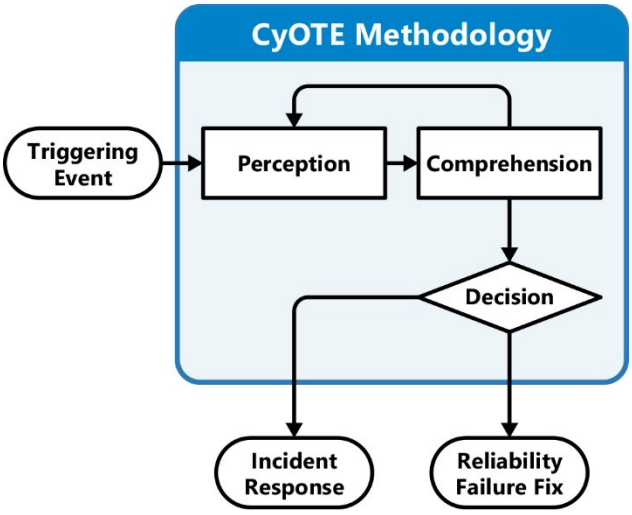


Figure 1. CyOTE Methodology

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

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

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

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

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

2.2. BACKGROUND ON THE ATTACK

Havex was a modular remote access trojan (RAT) that enumerated and exfiltrated information about networked assets within industrial operational technology (OT) environments. Adversaries used Havex to conduct network reconnaissance against critical infrastructure sectors such as energy, pharmaceutical, and manufacturing from February 2013 to May 2014 in multiple countries.[1]

Havex is one of the earliest known pieces of malware designed to identify and exfiltrate information on industrial assets and protocols.[2] Havex is also noteworthy due to the increasingly stealthy infection vectors adversaries employed in their aggressive and broad-scoped campaign.[3] For example, the adversaries initially employed spearphishing emails (D-120) to deploy the malware but quickly transitioned to stealthier methods of initial access, including drive-by and supply chain compromises that lasted almost a full year (D-335).[4]

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

Havex targeted Open Platform Communications (OPC), formerly known as Object Linking and Embedding (OLE) for Process Control, an industrial protocol in wide use in OT environments. OPC is known as a translation protocol prevalent in sectors that oversee OT assets.[5] OPC allows Windows-based software to communicate with diverse proprietary industrial protocols used by vendors, simplifying operation, monitoring, and data collection for the user.[6]

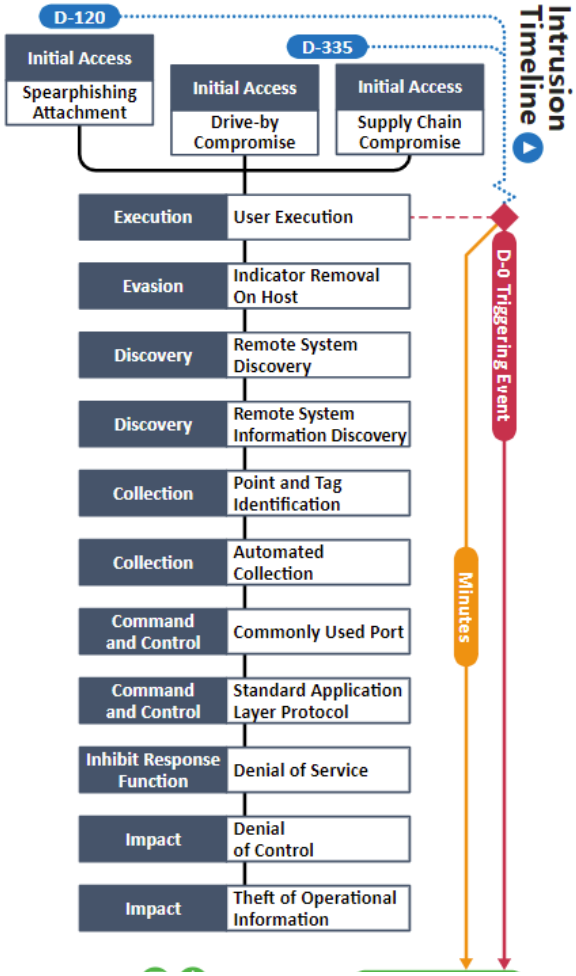


Figure 2. Intrusion Timeline

Once deployed, Havex would ascertain if there were any networked OPC assets within the local environment, as well as scan a number of TCP ports commonly used in industrial applications (M+10)[a] before exfiltrating the output of its scanning activities. This scanning activity can inadvertently cause OPC assets to malfunction, resulting in a temporary denial of service (D-0) or denial of control (D-0) scenario, as well as the theft of operational information (M+10).

This report focuses on Havex and its plugin that can enumerate OPC assets in a victim's environment, rather than the overarching cyberespionage campaign in which Havex was employed. Vendors and media outlets referred to this larger campaign as "Havex" but also as "Dragonfly 1.0". The "Dragonfly" moniker originates from Symantec, who dubbed the adversaries simultaneously using Havex and Karagany, another RAT, as Dragonfly in its reporting.[7] This study

[a] "M" corresponds to minutes prior to (M-) or after (M+) the triggering event; "D" events correspond to days prior to or afterward.

refers to the 2013-2014 campaign where the Havex RAT was observed in victim environments as the “Dragonfly 1.0 campaign” for clarity.

Analysis identified 14 techniques in a sequence and timeframe likely used by adversaries during this cyber attack. These attack techniques are defined according to MITRE’s ATT&CK® for ICS framework.

Table 1. Techniques Used in the Havex Case Study

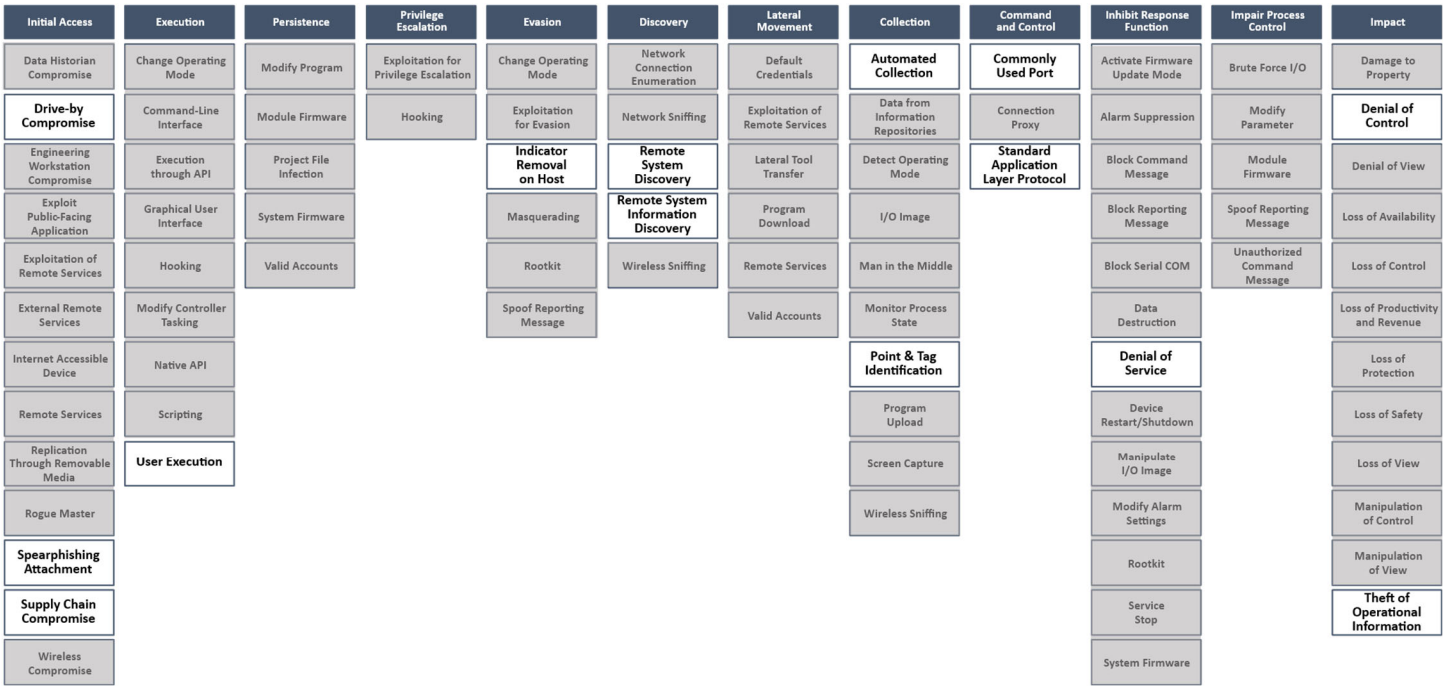


Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	14
Technique Observables	48
Precursor Techniques	11
Precursor Technique Observables	44
Highly Perceivable Precursor Technique Observable	42

3. OBSERVABLE AND TECHNIQUE ANALYSIS

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

3.1. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS

The adversaries behind Havex initially used malicious PDF documents in spearphishing emails sent to company executives and senior employees to deploy the malware into victim environments.[8] Spearphishing is a very common technique that both sophisticated and unsophisticated adversaries use to trick an unsuspecting end-user into installing malware by interacting with a malicious attachment, such as a PDF of Microsoft Office document. Email is one of the most popular vectors for an adversary to gain initial access into a victim environment. In the case of Havex, the spearphishing emails had titles like "*The Account*" and "*Settlement of delivery problem*".[9] The adversaries also used an exploit that allowed the embedded Havex payload to be executed within an XML-based companion to a PDF file, known as an XDP file.[10]

Targeted observers such as Support Staff and Management are the most likely to have observed this technique before any embedded malicious payload was executed. Spearphishing emails present an early perception opportunity for personnel as there are several cognitive processes that end-users can learn to determine if an email with an attachment is suspicious, even without interacting with it. One potential perception opportunity could be a solution as simple as "external" tags on all emails originating from outside the organization.

A total of five observables were identified with the use of the Spearphishing Attachment technique (T0865). This technique is important for investigation because it often is one of the first tactics an adversary would pursue to gain initial access. This technique is important for investigation, as it appears early and is often the first observable opportunity for end-users. Responding to this technique could potentially halt an attack early in the attack chain.

All five observables are assessed to be highly perceivable (Spearphishing Email; Malicious XML Attachments; Malicious XDP Attachments; Malicious PDF Attachments; Anomalous Downloads over HTTP).

Please see Appendix A for the list of observables.

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[b]	Support Staff and Management

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

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

The adversaries behind Havex also utilized drive-by compromises, also known as watering hole attacks, to spread and install the malware in targeted environments.[11] Specifically, the adversaries made use of iframes and several exploit kits to redirect the user's browser session to a second website that hosted the Havex payload.[12] Once the user's browser visited the compromised site, the victim's machine would download and execute Havex. The adversary targeted and infected websites of interest to the victim, which increased the likelihood a victim would interact with the compromised site.[13]

Observables include normal interaction with websites of interest to personnel in an organization, which severely hampers a perceivable opportunity for the end-user. IT or OT Cybersecurity is somewhat likely to see anomalous download activity on a host depending on their visibility within their respective environment.

Potential observers of this technique include IT Staff, OT Staff, Engineers, Management, and Support Staff.

A total of two observables, neither of which are assessed to be highly observable, were identified with the use of the Drive-By Compromise technique (T0817). This technique appears early in the attack chain and detecting and responding to a drive-by compromise will limit an adversary's ability to gain initial access to a victim's environment.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 24 artifacts could be generated by the Drive-By Compromise technique
Technique Observers	IT Staff, Support Staff, Management, OT Staff, Engineers

3.3. SUPPLY CHAIN COMPROMISE TECHNIQUE (T0862) FOR INITIAL ACCESS

In the later stages of the campaign, the adversaries compromised three original equipment manufacturers (OEMs) of ICS software Havex could use to piggyback in a supply chain attack (T0862) deeper into the production environment.[14] The adversaries embedded the Havex payload in legitimate software downloads hosted on three OEM websites, which victims then downloaded. This almost certainly guaranteed successful execution and infection of any host receiving the updated software from the three OEMs.[15] Infection through a supply chain attack could be especially problematic if the update was installed in the operations zone: this would position Havex to execute and exfiltrate victim information from within the OT/production network.

Potential observers for this technique include engineers or staff responsible for downloading and installing updates such as OT Staff, IT Staff, Engineers, and Support Staff. These observers likely would have interacted normally with vendor websites and downloaded relevant software updates as needed.

This technique modifies the host operating system files via the download and installation of Havex, resulting in the host being placed into a modified state. Additionally, mismatched software hashes present a potential observable if OEMs publish verified hashes and adversaries did not manipulate them; however, this could be obfuscated by adversaries by editing the hash and would minimize perceivability by both the OEM and victim. Anomalous activity instantiated by the compromised software, such as anomalous outbound communications, would be highly perceivable.

A total of three observables were identified with the use of the Supply Chain Compromise technique (T0862). Supply chain attacks are notoriously stealthy and difficult for defenders to counter. This technique appears early in the attack timeline and is an effective means for an adversary to gain initial access. Terminating the attack chain at this point is unlikely to prevent Havex from scanning as the malware will still execute in a victim's environment upon installation.

All three observables are assessed to be highly perceivable (Modification of Host Operating Files; Registry Key Created; Anomalous Outbound Communication).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 31 artifacts could be generated by the Supply Chain Compromise technique
Technique Observers	OT Staff, IT Staff, Engineers, Support Staff

3.4. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

A common factor among the three initial access vectors includes the User Execution technique (T0863) that triggers the download and installation of Havex malware onto a host. User actions that enable Havex infections include interacting with malicious email attachments in spearphishing emails, visiting a compromised website in a browser, and installing a trojan-infected update from an OEM. User execution is a common technique that adversaries regularly use to execute payloads within a victim's environment for follow-on activities such as reconnaissance or deployment of additional malicious software like ransomware.

Observers of and participants in this technique include all previously listed observers for the initial access phase. Observers include Management, IT Staff, IT Cybersecurity, OT Staff, Engineers, and Support Staff, as Havex leveraged multiple techniques related to initial access that hinge on user execution. These include malicious documents attached to spearphishing emails, drive-by compromises targeting vulnerable web browsers, and supply chain attacks. It is likely the most concrete perception opportunities for personnel are spearphishing emails as they are the least stealthy initial access technique among the three listed in this report.

This technique modifies the host operating system files via the download and installation of Havex, resulting in the host being placed into a modified state. If system backups are created after this technique is executed, data recovery and disaster recovery efforts will likely be impaired.

A total of three observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation as it is extremely common among sophisticated and unsophisticated adversaries to use early in the attack chain. This technique appears early in the timeline and is somewhat likely for defenders to perceive given the initial access techniques covered in sections 3.1 to 3.3.

All three observables are assessed to be highly perceivable (Spearphishing Email; Malicious PDF Attachment; AutoStart Registry Key Created).

Please see Appendix A for the list of observables.

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	Management, IT Staff, IT Cybersecurity, OT Staff, Engineers, Support Staff

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

Havex wipes files from disk to avoid detection after conducting its reconnaissance on an infected host. Havex writes files to disk in the %TEMP%, %System32%, and %AppData% directories, and deletes files once the output of its automated reconnaissance is sent off to a command and control (C2) server.[16]

Observers of Havex's indicator removal capabilities include host administrators, IT Staff, IT Cybersecurity, and OT Cybersecurity. This technique occurs relatively late in Havex's timeline as the malware will wipe any outputs of techniques related to Discovery tactics.

A total of three observables were identified with the use of the Indicator Removal on Host technique (T0863). This technique is important for investigation as it is common among sophisticated and unsophisticated adversaries to use in an attack chain. This technique appears throughout the attack timeline and, although difficult, is not impossible for defenders such as host administrators to observe. Terminating the attack chain at this point would potentially stop the exfiltration of operational information.

All three observables are assessed to be highly perceivable (Creation of .tmp, .dat, or .yls Files; Deletion of .tmp, .dat, or .yls Files; Deletion of Registry Keys).

Please see Appendix A for the list of observables.

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, OT Cybersecurity

3.6. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

Havex's network scanning capabilities provide its base reconnaissance function to gain insight into the target's environment through the Remote System Discovery technique (T0846). Havex can identify networked assets in the Local Area Network (LAN) using Windows Network (Wnet) calls.[17,18] Outputs of this baseline scanning activity determine what types of assets Havex will scan for next and are discussed in subsequent technique sections.

Observers include IT Staff, OT Staff, IT Cybersecurity, and OT Cybersecurity. These observers would likely see anomalous ARP (Address Resolution Protocol) traffic in the form of ARP requests to generate a series of replies from networked devices in that LAN.[19] Terminating the chain of techniques at this point would likely prevent the malware from spreading to other systems and conducting further reconnaissance.

A total of four observables were identified with the use of the Remote System Discovery technique (T0846). This technique appears early in the Havex timeline; Havex conducts this scanning as a basis for later reconnaissance activities.

All four observables associated with this technique are assessed to be highly perceivable (Anomalous ARP Requests; Anomalous ARP Replies; WNetOpenEnum API Calls; WNetEnumResources API Calls).

Please see Appendix A for the list of observables.

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, OT Staff, IT Cybersecurity, OT Cybersecurity

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

Havex can enumerate any networked OPC assets within a victim's environment via the Remote System Information Discovery technique (T0888). After mapping the victim's general network topography, Havex also scans hard-coded ports commonly used in industrial environments such as TCP/IP Ports 102 (Siemens S7), 502 (Schneider Electric), and 44818 (Rockwell Automation).[20] Havex also scans for Microsoft Distributed Component Object Model (COM/DCOM) interfaces.[21,22] If Havex receives a response to its COM/DCOM requests, Havex will then seek out specific OPC attributes, as detailed in a later technique section.

Observers of this scanning activity include IT Staff, OT Staff, IT Cybersecurity, OT Cybersecurity, who could observe abnormal scanning across a LAN on the listed TCP ports as well as anomalous COM/DCOM traffic.

A total of eight observables were identified with the use of the Remote System Information Discovery technique (T0888). This technique is important for investigation as anomalous scanning is an indicator of either a reliability issue or potential malicious activity in an enterprise or operations environment. This technique appears near the middle of the Havex attack chain. Terminating the attack chain at this point would likely prevent any additional scanning, including any that interferes with OPC assets, which is detailed in a later technique.

All eight observables are assessed to be highly perceivable (Anomalous Scanning over TCP Port 102; Anomalous Scanning over TCP Port 502; Anomalous Scanning over TCP Port 11234, Anomalous Scanning over TCP Port 12401; Anomalous Scanning over TCP Port 44818; Scanning over TCP Port 135; Anomalous COM/DCOM Traffic; Anomalous DCE/RPC Calls).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 8 artifacts could be generated by the Remote System Information Discovery technique
Technique Observers	IT Staff, OT Staff, IT Cybersecurity, OT Cybersecurity

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

After determining if a networked asset responds to COM/DCOM traffic, Havex collects information specific to OPC assets as part of the Point and Tag Identification technique. OPC allows Windows-based software to interact across numerous proprietary vendor protocols, simplifying inter-device communications within modern industrial environments. OPC assets use labels known as “points” and “tags” to reference various aspects of an OPC server or client. “Points” include values such as inputs, outputs, and other process-specific values and “tags” are labels given to various points for operator convenience.[23] Havex is capable of Point and Tag Identification (T0861) and searches for attributes such as server state, class identification, tag name, type, access, and identification number.[24] This information would be key to an adversary for either industrial espionage or as preparation for more tailored malicious cyber activity against that facility.

Observers of this technique include OT Staff and OT Cybersecurity. These observers likely would have seen unusual scanning from previous techniques, as well as anomalous OPC traffic. OPC Data Access (DA) is documented to run on TCP Port 135 but there are other ephemeral port configurations depending on facility requirements.

A total of five observables were identified with the use of the Point and Tag Identification technique (T0861). Randomly generated network traffic that is indicative of scanning within a victim’s network is a perception opportunity for defenders, likely prompting an investigation. This technique appears late in the timeline for Havex. Identifying the source of this activity, like the above techniques, presents a key comprehension opportunity for defenders. Termination of the attack chain at this stage would prevent any identification of exfiltration of information related to networked OPC assets.

All five observables are assessed to be highly perceivable (Scanning over TCP Port 135; Anomalous Scanning over TCP Port 1024-65535; Creation of OPCServer[random].txt files in %TEMP% Directory; CoInitializeEx API Calls; CoCreateInstance API calls).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 53 artifacts could be generated by the Point and Tag Identification technique
Technique Observers	OT Staff, OT Cybersecurity

3.9. AUTOMATED COLLECTION TECHNIQUE (T0802) FOR COLLECTION

Once Havex has mapped the victim's network and enumerated OPC assets, the malware then automatically collects data using the Automated Collection technique (T0802), compiles the results, encrypts the data, then sends it to a C2 server.

Havex outputs the scan results into a .txt file with the name of the OPC asset it identified, such as OPCServer[random].txt.dat, encrypts the .txt file in the %TEMP% directory, then sends the output to an external C2 server.[25,26,27]

Observers of this technique include IT Staff, OT Staff, IT Cybersecurity, and OT Cybersecurity staff.

A total of four observables were identified with the use of the Automated Collection technique (T0802). This technique appears late in the Havex attack chain. Terminating the chain of techniques at this point is somewhat likely to prevent Havex from exfiltrating data from the victim to a C2 under the adversary's control.

All four observables are assessed to be highly perceivable (Exfil Victim Data to C2 Server; Creation of .txt, .dat, or .yls File Containing Output of Havex OPC Reconnaissance Module; Encryption of .txt or .dat file; Creation of AutoStart Registry Key).

Please see Appendix A for the list of observables.

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, OT Staff, IT Cybersecurity, OT Cybersecurity staff

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

Havex utilizes the Commonly Used Ports technique (T0855) for its C2 traffic. Specifically, Havex uses HTTP over TCP/IP Port 80 to communicate with C2 servers.[28]

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

A total of three observables were identified with the use of the Commonly Used Port technique (T0885). This technique is important for investigation as it appears throughout Havex's attack timeline, which would allow defenders a greater opportunity to detect network activity between the malware and its C2 infrastructure. Terminating the attack chain here could either identify malicious activity in a victim's environment or prevent the malware from exfiltrating operational information to a C2 server.

All three observables are assessed to be highly perceivable (Traffic over TCP Port 80; HTTP GET Requests; HTTP POST Requests).

Please see Appendix A for the list of observables.

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

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

Havex uses the Standard Application Layer Protocol technique (T0869) to communicate with its C2 servers through HTTP. [29,30]

Observers of this technique include network administrators, IT Staff, IT Cybersecurity, and OT Cybersecurity.

This technique is important for investigation as it presents a detection and perception opportunity for defenders that warrants investigation, especially within a production environment. Terminating the attack chain here could either identify malicious activity in a victim's environment or prevent the malware from exfiltrating operational information to a C2 server.

A total of three observables were identified with the use of the Standard Application Layer Protocol technique.

All three observables are assessed to be highly perceivable (HTTP Traffic on TCP/80; HTTP GET Requests; HTTP POST Requests).

Please see Appendix A for the list of observables.

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

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

Although multiple researchers and vendors have stated that Havex was designed with the intent to inhibit processes or cause damage to assets in industrial control environments, ICS-CERT observed in testing that multiple OPC platforms crashed after a Havex infection, likely due to Havex's OPC scanning capabilities.[31,32] In such cases, a temporary denial of service effect could cause a denial of control incident for assets reliant on OPC for operation and control.[33]

Observers of this technique include OT Staff, OT Cybersecurity, and Engineers. These observers likely observe OPC clients or servers behaving abnormally or not functioning properly when in use.

A total of three observables were identified with the use of the Denial of Service technique (T0882). This technique is important for investigation as malfunctioning OPC assets represents a triggering event warranting investigation by an organization. Terminating the attack chain here would stop any active scanning conducted by the malware as well as prevent the exfiltration of operational information.

All three observables are assessed to be highly perceivable (OPC Clients not Functioning; OPC Servers not Functioning; Abnormal OPC Traffic).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 14 artifacts could be generated by the Denial of Service technique
Technique Observers	OT Staff, OT Cybersecurity, Engineers

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

After its automated reconnaissance is complete, Havex exfiltrates the output of its activities to an external C2 server. In addition to mapping network infrastructure and identifying OPC assets, Havex can also harvest credentials from applications such as email clients and web browsers used in enterprise environments. Havex outputs the results of its reconnaissance module into a .txt file, and then encrypts the .txt file into a .yls format, which helps ensure a casual observer would not know the purpose of such a file.[34,35]

Observers of this technique include IT Cybersecurity, OT Cybersecurity, and IT Staff such as host administrators. These observers likely would have observed brief activity within several common file directories on a compromised host along with the creation and deletion of several .txt and .yls files.

A total of three observables were identified with the use of the Theft of Operational Information technique (T0882). This technique is important for investigation because it represents an exfiltration of victim information that could be used in either industrial espionage or sabotage. This technique appears at the end of the attack chain beyond the point where a defender could take action to disrupt the attack.

All three observables are assessed to be highly perceivable (Creation of .txt or .dat File Containing Output of Havex's Activities; Deletion of .txt File; Deletion of .dat File; Deletion of .yls File, Anomalous Outbound Communications Over HTTP).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 4 artifacts could be generated by the Theft of Operational Information technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity

3.14. DENIAL OF CONTROL TECHNIQUE (T0813) FOR IMPACT

Multiple researchers and vendors have stated Havex was not capable of explicit destructive capability and was likely not designed to do so.[36] However, during testing ICS-CERT observed multiple OPC devices crashing due to Havex.[37,38] This is likely due to unforeseen errors stemming from Havex's OPC scanning module. The temporary denial of service effect on assets reliant on OPC could result in a temporary denial of control incident where operators who rely on OPC cannot control assets within an OT environment.

Observers of this technique include OT Staff, OT Cybersecurity, Engineers, and Plant Managers. These observers would likely witness industrial assets triggering alarms as they malfunction or crash. This technique is important for investigation because it represents a triggering event driven by reliability issues or potential malicious cyber activity. Terminating the attack chain here is not likely to prevent the exfiltration of Havex's reconnaissance data due to the immediacy of this technique.

One observable, assessed to be highly perceivable, was identified with the use of the Denial of Control technique (T0813) (OPC Assets Unable to be Controlled).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 8 artifacts could be generated by the Denial of Control technique
Technique Observers	OT Staff, OT Cybersecurity Staff, Engineers, Plant Managers

APPENDIX A: OBSERVABLES LIBRARY

Observables Associated with Spearphishing Attachment Technique (T0865)	
Observable 1	Victims Received Spearphishing Emails Designed To Trick End Users Into Interacting With Malicious Attachments
Observable 2	Victims Interacted With Malicious Adobe Documents In Spearphishing Emails That Would Install The Havex Malware Onto A Host
Observable 3	The Attached Malicious XML Documents Would Trigger A Download Of The Havex Payload
Observable 4	The Attached Malicious XDP Documents Would Trigger A Download Of The Havex Payload
Observable 5	The Attached Malicious PDF Documents Would Trigger A Download Of The Havex Payload

Observables Associated with Drive-by Compromise Technique (T0817)	
Observable 1	Iframes Were Placed On Compromised Websites To Redirect Victims To Sites Hosting The Havex Payload
Observable 2	Victims Visiting Compromised Websites Were Re-Routed To A Website Hosting The Havex Malware

Observables Associated with Supply Chain Compromise Technique (T0862)	
Observable 1	Victims Unknowingly Downloaded Compromised Software That Contained An Embedded Havex Payload
Observable 2	Victims Could Perceive Anomalous Outbound Traffic Upon Installation Of The Trojanized Software Updates; HTTP
Observable 3	Downloading The Trojanized Software Update Would Modify Host Files, Thereby Instantiating Malicious Activity Such As Anomalous Scanning

Observables Associated with User Execution Technique (T0863)	
Observable 1	Victims Received Spearphishing Emails Designed To Trick End Users Into Interacting With Malicious Attachments
Observable 2	Victims Interacted With Malicious Adobe PDF Documents That Would Install The Havex Malware Onto A Host
Observable 3	Havex Would Create An Autostart Registry Key To Maintain Persistence

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 1	Havex Deleted Files In %TEMP%, %Appdata%, %System32% Directories On Disk After Its Reconnaissance Activities Were Complete

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 2	Havex wrote and deleted files in several host directories on disk: Files Deleted in %TEMP%, %AppData%, %System32% Directories
Observable 3	Havex Created Then Deleted .tmp Files On An Infected Host: .tmp Files Created Or Deleted
Observable 4	Havex Created Then Deleted .yls Files On An Infected Host: .yls Files Created Or Deleted
Observable 5	Havex Created Then Deleted .dat Files On An Infected Host: .dat Files Created Or Deleted

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1	Havex Used ARP Requests To Identify Networked Assets For Further Reconnaissance: Anomalous ARP Requests
Observable 2	Havex Used ARP Replies To Identify Networked Assets For Further Reconnaissance: Anomalous ARP Replies

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 1	Havex Scanned On TCP PORT 102, A Port Associated With Siemens PLCs: Anomalous Traffic On TCP PORT 102
Observable 2	Havex Scanned On TCP PORT 502, A Port Associated With Modbus Over Ethernet: Anomalous Traffic On TCP PORT 502
Observable 3	Havex Scanned On TCP PORT 11234, A Port Associated With ScadaPro Communications: Anomalous Traffic On TCP PORT 11234
Observable 4	Havex Scanned On TCP PORT 12401, A Port Associated With 7-Technologies Graphical SCADA, GE Proficy License Server Manager, And WellinTech KingSCADA: Anomalous Traffic On TCP PORT 12401
Observable 5	Havex Scanned On TCP PORT 44818, A Port Associated With Rockwell Automation Software, Tec4Data Smartcooler, And Cisco IOS Common Industrial Protocol Processor: Anomalous Traffic On TCP PORT 44818
Observable 6	Havex Scanned On TCP PORT 135, A Port Associated With OPC DA: Anomalous Traffic On TCP PORT 135
Observable 7	Havex Scanned For COM And DCOM Objects To Help Identify Any OPC Assets In A LAN: Non-Standard COM/DCOM Traffic
Observable 8	DCOM Uses DCE As Its Transport Layer: DCE/RPC Calls

Observables Associated with Point and Tag Identification Technique (T0861)	
Observable 1	Havex Scanned Over TCP PORT 135 As OPC DA Is Associated With This Port, To Collect OPC-Specific Attributes: Scanning Over TCP PORT 135
Observable 2	Havex May Have Scanned On Other Ports Associated With OPC DA, As OPC DA Can Be Configured To Use Other Default Ephemeral Ports: Anomalous Scanning Over TCP PORT 1024-65535

Observables Associated with Automated Collection Technique (T0802)	
Observable 1	Havex Exfiltrated Its Scanning Output To An Adversary Controlled C2 Server
Observable 2	Havex Created .txt Files Of Its Reconnaissance Outputs
Observable 3	Havex Created Encrypted .yls Files From The .txt Files That Contained The Results Of Its Scanning Activities
Observable 4	Havex Created An Autostart Registry Key To Execute The Malware When A User Logs In, Helping To Ensure Persistence On An Infected Host

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 1	Havex Used HTTP For Its C2 Traffic, Which Uses TCP Port 80: Traffic Over TCP Port 80
Observable 2	Havex Used HTTP GET Requests To Communicate With Its C2 Server Or Download Additional Modules: HTTP GET Requests
Observable 3	Havex Used HTTP POST Requests To Communicate With Its C2 Server Or Exfiltrate Its Reconnaissance Output: HTTP POST Requests

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1	Havex Used HTTP GET Requests To Download Additional Modules Or Receive Commands From Its C2 Server: HTTP GET Requests
Observable 2	Havex Used HTTP POST Requests To Exfiltrate Its Scanning Output: HTTP POST Requests
Observable 3	Havex Used HTTP For Its C2 Traffic: HTTP

Observables Associated with Denial of Service Technique (T0814)	
Observable 1	Havex Was Observed Causing OPC Clients To Malfunction Due To Errors Related To Its Scanning Activities
Observable 2	Havex Was Observed Causing OPC Servers To Malfunction Due To Errors Related To Its Scanning Activities
Observable 3	Havex Scanned OPC Assets, Generating Additional And Abnormal OPC Traffic In An Environment

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 1	Havex Would Exfiltrate The Output Of Its Reconnaissance To Its C2 Server: HTTP Traffic
Observable 2	Havex Created Then Deleted .tmp Files On An Infected Host Pertaining To Its Reconnaissance Activities
Observable 3	Havex Created Then Deleted .yls Files On An Infected Host Pertaining To Its Reconnaissance Activities

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 4	Havex Created Then Deleted .dat Files On An Infected Host Pertaining To Its Reconnaissance Activities

Observables Associated with Denial of Control Technique (T0813)	
Observable 1	Havex Could Cause Organizations To Temporarily Lose Control Of Certain Assets Reliant On OPC Due To Unforeseen Errors Associated With Havex's Scanning Activities

APPENDIX B: ARTIFACTS LIBRARY

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

Artifacts Associated with Drive-by Compromise Technique (T0817)	
Artifact 1	Application Log
Artifact 2	cmd.exe Application Start
Artifact 3	Dialog Boxes Open
Artifact 4	POWERSHELL Cmdlet Open
Artifact 5	POWERSHELL Log Creation
Artifact 6	Source IP Address
Artifact 7	Destination IP Address
Artifact 8	File Creation
Artifact 9	Memory Evidence
Artifact 10	Disk Read
Artifact 11	Disk Write
Artifact 12	TLS Certificates
Artifact 13	Website
Artifact 14	Industrial Application Process
Artifact 15	Industrial Application Disk Write
Artifact 16	Prefetch Files
Artifact 17	.LNK Files
Artifact 18	HTTP Traffic
Artifact 19	DNS Traffic
Artifact 20	HTTPS Traffic
Artifact 21	SMB Traffic
Artifact 22	Process Creation
Artifact 23	Process Ending
Artifact 24	Child Processes Created

Artifacts Associated with Supply Chain Compromise Technique (T0862)	
Artifact 1	DNS Queries Traffic Port
Artifact 2	MAC Address
Artifact 3	Source IP Address
Artifact 4	Destination IP Address
Artifact 5	Network Discover Protocols
Artifact 6	SMB Port
Artifact 7	SNMP Port

Artifacts Associated with Supply Chain Compromise Technique (T0862)	
Artifact 8	LLDP Requests
Artifact 9	HTTP Port
Artifact 10	Ping Echo Port
Artifact 11	Static Source IP Address
Artifact 12	Usage of Default Account
Artifact 13	Usage of Vendor Maintenance Account
Artifact 14	Domain Name
Artifact 15	Domain Registrant Data
Artifact 16	Domain IP Resolution
Artifact 17	Domain Autonomous System Number
Artifact 18	Hardware Serial Number Missing
Artifact 19	Additional Hardware Inserted on Devices
Artifact 20	Mismatched Software Hashes
Artifact 21	Device Failures
Artifact 22	Device Incompatibility Issues
Artifact 23	Hardware Tampering Evidence
Artifact 24	Hardware Failed Site Acceptance Test
Artifact 25	Physical Defects to Hardware
Artifact 26	Unscheduled FIRMWARE Updates
Artifact 27	Manipulation of Signature on Digital Certifications
Artifact 28	Inconsistencies in Software Bill of Materials
Artifact 29	Inconsistencies in Hardware Bill of Materials
Artifact 30	Factory Acceptance Test Failure
Artifact 31	Inaccurate Delivery Based on Design Documents

Artifacts Associated with User Execution Technique (T0863)	
Artifact 1	Application Log
Artifact 2	Prefetch Files
Artifact 3	System Log
Artifact 4	Registry Modification
Artifact 5	File Modifications
Artifact 6	File Renaming
Artifact 7	System Patches Installed

Artifacts Associated with User Execution Technique (T0863)	
Artifact 8	Files Opening
Artifact 9	File Signature Validation
Artifact 10	Installers Created
Artifact 11	Process Termination
Artifact 12	File Creation
Artifact 13	Service Termination
Artifact 14	File Changes
Artifact 15	User Account Modification
Artifact 16	Increased ICMP Traffic (Network Scanning)
Artifact 17	File Execution
Artifact 18	Network Traffic Changes
Artifact 19	Process Creation
Artifact 20	Network Connection Creation
Artifact 21	Command Execution
Artifact 22	Application Log Content
Artifact 23	Application Installation

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

Artifacts Associated with Indicator Removal on Host Technique (T0872)	
Artifact 16	Windows Security Log 1102 for Cleared Events
Artifact 17	File Deletion
Artifact 18	File Modification
Artifact 19	Sdelete Executable Loaded
Artifact 20	Sdelete Executable Executed
Artifact 21	File Metadata Changes
Artifact 22	Timestamp Inconsistencies
Artifact 23	User Authentication

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 1	Common Network Traffic
Artifact 2	IEC 103 Traffic (For North America)
Artifact 3	IEC 61850 MMS and
Artifact 4	Controller Proprietary Traffic
Artifact 5	Echo Type 8 Traffic
Artifact 6	ICMP Type 7 Traffic
Artifact 7	SNMP Port 162 Traffic
Artifact 8	SNMP Port 161 Traffic
Artifact 9	Command Line Dialog Box Open
Artifact 10	Operating System Queries
Artifact 11	DNS Port 53 Zone Transfers
Artifact 12	Industrial Network Traffic Content About Hostnames
Artifact 13	Polling Network Traffic from Unauthorized IP Sender Addresses
Artifact 14	NETBIOS Name Services Port
Artifact 15	LDAP Port
Artifact 16	Active Directory Calls
Artifact 17	Email Server Calls
Artifact 18	SMTP Port 25 Traffic
Artifact 19	DNS Lookup Queries
Artifact 20	ARP Scans
Artifact 21	TCP Connect Scan
Artifact 22	TCP SYN Scans
Artifact 23	Scans Over Industrial Network Ports with Target IPS

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 24	TCP FIN Scans
Artifact 25	TCP Reverse Ident Scan
Artifact 26	TCP XMAS Scan
Artifact 27	TCP ACK Scan
Artifact 28	VNC Port 5900 Calls
Artifact 29	Protocol Content Enumeration
Artifact 30	Protocol Header Enumeration
Artifact 31	Recurring Protocol SYN Traffic
Artifact 32	Sequential Protocol SYN Traffic
Artifact 33	Statistical Anomalies in Network Traffic
Artifact 34	Industrial Network Traffic Content Containing Logical Identifiers
Artifact 35	Device Failure
Artifact 36	Device Reboot
Artifact 37	Bandwidth Degradation
Artifact 38	Host Recent Connection Logs
Artifact 39	Industrial Network Traffic
Artifact 40	OPC Network Traffic
Artifact 41	IEC 104
Artifact 42	IEC 102
Artifact 43	IEC 101 Traffic to Serial Devices

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

Artifacts Associated with Point and Tag Identification Technique (T0861)	
Artifact 1	Industrial Network Traffic
Artifact 2	Control Server Logoff
Artifact 3	Application Logs
Artifact 4	Application Manipulation
Artifact 5	Application User Event
Artifact 6	Application Reads
Artifact 7	Application Copy
Artifact 8	Point and Tag Data Exfiltration
Artifact 9	Host System Registry Modification
Artifact 10	User Registry Changes
Artifact 11	Memory Location Changes
Artifact 12	Common Network Traffic
Artifact 13	OPC Requests
Artifact 14	.dll Creation
Artifact 15	.dll Execution
Artifact 16	.dll Hooking
Artifact 17	SQL Network Traffic
Artifact 18	Database Vendor Specific Protocol Request
Artifact 19	Network Traffic Content Focused On Point and Tag Reads
Artifact 20	External Point and Tag Read Requests Over Network Trust Boundaries
Artifact 21	Data Historian Reads
Artifact 22	Data Historian Writes
Artifact 23	Database Reads
Artifact 24	Control Server Reads
Artifact 25	Data Historian Logon Event
Artifact 26	Database Logon Event
Artifact 27	Control Server Logon
Artifact 28	DNS Queries Traffic Port
Artifact 29	MAC Address
Artifact 30	Source IP Address
Artifact 31	Destination IP Address
Artifact 32	Network Discover Protocols
Artifact 33	SMB Port

Artifacts Associated with Point and Tag Identification Technique (T0861)	
Artifact 34	SNMP Port
Artifact 35	LLDP Requests
Artifact 36	HTTP Port
Artifact 37	Ping Echo Port
Artifact 38	Static Source IP Address
Artifact 39	Usage of Default Account
Artifact 40	Usage of Vendor Maintenance Account
Artifact 41	Domain Name
Artifact 42	Domain Registrant Data
Artifact 43	Domain IP Resolution
Artifact 44	Domain Autonomous System Number
Artifact 45	Hardware Serial Number Missing
Artifact 46	Additional Hardware Inserted On Devices
Artifact 47	Mismatched Software Hashes
Artifact 48	Device Failure
Artifact 49	Device Incompatibility Issues
Artifact 50	Hardware Tampering Evidence
Artifact 51	Hardware Failed Site Acceptance Test
Artifact 52	Physical Defects to Hardware
Artifact 53	Unscheduled Firmware Updates

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 1	Network Read Request
Artifact 2	OPC Read Requests
Artifact 3	Local Memory Read Requests
Artifact 4	Database Read Request
Artifact 5	POWERSHELL Command Arguments
Artifact 6	User Account Logs
Artifact 7	SMB Traffic Port
Artifact 8	File Transfer
Artifact 9	Application Log

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 10	Service Log
Artifact 11	Native Tool Use
Artifact 12	External Network Connections
Artifact 13	Command Line Arguments
Artifact 14	File Creation
Artifact 15	File Execution
Artifact 16	Command Execution
Artifact 17	Internal Network Connections
Artifact 18	IP Addresses
Artifact 19	MAC Addresses
Artifact 20	Operational Data Exfiltration
Artifact 21	User Account Creation
Artifact 22	User Account Privilege Change
Artifact 23	SQL Read Requests

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

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

Artifacts Associated with Standard Application Layer Protocol Technique (T0869)	
Artifact 10	RDP Traffic Port
Artifact 11	HTTP Post Request
Artifact 12	External IP Addresses

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

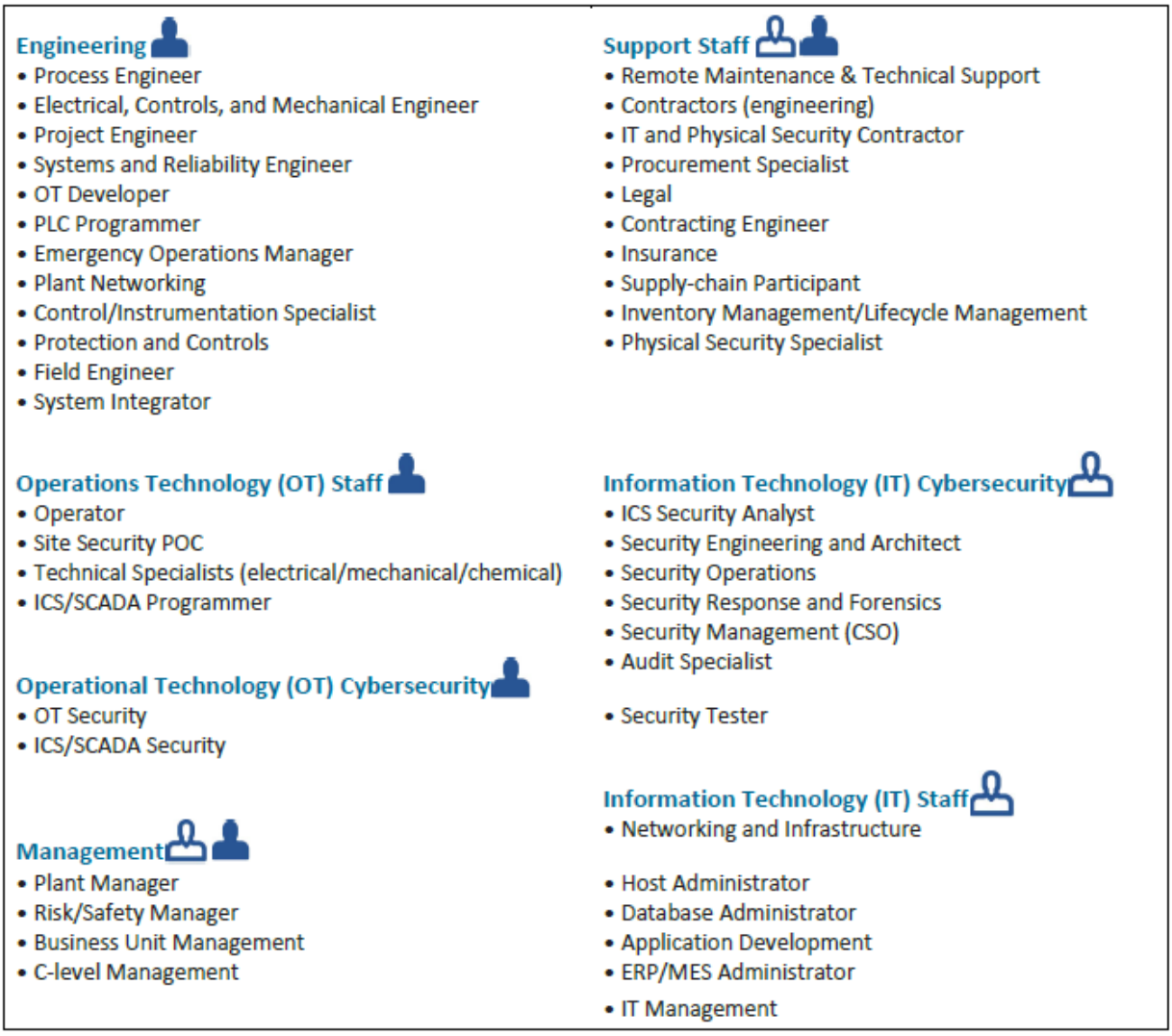
Artifacts Associated with Theft of Operational Information Technique (T0882)	
Artifact 1	Exfiltration of Endpoint Host Data (Spreadsheets, Diagrams, Documents, Configurations, etc.) via Industrial Protocols
Artifact 2	Exfiltration of Endpoint Host Data (Spreadsheets, Diagrams, Documents, Configurations,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

Artifacts Associated with Denial of Control Technique (T0813)	
Artifact 1	Input Failure
Artifact 2	Increased Network Packet Delivery
Artifact 3	Process Failure
Artifact 4	Process Reboot

Artifacts Associated with Denial of Control Technique (T0813)	
Artifact 5	Serial Communication Failure
Artifact 6	Network Ports Opened
Artifact 7	Network Ports Closed
Artifact 8	Process Nonresponsive

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] [Symantec| "Dragonfly" | https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers | 7 July 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

[2] [Belden | Joel Langill | “Defending Against the Dragonfly Cyber Security Attacks” | https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en | 22 October 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

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

[4] [Belden | Joel Langill | “Defending Against the Dragonfly Cyber Security Attacks” | "https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en" | 22 October 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

[5] [OPC Foundation | "What is OPC?" | https://opcfoundation.org/about/what-is-opc/ | Accessed on 24 April 2022 | This source is publicly available and does not contain classified markings]

[6] IBID

[7] [Symantec| "Dragonfly" | https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers | 7 July 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

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

[9] [Symantec| "Dragonfly" | https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers | 7 July 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

[10] [Belden | Joel Langill | “Defending Against the Dragonfly Cyber Security Attacks” | "https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en" | 22 October 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

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

[12] [Belden | Joel Langill | “Defending Against the Dragonfly Cyber Security Attacks” | "https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en" | 22 October 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

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

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

[15] [Belden | Joel Langill | “Defending Against the Dragonfly Cyber Security Attacks” | "https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en" | 22 October 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

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

[17] [FireEye | Kyle Wilhoit| "Havex, It's Down With OPC" | https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html | 17 July 2014 | Accessed on 2 April 2022 | The source is publicly available information and does not contain classification markings]

[18] [ACSAC | Rrushi & Others | "A Quantitative Evaluation of the Target Selection of Havex ICS Malware Plugin" | 2015 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

[19] [Hybrid Analysis | "7933809aecb1a9d2110a6fd8a18009f2d9c58b3c7dbda770251096d4fcc18849" | https://www.hybrid-analysis.com/sample/7933809aecb1a9d2110a6fd8a18009f2d9c58b3c7dbda770251096d4fcc18849/5f86585c401535319c375515 | 14 October 2020 | Accessed on 25 April 2022 | This source is publicly available and does not contain classification markings]

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

[21] [FireEye | Kyle Wilhoit| "Havex, It's Down With OPC" | https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html | 17 July 2014 | Accessed on 2 April 2022 | The source is publicly available information and does not contain classification markings]

[22] [ACSAC | Rrushi & Others | "A Quantitative Evaluation of the Target Selection of Havex ICS Malware Plugin" | 2015 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

[23] [FireEye | Kyle Wilhoit| "Havex, It's Down With OPC" | https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html | 17 July 2014 | Accessed on 2 April 2022 | The source is publicly available information and does not contain classification markings]

[24] IBID

[25] [S4 Events | Kyle Wilhoit | "ICS Malware: Havex and Black Energy" | https://www.youtube.com/watch?v=eywmb7UDODY | 7 August 2019 | Accessed on 20 April 2022| Source is publicly available]

[26] IBID

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

[28] [S4 Events | Corey Thuen | "Havex Deep Dive" | https://www.youtube.com/watch?v=SyupAcnURtA | 3 September 2017 | Accessed on 21 March 2022 | Sources is publicly available information and does not contain classification markings]

[29] [Belden | Joel Langill | “Defending Against the Dragonfly Cyber Security Attacks” | "https://www.belden.com/hubfs/resources/knowledge/white-papers/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks-AB_Original_68751.pdf?hsLang=en" | 22 October 2014 | Accessed on 21 March 2022 | The source is publicly available information and does not contain classification markings]

[30] [S4 Events | Corey Thuen | "Havex Deep Dive" | https://www.youtube.com/watch?v=SyupAcnURtA | 3 September 2017 | Accessed on 21 March 2022 | Sources is publicly available information and does not contain classification markings]

[31] [Cybersecurity Infrastructure Security Agency | "ICS Alert - 14-176-02A" | https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-14-176-02A | 27 June 2014 | Accessed 22 March 2022 | This source is publicly available and does not contain classification markings]

[32] [Cybersecurity Infrastructure Security Agency | "Alert AA22-083A" | https://www.cisa.gov/uscert/ncas/alerts/aa22-083a | 24 March 2022 | Accessed 25 March 2022 | This source is publicly available and does not contain classification markings]

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

[34] [S4 Events | Corey Thuen | "Havex Deep Dive" | https://www.youtube.com/watch?v=SyupAcnURtA | 3 September 2017 | Accessed on 21 March 2022 | Sources is publicly available information and does not contain classification markings]

[35] [S4 Events | Kyle Wilhoit | "ICS Malware: Havex and Black Energy" | https://www.youtube.com/watch?v=eywmb7UDODY | 7 August 2019 | Accessed on 20 April 2022| Source is publicly available]

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

[37] [Cybersecurity Infrastructure Security Agency | "ICS Alert - 14-176-02A" | https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-14-176-02A | 27 June 2014 | Accessed 22 March 2022 | This source is publicly available and does not contain classification markings]

[38] [Cybersecurity Infrastructure Security Agency | "Alert AA22-083A" | https://www.cisa.gov/uscert/ncas/alerts/aa22-083a | 24 March 2022 | Accessed 25 March 2022 | This source is publicly available and does not contain classification markings]