# PRECUSOR ANALYSIS REPORT: LOCKERGOGA RANSOMWARE ATTACK ON NORSK HYDRO 2019

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-22-69758**

# TABLE OF CONTENTS

# FIGURES

# TABLES

# PRECUSOR ANALYSIS REPORT: LOCKERGOGA RANSOMWARE ATTACK ON NORSK HYDRO 2019

## 1. EXECUTIVE SUMMARY

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

Norsk Hydro is one of the largest energy producers in Norway, powering over 900,000 homes per year. The company is also one of the largest aluminum manufacturers in the world.[1] On 18 March 2019, adversaries used a malware known as LockerGoga to carry out an attack on the company. The attack began when adversaries used a spoofed customer account to engage a Norsk Hydro employee, deceiving the victim into downloading a malicious attachment through a spearphishing email.

LockerGoga propagated across the victim network, causing Norsk Hydro to shut down over 23,000 PCs and 3,000 servers.[2] The company's 35,000 employees worked manually for approximately three weeks following the attack to complete tasks typically facilitated by both Information Technology (IT) and Operational Technology (OT) systems.[3] Norsk Hydro began to recover approximately four weeks after the attack, which cost the company over $71 million in losses.[4] Norsk Hydro decided not to pay the ransom demanded by the adversaries and instead planned to recover data through cloud backups, with full recovery taking over a year. The financial loss and impact on operations caused the company to implement significant changes to its cybersecurity processes and operational practices.

Researchers and analysts identified 13 unique techniques during the attack with a total of 157 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. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Eight of the identified techniques used during the Norsk Hydro cyber attack were precursors to the triggering event. Case study analysis identified 123 observables associated with these precursor techniques, 105 of which were assessed to have an increased likelihood of being perceived in the 30 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

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

# 2. INTRODUCTION

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

## 2.1. APPLYING THE CYOTE METHODOLOGY

The CyOTE methodology, as shown in Figure 1, 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.

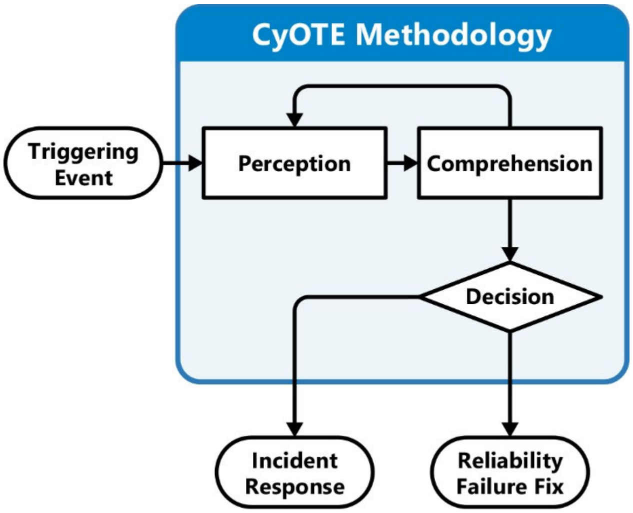


*Figure 1. CyOTE Methodology*

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 for practitioners and developers to support the comprehension of indicators of attack.

## 2.2. BACKGROUND ON THE ATTACK

Adversaries gained initial access to the Norsk Hydro network through a spearphishing email three months (D-90) before the Service Stop (D-0) triggering event on 18 March 2019.[5] The spearphishing email attachment, with embedded LockerGoga malware, provided the adversaries with initial access to the company's network.

LockerGoga propagated across Norsk Hydro's network, encrypting files and data. An operator working at the extrusion plant was the first to notice a ransom note on a desktop machine at 10:45 PM[a] on 18 March (D-0).[6] The extrusion plant experienced the largest financial losses among the Norsk Hydro subsidiaries operating across 50 countries.[7]

At about 3:00 AM on 19 March (H+5), Norsk Hydro's Head of Enterprise Service Management made the decision to shut down over 23,000 PCs and 3,000 servers.[8]

CyOTE analysts assess that Norsk Hydro achieved comprehension of the attack on 19 March (D+1), when company officials held a press conference and announced they would not pay the ransom.[9]

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

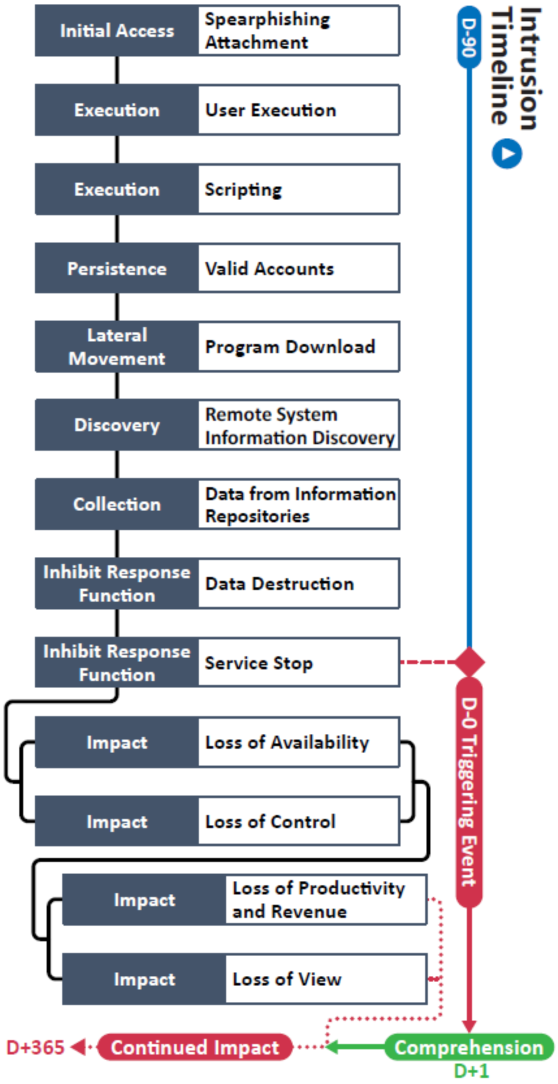


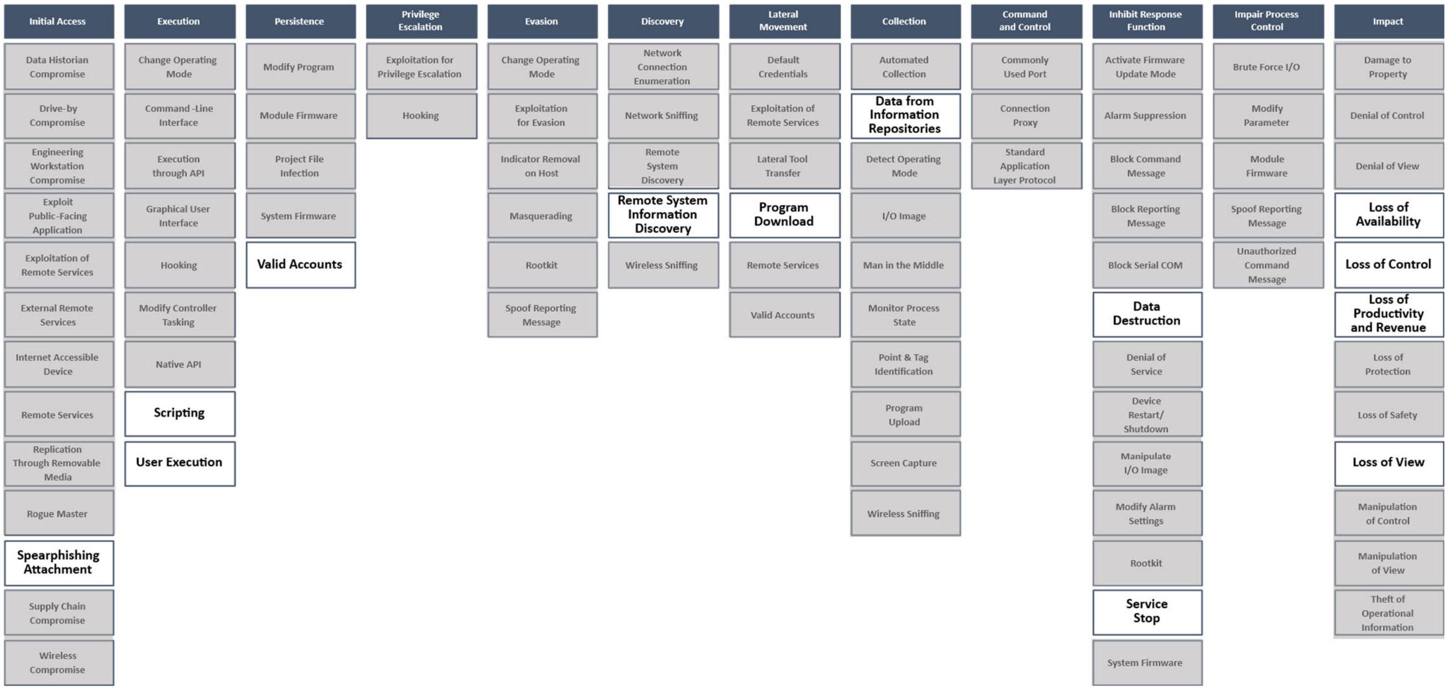
*Figure 2. Intrusion Timeline*

Norsk Hydro's 35,000 employees carried out both Information Technology (IT) and OT tasks manually for nearly a month (D+30) after the attack and were unable to fully recover all business areas until over a year later (D+365).[10] The attack on Norsk Hydro cost the company over $71 million in losses.[11]

Analysis identified 13 unique techniques in a sequence and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

[a] All times given are for GMT/UTC.

***Table 1. Techniques Used in the Norsk Hydro Cyber Attack***



| Initial Access | Execution | Persistence | Privilege Escalation | Evasion | Discovery | Lateral Movement | Collection | Command and Control | Inhibit Response Function | Impair Process Control | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Data Historian Compromise | Change Operating Mode | Modify Program | Exploitation for Privilege Escalation | Change Operating Mode | Network Connection Enumeration | Default Credentials | Automated Collection | Commonly Used Port | Activate Firmware Update Mode | Brute Force I/O | Damage to Property |
| Drive-by Compromise | Command -Line Interface | Module Firmware | Hooking | Exploitation for Evasion | Network Sniffing | Exploitation of Remote Services | **Data from Information Repositories** | Connection Proxy | Alarm Suppression | Modify Parameter | Denial of Control |
| Engineering Workstation Compromise | Execution through API | Project File Infection | | Indicator Removal on Host | Remote System Discovery | Lateral Tool Transfer | Detect Operating Mode | Standard Application Layer Protocol | Block Command Message | Module Firmware | Denial of View |
| Exploit Public-Facing Application | Graphical User Interface | System Firmware | | Masquerading | **Remote System Information Discovery** | **Program Download** | I/O Image | | Block Reporting Message | Spoof Reporting Message | **Loss of Availability** |
| Exploitation of Remote Services | Hooking | **Valid Accounts** | | Rootkit | Wireless Sniffing | Remote Services | Man in the Middle | | Block Serial COM | Unauthorized Command Message | **Loss of Control** |
| External Remote Services | Modify Controller Tasking | | | Spoof Reporting Message | | Valid Accounts | Monitor Process State | | **Data Destruction** | | **Loss of Productivity and Revenue** |
| Internet Accessible Device | Native API | | | | | | Point & Tag Identification | | Denial of Service | | Loss of Protection |
| Remote Services | **Scripting** | | | | | | Program Upload | | Device Restart/ Shutdown | | Loss of Safety |
| Replication Through Removable Media | **User Execution** | | | | | | Screen Capture | | Manipulate I/O Image | | **Loss of View** |
| Rogue Master | | | | | | | Wireless Sniffing | | Modify Alarm Settings | | Manipulation of Control |
| **Spearphishing Attachment** | | | | | | | | | Rootkit | | Manipulation of View |
| Supply Chain Compromise | | | | | | | | | **Service Stop** | | Theft of Operational Information |
| Wireless Compromise | | | | | | | | | System Firmware | | |

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

| Precursor Analysis Report Quantitative Summary | Totals |
|---|---|
| **MITRE ATT&CK® for ICS Techniques** | **13** |
| **Technique Observables** | **157** |
| **Precursor Techniques** | **8** |
| **Precursor Technique Observables** | **123** |
| **Highly Perceivable Precursor Technique Observable** | **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. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS

Approximately three months before the attack, adversaries sent a spearphishing attachment to a Norsk Hydro employee from a spoofed customer account, mirroring a legitimate employee conversation with customers.[12] The attachment contained LockerGoga, a trojan malware.

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

A total of seven observables were identified with the use of the Spearphishing Attachment technique (T0865). This technique is important for investigation because it allows adversaries to gain initial access. 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 gaining access to the system.

Of the seven observables associated with this technique, six are assessed to be highly perceivable (Anomalous Email with Attachment; Email Attachment with Anomalous Embedded Scripts; Email with Anomalous Word Document; Email with Anomalous Word Document with Object Linking and Embedding (OLE); Email with Anomalous Excel File; Email with Anomalous Excel File with Object Linking and Embedding (OLE)).

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] | IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, 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. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

A Norsk Hydro employee likely opened the spearphishing email and unknowingly executed the infected attachment two to three weeks prior to the triggering event (18 March 2019), granting adversaries access to the network.[13]

LockerGoga initially downloads malicious executables into the %TEMP% folder on the host machine. The malware then creates a file in the %TEMP% folder with the following schema: %TEMP%\svc{random}.{random number}.exe. LockerGoga also creates another file in the %TEMP% folder with the following schema: File e%TEMP%\tgytutrc{4 Random Numbers}.exe. An anomalous process is spawned from a binary renamed from PsExec with the -m parameter. LockerGoga then executes both folders, which spawn up a primary and several secondary processes.[14] The primary process leverages the Boost InterProcess Communication (IPC) Library to communicate with the secondary processes through writes to shared memory space. The primary process searches for files to encrypt, passing the paths of these selected files to the secondary processes through the shared memory space via the IPC method. The secondary processes take these paths and perform the encryption on each file path passed by the primary process.

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe the LockerGoga malware, email attachment, and associated processes.

A total of 13 observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation because it allows malware access to the host. This technique will generate anomalous files and directories on the host. This technique modifies the host operating system files via the download and installation of the LockerGoga malware, placing the host into a modified or compromised state. This technique also appears relatively early in the timeline and responding to it would effectively halt the adversaries' lateral movement. Terminating the chain of techniques at this point would prevent the malware from infecting the host, limiting operational damage in both the IT and OT environments.

Of the 13 observables associated with this technique, eight are assessed to be highly perceivable (Anomalous Access from External Host; Anomalous Remote Process Execution Using Renamed PsExec; Creation of Anomalous Executable Files in %TEMP%\svc{random}.{random number}.exe; Anomalous File Execution from %TEMP%\svc{random}.{random number}.exe-{random} -{random} {random}; Anomalous File Execution from %TEMP%\tgytutrc{4 Random Numbers}.exe; Anomalous Process Spawned from PsExec with the -m Parameter; Anomalous Process Spawned from Anomalous Binary Renamed from PsExec with the -m Parameter; A New Process Has Been Created Windows Event Log (Windows Event ID 4688)).

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** | IT Staff, IT Cybersecurity, OT Cybersecurity |

## 3.3. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

Once installed, LockerGoga can modify the user's credentials using Mimikatz, Cobalt Strike, PsExec, and Metasploit, allowing adversaries to access privileged accounts within the network.[15,16] Malware analysis revealed that a renamed PsExec tool was dropped and executed, generating logins into the "usual subject" Windows Event Log and pulling administrative rights within Windows Active Directory (AD).[17] CyOTE analysis has determined successful and failed login attempts in the Windows AD likely could have been observed within the Norsk Hydro network displaying Event ID 4624 if login was successful or if login failure occurred.

PsExec displays two Event IDs, 4697 for a new service installation and 7045 for a new service creation on the local machine.[18] CyOTE analysis determined that adversaries likely attempted to change the target user account's password. Event ID 4723 is triggered when a user attempts to change their own user password and displays it in the Windows AD. Each time adversaries encrypt a file with LockerGoga the Current User HKEY is modified. LockerGoga leaves a ransom note in a file named README_LOCKED.txt within the desktop folder.[19] In the case of Norsk Hydro, employees found this ransom note on an infected desktop workstation.[20]

IT Staff, IT Cybersecurity, and Support Staff personnel may have been able to observe the tools, Windows Event IDs, and commands associated with LockerGoga.

A total of 25 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because the system event logs in the AD could have potentially notified observers of the Norsk Hydro network intrusion. This technique also modifies the host operating system files via the creation of anomalous services and modification of user accounts, resulting in the host being placed into a modified or compromised state. This technique appears early in the attack timeline and responding to it will disrupt further infection of a network. Terminating the chain of techniques at this point would limit adversaries' ability to cause operational damage with LockerGoga malware.

Of the 25 observables associated with this technique, 17 are assessed to be highly perceivable as indicated in Appendix A.[c]

| 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, Support Staff |

[c] For purposes of clarity, excessively long lists of highly perceivable observables will be listed only in the associated technique tables in Appendix A, rather than in the technique narrative sections.

## 3.4. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

The LockerGoga malware compromised standard user accounts within the Norsk Hydro network, eventually gaining privileges to control the entire IT infrastructure.[21,22]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous traffic between Norsk Hydro's systems and unknown external IP addresses.

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

Of the five observables associated with this technique, three are assessed to be highly perceivable (Anomalous Interactive Successful Logons (Windows Event ID 4624 Type 3 or 10); An Account Was Successfully Logged on Windows Log Event (Windows Event ID 4624); Special Privileges Assigned to New Logon Windows Log Event (Windows Event ID 4672)).

Please see Appendix A for the list of observables.

| 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 |

## 3.5. PROGRAM DOWNLOAD TECHNIQUE (T0843) FOR LATERAL MOVEMENT

Adversaries can install LockerGoga by equipping the malicious email attachment with an executable capable of downloading programs. In the case of the attack on Norsk Hydro, LockerGoga's payload likely sat dormant on an infected computer on the company's network for two to three weeks before the first ransom note appeared on the night of 18 March.[23]

LockerGoga downloads different processes to perform and accelerate file encryption within the system.[24] In addition, adversaries downloaded Metaspolit and Cobalt Strike to pivot to other systems within Norsk Hydro's network and used Mimikatz to gather user credentials.[25]

LockerGoga malware demonstrates unusual Central Processing Unit (CPU) behavior due to its ability to utilize all available CPU resources.[26] LockerGoga's main access point is Windows AD domain services through the Domain Controller.[27]

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe the downloading of Metasploit, Mimikatz, and Cobalt Strike. Personnel may have also observed unusual CPU activity.

A total of 18 observables were identified with the use of the Program Download technique (T0843). This technique is important for investigation because it enables LockerGoga to perform file encryption, concealing content information with code. Through downloading of various modules, LockerGoga is able to perform file encryption. This technique modifies the host operating system files via the creation of anomalous services and modification of user accounts, placing the host into a modified or compromised state. This technique appears in the middle of the timeline and responding to it will prevent the installation of additional malware. Terminating the chain of techniques at this point would prevent the compromise of host devices.

Of the 18 observables associated with this technique, 9 are assessed to be highly perceivable (Anomalous Application Event Log Entries; Application Event Log Entries Associated with Anomalous Executable; Network Traffic Associated with Anomalous Metasploit Content; Network Traffic Associated with Metasploit Download; Network Traffic Associated with Anomalous Mimkatz Content; Network Traffic Associated with Mimikatz Download; Network Traffic Associated with Anomalous Cobalt Strike Content; Network Traffic Associated with Cobalt Strike Download; Anomalous Increase in System Resource Usage Management (SRUM)).

Please see Appendix A for the list of observables.

| 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, OT Cybersecurity |

## 3.6. REMOTE SYSTEM INFORMATION DISCOVERY TECHNIQUE (T0888) FOR DISCOVERY

Adversaries compromised the Windows AD server, causing Norsk Hydro to lose control of their entire IT infrastructure. Adversaries also used domain controller permissions to compromise all targeted files from the AD endpoints.[28] Associated Event IDs that could be found in the Windows Security Log are 4839 and 5136 to 5141.[29]

Metasploit, Powershell Empire, Cobalt Strike, Mimikatz, and PsExec are all tools associated with the use of LockerGoga malware.[30,31] Adversaries likely utilized PsExec to enable remote execution on the victim, creating copies of itself on various machines. They used Mimikatz and Metasploit to pull credentials from the AD server, PowerShell for remote code execution, and Cobalt Strike for port scanning and for remote service discovery.

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

A total of 12 observables were identified with the use of the Remote System Information Discovery technique (T0888). This technique is important for investigation because it serves as a vector to access additional systems, facilitating the spread of malware beyond the current target. This technique appears in the middle of the timeline and responding to it would likely prevent lateral movement within the environment. Terminating the chain of techniques at this point would prevent LockerGoga from spreading to other systems via lateral movement.

All 12 observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

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

## 3.7. DATA FROM INFORMATION REPOSITORIES TECHNIQUE (T0811) FOR COLLECTION

LockerGoga gathers the victim's information and other identifiable information through the system, likely gathering administrative credentials, changing the user's login, and locking the user out of the system.[32]

IT Staff and IT Cybersecurity personnel may have been able to observe adversaries capturing administrative credentials.

Two observables were identified with the use of the Data from Information Repositories technique (T0811). This technique is important for investigation because the victim could prevent credential harvesting and authorized user lock-out. This technique appears in the middle of 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.

Both of the observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

| 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 |

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

Adversaries were able to destroy some backups and encrypt data within the Norsk Hydro network. After the victim opened the malicious attachment, the ransomware encrypted files via Crypto++ using RSA-4096 and AES-256 algorithms.[33] The LockerGoga malware encrypts documents, PDFs, spreadsheets, PowerPoint files, database files, videos, JavaScript, and Python files.[34] LockerGoga utilizes every CPU core and thread during the encryption process.[35]

LockerGoga leaves a ransom note in a file named README_LOCKED.txt in the desktop folder, which is what Norsk Hydro employees found on a desktop workstation.[36]

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe the file encryption.

A total of 41 observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because it encrypts victim files, rendering systems inoperable and effectively destroying data. This technique necessitates the unplanned restoration of data from backups and can result in unexpected expenses related to data recovery efforts. Appearing relatively late in the timeline, terminating the chain of techniques at this point would limit the destruction of data and resultant business interruptions.

Of the 41 observables associated with this technique, 38 are assessed to be highly perceivable (Anomalously Missing Files with extension bak, iso, doc, dot, docx, docb, dotx, wkb, xlm, xml, xls, xlsx, xlt, xltx, xlw, ppt, pps, pot, ppsx, pptx, posx, potx, sldx, pdf, db, sql, cs, ts, js, py); Hosts in Domain Anomalously Crash; Hosts Throw Error Messages; Host System with Anomalously Slow Response Time; Anomalous Increase in System Resource Usage Management (SRUM); Anomalously High System CPU Utilization; Anomalous Creation of Text File; Anomalous Creation of README_LOCKED.txt File).

Please see Appendix A for the list of observables.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** **(See Appendix B)** | A total of 27 artifacts could be generated by the Data Destruction technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Cybersecurity |

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

An operator was the first employee to notice the ransomware note on a PC at the Magnor extrusion plant, one of Norsk Hydro's 160 sites. The operator found the note at approximately 10:45 PM on 18 March.[37] Early on 19 March, Norsk Hydro's Head of Enterprise Service Management made the executive decision to shut down 23,000 PCs and 3,000 servers across the network.[38] Employees pulled power and network cables from outlets one by one to shut the systems down.[39] To successfully communicate the emergency shutdown internally, the Norsk Hydro communication team used Office 365 to communicate via email.[40] Norsk Hydro continued to spread information by hanging up flyers, posting on websites, and communicating through their social media pages.[41]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe Norsk Hydro's shutdown.

A total of ten observables were identified with the use of the Inhibit Response Function technique (T0881). Appearing late in the timeline, terminating the chain of techniques at this point would limit product and delivery services to Norsk Hydro customers.

All ten observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

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

## 3.10. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

Adversaries deleted and encrypted Human-Machine Interface (HMI) Controls, workstations, and databases.[42] Employees continued operations manually, tracking manufacturing and finances with pen and paper. Employees were only able to connect devices to personal hotspots to provide limited functionality.[43] To avoid further damage the company decided not to pay the ransom, and instead planned to restore data from cloud backups.[44]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe encrypted HMI controls, workstations, and databases.

A total of 14 observables were identified with the use of the Loss of Availability technique (T0826). This technique is important for investigation because it prevents owners and operators from delivering products or services. This technique also presents noticeable effects, resulting in unresponsive equipment and limited network functionality. Appearing late in the timeline, terminating the chain of techniques at this point would limit the ability of LockerGoga to encrypt proprietary information.

All 14 observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

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

## 3.11. LOSS OF CONTROL TECHNIQUE (T0827) FOR IMPACT

Nearly 35,000 Norsk Hydro employees lost control of their workstations, networks, and servers on 19 March when the company shut down its network.[45]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe control loss over workstations, networks, and servers.

A total of five observables were identified with the use of the Loss of Control technique (T0827). This technique is important for investigation because it prevents owners and operators from issuing commands to equipment. This technique also presents noticeable effects, particularly unresponsive equipment. Appearing after the triggering event, terminating the chain of techniques at this point would not limit destruction or business impacts.

All five observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts (See Appendix B)** | A total of 13 artifacts could be generated by the Loss of Control technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management |

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

Nearly a month after the cyber attack, the majority of Norsk Hydro's 160 business segments were still operating manually. The company suffered financial losses of approximately $71 million, primarily in revenues from its Extruded Solutions business division, which was the most impacted by the ransomware attack.[46]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe manual operations and revenue loss.

A total of two observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation because it involves a direct loss of revenue and productivity for the victim. Additionally, this technique may present an impact for the end users or consumers of products and services. Terminating the chain of techniques at this point would not limit destruction or business impacts.

Both observables are assessed to be highly perceivable.

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 Loss of Productivity and Revenue technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management |

## 3.13. LOSS OF VIEW TECHNIQUE (T0829) FOR IMPACT

With the executive decision to shut down 23,000 PCs and 3,000 servers within the network, employees had to resort to manual operations for nearly a month, as they were unable to connect to their production systems.[47]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe the loss of view to operational systems.

A total of three observables were identified with the use of the Loss of View technique (T0829). This technique is important for investigation as it prevents owners and operators from delivering products or services. This technique also presents noticeable effects, such as non-responsive equipment. This technique appears at the end of the timeline, beyond the point at which a defender could take action to disrupt the attack.[48]

All three observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

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

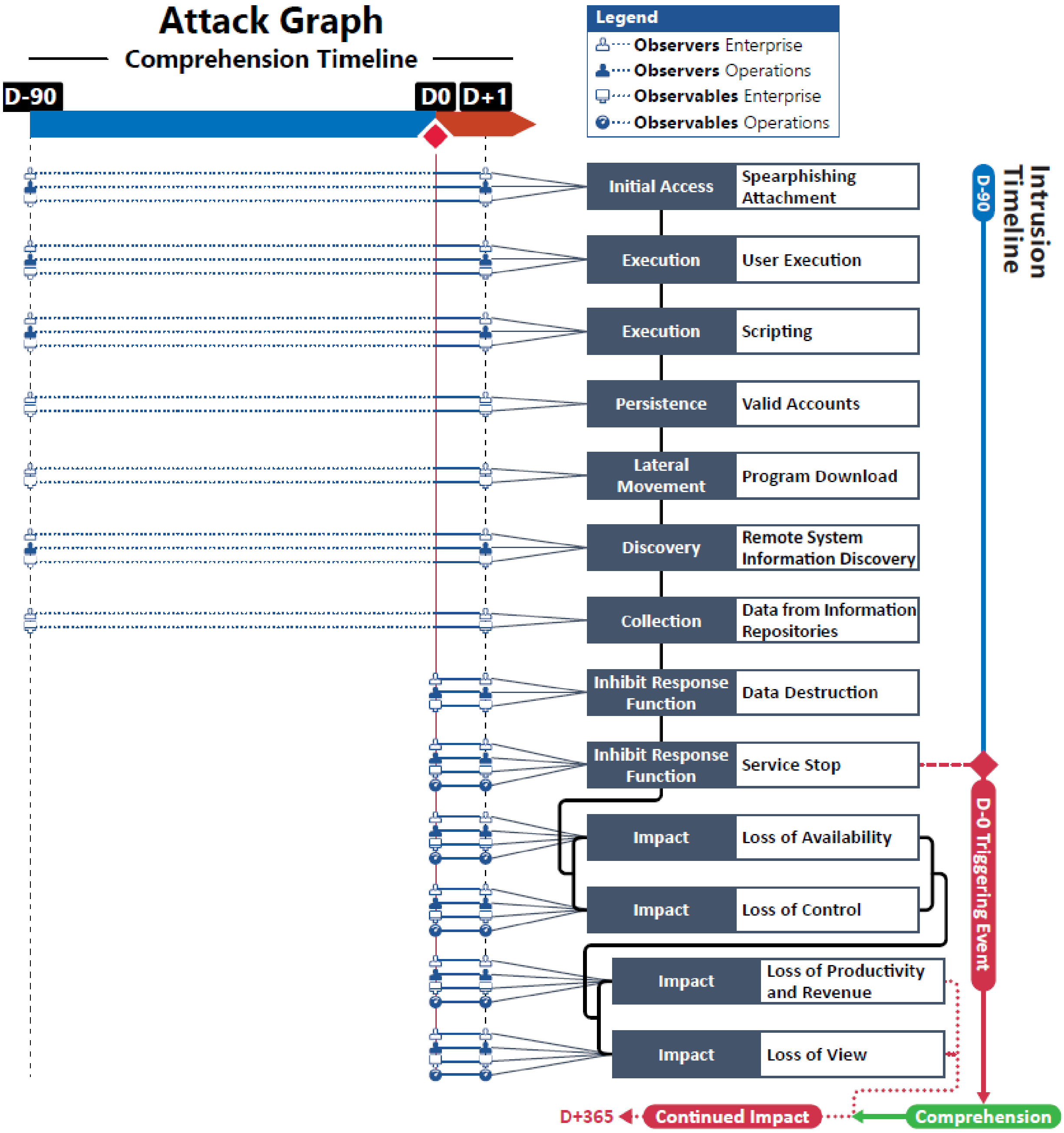


*Figure 3. Attack Graph*

# APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

| Observables Associated with Spearphishing Attachment Technique (T0865) | |
|---|---|
| **Observable 1** | *Anomalous Email with Attachment* |
| **Observable 2** | *Email Attachment with Anomalous Embedded Scripts* |
| **Observable 3** | Anomalous SMTP Traffic Over TCP Port 25 |
| **Observable 4** | *Email with Anomalous Word Document* |
| **Observable 5** | *Email with Anomalous Word Document with Object Linking and Embedding (OLE)* |
| **Observable 6** | *Email with Anomalous Excel File* |
| **Observable 7** | *Email with Anomalous Excel File with Object Linking and Embedding (OLE)* |

| Observables Associated with User Execution Technique (T0863) | |
|---|---|
| **Observable 1** | *Anomalous Access from External Host* |
| **Observable 2** | Anomalous User Collecting Credentials |
| **Observable 3** | Anomalous Remote Process Execution |
| **Observable 4** | *Anomalous Remote Process Execution Using Renamed PsExec* |
| **Observable 5** | Creation of Anomalous Executable Files |
| **Observable 6** | *Creation of Anomalous Executable Files in %TEMP%\svc{random}.{random number}.exe* |
| **Observable 7** | Anomalous File Execution |
| **Observable 8** | *Anomalous File Execution from %TEMP%\svc{random}.{random number}.exe-{random} -{random} {random}* |
| **Observable 9** | *Anomalous File Execution from %TEMP%\tgytutrc{4 Random Numbers}.exe* |
| **Observable 10** | *Anomalous Process Spawned from PsExec with the -m Parameter* |
| **Observable 11** | *Anomalous Process Spawned from Anomalous Binary Renamed from PsExec with the -m Parameter* |
| **Observable 12** | File Creation Windows Event Log (Sysmon Event ID: 11) |
| **Observable 13** | *A New Process Has Been Created Windows Event Log (Windows Event ID 4688)* |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| **Observable 1** | Anomalous Traffic over TCP port 135 |
| **Observable 2** | *Anomalous Traffic over TCP port 135 Associated with PsExec* |
| **Observable 3** | *Anomalous Traffic over TCP port 44* |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| **Observable 4** | *Anomalous Traffic over TCP port 44 Associated with PsExec* |
| **Observable 5** | Anomalous Renamed PsExec Executable Downloaded to Internal Host |
| **Observable 6** | *A User Account was Successfully Logged on (Windows Event ID 4624)* |
| **Observable 7** | *A User Account Failed to Log on (Windows Event ID 4625)* |
| **Observable 8** | *A Service was Installed in the System (Windows Event ID 4697)* |
| **Observable 9** | *A New Service was Installed in the System (Windows Event ID 7045)* |
| **Observable 10** | Anomalous Execution of Command |
| **Observable 11** | Anomalous Execution of "task kill" Command |
| **Observable 12** | *Anomalous Processes Killed* |
| **Observable 13** | *Anomalous Anti-Virus Process Killed* |
| **Observable 14** | *Anomalous Execution of Script* |
| **Observable 15** | *Anomalous Execution of Logoff.exe Script* |
| **Observable 16** | *Anomalous Modification of Registry Key* |
| **Observable 17** | *Anomalous Modification of Registry Key: (HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session00{01-20})* |
| **Observable 18** | Anomalous Creation of File |
| **Observable 19** | *Anomalous Creation of File Named README_LOCKED.txt* |
| **Observable 20** | Anomalous TCP Traffic Over Port 445 |
| **Observable 21** | *Anomalous TCP Traffic Over Port 445 Associated with Mimikatz* |
| **Observable 22** | *An Account was Successfully Logged on Windows Log Event (Windows Event ID 4624)* |
| **Observable 23** | *Special Privileges Assigned to New Logon Windows Log Event (Windows Event ID 4672)* |
| **Observable 24** | Anomalous Executable Download |
| **Observable 25** | Anomalous mimikatz.exe Executable Download |

| Observables Associated with Valid Accounts Technique (T0859) | |
|---|---|
| **Observable 1** | *Anomalous Interactive Successful Logons (Windows Event ID 4624 Type 3 or 10)* |
| **Observable 2** | Anomalous Access to Administrator Credential Hashes |
| **Observable 3** | Anomalous System Logon Event Timestamp |
| **Observable 4** | *An Account was Successfully Logged on Windows Log Event (Windows Event ID 4624)* |
| **Observable 5** | *Special Privileges Assigned to New Logon Windows Log Event (Windows Event ID 4672)* |

| Observables Associated with Program Download (T0843) | |
|---|---|
| **Observable 1** | *Anomalous Application Event Log Entries* |
| **Observable 2** | *Application Event Log Entries Associated with Anomalous Executable* |
| **Observable 3** | Anomalous File Installed |
| **Observable 4** | Anomalous File Installed Associated with LockerGoga |
| **Observable 5** | Anomalous Network Traffic Content |
| **Observable 6** | *Network Traffic Associated with Anomalous Metasploit Content* |
| **Observable 7** | Anomalous Network GET Request to an External Source |
| **Observable 8** | Network Traffic Associated with Anomalous Executable Download |
| **Observable 9** | *Network Traffic Associated with Metasploit Download* |
| **Observable 10** | *Network Traffic Associated with Anomalous Mimikatz Content* |
| **Observable 11** | Anomalous Network GET Request to an External Source |
| **Observable 12** | Network Traffic Associated with Anomalous Executable Download |
| **Observable 13** | *Network Traffic Associated with Mimikatz Download* |
| **Observable 14** | *Network Traffic Associated with Anomalous Cobalt Strike Content* |
| **Observable 15** | Anomalous Network GET Request to an External Source |
| **Observable 16** | Network Traffic Associated with Anomalous Executable Download |
| **Observable 17** | *Network Traffic Associated with Cobalt Strike Download* |
| **Observable 18** | *Anomalous Increase in System Resource Usage Management (SRUM)* |

| Observables Associated with Remote System Information Discovery Technique (T0888) | |
|---|---|
| **Observable 1** | *Anomalous Internal Network Communication to Windows AD Domain Controller* |
| **Observable 2** | *Anomalous User Accessing Domain Controller* |
| **Observable 3** | *Anomalous User Attempted to Validate Credentials for An Account (Windows 4776)* |
| **Observable 4** | *A Domain Policy Was Changed to Domain Controller (Windows Event ID 4739)* |
| **Observable 5** | *Network Traffic Associated with Metasploit Download* |
| **Observable 6** | *Network Traffic Associated with Mimikatz Download* |
| **Observable 7** | *Anomalous Network Scanning Traffic Associated with Cobalt Strike Download* |
| **Observable 8** | *Anomalous Code Execution Across Internal Domain* |
| **Observable 9** | *Anomalous Code Execution Across Internal Domain Associated with PowerShell* |
| **Observable 10** | *Anomalous Traffic over TCP port 135 Associated with PsExec from Domain Controller to Host on Internal Domain* |
| **Observable 11** | *Anomalous Traffic over TCP port 44 Associated with PsExec from Domain Controller to Host on Internal Domain* |

| Observables Associated with Remote System Information Discovery Technique (T0888) | |
|---|---|
| **Observable 12** | *A Directory Service Object Was Modified Event (Windows Event ID 5136)* |

| Observables Associated with Data from Information Repositories Technique (T0811) | |
|---|---|
| **Observable 1** | *Anomalous Account Logon Information Changed (Windows Event ID 5136)* |
| **Observable 2** | *Anomalous Increase in User Account Logon Failures (Windows Event ID 4625)* |

| Observables Associated with Data Destruction Technique (T0809) | |
|---|---|
| **Observable 1** | *Anomalously Missing Backup Files .bak* |
| **Observable 2** | *Anomalously Missing Image Files .iso* |
| **Observable 3** | Anomalously Missing Files |
| **Observable 4** | *Anomalously Missing Files with Extension (.doc)* |
| **Observable 5** | *Anomalously Missing Files with Extension (.dot)* |
| **Observable 6** | *Anomalously Missing Files with Extension (.docx)* |
| **Observable 7** | *Anomalously Missing Files with Extension (.docb)* |
| **Observable 8** | *Anomalously Missing Files with Extension (.dotx)* |
| **Observable 9** | *Anomalously Missing Files with Extension (.wkb)* |
| **Observable 10** | *Anomalously Missing Files with Extension (.xlm)* |
| **Observable 11** | *Anomalously Missing Files with Extension (.xml)* |
| **Observable 12** | *Anomalously Missing Files with Extension (.xls)* |
| **Observable 13** | *Anomalously Missing Files with Extension (.xlsx)* |
| **Observable 14** | *Anomalously Missing Files with Extension (.xlt)* |
| **Observable 15** | *Anomalously Missing Files with Extension (.xltx)* |
| **Observable 16** | *Anomalously Missing Files with Extension (.xlw)* |
| **Observable 17** | *Anomalously Missing Files with Extension (.ppt)* |
| **Observable 18** | *Anomalously Missing Files with Extension (.pps)* |
| **Observable 19** | *Anomalously Missing Files with Extension (.pot)* |
| **Observable 20** | *Anomalously Missing Files with Extension (.ppsx)* |
| **Observable 21** | *Anomalously Missing Files with Extension (.pptx)* |
| **Observable 22** | *Anomalously Missing Files with Extension (.posx)* |
| **Observable 23** | *Anomalously Missing Files with Extension (.potx)* |
| **Observable 24** | *Anomalously Missing Files with Extension (.sldx)* |
| **Observable 25** | *Anomalously Missing Files with Extension (.pdf)* |
| **Observable 26** | *Anomalously Missing Files with Extension (.db)* |
| **Observable 27** | *Anomalously Missing Files with Extension (.sql)* |

| **Observables Associated with Data Destruction Technique (T0809)** | |
|---|---|
| **Observable 28** | *Anomalously Missing Files with Extension (.cs)* |
| **Observable 29** | *Anomalously Missing Files with Extension (.ts)* |
| **Observable 30** | *Anomalously Missing Files with Extension (.js)* |
| **Observable 31** | *Anomalously Missing Files with Extension (.py)* |
| **Observable 32** | *Hosts in Domain Anomalously Crash* |
| **Observable 33** | *Hosts Throw Error Messages* |
| **Observable 34** | *Host System with Anomalously Slow Response Time* |
| **Observable 35** | *Anomalous Increase in System Resource Usage Management (SRUM)* |
| **Observable 36** | *Anomalously Hight System CPU Utilization* |
| **Observable 37** | Anomalous Call to Encryption Library |
| **Observable 38** | Anomalous Call to Crypto++ Encryption Library |
| **Observable 39** | Anomalous Call to RSA-2096 and AES-256 Encryption Libraries |
| **Observable 40** | *Anomalous Creation of Text File* |
| **Observable 41** | *Anomalous Creation of README_LOCKED.txt File* |

| **Observables Associated with Service Stop Technique (T0881)** | |
|---|---|
| **Observable 1** | *Host Systems Shut Down for Extended Period of Time* |
| **Observable 2** | *23,000 Host Systems Shut Down for Extended Period of Time (30 days)* |
| **Observable 3** | *Network Servers Shut Down for Extended Period of Time* |
| **Observable 4** | *3,000 Network Servers Shut Down for Extended Period of Time (30 days)* |
| **Observable 5** | *Information Technology Processes Anomalously Fail* |
| **Observable 6** | *Operational Technology Processes Anomalously Fail* |
| **Observable 7** | *Information Technology Applications Anomalously Fail* |
| **Observable 8** | *Operational Technology Applications Anomalously Fail* |
| **Observable 9** | *Host Shutdown Event (Windows Event ID 4609)* |
| **Observable 10** | *Specific Windows Service Stopped (Windows Event ID 7040)* |

| **Observables Associated with Loss of Availability Technique (T0826)** | |
|---|---|
| **Observable 1** | *HMI Controls Unavailable* |
| **Observable 2** | *HMI Controls Unavailable for 30 days* |
| **Observable 3** | *Network Communication Unavailable* |
| **Observable 4** | *Network Communication Unavailable for 30 days* |
| **Observable 5** | *Host Applications Failing to Run* |
| **Observable 6** | *Server Applications Failing to Run* |

| Observables Associated with Loss of Availability Technique (T0826) | |
|---|---|
| **Observable 7** | *Host Applications Failing to Run for 30 days* |
| **Observable 8** | *Server Applications Failing to Run for 30 days* |
| **Observable 9** | *Inability to Utilize Services Within the IT Network* |
| **Observable 10** | *Inability to Utilize Services Within the IT Network for 30 days* |
| **Observable 11** | *Inability to Access Systems Within the OT Network* |
| **Observable 12** | *Inability to Access Systems Within the OT Network for 30 days* |
| **Observable 13** | *Encrypted System Files* |
| **Observable 14** | *Failed Attempt to Start Normal Functions* |

| Observables Associated with Loss of Control Technique (T0827) | |
|---|---|
| **Observable 1** | *Emergency Shutdown Initiated for 30 days* |
| **Observable 2** | *Manual Operations for 30 days* |
| **Observable 3** | *Systems Remotely Inaccessible/Not Responsive for 30 days* |
| **Observable 4** | *Host Shutdown Event (Windows Event ID 4609)* |
| **Observable 5** | *Specific Windows Service Stopped (Windows Event ID 7040)* |

| Observables Associated with Loss of Productivity and Revenue Technique (T0828) | |
|---|---|
| **Observable 1** | *Network Shut Down for Approximately Three Weeks* |
| **Observable 2** | *Approximately $71 Million Lost in Revenue* |

| Observables Associated with Loss of View Technique (T0829) | |
|---|---|
| **Observable 1** | *Loss of View of 23,000 PCs* |
| **Observable 2** | *Loss of View of 3,000 Servers* |
| **Observable 3** | *Loss of View of OT Operations* |

# APPENDIX B: ARTIFACTS LIBRARY

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

| Artifacts Associated with User Execution Technique (T0863) | |
|---|---|
| **Artifact 1** | Command Execution |
| **Artifact 2** | Service Termination |

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

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

| Artifacts Associated with Scripting Technique (T0853) | |
|---|---|
| **Artifact 12** | Windows API Event Log |

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

| Artifacts Associated with 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 |
| **Artifact 14** | Authentication Success |

| Artifacts Associated with Data from Information Repositories Technique (T0811) | |
|---|---|
| **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 Data Destruction Technique (T0809) | |
|---|---|
| **Artifact 1** | Command Line Arguments |
| **Artifact 2** | Files Moved to Recycle Bin |
| **Artifact 3** | Missing Files |
| **Artifact 4** | Host System Reboot Failure |
| **Artifact 5** | Process Logic Failure |
| **Artifact 6** | Event Log Creation |
| **Artifact 7** | System Call |
| **Artifact 8** | System Application Interruption |
| **Artifact 9** | Device Failure |
| **Artifact 10** | Recovery Attempt Failure |
| **Artifact 11** | TFTP Port |

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

| Artifacts Associated with Service Stop Technique (T0881) | |
|---|---|
| **Artifact 1** | Internal System Logs |
| **Artifact 2** | Alarm Event |
| **Artifact 3** | OS API Call |
| **Artifact 4** | Application Error Messages |
| **Artifact 5** | Process Error Messages |
| **Artifact 6** | Application Service Stop |
| **Artifact 7** | Registry Change HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES |
| **Artifact 8** | OS Service Crash |
| **Artifact 9** | System Event Logs |
| **Artifact 10** | Application Event Logs |
| **Artifact 11** | System Resource Usage Manager Application Usage Change |
| **Artifact 12** | Command Line System Argument |
| **Artifact 13** | Process Failure |

| Artifacts Associated with Loss of Availability Technique (T0826) | |
|---|---|
| **Artifact 1** | Process Failure Due to Loss of Required Network or System Dependency |

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

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

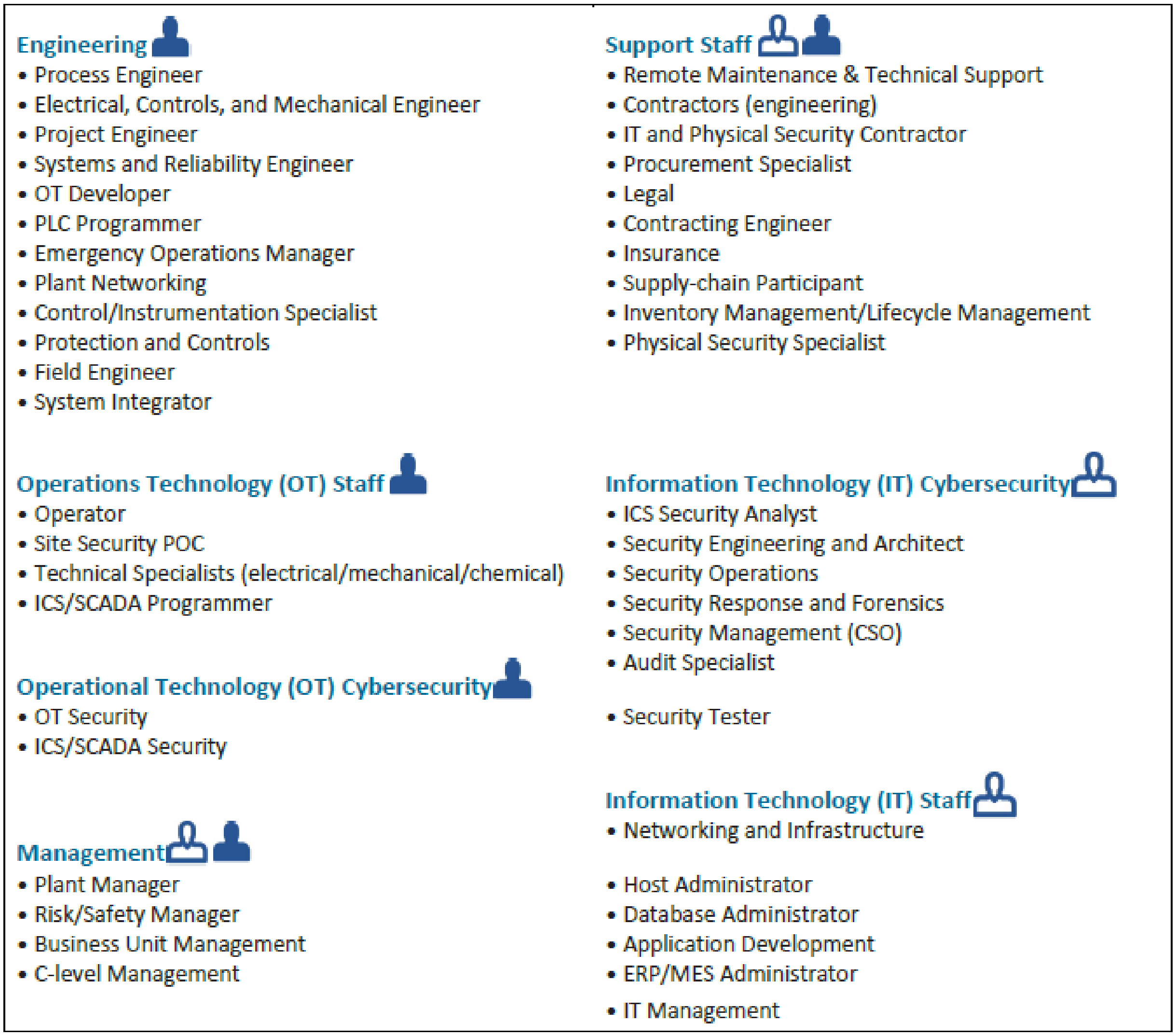
| Artifacts Associated with Loss of Productivity and Revenue Technique (T0828) | |
|---|---|
| **Artifact 1** | Loss of Confidence in a Safety System Due to Unreliability Might Result in a Risk Management Driven Shutdown of a Plant |
| **Artifact 2** | Wormable or Other Highly Propagating Malware Might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

| | |
|---|---|
| **Artifact 5** | File System Modification Artifacts Might Be Associated with The Loss of Productivity and Revenue Attack Might Be Present on Disk |

| **Artifacts Associated with Loss of View Technique (T0829)** | |
|---|---|
| **Artifact 1** | Blocking Communications Paths and Channels (Comms, Network Infrastructure, Host Packet Routing) Might Occur via an OS or Device Modification |
| **Artifact 2** | Masked Reconfiguration of Alarm Thresholds or Other Configuration Settings Might Result in Unexpected Lack of Situational Awareness |
| **Artifact 3** | File System Modification Artifacts Might Be Associated with The Loss of View Attack Might Be Present on Disk |
| **Artifact 4** | Application Logic Hooks or Modifications Might Prevent Proper Reporting to/from an Industrial Application |

# 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.



Engineering

- Process Engineer
- Electrical, Controls, and Mechanical Engineer
- Project Engineer
- Systems and Reliability Engineer
- OT Developer
- PLC Programmer
- Emergency Operations Manager
- Plant Networking
- Control/Instrumentation Specialist
- Protection and Controls
- Field Engineer
- System Integrator

Operations Technology (OT) Staff

- Operator
- Site Security POC
- Technical Specialists (electrical/mechanical/chemical)
- ICS/SCADA Programmer

Operational Technology (OT) Cybersecurity

- OT Security
- ICS/SCADA Security

Management

- Plant Manager
- Risk/Safety Manager
- Business Unit Management
- C-level Management

Support Staff

- Remote Maintenance & Technical Support
- Contractors (engineering)
- IT and Physical Security Contractor
- Procurement Specialist
- Legal
- Contracting Engineer
- Insurance
- Supply-chain Participant
- Inventory Management/Lifecycle Management
- Physical Security Specialist

Information Technology (IT) Cybersecurity

- ICS Security Analyst
- Security Engineering and Architect
- Security Operations
- Security Response and Forensics
- Security Management (CSO)
- Audit Specialist
- Security Tester

Information Technology (IT) Staff

- Networking and Infrastructure
- Host Administrator
- Database Administrator
- Application Development
- ERP/MES Administrator
- IT Management

# REFERENCES

[1] [Norsk Hydro | “Power and market operations” | https://www.hydro.com/en-US/energy/power-and-market-operations/ | 26 July 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[2] [YouTube | Insignia – Crisis Management Specialists | Jonathan Hemus and Inger Sethov | “Webinar: How Norsk Hydro emerged from a cyber attack with its reputation enhanced” | https://www.youtube.com/watch?v=C6MDz-AgQuE&t=12s | 22 April 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[3] [YouTube | Norsk Hydro | “The cyber attack rescue operation in Hydro Toulouse” | https://www.youtube.com/watch?v=o6eEN0mUakM | 16 April 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[4] [Microsoft | Bill Briggs | “Hackers hit Norsk Hydro with ransomware. The company responded with transparency” | https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ | 16 December 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[5] [Microsoft | Bill Briggs | “Hackers hit Norsk Hydro with ransomware. The company responded with transparency” | https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ | 16 December 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[6] [YouTube | Norsk Hydro | “Cyber attack on Hydro Magnor” | https://www.youtube.com/watch?v=S-ZlVuM0we0 | 28 October 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[7] [DoublePulsar | Kevin Beaumont | “How Lockergoga took down Hydro – ransomware used in targeted attacks aimed at big business” | https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880 | 21 Mar 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[8] [YouTube | Insignia – Crisis Management Specialists | Jonathan Hemus and Inger Sethov | “Webinar: How Norsk Hydro emerged from a cyber attack with its reputation enhanced” | https://www.youtube.com/watch?v=C6MDz-AgQuE&t=12s | 22 April 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[9] [YouTube | Norsk Hydro | “Why Hydro chose to be transparent during cyber-attack” | https://www.youtube.com/watch?v=C6MDz-AgQuE&t=12s | 28 October 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[10] [YouTube | Norsk Hydro | “The cyber attack rescue operation in Hydro Toulouse” | https://www.youtube.com/watch?v=o6eEN0mUakM | 16 April 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[11] [ZDNet | Catalin Cimpanu | “Norsk Hydro ransomware incident losses reach $40 million after one week” | https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week/ | 26 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[12] [Microsoft | Bill Briggs | “Hackers hit Norsk Hydro with ransomware. The company responded with transparency” | https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ | 16 December 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[13] [Microsoft | Bill Briggs | “Hackers hit Norsk Hydro with ransomware. The company responded with transparency” | https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ | 16 December 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[14] [TrendMicro | “What You Need to Know About the LockerGoga Ransomware” | https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware | 20 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[15] [Dragos | Joe Slowik | “Spyware Stealer Locker Wiper: LockerGoga Revisited” | https://www.dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/ | 16 March 2020 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[16] [WIRED| Andy Greenburg | “Meet LockerGoga, the Ransomware Crippling Industrial Firms” | https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/ | 25 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[17] [TrendMicro | “What You Need to Know About the LockerGoga Ransomware” | https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware | 20 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[18] [Microsoft | Justin Hall, Andrea Bichsel, Nick Schonning, and others | “5136(S): A directory service object was modified.” | https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5136 | 15 December 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[19] [TrendMicro | “What You Need to Know About the LockerGoga Ransomware” | https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware | 20 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[20] [YouTube | Norsk Hydro | “Cyber attack on Hydro Magnor” | https://www.youtube.com/watch?v=S-ZlVuM0we0 | 28 October 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[21] [Microsoft | Bill Briggs | “Hackers hit Norsk Hydro with ransomware. The company responded with transparency” | https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ | 16 December 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[22] [Fastmarkets AMM | Andrea Hotter | “How the Norsk Hydro cyberattack unfolded” | https://www.amm.com/Article/3890250/How-the-Norsk-Hydro-cyberattack-unfolded.html | 22 August 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[23] [DoublePulsar | Kevin Beaumont | “How Lockergoga took down Hydro – ransomware used in targeted attacks aimed at big business” | https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880 | 21 Mar 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[24] [McAfee | ATR Operational Intelligence Team, and Marc RiveroLopez | “LockerGoga Ransomware Family Used in Targeted Attacks” | https://www.mcafee.com/blogs/other-blogs/mcafee-labs/lockergoga-ransomware-family-used-in-targeted-attacks/ | 29 April 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[25] [WIRED| Andy Greenburg | “Meet LockerGoga, the Ransomware Crippling Industrial Firms” | https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/ | 25 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[26] [McAfee | ATR Operational Intelligence Team, and Marc RiveroLopez | “LockerGoga Ransomware Family Used in Targeted Attacks” | https://www.mcafee.com/blogs/other-blogs/mcafee-labs/lockergoga-

ransomware-family-used-in-targeted-attacks/ | 29 April 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[27] [SciVerse ScienceDirect | Suvi Leppänen, Shohel Ahmed, and Robin Granqvist | "Cyber Security Incident Report – Norsk Hydro" | https://mycourses.aalto.fi/pluginfile.php/923542/mod_folder/content/0/Group%20CSS%20Norsk%20Hydro%202019.pdf | March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[28] [SciVerse ScienceDirect | Suvi Leppänen, Shohel Ahmed, and Robin Granqvist | "Cyber Security Incident Report – Norsk Hydro" | https://mycourses.aalto.fi/pluginfile.php/923542/mod_folder/content/0/Group%20CSS%20Norsk%20Hydro%202019.pdf | March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[29] [Microsoft | Justin Hall, Andrea Bichsel, Nick Schonning, and others | "54624(S): An account was successfully logged on." | https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624 | 14 December 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[30] [Dragos | Joe Slowik | "Spyware Stealer Locker Wiper: LockerGoga Revisited" | https://www.dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/ | 16 March 2020 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[31] [Microsoft | Justin Hall, Andrea Bichsel, Nick Schonning, and others | "54624(S): An account was successfully logged on." | https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624 | 14 December 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[32] [TrendMicro | "What You Need to Know About the LockerGoga Ransomware" | https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware | 20 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[33] [Fastmarkets AMM | Andrea Hotter | "How the Norsk Hydro cyberattack unfolded" | https://www.amm.com/Article/3890250/How-the-Norsk-Hydro-cyberattack-unfolded.html | 22 August 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[34] [TrendMicro | "What You Need to Know About the LockerGoga Ransomware" | https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware | 20 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[35] [SciVerse ScienceDirect | Suvi Leppänen, Shohel Ahmed, and Robin Granqvist | "Cyber Security Incident Report – Norsk Hydro" | https://mycourses.aalto.fi/pluginfile.php/923542/mod_folder/content/0/Group%20CSS%20Norsk%20Hydro%202019.pdf | March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[36] [TrendMicro | "What You Need to Know About the LockerGoga Ransomware" | https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware | 20 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[37] [Microsoft | Bill Briggs | "Hackers hit Norsk Hydro with ransomware. The company responded with transparency" | https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ | 16 December 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[38] [YouTube | Insignia – Crisis Management Specialists | Jonathan Hemus and Inger Sethov | “Webinar: How Norsk Hydro emerged from a cyber attack with its reputation enhanced” | https://www.youtube.com/watch?v=C6MDz-AgQuE&t=12s | 22 April 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[39] [SciVerse ScienceDirect | Suvi Leppänen, Shohel Ahmed, and Robin Granqvist | “Cyber Security Incident Report – Norsk Hydro” | https://mycourses.aalto.fi/pluginfile.php/923542/mod_folder/content/0/Group%20CSS%20Norsk%20Hydro%202019.pdf | March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[40] [YouTube | Norsk Hydro | “Why Hydro chose to be transparent during cyber-attack” | https://www.youtube.com/watch?v=C6MDz-AgQuE&t=12s | 28 October 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[41] [YouTube | Insignia – Crisis Management Specialists | Jonathan Hemus and Inger Sethov | “Webinar: How Norsk Hydro emerged from a cyber attack with its reputation enhanced” | https://www.youtube.com/watch?v=C6MDz-AgQuE&t=12s | 22 April 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[42] [Dragos | Joe Slowik | “Spyware Stealer Locker Wiper: LockerGoga Revisited” | https://www.dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/ | 16 March 2020 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[43] [YouTube | Insignia – Crisis Management Specialists | Jonathan Hemus and Inger Sethov | “Webinar: How Norsk Hydro emerged from a cyber attack with its reputation enhanced” | https://www.youtube.com/watch?v=C6MDz-AgQuE&t=12s | 22 April 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[44] [ZDNet | Catalin Cimpanu | “Norsk Hydro ransomware incident losses reach $40 million after one week” | https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week/ | 26 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[45] [Microsoft | Bill Briggs | “Hackers hit Norsk Hydro with ransomware. The company responded with transparency” | https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ | 16 December 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[46] [ZDNet | Catalin Cimpanu | “Norsk Hydro ransomware incident losses reach $40 million after one week” | https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week/ | 26 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[47] [TrendMicro | “What You Need to Know About the LockerGoga Ransomware” | https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware | 20 March 2019 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]

[48] [YouTube | Insignia – Crisis Management Specialists | Jonathan Hemus and Inger Sethov | “Webinar: How Norsk Hydro emerged from a cyber attack with its reputation enhanced” | https://www.youtube.com/watch?v=C6MDz-AgQuE&t=12s | 22 April 2021 | Accessed 18 May 2022 | The source is publicly available information and does not contain classification markings]