PRECURSOR ANALYSIS REPORT: JBS FOODS RANSOMWARE ATTACK 2021

Cybersecurity for the Operational Technology Environment (CyOTE)

31 MARCH 2023

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-23-71884

TABLE OF CONTENTS

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: JBS FOODS 2021 RANSOMWARE ATTACK

1. EXECUTIVE SUMMARY

The JBS Foods 2021 Ransomware Attack Precursor Analysis Report leverages publicly available information about the JBS ransomware 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.

In late May 2021, one of the world's largest meat producers, JBS Foods, announced they had fallen victim to a worldwide ransomware attack, later found to be REvil ransomware. In the United States alone, JBS Foods accounts for nearly 25% of beef and roughly 20% of pork production.[1] Adversaries initially launched a Distributed Denial of Service (DDoS) attack on the company's Information Technology (IT) networks in Australia, but the attack impacted operations in Brazil, Canada, and the United States, as well. The attack caused plant operations in all four countries to shut down for at least one day. All nine of the U.S. meatpacking plants temporarily shut down because of the attack.

The adversaries initially demanded a $22 million ransom for the company's data, but later negotiated the ransom down to $11 million even after JBS Foods restored most of their systems. JBS Foods eventually paid the $11 Million for reassurance from the adversaries that none of their customers' data would be compromised in the future.[2] Despite its short duration, the attack still caused large stocks of meat to spoil. The incident also underscored how adversaries can simultaneously compromise and move laterally through global subsidiaries of an organization.

Researchers and analysts identified 22 unique techniques (in a sequence of 21 steps) utilized during the attack with a total of 361 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Sixteen of the identified techniques used during the JBS Foods cyber attack were precursors to the triggering event. Analysis identified 308 observables associated with these precursor techniques, 163 of which were assessed to have an increased likelihood of being perceived in the 75 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.

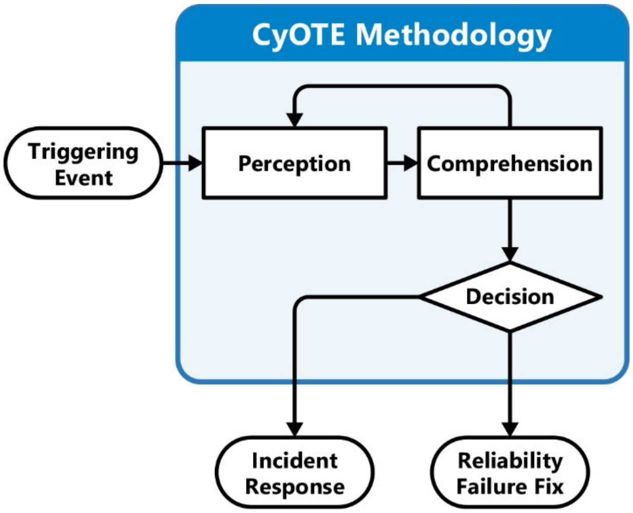


Figure 1. CyOTE Methodology

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

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

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

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

2.2. BACKGROUND ON THE ATTACK

Adversaries gained initial access to JBS Foods Australia's Information Technology (IT) network in mid-February 2021 (D-75) after deploying an intrusion package known as Qakbot or Qbot.[3] Adversaries often use third party intrusion packages to gain initial access to deploy malware once access is obtained. This intrusion package delivered spearphishing emails with malicious attachments to JBS's IT network from spoofed legitimate accounts. The attachment contained a macro that, once opened, ran malicious code to establish a connection to a remote server for Command and Control (C2).

Once C2 was established, the adversaries began a reconnaissance campaign for nearly two weeks, mapping network connectivity in the company's IT networks in Australia and Brazil, where JBS Foods is headquartered. CyOTE analysts assess that the adversaries gained access to JBS Foods' Canadian and U.S. IT networks through this vector.

The adversaries used multiple techniques to move laterally through the JBS global networks. They attempted to move laterally using a Remote Desktop Protocol (RDP) connection on 28 February (D-62) that failed. They then succeeded in moving through the company's global network by using tools such as CobaltStrike and TeamViewer. The adversaries also harvested credentials and elevated privileges by exploiting a known vulnerability in Windows systems (CVE-2018-8453).

By 1 March (D-61), the adversaries began exfiltrating large amounts of sensitive data from JBS Australia and the company's IT network in Brazil.

On 30 May (D-0), adversaries encrypted most of the company's worldwide domain and deleted multiple backup databases. The company became aware of the intrusion early in the morning of 31 May (D+1) before announcing it had been the victim of a Distributed Denial of Service (DDoS) attack that affected operations in multiple countries. The attack caused plant operations in all four countries, including all nine U.S. meatpacking plants, to shut down for at least one day.

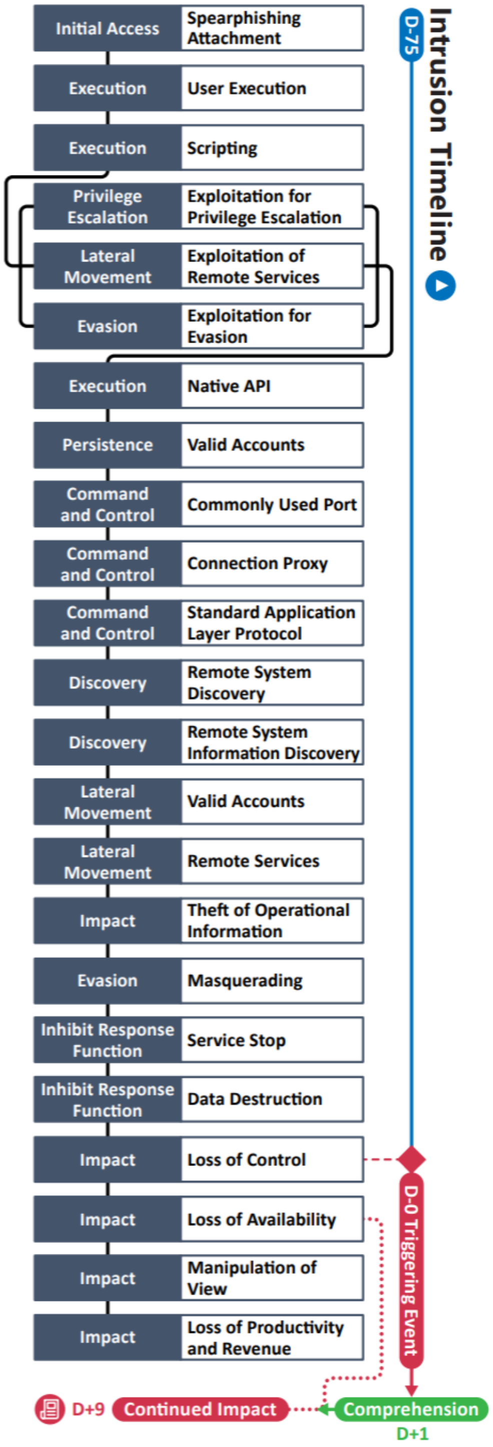


Figure 2. Intrusion Timeline

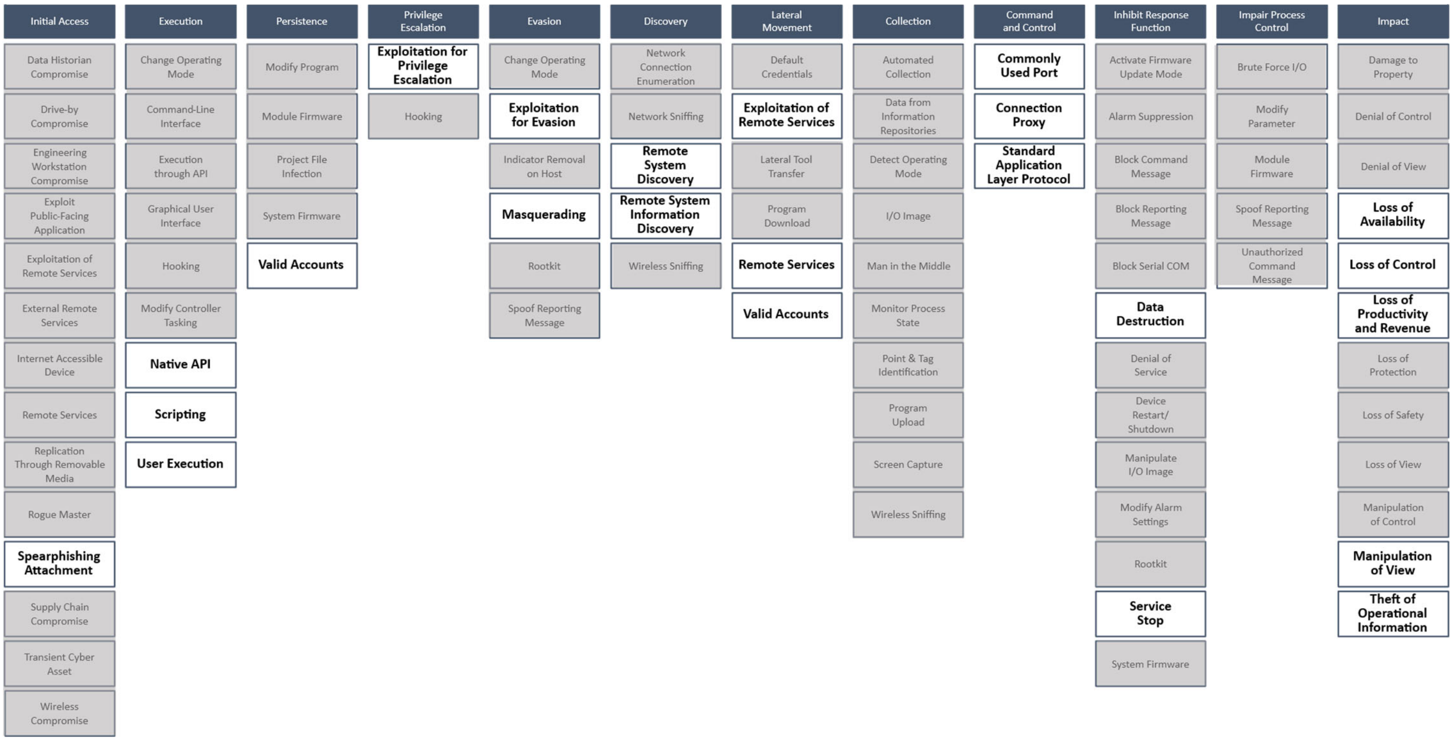
A timeline of adversarial techniques is shown in Figure 2. The timeline includes the estimated number of days prior to and after the triggering event. The timeline after the triggering event includes the assessed victim comprehension timeline.

In total, the adversaries exfiltrated nearly five terabytes (TB) of data from JBS Foods' worldwide domain, including OT data specific to the Australian, Canadian, and U.S. packing plants.[4] Though the adversaries initially demanded $22 million in ransom for the company's data, the amount was negotiated down to $11 million after JBS Foods was able to restore all but a few databases.

JBS Foods stated on 9 June (D+9) that payment was made to the adversaries to ensure that their customers' data would not be compromised in the future.[5]

Analysis identified 19 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.

Table 1. Techniques Used in the JBS Foods 2021 Ransomware 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**
Transient Cyber Asset									System Firmware		
Wireless Compromise											

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	**20**
Technique Observables	**362**
Precursor Techniques	**16**
Precursor Technique Observables	**338**
Highly Perceivable Precursor Technique Observable	**185**

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 TECHNIQUE (T0865) FOR INITIAL ACCESS

One of the most common attack vectors used by adversaries to deploy REvil malware is through spearphishing. Adversaries send spam emails with malicious MS Office attachments that execute malware when opened.[6] In the attack on JBS, adversaries deployed a spam email intrusion package known as Qakbot or Qbot in February 2021 that spoofed legitimate email addresses within JBS Australia's IT networks. This eventually allowed the adversaries to gain a foothold within the victim's operating environment. Qbot can compromise victim IT and OT environments, directing compromised hosts to download and install additional malware for enhanced adversarial capabilities. The adversaries utilized Qbot to craft and deliver REvil malware to the victim, including spam emails with encrypted MS Excel spreadsheets.[7]

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

A total of 20 observables were identified with the use of the Spearphishing technique (T0865). This technique is important for investigation because adversaries may leverage seemingly routine email traffic to obtain a foothold on a victim's IT network. This technique appears at the beginning of the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would limit initial access vectors into the victim environment.

Of the 20 observables associated with this technique, 12 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 29 artifacts could be generated by the Spearphishing technique
Technique Observers[a]	IT Staff, IT Cybersecurity, Support Staff

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

3.2. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

An unsuspecting user within the victim organization received a spearphishing email with an attached Microsoft Excel spreadsheet. This spreadsheet had the REvil malware embedded within scripts. The victim opened the MS Excel attachment, causing a macro within the document to install and execute a Dynamic Link Library (DLL) containing REvil malware directly to the host machine.[8]

IT Staff, IT Cybersecurity, and Support Staff personnel may have been able to observe requests to execute embedded scripts within the Excel spreadsheet attachment.

A total of 26 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. 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. This technique appears early in the timeline and responding to it would effectively halt the adversaries' lateral movement. Terminating the chain of technique at this point would prevent the malware from infecting the host, eliminating the possibility of operational damage in both the IT and OT environments.

Of the 26 observables associated with this technique, 18 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.3. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

The phishing email contained a malicious Excel attachment, which allowed adversaries access to the victim's OT environment. Qbot malware was delivered through embedded macros within the malicious Excel spreadsheet. These macros contained an obfuscated command which retrieved, downloaded, and installed DLLs associated with Qbot. The Qbot DLLs were downloaded into a specific path on the victim's machine and executed via regsvr32.exe. These malicious DLLs utilize process injection via explorer.exe, creating a scheduled task to enable C2 and persistence within the victim's environment.[9]

IT Staff, IT Cybersecurity, and Support Staff personnel may have been able to observe anomalous user interaction with an email attachment and Excel file. They may also have observed spawned, anomalous processes associated with Microsoft legitimate binary usage and Windows Event IDs on infected hosts.

A total of 25 observables were identified with the use of the Scripting Technique (T0853). This technique is important for investigation because it allows the adversary to conduct malicious actions in a victim's environment, often establishing an initial foothold. This technique appears early in the timeline and responding to it will likely halt further adversary activity within the victim's environment. Terminating the chain of techniques at this point would limit malicious activity in the victim's environment, as well as avert future events such as theft of operational information and manipulation of view.

Of the 25 observables associated with this technique, 13 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.4. EXPLOITATION FOR PRIVELEGE ESCALATION TECHNIQUE (T0890) FOR PRIVILEGE ESCALATION

Once the malicious attachment successfully downloads and installs the REvil malware from a remote server, it creates a mutual exclusion object (mutex) that prioritizes its own processes above all others on the Central Processing Unit (CPU). While mutex creation is a normal process, each mutex has a hard-coded value, which may indicate the presence of malware.[10]

REvil then creates a registry key to launch when Windows starts up. This key seeks to exploit a known Windows vulnerability (CVE-2018-8453) to elevate privileges on the host. While the creation of registry keys is also common, REvil creates keys that are saved in temporary files, which is rarely done by legitimate programs.[11] REvil verifies that it is currently running with administrative rights by ensuring its TokenElevationType is set to TokenElevationTypeFull and its integrity level is set to a minimum level of High. If the process is running with Low integrity, REvil terminates the current process and launches another instance of itself via ShellExecute using the runas command, which executes the new instance with administrative rights.[12]

IT Staff and IT Cybersecurity personnel may have been able to observe large amounts of CPU usage for anomalous processes, anomalous execution of the native operating system utilities on the core server host, anomalous files in the temporary folder, and anomalous creation of multiple services.

A total of 13 observables were identified with the use of the Exploitation for Privilege Escalation technique (T0890). This technique is important for investigation because it provides the adversary with the means to control a victim machine by acquiring a domain admin account. This technique appears early in the timeline and responding to it has the potential to prevent the adversary from reaching a DC. Terminating the chain of techniques at this point would keep the adversary from escalating privileges required to reach a DC.

Of the 13 observables associated with this technique, nine are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.5. EXPLOITATION OF REMOTE SERVICES TECHNIQUE (T0866) FOR LATERAL MOVEMENT

REvil communicates with the C2 server associated with anomalous domains via Domain Name Service (DNS) over Port 53. This technique was used to exploit a known Oracle WebLogic Server vulnerability (CVE-2019-2725) that allows remote execution via HTTP/S without the need for credentials. Adversaries also use Cobalt Strike to move laterally by compromising a Microsoft Exchange server before pivoting to domain controllers (DCs) and other victim servers using Server Message Block (SMB).[13] This is likely how REvil performed network discovery and proliferated within JBS Foods' global network.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network traffic across numerous endpoints within a network and anomalous programs such as Cobalt Strike running on the host.

A total of seven observables were identified with the use of the Exploitation of Remote Services technique (T0866). This technique is important for investigation because it allows adversaries to pivot to other machines and conduct network discovery. This technique appears early in the timeline and responding to it may stop malware from proliferating throughout the victim's network. Terminating the chain of techniques at this point would limit the number of machines impacted by ransomware.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 31 artifacts could be generated by the Exploitation for Privilege Escalation technique
Technique Observers	IT Staff, IT Cybersecurity

3.6. EXPLOITATION FOR EVASION TECHNIQUE (T0820) FOR EVASION

REvil creates an auto-start registry key to launch when Windows starts up. This key seeks to exploit a known Windows vulnerability (CVE-2018-8453). Once processes run with system-level integrity[b,14], REvil attempts to impersonate the security context of the first instance of the "explorer.exe" process it finds running on the compromised system.[15] This technique is difficult to detect since the system does not recognize this as anomalous activity.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous registry keys at startup and anomalous instances of explorer.exe running on host machines.

A total of 10 observables were identified with the use of the Exploitation for Evasion technique (T0820). This technique is important for investigation because exploitation of this known vulnerability is easy to prevent by installing patches, but difficult to detect once exploitation occurs. This technique appears early in the timeline and responding to it would prevent adversaries from gaining a foothold on victim networks. Terminating the chain of techniques at this point would limit the adversaries' access and prevent further execution of the ransomware.

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

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

[b] Windows defines four integrity levels: low, medium, high, and system. Standard users receive medium, elevated users receive high. Processes you start and objects you create receive your integrity level (medium or high) or low if the executable file's level is low; system services receive system integrity.[x]

3.7. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

One of the ways in which Qbot, and by extension REvil, infiltrated JBS Australia's network was through using the Windows Management Interface Command Utility (WMIC). This was the method through which the Qbot DLLs were loaded and executed onto a JBS Foods Australia system using regsver32.exe, posing as a Graphics Interface Format (GIF) file in the anomalous email attachment.[16]

REvil also deletes any key that may interfere with its own operation. Examples of this include the deletion of keys involved in file signature management and certificates, and keys that look after application compatibility.[17]

In addition, REvil leverages the Native API technique in later stages of an attack to accomplish lateral movement by writing anomalous programs to system memory, using PowerShell to load Mimikatz for credential harvesting, and PsExec to propagate and remotely execute the ransomware and other files.[18]

IT Staff and IT Cybersecurity personnel may have been able to observe large amounts of CPU usage for anomalous processes, anomalous execution of the native operating system utilities on the core server host, and anomalous creation of multiple services.

A total of 24 observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because changes to the native system could indicate remote execution by an adversary. This technique appears early and continues through the late stages of the attack because it occurs any time the malware is written to a host; responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access, as well as prevent installation and execution of the ransomware.

Of the 24 observables associated with this technique, 21 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.8. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

Adversaries gained access to credentials tied to JBS Foods Australia's network to establish persistence on a victim server. Adversaries achieved this by using credential harvester malware like Mimikatz and KPOT injected into machine memory when the Qbot binary executed.[19] As noted in the previous section, REvil uses captured administrative credentials to elevate its TokenElevationType to Full to prioritize its own processes running on a victim machine.

IT Staff and IT Cybersecurity personnel may have been able to observe an increased number of logins with multiple accounts not associated with known legitimate user activity. These observers would be able to follow up with users to ensure anomalous account usage reflected their actual behavior. Valid account usage by adversaries is difficult to perceive without observers auditing account usage.

A total of 12 observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because harvested credentials not only allow malware to persist by elevating privileges, but to move laterally and proliferate throughout a victim's network. This technique appears relatively early in the timeline and responding to it will limit or delay adversaries' ability to gain control of a system. Terminating the chain of techniques at this point would limit the impact of ransomware to a localized portion of a network, as well as limit the adversaries' continued presence on hosts throughout the network.

Of the 12 observables associated with this technique, nine are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

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

REvil attempts to establish connection between an external remote server and the victim's host server through multiple commonly used ports, including Transmission Control Protocol (TCP) Ports 80, 443, and 53. Adversaries also leveraged The Onion Router (TOR) network to establish anonymous worldwide connectivity. This was the method by which adversaries requested JBS Foods submit their ransom payment. The use of a TOR network name appears as a folder name referenced in one of REvil's registry keys that whitelists certain folders.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous C2 traffic between the host and domains located in countries where the victim does not operate.

A total of six observables were identified with the use of the Commonly Used Port technique (T0885). This technique is important for investigation because it allows defenders a greater opportunity to detect network activity between the malware and its C2 infrastructure. This technique appears relatively early in the timeline and responding to it will effectively halt all future events. 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.

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

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

3.10. CONNECTION PROXY TECHNIQUE (T0884) FOR COMMAND AND CONTROL

Once REvil's code downloads and executes on the victim's host server, it beacons out to external C2 servers associated with domains such as cloudmetric[.]online (45.86.163.78) and smalleststores[.]com (195.189.99.74). Cobalt Strike is subsequently used to establish and maintain C2 connections to the host network.[20] REvil sends a report and system information to its C2 server over TCP Port 443 by generating pseudorandom URLs based on the standardized format: https://{Domain}/{String 1}/{String 2}/{random characters}.{String 3}.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network connections, network traffic, and anomalous processes on infected hosts.

A total of 19 observables were identified with the use of the Connection Proxy technique (T0884). This technique is important for investigation because this technique is often a precursor to network enumeration and discovery to compromise an entire domain and is an indicator of an impending ransomware attack.[21] Additionally, this technique is used to obfuscate malicious actions, thwarting detection and response capabilities. This technique appears relatively early and persists throughout the timeline, and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent the adversaries from performing network discovery, establishing C2, and exfiltrating data.

All 19 observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

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

Once executed on a victim machine, REvil sends a POST request using generated pseudorandom URLs sent via HTTP Secure (HTTPS) over Port 443 to beacon the C2 server.[22] Adversaries also leveraged TOR networks to establish two-way communication between the host and C2 server during the attack on JBS.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network connections over HTTP or Simple Mail Transfer Protocol (SMTP), or DNS requests to anomalous external URLs.

A total of nine observables were identified with the use of the Standard Application Protocol technique (T0869). This technique is important for investigation because defenders within the victim's environments may be able to identify which internal host(s) is communicating with anomalous external domains. Defenders could deny anomalous external communications after they identify hosts that have established connections. This technique appears throughout the timeline and responding to it will alert defenders to malicious activity within their environment. Terminating the chain of techniques at this point would likely halt any further adversary activity if defenders took steps to block the malicious network traffic. Terminating the chain of techniques at this point would end the adversaries' ability to exfiltrate sensitive information.

All nine observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.12. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

REvil discovered connectivity on the JBS Foods Australia network by modifying Windows firewall settings and turning on Network Discovery, making it easier to find other machines on the network to which it could spread.[23] The ransomware may have also carried out additional discovery by using ADFind, Sharpsploit, Bloodhound and NBTScan, as these were capabilities REvil was known to use at the time.[24] Adversaries also utilized the Ping utility to examine connections between the DCs and other domain-joined systems, such as JBS Foods' U.S. and Canadian networks.

IT Staff and IT Cybersecurity personnel may have been able to observe changes to the system's firewall settings and the presence and operation of anomalous tools on infected hosts.

A total of nine observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation because if the defenders can prevent the adversary from collecting system information using this technique, the adversary will have to use more complicated techniques to understand the victim's network. This technique appears in the middle of the timeline and responding to it will help identify and scope which hosts the adversaries have infected and which hosts they are targeting. In so doing, defenders may be able to prevent continual scanning and contain infected hosts. If the defenders identify and contain this activity, they could degrade the adversaries' ability to discover hosts, remotely connect, or collect operational information from compromised machines. Terminating the chain of techniques at this point would limit the adversaries' ability to identify systems with operational information.

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

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

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

In addition to changing firewall settings and using open-source tools to discover information about the JBS Australia network, REvil queried the type of operating system (OS) of the infected machine using the GetSystemNativeInfo function to determine if the machine was running on a 32-bit or 64-bit system before exfiltrating the resulting information back to the C2 server.[25] REvil profiled the compromised host by collecting the following information: current username, host name, workgroup/domain name, locale, keyboard configuration, operating system product name, fixed drive details, and CPU architecture.[26]

REvil's ability to check the keyboard configuration or the language of the infected system is especially interesting, as it whitelists, or avoids infecting, systems in certain countries. If the host's configuration or language is not whitelisted, REvil executes the next phase of its infection.

Adversaries also attempted to identify potential RDP connections on the JBS Australia network. On 28 February, a connection request was observed between an anomalous external IP address and a JBS Foods Australia Internet Protocol (IP) address.[27] This demonstrates that the adversaries verified whether an RDP service was running on a local server. However, in this instance the target IP address did not have RDP capability and thus did not provide a response to the RDP request.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous traffic within the network, including anomalous RDP requests and sessions.

A total of 79 observables were identified with the use of the Remote System Information Discovery technique (T0888). This technique is important for investigation because it provides adversaries with detailed information about target devices, allowing them to attack with enhanced specificity. This technique appears near the middle of the timeline and responding to it will prevent adversaries from properly identifying intended target devices. Terminating the chain of techniques at this point would limit data exfiltration and possibly operational damage.

Of the 79 observables associated with this technique, three are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.14. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

After the adversaries concluded their network discovery, they used a CobaltStrike beacon to dump previously harvested credentials on the host server and DC. These credentials were then used to elevate privileges on all connected devices, allowing the malware to proliferate across the JBS Australia network, along with connected systems in the U.S. and Canada.[28] Login credentials for several JBS Australia employees were released on the darkweb shortly thereafter, further indicating that a breech had occurred.[29]

IT Staff and IT Cybersecurity personnel may have been able to observe an increase in logons of user accounts moving from system to system across enterprise environments.

A total of seven observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it is the primary mechanism by which the adversary propagates through multiple networks. This technique appears in the middle of the timeline and responding to it may effectively halt all future events. Terminating the chain of techniques at this point would limit adversarial movement through the enterprise.

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

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

3.15. REMOTE SERVICES TECHNIQUE (T0886) FOR LATERAL MOVEMENT

The adversaries attempted to gain initial access to JBS Foods' Australian IT network IP address space via RDP over TCP Port 3389 on 28 February. However, the adversaries did not receive any response from the targeted host server because it was not running an RDP service. The IP address of the attempted RDP connection was not associated with JBS, but rather one associated with an anomalous source.[30]

Adversaries likely installed TeamViewer, a remote access software, within JBS Australia's network environment at this time. An unusually long-duration connection was observed between 18 and 24 May with an anomalous external server, when a connection to TeamViewer was established for five consecutive days.[31]

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

A total of two observables were identified with the use of the Remote Services technique (T0886). This technique is important for investigation as it is often leveraged to facilitate lateral movement in a victim's environment, allowing for further malicious activity. This technique appears toward the middle of the timeline and responding to it will limit the adversaries' ability to remotely access and control victim machines. Terminating the chain of techniques at this point would limit adversary activity in the victim's environment and limit the exfiltration of sensitive data directly from infected machines.

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

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

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

During the same time as the RDP connections, adversaries began exfiltrating unencrypted data from the JBS Australia domain with tools like FileZilla and Rclone.[32] TeamViewer likely was also used to exfiltrate data. Forensics found an excess of 45 GB of data exfiltrated from the Australia domain between 19 April and 25 May. Over the entirety of the attack (1 March to 29 May), 5 TB of data were exfiltrated from various JBS locations. The data was being exfiltrated to the file-sharing site Mega and to multiple IP addresses in Hong Kong.[33]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous outbound network traffic to an unknown external server, as well as anomalous RDP sessions.

A total of 27 observables were identified with the use of the Theft of Operational Information technique (T0882). This technique is important for investigation because it is a critical point at which adversaries obtain sensitive data that enables malicious behaviors through the end of the timeline. This technique appears late in the timeline and responding to it will prevent the adversaries from exfiltrating data from the enterprise and OT environments. Terminating the chain of techniques at this point would limit operational damage and the loss of sensitive OT documentation.

Of the 26 observables associated with this technique, six are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.17. MASQUERADING TECHNIQUE (T0849) FOR EVASION

REvil performs another privilege-related validation within its main function prior to profiling host information. If the current process is running with system-level integrity, then the process will try to impersonate the security context of the first process found on the system right before the infected system shuts down. This automatically removes any traces of REvil when the system restarts. Implementing the persistence mechanism just prior to shutdown prevents security programs from detecting anomalous behavior.[34]

IT Staff, IT Cybersecurity, and Support Staff personnel may have been able to observe the presence of anomalous executable files in the enterprise network.

A total of 10 observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation because it shields adversarial behavior from the defenders. Specifically, this technique is used to disguise malicious payloads from automated or manual detection. This technique appears late in the timeline and responding to it will likely halt the execution of the malware, although this is unlikely given the brief time from disabling services to ransomware execution. Terminating the chain of techniques at this point would halt the deployment of the ransomware.

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

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

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

Before encryption occurs, REvil malware searches for processes in the prc field within its configuration file and terminates each process.[35] The adversaries utilize various legitimate tools, such as PC Hunter and Process Hacker, to discover and terminate services and processes associated with antivirus products.[36] KillAV is a custom malicious binary designed to uninstall antivirus-related products by either querying the uninstall registry and uninstalling the associated program or by terminating processes from the list.[37]

IT Staff and IT Cybersecurity personnel may have been able to observe the anomalous termination of processes and services, including those related to antivirus products.

A total of 21 observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation because it disables critical security tools that can alert a victim to malicious cyber activity. This technique appears late in the timeline and responding to it would likely halt final execution of the ransomware, although it is highly unlikely defenders would have sufficient time to act. Terminating the chain of techniques at this point would likely have minimal influence on the outcome of the attack.

All 21 observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.19. DATA DESTRUCTION TECHNIQUE (T0809) FOR INHIBIT RESPONSE FUNCTION

Adversaries also disable and delete keys associated with processes and services to limit the victim's ability to interfere with the operation of the malicious code. This includes deleting backups of encrypted systems so that local file restoration is not available.[38] The command that REvil adversaries use to delete backups also disables access to recovery tools, which typically are available when rebooting a Windows system. Disabling these tools further cripples a system and prevents it from easily being restored. Of note, REvil only deletes backup files with the exact name of "backup", but not "backup1" or "database backup".[39] As a result, JBS foods was able to recover data from backups for all but two databases.

IT Staff, IT Cybersecurity, and Support Staff personnel may have been able to observe the deletion of files on targeted hosts, an increase in system resource utilization, and anomalous encryption of files.

A total of 12 observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because it renders files crucial to business and other enterprise operations unusable. This technique appears late in the technique timeline and responding to it has the potential to ensure recovery of all systems through backups. Terminating the chain of techniques at this point may limit the extent of backup deletion but would not prevent the adversary from being able to extort the victim for ransom.

All 12 observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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, Support Staff

3.20. LOSS OF CONTROL TECHNIQUE (T0827) FOR IMPACT

Once exfiltration and deletion of backup files were complete, the adversaries encrypted most of the company's worldwide domain and wiped multiple backup databases on 30 May (D-0). This resulted in the victim being unable to control IT assets within their enterprise.

REvil queues all targeted or blacklisted folders and encrypts each file by first reading the file contents into a buffer, then encrypting the contents of the buffer. REvil then writes the encrypted contents of the buffer to the original file, overwriting the original file content before renaming the original file with a previously generated random extension.

To create the file extension, REvil generates a unique identifier (UID) for the host by first obtaining the volume serial number for the system drive. REvil then generates a CRC32 hash of the volume serial number using the hard-coded seed value of 0x539. Next, REvil generates a CRC32 hash of the value returned by the CPUID assembly instruction using the CRC32 hash for the volume serial number as a seed value before appending the volume serial number to the CPUID CRC32 hash.[40]

This value contains the random extension generated at runtime that is appended to encrypted files. If this registry value does not exist, the malware would generate a random string of lowercase letters (a-z) and numbers (0-9) ranging from five to ten characters in length and preceded by a period (e.g., .5937gzq9). This string is assigned to the rnd_ext value within the recfg registry subkey.[41]

IT Staff, IT Cybersecurity and Support Staff personnel may have been able to observe the loss of functionality of IT and OT assets, anomalously encrypted files and modified desktop backgrounds, and ransom notes on the desktop.

A total of 29 observables were identified with the use of the Loss of Control technique (T0827). This technique is important for investigation because it prevents victim organizations from controlling mission-critical assets, resulting in loss of functionality and most likely financial loss. This technique appears at the end of the timeline and represents the triggering event. Responding to it will not have any significant impact. Terminating the chain of techniques at this point would not prevent the adversary from being able to extort the victim for ransom. However, rapid response may reduce impact severity and recovery time.

Of the 29 observables associated with this technique, 22 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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, Support Staff

3.21. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

After REvil encrypted the files, JBS Foods employees became aware on 31 May (D+1) that affected computers were largely unavailable. Since the adversaries encrypted large amounts of JBS Foods' data, entire domains, including OT environments of all nine U.S. plants, became mostly unavailable. Although most of the attack on JBS Foods was aimed at the company's IT networks, it was forced to shut down operations at multiple plants worldwide because the encryption of critical OT files had rendered them unusable.[42]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Management, Support Staff, and Engineering personnel may have been able to observe the results of the loss of availability when trying to control or restart various systems or accessing backup files.

A total of 10 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. Appearing at the end of the timeline, terminating the chain of techniques at this point would not prevent the adversary from being able to extort the victim for ransom. Successfully returning the systems to normal operations is the only way to prevent further damage or loss.

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

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, Management, Support Staff, Engineering

3.22. MANIPULATION OF VIEW TECHNIQUE (T0832) FOR IMPACT

The adversaries created additional files in a file folder containing information on how to pay the ransom. The adversaries then changed the desktop wallpaper to inform the user that the system was compromised. The new wallpaper also referred the user to the ransom file containing instructions on recovering the files after paying the ransom.[43]

IT Staff, IT Cybersecurity, and Support Staff personnel may have been able to observe the ransom note on infected hosts in the enterprise environment as well as anomalously encrypted files.

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

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

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

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

The REvil ransomware caused plant operations in all four countries, including all 9 U.S. meatpacking plants, to shut down for at least one day. The adversaries initially demanded $22 million in ransom for the company's data, yet the company negotiated the amount to $11 million after JBS Foods was able to restore all but a few databases. At the time of payment, most facilities were operational. The payment was made to the adversaries to ensure that JBS customers' data would not be compromised in the future.[44]

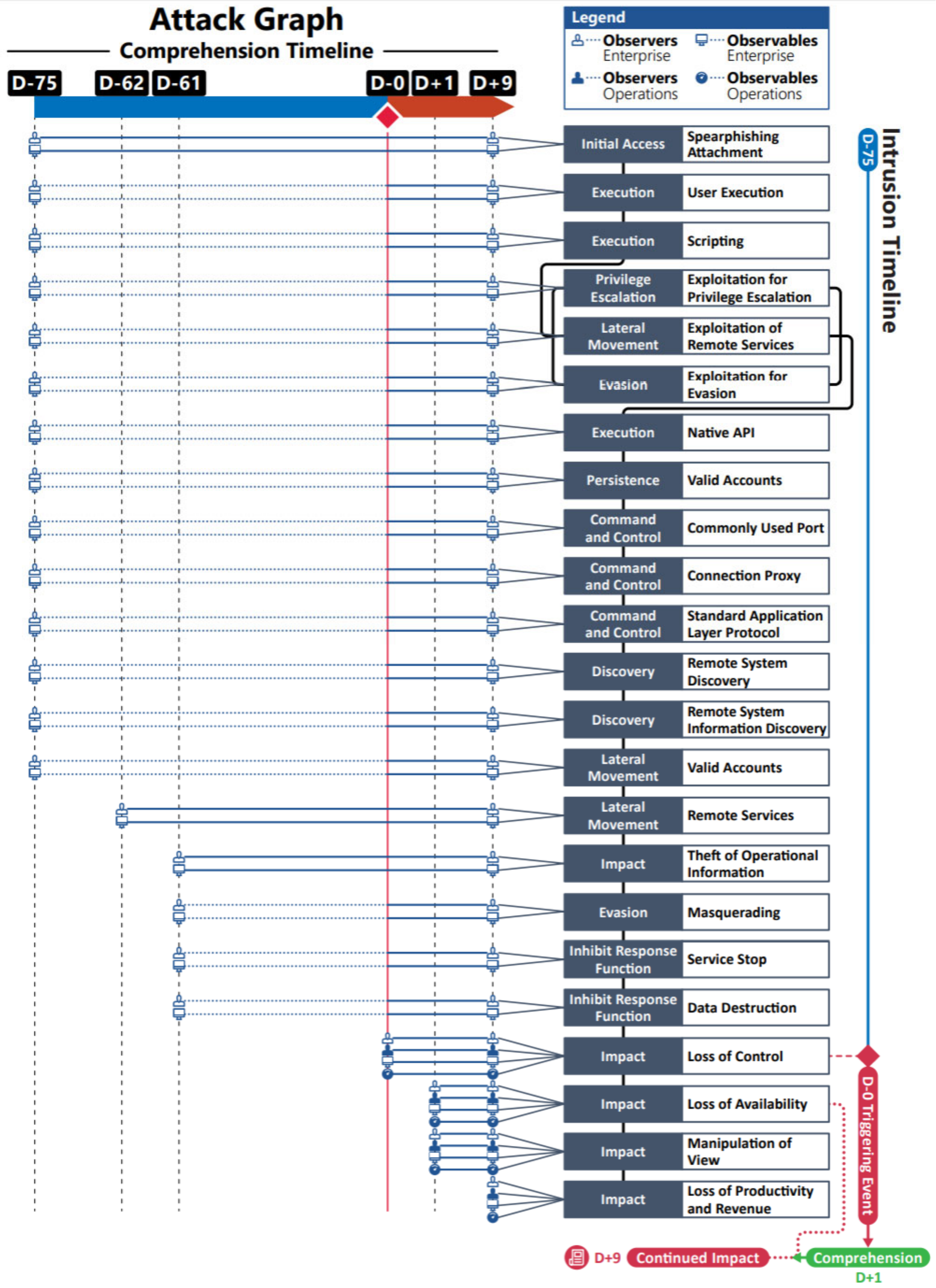
IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Management, Support Staff, and Engineering personnel may have been able to observe anomalous loss of productivity and revenue.

A total of five 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. If adversarial behavior is not identified as a contributing cause, continued adversarial behavior may cause additional financial impacts to the victim. This technique appears at the end of the timeline and responding to it will include efforts to regain operational functionality and to resume normal operation.

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

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

Figure 3. Attack Graph



APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †

Observables Associated with Spearphishing Technique (T0865)	
Observable 1 †	*Presence of Anomalous Email: Containing an Attachment: Office Document: Excel Document: Excel Open XML Macro-Enabled Spreadsheet (XLSM) Document*
Observable 2	Anomalous Network Traffic
Observable 3	Anomalous Network Traffic: From Local Host to External Host
Observable 4 †	*Anomalous System Behavior on Local Host: Anomalous Prompt to Enable Macros: Visual Basic for Application (VBA) Code Within Macro: Macros Contain Junk Parameters and Conditions*
Observable 5 †	*Anomalous System Behavior on Local Host: Anomalous Prompt to Enable Macros: Visual Basic for Application (VBA) Code Within Macro: Macros Contain Obfuscated Code*
Observable 6 †	*Anomalous Network Traffic: From External Host to Local Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): Download of Anomalous Executable on Local Host: Microsoft-Word[.]exe*
Observable 7 †	*Anomalous Network Traffic: From External Host to Local Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): With host "hxxp://blaerck.xyz"*
Observable 8 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "blaerck.xyz"*
Observable 9 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "cymru.futbol"*
Observable 10 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "altocontratto.net"*
Observable 11 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "rvside.com"*
Observable 12 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "noda.com.ua"*
Observable 13 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "christianscholz.de"*
Observable 14 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "wallflowersandrakes.com"*
Observable 15	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: cymru.futbol
Observable 16	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: altocontratto.net
Observable 17	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: rvside.com

Observables Associated with Spearphishing Technique (T0865)	
Observable 18	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: noda.com.ua
Observable 19	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: christianscholz.de
Observable 20	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: wallflowersandrakes.com

Observables Associated with User Execution Technique (T0863)	
Observable 1 †	*Presence of Anomalous Email: Containing an Attachment: PDF Document*
Observable 2 †	*Presence of Anomalous Email: Containing an Attachment: Office Document: Excel Document: Excel Open XML Macro-Enabled Spreadsheet (XLSM) Document*
Observable 3 †	*Anomalous System Behavior on Local Host: Anomalous Prompt to Enable Macros*
Observable 4 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): with Host "nomovee[.].website"*
Observable 5 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): with Host "nomovee[.].website"*
Observable 6 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "nomovee[.].website"*
Observable 7 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "blaerck.xyz"*
Observable 8 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "cymru.futbol"*
Observable 9 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "altocontratto.net"*
Observable 10 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "rvside.com"*
Observable 11 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "noda.com.ua"*
Observable 12 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "christianscholz.de"*
Observable 13 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "wallflowersandrakes.com"*
Observable 14 †	*Presence of Anomalous File on Local Host: Anomalous Graphics Interchange Format (GIF) File*
Observable 15	Read of Anomalous File on Local Host: Anomalous Graphics Interchange Format (GIF) File

Observables Associated with User Execution Technique (T0863)	
Observable 16 †	*Presence of Anomalous Binary on Host: Anomalous Dynamic Link Library (.dll) File*
Observable 17 †	*Execution of Anomalous Binary on Host: Anomalous Dynamic Link Library (.dll) File*
Observable 18	Initiation of Anomalous Windows Management Interface (WMIC) Command: IcedID
Observable 19 †	*Presence of Anomalous Executable on Host: rundll32.exe*
Observable 20 †	*Execution of Anomalous Executable on Host: rundll32.exe*
Observable 21	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: cymru.futbol
Observable 22	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: altocontratto.net
Observable 23	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: rvside.com
Observable 24	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: noda.com.ua
Observable 25	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: christianscholz.de
Observable 26	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: wallflowersandrakes.com

Observables Associated with Scripting Technique (T0853)	
Observable 1 †	*Presence of Vulnerability on Local Host: Microsoft Windows Workstation: Win32k Task Scheduler (CVE-2018-8453)*
Observable 2 †	*Presence of Anomalous File on Host: Excel Macro-Enabled Workbook (XLSM) File: With anomalous macros*
Observable 3 †	*Execution of Anomalous File on Host: Excel Macro-Enabled Workbook (XLSM) File: With anomalous macros*
Observable 4 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): HTTPS GET Request*
Observable 5 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): HTTP GET Request*
Observable 6 †	*Anomalous Network Traffic: From External Host to Local Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): HTTPS GET Request*
Observable 7 †	*Presence of Anomalous Script on Host: PowerShell script*

Observables Associated with Scripting Technique (T0853)	
Observable 8 †	*Presence of Anomalous File on Host: Graphics Interchange Format (GIF) File*
Observable 9	Anomalous System Behavior on Local Host: Initiation of anomalous Windows Management Interface (WMIC) Command: IcedID
Observable 10 †	*Anomalous Network Traffic: From External Host to Local Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): Download of Anomalous Executable on Local Host: MicrosoftOfficeWord_upd.v.88735.34.5.exe: With Hash 720fbe60f049848f02ba9b2b91926f80ba65b84f0d831a55f4e634c820bd0848*
Observable 11 †	*Presence of Anomalous Executable on Host: MicrosoftOfficeWord_upd.v.88735.34.5.exe: With Hash 720fbe60f049848f02ba9b2b91926f80ba65b84f0d831a55f4e634c820bd0848*
Observable 12 †	*Execution of Anomalous Executable on Host: MicrosoftOfficeWord_upd.v.88735.34.5.exe: With hash 720fbe60f049848f02ba9b2b91926f80ba65b84f0d831a55f4e634c820bd0848*
Observable 13 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "nomovee[.].website"*
Observable 14 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): with Host "nomovee[.].website"*
Observable 15	Execution of Anomalous Executable on Host: rundll32.exe
Observable 16	Anomalous System Behavior on Local Host: Initiation of Anomalous Process on Host: "int Current PID": Comparison of CRC32 Hash of Function Names: "Revil_ResolveFunctions( )"
Observable 17	Anomalous System Behavior on Local Host: Anomalous Creation of Mutex: Named with Hard-Coded Value: C19C0A84-FA11-3F9C-C3BC-0BCB16922ABF
Observable 18	Anomalous System Behavior on Local Host: Initiation of Anomalous Process on Host: "Revil_ResolveFunctions( )": "if (Revil_Get_exp_ConfigValue( )) ; :REvil_AttemptExploit_CVE_2018-8453"
Observable 19	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: cymru.futbol
Observable 20	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: altocontratto.net
Observable 21	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: rvside.com
Observable 22	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: noda.com.ua
Observable 23	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: christianscholz.de

Observables Associated with Scripting Technique (T0853)	
Observable 24	Presence of Anomalous Binary on Local Host: .m69: Anomalous Configuration Keys Within String: "dmn": Presence of Anomalous Domain Name Within Configuration Key: wallflowersandrakes.com
Observable 25	Execution of Anomalous Binary on Local Host: regsvr32

Observables Associated with Exploitation for Privilege Escalation Technique (T0890)	
Observable 1 †	Presence of Vulnerability on Local Host: Microsoft Windows Workstation: Win32k Task Scheduler (CVE-2018-8453)
Observable 2 †	Presence of Anomalous Binary on Local Host: Mimikatz
Observable 3	Anomalous System Behavior on Local Host: Anomalous Memory-write: by Mimikatz Binary
Observable 4 †	Presence of Anomalous Executable on Host: 9b46d03b69bda0df57c0ebb8dae0aebdd1d131beb500242fa8fe59cb260eed1.exe
Observable 5 †	Presence of Anomalous Registry Key on Host: machine\software\wow6432node\blacklivesmatter
Observable 6 †	Presence of anomalous registry key on host: wJWsTYE
Observable 7 †	Execution of Anomalous Executable on Host: 9b46d03b69bda0df57c0ebb8dae0aebdd1d131beb500242fa8fe59cb260eed1.exe
Observable 8	Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: SystemParametersInfoW
Observable 9	Anomalous System Behavior on Local Host: Anomalous Creation of Mutex: Named with Hard-Coded Value: C19C0A84-FA11-3F9C-C3BC-0BCB16922ABF
Observable 10 †	Anomalous System Behavior on Local Host: Anomalous Execution of ShellCode: Anomalous Elevation of Privileges
Observable 11	Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: TokenElevationType
Observable 12 †	Anomalous System Behavior on Local Host: Anomalous Command Line: 'runas': Creation of New Process Using ShellExecute: With Administrative Rights
Observable 13 †	Anomalous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657): Anomalous creation of registry key "autorun": mapped to temporary folder

Observables Associated with Exploitation of Remote Services Technique (T0866)	
Observable 1 †	Presence of Vulnerability on Local Host: Oracle WebLogic Server: Deserialization Vulnerability CVE-2019-2725
Observable 2 †	Anomalous Network Traffic: From External Host to Local Host: Over TCP Port 7001 (Oracle WebLogic)

Observables Associated with Exploitation of Remote Services Technique (T0866)	
Observable 3	Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query domain "alhashem.net"
Observable 4 †	Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query domain "echtveilig.nl"
Observable 5 †	Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query domain "nuzech.com"
Observable 6 †	Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query domain "stopilhan.com"
Observable 7 †	Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query domain "ra-staudte.de"

Observables Associated with Exploitation for Evasion Technique (T0820)	
Observable 1 †	Presence of Vulnerability on Local Host: Microsoft Windows Workstation: Win32k Task Scheduler (CVE-2018-8453)
Observable 2 †	Execution of Anomalous Executable on Host: 9b46d03b69bda0df57c0ebb8dae0aebdd1d131beb500242fa8fe59cb260eed1.exe
Observable 3	Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: SystemParametersInfoW
Observable 4	Anomalous System Behavior on Local Host: Anomalous Creation of Mutex: Named with Hard-Coded Value: C19C0A84-FA11-3F9C-C3BC-0BCB16922ABF
Observable 5 †	Anomalous System Behavior on Local Host: Anomalous Execution of ShellCode: Anomalous Elevation of Privileges
Observable 6	Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: TokenElevationType
Observable 7 †	Anomalous System Behavior on Local Host: Anomalous Command Line: 'runas': Creation of New Process Using ShellExecute: With Administrative Rights
Observable 8 †	Anomalous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657): Anomalous creation of registry key "autorun": mapped to temporary folder
Observable 9 †	Presence of Anomalous Executable on Host: explorer.exe
Observable 10 †	Execution of Anomalous Executable on Host: explorer.exe

Observables Associated with Native API Technique (T0834)	
Observable 1 †	Presence of Anomalous Binary on Local Host: Mimikatz
Observable 2	Anomalous System Behavior on Local Host: Anomalous Memory-write: by Mimikatz Binary

Observables Associated with Native API Technique (T0834)	
Observable 3 †	Presence of Anomalous Executable on Host: 9b46d03b69bda0df57c0ebb8dae0aebdd1d131beb500242fa8fe59cb260eed1.exe
Observable 4 †	Presence of Anomalous Registry Key on Host: machine\software\wow6432node\blacklivesmatter
Observable 5 †	Presence of anomalous registry key on host: wJWsTYE
Observable 6 †	Execution of Anomalous Executable on Host: 9b46d03b69bda0df57c0ebb8dae0aebdd1d131beb500242fa8fe59cb260eed1.exe
Observable 7	Anomalous System Behavior on Local Host: Anomalous Creation of Mutex: Named with Hard-Coded Value: C19C0A84-FA11-3F9C-C3BC-0BCB16922ABF
Observable 8 †	Anomalous System Behavior on Local Host: Anomalous Execution of ShellCode: Anomalous Elevation of Privileges
Observable 9 †	Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: TokenElevationType
Observable 10	Anomalous System Behavior on Local Host: Anomalous Command Line: 'runas': Creation of New Process Using ShellExecute: With Administrative Rights
Observable 11 †	Anomalous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657): Anomalous Creation of Registry Key "Autorun": Mapped to Temporary Folder
Observable 12 †	Presence of Anomalous Binary on Host: services.exe
Observable 13 †	Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: Machine\system\controlset001\services\aelookupsvc "DeleteFlag"
Observable 14 †	Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: Machine\system\controlset001\services\aelookupsvc "Start"
Observable 15 †	Execution of Anomalous Binary on Host: services.exe
Observable 16 †	Anomalous System Behavior on Local Host: Windows Process Terminated (Event ID 4689): Startup Services halted
Observable 17 †	Anomalous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657): Machine\system\controlset001\services\aelookupsvc "DeleteFlag"
Observable 18 †	Anomalous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657): Machine\system\controlset001\services\aelookupsvc "Start"
Observable 19 †	Anomalous System Behavior on Local Host: Anomalous Command Line: C:\Windows\System32\cmd.exe"/c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default}bootstatuspolicy ignoreallfailures
Observable 20 †	Anomalous System Behavior on Local Host: Anomalous Command Line: vssadmin.exe Delete Shadows/All/Quiet
Observable 21 †	Anomalous System Behavior on Local Host: C:\Windows\System32\cmd.exe"/c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default}recoveryenabled No & bcdedit/set {default} bootstatuspolicy ignoreallfailures

Observables Associated with Native API Technique (T0834)	
Observable 22 †	Anomalous System Behavior on Local Host: Anomalous Increase in System Resource Utilization: Increase in CPU Utilization
Observable 23 †	Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity
Observable 24 †	Anomalous Deletion of Data: Deletion of Windows Shadow Volume

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1 †	*Presence of Anomalous Binary on Host: KPOT*
Observable 2 †	*Presence of Anomalous Binary on Host: SharpSploit*
Observable 3 †	*Presence of Anomalous Binary on Host: Mimikatz*
Observable 4 †	*Execution of anomalous Binary on Host: KPOT*
Observable 5 †	*Execution of anomalous Binary on Host: SharpSploit*
Observable 6 †	*Execution of anomalous Binary on Host: Mimikatz*
Observable 7	Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: TokenElevationType
Observable 8 †	*Anomalous System Behavior on Local Host: Anomalous Command Line: 'runas': Creation of New Process Using ShellExecute: With Administrative Rights*
Observable 9 †	*Presence of Anomalous Executable on Host: explorer.exe*
Observable 10 †	*Execution of Anomalous Executable on Host*
Observable 11	Execution of Anomalous Executable on Host: explorer.exe
Observable 12	Anomalous Presence of Legitimate Credentials Available on The Web: Multiple Employee Credentials: @jbssa.com.au:ducati

Observables Associated with Commonly Used Port Technique (T0859)	
Observable 1	Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): GET Request
Observable 2	Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): GET Request
Observable 3	Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS)
Observable 4 †	Anomalous Network Traffic: From Local Host to External Host: The Onion Router (TOR) Traffic
Observable 5 †	Anomalous Network Traffic: From External Host to Local Host: The Onion Router (TOR) Traffic
Observable 6 †	Anomalous Network Traffic: From External Host to Local Host: Over TCP Port 7001 (Oracle WebLogic)

Observables Associated with Connection Proxy Technique (T0884)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to External Host: The Onion Router (TOR) Traffic*
Observable 2 †	*Anomalous Network Traffic: From External Host to Local Host: The Onion Router (TOR) Traffic*
Observable 3 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "alhashem.net"*
Observable 4 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "echtveilig.nl"*
Observable 5 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "nuzech.com"*
Observable 6 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "stopilhan.com"*
Observable 7 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "ra-staudte.de"*
Observable 8 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "cloudmetric[.]online"*
Observable 9 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "smalleststores[.]com"*
Observable 10 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): https://{Domain}/{String 1}/{String 2}/{random characters}.{String 3}*
Observable 11 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): Download of Anomalous Binary on Local Host: Cobalt Strike binary*
Observable 12 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): With Host "cloudmetric[.]online": Over Session Lasting Multiple Hours*
Observable 13 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): With host 45.86.163.78: Over Session Lasting Multiple Hours*
Observable 14 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): With host "smalleststores[.]com": Over Session Lasting Multiple Hours*
Observable 15 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): With host 195.189.99.74: Over Session Lasting Multiple Hours*
Observable 16 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): With host "cloudmetric[.]online": Over Session Lasting Multiple Hours*
Observable 17 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): With host 45.86.163.78: Over Session Lasting Multiple Hours*

Observables Associated with Connection Proxy Technique (T0884)	
Observable 18 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): With host "smalleststores[.]com": Over Session Lasting Multiple Hours*
Observable 19 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 80: Hypertext Transfer Protocol (HTTP): With host 195.189.99.74: Over Session Lasting Multiple Hours*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1 †	*Presence of Vulnerability on Local Host: Oracle WebLogic Server: Deserialization Vulnerability CVE-2019-2725*
Observable 2 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): HTTPS POST Request: https://<c2_domain>/<URI_sub1>/<URI_sub2>/<random_resource_name>.<ext>*
Observable 3 †	*Anomalous Network Traffic: From Local Host to External Host: The Onion Router (TOR) Traffic*
Observable 4 †	*Anomalous Network Traffic: From External Host to Local Host: The Onion Router (TOR) Traffic*
Observable 5 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "alhashem.net"*
Observable 6 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "echtveilig.nl"*
Observable 7 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "nuzech.com"*
Observable 8 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "stopilhan.com"*
Observable 9 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 53: Domain Name Service (DNS): Query Domain "ra-staudte.de"*

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1	Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS)
Observable 2 †	Presence of Anomalous Binary on Host: Network Scanning Utility: NBTScan
Observable 3 †	Presence of Anomalous Binary on Host: Network Scanning Utility: Bloodhound
Observable 4 †	Presence of Anomalous Binary on Host: Network Scanning Utility: SharpSploit
Observable 5	Anomalous System Behavior on Local Host: Anomalous Execution of Native OS API: GetSystemNativeInfoW
Observable 6	Anomalous System Behavior on Local Host: User Privilege Escalation: To 0x3000: From 0x2000
Observable 7	Anomalous System Behavior on Local Host: User Privilege Escalation: 0x1000

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 8	Anomalous System Behavior on Local Host: Anomalous Command Line
Observable 9 †	*Anomalous System Behavior on Local Host: Anomalous Command Line: 'netsh advfirewall firewall set rule group=*Network Discovery* new enable=Yes'*

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 1	Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS)
Observable 2 †	*Presence of Anomalous Binary on Host: Network Scanning Utility: NBTScan*
Observable 3 †	*Presence of Anomalous Binary on Host: Network Scanning Utility: Bloodhound*
Observable 4 †	*Presence of Anomalous Binary on Host: Network Scanning Utility: SharpSploit*
Observable 5	Anomalous System Behavior on Local Host: Anomalous Execution of Native OS API: GetSystemNativeInfoW
Observable 6	Anomalous System Behavior on Local Host: User Privilege Escalation: To 0x3000: From 0x2000
Observable 7	Anomalous System Behavior on Local Host: User Privilege Escalation: 0x1000
Observable 8	Anomalous System Behavior on Local Host: Anomalous Command Line: 'runas'
Observable 9	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting
Observable 10	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000041c (Albanian)
Observable 11	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000042b (Armenian Eastern)
Observable 12	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0002042b (Armenian Phonetic)
Observable 13	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0003042b (Armenian Typewriter)
Observable 14	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0001042b (Armenian Western)
Observable 15	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting:

Observables Associated with Remote System Information Discovery Technique (T0888)	
	GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0001042C (Azerbaijani (Standard))
Observable 16	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000082c (Azerbaijani Cyrillic)
Observable 17	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000042C (Azerbaijani Latin)
Observable 18	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000423 (Belarusian)
Observable 19	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000201a (Bosnian (Cyrillic))
Observable 20	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000429 (Central Kurdish)
Observable 21	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000041a (Croatian)
Observable 22	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000439 (Devanagari-INSCRIPT)
Observable 23	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000425 (Estonian)
Observable 24	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000438 (Faeroese)
Observable 25	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0001083b (Finnish with Sami)
Observable 26	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000437 (Georgian)

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 27	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00020437 (Georgian (Ergonomic))
Observable 28	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00010437 (Georgian (QWERTY))
Observable 29	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00030437 (Georgian Ministry of Education and Science Schools)
Observable 30	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00040437 (Georgian (Old Alphabets))
Observable 31	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00010439 (Hindi Traditional)
Observable 32	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000043f (Kazakh)
Observable 33	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000440 (Kyrgyz Cyrillic)
Observable 34	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00020426 (Latvian (Standard))
Observable 35	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00010426 (Latvian (Legacy))
Observable 36	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00010427 (Lithuanian)
Observable 37	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000427 (Lithuanian IBM)
Observable 38	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting:

Observables Associated with Remote System Information Discovery Technique (T0888)	
	GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00020427 (Lithuanian Standard)
Observable 39	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000042f (Macedonia (FYROM))
Observable 40	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0001042f (Macedonia (FYROM) -Standard)
Observable 41	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000043a (Maltese 47-Key)
Observable 42	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0001043a (Maltese 48-Key)
Observable 43	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000043b (Norwegian with Sami)
Observable 44	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000429 (Persian)
Observable 45	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00050429 (Persian (Standard)
Observable 46	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000418 (Romanian (Legacy))
Observable 47	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00020418 (Romanian (Programmers))
Observable 48	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00010418 (Romanian (Standard)
Observable 49	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000419 (Russian)

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 50	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00020419 (Russian - Mnemonic)
Observable 51	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00010419 (Russian (Typewriter))
Observable 52	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0002083b (Sami Extended Finland-Sweden)
Observable 53	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0001043b (Sami Extended Norway)
Observable 54	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000c1a (Serbian (Cyrillic)
Observable 55	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000081a (Serbian (Latin))
Observable 56	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000432 (Setswana)
Observable 57	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000041b (Slovak)
Observable 58	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0001041b (Slovak (QWERTY))
Observable 59	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000424 (Slovenian)
Observable 60	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0001042e (Sorbian Extended)
Observable 61	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting:

Observables Associated with Remote System Information Discovery Technique (T0888)	
	GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0002042e (Sorbian Standard)
Observable 62	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000042e (Sorbian Standard - Legacy)
Observable 63	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000041d (Swedish)
Observable 64	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000083b (Swedish with Sami)
Observable 65	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000428 (Tajik)
Observable 66	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00010444 (Tatar)
Observable 67	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000444 (Tatar (Legacy))
Observable 68	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000041e (Thai Kedmanee)
Observable 69	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0002041e (Thai Kedmanee (non-ShiftLock)
Observable 70	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0001041e (Thai Pattachote)
Observable 71	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0003041e (Thai Pattachote (non-ShiftLock)
Observable 72	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0001041f (Turkish F)

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 73	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000041f (Turkish QoETO.exe)
Observable 74	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000442 (Turkmen)
Observable 75	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000422 (Ukrainian)
Observable 76	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00020422 (Ukrainian (Enhanced))
Observable 77	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000420 (Urdu)
Observable 78	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x00000843 (Uzbeck Cyrillic)
Observable 79	Anomalous System Behavior on Local Host: Anomalous Call to System Binary on Host: user32.dll: Whitelisting by Keyboard Language Setting: GetKeyboardLayoutList: Return Value "True": Values x18 through x44 inclusive: 0x0000042a (Vietnamese)

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1 †	Presence of Vulnerability on Local Host: Microsoft Windows Workstation: Win32k Task Scheduler (CVE-2018-8453)
Observable 2	Anomalous Presence of Legitimate Credentials Available on Web: Multiple Employee Credentials: @jbssa.com.au:ducati
Observable 3	Anomalous Presence of Legitimate Credentials Available on Web: Multiple Employee Credentials: @jbssa.com.au:cookieyum
Observable 4 †	*Anomalous System Behavior on Local Host: Anomalous Execution of ShellCode: Anomalous Elevation of Privileges*
Observable 5	Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: TokenElevationType
Observable 6 †	*Anomalous System Behavior on Local Host: Anomalous Command Line: 'runas': Creation of New Process Using ShellExecute: With Administrative Rights*
Observable 7 †	*Anomalous System Behavior on Local Host: Anomalous Command Line Argument: Explorer.EXE*

Observables Associated with Remote Service Technique (T0886)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): To 45.86.163.78*
Observable 2 †	*Anomalous System Behavior on Local Host: Anomalous Use of TeamViewer on local host: Authentication with user outside of country of operations: 5 day long session*

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): To 45.86.163.78*
Observable 2 †	*Anomalous System Behavior on Local Host: Anomalous Use of Teamviewer on local host: Authentication with User Outside of Country of Operations: 5 day long session*
Observable 3 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): To 45.86.163.78*
Observable 4 †	*Anomalous Network Traffic: From Local Host to External Host: Over TCP Port 443: Hypertext Transfer Protocol Secure (HTTPS): Transfer of 5 Terabytes (TB) of Unencrypted Operational Data: Outside Country of Operations: Between 1 March 2021 and 25 May 2021*
Observable 5 †	*Presence of Anomalous Binary on Host: FileZilla*
Observable 6 †	*Presence of Anomalous Binary on Host: Mega*
Observable 7	Anomalous System Behavior on Local Host
Observable 8	Anomalous System Behavior on Local Host: Anomalous Creation of Mutex
Observable 9	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "pk" Key
Observable 10	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "pid" Key
Observable 11	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "sub" Key
Observable 12	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "dbg" Key
Observable 13	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "fast" Key
Observable 14	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "wipe" Key
Observable 15	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "fld" Key
Observable 16	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "fls" Key
Observable 17	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "ext" Key

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 18	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "wfld" Key
Observable 19	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "prc" Key
Observable 20	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "dmn" Key
Observable 21	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "net" Key
Observable 22	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "nbody" Key
Observable 23	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "nname" Key
Observable 24	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "exp" Key
Observable 25	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "img" Key
Observable 26	Anomalous System Behavior on Local Host: Anomalous JSON File Embedded in Anomalous Binary File: Presence of "svc" Key

Observables Associated with Masquerading Technique (T0849)	
Observable 1	Presence of Anomalous Binary on Host: Anomalous Dynamic Link Library (.dll) File
Observable 2	Execution of Anomalous Binary on Host: Anomalous Dynamic Link Library (.dll) File
Observable 3 †	*Presence of Anomalous Executable on Host: explorer.exe*
Observable 4 †	*Execution of Anomalous Executable on Host: explorer.exe*
Observable 5	Execution of Anomalous Script on Host: Immediately prior to System Shutdown
Observable 6 †	*Presence of Anomalous Binary on Host: FileZilla*
Observable 7 †	*Presence of Anomalous Binary on Host: Mega*
Observable 8 †	*Presence of Anomalous Binary on Host: KillAV*
Observable 9 †	*Anomalous System Behavior on Local Host: Anomalous Initiation of Safe Mode*
Observable 10 †	*Anomalous System Behavior on Local Host: Anomalous Command Line: Argument in Command Line: safe mode (s-mode)*

Observables Associated with Service Stop Technique (T0881)	
Observable 1 †	*Presence of Anomalous Binary on Host: PC Hunter*
Observable 2 †	*Presence of Anomalous Binary on Host: Process Hacker*
Observable 3 †	*Presence of Anomalous Binary on Host: KillAV*

Observables Associated with Service Stop Technique (T0881)	
Observable 4 †	*Execution of anomalous Binary on host: PC Hunter*
Observable 5 †	*Execution of anomalous Binary on host: Process Hacker*
Observable 6 †	*Execution of anomalous Binary on host: KillAV*
Observable 7 †	*Anomalous System Behavior on Local Host: Anomalous Usage of kernel32.dll: Terminate Process: mysql.exe*
Observable 8 †	*Presence of Anomalous Binary on Host: services.exe*
Observable 9 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: Machine\system\controlset001\services\aelookupsvc "DeleteFlag"*
Observable 10 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: Machine\system\controlset001\services\aelookupsvc "Start"*
Observable 11 †	*Execution of Anomalous Binary on Host: services.exe*
Observable 12 †	*Anomalous System Behavior on Local Host: Windows Process Terminated (Event ID 4689): Startup Services Halted*
Observable 13 †	*Anomalous System Behavior on Local Host: Windows Process Terminated (Event ID 4689): mysql.exe*
Observable 14 †	*Anomalous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657): Machine\system\controlset001\services\aelookupsvc "DeleteFlag"*
Observable 15 †	*Anomalous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657): Machine\system\controlset001\services\aelookupsvc "Start"*
Observable 16 †	*Anomalous System Behavior on Local Host: Anomalous Command Line: C:\Windows\System32\cmd.exe"/c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default}bootstatuspolicy ignoreallfailures*
Observable 17 †	*Anomalous System Behavior on Local Host: Anomalous Command Line: vssadmin.exe Delete Shadows/All/Quiet*
Observable 18 †	*Anomalous System Behavior on Local Host: C:\Windows\System32\cmd.exe"/c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default}recoveryenabled No & bcdedit/set {default} bootstatuspolicy ignoreallfailures*
Observable 19 †	*Anomalous System Behavior on Local Host: Anomalous Increase in System Resource Utilization: Increase in CPU Utilization*
Observable 20 †	*Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity*
Observable 21 †	*Anomalous Deletion of Data*

Observables Associated with Data Destruction Technique (T0809)	
Observable 1 †	*Presence of Anomalous Binary on Host: services.exe*
Observable 2 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: Machine\system\controlset001\services\aelookupsvc "DeleteFlag"*
Observable 3 †	*Execution of Anomalous Binary on Host: services.exe*

Observables Associated with Data Destruction Technique (T0809)	
Observable 4 †	*Anomalous System Behavior on Local Host: Windows Process Terminated (Event ID 4689): Startup Services Halted*
Observable 5 †	*Anomalous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657): Machine\system\controlset001\services\aelookupsvc "DeleteFlag"*
Observable 6 †	*Anomalous System Behavior on Local Host: Deletion of Files Named "backup"*
Observable 7 †	*Anomalous System Behavior on Local Host: Anomalous Command Line: C:\Windows\System32\cmd.exe"/c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default}bootstatuspolicy ignoreallfailures*
Observable 8 †	*Anomalous System Behavior on Local Host: Anomalous Command Line: vssadmin.exe Delete Shadows/All/Quiet*
Observable 9 †	*Anomalous System Behavior on Local Host: C:\Windows\System32\cmd.exe"/c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default}recoveryenabled No & bcdedit/set {default} bootstatuspolicy ignoreallfailures*
Observable 10 †	*Anomalous System Behavior on Local Host: Anomalous Increase in System Resource Utilization: Increase in CPU Utilization*
Observable 11 †	*Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity*
Observable 12 †	*Anomalous Deletion of Data: Deletion of Windows Shadow Volume*

Observables Associated with Loss of Control Technique (T0827)	
Observable 1	Anomalous System Behavior on Local Host: Creation of Anomalous CRC32 Hash: Using Hard-coded Seed Value: 0x539
Observable 2	Anomalous System Behavior on Local Host: Creation of Anomalous CRC32 Hash: Machine Serial Number Present in CRC32 Hash
Observable 3	Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: Containing Session Encryption Key "pk_key"
Observable 4	Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: Containing Session Encryption Key "ps_key"
Observable 5	Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: Containing Session Encryption Key "ps_key"
Observable 6	Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: Containing Session Encryption Key "0_key": ASCII Hash 79CD20FCE73EE1B81A433812C156281A04C92255E0D708BB9F0B1F1CB9130635
Observable 7 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Subkey: Hard-coded Value: "Software\recfg"*
Observable 8 †	*Anomalous System Behavior on Local Host: Presence of Anomalous File Extension: Random File Extension*

Observables Associated with Loss of Control Technique (T0827)	
Observable 9 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "bit" (CPU Architecture of the Host (86 refers to x86 or 32-bit CPU))*
Observable 10 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "bro" (True/false value indicating if a Russian keyboard layout was detected)*
Observable 11 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "dsk" (Base64-encoded binary value describing the host's fixed drive, including the drive letter, drive type, total size, and free space)*
Observable 12 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "grp" (Host's workgroup name)*
Observable 13 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "lng" (Host's locale information)*
Observable 14 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "net" (Host's hostname)*
Observable 15 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "os" (Host's operating system)*
Observable 16 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "pid" (Unknown integer value obtained from the ransomware's configuration; likely associated with the sub key and could be a campaign or affiliate identifier)*
Observable 17 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "pk" (Base64-encoded attacker's public key obtained from the ransomware's configuration and used in the file encryption process)*
Observable 18 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "sk" (Base64-encoded encrypted session private key generated at runtime and encrypted using the attacker's public key)*
Observable 19 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "sub" (Unknown integer value obtained from the ransomware's configuration; likely associated with the pid key and could be a campaign or affiliate identifier)*
Observable 20 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "uid" (UID value generated at runtime comprised of the CRC32 hash of both the host's volume serial number and CPUID)*
Observable 21 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "unm" (Victim's username)*
Observable 22 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: With JSON Structure: "ver" (Unknown hard-coded value that could be the ransomware executable version number)*
Observable 23 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: \Software\recfg\: With JSON Structure: "stat": 367D49308535C2C368604B4B7ABE8353ABE68E42F9C662A5D06AADC6F17DF61D*

Observables Associated with Loss of Control Technique (T0827)	
Observable 24 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Message on Screen: Ransom Note Demanding Payment: Request to Use TOR Browser*
Observable 25 †	*Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity*
Observable 26 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Registry Key: "wht": Folder Listed Within Configuration Key: "Tor Browser"*
Observable 27	Anomalous System Behavior on Local Host: Anomalous Read of File Contents Into Buffer
Observable 28 †	*Anomalous System Behavior on Local Host: Anomalous Overwrite of Existing Files: With Random Extensions*
Observable 29 †	*Anomalous System Behavior on Local Host: Anomalous Allocation of All Processing Capacity: Multiple Threads*

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1 †	*Anomalous System Behavior on Local Host: Presence of Anomalous File Extension: Random File Extension*
Observable 2 †	*Anomalous System Behavior on Local Host: Modification of Desktop Wallpaper: Bitmap Image: Grainy Blue Background: Semi-Random Integer Pixelation*
Observable 3	Anomalous System Behavior on Local Host: Anomalous Call to Binary on Host: user32.dll: SystemParametersInfoW Function
Observable 4	Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: SystemParametersInfoW
Observable 5	Anomalous System Behavior on Local Host: Creation of Anomalous Files: Within %TEMP% Folder: Random Characters in File Name: BMP Extension
Observable 6 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Message on Desktop: Ransom Note Demanding Payment: Request To Use TOR Browser*
Observable 7 †	*Anomalous System Behavior on Local Host: Loss of Application Functionality: Blank icon: Application Does Not Run Once Opened*
Observable 8 †	*Anomalous Loss of OT System Availability: Halt in Operations: Multiple Plants Worldwide*
Observable 9 †	*Anomalous System Behavior on Local Host: Presence of Anomalous File: .txt.file: {EXT}-HOW-TO-DECRYPT.txt*
Observable 10 †	*Anomalous System Behavior on Local Host: Presence of Anomalous File: Referencing BitCoin Address: 3E9F7gE3upQ8rgsPjwiKH7ugfdneypPjqj: (Hash 160) - 88975624eb26ac578b1911ae12f65593ff916025*

Observables Associated with Manipulation of View Technique (T0832)	
Observable 1 †	*Anomalous System Behavior on Local Host: Creation of Anomalous Files: Ransom Note*

Observables Associated with Manipulation of View Technique (T0832)	
Observable 2 †	*Presence of Anomalous Files on Host: Files with Anomalous File Names: Ransom Note*
Observable 3 †	*Anomalous System Behavior on Local Host: Modification of Desktop Wallpaper: Bitmap Image: Grainy Blue Background: Semi-Random Integer Pixelation*
Observable 4	Anomalous System Behavior on Local Host: Anomalous Call to Binary On Host: user32.dll: SystemParametersInfoW Function
Observable 5	Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: SystemParametersInfoW
Observable 6	Anomalous System Behavior on Local Host: Creation of Anomalous Files: Within %TEMP% folder: Random Characters in File Name: BMP Extension
Observable 7 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Message on Desktop: Ransom Note Demanding Payment: Request To Use TOR Browser*
Observable 8 †	*Anomalous System Behavior on Local Host: Creation of Anomalous Files: \Users\Adminstrator\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper*
Observable 9 †	*Anomalous System Behavior on Local Host: Presence of Anomalous Message on Screen: Ransom Note Demanding Payment: Request to Use TOR Browser*

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1 †	*Anomalous Loss of Revenue: Ransom Payment: $11,000,000*
Observable 2 †	*Anomalous Loss of Productivity: Multi-day Closure of Plant Operations: Nine U.S. Plants: Loss of One-Quarter of U.S. Beef-processing Capacity*
Observable 3 †	*Anomalous Loss of Productivity: Multi-day Closure of Plant Operations: Multiple Australian Plants*
Observable 4 †	*Anomalous Loss of Productivity: Multi-day Closure of Plant Operations: 1 Canadian Plant*
Observable 5 †	*Anomalous Loss of Revenue: Company Stock Valuation Decrease*

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 Exploitation for Privilege Escalation Technique (T0890)	
Artifact 1	Unexpected Process Crash
Artifact 2	Network Traffic Associated with Privilege Escalation Vulnerabilities (CVE-2014-4076 Sent a Specially Crafted TCP Packet to \\.\\ TCP Device Through DEVICEIOCONTROL Function
Artifact 3	Unusual Process Activity (Thread Suspension of Everything Except Thread Running In a Process Other Than Exploit Thread)*
Artifact 4	SYSMON Event 8 CREATEREMOTETHREAD Process Injection Detected
Artifact 5	Unusual Command Line History Associated with Known CVE Techniques (CVE-2019-5736 Privilege Escalation Is Visible via Unusual Command Line Commands)
Artifact 6	Suspicious File Write to System Directory Followed by Privileged Execution of File
Artifact 7	Execution of a Suspicious File in The System32 or Windows Directory At Privileged Level
Artifact 8	Unusual or Unexpected KERBEROS Ticket Requests
Artifact 9	Suspicious Files Written to Disk
Artifact 10	Suspicious Program Running Under SYSTEM or Other Elevated Account
Artifact 11	Driver Loaded (SYSMON Event)
Artifact 12	Network Traffic Matching Vulnerability (Snort, SURICATA)
Artifact 13	Abnormal Reads/Writes Between Processes
Artifact 14	Unusual Command Line Arguments to Application (lolbins)
Artifact 15	Artifacts Associated with Known Privilege Escalation CVES (PE Hard Coded Debug File Path for APT28 Malware Included Reference to CVE-2014-4076 Privilege Escalation)
Artifact 16	Unusual or Unexpected Child Process Running At Elevated Privileges

Artifacts Associated with Exploitation of Remote Services Technique (T0866)	
Artifact 1	Application Logs
Artifact 2	Connection to HMI End Points
Artifact 3	Connection to EWS End Points
Artifact 4	Connection to Data Historian End Points
Artifact 5	Connection to Controller End Points
Artifact 6	Manipulation of Process
Artifact 7	Manipulation of Set Points

Artifacts Associated with Exploitation of Remote Services Technique (T0866)	
Artifact 8	Misconfigurations of End Points
Artifact 9	Process Failure
Artifact 10	Controller Failure
Artifact 11	Code Injections into Application
Artifact 12	Application Logon Event
Artifact 13	Code Injection into The OS
Artifact 14	OPC Code Injection
Artifact 15	Database Command Executions
Artifact 16	User Events Across Multiple Devices
Artifact 17	Host System Registry Changes
Artifact 18	Security Events Across Multiple Devices
Artifact 19	Kernel Level Events
Artifact 21	System Reboots
Artifact 22	Blank Screens
Artifact 23	Safe Mode Reboot
Artifact 24	Application Logoff Event
Artifact 25	Alarm Events
Artifact 26	Absence of Alarm Events
Artifact 27	Common Network Traffic
Artifact 28	Remote Network Traffic
Artifact 29	Vendor Specific Network Traffic
Artifact 30	Industrial Protocol Network Traffic
Artifact 31	SQL Protocol

Artifacts Associated with Exploitation for Evasion Technique (T0820)	
Artifact 1	External Sender IP Address
Artifact 2	Software Vulnerability
Artifact 3	Zero-Day Announcement
Artifact 4	Protocol Vulnerability
Artifact 5	Pip Use

Artifacts Associated with Native API Technique (T0834)	
Artifact 1	Alert Generated
Artifact 2	System Resource Usage Management Changes

Artifacts Associated with Native API Technique (T0834)	
Artifact 3	.dll Modifications
Artifact 4	Imports Hash Changed
Artifact 5	Files Created
Artifact 6	Processes Initiated
Artifact 7	Services Initiated
Artifact 8	SYSMON Events Created
Artifact 9	Performance Degradation
Artifact 10	Blue Screen
Artifact 11	Configuration Change
Artifact 12	Command Execution
Artifact 13	Industrial Protocol Command Packet
Artifact 14	Host Device Failure
Artifact 15	Industrial Network Traffic
Artifact 16	Device Reads
Artifact 17	Device I/O Image Table Manipulated
Artifact 18	Device Failure
Artifact 19	Systems Calls
Artifact 20	Device Performance Degradation
Artifact 21	Device Memory Modification
Artifact 22	Device Alarm
Artifact 23	Device Live Data Changes
Artifact 24	Alter Process Logic
Artifact 25	Memory Corruption

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

Artifacts Associated with Valid Accounts Technique (T0859)	
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 Commonly Used Port Technique (T0885)	
Artifact 1	Unexpected Process Usage of Common Port Observed via Firewall Logs
Artifact 2	Unexpected Process Usage of Common Port Observed via OS Commands (netstat)
Artifact 3	Unexpected Process Usage of Common Port Observed via Memory
Artifact 4	Unexpected Process Usage of Common Port Observed via OS Logs
Artifact 5	Unexpected Host Communicating with Common Port on Industrial Asset

Artifacts Associated with Connection Proxy Technique (T0884)	
Artifact 1	Unexpected Process Usage of Network Proxy Port Observed via Memory
Artifact 2	Unusual Network or Host Communications Identified in Network Proxy Log
Artifact 3	Unexpected Host Communicating with Network Proxy Port on Industrial Asset
Artifact 4	Unexpected Process Usage of Network Proxy Port Observed via OS Logs
Artifact 5	Unexpected Application Communication to Network Proxy Port in Command Line Output (netstat)
Artifact 6	Unexpected Process Usage of Network Proxy Port Observed via Firewall Logs

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

Artifacts Associated with Standard Application Layer Protocol Technique (T0869)	
Artifact 9	DNS Traffic Port
Artifact 10	HTTP Post Request
Artifact 11	HTTPS Traffic Port
Artifact 12	Network Content Metadata

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

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

Artifacts Associated with 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 Remote Services Technique (T0886)	
Artifact 1	Mouse Movement
Artifact 2	Authentication Logs
Artifact 3	Network Traffic Content Creation
Artifact 4	Remote Session Creation Timestamp
Artifact 5	Process Creation

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 6	VNC Traffic
Artifact 7	SMB Traffic
Artifact 8	SSH Traffic
Artifact 9	MSSQL Traffic 1433 Port
Artifact 10	File Movement
Artifact 11	Desktop Prompt Windows Created
Artifact 12	GUI Modifications
Artifact 13	System Log Event
Artifact 14	RDP Traffic
Artifact 15	Application Log
Artifact 16	Session Cache
Artifact 17	Unexpected
Artifact 18	Registry Connection Change
Artifact 19	Registry Changes
Artifact 20	Logoff Event
Artifact 21	Logoff
Artifact 22	Logon Event
Artifact 23	Remote Client Connection
Artifact 24	Data File Size in Network Content

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

Artifacts Associated with Masquerading Technique (T0849)	
Artifact 1	Command Line Execution
Artifact 2	Additional Functionality in Applications
Artifact 3	Applications Causing Unintended Actions
Artifact 4	Leetspeak File Creation

Artifacts Associated with Masquerading Technique (T0849)	
Artifact 5	File Modification
Artifact 6	Process Metadata Changes
Artifact 7	Common Application with Non-Native Child Processes
Artifact 8	Scheduled Job Metadata
Artifact 9	Services Metadata
Artifact 10	Service Creation
Artifact 11	Scheduled Job Modification
Artifact 12	Additional File Directories Created
Artifact 13	File Creation with Common Name
Artifact 14	Leetspeak User Metadata
Artifact 15	Warez Application Use

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

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 7	System Call
Artifact 8	System Application Interruption
Artifact 9	Device Failure
Artifact 10	Recovery Attempt Failure
Artifact 11	TFTP Port
Artifact 12	SFTP Port
Artifact 13	Memory Corruption
Artifact 14	Use of File Transfer Protocols
Artifact 15	SCP Port
Artifact 16	File Encryptions
Artifact 17	Non-Native Files
Artifact 18	External Network Connections
Artifact 19	Transient Device Connections
Artifact 20	Program Execution
Artifact 21	Telnet Port
Artifact 22	FTPS Port
Artifact 23	HTTP Port
Artifact 24	HTTPS Port
Artifact 25	Local Network Connections
Artifact 26	FTP Port
Artifact 27	SMB Port

Artifacts Associated with 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

Artifacts Associated with Loss of Control Technique (T0827)	
Artifact 12	Process Alarms
Artifact 13	Device Failure

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

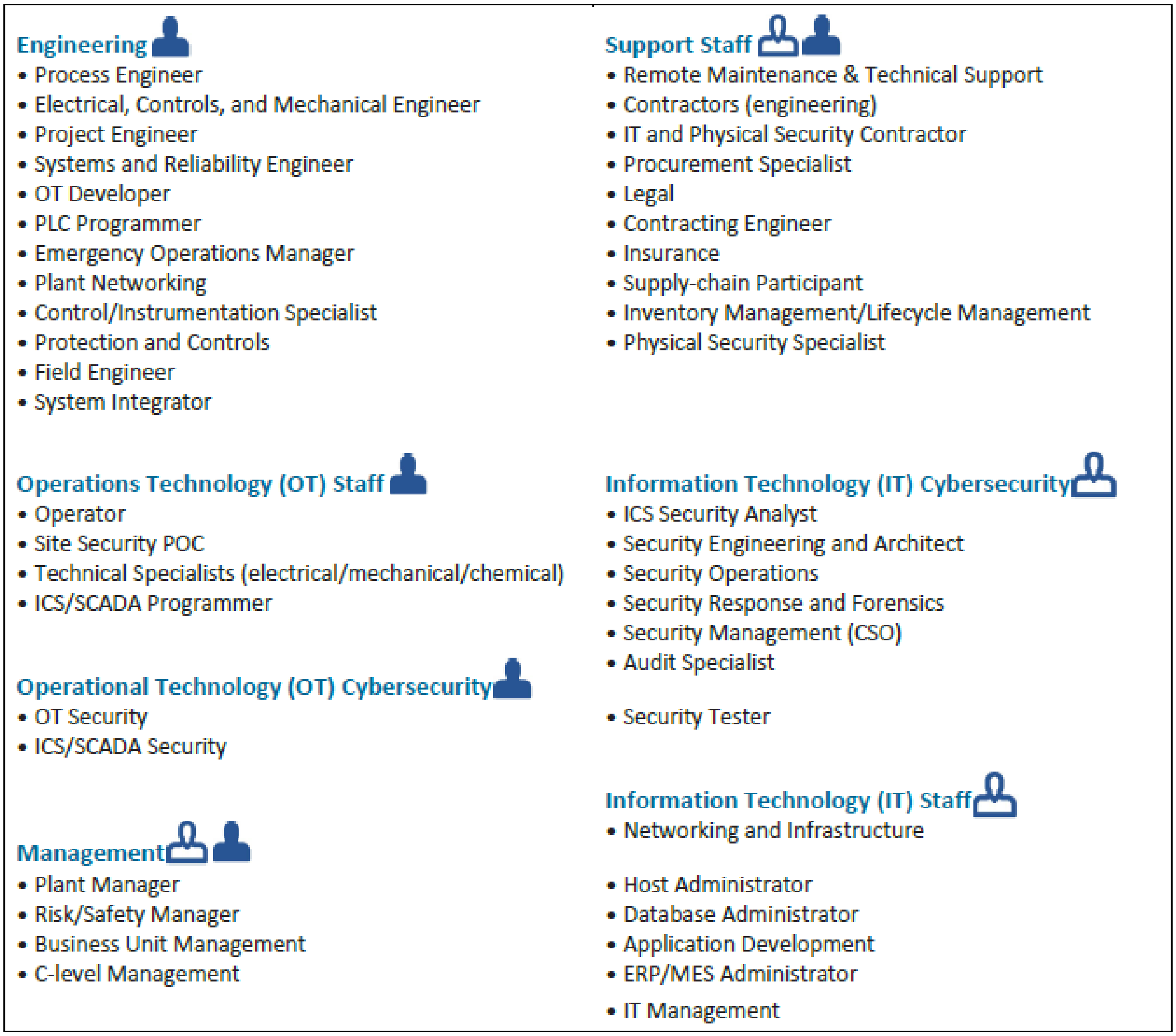
Artifacts Associated with Manipulation of View Technique (T0832)	
Artifact 1	Modification of Operating System or The Installation of a Filter Driver Could Lead to Manipulations of Packet at The Kernel Level
Artifact 2	File System Modification Artifacts Might Be Associated with The Manipulation of View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

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

Artifacts Associated with Loss of Productivity and Revenue Technique (T0828)	
Artifact 5	File System Modification Artifacts Might Be Associated with the Loss of Productivity and Revenue Attack Might Be Present on Disk

APPENDIX C: OBSERVERS

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



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] [NPR | “REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says” | https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says | 3 June 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[2] [JBS Foods | “JBS USA Cyberattack Media Statement - June 9” | https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9 | 9 June 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[3] [Trend Micro | “QAKBOT Loader Returns with New Techniques and Tools” | https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html | 13 November 2021 | Accessed on 16 February 2023 | The source is publicly available information and does not contain classification markings]

[4] [SecurityScorecard | Ryan Sherstobitoff | “JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified” | https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march | 8 June 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[5] [JBS Foods | “JBS USA Cyberattack Media Statement - June 9” | https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9 | 9 June 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[6] [MITRE Att&ck Framework | Edward Millington | “REvil” | https://attack.mitre.org/software/S0496/ | 4 August 2020 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[7] [U.S. Department of Health and Human Services | Ryan Sherstobitoff | “Qbot and Ransomware” | https://www.hhs.gov/sites/default/files/qbot-qakbot-ransomware-tlpwhite.pdf | 5 August 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[8] [U.S. Department of Health and Human Services | Ryan Sherstobitoff | “Qbot and Ransomware” | https://www.hhs.gov/sites/default/files/qbot-qakbot-ransomware-tlpwhite.pdf | 5 August 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[9][Trend Micro | “QAKBOT Loader Returns with New Techniques and Tools” | https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html | 13 November 2021 | Accessed on 16 February 2023 | The source is publicly available information and does not contain classification markings]

[10] [Secureworks | Counter Threat Unit Research Team | “REvil/Sodinokibi Ransomware” | https://www.secureworks.com/research/revil-sodinokibi-ransomware | 24 September 2019 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[11] [CISCO | “Security Threat Protection: The REvil Ransomware” | https://blogs.cisco.com/security/threat-protection-the-revil-ransomware | 11 August 2021 | Accessed 16 February 2023 | The source is publicly available information and does not contain classification markings]

[12] [Secureworks | Counter Threat Unit Research Team | “REvil/Sodinokibi Ransomware” | https://www.secureworks.com/research/revil-sodinokibi-ransomware | 24 September 2019 | Accessed on

20 December 2022 | The source is publicly available information and does not contain classification markings]

[13] [IronNet | Morgan Demboski, Joey Fitzpatrick, and others | “How IronNet's Behavioral Analytics Detect REvil and Conti Ransomware” | https://www.ironnet.com/blog/ransomware-graphic-blog | 16 November 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[14] [Microsoft | Windows App Development | “Mandatory Integrity Control” | https://learn.microsoft.com/en-us/windows/win32/secauthz/mandatory-integrity-control | 25 March 2021 | Accessed 22 March 2023 | The source is publicly available information and does not contain classification markings]

[15] [Secureworks | Counter Threat Unit Research Team | “REvil/Sodinokibi Ransomware” | https://www.secureworks.com/research/revil-sodinokibi-ransomware | 24 September 2019 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[16] [IronNet | Morgan Demboski, Joey Fitzpatrick, and others | “How IronNet's Behavioral Analytics Detect REvil and Conti Ransomware” | https://www.ironnet.com/blog/ransomware-graphic-blog | 16 November 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[17] [CISCO | “Security Threat Protection: The REvil Ransomware” | https://blogs.cisco.com/security/threat-protection-the-revil-ransomware | 11 August 2021 | Accessed on 16 February 2023 | The source is publicly available information and does not contain classification markings]

[18] [Trend Micro | “REvil” | https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil | 20 December 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[19] [U.S. Department of Health and Human Services | Ryan Sherstobitoff | “Qbot and Ransomware” | https://www.hhs.gov/sites/default/files/qbot-qakbot-ransomware-tlpwhite.pdf | 5 August 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[20] [IronNet | Morgan Demboski, Joey Fitzpatrick, and others | “How IronNet's Behavioral Analytics Detect REvil and Conti Ransomware” | https://www.ironnet.com/blog/ransomware-graphic-blog | 16 November 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[21] [Trend Micro | “REvil” | https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil | 20 December 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[22] [MITRE Att&ck Framework | Edward Millington | “REvil” | https://attack.mitre.org/software/S0496/ | 4 August 2020 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[23] [CISCO | “Security Threat Protection: The REvil Ransomware” | https://blogs.cisco.com/security/threat-protection-the-revil-ransomware | 11 August 2021 | Accessed on 16 February 2023 | The source is publicly available information and does not contain classification markings]

[24] [Trend Micro | “REvil” | https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil | 20 December 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[25] [McAfee | “McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – What The Code Tells Us” | https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-

revil-ransomware-as-a-service-what-the-code-tells-us/ | 2 October 2019 |Accessed 20 December 2022 | The source is publicly available information and does not contain classification markings]

[26] [Secureworks | Counter Threat Unit Research Team | "REvil/Sodinokibi Ransomware" | https://www.secureworks.com/research/revil-sodinokibi-ransomware | 24 September 2019 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[27] [SecurityScorecard | Ryan Sherstobitoff | "JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified" | https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march | 8 June 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[28] [IronNet | Morgan Demboski, Joey Fitzpatrick and others | "How IronNet's Behavioral Analytics Detect REvil and Conti Ransomware" | https://www.ironnet.com/blog/ransomware-graphic-blog | 16 November 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[29] [SecurityScorecard | Ryan Sherstobitoff | "JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified" | https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march | 8 June 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[30] [SecurityScorecard | Ryan Sherstobitoff | "JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified" | https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march | 8 June 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[31] [SecurityScorecard | Ryan Sherstobitoff | "JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified" | https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march | 8 June 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[32] [Trend Micro | "QAKBOT Loader Returns with New Techniques and Tools" | https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html | 13 November 2021 | Accessed on 16 February 2023 | The source is publicly available information and does not contain classification markings]

[33] [SecurityScorecard | Ryan Sherstobitoff | "JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified" | https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march | 8 June 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[34] [U.S. Department of Health and Human Services | Ryan Sherstobitoff | "Qbot and Ransomware" | https://www.hhs.gov/sites/default/files/qbot-qakbot-ransomware-tlpwhite.pdf | 5 August 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[35] [MITRE Att&ck Framework | Edward Millington | "REvil" | https://attack.mitre.org/software/S0496/ | 4 August 2020 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[36] [Trend Micro | "QAKBOT Loader Returns with New Techniques and Tools" | https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html | 13 November 2021 | Accessed on 16 February 2023 | The source is publicly available information and does not contain classification markings]

[37] [Trend Micro | "QAKBOT Loader Returns with New Techniques and Tools" | https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-

tools.html | 13 November 2021 | Accessed on 16 February 2023 | The source is publicly available information and does not contain classification markings]

[38] [CISCO | “Security Threat Protection: The REvil Ransomware” | https://blogs.cisco.com/security/threat-protection-the-revil-ransomware | 11 August 2021 | Accessed on 16 February 2023 | The source is publicly available information and does not contain classification markings]

[39] [Secureworks | Counter Threat Unit Research Team | “REvil/Sodinokibi Ransomware” | https://www.secureworks.com/research/revil-sodinokibi-ransomware | 24 September 2019 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[40] [Secureworks | Counter Threat Unit Research Team | “REvil/Sodinokibi Ransomware” | https://www.secureworks.com/research/revil-sodinokibi-ransomware | 24 September 2019 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[41][Secureworks | Counter Threat Unit Research Team | “REvil/Sodinokibi Ransomware” | https://www.secureworks.com/research/revil-sodinokibi-ransomware | 24 September 2019 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[42] [ProQuest | Matthew Fitzgerald | “Tactics, Techniques, and Procedures (TTPs) of Ransomware Groups and the Threats Posed to United States National Security” | https://www.proquest.com/openview/a1c2c2ab19921b6dbd43cf2ba343ecba/1?pq-origsite=gscholar&cbl=18750&diss=y | 1 June 2022 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]

[43] [CISCO | “Security Threat Protection: The REvil Ransomware” | https://blogs.cisco.com/security/threat-protection-the-revil-ransomware | 11 August 2021 | Accessed on 16 February 2023 | The source is publicly available information and does not contain classification markings]

[44] [JBS Foods | “JBS USA Cyberattack Media Statement - June 9” | https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9 | 9 June 2021 | Accessed on 20 December 2022 | The source is publicly available information and does not contain classification markings]