DISCLAIMER

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

PRECURSOR ANALYSIS REPORT: BLACKMATTER RANSOMWARE ATTACK ON NEW COOPERATIVE 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

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

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

TABLE OF CONTENTS

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: BLACKMATTER RANSOMWARE ATTACK ON NEW COOPERATIVE 2021

1. EXECUTIVE SUMMARY

The BlackMatter Ransomware Attack on New Cooperative 2021 Precursor Analysis Report leverages publicly available information about the New Cooperative cyber attack and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

The BlackMatter ransomware was first identified in July 2021 and is reported to have infected more than 50 corporations around the world.[1,2] The Iowa-based grain cooperative, New Cooperative, was impacted by the BlackMatter ransomware on or before 18 September 2021.[3] The adversary likely resided on New Cooperative's networks for 15 days prior to encrypting its network and demanding New Cooperative pay $5.9 million in ransom by 25 September to unlock systems and prevent 1 terabyte (TB) of sensitive data from being publicly released.[4] It is not clear if New Cooperative paid the ransom.

The full impact of the ransomware attack is not known; however, according to New Cooperative's general manager, the attack caused the company's automated processes to revert back to processes used in the 1970s.[5,6] As of 6 October, only 50 percent of New Cooperative's operations were utilizing automated processes.[7] The company took eight weeks to rebuild the entire network and information technology (IT) systems from the ground up, which puts the date of fully recovery around 13 November.[8]

Researchers and analysts identified 20 unique techniques utilized during the attack with a total of 404 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. Seventeen of the identified techniques used during the New Cooperative cyber attack were precursors to the triggering event. Analysis identified 360 observables associated with these precursor techniques, 284 of which were assessed to have an increased likelihood of being perceived in the 15 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

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

2. INTRODUCTION

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

2.1. APPLYING THE CYOTE METHODOLOGY

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

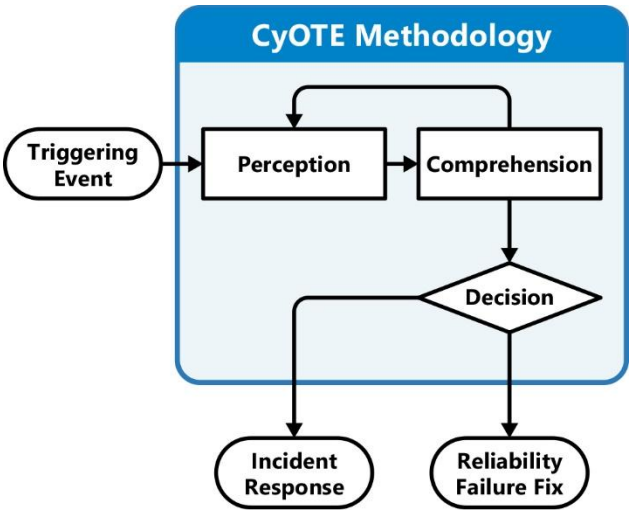

Figure 1. CyOTE Methodology

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

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

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

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

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

2.2. BACKGROUND ON THE ATTACK

The Iowa-based grain cooperative, New Cooperative, was a victim of a human-operated[a] BlackMatter ransomware attack on or before 18 September 2021 (D-0).[9,10]

The adversary first stole 1 Terabyte (TB) of sensitive data, then encrypted hosts on New Cooperative's network, leaving ransom notes on the backgrounds of computer screens.

The adversary then demanded the company pay a $5.9 million ransom by 25 September to unlock systems and prevent public release of the stolen data.[11]

The full impact of the attack is not known; however, according to New Cooperative's general manager, the attack caused the company's automated processes to revert to processes used in the 1970s.[12,13] It took the company roughly eight weeks to recover from the attack.

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.

CyOTE analysts assess that New Cooperative was likely compromised on 3 September (D-15), based on two prior BlackMatter ransomware infections, both of which involved 15-day lead times.[14]

The initial access vector for New Cooperative has not been confirmed, although public-facing applications likely were exploited to gain network access. Exploitation of compromised credentials may have also been used to enable access.[15,16]

Shortly after the initial infection, the adversary likely established command-and-control (C2) infrastructure over hypertext transfer protocol secure (HTTPS) using advance encryption standard (AES) encryption. [17,18,19] This was likely done to disguise adversary actions as benign network traffic.[20]

During this two-week period before New Cooperative's network was encrypted, the adversary enumerated the victim's network using native application programmatic interface (API) and automated collection techniques. The adversary was also able to traverse the victim's network and execute commands using remote services.

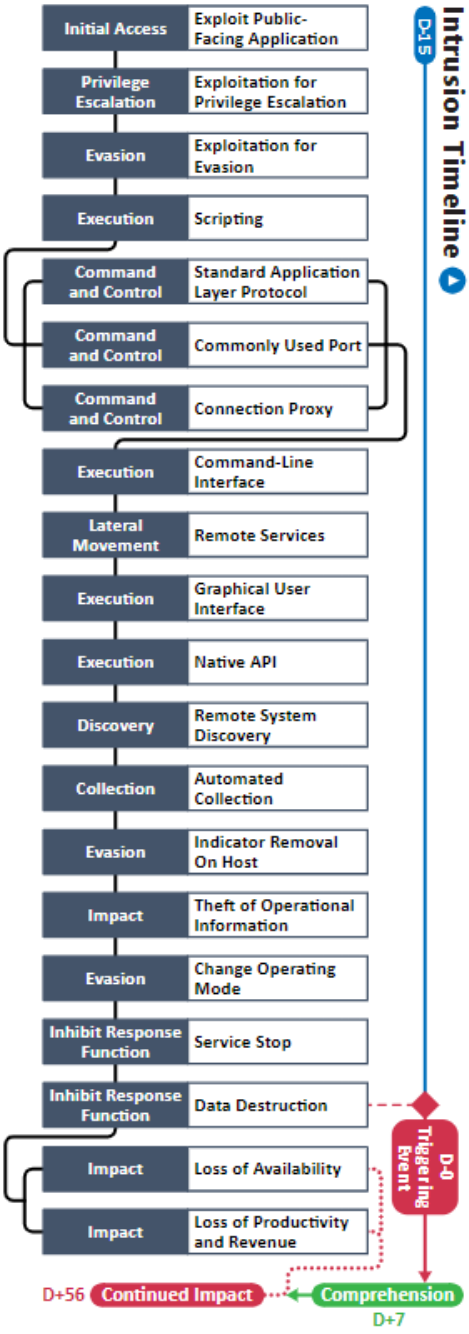

Figure 2. Intrusion Timeline

[a] BlackMatter is a human-operated ransomware in which an adversary uses their insights to infiltrate a network, navigate and enumerate the network while seeking to elevate privileges, and then deploying the ransomware.

The adversary collected and exfiltrated 1 TB of sensitive corporate data prior to beginning the encryption process, which CyOTE analysts assess took place on or before 18 September (D-0). The initial steps of the encryption process likely involved the adversary terminating processes and services and deleting backup files.[21] File encryption was carried out from a single network share by remotely distributing the encryption executable to domain servers inside the system volume (SYSVOL) folder, which impacted all systems in the domain.[22] BlackMatter ransomware uses Salsa20 cipher and an RSA-1024 public key to encrypt key files.[23,24] As part of the encryption process, ransom note files were saved to files, and also were displayed on the background of computer screens, which served as the triggering event for the attack (D-0).[25]

According to New Cooperative's general manager, the attack caused the company's automated processes to become inoperable, and on 25 September (D+7) the adversary demanded New Cooperative pay a $5.9 million ransom to unlock systems and prevent the stolen sensitive data from being publicly released.[26]

In terms of impact, as of 6 October 50 percent of the company's operations were utilizing automated processes. Recovery reportedly required eight weeks to rebuild the entire network and IT systems, which puts the date of full recovery around 13 November (D+56).[27]

Analysis identified 20 unique techniques in a sequence and timeframe likely used by adversaries during this cyber attack (**Error! Reference source not found.** 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Blackmatter New Cooperative 2021 Cyber Attack

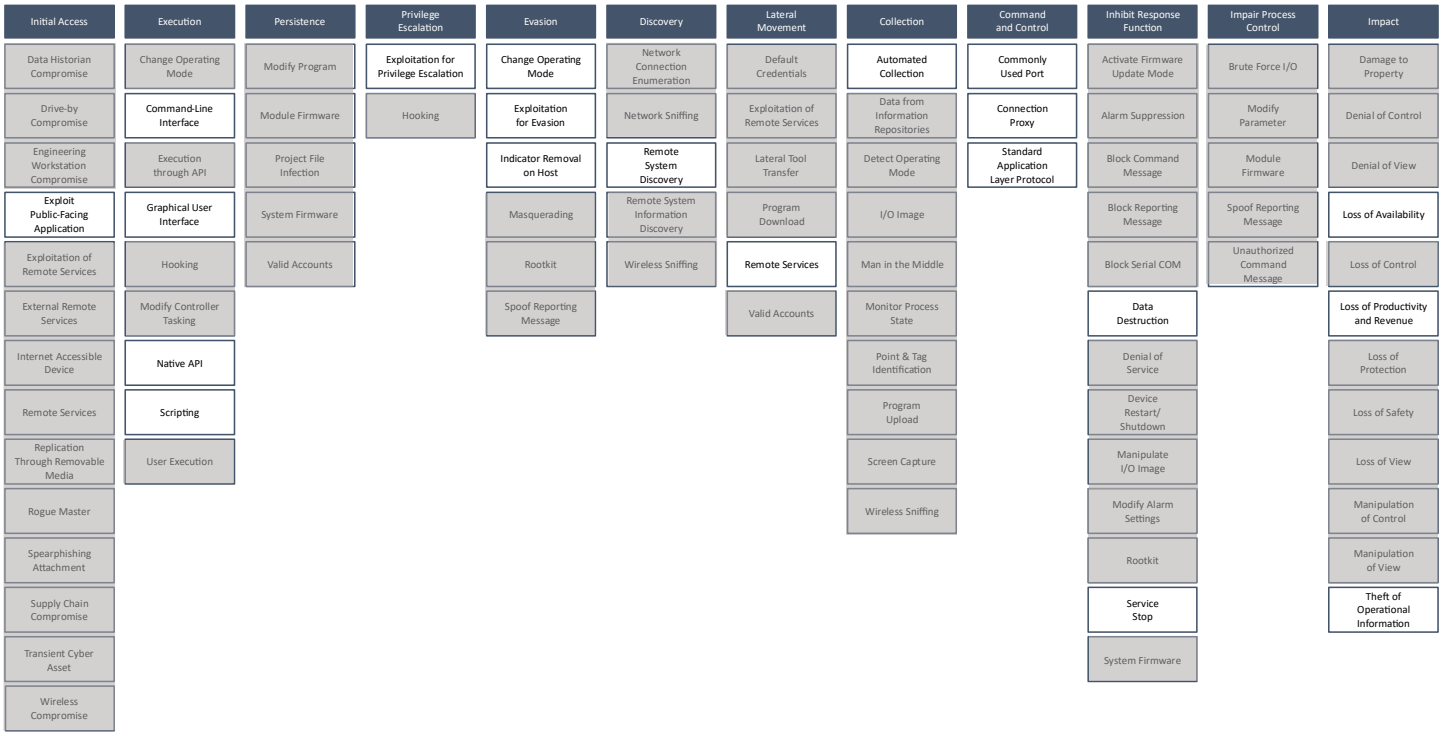

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	**20**
Technique Observables	**404**
Precursor Techniques	**17**
Precursor Technique Observables	**160**
Highly Perceivable Precursor Technique Observable	**281**

3. OBSERVABLE AND TECHNIQUE ANALYSIS

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

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

The initial access vector for New Cooperative has not been confirmed; however, previous reporting indicates public-facing applications, along with exploitation of compromised credentials, may have been exploited to gain network access. In addition, the adversary may have used Microsoft Exchange vulnerabilities (CVE-2022-41040 and CVE-2022-41082) in the attack.[28,29,30]

IT Staff and IT Cybersecurity personnel may have been able to observe the adversary's unauthorized access via vulnerable edge devices from anomalous IPs, login timestamps, and client information present within log entries.

A total of 23 observables were identified with the use of the Exploit Public-Facing Application technique (T0819). This technique is important for investigation to understand how the adversary accessed and traversed the network, as it provides both network and host-based evidence of adversarial behavior in the IT environment. Terminating the chain of techniques at this point would minimize the opportunities for an adversary to gain access to the IT environment.

Of the 23 observables associated with this technique, 17 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 55 artifacts could be generated by the Exploit Public-Facing Application technique
Technique Observers[b]	IT Staff, IT Cybersecurity
Resources	Technique Detection References

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

3.2. EXPLOITATION FOR PRIVILEGE ESCALATION TECHNIQUE (T0890) FOR PRIVILEGE ESCALATION

BlackMatter verifies user privileges and if the privileges are restricted by Microsoft's User Account Control (UAC), privileges may be escalated using the ICMLuaUtil COM interface.[31] ICMLuaUtil is essentially a UAC bypass on some Windows Operating Systems (OS) to elevate privileges.[32]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous log activity.

A total of 19 observables were identified with the use of the Exploitation for Privilege Escalation technique (T0890). This technique is important for investigation to understand how the adversary can elevate privileges, enabling network traversal. This technique appears early in the timeline and responding to it will limit the adversary's privileges to that of the user account being leveraged. Terminating the chain of techniques at this point would challenge the adversary's ability to spread throughout the network.

Of the 19 observables associated with this technique, 15 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 16 artifacts could be generated by the Exploitation for Privilege Escalation technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

3.3. EXPLOITATION FOR EVASION TECHNIQUE (T0820) FOR EVASION

The BlackMatter adversary exploits the Windows OS vulnerability, ICMLuaUtil COM interface, to escalate privileges and evade detection by circumventing Microsoft's UAC. [33]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous system behavior and network traffic.

A total of 12 observables were identified with the use of the Exploitation for Evasion technique (T0820). This technique is important for investigation, as it is a mechanism by which an adversary could minimize detection. This technique appears early in the timeline and responding to it will challenge the adversary's ability to operate undetected.

Of the 12 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	A total of 30 artifacts could be generated by the Exploitation for Evasion technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

3.4. SCRIPTING TECHINQUE (T0853) FOR EXECUTION

The adversary used scripts with remote service tools to execute commands throughout the attack to accomplish specific tasks, including discovery, lateral movement, and performing uploads and downloads.[34]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous commands being issued in unexpected locations throughout the network via network monitoring and log inspections.

A total of 26 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation as it is a powerful mechanism by which an adversary can remotely execute commands to exert control throughout the network. This technique appears early in the timeline and responding to it will challenge the adversary's ability to execute commands and laterally move through the network.

Of the 26 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	A total of 12 artifacts could be generated by the Scripting technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

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

Following initial access and infection, the BlackMatter ransomware establishes communications with the adversary's C2 infrastructure over HTTPS using AES encryption.[35] Commonly used application layer protocols may be used to disguise adversary actions as benign network traffic. As part of C2 communications, the adversary uses a POST request with AES-128 encryption to obtain information, which includes the victim's machine name, OS version, CPU architecture, OS language, username, domain name, disk sizes, and potential encryption keys.[36] The BlackMatter ransomware is known to impersonate the following user-agent strings: Mozilla/5.0 (Windows NT 6.1), Firefox/89.0, Gecko/20100101, Edge/91.0.864.37, and Safari/537.36.[37]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous traffic and protocol usage associated with the adversary's C2 communications.

A total of 14 observables were identified with the use of the Standard Application Protocol technique (T0869). This technique is important for investigation because it allows defenders to identify which internal hosts are communicating with anomalous external domains and hosts. This technique appears early in the timeline, and responding to it will degrade adversarial external C2 communications. 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 14 observables associated with this technique, 11 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

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

BlackMatter infections use HTTPS (Port 443) for C2 communications, which may be utilized to bypass the firewall or network detection systems and to blend in with benign network traffic.[38,39]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous traffic and protocol usage associated with the adversary's C2 communications.

A total of 14 observables were identified with the use of the Commonly Used Port technique (T0885). This technique is important for investigation because it allows the adversary to disguise and blend their traffic with legitimate network traffic passing through passive boundary protection defenses. This technique appears repeatedly throughout the timeline and responding to it will prevent the adversary from establishing C2 communication between the victim's network and the adversary's C2 servers.

Of the 14 observables associated with this technique, 11 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

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

BlackMatter infections use the GO Simple Tunnel (GOST), which is a tool that acts as a proxy and establishes a reverse SSH tunnel to a C2 server.[40]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous traffic and protocol usage associated with the adversary's C2 communications.

A total of seven observables were identified with the use of the Connection Proxy technique (T0884). This technique is important for investigation as it presents a detection and perception opportunity for defenders within the local network. This technique appears in the middle of the timeline and terminating the attack chain here would prevent the malware from exchanging data with the C2 server.

Of the seven 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	A total of six artifacts could be generated by the Connection Proxy technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

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

The adversary employed the command-line interface (CLI) technique via cmd.exe to issue commands such as remote services.[41]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe via network traffic and log activity.

A total of 17 observables were identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation because it is the means by which the adversary loads, transfers, and executes malware while manipulating local hosts and network environments. This technique appears throughout the timeline and responding to it will effectively eliminate the adversary's primary means of execution.

Of the 17 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	A total of 25 artifacts could be generated by the Command-Line Interface technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.9. REMOTE SERVICES TECHNIQUE (T0886) FOR LATERAL MOVEMENT

While the use of this technique has not been confirmed for the New Cooperative incident, in other BlackMatter attacks the adversary used remote services for network traversal and to execute commands on remote systems. The primary tools include Impacket's wmiexec, PowerShell using WinRM service, RemCom (open-source version of PSECEC), and Microsoft Remote Desktop Protocol (RDP), which was used for GUI access to remote systems.[42]

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

A total of 17 observables were identified with the use of the Remote Services technique (T0886). This technique is important for investigation because it is how the adversary remotely accesses and transmits data between discovered local network hosts. This technique appears throughout the timeline and responding to it will effectively eliminate the adversary's remote access to local network hosts. Terminating the chain of techniques at this point would limit the spread of malware within the victim's internal network and limit the means for data exfiltration.

Of the 17 observables associated with this technique, 15 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.10. GRAPHICAL USER INTERFACE TECHNIQUE (T0823) FOR EXECUTION

The adversary used RDP to obtain a GUI to the victims' systems in prior BlackMatter attacks.[43] A GUI allows the adversary to execute applications and programs in the victim's environment using a cursor and keyboard, as opposed to a command line interface.[44]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe anomalous logs, running processes, and files.

A total of 14 observables were identified with the use of the Graphical User Interface technique (T0823). This technique is important for investigation because adversaries may enhance their execution capabilities and gain access to additional hosts. This technique appears in the middle of the timeline, and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would limit operational damage, as the adversary would not have enhanced functionality to access victim computing assets or pivot into additional subnets within the victim's operating environment.

Of the 14 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	A total of 60 artifacts could be generated by the Graphical User Interface technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.11. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

The adversary employs OS APIs to call OS functions.[45] The ransomware uses standard API functions to enumerate computers in Active Directory (AD) via ADsOpenObject, ADsBuildEnumerator, and ADsEnumerateNext.[46] The BlackMatter ransomware internally resolves Win32 API calls at runtime, making suspicious imports and functions less obvious.[47] The ransomware also uses dynamic API functions to prevent anomalous files from being detected.[48]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe anomalous operations and performance issues.

A total of 19 observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because it is the lowest-level means of execution to call to hardware, memory space, and process services for execution evasion. This technique appears repeatedly throughout the timeline and responding to it has the potential to effectively eliminate the ability of BlackMatter to discover additional hosts within the victim's operating environment.

Of the 19 observables associated with this technique, 17 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.12. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

The adversary uses the NetShareEnum function, via a remote procedure call (RPC), to retrieve information about each shared resource as part of the discovery process.[49,50] Lightweight Directory Access Protocol (LDAP) and Server Message Block (SMB) protocols are used to discover all hosts in the AD.[51]

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

A total of 20 observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation as it determines how the adversary enumerates systems and traverses the network. This technique appears in the middle of the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent system discovery, stopping further lateral movement through the network.

Of the 20 observables associated with this technique, 17 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 43 artifacts could be generated by the Remote System Discovery technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

3.13. AUTOMATED COLLECTION TECHNIQUE (T0802) FOR COLLECTION

Adversaries use protocols to automate collection of data about victims' environments. LDAP and SMB protocols are used to access AD to discover all hosts on the network.[52] Attributes for each computer account are retrieved via LDAP from AD, while shares are accessed with SMB.[53]

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

A total of 21 observables were identified with the use of the Automated Collection technique (T0802). This technique is important for investigation as it determines how the adversary enumerates systems and traverses the network. This technique appears in the middle of the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent system discovery.

Of the 21 observables associated with this technique, 15 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 23 artifacts could be generated by the Automated Collection technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

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

BlackMatter ransomware takes multiple steps to evade detection, which includes deleting files and logs. To hide the malware's process execution, the called functions are decoded and loaded to memory prior to execution. Following execution, related files are deleted.[54,55]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe anomalies in logs, such as gaps and missing files.

A total of 23 observables were identified with the use of the Indicator Removal on Host technique (T0872). This technique is important for investigation to identify anomalies resulting from infections. This technique appears in the middle of the timeline and responding to it will support detection and prevention efforts. Terminating the chain of techniques at this point would prevent further damage to the system.

Of the 23 observables associated with this technique, 20 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 23 artifacts could be generated by the Indicator Removal on Host technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

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

Prior to data encryption, BlackMatter exfiltrates data that will be used as leverage by the adversary, who will threaten to release it to coerce victims into paying the ransom.[56] The malware exfiltrates files with extensions doc, docx, xls, xlsx, pdf, msg, png, ppt, pptx, sda, sdm, sdw, and csv.[57]

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

A total of 29 observables were identified with the use of the Theft of Operational Information technique (T0882). This technique is important for investigation as data exhilaration can be used to identify anomalous network traffic. This technique appears near the triggering event and responding to it may challenge the adversary's access to some corporate data that could be used as leverage. Terminating the chain of techniques at this point would prevent further operational damage.

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

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

3.16. CHANGE OPERATING MODE TECHNIQUE (T0858) FOR EVASION

BlackMatter enables the Windows local administrator account, which is set for automatic sign in when in safe mode, to stealthily execute the ransomware payload. Initiating encryption this way may reduce the likelihood of interference from security controls.[58]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe this activity through Windows event logs.

A total of 12 observables were identified with the use of the Change Operating Mode technique (T0858). This technique is important for investigation to identify system changes impacting security posture. This technique appears near the end of the timeline and responding to it may reduce stealth of initiation of the encryption process.

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	A total of 24 artifacts could be generated by the Change Operating Mode technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity
Resources	Technique Detection References

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

BlackMatter stops some running processes and services and prevents starting of new sessions.[59] Impacted processes and services could possibly be shut down in some instances to unlock files for encryption, which increases the number of encrypted files. Impacted processes and services include: Ensvc, thebat, mydesktopqos, xfssvccon, firefox, infopath, winword, Steam, Synctime, Notepad, Ocomm, Onenote, Mspub, Thunderbird, Agensvc, Sql, Excel, Powerpnt, Outlook, Wordpad, dbeng50, isqlplussvc, sqbcoreservice, oracle, ocautoupds, dbsnmp, msaccess, tbirdconfig, ocssd, mydesktopservice, visio, mepocs, memtas, veeam, svc$, backup, sql, and vss.[60]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe operational impacts resulting from stopped processes and services.

A total of 73 observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation as it can be used to identify anomalous activity and help in triaging malicious activity. This technique appears late in the timeline and responding to it will likely facilitate detection of malicious activity. Terminating the chain of techniques at this point would possibly limit the number of encrypted files BlackMatter creates.

Of the 73 observables associated with this technique, 69 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 13 artifacts could be generated by the Service Stop technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management
Resources	Technique Detection References

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

BlackMatter deletes volume shadow copies of the targeted directories to prevent recovery.[61,62] The volume shadow copy, also known as Volume Snapshot Service (VSS), is used to backup application data without taking applications offline.[63]

The ransomware also encrypts system files. The encryption file is loaded in the domain servers, where it is accessible to all network domains, and is encrypted from the remote share. The data is encrypted using the Salsa20 cipher and an RSA-1024 public key. The files are damaged during the encryption process and an extension with nine mixed-case alphanumeric characters is appended to file names. Following encryption, ransom notes are left in all directories and on the background of the desktop.[64,65]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe an absence of running services.

A total of 32 observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation, as it can be used to identify possible malicious activity. This technique represents the triggering event and responding to could limit the amount of the victim's backup data from being deleted.

Of the 32 observables associated with this technique, 26 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.19. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

File encryption is executed from a single network share by remotely distributing the encryption executable to domain servers inside the SYSVOL folder, which impacts all systems in the domain.[66] BlackMatter ransomware uses Salsa20 cipher and an RSA-1024 public key to encrypt key files on victim networks, which denies availability of corporate data and network resources.[67,68]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe a lack of availability of computer systems.

A total of six observables were identified with the use of the Loss of Availability technique (T0826). This technique is important for investigation as it the impact of the BlackMatter ransomware. This technique appears late in the timeline, after the triggering event, and terminating the chain of techniques at this point would not reduce the impact of the attack.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of eight artifacts could be generated by the Loss of Availability technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management
Resources	Technique Detection References

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

BlackMatter ransomware encrypts key system files, which prevents access to corporate data, applications, and impedes normal business functions. As a result, the malware negatively impacts productivity and generation of revenue.

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe a lack of availability of computer systems, which impact productivity and generation of revenue.

A total of six observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation as part of the restoration and recovery process. This technique appears last in the timeline, and terminating the chain of techniques at this point would not reduce the impact of the attack.

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

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

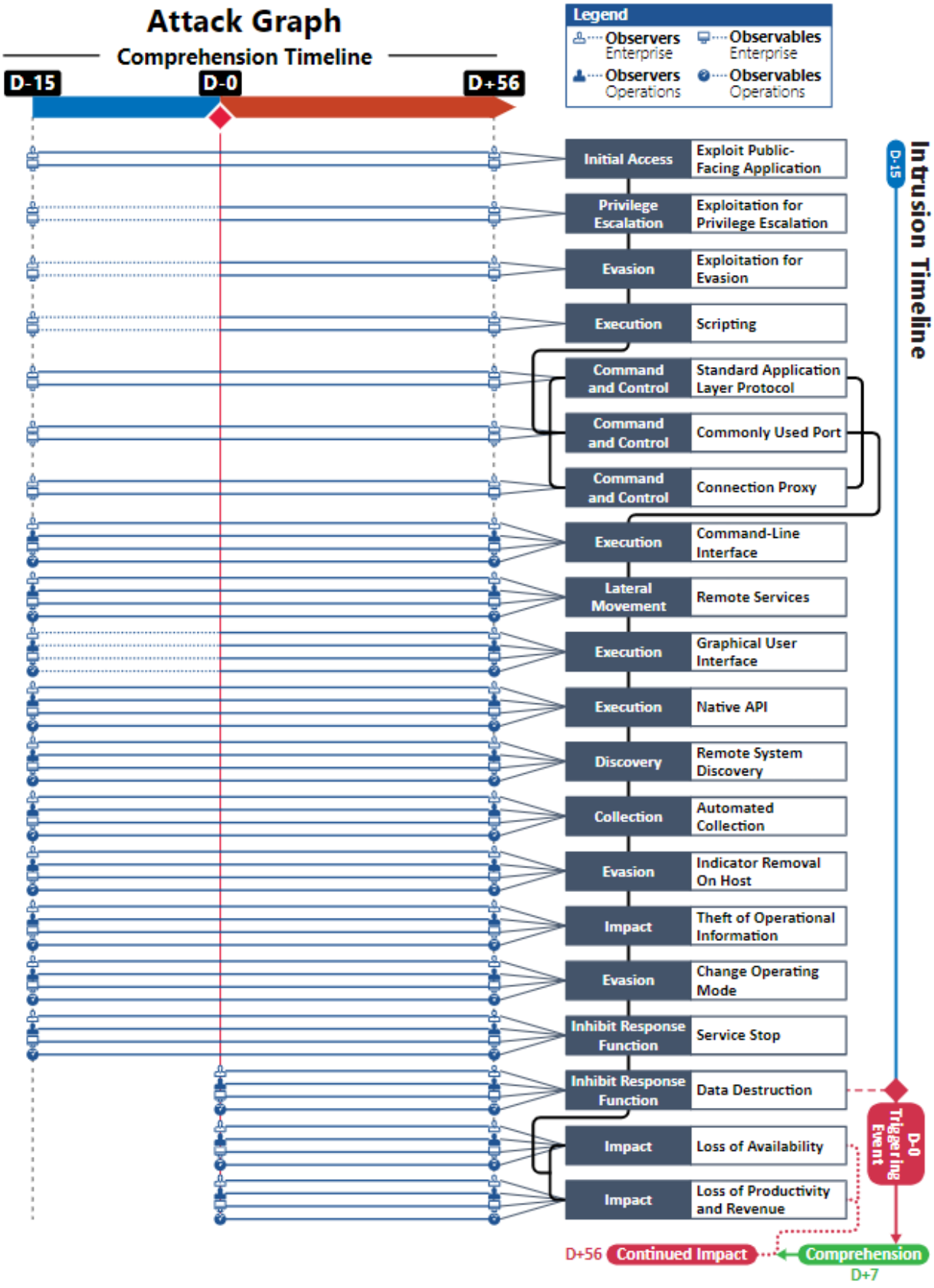

Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †

Observables Associated with Public-Facing Application Technique (T0819)	
Observable 1 †	*Presence of Vulnerability on Local Host*
Observable 2 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server*
Observable 3 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2013 (CVE-2022-41040)*
Observable 4 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2013 (CVE-2022-41082)*
Observable 5 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2016 (CVE-2022-41040)*
Observable 6 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2016 (CVE-2022-41082)*
Observable 7 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2019 (CVE-2022-41040)*
Observable 8 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2019 (CVE-2022-41082)*
Observable 9	Anonymous System Behavior on Local Host
Observable 10	Anonymous System Behavior on Local Host: Anomalous Usage of Exchange Server API
Observable 11 †	*Anonymous System Behavior on Local Host: Anomalous Usage of Web-Based Enterprise Management (WBEM)*
Observable 12 †	*Anonymous System Behavior on Local Host: Anomalous Usage of Windows Remote Management (PsRemoting)*
Observable 13 †	*Anonymous System Behavior on Local Host: Anomalous Usage of Exchange Autodiscover Service*
Observable 14 †	*Anomalous Network Traffic*
Observable 15 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 16	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server
Observable 17	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 18	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443: “https://<SMTP-address-domain>/autodiscover/autodiscover.xml”
Observable 19	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443: “https://autodiscover.<smtp-address-domain>/autodiscover/autodiscover.xml”
Observable 20 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC)*

Observables Associated with Public-Facing Application Technique (T0819)	
Observable 21 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Lightweight Directory Access Protocol (LDAP) TCP Port 389*
Observable 22 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*
Observable 23 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Simple Mail Transport Protocol (SMTP) TCP Port 25*

Observables Associated with Exploitation for Privilege Escalation Technique (T0890)	
Observable 1 †	*Presence of Vulnerability on Local Host*
Observable 2 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server*
Observable 3 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2013 (CVE-2022-41040)*
Observable 4 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2013 (CVE-2022-41082)*
Observable 5 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2016 (CVE-2022-41040)*
Observable 6 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2016 (CVE-2022-41082)*
Observable 7 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2019 (CVE-2022-41040)*
Observable 8 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2019 (CVE-2022-41082)*
Observable 9	Anonymous System Behavior on Local Host
Observable 10 †	*Anonymous System Behavior on Local Host: Privileged Command Execution*
Observable 11 †	*Anomalous Network Traffic*
Observable 12 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 13 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 14	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 15 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC)*
Observable 16 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Server Message Block (SMB) TCP Port 445*
Observable 17 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*
Observable 18	Anomalous Call to Windows API on Local Host
Observable 19	Anomalous Call to Windows API on Local Host: NetShareEnum

Observables Associated with Exploitation for Evasion Technique (T0820)	
Observable 1	Anonymous System Behavior on Local Host
Observable 2 †	*Anonymous System Behavior on Local Host: Bypass of User Account Control (UAC)*
Observable 3 †	*Anonymous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657)*
Observable 4 †	*Anonymous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657): Modification of Group Policy on Local Host*
Observable 5	Anomalous Call to Windows API on Local Host
Observable 6	Anomalous Call to Windows API on Local Host: ICMLuaUtil
Observable 7	Anomalous Network Traffic
Observable 8 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 9 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 10	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 11 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC)*
Observable 12 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*

Observables Associated with Scripting Technique (T0853)	
Observable 1 †	*Presence of Vulnerability on Local Host*
Observable 2 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server*
Observable 3 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2013 (CVE-2022-41040)*
Observable 4 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2013 (CVE-2022-41082)*
Observable 5 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2016 (CVE-2022-41040)*
Observable 6 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2016 (CVE-2022-41082)*
Observable 7 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2019 (CVE-2022-41040)*
Observable 8 †	*Presence of Vulnerability on Local Host: Microsoft Exchange Server: Exchange Server 2019 (CVE-2022-41082)*
Observable 9	Anonymous System Behavior on Local Host
Observable 10 †	*Anonymous System Behavior on Local Host: Privileged Command Execution*

Observables Associated with Scripting Technique (T0853)	
Observable 11 †	*Anonymous System Behavior on Local Host: Privileged Command Execution: \\<domaincontroller>\netlogon\def.vbs*
Observable 12	Anomalous Call to Windows API on Local Host
Observable 13 †	*Anomalous Call to Windows API on Local Host: NetShareEnum*
Observable 14 †	*Anomalous Call to Windows API on Local Host: AdsOpenObject*
Observable 15 †	*Anomalous Call to Windows API on Local Host: AdsBuildEnumerator*
Observable 16 †	*Anomalous Call to Windows API on Local Host: AdsEnumerateNext*
Observable 17 †	*Anomalous Call to Windows API on Local Host: NetShareEnum*
Observable 18 †	*Anomalous Call to Windows API on Local Host: NetShareEnumAll*
Observable 19 †	*Anomalous Call to Windows API on Local Host: EnumServicesStatusExW*
Observable 20	Anomalous Network Traffic
Observable 21 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 22 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 23	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 24 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC)*
Observable 25 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Server Message Block (SMB) TCP Port 445*
Observable 26 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*

Observables Associated with Standard Application Protocol Technique (T0869)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 5 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*

Observables Associated with Standard Application Protocol Technique (T0869)	
Observable 7 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 8 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 9	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22
Observable 10 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC)*
Observable 11 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Lightweight Directory Access Protocol (LDAP) TCP Port 389*
Observable 12 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*
Observable 13 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Server Message Block (SMB) TCP Port 445*
Observable 14 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Simple Mail Transport Protocol (SMTP) TCP Port 25*

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 5 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 7 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 8 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 9	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 10 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC)*
Observable 11 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Lightweight Directory Access Protocol (LDAP) TCP Port 389*
Observable 12 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*
Observable 13 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Server Message Block (SMB) TCP Port 445*
Observable 14 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Simple Mail Transport Protocol (SMTP) TCP Port 25*

Observables Associated with Connection Proxy Technique (T0884)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 5 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Presence of Anomalous Executable on Host*
Observable 7 †	*Presence of Anomalous Executable on Host: system.exe*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 5 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 7 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 8 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 9	Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC)
Observable 10 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Lightweight Directory Access Protocol (LDAP) TCP Port 389*
Observable 11 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*
Observable 12	Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Simple Mail Transport Protocol (SMTP) TCP Port 25
Observable 13 †	*Anomalous Command Line*
Observable 14 †	*Anomalous Command Line: cmd.exe /q /c reg add hkey_local_machine\system\currentcontrolset\control\lsa /v disablerestrictedadmin /t reg_dword /d 0 1> \\127.0.0.1\admin\$__<timestamp>\.<num> 2>&1*
Observable 15 †	*Anomalous Command Line: cmd.exe /c \\<domaincontroller>\netlogon\def.vbs*
Observable 16 †	*Anonymous System Behavior on Local Host*
Observable 17 †	*Anonymous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657)*

Observables Associated with Remote Services Technique (T0886)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 5 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*

Observables Associated with Remote Services Technique (T0886)	
Observable 7 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 8 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 9 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC)*
Observable 10 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Lightweight Directory Access Protocol (LDAP) TCP Port 389*
Observable 11 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*
Observable 12 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Server Message Block (SMB) TCP Port 445*
Observable 13 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Simple Mail Transport Protocol (SMTP) TCP Port 25*
Observable 14 †	*Presence of Anomalous Executable on Host*
Observable 15 †	*Presence of Anomalous Executable on Host: GOST system.exe*
Observable 16 †	*Presence of Anomalous Script on Host*
Observable 17 †	*Presence of Anomalous Script on Host: Impacket WMIExec.py*

Observables Associated with Graphical User Interface Technique (T0823)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 5 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 7 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 8 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*

Observables Associated with Graphical User Interface Technique (T0823)	
./Observable 9 †	*Presence of Anomalous Executable on Host*
Observable 10 †	*Presence of Anomalous Executable on Host: GOST system.exe*
Observable 11 †	*Presence of Dialogue Box on Local Host*
Observable 12 †	*Anomalous Command Line*
Observable 13 †	*Anomalous Command Line: cmd.exe /q /c reg add hkey_local_machine\system\currentcontrolset\control\lsa /v disablerestrictedadmin /t reg_dword /d 0 1> \\127.0.0.1\admin\$__<timestamp>\.<num> 2>&1*
Observable 14 †	*Anomalous Command Line: cmd.exe /c \\<domaincontroller>\netlogon\def.vbs*

Observables Associated with Native API Technique (T0834)	
Observable 1	Anomalous Call to Windows API on Local Host
Observable 2 †	*Anomalous Call to Windows API on Local Host: NetShareEnum*
Observable 3 †	*Anomalous Call to Windows API on Local Host: ADsOpenObject*
Observable 4 †	*Anomalous Call to Windows API on Local Host: AdsBuildEnumerator*
Observable 5 †	*Anomalous Call to Windows API on Local Host: ADsEnumerateNext*
Observable 6 †	*Anomalous Call to Windows API on Local Host: NetShareEnumAll*
Observable 7 †	*Anomalous Call to Windows API on Local Host: EnumServicesStatusExW*
Observable 8 †	*Anomalous Call to Windows API on Local Host: NtQuerySystemInformation*
Observable 9 †	*Usage of Dialogue Box on Local Host*
Observable 10 †	*Anomalous Network Traffic*
Observable 11	Anomalous Network Traffic: From External Host to Internal Application Server
Observable 12 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 13 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443*
Observable 14 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 15 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 16 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*

Observables Associated with Native API Technique (T0834)	
Observable 17 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 18 †	*Presence of Anomalous Executable on Host*
Observable 19 †	*Presence of Anomalous Executable on Host: GOST system.exe*

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 5 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 7 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 8 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 9 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*
Observable 10 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Server Message Block (SMB) TCP Port 445*
Observable 11	Anomalous Call to Windows API on Local Host
Observable 12 †	*Anomalous Call to Windows API on Local Host: NetShareEnum*
Observable 13 †	*Anomalous Call to Windows API on Local Host: ADsOpenObject*
Observable 14 †	*Anomalous Call to Windows API on Local Host: AdsBuildEnumerator*
Observable 15 †	*Anomalous Call to Windows API on Local Host: ADsEnumerateNext*
Observable 16 †	*Anomalous Call to Windows API on Local Host: NetShareEnumAll*
Observable 17 †	*Anomalous Call to Windows API on Local Host: EnumServicesStatusExW*
Observable 18 †	*Anomalous Call to Windows API on Local Host: NtQuerySystemInformation*
Observable 19 †	*Presence of Anomalous Executable on Host*

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 20 †	*Presence of Anomalous Executable on Host: GOST system.exe*

Observables Associated with Automated Collection Technique (T0802)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 5 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 7 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 8 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 9 †	*Presence of Anomalous Executable on Host*
Observable 10 †	*Presence of Anomalous Executable on Host: GOST system.exe*
Observable 11 †	*Presence of Anomalous Binary on Host*
Observable 12 †	*Presence of Anomalous Binary on Host: comsvcs.dll*
Observable 13 †	*Presence of Anomalous Binary on Host: Sysinternals Procmon*
Observable 14 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*
Observable 15 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Server Message Block (SMB) TCP Port 445*
Observable 16	Anomalous Call to Windows API on Local Host
Observable 17 †	*Anomalous Call to Windows API on Local Host: NtQuerySystemInformation*
Observable 18 †	*Anomalous Call to Windows API on Local Host: EnumServicesStatusExW*
Observable 19	Anomalous System Behavior on Local Host
Observable 20	Anomalous System Behavior on Local Host: Anomalous access of Local Security Authority Subsystem Service (LSASS) Memory

Observables Associated with Automated Collection Technique (T0802)	
Observable 21	Anomalous System Behavior on Local Host: Enumeration of Running Services

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 1 †	*Anomalous Deletion of Data*
Observable 2 †	*Anomalous Deletion of Data: Deletion of Windows Shadow Volume*
Observable 3 †	*Anomalous Deletion of Data: Deletion of Windows Service*
Observable 4 †	*Anomalous Deletion of Data: Deletion of Windows Service: mepocs*
Observable 5 †	*Anomalous Deletion of Data: Deletion of Windows Service: memtas*
Observable 6 †	*Anomalous Deletion of Data: Deletion of Windows Service: veeam*
Observable 7 †	*Anomalous Deletion of Data: Deletion of Windows Service: svc$*
Observable 8 †	*Anomalous Deletion of Data: Deletion of Windows Service: backup*
Observable 9 †	*Anomalous Deletion of Data: Deletion of Windows Service: sql*
Observable 10 †	*Anomalous Deletion of Data: Volume Shadow Copy*
Observable 11	*Anomalous Command Line*
Observable 12 †	Anomalous Command Line: IWbemServices::ExecQuery - ROOT\CIMV2 : SELECT * FROM Win32_ShadowCopy
Observable 13	*Anomalous Network Traffic*
Observable 14 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 15 †	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server
Observable 16	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443*
Observable 17 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 18 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 19 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 20 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 21 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*
Observable 22 †	*Presence of Anomalous Executable on Host*
Observable 23 †	*Presence of Anomalous Executable on Host: GOST system.exe*

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 5 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 7 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 8 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 9	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22
Observable 10	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files
Observable 11	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension
Observable 12	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .doc
Observable 13	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .docx
Observable 14	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .xls
Observable 15	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .xlsx
Observable 16	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .pdf

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 17	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .msg
Observable 18	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .png
Observable 19	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .ppt
Observable 20	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .pptx
Observable 21	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .sda
Observable 22	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .sdm
Observable 23	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .sdw
Observable 24	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Files: With Extension .csv
Observable 25	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Data
Observable 26	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Data: 1TB of data
Observable 27	Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Secure Shell (SSH) TCP Port 22: Transfer of Data: 653 Domain Credentials
Observable 28 †	*Presence of Anomalous Executable on Host*
Observable 29 †	*Presence of Anomalous Executable on Host: GOST system.exe*

Observables Associated with Change Operating Mode Technique (T0858)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443

Observables Associated with Change Operating Mode Technique (T0858)	
Observable 5 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 7 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 8 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 9	Anomalous System Behavior on Local Host
Observable 10 †	*Anomalous System Behavior on Local Host: Windows 'safe mode' enabled*
Observable 11 †	*Anomalous System Behavior on Local Host: Windows 'safe mode' enabled: automatic sign-in of local administrator account*
Observable 12 †	*Anonymous System Behavior on Local Host: Registry Key Value Was Modified (Event ID 4657): Modification of Group Policy on Local Host*

Observables Associated with Service Stop Technique (T0881)	
Observable 1	Anomalous Network Traffic
Observable 2 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 3 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 4	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 5 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 6 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 7 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 8 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 9	Anomalous System Behavior on Local Host
Observable 10 †	*Anomalous System Behavior on Local Host: Windows Process Terminated (Event ID 4689)*

Observables Associated with Service Stop Technique (T0881)	
Observable 11 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: ensvc*
Observable 12 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: thebat*
Observable 13 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: mydesktopqos*
Observable 14 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: xfssvccon*
Observable 15 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: firefox*
Observable 16 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: infopath*
Observable 17 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: winword*
Observable 18 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: steam*
Observable 19 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: synctime*
Observable 20 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: notepad*
Observable 21 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: ocomm*
Observable 22 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: onenote*
Observable 23 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: mspub*
Observable 24 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: thunderbird*
Observable 25 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: agensvc*
Observable 26 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: sql*
Observable 27 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: excel*
Observable 28 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: powerpnt*
Observable 29 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: outlook*
Observable 30 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: wordpad*
Observable 31 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: dbeng50*

Observables Associated with Service Stop Technique (T0881)	
Observable 32 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: isqlplussvc*
Observable 33 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: sqbcoreservice*
Observable 34 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: oracle*
Observable 35 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: ocautoupds*
Observable 36 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: dbsnmp*
Observable 37 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: msaccess*
Observable 38 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: tbirdconfig*
Observable 39 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: ocssd*
Observable 40 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: mydesktopservice*
Observable 41 †	*Anomalous System Behavior on Local Host: Windows Process Terminated: visioP*
Observable 42	Anomalous Command Line
Observable 43 †	*Anomalous Command Line: pskill ensvc*
Observable 44 †	*Anomalous Command Line: pskill thebat*
Observable 45 †	*Anomalous Command Line: pskill mydesktopqos*
Observable 46 †	*Anomalous Command Line: pskill xfssvccon*
Observable 47 †	*Anomalous Command Line: pskill firefox*
Observable 48 †	*Anomalous Command Line: pskill infopath*
Observable 49 †	*Anomalous Command Line: pskill winword*
Observable 50 †	*Anomalous Command Line: pskill steam*
Observable 51 †	*Anomalous Command Line: pskill synctime*
Observable 52 †	*Anomalous Command Line: pskill notepad*
Observable 53 †	*Anomalous Command Line: pskill ocomm*
Observable 54 †	*Anomalous Command Line: pskill onenote*
Observable 55 †	*Anomalous Command Line: pskill mspub*
Observable 56 †	*Anomalous Command Line: pskill thunderbird*
Observable 57 †	*Anomalous Command Line: pskill agensvc*
Observable 58 †	*Anomalous Command Line: pskill sql*
Observable 59 †	*Anomalous Command Line: pskill excel*

Observables Associated with Service Stop Technique (T0881)	
Observable 60 †	*Anomalous Command Line: pskill powerpnt*
Observable 61 †	*Anomalous Command Line: pskill outlook*
Observable 62 †	*Anomalous Command Line: pskill wordpad*
Observable 63 †	*Anomalous Command Line: pskill dbeng50*
Observable 64 †	*Anomalous Command Line: pskill isqlplussvc*
Observable 65 †	*Anomalous Command Line: pskill sqbcoreservice*
Observable 66 †	*Anomalous Command Line: pskill oracle*
Observable 67 †	*Anomalous Command Line: pskill ocautoupds*
Observable 68 †	*Anomalous Command Line: pskill dbsnmp*
Observable 69 †	*Anomalous Command Line: pskill msaccess*
Observable 70 †	*Anomalous Command Line: pskill tbirdconfig*
Observable 71 †	*Anomalous Command Line: pskill ocssd*
Observable 72 †	*Anomalous Command Line: pskill mydesktopservice*
Observable 73 †	*Anomalous Command Line: pskill visioP*

Observables Associated with Data Destruction Technique (T0809)	
Observable 1	Anomalous System Behavior on Local Host
Observable 2 †	*Anomalous System Behavior on Local Host: Anomalous increase in system resource utilization*
Observable 3 †	*Anomalous System Behavior on Local Host: Anomalous increase in system resource utilization: Increase in CPU utilization*
Observable 4 †	*Anomalous increase in system resource utilization: Increase in Hard Drive activity*
Observable 5 †	*Anomalous Deletion of Data*
Observable 6 †	*Anomalous Deletion of Data: Deletion of Windows Shadow Volume*
Observable 7 †	*Anomalous Deletion of Data: Deletion of Windows Service*
Observable 8 †	*Anomalous Deletion of Data: Deletion of Windows Service: mepocs*
Observable 9 †	*Anomalous Deletion of Data: Deletion of Windows Service: memtas*
Observable 10 †	*Anomalous Deletion of Data: Deletion of Windows Service: veeam*
Observable 11 †	*Anomalous Deletion of Data: Deletion of Windows Service: svc$*
Observable 12 †	*Anomalous Deletion of Data: Deletion of Windows Service: backup*
Observable 13 †	*Anomalous Deletion of Data: Deletion of Windows Service: sql*
Observable 14 †	*Anomalous Deletion of Data: Volume Shadow Copy*
Observable 15	Anomalous Command Line
Observable 16 †	*Anomalous Command Line: IWbemServices::ExecQuery - ROOT\CIMV2 : SELECT * FROM Win32_ShadowCopy*

Observables Associated with Data Destruction Technique (T0809)	
Observable 17	Anomalous Network Traffic
Observable 18 †	*Anomalous Network Traffic: From External Host to Internal Application Server*
Observable 19 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server*
Observable 20	Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over HyperText Transfer Protocol Secure (HTTPS) TCP Port 443
Observable 21 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 22 †	*Anomalous Network Traffic: From External Host to Internal Application Server: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 23 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over GoLang (GO) Simple Tunnel (GOST) UDP Port 5353*
Observable 24 †	*Anomalous Network Traffic: From Internal Application Server to External Host: Microsoft Exchange Server: Over Remote Desktop Protocol (RDP) TCP Port 3389*
Observable 25 †	*Anomalous Network Traffic: From Internal Exchange Server to Internal Domain Controller (DC): Over Remote Procedure Call (RPC) TCP Port 135*
Observable 26 †	*Presence of Anomalous Executable on Host*
Observable 27 †	*Presence of Anomalous Executable on Host: GOST system.exe*
Observable 28	Anomalous Modification of Files
Observable 29 †	*Anomalous Modification of Files: File Extension Appended to Filenames*
Observable 30 †	*Anomalous Modification of Files: File Extension Appended to Filenames: Nine Mixed-Case Alphanumeric Characters*
Observable 31 †	*Anomalous Modification of Files: Files Encrypted Using Salsa20*
Observable 32	Anomalous Modification of Files: Files Encrypted Using Salsa20: With 1024-bit RSA keys

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1	Anomalous System Behavior on Local Host
Observable 2 †	*Anomalous System Behavior on Local Host: Automated Systems Rendered Inoperable*
Observable 3 †	*Anomalous Interruption of Automated Processes*
Observable 4 †	*Anomalous Interruption of Automated Processes: 8 Weeks*
Observable 5 †	*Anomalous Interruption of Automated Processes: 8 Weeks: Information Technology (IT) Systems*
Observable 6 †	*Anomalous Interruption of Automated Processes: 8 Weeks: Production Systems*

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1	Anomalous System Behavior on Local Host
Observable 2 †	*Anomalous System Behavior on Local Host: Automated Systems Rendered Inoperable*
Observable 3 †	*Anomalous Interruption of Automated Processes: 8 Weeks*
Observable 4 †	*Anomalous Interruption of Automated Processes: 8 Weeks: Information Technology (IT) Systems*
Observable 5 †	*Anomalous Interruption of Automated Processes: 8 Weeks: Production Systems*
Observable 6 †	*Anomalous Interruption of Automated Processes: 8 Weeks*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Exploit Public-Facing Application Technique (T0819)	
Artifact 1	Logon Security Event
Artifact 2	Logon Timestamp
Artifact 3	Process Failure
Artifact 4	Process State Change
Artifact 5	Operational Data Modification
Artifact 6	Operational Data Corruption
Artifact 7	Open Platform Communication (OPC) Communication (COM) Objects
Artifact 8	Remote Connections
Artifact 9	External Network Connections
Artifact 10	Logon Event
Artifact 11	Prefetch
Artifact 12	Logon Event
Artifact 13	Administrator Logon
Artifact 14	External Network Connections
Artifact 15	Remote Connections
Artifact 16	Ransom Note
Artifact 17	Logon Timestamp After Hours
Artifact 18	MAC Address
Artifact 19	IP Address
Artifact 20	Process Ending
Artifact 21	HTTP Traffic Port
Artifact 22	External Industrial Protocol Connections
Artifact 23	Web Server Log
Artifact 24	Virtual Network Computing (VNC) Traffic Port
Artifact 25	Secure Shell (SSH) Traffic Port
Artifact 26	Logon Security Event
Artifact 27	Telnet Traffic
Artifact 28	Increase Number of Logon Attempts
Artifact 29	Trivial File Transfer Protocol (TFTP) Port
Artifact 30	File Transfer Protocol (FTP) Port
Artifact 31	Application Failure
Artifact 32	HTTPS Port
Artifact 33	User Account

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

Artifacts Associated with Exploitation for Privilege Escalation Technique (T0890)	
Artifact 1	SYSMON Event 8 CREATEREMOTETHREAD Process Injection Detected
Artifact 2	Unexpected Process Crash
Artifact 3	Network Traffic Associated with Privilege Escalation Vulnerabilities (CVE-2014-4076 Sent a Specially Crafted TCP Packet to \\.\\ TCP Device Through DEVICEIOCONTROL Function)
Artifact 4	Unusual Process Activity (Thread Suspension of Everything Except Thread Running in a Process Other Than Exploit Thread)
Artifact 5	Suspicious Files Written to Disk
Artifact 6	Unusual Command Line History Associated with Known CVE Techniques (CVE-2019-5736 Privilege Escalation is Visible via Unusual Command Line Commands)
Artifact 7	Suspicious File Write to System Directory Followed by Privileged Execution of File

Artifacts Associated with Exploitation for Privilege Escalation Technique (T0890)	
Artifact 8	Unusual or Unexpected KERBEROS Ticket Requests
Artifact 9	Suspicious Program Running Under SYSTEM or Other Elevated Account
Artifact 10	Driver Loaded (SYSMON Event)
Artifact 11	Network Traffic Matching Vulnerability (Snort, SURICATA)
Artifact 12	Abnormal Reads/Writes Between Processes
Artifact 13	Unusual Command Line Arguments to Application (lolbins)
Artifact 14	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 15	Unusual or Unexpected Child Process Running at Elevated Privileges
Artifact 16	Execution of a Suspicious File in the System32 or Windows Directory at Privileged Level

Artifacts Associated with Exploitation for Evasion Technique (T0820)	
Artifact 1	Internal Sender IP Address
Artifact 2	Disk Writes
Artifact 3	Memory Writes
Artifact 4	HTTP Traffic
Artifact 5	Industrial Protocol Traffic
Artifact 6	Server Message Block (SMB) Traffic
Artifact 7	External Industrial Protocol Connections
Artifact 8	Web Proxy Logs
Artifact 9	HTTPS Port
Artifact 10	File Creation
Artifact 11	Application Log
Artifact 12	Destination Address
Artifact 13	FTPS Port
Artifact 14	FTP Port
Artifact 15	TFTP Port
Artifact 16	Firewall Log
Artifact 17	Telnet Traffic
Artifact 18	MAC Address
Artifact 19	SSH Traffic Port
Artifact 20	VNC Traffic Port
Artifact 21	RDP Traffic Port
Artifact 22	Kernel Error

Artifacts Associated with Exploitation for Evasion Technique (T0820)	
Artifact 23	OS Version Modification
Artifact 24	Firmware Version Modification
Artifact 25	Process Creation
Artifact 26	Software Vulnerability
Artifact 27	Zero-Day Announcement
Artifact 28	Protocol Vulnerability
Artifact 29	Pip Use
Artifact 30	External Sender IP Address

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

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

Artifacts Associated with Standard Application Layer Protocol Technique (T0869)	
Artifact 11	HTTPS Traffic Port
Artifact 12	Network Content Metadata

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

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

Artifacts Associated with Command-Line Interface Technique (T0807)	
Artifact 15	Event Log Type
Artifact 16	Failed Logon Event
Artifact 17	Command Line Memory Data
Artifact 18	cmd.exe Application Execution
Artifact 19	RDP Traffic
Artifact 20	Industrial Application Execution
Artifact 21	POWERSHELL Cmdlet Application Execution
Artifact 22	Event ID 4103 POWERSHELL Command
Artifact 23	Event ID 4688 Command Line Execution
Artifact 24	NTUSER Application Execution Entries
Artifact 25	External Network Connection

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 1	Mouse Movement
Artifact 2	Authentication Logs
Artifact 3	Network Traffic Content Creation
Artifact 4	Remote Session Creation Timestamp
Artifact 5	Process Creation
Artifact 6	VNC Traffic
Artifact 7	SMB Traffic
Artifact 8	SSH Traffic
Artifact 9	Microsoft SQL (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

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 23	Remote Client Connection
Artifact 24	Data File Size in Network Content

Artifacts Associated with Graphical User Interface Technique (T0823)	
Artifact 1	Cursor Movement
Artifact 2	SSH Connections
Artifact 3	Host-Screen Adjustments
Artifact 4	Code Injections
Artifact 5	Program Executions
Artifact 6	RDP Connections
Artifact 7	VNC Connections
Artifact 8	Prefetch Files Created
Artifact 9	SSH Port
Artifact 10	Keyboard Entries
Artifact 11	Mouse Movement
Artifact 12	RDP Port
Artifact 13	SMB Port
Artifact 14	Application Execution via Input Devices
Artifact 15	Service Creation
Artifact 16	Service Modification
Artifact 17	Process Input Changes
Artifact 18	JUMPLIST Creation
Artifact 19	SHELLBAG Creation
Artifact 20	System Resource Use Management Changes
Artifact 21	Network Connection Durations
Artifact 22	Changes in Bytes Sent and Received
Artifact 23	Increase CPU Cycles
Artifact 24	Host System Crash
Artifact 25	Application Usage Increase
Artifact 26	Remote Client Execution
Artifact 27	Logon Event
Artifact 28	Screen Resolution Changes
Artifact 29	Network Bandwidth Changes
Artifact 30	Remote Vendor Connections
Artifact 31	Event Log Creation

Artifacts Associated with Graphical User Interface Technique (T0823)	
Artifact 32	VPN Connections
Artifact 33	Session Authentication
Artifact 34	Failed Logons Event
Artifact 35	Session Timestamp
Artifact 36	Logon Event Type 3
Artifact 37	Logon Event Type 10
Artifact 38	Logon Event Type 11
Artifact 39	Remote Session Key
Artifact 40	System Registry Network Interfaces
Artifact 41	Remote Services Logon
Artifact 42	Transport Layer Security (TLS) Certificate
Artifact 43	Session Logoff Event
Artifact 44	Domain Controller Log
Artifact 45	External IP Address
Artifact 46	Process Creations
Artifact 47	External MAC Address
Artifact 48	Encrypted Network Traffic
Artifact 49	Remote Services Protocols
Artifact 50	Blocked Incoming Packet Event
Artifact 51	Blocked Incoming Connections Event
Artifact 52	User Account Creation
Artifact 53	Security Account Manager Registry Password Hashes
Artifact 54	Command Prompt Window Opened
Artifact 55	Mouse Movement
Artifact 56	Dialog Box Pop-Up
Artifact 57	Security Account Manager Registry Entries
Artifact 58	User Client Address
Artifact 59	User Account Name
Artifact 60	User Privileges Change

Artifacts Associated with Native API Technique (T0834)	
Artifact 1	Alert Generated
Artifact 2	System Resource Usage Management Changes
Artifact 3	.dll Modifications
Artifact 4	Imports Hash Changed

Artifacts Associated with Native API Technique (T0834)	
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 Remote System Discovery Technique (T0846)	
Artifact 1	Protocol Header Enumeration
Artifact 2	Protocol Content Enumeration
Artifact 3	VNC Port 5900 Calls
Artifact 4	TCP ACK Scan
Artifact 5	TCP XMAS Scan
Artifact 6	Recurring Protocol SYN Traffic
Artifact 7	TCP FIN Scans
Artifact 8	Device Failure
Artifact 9	TCP Reverse Ident Scan
Artifact 10	Sequential Protocol SYN Traffic
Artifact 11	Scans Over Industrial Network Ports with Target IPs
Artifact 12	Industrial Network Traffic Content Containing Logical Identifiers

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 13	Simple Mail Transfer Protocol (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 Multimedia Messaging System (MMS)
Artifact 27	Controller Proprietary Traffic
Artifact 28	Echo Type 8 Traffic
Artifact 29	ICMP Type 7 Traffic
Artifact 30	Simple Network Management Protocol (SNMP) Port 162 Traffic
Artifact 31	SNMP Port 161 Traffic
Artifact 32	Address Resolution Protocol 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	Lightweight Directory Access Protocol (LDAP) Port
Artifact 39	Active Directory Calls
Artifact 40	Email Server Calls
Artifact 41	DNS Lookup Queries
Artifact 42	TCP Connect Scan
Artifact 43	Command Line Dialog Box Open

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 1	POWERSHELL Command Arguments
Artifact 2	External Network Connections

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 3	SQL Read Requests
Artifact 4	User Account Creation
Artifact 5	Operational Data Exfiltration
Artifact 6	MAC Addresses
Artifact 7	IP Addresses
Artifact 8	Internal Network Connections
Artifact 9	Command Execution
Artifact 10	File Execution
Artifact 11	Local Memory Read Requests
Artifact 12	Command Line Arguments
Artifact 13	Network Read Request
Artifact 14	Native Tool Use
Artifact 15	Service Log
Artifact 16	Application Log
Artifact 17	File Transfer
Artifact 18	SMB Traffic Port
Artifact 19	User Account Logs
Artifact 20	User Account Privilege Change
Artifact 21	Database Read Request
Artifact 22	Open Platform Communications (OPC) Read Requests
Artifact 23	File Creation

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

Artifacts Associated with Indicator Removal on Host Technique (T0872)	
Artifact 13	Missing Log Events
Artifact 14	Unexpected Reboots
Artifact 15	Windows Security Log 1102 for Cleared Events
Artifact 16	File Deletion
Artifact 17	File Modification
Artifact 18	Sdelete Executable Loaded
Artifact 19	Sdelete Executable Executed
Artifact 20	File Metadata Changes
Artifact 21	Timestamp Inconsistencies
Artifact 22	User Authentication
Artifact 23	Memory Writes

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

Artifacts Associated with Change Operating Mode Technique (T0858)	
Artifact 1	Vendor Proprietary Protocol Use
Artifact 2	Network Packet Metadata Change
Artifact 3	Controlled Device Alarm
Artifact 4	Process State Change
Artifact 5	Controlled Device State Change
Artifact 6	Program File Manipulation
Artifact 7	Remote Network Traffic
Artifact 8	Wireless Connections
Artifact 9	.dll File Creation
Artifact 10	Application Log Event
Artifact 11	Sender IP Address
Artifact 12	Radio Connections
Artifact 13	Network Connection Reconfigured
Artifact 14	Industrial Network Traffic

Artifacts Associated with Change Operating Mode Technique (T0858)	
Artifact 15	End-Point IP Address
Artifact 16	Application Modification
Artifact 17	Controlled Device Failure
Artifact 18	Mode Key Position Change
Artifact 19	Controlled Device Reboot
Artifact 20	Controlled Device Manipulation
Artifact 21	Logon Event
Artifact 22	Logoff Event
Artifact 23	User Account Information
Artifact 24	Common Network Traffic

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
Artifact 7	System Call

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 8	System Application Interruption
Artifact 9	Device Failure
Artifact 10	Recovery Attempt Failure
Artifact 11	TFTP Port
Artifact 12	Secure File Transfer Protocol (SFTP) Port
Artifact 13	Memory Corruption
Artifact 14	Use of File Transfer Protocols
Artifact 15	Secure Copy Protocol (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 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 Loss of Productivity and Revenue Technique (T0828)	
Artifact 1	Loss of Confidence in a Safety System Due to Unreliability Might Result in a Risk Management Driven Shutdown of a Plant
Artifact 2	Wormable or Other Highly Propagating Malware Might Result in the Shutdown of a Plant to Prevent Ransomware or Other Destructive Attacks
Artifact 3	Extortion Attempts Might Lead to Reduced Operations Due to Potential Presence of Malicious Attackers
Artifact 4	Loss of Control of Critical Systems Due to Ransomware or Loss of Confidence Might Lead to a Degraded Productivity or Revenue Operating State
Artifact 5	File System Modification Artifacts Might be Associated with the Loss of Productivity and Revenue Attack Might be Present on Disk

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] [DHS/CISA | "Alert (AA21-291A) - BlackMatter Ransomware" | https://www.cisa.gov/uscert/ncas/alerts/aa21-291a | 18 October 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[2] [SecurityWeek | Ionut Arghire | "BlackMatter Ransomware Gang Announces Shutdown" | https://www.securityweek.com/blackmatter-ransomware-gang-announces-shutdown/ | Accessed on 8 March 2022 | The source is publicly available information and does not contain classification markings]

[3] [Wall Street Journal | David Uberti | "Iowa Grain Cooperative Hit by Cyberattack Linked to Ransomware Group" | https://www.wsj.com/articles/iowa-grain-cooperative-hit-by-cyberattack-linked-to-ransomware-group-11632172945 | 20 September 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[4] [Des Moines Register | Donnelle Eller | "Iowa grain cooperative says it's working to restore automated operations, but remains silent on cyberattack ransom" | https://www.desmoinesregister.com/story/money/agriculture/2021/10/06/iowa-grain-cooperative-recovering-cyberattack-remains-mum-ransom/6007123001/ | 6 October 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[5] [Bleeping Computer | Lawrence Abrams | "US farmer cooperative hit by $5.9M BlackMatter ransomware attack" | https://www.bleepingcomputer.com/news/security/us-farmer-cooperative-hit-by-59m-blackmatter-ransomware-attack/ | 20 September 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[6] [New Cooperative Newsletter | "Directions" | https://www.newcoop.com/wp-content/uploads/2022/01/DECEMBER-2021-web.pdf | December 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[7] [Des Moines Register | Donnelle Eller | "Iowa grain cooperative says it's working to restore automated operations, but remains silent on cyberattack ransom" | https://www.desmoinesregister.com/story/money/agriculture/2021/10/06/iowa-grain-cooperative-recovering-cyberattack-remains-mum-ransom/6007123001/ | 6 October 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[8] [New Cooperative Newsletter | "Directions" | https://www.newcoop.com/wp-content/uploads/2022/01/DECEMBER-2021-web.pdf | December 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[9] [Wall Street Journal | David Uberti | "Iowa Grain Cooperative Hit by Cyberattack Linked to Ransomware Group" | https://www.wsj.com/articles/iowa-grain-cooperative-hit-by-cyberattack-linked-to-ransomware-group-11632172945 | 20 September 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[10] [Microsoft | "What is Ransomware?" | https://learn.microsoft.com/en-us/security/compass/human-operated-ransomware | 3 March 2023 | Accessed on 22 March 2023 | The source is publicly available information and does not contain classification markings]

[11] [Des Moines Register | Donnelle Eller | "Iowa grain cooperative says it's working to restore automated operations, but remains silent on cyberattack ransom" | https://www.desmoinesregister.com/story/money/agriculture/2021/10/06/iowa-grain-cooperative-recovering-cyberattack-remains-mum-ransom/6007123001/ | 6 October 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[12] [Bleeping Computer | Lawrence Abrams | "US farmer cooperative hit by $5.9M BlackMatter ransomware attack" | https://www.bleepingcomputer.com/news/security/us-farmer-cooperative-hit-by-

59m-blackmatter-ransomware-attack/ | 20 September 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[13] [New Cooperative Newsletter | "Directions" | https://www.newcoop.com/wp-content/uploads/2022/01/DECEMBER-2021-web.pdf | December 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[14] [Talos | Tiago Pereira, Caitlin Huey | "From BlackMatter to BlackCat: Analyzing two attacks from one affiliate" | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[15] [Talos | Tiago Pereira, Caitlin Huey | "From BlackMatter to BlackCat: Analyzing two attacks from one affiliate" | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[16] [Varonis | Dvir Sason | "BlackMatter Ransomware: In-Depth Analysis & Recommendations" | https://www.varonis.com/blog/blackmatter-ransomware | 2 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[17] [Infosec | Pedro Tavares | "A full analysis of the BlackMatter ransomware" | https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/ | 10 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[18] [Talos | Tiago Pereira, Caitlin Huey | "From BlackMatter to BlackCat: Analyzing two attacks from one affiliate" | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[19] [Varonis | Dvir Sason | "BlackMatter Ransomware: In-Depth Analysis & Recommendations" | https://www.varonis.com/blog/blackmatter-ransomware | 2 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[20] [Mitre | "Standard Application Layer Protocol" | https://attack.mitre.org/techniques/T0869/ | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[21] [InfoSec | Pedro Tavares | "A full analysis of the BlackMatter ransomware" | https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/ | 10 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[22] [Talos | Tiago Pereira, Caitlin Huey | "From BlackMatter to BlackCat: Analyzing two attacks from one affiliate" | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[23] [Microsoft | "Ransom:Win32/BlackMatter.PA!MTB" | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/BlackMatter.PA!MTB&ThreatID=2147788436 | 19 August 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[24] [InfoSec | Pedro Tavares | "A full analysis of the BlackMatter ransomware" | https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/ | 10 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[25] [Talos | Tiago Pereira, Caitlin Huey | "From BlackMatter to BlackCat: Analyzing two attacks from one affiliate" | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 |

Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[26] [Des Moines Register | Donnelle Eller | “Iowa grain cooperative says it's working to restore automated operations, but remains silent on cyberattack ransom” | https://www.desmoinesregister.com/story/money/agriculture/2021/10/06/iowa-grain-cooperative-recovering-cyberattack-remains-mum-ransom/6007123001/ | 6 October 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[27] [New Cooperative Newsletter | “Directions” | https://www.newcoop.com/wp-content/uploads/2022/01/DECEMBER-2021-web.pdf | December 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[28] [Talos | Tiago Pereira, Caitlin Huey | “From BlackMatter to BlackCat: Analyzing two attacks from one affiliate” | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[29] [Varonis | Dvir Sason | “BlackMatter Ransomware: In-Depth Analysis & Recommendations” | https://www.varonis.com/blog/blackmatter-ransomware | 2 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[30] [Microsoft | “Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server” | https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/ | 29 September 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[31] [EMSISOFT | EMSISOFT MALWARE LAB | “Ransomware Profile: BlackMatter” | https://www.emsisoft.com/en/blog/39121/ransomware-profile-blackmatter/ | 20 September 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[32] [Varonis | Dvir Sason | “BlackMatter Ransomware: In-Depth Analysis & Recommendations” | https://www.varonis.com/blog/blackmatter-ransomware | 2 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[33] [Varonis | Dvir Sason | “BlackMatter Ransomware: In-Depth Analysis & Recommendations” | https://www.varonis.com/blog/blackmatter-ransomware | 2 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[34] [Talos | Tiago Pereira, Caitlin Huey | “From BlackMatter to BlackCat: Analyzing two attacks from one affiliate” | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[35] [Talos | Tiago Pereira, Caitlin Huey | “From BlackMatter to BlackCat: Analyzing two attacks from one affiliate” | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[36] [Infosec | Pedro Tavares | “A full analysis of the BlackMatter ransomware” | https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/ | 10 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[37] [Varonis | Dvir Sason | “BlackMatter Ransomware: In-Depth Analysis & Recommendations” | https://www.varonis.com/blog/blackmatter-ransomware | 2 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[38] [Talos | Tiago Pereira, Caitlin Huey | “From BlackMatter to BlackCat: Analyzing two attacks from one affiliate” | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 |

Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[39] [Varonis | Dvir Sason | "BlackMatter Ransomware: In-Depth Analysis & Recommendations" | https://www.varonis.com/blog/blackmatter-ransomware | 2 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[40] [Talos | Tiago Pereira, Caitlin Huey | "From BlackMatter to BlackCat: Analyzing two attacks from one affiliate" | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[41] [Talos | Tiago Pereira, Caitlin Huey | "From BlackMatter to BlackCat: Analyzing two attacks from one affiliate" | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[42] [Talos | Tiago Pereira, Caitlin Huey | "From BlackMatter to BlackCat: Analyzing two attacks from one affiliate" | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[43] [Talos | Tiago Pereira, Caitlin Huey | "From BlackMatter to BlackCat: Analyzing two attacks from one affiliate" | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[44] [Mitre | "Graphical User Interface" | https://attack.mitre.org/techniques/T0823/ | 21 May 2020 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[45] [Mitre | "Native API" | https://attack.mitre.org/techniques/T0834/ | 13 April 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[46] [Illusive | Shahar Zelig | "Preventing BlackMatter Ransomware from Encryption of Available Remote Share" | https://illusive.com/resources/threat-research-blog/preventing-blackmatter-ransomware-from-encryption-of-available-remote-share/ | 7 January 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[47] [Infosec | Pedro Tavares | "A full analysis of the BlackMatter ransomware" | https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/ | 10 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[48] [Microsoft | "Ransom:Win32/BlackMatter.PA!MTB" | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/BlackMatter.PA!MTB&ThreatID=2147788436 | 19 August 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[49] [Illusive | Shahar Zelig | "Preventing BlackMatter Ransomware from Encryption of Available Remote Share" | https://illusive.com/resources/threat-research-blog/preventing-blackmatter-ransomware-from-encryption-of-available-remote-share/ | 7 January 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[50] [DHS/CISA | "Alert (AA21-291A) - BlackMatter Ransomware" | https://www.cisa.gov/uscert/ncas/alerts/aa21-291a |18 October 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[51] [DHS/CISA | "Alert (AA21-291A) - BlackMatter Ransomware" | https://www.cisa.gov/uscert/ncas/alerts/aa21-291a |18 October 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[52] [DHS/CISA | “Alert (AA21-291A) - BlackMatter Ransomware” | https://www.cisa.gov/uscert/ncas/alerts/aa21-291a |18 October 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[53] [Illusive | Shahar Zelig | “Preventing BlackMatter Ransomware from Encryption of Available Remote Share” | https://illusive.com/resources/threat-research-blog/preventing-blackmatter-ransomware-from-encryption-of-available-remote-share/ | 7 January 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[54] [Varonis | Dvir Sason | “BlackMatter Ransomware: In-Depth Analysis & Recommendations” | https://www.varonis.com/blog/blackmatter-ransomware | 2 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[55] [Symantec | “BlackMatter: New Data Exfiltration Tool Used in Attacks” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackmatter-data-exfiltration | 1 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[56] [TrendMicro | Maria Emreen Viray | “Ransom.Win32.BLACKMATTER.THGOCBA” | https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom.win32.blackmatter.thgocba | 4 August 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[57] [Symantec | “BlackMatter: New Data Exfiltration Tool Used in Attacks” | 1 November 2021 | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackmatter-data-exfiltration | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[58] [Varonis | Dvir Sason | “BlackMatter Ransomware: In-Depth Analysis & Recommendations” | https://www.varonis.com/blog/blackmatter-ransomware | 2 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[59] [Infosec | Pedro Tavares | “A full analysis of the BlackMatter ransomware” | https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/ | 10 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[60] [Infosec | Pedro Tavares | “A full analysis of the BlackMatter ransomware” | https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/ | 10 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[61] [Infosec | Pedro Tavares | “A full analysis of the BlackMatter ransomware” | https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/ | 10 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[62] [EMSISOFT | EMSISOFT MALWARE LAB | “Ransomware Profile: BlackMatter” | https://www.emsisoft.com/en/blog/39121/ransomware-profile-blackmatter/ | 20 September 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[63] [Microsoft | “Volume Shadow Copy Service” | https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service | 7 December 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[64] [Microsoft | “Ransom:Win32/BlackMatter.PA!MTB” | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/BlackMatter.PA!MTB&ThreatID=2147788436 | 19 August 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[65] [InfoSec | Pedro Tavares | “A full analysis of the BlackMatter ransomware” | https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/ | 10 November

2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[66] [Talos | Tiago Pereira, Caitlin Huey | “From BlackMatter to BlackCat: Analyzing two attacks from one affiliate” | https://blog.talosintelligence.com/from-blackmatter-to-blackcat-analyzing/ | 22 March 2022 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[67] [Microsoft | “Ransom:Win32/BlackMatter.PA!MTB” | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/BlackMatter.PA!MTB&ThreatID=2147788436 | 19 August 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]

[68] [Infosec | Pedro Tavares | “A full analysis of the BlackMatter ransomware” | https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/ | 10 November 2021 | Accessed on 14 December 2022 | The source is publicly available information and does not contain classification markings]