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: RYUK RANSOMWARE ATTACK ON UNIVERSAL HEALTH SERVICES 2020

Cybersecurity for the Operational Technology Environment (CyOTE)

31 MARCH 2023

CyOTE Cybersecurity for the Operational Technology Environment

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

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

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

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY 2

2. INTRODUCTION 3

2.1. APPLYING THE CYOTE METHODOLOGY 3
2.2. BACKGROUND ON THE ATTACK 5

3. OBSERVABLE AND TECHNIQUE ANALYSIS 8

3.1. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS 8
3.2. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION 9
3.3. DRIVE-BY COMPROMISE TECHNIQUE (T0817) FOR INITIAL ACCESS 10
3.4. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION 11
3.5. MASQUERADING TECHNIQUE (T0849) FOR EVASION 12
3.6. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION 13
3.7. NATIVE API TECHNIQUE (T0834) FOR EXECUTION 14
3.8. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY 15
3.9. STANDARD APPLICATION LAYER PROTOCOL TECHNIQUE (T0869) FOR COMMAND AND CONTROL 16
3.10. COMMONLY USED PORTS TECHNIQUE (T0885) FOR COMMAND AND CONTROL 17
3.11. COMMAND-LINE INTERFACE TECHNIQUE (T0807) FOR EXECUTION 18
3.12. LATERAL TOOL TRANSFER TECHNIQUE (T0867) FOR LATERAL MOVEMENT 19
3.13. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE 20
3.14. REMOTE SYSTEM INFORMATION DISCOVERY TECHNIQUE (T0888) FOR DISCOVERY 21
3.15. SERVICE STOP TECHNIQUE (T0881) FOR INHIBIT RESPONSE FUNCTION 22
3.16. DEVICE SHUTDOWN/RESTART TECHNIQUE (T0816) FOR INHIBIT RESPONSE FUNCTION 23
3.17. DATA DESTRUCTION TECHNIQUE (T0809) FOR INHIBIT RESPONSE FUNCTION 24
3.18. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT 25
3.19. LOSS OF PRODUCTIVITY AND REVENUE TECHNIQUE (T0828) FOR IMPACT 26

APPENDIX A: OBSERVABLES LIBRARY 28

APPENDIX B: ARTIFACTS LIBRARY 37

APPENDIX C: OBSERVERS 48

REFERENCES 49

FIGURES

FIGURE 1. CYOTE METHODOLOGY 3

FIGURE 2. INTRUSION TIMELINE 5

FIGURE 3. ATTACK GRAPH 27

TABLES

TABLE 1. TECHNIQUES USED IN THE RYUK RANSOMWARE ATTACK ON UNIVERSAL HEALTH SERVICES 2020 CYBER ATTACK 7

TABLE 2. PRECURSOR ANALYSIS REPORT QUANTITATIVE SUMMARY 7

PRECURSOR ANALYSIS REPORT: RYUK RANSOMWARE ATTACK ON UNIVERSAL HEALTH SERVICES 2020

1. EXECUTIVE SUMMARY

The Ryuk Ransomware Attack on Universal Health Services (UHS) 2020 Precursor Analysis Report leverages publicly available information about the 2020 UHS cyber attack and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

UHS manages over 400 hospitals and is one of the largest healthcare providers in the United States with 3.5 million patients each year.[1] On 27 September 2020, UHS suffered a widespread ransomware attack that resulted in a denial of service to critical internet-dependent healthcare systems including workstations, phones, and data centers. Employees resorted to filing patient details with pen and paper, while other facilities had to redirect ambulances and urgent patients to other facilities for adequate care. Adversaries carried out the attack with Ryuk, a ransomware that encrypts data and generates a RyukReadMe.txt ransom note with the ransom fee to decrypt the data, varying from 15 Bitcoin (BTC) to 50 BTC, equivalent to roughly $353,892 to $964,617. UHS did not pay the ransom and was able to recover data through backups, but still reported an impact of $67 million dollars in recovery costs.[2] On 29 October, one month after the attack, UHS made an official statement that their systems had been restored and they were resuming normal operations.[3]

Researchers and analysts identified 18 unique techniques (used in a sequence of 19 steps) utilized during the attack with a total of 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. Fourteen of the identified techniques used during the UHS cyber attack were precursors to the triggering event. Analysis identified 106 observables associated with these precursor techniques, 82 of which were assessed to have an increased likelihood of being perceived in the 30 days to two hours 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.

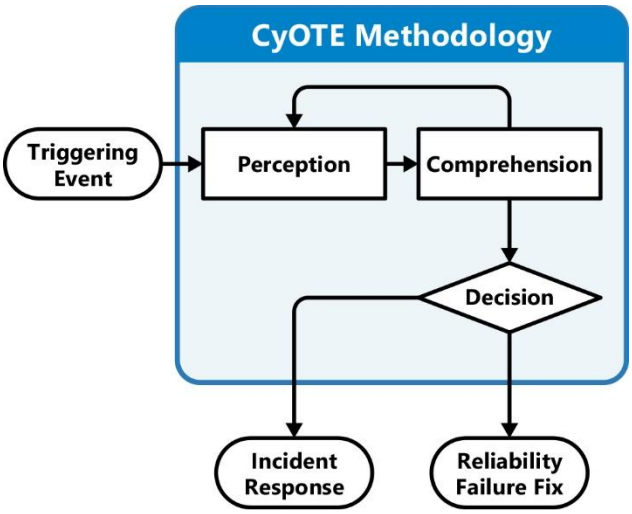

Figure 1. CyOTE Methodology

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

On the morning of 27 September 2020 (D-0), Universal Health Services (UHS) suffered a ransomware attack that disabled Information Technology (IT) systems including phone systems, medical record workstations, patient test results, and imaging equipment.[4] Based in Pennsylvania, UHS headquarters manages over 400 hospitals and is one of the largest healthcare suppliers in the United States with 3.5 million patients each year.[5]

The adversaries most likely gained initial access through a spearphishing email, although specifically when this occurred is not known from available information. UHS employees observed adversaries disabling multiple antivirus programs and actively accessing hard drives prior to the loss of availability of critical information (H-2).[a] In addition, files were renamed to include the .ryk extension, a signature tactic employed by the Ryuk ransomware adversaries. The timeline from these staff observations to the ransom note appearing is unknown. Adversaries very likely used these techniques several hours prior to the triggering event.[6]

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.

The ransom note displayed on 27 September (D-0) appeared after a loss of availability for various critical information systems and demanded UHS to immediately pay the ransom to recover the various systems or lose encrypted data. The displayed ransom note contained the phrase “Shadow of the Universe”, which previous Ryuk ransomware attacks displayed.[7]

Employees lost access to vital internet-dependent systems, including patient information and diagnostics.[8] Some employees had to resort to manually filing patient details with pen and paper, while other facilities had to redirect ambulances and urgent cases to other facilities for adequate care.[9] Once the IT team noticed the activity, they took all systems offline to prevent further damage and propagation of the malware.[10]

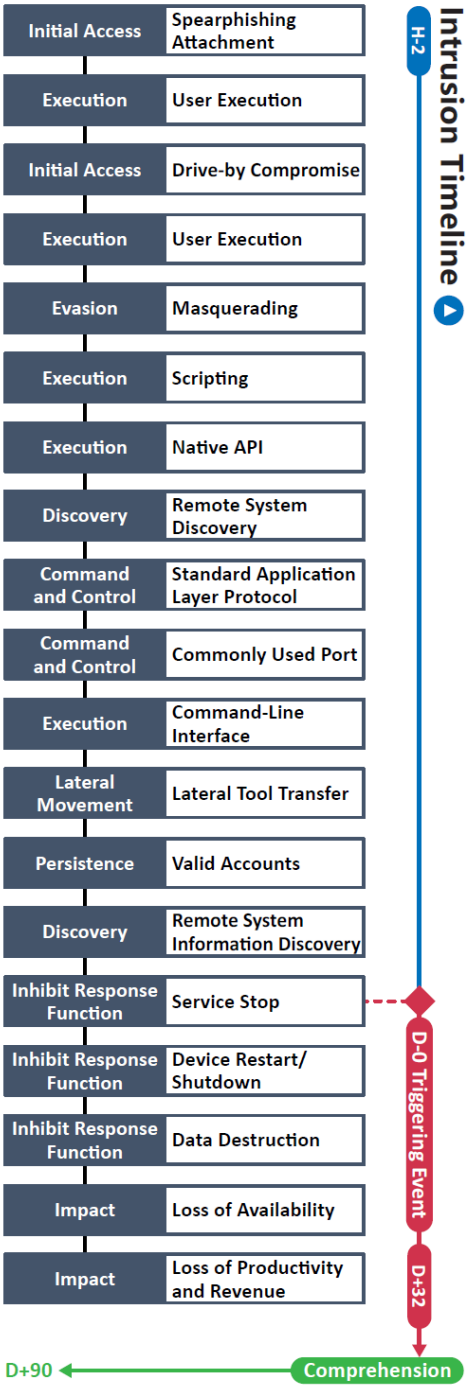

Figure 2. Intrusion Timeline

On 28 September (D+1), UHS stated they implemented extensive IT security protocols and were working diligently with IT security partners to restore operations as quickly as possible. UHS reported again on 29 October (D+32), roughly one month after the attack, that all systems were restored, and normal operations were resuming. [11] During this time, facilities utilized established

[a] “H” corresponds to hours prior to (H-) or after (H+) the triggering event; “D” events correspond to days prior to or after; and “M” events correspond to minutes prior to or after.

back-up processes, including offline documentation methods, to continue patient care.[12] UHS maintained that no patient or employee data had been accessed, copied, or misused. UHS did not pay the ransom, but the attack still had an estimated total impact of $67 million in losses in revenue and productivity as well as recovery costs for that year.[13]

Analysis identified 18 unique techniques in a sequence and timeframe likely used by adversaries during this cyber attack (**Error! Reference source not found.** 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Ryuk Ransomware Attack on Universal Health Services 2020 Cyber Attack

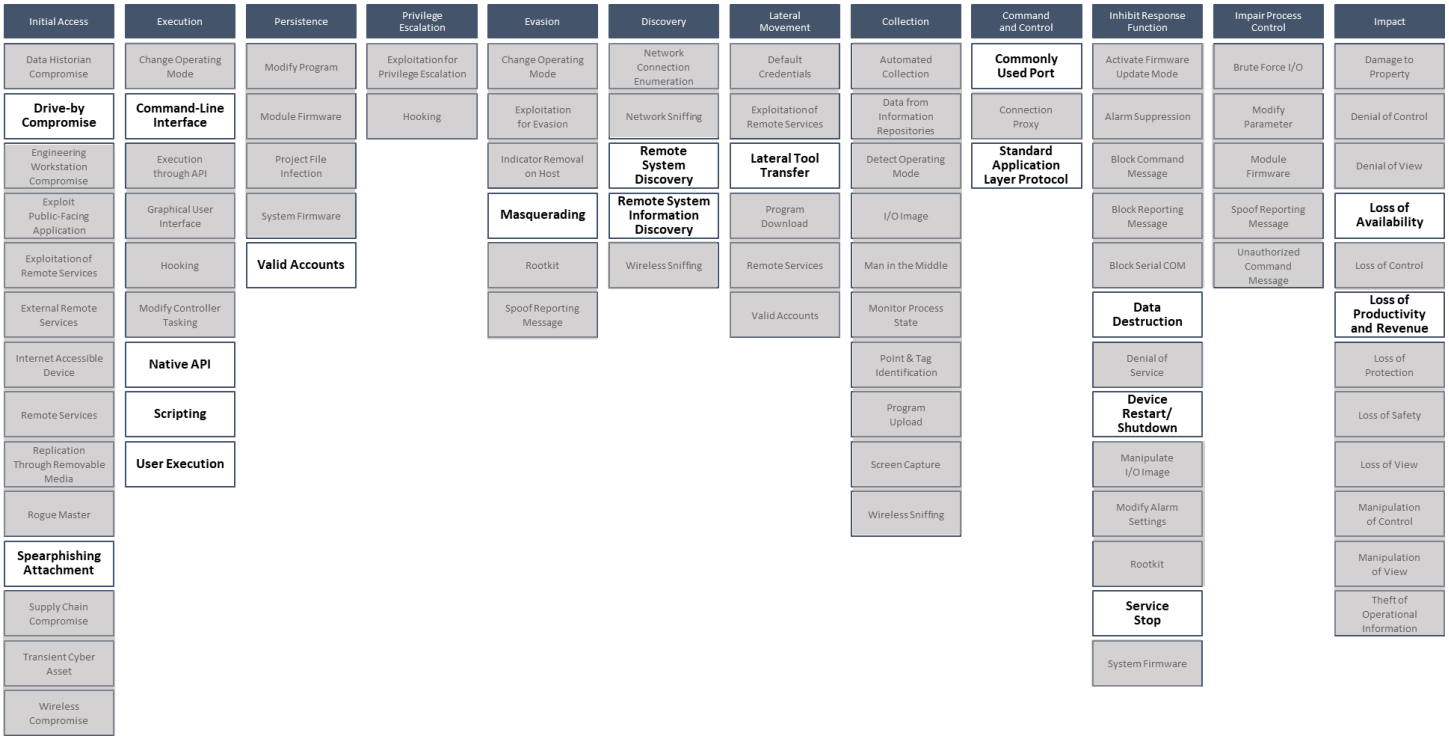

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	19
Technique Observables	185
Precursor Techniques	14
Precursor Technique Observables	106
Highly Perceivable Precursor Technique Observable	82

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

Adversaries likely used one or more malicious spearphishing attachment campaigns to facilitate the download and execution of the common initial access malware Emotet.[14] Emotet is a banking trojan that often acts as an initial access vector for financially motivated adversaries, including ransomware groups. Ransomware groups then buy access from botnet operators and conduct further malicious activity in a victim's environment, including installing secondary payloads such as Bazarloader that can ultimately result in ransomware deployment.[15]

Botnet operators that sell banking trojans make use of malicious office documents and legitimate infrastructure, such as Google Drive and OneDrive, to convince end-users to install malware. Emotet operators likely leveraged Sendgrid, a communication tool used to send marketing emails, to send malicious emails to UHS employees.[16] During 2020, COVID-19-themed lures were extremely popular and effective, and cybercriminals leveraged them with great effect. These emails likely contained Google Drive links, which when clicked on, would route the end-user to a webpage that displayed a prompt to download a malicious executable that would then install Emotet.

IT Staff, IT Cybersecurity, Support Staff, and Management personnel may have been able to observe spearphishing emails and targeted links.

A total of four observables were identified with the use of the Spearphishing Attachment technique (T0856). This technique is important for investigation because it is often the first technique adversaries use to gain initial access to gather information about a victim organization. This technique appears at the beginning of the 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 four observables associated with this technique, three are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 29 artifacts could be generated by the Spearphishing Attachment technique
Technique Observers[b]	IT Staff, IT Cybersecurity, Support Staff, Management
Resources	Technique Detection References

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

3.2. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

For the initial attack to be successful, one or more UHS employees likely interacted with the emails by clicking on the Google Drive link. This malicious link would then route the employees to a webpage hosting a malicious document that would install Emotet.[17]

IT Staff, IT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe the malicious Google Drive documents, or the browser update prompts that downloaded the Bazarloader trojan.

A total of seven observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation because it is one of the most common methods adversaries utilize to gain initial access. This technique appears early in the timeline and responding to it will likely halt all future adversary activity in the victim's environment. Terminating this chain of techniques at this point would effectively halt all further adversary activity and limit impact to business operations.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 23 artifacts could be generated by the User Execution technique
Technique Observers	IT Staff, IT Cybersecurity, Engineering, Support Staff, Management
Resources	Technique Detection References

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

UHS has not disclosed details of the Ryuk ransomware spearphishing attack, but it is likely one or more employees across several UHS facilities opened an email that contained a link to Google Drive.[18] This malicious Google Drive link would then route the employee(s) to a webpage hosting a malicious document that would ultimately install Emotet. One or more UHS employees likely interacted with the emails by clicking on the Google Drive link. The mail would route the user to a new webpage, likely Google Drive, that then prompted them to download a malicious document.[19]

IT Staff, IT Cybersecurity, Support Staff, and Management personnel may have been able to observe a re-routing email link that took them to Google Drive and requested a document download.

A total of six observables were identified with the use of the Drive-by Compromise technique (T0817). This technique is important for investigation because adversaries may gain access to a system when a user visits a website. With this technique, the user's web browser becomes a target simply by visiting the compromised website. This technique appears early in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would limit initial access into the system.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 24 artifacts could be generated by the Drive-by Compromise technique
Technique Observers	IT Staff, IT Cybersecurity, Support Staff, Management
Resources	Technique Detection References

3.4. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

Once the user opens the downloaded document from the Google Drive webpage, the malicious document installs and executes Emotet.[20] Once installed, the operators can sell access to other adversaries, who then install malware of their own, like Bazarloader. As a result, the adversaries can start conducting discovery and lateral movement activity within the victim's environment.[21]

IT Staff, IT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe the malicious Google Drive documents, or the update prompts that downloaded the Bazarloader trojan.

One observable was identified with the use of the User Execution technique (T0863). This technique is important for investigation because it is one of the most common gateways adversaries utilize to gain initial access. This technique appears early in the timeline and responding to it will likely halt all future adversary activity in the victim's environment. Terminating this chain of techniques at this point would effectively halt all further adversary activity and limit impact to business operations.

The one observable associated with this technique is assessed to be highly perceivable. It is 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, Engineering, Support Staff, Management
Resources	Technique Detection References

3.5. MASQUERADING TECHNIQUE (T0849) FOR EVASION

Ryuk ransomware makes use of stolen administrative credentials to evade detection engines and ensure successful execution of the malware. Adversaries likely used a credential tool such as Mimikatz, an open-source penetration testing tool that allows users to view and harvest authentication credentials and other information from a targeted machine's memory.[22] Once the adversary gains credentials, they are able to masquerade as legitimate users throughout the system.

Adversaries also ensured the processes and tasks of Bazarloader and other secondary tools were renamed after common, legitimate Windows processes and files and placed in directories that mimicked normal background activity.[23]

Bazarloader is a backdoor that allows an adversary to communicate remotely with infected machines to conduct reconnaissance or move additional payloads into the environment via Domain Name System (DNS). This allows Ryuk to evade typical network defenses and allow their nefarious communications to blend in with legitimate DNS traffic.[24]

IT Cybersecurity personnel may have been able to observe stolen credentials and the renaming of tools.

A total of five observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation because it circumvents critical security tools that can alert a victim of malicious cyber activity. This technique appears in the middle of the timeline and responding to it will likely halt the execution of the malware, although this is unlikely given the brief time from disabling services to ransomware execution. Terminating the chain of techniques at this point would halt the deployment of the ransomware.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 15 artifacts could be generated by the Masquerading technique
Technique Observers	IT Cybersecurity
Resources	Technique Detection References

3.6. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

Financially motivated adversaries often abuse Visual Basic for Applications (VBA) or JavaScript to automatically execute commands embedded in the malicious documents.[25] Later in the intrusion, adversaries often use Cobalt Strike, a popular penetration testing tool to executed batch scripts and network discovery commands.[26] Adversaries then utilize scripting to send a list of commands, eventually gaining administrative credentials and access to the domain controller.[27]

IT Staff and IT Cybersecurity personnel may have been able to observe batch scripting and network discovery commands.

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

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

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

3.7. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

Multiple native application programming interfaces (APIs) are utilized throughout the attack. These including ShellExecuteW to run the executables, GetWindowsDirectoryW to create folders, and VirtualAlloc, WriteProcessMemory, and CreateRemoteThread for process. Ryuk also interacts with Windows OS native applications throughout the execution stages of the malware.[28]

Additionally, the adversaries may attempt to uninstall the victim's security applications that could prevent the ransomware from executing, using scripting or manually disabling the applications.[29]

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

A total of seven 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 further execution of the malware.

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

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

3.8. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

On the first domain controller after initial compromise, adversaries dropped a Dynamic Link-Library (DLL) and executed it via rundll32.exe to evade detection and gain additional access. This step is vital in the progression of the attack. [30] Once the adversaries gained access into a UHS domain controller, they likely proceeded to dump Active Directory (AD) credentials to discover any accounts with administrative-level privileges. To do this remotely, adversaries likely used Remote Desktop Protocol (RDP) to connect to the domain controller with the administrator credentials obtained early in the intrusion. They then performed a folder drop on the domain controller to spread files to additional servers, such as file shares, Windows Management Instrumentation (WMI), and RDP clipboard transfer.[31]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe anomalous network connections from internal hosts to other internal hosts, in both the IT and OT environments.

A total of 10 observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation because if the defenders can prevent the adversary from collecting system information with this technique, the adversary will have to use more complicated techniques to understand the victim's network. This technique appears in the middle and late stage of the timeline and responding to it will help identify and scope which hosts the adversaries have infected and which hosts they are targeting. This may provide defenders an opportunity to prevent continual scanning and contain infected hosts. If the defenders identify and contain this activity, they could degrade the adversaries' ability to discover hosts, remotely connect, or collect operational information from compromised machines. Terminating the chain of techniques at this point would limit the adversaries' ability to identify systems with operational information.

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

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

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

The adversaries used several standard application layer protocols throughout the intrusion for C2 communications, including DNS and HTTP.[32] Malware like Emotet commonly utilizes Hypertext Transfer Protocol (Secure) (HTTP and HTTPS) for C2 communications, as well as for downloading other payloads from external resources. In addition, RDP is likely used to connect to the victim's domain controller.[33]

IT Staff and IT Cybersecurity personnel may have been able to observe C2 traffic associated with Emotet, as well as network traffic from external adversary infrastructure to the local domain controller.[34]

A total of three observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation as prolonged anomalous network traffic is an indication of adversary activity. This technique appears throughout the timeline and responding to it will alert defenders to malicious activity within their environment. Terminating the chain of techniques at this point would likely halt any further adversary activity if defenders took steps to block the malicious network traffic.

Of the three observables associated with this technique, two 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

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

Malware such as Bazarloader acts as a backdoor that allows infected machines to communicate with C2 servers over DNS to appear as typical network defense products and allows their malicious communications to blend in with legitimate DNS traffic.[35] HTTP/HTTPS, RDP, and DNS commonly used ports were very likely used by the adversaries, as there was no evidence to suggest non-standard ports were used in the attack.

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe the anomalous traffic to and from C2 servers, as well as outbound data exfiltration traffic at odd hours.

A total of three observables were identified with the use of the Commonly Used Port technique (T0885). This technique is important for investigation as port usage is an indicator of adversary activity in the victim's environment. This technique appears throughout the timeline and responding to it may halt future activity. Terminating the chain of techniques at this point would limit adversary activity in the victim's environment and prevent communication with malware already present.

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

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

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

Adversaries used the Command-Line Interface technique (T0807) throughout the course of the intrusion. Through access from malware such as Emotet or Bazarloader, adversaries were able to remotely open a command prompt on an infected host and execute commands related to discovery or lateral movement.[36] Additionally, adversaries may use the command line to operate post-exploitation tools such as Cobalt Strike. Once Cobalt Strike installs on the infected host, it can communicate with a C2 server to help an adversary gain access to the domain controller.[37] Finally, adversaries may have used the command line to remotely generate malicious Service User Accounts.[38]

IT Staff and IT Cybersecurity personnel may have been able to observe various command-line executions associated with Emotet, Bazarloader, or Cobalt Strike.

A total of nine observables were identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation because it allows adversaries to execute malicious payloads within the victim's environment or to conduct reconnaissance. This technique appears throughout the timeline and responding to it may prevent the adversaries from deploying or executing the ransomware. Terminating the chain of techniques at this point would prevent prolonged data exfiltration.

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

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

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

Adversaries utilized the Lateral Tool Transfer technique (T0867) throughout the intrusion. They likely used Emotet to download and execute Bazarloader within UHS's environment. From there, adversaries proceeded to deploy additional tools, such as Cobalt Strike, and likely Mimikatz, AdFind, and Bloodhound to elevate privileges and move laterally, until they obtained credentials that provided access to the domain controller.[39,c]

IT Staff and IT cybersecurity personnel may have been able to observe the presence of anomalous files, as well as the anomalous network traffic associated with the download of additional tools and payloads.

A total of 23 observables were identified with the use of the Lateral Tool Transfer technique (T0867). This technique is important for investigation because it indicates adversaries are moving additional tools and payloads into the victim environment to perform further malicious activity. This technique appears throughout the timeline and responding to it will limit further adversary activity. Terminating the chain of techniques at this point would prevent ransomware deployment and data exfiltration from the enterprise environment.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 22 artifacts could be generated by the Lateral Tool Transfer technique
Technique Observers	IT Staff, IT Cybersecurity
Resources	Technique Detection References

[c] The Ryuk observables in Appendix A outlines a list of other tools likely used for lateral movement throughout the attack.

3.13. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

Ryuk adversaries leveraged stolen administrative credentials to gain access to the UHS domain controller without detection.[40] They likely used tools like Mimikatz to obtain necessary credentials for escalation into the network. After gaining access, adversaries continued discovery, privilege escalation, and lateral movement.[41]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe logons from valid user credentials at anomalous hours.

A total of six observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because adversaries may use stolen or compromised credentials to bypass access controls to various resources within a network or grant an adversary increased privileges to specific systems and devices. Compromised or stolen credentials may limit the ability of defenders to detect potential intrusions or compromises due to elevated access levels and privileges afforded by unsecured accounts. This technique appears in the middle of the timeline and responding to it will deny an adversary continued access to any internal resources. Terminating the chain of techniques at this point would prevent an adversary from moving laterally to shared resources.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering
Resources	Technique Detection References

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

The adversaries used a PowerShell command to gather information while accessing AD data and generated a dump file (ALLWindows.csv) containing log-in, domain controller, and Operating System (OS) data for Windows computers on the network.[42] To enumerate the AD information, Ryuk ransomware operators likely relied on AdFind, an AD query tool, and the post-exploitation tool Bloodhound that explores and discovers relationships in an AD domain to find attack paths.[43]

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

A total of 16 observables were identified with the use of the Remote System Information Discovery technique (T0888). This technique is important for investigation because it provides adversaries detailed information about target devices, allowing them to attack with enhanced specificity. This technique appears near the middle of the timeline and responding to it will prevent adversaries from properly identifying intended target devices. Terminating the chain of techniques at this point would limit data exfiltration and possibly operational damage.

Of the 16 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 eight artifacts could be generated by the Remote System Information Discovery technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity
Resources	Technique Detection References

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

On 27 September 2020, UHS employees noticed abnormal behavior on their personal computers, such as antivirus programs disabling and actively accessing hard drives, likely caused by the Ryuk ransomware.[44] Employees started losing access to vital, internet-dependent systems, including previous patient information and diagnostic systems. Some employees had to resort to filing patient details with pen and paper, while other facilities had to redirect ambulances and urgent care patients to other facilities. File names were changed to include the .ryk extension, which is associated with the Ryuk ransomware group. The displayed ransom note read "Shadow of the Universe," which has been seen in previous Ryuk ransomware attacks.[45]

In a public statement made by UHS on 29 September, Ryuk called kill.bat for stopping services, disabling services, and killing processes. Certain clinics utilized established back-up processes, including offline documentation methods, to continue working.[46]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Support Staff, and Management personnel may have been able to observe antivirus programs disabling, losing vital systems, and observing their files being renamed with a .ryk extension.

A total of 27 observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation because it disables critical security tools that can alert a victim to malicious cyber activity. This technique appears late in the timeline and represents the triggering event. Responding to it would likely halt final execution of the ransomware, although it is highly unlikely defenders would have sufficient time to act. Terminating the chain of techniques at this point would limit operational damage.

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

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

3.16. DEVICE SHUTDOWN/RESTART TECHNIQUE (T0816) FOR INHIBIT RESPONSE FUNCTION

The attack shut down UHS computers and resulted in a loss of access to anything computer-based, including lab test results and radiology studies, forcing care providers to turn away patients.[47] Once the IT team at UHS noticed the activity and employees began reporting their concerns, they took all systems offline to prevent further damage and propagation of the malware.[48]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe anomalous host shutdowns and restarts.

One observable was identified with the use of the Device Restart/Shutdown technique (T0816). This technique is important for investigation because anomalous shutdowns often are part of the final stage of an enterprise-wide ransomware attack. Anomalous shutdowns may also indicate a reliability incident with malfunctioning equipment. This technique appears after the triggering event and terminating the chain of techniques at this point could halt the execution of the ransomware, although it is highly unlikely defenders would have sufficient time to act.

The one observable associated with this technique is assessed to be highly perceivable. It is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts	A total of 17 artifacts could be generated by the Device Shutdown/Restart technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management
Resources	Technique Detection References

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

Upon execution, the malware encrypts files with targeted file extensions and appends a .ryk file extension to them. This effectively renders any targeted files unusable unless decrypted. Infected hosts would also display a ransom note on enterprise systems informing users that their files had been encrypted and the only way to decrypt them was to pay the ransom.

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management likely observed files with the .ryk file extension and were unable to access common file types.

A total of 35 observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because it renders files crucial to business and other enterprise operations unusable. This technique appears after the triggering event and responding to it at this point in the timeline is unlikely to minimize the impact of Ryuk ransomware deployment.

All 35 observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

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

3.18. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

Once the Ryuk ransomware is deployed, all files except for extensions .dll, .lnk, .ini, and .exe are encrypted; these files are exempted so the system remains capable of file restoration if the victim pays the ransom.[49] Ryuk implements a unique AES-256 encryption key which changes the targeted file extensions to .ryk, which is then encrypted with a hardcoded RSA-4096 public encryption key.[50] There was likely an increase in system resource utilization due to the encryption process. In the meantime, UHS employees continued operations manually, tracking patient information and details with pen and paper.

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

A total of 15 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 after 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.

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

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

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

In late October 2020, nearly a month after the attack, UHS announced it had restored most of the affected computing systems at behavioral and acute care health hospitals. Further, IT support was able to bring back systems vital to hospital operations including laboratory and electronic records management.[51]

Though UHS did not pay the ransom, they announced that the Ryuk ransomware attack had an estimated impact of $67 million and had an aggregate unfavorable pre-tax impact for 2020. Most of the impact was attributed to acute care services (i.e., diagnostics and surgeries) and a decrease in patient activity.[52]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe loss of revenue and productivity while repairs were taking place.

One observable was identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation because it demonstrates financial exposure to cyber-physical adversarial behavior. If adversarial behavior is not identified as a contributing cause, continued adversarial behavior may cause additional physical and financial impacts to the victim. This technique appears at the end of the timeline and responding to it will include efforts to regain operational functionality and resume normal operations.

The one observable associated with this technique is assessed to be highly perceivable. It is italicized and marked † in Appendix A.

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

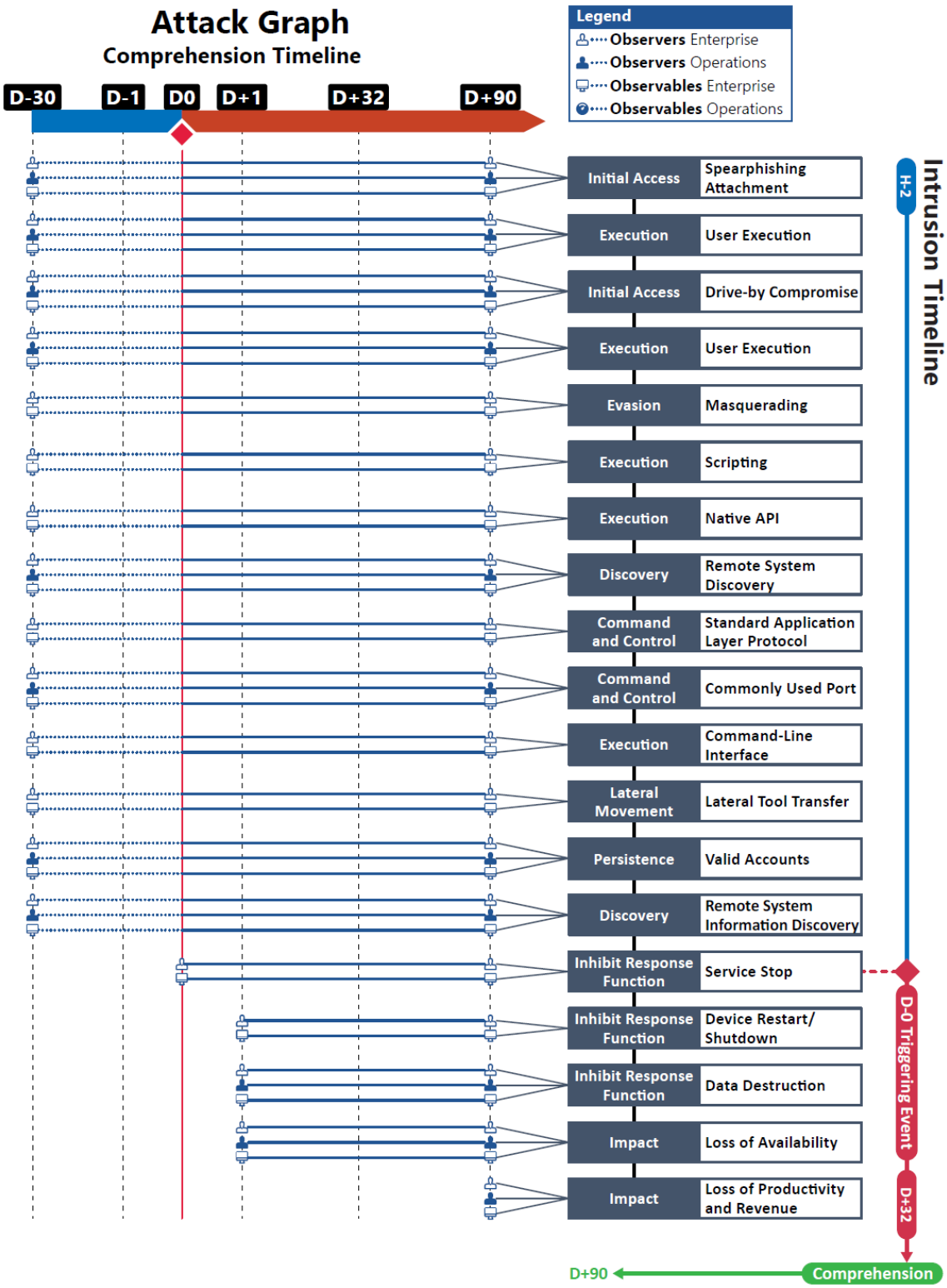

Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †.

Observables Associated with Spearphishing Attachment Technique (T0865)	
Observable 1 †	*Presence of Anomalous Email Containing a Web Link: Google Drive: docs.google.com*
Observable 2 †	*Anomalous Network Traffic: From Local Host to External Host: HyperText Transfer Protocol (HTTP) Over Transmission Control Protocol (TCP) Port 80: HTTP GET Request: docs.google.com*
Observable 3	Anomalous Network Traffic: From Local Host to External Host: HyperText Transfer Protocol Secure (HTTPS) Over Transmission Control Protocol (TCP) Port 443: HTTPS Get Request: docs.google.com
Observable 4 †	*Anomalous Network Traffic: From Local Host to External Server: Domain Name System (DNS) Over Transmission Control Protocol (TCP) Port 53: docs.google.com*

Observables Associated with User Execution Technique (T0863)	
Observable 1 †	*Presence of Anomalous Email Containing a Web Link: Google Drive: docs.google.com*
Observable 2 †	*User Interaction with Anomalous Web Link: Google Drive: docs.google.com*
Observable 3 †	*Anomalous Network Traffic: From Local Host to External Host: HyperText Transfer Protocol (HTTP) Over Transmission Control Protocol (TCP) Port 80: HTTP GET Request: docs.google.com*
Observable 4	Anomalous Network Traffic: From Local Host to External Host: HyperText Transfer Protocol Secure (HTTPS) Over Transmission Control Protocol (TCP) Port 443: HTTPS Get Request: docs.google.com
Observable 5 †	*Anomalous Network Traffic: From Local Host to External Server: Domain Name System (DNS) Over Transmission Control Protocol (TCP) Port 53: docs.google.com*
Observable 6 †	*Presence of Anomalous Email Containing a Web Link: Google Drive: docs.google.com*
Observable 7 †	*User Interaction with Anomalous Web Link*

Observables Associated with Drive-by Compromise Technique (T0817)	
Observable 1 †	*Presence of Anomalous Email Containing a Web Link: Google Drive: docs.google.com*
Observable 2 †	*Anomalous Network Traffic: From Local Host to External Host: HyperText Transfer Protocol (HTTP) Over Transmission Control Protocol (TCP) Port 80: HTTP GET Request*
Observable 3 †	*Anomalous Network Traffic: From Local Host to External Host: HyperText Transfer Protocol Secure (HTTPS) Over Transmission Control Protocol (TCP) Port 443: HTTPS Get Request*

Observables Associated with Drive-by Compromise Technique (T0817)	
Observable 4 †	*Anomalous Network Traffic: From Local Host to External Server: Domain Name System (DNS) Over Transmission Control Protocol (TCP) Port 53: docs.google.com*
Observable 5 †	*Anomalous Network Traffic: From External Server to Local Host: HyperText Transfer Protocol (HTTP) Over Transmission Control Protocol (TCP) Port 80: HTTP GET Request*
Observable 6	Anomalous Network Traffic: From External Server to Local Host: HyperText Transfer Protocol Secure (HTTPS) Over Transmission Control Protocol (TCP) Port 443: HTTPS Get Request

Observables Associated with User Execution Technique (T0863)	
Observable 1 †	*User Interaction with Anomalous Web Link: Google Drive: docs.google.com*

Observables Associated with Masquerading Technique (T0849)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to External Domain Server: From Host Executing print_document.exe to External Domain: Over Domain Name System (DNS) UDP Port 53*
Observable 2 †	*Anomalous Network Traffic: From Local Host to External Web Server: From Host Executing print_document.exe to External Web Server: Over HyperText Transfer Protocol (HTTP) Transmission Control Protocol (TCP) Port 80*
Observable 3	Anomalous Network Traffic: From Local Host to External Web Server: From Host Executing print_document.exe to External Web Server: Over HyperText Transfer Protocol Secure (HTTPS) Transmission Control Protocol (TCP) Port 443
Observable 4 †	*Anomalous Binary on Local Host: Dynamic Link Libraries (.DLL):*
Observable 5 †	*Anomalous Binary on Local Host: Rich Text Files (.RTF):*

Observables Associated with Scripting Technique (T0853)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to Domain Controller: Over SMB Transmission Control Protocol (TCP) Port 135*
Observable 2 †	*Anomalous Network Traffic: From Local Host to Domain Controller: Over RPC Transmission Control Protocol (TCP) Port 139*
Observable 3	Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C whoami /groups
Observable 4 †	*Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C nltest /domain_trusts /all_trusts*
Observable 5 †	*Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C net group "enterprise admins" /domain*
Observable 6 †	*Anomalous Command Line: C:\WINDOWS\system32\net1 group "domain admins" /domain*

Observables Associated with Native API Technique (T0834)	
Observable 1 †	*Presence of Anomalous Binary on Host: print_document.exe*
Observable 2 †	*Execution of Anomalous Binary on Host: print_document.exe*
Observable 3 †	*Anomalous Execution of Native Operating System (OS) Application Programming Interface (API): Windows API: ShellExecuteW*
Observable 4 †	*Anomalous Execution of Native Operating System (OS) Application Programming Interface (API): Windows API: GetWindowsDirectoryW*
Observable 5	Anomalous Execution of Native Operating System (OS) Application Programming Interface (API): Windows API: VirtualAlloc
Observable 6	Anomalous Execution of Native Operating System (OS) Application Programming Interface (API): Windows API: WriteProcessMemory
Observable 7	Anomalous Execution of Native Operating System (OS) Application Programming Interface (API): Windows API: CreateRemoteThread

Observables Associated with Remote System Discovery (T0846)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to Domain Controller: Over Server Message Block (SMB) Transmission Control Protocol (TCP) Port 135*
Observable 2 †	*Anomalous Network Traffic: From Local Host to Domain Controller: Over Remote Procedure Call (RPC) Transmission Control Protocol (TCP) Port 139*
Observable 3 †	*Anomalous Network Traffic: From Local Host to Domain Controller: Over Server Message Block (SMB) Transmission Control Protocol (TCP) Port 445*
Observable 4 †	*Anomalous Network Traffic: From Local Host to Domain Controller: Over Remote Desktop Protocol (RDP) Transmission Control Protocol (TCP) Port 3389*
Observable 5 †	*Anomalous Command Line: C:\Windows\system32\cmd.exe /C rundll32 C:\Windows\system32\SQL.dll, StartW*
Observable 6 †	*Anomalous Command Line: rundll32 C:\PerfLogs\arti64.dll, rundll*
Observable 7 †	*Anomalous Command Line: regsvr32 C:\PerfLogs\arti64.dll*
Observable 8 †	*Anomalous Command Line: rundll32 C:\PerfLogs\socks64.dll*
Observable 9 †	*Anomalous Host Activity: Anomalous Increase in System Resource Utilization*
Observable 10 †	*Anomalous Host Activity: Anomalous Increase in Network Utilization*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to External Domain Server: From Host Executing print_document.exe to External Domain: Over Domain Name System (DNS) UDP Port 53*
Observable 2 †	*Anomalous Network Traffic: From Local Host to External Web Server: From Host Executing print_document.exe to External Web Server: Over HyperText Transfer Protocol (HTTP) Transmission Control Protocol (TCP) Port 80*
Observable 3	Anomalous Network Traffic: From Local Host to External Web Server: From Host executing print_document.exe to External Web Server: Over HyperText

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
	Transfer Protocol Secure (HTTPS) Transmission Control Protocol (TCP) Port 443

Observables Associated with Commonly Used Ports Technique (T0855)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to External Domain Server: From Host Executing print_document.exe to External Domain: Over Domain Name System (DNS) UDP Port 53*
Observable 2 †	*Anomalous Network Traffic: From Local Host to External Web Server: From Host Executing print_document.exe to External Web Server: Over HyperText Transfer Protocol (HTTP) Transmission Control Protocol (TCP) Port 80*
Observable 3	Anomalous Network Traffic: From Local Host to External Web Server: From Host Executing print_document.exe to External Web Server: Over HyperText Transfer Protocol Secure (HTTPS) Transmission Control Protocol (TCP) Port 443

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 1 †	*Anomalous Network Traffic: From Local Host to Domain Controller: Over SMB Transmission Control Protocol (TCP) Port 135, Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C nltest /domain_trusts /all_trusts*
Observable 2 †	*Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C net group "enterprise admins" /domain*
Observable 3 †	*Anomalous Command Line: C:\WINDOWS\system32\net1 group "domain admins" /domain*
Observable 4 †	*Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C net localgroup administrators*
Observable 5 †	*Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C ipconfig*
Observable 6 †	*Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C nltest /dclist:[target company domain name]*
Observable 7 †	*Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C nltest /dclist:[target company name]*
Observable 8 †	*Presence of Anomalous Binary on Host: print_document.exe*
Observable 9 †	*Execution of Anomalous Binary on Host: print_document.exe*

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 1 †	*Presence of Anomalous Binary on Host: qoipozincyusury.exe*
Observable 2 †	*Anomalous Network Traffic: From Local Host to External IP: Over HyperText Transfer Protocol (HTTP) Transmission Control Protocol (TCP) Port 80: HTTP GET Request*
Observable 3	Anomalous Network Traffic: From Local Host to External IP: Over HyperText Transfer Secure Protocol (HTTPS) Transmission Control Protocol (TCP) Port 443: HTTPS GET Request

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 4	Anomalous Network Traffic: From Local Host to External IP: Over File Transfer Protocol (FTP) Transmission Control Protocol (TCP) Port 22
Observable 5	Anomalous Network Traffic: From Local Host to External IP: Over Secure File Transfer Protocol (SFTP) Transmission Control Protocol (TCP) Port 23
Observable 6 †	*Anomalous Network Traffic: From Local Host to External IP: Via Rclone Application*
Observable 7 †	*Anomalous Network Traffic: From Local Host to External IP: Over Transmission Control Protocol (TCP) Port 445*
Observable 8 †	*Anomalous Network Traffic: From External IP to Local Host: Over HyperText Transfer Protocol (HTTP) Transmission Control Protocol (TCP) Port 80: HTTP POST Request*
Observable 9	Anomalous Network Traffic: From External IP to Local Host: Over HyperText Transfer Secure Protocol (HTTPS) Transmission Control Protocol (TCP) Port 443: HTTPS POST Request
Observable 10	Anomalous Network Traffic: From External IP to Local Host: Over File Transfer Protocol (FTP) Transmission Control Protocol (TCP) Port 22
Observable 11	Anomalous Network Traffic: From External IP to Local Host: Over Secure File Transfer Protocol (SFTP) Transmission Control Protocol (TCP) Port 23
Observable 12 †	*Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) Transmission Control Protocol (TCP) Port 445*
Observable 13 †	*Anomalous Command Line: rclone copy <source:sourcepath> <dest:destpath>*
Observable 14 †	*Anomalous Command Line: mega-export -a <Local Host File Path> <Remote Host File Path>*
Observable 15 †	*AnomalousCommand Line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe*
Observable 16 †	*Anomalous Binary on Local Host: rclone.exe*
Observable 17 †	*Anomalous Binary on Local Host: MEGAcmdShell.exe*
Observable 18 †	*Anomalous Binary on Local Host: empire.exe*
Observable 19 †	*Anomalous Binary on Local Host: koadic.exe*
Observable 20 †	*Execution of Anomalous Binary on Host: rclone.exe*
Observable 21 †	*Execution of Anomalous Binary on Host: MEGAcmdShell.exe*
Observable 22 †	*Execution of Anomalous Binary on Host: empire.exe*
Observable 23 †	*Execution of Anomalous Binary on Host: koadic.exe*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1 †	*Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) Transmission Control Protocol (TCP) Port 445*
Observable 2 †	*Anomalous Network Traffic: From External IP to Local Host: Over Remote Desktop Protocol (RDP) Transmission Control Protocol (TCP) Port 3389*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 3 †	*Anomalous Host Activity: Successful Logon from External Host: An Account Was Successfully Logged On (Windows Event ID 4624): Anomalous Timestamp*
Observable 4 †	*Anomalous Host Activity: Successful Logon from External Host: An Account Was Successfully Logged On (Windows Event ID 4624): Anomalous Remote IP*
Observable 5 †	*Anomalous Host Activity: Increase in Failed Login Attempts: An Account Failed to Log On (Windows Event ID 4625): Anomalous Timestamp*
Observable 6 †	*Anomalous Host Activity: Increase in Failed Login Attempts: An Account Failed to Log On (Windows Event ID 4625): Anomalous Remote IP*

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 1 †	Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) Transmission Control Protocol (TCP) Port 445
Observable 2 †	Anomalous Network Traffic: From External IP to Local Host: Over Remote Desktop Protocol (RDP) Transmission Control Protocol (TCP) Port 3389
Observable 3	Presence of Anomalous File on Host: Anomalous Comma Separated Value (CSV) file: ALLWindows.csv
Observable 4 †	*Anomalous Command-Line: C:\Windows\system32\cmd.exe /C Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name, DNSHostName, OperatingSystem, LastLogonDate | Export-CSV C:\Users\AllWindows.csv -NoTypeInformation -Encoding UTF8*
Observable 5	Anomalous Command-Line: adfind.exe -f "(objectcategory=person)"
Observable 6	Anomalous Command-Line: adfind.exe -f "objectcategory=computer"
Observable 7	Anomalous Command-Line: adfind.exe -f "(objectcategory=organizationalUnit)"
Observable 8	Anomalous Command-Line: adfind.exe -sc trustdmp
Observable 9	Anomalous Command-Line: adfind.exe -subnets -f (objectCategory=subnet)
Observable 10	Anomalous Command-Line: adfind.exe -f "(objectcategory=group)"
Observable 11	Anomalous Command-Line: adfind.exe -gcb -sc trustdmpobjectcategory=group)"
Observable 12 †	*Anomalous Command-Line: nltest /domain_trusts /all_trusts*
Observable 13 †	*Presence of Anomalous Binary: C:\Windows\Temp\adf\AdFind.exe*
Observable 14 †	*Presence of Anomalous Script: C:\Windows\Temp\adf\adf.bat*
Observable 15 †	*Execution of Anomalous Binary: C:\Windows\Temp\adf\AdFind.exe*
Observable 16 †	*Execution of Anomalous Script: C:\Windows\Temp\adf\adf.bat*

Observables Associated with Service Stop Technique (T0881)	
Observable 1 †	*Anomalous Host Activity: Windows Service Stop (Event ID 6006)*
Observable 2 †	*Anomalous Host Activity: Windows Service Stopped: avpsus*
Observable 3 †	*Anomalous Host Activity: Windows Service Stopped: McAfeeDLPAgentService*

Observables Associated with Service Stop Technique (T0881)	
Observable 4 †	*Anomalous Host Activity: Windows Service Stopped: mfewc*
Observable 5 †	*Anomalous Host Activity: Windows Service Stopped: Bare Metal Backup (BMR) Boot Service*
Observable 6 †	*Anomalous Host Activity: Windows Service Stopped: NetBackup BMR MTFTP Service*
Observable 7 †	*Anomalous Host Activity: Windows Service Disabled (Event ID 7040)*
Observable 8 †	*Anomalous Host Activity: Windows Service Disabled: SQLTELEMETRY*
Observable 9 †	*Anomalous Host Activity: Windows Service Disabled: SQLTELEMETRY$ECWDB2*
Observable 10 †	*Anomalous Host Activity: Windows Service Disabled: SQLWriter*
Observable 11 †	*Anomalous Host Activity: Windows Service Disabled: SstpSvc*
Observable 12 †	*Anomalous Host Activity: Windows Task Halted: mspub.exe*
Observable 13 †	*Anomalous Host Activity: Windows Task Halted: mydesktopqos.exe*
Observable 14 †	*Anomalous Host Activity: Windows Task Halted: mydesktopservice.exe*
Observable 15 †	*Presence of Anomalous Script: kill.bat*
Observable 16 †	*Anomalous Command-Line: net stop avpsus /y*
Observable 17 †	*Anomalous Command-Line: net stop McAfeeDLPAgentService /y*
Observable 18 †	*Anomalous Command-Line: net stop mfewc /y*
Observable 19 †	*Anomalous Command-Line: net stop BMR Boot Service /y*
Observable 20 †	*Anomalous Command-Line: net stop NetBackup BMR MTFTP Service /y*
Observable 21 †	*Anomalous Command-Line: sc config SQLTELEMETRY start= disabled*
Observable 22 †	*Anomalous Command-Line: sc config SQLTELEMETRY$ECWDB2 start= disabled*
Observable 23 †	*Anomalous Command-Line: sc config SQLWriter start= disabled*
Observable 24 †	*Anomalous Command-Line: sc config SstpSvc start= disabledig SQLWriter start= disabled*
Observable 25 †	*Anomalous Command-Line: taskkill /IM mspub.exe /F*
Observable 26 †	*Anomalous Command-Line: taskkill /IM mydesktopqos.exe /F*
Observable 27 †	*Anomalous Command-Line: taskkill /IM mydesktopservice.exe /F*

Observables Associated with Device Restart/Shutdown Technique (T0816)	
Observable 1 †	*Anomalous Host Activity: Host Shuts Down (Event ID)*

Observables Associated with Data Destruction Technique (T0809)	
Observable 1 †	*Presence of Anomalous Script: kill.bat*
Observable 2 †	*Anomalous Increase in System Resource Utilization: Increase in CPU Utilization*

Observables Associated with Data Destruction Technique (T0809)	
Observable 3 †	*Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity*
Observable 4 †	*Anomalous Command Line: vssadmin Delete Shadows /all /quiet*
Observable 5 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB*
Observable 6 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded*
Observable 7 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB*
Observable 8 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded*
Observable 9 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB*
Observable 10 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded*
Observable 11 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB*
Observable 12 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded*
Observable 13 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB*
Observable 14 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded*
Observable 15 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB*
Observable 16 †	*Anomalous Command Line: vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded*
Observable 17 †	*Anomalous Command Line: vssadmin Delete Shadows /all /quiet*
Observable 18 †	*Anomalous Command Line: del /s /f /q c:*.VHD c:*.bac c:*.bak c:*.wbcat c:*.bkf c:\Backup*.* c:\backup*.* c:*.set c:*.win c:*.dsk*
Observable 19 †	*Anomalous Command Line: del /s /f /q d:*.VHD d:*.bac d:*.bak d:*.wbcat d:*.bkf d:\Backup*.* d:\backup*.* d:*.set d:*.win d:*.dsk*
Observable 20 †	*Anomalous Command Line: del /s /f /q e:*.VHD e:*.bac e:*.bak e:*.wbcat e:*.bkf e:\Backup*.* e:\backup*.* e:*.set e:*.win e:*.dsk*
Observable 21 †	*Anomalous Command Line: del /s /f /q f:*.VHD f:*.bac f:*.bak f:*.wbcat f:*.bkf f:\Backup*.* f:\backup*.* f:*.set f:*.win f:*.dsk*
Observable 22 †	*Anomalous Command Line: del /s /f /q g:*.VHD g:*.bac g:*.bak g:*.wbcat g:*.bkf g:\Backup*.* g:\backup*.* g:*.set g:*.win g:*.dsk*
Observable 23 †	*Anomalous Command Line: del /s /f /q h:*.VHD h:*.bac h:*.bak h:*.wbcat h:*.bkf h:\Backup*.* h:\backup*.* h:*.set h:*.win h:*.dsk*
Observable 24 †	*Anomalous Command Line: del %0*
Observable 25 †	*Anomalous Deletion of Data: Deletion of Windows Shadow Volume*

Observables Associated with Data Destruction Technique (T0809)	
Observable 26 †	*Anomalous Modification of Files: .RYK appended to filenames*
Observable 27 †	*Anomalous Deletion of Files: With Extension: Virtual Hard Disk (.VHD)*
Observable 28 †	*Anomalous Deletion of Files: With Extension: Avantrix Backup Plus files (.bac)*
Observable 29 †	*Anomalous Deletion of Files: With Extension: backup copy (.bak)*
Observable 30 †	*Anomalous Deletion of Files: With Extension: Windows Backup Catalog File (.wbcat)*
Observable 31 †	*Anomalous Deletion of Files: With Extension: Windows Backup Utility File (.bfk)*
Observable 32 †	*Anomalous Deletion of Files: With Extension: setting files (.set)*
Observable 33 †	*Anomalous Deletion of Files: With Extension: Windows Backup File (.win)*
Observable 34 †	*Anomalous Deletion of Files: With Extension: Disk Images (.dsk)*
Observable 35 †	*Anomalous Deletion of Files: all folders that start with "Backup"*

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1 †	*Anomalous Host Activity: Windows Process Disabled: Excel.exe*
Observable 2 †	*Anomalous Host Activity: Windows Process Disabled: Firefoxconfig.exe*
Observable 3 †	*Anomalous Host Activity: Windows Process Disabled: Infopath.exe*
Observable 4 †	*Anomalous Host Activity: Windows Process Disabled: Isqlplussvc.exe*
Observable 5 †	*Anomalous Host Activity: Windows Process Disabled: Mspub.exe*
Observable 6 †	*Anomalous Host Activity: Windows Process Disabled: Mydesktopservice.exe*
Observable 7 †	*Anomalous Host Activity: Windows Process Disabled: Outlook.exe*
Observable 8 †	*Anomalous Host Activity: Windows Process Disabled: Powerpnt.exe*
Observable 9 †	*Anomalous Host Activity: Windows Process Disabled: Onenote.exe*
Observable 10 †	*Anomalous Host Activity: Windows Process Disabled: Oracle.exe*
Observable 11 †	*Anomalous Host Activity: Windows Process Disabled: Steam.exe*
Observable 12 †	*Anomalous Host Activity: Windows Process Disabled: Syntcime.exe*
Observable 13 †	*Anomalous Host Activity: Windows Process Disabled: Wordpard.exe*
Observable 14 †	*Anomalous Host Activity: Windows Process Disabled: Winword.exe*
Observable 15 †	*Anomalous Host Activity: Windows Process Disabled: Mbamtray.exe*

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1 †	*Anomalous Loss of Revenue: $67 Million*

APPENDIX B: ARTIFACTS LIBRARY

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

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

Artifacts Associated with User Execution Technique (T0863)	
Artifact 3	File Changes
Artifact 4	Increased Internet Control Message Protocol (ICMP) Traffic (Network Scanning)
Artifact 5	Network Traffic Changes
Artifact 6	Application Installation
Artifact 7	Network Connection Creation
Artifact 8	Application Log Content
Artifact 9	User Account Modification
Artifact 10	File Creation
Artifact 11	Process Creation
Artifact 12	System Log
Artifact 13	Process Termination
Artifact 14	File Execution
Artifact 15	Prefetch Files
Artifact 16	Registry Modification
Artifact 17	File Modifications
Artifact 18	File Renaming
Artifact 19	System Patches Installed
Artifact 20	Files Opening
Artifact 21	File Signature Validation
Artifact 22	Installers Created
Artifact 23	Application Log

Artifacts Associated with Drive-by Compromise Technique (T0817)	
Artifact 1	Destination IP Address
Artifact 2	Industrial Application Disk Write
Artifact 3	Industrial Application Process
Artifact 4	Website
Artifact 5	Transport Layer Security (TLS) Certificates
Artifact 6	Disk Write
Artifact 7	Disk Read
Artifact 8	Application Log
Artifact 9	File Creation
Artifact 10	Source IP Address
Artifact 11	POWERSHELL Log Creation

Artifacts Associated with Drive-by Compromise Technique (T0817)	
Artifact 12	POWERSHELL Cmdlet Open
Artifact 13	Dialog Boxes Open
Artifact 14	cmd.exe Application Start
Artifact 15	Memory Evidence
Artifact 16	HTTP Traffic
Artifact 17	Child Processes Created
Artifact 18	Process Ending
Artifact 19	Process Creation
Artifact 20	SMB Traffic
Artifact 21	HTTPS Traffic
Artifact 22	DNS Traffic
Artifact 23	.lnk Files
Artifact 24	Prefetch Files

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 Scripting Technique (T0853)	
Artifact 1	Startup Menu Modification
Artifact 2	OS Service Installation

Artifacts Associated with Scripting Technique (T0853)	
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 Dropped 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
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

Artifacts Associated with Native API Technique (T0834)	
Artifact 23	Device Live Data Changes
Artifact 24	Alter Process Logic
Artifact 25	Memory Corruption

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 1	Protocol Header Enumeration
Artifact 2	Protocol Content Enumeration
Artifact 3	Virtual Network Computing (VNC) Port 5900 Calls
Artifact 4	TCP ACK Scan
Artifact 5	TCP XMAS Scan
Artifact 6	Recurring Protocol SYN Traffic
Artifact 7	TCP FIN Scans
Artifact 8	Device Failure
Artifact 9	TCP Reverse Ident Scan
Artifact 10	Sequential Protocol SYN Traffic
Artifact 11	Scans Over Industrial Network Ports with Target IPs
Artifact 12	Industrial Network Traffic Content Containing Logical Identifiers
Artifact 13	SMTP Port 25 Traffic
Artifact 14	Device Reboot
Artifact 15	Bandwidth Degradation
Artifact 16	Host Recent Connection Logs
Artifact 17	IEC 101 Traffic to Serial Devices
Artifact 18	IEC 102
Artifact 19	IEC 104
Artifact 20	Open Platform Communications (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 Manufacturing Message Specification (MMS)
Artifact 27	Controller Proprietary Traffic
Artifact 28	Echo Type 8 Traffic
Artifact 29	ICMP Type 7 Traffic

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 30	Simple Network Management Protocol (SNMP) Port 162 Traffic
Artifact 31	SNMP Port 161 Traffic
Artifact 32	Address Resolution Protocol (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	Lightweight Directory Access Protocol (LDAP) Port
Artifact 39	Active Directory Calls
Artifact 40	Email Server Calls
Artifact 41	DNS Lookup Queries
Artifact 42	TCP Connect Scan
Artifact 43	Command Line Dialog Box Open

Artifacts Associated with 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

Artifacts Associated with Commonly Used Port Technique (T0885)	
Artifact 5	Unexpected Host Communicating with Common Port on Industrial Asset

Artifacts Associated with Command-Line Interface Technique (T0807)	
Artifact 1	Command Execution
Artifact 2	Application Log
Artifact 3	HTTP Traffic
Artifact 4	Telnet Traffic
Artifact 5	SSH Traffic
Artifact 6	VNC Traffic Port
Artifact 7	Process Creation
Artifact 8	Remote Connections
Artifact 9	Process Ending
Artifact 10	Script Execution
Artifact 11	User Account Logon
Artifact 12	User Account Privilege Change
Artifact 13	Logon Event
Artifact 14	Event Log Type
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 Lateral Tool Transfer Technique (T0867)	
Artifact 1	Remote Network Traffic
Artifact 2	File Metadata Changes
Artifact 3	User Information Changes
Artifact 4	Process Creation

Artifacts Associated with Lateral Tool Transfer Technique (T0867)	
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 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
Artifact 12	Application Log
Artifact 13	Domain Permission Requests
Artifact 14	Permission Elevation Requests

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 15	Application Use Times
Artifact 16	Configuration Changes

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

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

Artifacts Associated with Device Restart/Shutdown Technique (T0816)	
Artifact 1	Logon Events
Artifact 2	Process Alarm
Artifact 3	Memory Corruption
Artifact 4	Unauthorized Input

Artifacts Associated with Device Restart/Shutdown Technique (T0816)	
Artifact 5	Command Prompt Opened
Artifact 6	Hardware Failure
Artifact 7	Logoff Events
Artifact 8	Local Network Connections
Artifact 9	Significant Operational Data Changes
Artifact 10	Blue Screen
Artifact 11	Reboot Screen
Artifact 12	Network Command Packets
Artifact 13	Loss of Network Connection
Artifact 14	Process Environmental Changes
Artifact 15	Process Failure
Artifact 16	Process Application Event
Artifact 17	External Network Connections

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	Trivial File Transfer Protocol (TFTP) Port
Artifact 12	SFTP Port
Artifact 13	Memory Corruption
Artifact 14	Use of File Transfer Protocols
Artifact 15	Secure Copy Protocol (SCP) Port
Artifact 16	File Encryptions
Artifact 17	Non-Native Files
Artifact 18	External Network Connections
Artifact 19	Transient Device Connections

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 20	Program Execution
Artifact 21	Telnet Port
Artifact 22	FTPS Port
Artifact 23	HTTP Port
Artifact 24	HTTPS Port
Artifact 25	Local Network Connections
Artifact 26	FTP Port
Artifact 27	SMB Port

Artifacts Associated with Loss of Availability Technique (T0826)	
Artifact 1	Process Failure Due to Loss of Required Network or System Dependency
Artifact 2	Unexplained Loss of User Data
Artifact 3	Changes In Network Routing or Usage of Redundant Control System Network Connection Due to Failed Network Path
Artifact 4	Significant Reduction or Increase in Network Traffic Due to Malware Propagation of Disappearance of Services
Artifact 5	Significant Logged Usage of Native Crypto Functions or Presence of Import of Crypto Functions in Binaries
Artifact 6	Operator or User Discovery of Encrypted or Inoperable Systems
Artifact 7	File System Modification Artifacts Might Be Associated with the Loss of Availability Might Be Present on Disk
Artifact 8	Unexplained Loss of Application Data

Artifacts Associated with Loss of Productivity and Revenue Technique (T0828)	
Artifact 1	Loss of Confidence in a Safety System Due to Unreliability Might Result in a Risk Management Driven Shutdown of a Plant
Artifact 2	Wormable or Other Highly Propagating Malware Might Result in the Shutdown of a Plant to Prevent Ransomware or Other Destructive Attacks
Artifact 3	Extortion Attempts Might Lead to Reduced Operations Due to Potential Presence of Malicious Attackers
Artifact 4	Loss of Control of Critical Systems Due to Ransomware or Loss of Confidence Might Lead to a Degraded Productivity or Revenue Operating State
Artifact 5	File System Modification Artifacts Might Be Associated with the Loss of Productivity and Revenue Attack Might Be Present on Disk

APPENDIX C: OBSERVERS

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

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

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

Operational Technology (OT) Cybersecurity
- OT Security
- ICS/SCADA Security

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

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

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

Information Technology (IT) Staff
- Networking and Infrastructure
- Host Administrator
- Database Administrator
- Application Development
- ERP/MES Administrator
- IT Management

REFERENCES

[1] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[2] [BleepingComputer | Sergiu Gatlan | "Universal Health Services lost $67 million due to Ryuk ransomware attack" | https://www.bleepingcomputer.com/news/security/universal-health-services-lost-67-million-due-to-ryuk-ransomware-attack/ | 1 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[3] [BleepingComputer | Sergiu Gatlan | "Universal Health Services lost $67 million due to Ryuk ransomware attack" | https://www.bleepingcomputer.com/news/security/universal-health-services-lost-67-million-due-to-ryuk-ransomware-attack/ | 1 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[4] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[5] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[6] [Cybersecurity & Infrastructure Security Agency | "Alert (AA21-076A)" | https://www.cisa.gov/uscert/ncas/alerts/aa21-076a | 17 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[7] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[8] [Cybersecurity & Infrastructure Security Agency | "Alert (AA21-076A)" | https://www.cisa.gov/uscert/ncas/alerts/aa21-076a | 17 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[9] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[10] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[11] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[12] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[13] [BleepingComputer | Sergiu Gatlan | "Universal Health Services lost $67 million due to Ryuk ransomware attack" | https://www.bleepingcomputer.com/news/security/universal-health-services-lost-67-million-due-to-ryuk-ransomware-attack/ | 1 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[14] [BleepingComputer | Sergiu Gatlan | "Universal Health Services lost $67 million due to Ryuk ransomware attack" | https://www.bleepingcomputer.com/news/security/universal-health-services-lost-67-million-due-to-ryuk-ransomware-attack/ | 1 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[15] [Sophos | Sean Gallagher | "They're back: inside a new Ryuk ransomware attack" | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[16] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[17] [Sophos | Sean Gallagher | "They're back: inside a new Ryuk ransomware attack" | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[18] [Sophos | Sean Gallagher | "They're back: inside a new Ryuk ransomware attack" | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[19] [Sophos | Sean Gallagher | "They're back: inside a new Ryuk ransomware attack" | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification marking]

[20] [The DIFR Report | "Ryuk Speed Run, 2 Hours to Ransom" | https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/ | 5 November 2020 | The source is publicly available information and does not contain classification markings]

[21] [Sophos | Sean Gallagher | "They're back: inside a new Ryuk ransomware attack" | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[22] [Sophos | Sean Gallagher | "They're back: inside a new Ryuk ransomware attack" | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[23] [Sophos | Sean Gallagher | "They're back: inside a new Ryuk ransomware attack" | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[24] [Cybersecurity & Infrastructure Security Agency | "Ransomware Activity Targeting the Healthcare and Public Health Sector" |https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a | 17 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[25] [GAP Mobilize| John Browne | "Ransomware hack: what we can learn about VB6" | https://www.mobilize.net/blog/ransomware-hack-what-we-can-learn-about-vb6 | 17 May 2017 | Accessed on 20 January 2023 | The source is publicly available information and does not contain classification markings]

[26] [Sophos | Sean Gallagher | “They’re back: inside a new Ryuk ransomware attack” | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[27] [Sophos | Sean Gallagher | “They’re back: inside a new Ryuk ransomware attack” | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[28] [Sophos | Sean Gallagher | “They’re back: inside a new Ryuk ransomware attack” | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[29] [Cybersecurity & Infrastructure Security Agency | “Alert (AA21-076A)” | https://www.cisa.gov/uscert/ncas/alerts/aa21-076a | 17 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[30] [Sophos | Sean Gallagher | “They’re back: inside a new Ryuk ransomware attack” | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[31] [The DIFR Report | “Ryuk Speed Run, 2 Hours to Ransom” | https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/ | 5 November 2020 | The source is publicly available information and does not contain classification markings]

[32] [The DIFR Report | “Ryuk Speed Run, 2 Hours to Ransom” | https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/ | 5 November 2020 | The source is publicly available information and does not contain classification markings]

[33] [Sophos | Sean Gallagher | “They’re back: inside a new Ryuk ransomware attack” | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[34] [Sophos | Sean Gallagher | “They’re back: inside a new Ryuk ransomware attack” | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[35] [Sophos | Sean Gallagher | “They’re back: inside a new Ryuk ransomware attack” | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[36] [Sophos | Sean Gallagher | “They’re back: inside a new Ryuk ransomware attack” | https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[37] [TrendMicro | “What Is RYUK Ransomware?” | https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html | 18 June 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[38] [Tech-Refresh | Bryan Macrario | “Universal Health Services Ryuk Ransomware Attack” | https://tec-refresh.com/uhs-ryuk-ransomware-attack/ | 18 June 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[39] [Sophos | Sean Gallagher | “They’re back: inside a new Ryuk ransomware attack”| https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 |

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

[40] [The DIFR Report | "Ryuk Speed Run, 2 Hours to Ransom" | https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/ | 5 November 2020 | The source is publicly available information and does not contain classification markings]

[41] [The DIFR Report | "Ryuk Speed Run, 2 Hours to Ransom" | https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/ | 5 November 2020 | The source is publicly available information and does not contain classification markings]

[42] [Sophos | Sean Gallagher | "They're back: inside a new Ryuk ransomware attack"| https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[43] [Sophos | Sean Gallagher | "They're back: inside a new Ryuk ransomware attack"| https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/ | 14 October 2020 | Accessed on 20 November 2022 | The source is publicly available information and does not contain classification markings]

[44] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[45] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[46] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[47] [Fierce Healthcare | Heather Landi | "UHS hit with massive cyberattack as hospitals reportedly divert surgeries, ambulances" | https://www.fiercehealthcare.com/tech/uhs-hit-massive-cyber-attack-as-hospitals-divert-surgeries-ambulances | 28 September 2020 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[48] [BleepingComputer | Sergiu Gatlan | "Universal Health Services lost $67 million due to Ryuk ransomware attack" | https://www.bleepingcomputer.com/news/security/universal-health-services-lost-67-million-due-to-ryuk-ransomware-attack/ | 1 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[49] [CSO Online | Lucian Constantin | "Ryuk explained: Targeted, devastatingly effective ransomware" | https://www.csoonline.com/article/3541810/ryuk-explained-targeted-devastatingly-effective-ransomware.html | 19 March 2021 | The source is publicly available information and does not contain classification markings]

[50] [Cybersecurity & Infrastructure Security Agency | "Alert (AA21-076A)" | https://www.cisa.gov/uscert/ncas/alerts/aa21-076a | 17 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[51] [BleepingComputer | Sergiu Gatlan | "Universal Health Services lost $67 million due to Ryuk ransomware attack" | https://www.bleepingcomputer.com/news/security/universal-health-services-lost-67-million-due-to-ryuk-ransomware-attack/ | 1 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]

[52] [BleepingComputer | Sergiu Gatlan | "Universal Health Services lost $67 million due to Ryuk ransomware attack" | https://www.bleepingcomputer.com/news/security/universal-health-services-lost-67-million-due-to-ryuk-ransomware-attack/ | 1 March 2021 | Accessed on 30 September 2022 | The source is publicly available information and does not contain classification markings]