



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

Cybersecurity for the Operational Technology  
Environment (CyOTE)

**31 MARCH 2023**



U.S. DEPARTMENT OF  
**ENERGY**

*Office of*  
**Cybersecurity, Energy Security,  
and Emergency Response**

INL/RPT-23-71881

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

This *paper* is the product of *research* conducted by the Cybersecurity for the Operational Technology Environment (CyOTE) program and was funded by the Department of Energy Office of Cybersecurity, Energy Security and Emergency Response (DOE CESER). No updates have been made since the date of publication and no further funding has been approved.

## TABLE OF CONTENTS

<b>1. EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>2. INTRODUCTION .....</b>	<b>2</b>
2.1. APPLYING THE CYOTE METHODOLOGY .....	2
2.2. BACKGROUND ON THE ATTACK .....	4
<b>3. OBSERVABLE AND TECHNIQUE ANALYSIS .....</b>	<b>7</b>
3.1. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS .....	7
3.2. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION .....	8
3.3. DRIVE-BY COMPROMISE TECHNIQUE (T0817) FOR INITIAL ACCESS .....	9
3.4. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION .....	10
3.5. MASQUERADING TECHNIQUE (T0849) FOR EVASION .....	11
3.6. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION .....	12
3.7. NATIVE API TECHNIQUE (T0834) FOR EXECUTION .....	13
3.8. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY .....	14
3.9. STANDARD APPLICATION LAYER PROTOCOL TECHNIQUE (T0869) FOR COMMAND AND CONTROL .....	15
3.10. COMMONLY USED PORTS TECHNIQUE (T0885) FOR COMMAND AND CONTROL .....	16
3.11. COMMAND-LINE INTERFACE TECHNIQUE (T0807) FOR EXECUTION .....	17
3.12. LATERAL TOOL TRANSFER TECHNIQUE (T0867) FOR LATERAL MOVEMENT .....	18
3.13. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE .....	19
3.14. REMOTE SYSTEM INFORMATION DISCOVERY TECHNIQUE (T0888) FOR DISCOVERY .....	20
3.15. SERVICE STOP TECHNIQUE (T0881) FOR INHIBIT RESPONSE FUNCTION .....	21
3.16. DEVICE SHUTDOWN/RESTART TECHNIQUE (T0816) FOR INHIBIT RESPONSE FUNCTION .....	22
3.17. DATA DESTRUCTION TECHNIQUE (T0809) FOR INHIBIT RESPONSE FUNCTION .....	23
3.18. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT .....	24
3.19. LOSS OF PRODUCTIVITY AND REVENUE TECHNIQUE (T0828) FOR IMPACT .....	25
<b>APPENDIX A: OBSERVABLES LIBRARY .....</b>	<b>27</b>
<b>APPENDIX B: ARTIFACTS LIBRARY .....</b>	<b>37</b>
<b>APPENDIX C: OBSERVERS .....</b>	<b>48</b>
<b>REFERENCES .....</b>	<b>49</b>

## FIGURES

<b>FIGURE 1. CYOTE METHODOLOGY .....</b>	<b>2</b>
<b>FIGURE 2. INTRUSION TIMELINE .....</b>	<b>4</b>
<b>FIGURE 3. ATTACK GRAPH .....</b>	<b>26</b>

## TABLES

<b>TABLE 1. TECHNIQUES USED IN THE RYUK RANSOMWARE ATTACK ON UNIVERSAL HEALTH SERVICES 2020 CYBER ATTACK .....</b>	<b>6</b>
<b>TABLE 2. PRECURSOR ANALYSIS REPORT QUANTITATIVE SUMMARY .....</b>	<b>6</b>

# 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.<sup>1</sup> 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.<sup>2</sup> 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.<sup>3</sup>

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.

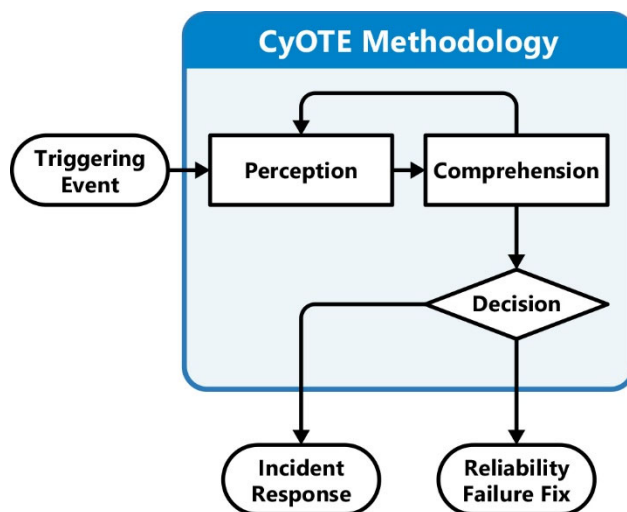
The information gathered in this report contributes to a library of observables tied to a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack. Asset owners and operators can use these products 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.<sup>4</sup> 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.<sup>5</sup>

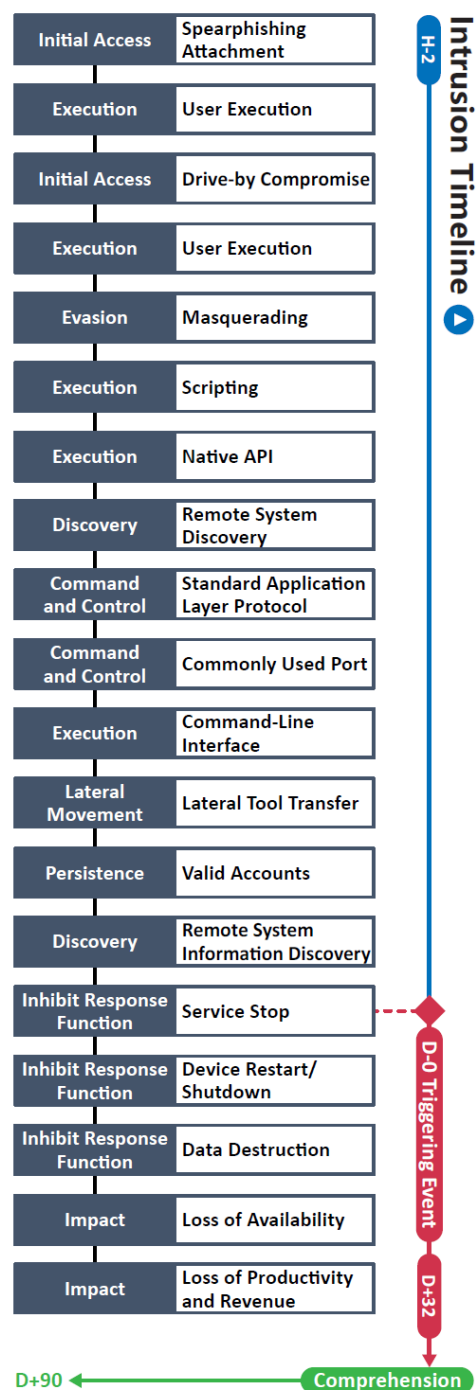
The adversaries most likely gained initial access through a spearphishing email, although specifically when this occurred is not known from available information. UHS employees observed adversaries disabling multiple antivirus programs and actively accessing hard drives prior to the loss of availability of critical information (H-2).<sup>a</sup> 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.<sup>6</sup>

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

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.<sup>7</sup>

Employees lost access to vital internet-dependent systems, including patient information and diagnostics.<sup>8</sup> 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.<sup>9</sup> Once the IT team noticed the activity, they took all systems offline to prevent further damage and propagation of the malware.<sup>10</sup>

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



**Figure 2. Intrusion Timeline**

<sup>a</sup> “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.

restored, and normal operations were resuming.<sup>11</sup> During this time, facilities utilized established back-up processes, including offline documentation methods, to continue patient care.<sup>12</sup> 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.<sup>13</sup>

Analysis identified 18 unique techniques in a sequence and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.



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

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

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

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

### 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.<sup>14</sup> 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.<sup>15</sup>

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.<sup>16</sup> 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	
<b>Artifacts</b> (See Appendix B)	A total of 29 artifacts could be generated by the Spearphishing Attachment technique
<b>Technique Observers<sup>b</sup></b>	IT Staff, IT Cybersecurity, Support Staff, Management

<sup>b</sup> 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.<sup>17</sup>

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	
<b>Artifacts (See Appendix B)</b>	A total of 23 artifacts could be generated by the User Execution technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity, Engineering, Support Staff, Management

### 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.<sup>18</sup> 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.<sup>19</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of 24 artifacts could be generated by the Drive-by Compromise technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity, Support Staff, Management

### 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.<sup>20</sup> 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.<sup>21</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of 23 artifacts could be generated by the User Execution technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity, Engineering, Support Staff, Management

### 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.<sup>22</sup> 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.<sup>23</sup>

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.<sup>24</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of 15 artifacts could be generated by the Masquerading technique
<b>Technique Observers</b>	IT Cybersecurity

### 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.<sup>25</sup> Later in the intrusion, adversaries often use Cobalt Strike, a popular penetration testing tool to executed batch scripts and network discovery commands.<sup>26</sup> Adversaries then utilize scripting to send a list of commands, eventually gaining administrative credentials and access to the domain controller.<sup>27</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of 12 artifacts could be generated by the Scripting technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity

### 3.7. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

Multiple native application programming interfaces (APIs) are utilized throughout the attack. These include 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.<sup>28</sup>

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.<sup>29</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of 25 artifacts could be generated by the Native API technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity



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.<sup>30</sup> 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.<sup>31</sup>

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 (See Appendix B)	A total of 43 artifacts could be generated by the Remote System Discovery technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity

### 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.<sup>32</sup> 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.<sup>33</sup>

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.<sup>34</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of 12 artifacts could be generated by the Standard Application Layer Protocol technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity

### 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.<sup>35</sup> 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	
<b>Artifacts</b> (See Appendix B)	A total of five artifacts could be generated by the Commonly Used Ports technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity

### 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.<sup>36</sup> 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.<sup>37</sup> Finally, adversaries may have used the command line to remotely generate malicious Service User Accounts.<sup>38</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of 25 artifacts could be generated by the Command Line Interface technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity

### 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.<sup>39,c</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of 22 artifacts could be generated by the Lateral Tool Transfer technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity

---

<sup>c</sup> 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.<sup>40</sup> 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.<sup>41</sup>

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 (See Appendix B)	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering

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.<sup>42</sup> 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.<sup>43</sup> 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 with detailed information about target devices, allowing them to attack with enhanced specificity. This technique appears near the middle of the timeline and responding to it will prevent adversaries from properly identifying intended target devices. Terminating the chain of techniques at this point would limit data exfiltration and possibly operational damage.

Of the 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 (See Appendix B)	A total of eight artifacts could be generated by the Remote System Information Discovery technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity

### 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.<sup>44</sup> 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.<sup>45</sup>

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.<sup>46</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of 13 artifacts could be generated by the Service Stop technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Support Staff, Management



### 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.<sup>47</sup> 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.<sup>48</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of 17 artifacts could be generated by the Device Shutdown/Restart technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management

### 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	
<b>Artifacts</b> (See Appendix B)	A total of 27 artifacts could be generated by the Data Destruction technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management

### 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.<sup>49</sup> 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.<sup>50</sup> 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	
<b>Artifacts</b> (See Appendix B)	A total of eight artifacts could be generated by the Loss of Availability technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity, Support Staff, Management

### 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.<sup>51</sup>

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.<sup>52</sup>

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	
<b>Artifacts</b> (See Appendix B)	A total of five artifacts could be generated by the Loss of Productivity and Revenue technique
<b>Technique Observers</b>	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management

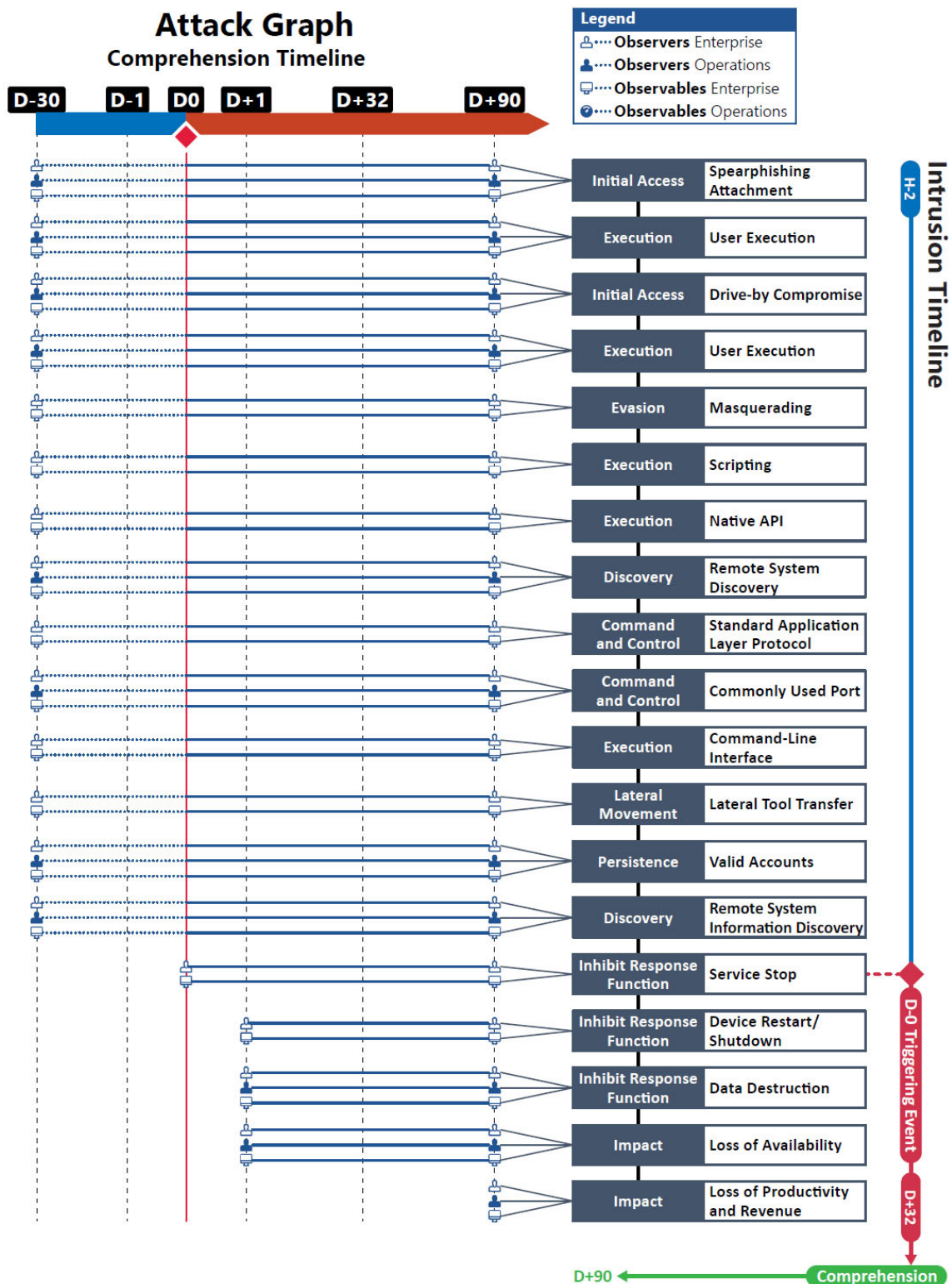


Figure 3. Attack Graph

## APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †.

Observables Associated with Spearphishing Attachment Technique (T0865)	
<b>Observable 1 †</b>	<i>Presence of Anomalous Email Containing a Web Link: Google Drive: docs.google.com</i>
<b>Observable 2 †</b>	<i>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</i>
<b>Observable 3</b>	<i>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</i>
<b>Observable 4 †</b>	<i>Anomalous Network Traffic: From Local Host to External Server: Domain Name System (DNS) Over Transmission Control Protocol (TCP) Port 53: docs.google.com</i>

Observables Associated with User Execution Technique (T0863)	
<b>Observable 1 †</b>	<i>Presence of Anomalous Email Containing a Web Link: Google Drive: docs.google.com</i>
<b>Observable 2 †</b>	<i>User Interaction with Anomalous Web Link: Google Drive: docs.google.com</i>
<b>Observable 3 †</b>	<i>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</i>
<b>Observable 4</b>	<i>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</i>
<b>Observable 5 †</b>	<i>Anomalous Network Traffic: From Local Host to External Server: Domain Name System (DNS) Over Transmission Control Protocol (TCP) Port 53: docs.google.com</i>
<b>Observable 6 †</b>	<i>Presence of Anomalous Email Containing a Web Link: Google Drive: docs.google.com</i>
<b>Observable 7 †</b>	<i>User Interaction with Anomalous Web Link</i>

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

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

Observables Associated with User Execution Technique (T0863)	
<b>Observable 1 †</b>	<i>User Interaction with Anomalous Web Link: Google Drive: docs.google.com</i>

Observables Associated with Masquerading Technique (T0849)	
<b>Observable 1 †</b>	<i>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</i>
<b>Observable 2 †</b>	<i>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</i>
<b>Observable 3</b>	<i>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</i>
<b>Observable 4 †</b>	<i>Anomalous Binary on Local Host: Dynamic Link Libraries (.DLL):</i>
<b>Observable 5 †</b>	<i>Anomalous Binary on Local Host: Rich Text Files (.RTF):</i>

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



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

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

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
<b>Observable 1 †</b>	<i>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</i>
<b>Observable 2 †</b>	<i>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</i>



Observables Associated with Standard Application Layer Protocol Technique (T0869)	
<b>Observable 3</b>	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 Commonly Used Ports Technique (T0855)	
<b>Observable 1 †</b>	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
<b>Observable 2 †</b>	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
<b>Observable 3</b>	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)	
<b>Observable 1 †</b>	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
<b>Observable 2 †</b>	Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C net group "enterprise admins" /domain
<b>Observable 3 †</b>	Anomalous Command Line: C:\WINDOWS\system32\net1 group "domain admins" /domain
<b>Observable 4 †</b>	Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C net localgroup administrators
<b>Observable 5 †</b>	Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C ipconfig
<b>Observable 6 †</b>	Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C nltest /dclist:[target company domain name]
<b>Observable 7 †</b>	Anomalous Command Line: C:\WINDOWS\system32\cmd.exe /C nltest /dclist:[target company name]
<b>Observable 8 †</b>	Presence of Anomalous Binary on Host: print_document.exe
<b>Observable 9 †</b>	Execution of Anomalous Binary on Host: print_document.exe

Observables Associated with Lateral Tool Transfer Technique (T0867)	
<b>Observable 1 †</b>	Presence of Anomalous Binary on Host: qipozincyusury.exe
<b>Observable 2 †</b>	Anomalous Network Traffic: From Local Host to External IP: Over HyperText Transfer Protocol (HTTP) Transmission Control Protocol (TCP) Port 80: HTTP GET Request

Observables Associated with Lateral Tool Transfer Technique (T0867)	
<b>Observable 3</b>	Anomalous Network Traffic: From Local Host to External IP: Over HyperText Transfer Secure Protocol (HTTPS) Transmission Control Protocol (TCP) Port 443: HTTPS GET Request
<b>Observable 4</b>	Anomalous Network Traffic: From Local Host to External IP: Over File Transfer Protocol (FTP) Transmission Control Protocol (TCP) Port 22
<b>Observable 5</b>	Anomalous Network Traffic: From Local Host to External IP: Over Secure File Transfer Protocol (SFTP) Transmission Control Protocol (TCP) Port 23
<b>Observable 6 †</b>	<i>Anomalous Network Traffic: From Local Host to External IP: Via Rclone Application</i>
<b>Observable 7 †</b>	<i>Anomalous Network Traffic: From Local Host to External IP: Over Transmission Control Protocol (TCP) Port 445</i>
<b>Observable 8 †</b>	<i>Anomalous Network Traffic: From External IP to Local Host: Over HyperText Transfer Protocol (HTTP) Transmission Control Protocol (TCP) Port 80: HTTP POST Request</i>
<b>Observable 9</b>	Anomalous Network Traffic: From External IP to Local Host: Over HyperText Transfer Secure Protocol (HTTPS) Transmission Control Protocol (TCP) Port 443: HTTPS POST Request
<b>Observable 10</b>	Anomalous Network Traffic: From External IP to Local Host: Over File Transfer Protocol (FTP) Transmission Control Protocol (TCP) Port 22
<b>Observable 11</b>	Anomalous Network Traffic: From External IP to Local Host: Over Secure File Transfer Protocol (SFTP) Transmission Control Protocol (TCP) Port 23
<b>Observable 12 †</b>	<i>Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) Transmission Control Protocol (TCP) Port 445</i>
<b>Observable 13 †</b>	<i>Anomalous Command Line: rclone copy &lt;source:sourcepath&gt; &lt;dest:destpath&gt;</i>
<b>Observable 14 †</b>	<i>Anomalous Command Line: mega-export -a &lt;Local Host File Path&gt; &lt;Remote Host File Path&gt;</i>
<b>Observable 15 †</b>	<i>Anomalous Command Line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</i>
<b>Observable 16 †</b>	<i>Anomalous Binary on Local Host: rclone.exe</i>
<b>Observable 17 †</b>	<i>Anomalous Binary on Local Host: MEGAcmdShell.exe</i>
<b>Observable 18 †</b>	<i>Anomalous Binary on Local Host: empire.exe</i>
<b>Observable 19 †</b>	<i>Anomalous Binary on Local Host: koadic.exe</i>
<b>Observable 20 †</b>	<i>Execution of Anomalous Binary on Host: rclone.exe</i>
<b>Observable 21 †</b>	<i>Execution of Anomalous Binary on Host: MEGAcmdShell.exe</i>
<b>Observable 22 †</b>	<i>Execution of Anomalous Binary on Host: empire.exe</i>
<b>Observable 23 †</b>	<i>Execution of Anomalous Binary on Host: koadic.exe</i>

Observables Associated with Valid Accounts Technique (T0859)	
<b>Observable 1 †</b>	<i>Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) Transmission Control Protocol (TCP) Port 445</i>

Observables Associated with Valid Accounts Technique (T0859)	
<b>Observable 2 †</b>	<i>Anomalous Network Traffic: From External IP to Local Host: Over Remote Desktop Protocol (RDP) Transmission Control Protocol (TCP) Port 3389</i>
<b>Observable 3 †</b>	<i>Anomalous Host Activity: Successful Logon from External Host: An Account Was Successfully Logged On (Windows Event ID 4624): Anomalous Timestamp</i>
<b>Observable 4 †</b>	<i>Anomalous Host Activity: Successful Logon from External Host: An Account Was Successfully Logged On (Windows Event ID 4624): Anomalous Remote IP</i>
<b>Observable 5 †</b>	<i>Anomalous Host Activity: Increase in Failed Login Attempts: An Account Failed to Log On (Windows Event ID 4625): Anomalous Timestamp</i>
<b>Observable 6 †</b>	<i>Anomalous Host Activity: Increase in Failed Login Attempts: An Account Failed to Log On (Windows Event ID 4625): Anomalous Remote IP</i>

Observables Associated with Remote System Information Discovery Technique (T0888)	
<b>Observable 1 †</b>	<i>Anomalous Network Traffic: From External IP to Local Host: Over Server Message Block (SMB) Transmission Control Protocol (TCP) Port 445</i>
<b>Observable 2 †</b>	<i>Anomalous Network Traffic: From External IP to Local Host: Over Remote Desktop Protocol (RDP) Transmission Control Protocol (TCP) Port 3389</i>
<b>Observable 3</b>	<i>Presence of Anomalous File on Host: Anomalous Comma Separated Value (CSV) file: ALLWindows.csv</i>
<b>Observable 4 †</b>	<i>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 -NoTypeInfo -Encoding UTF8</i>
<b>Observable 5</b>	<i>Anomalous Command-Line: adfind.exe -f "(objectcategory=person)"</i>
<b>Observable 6</b>	<i>Anomalous Command-Line: adfind.exe -f "objectcategory=computer"</i>
<b>Observable 7</b>	<i>Anomalous Command-Line: adfind.exe -f "(objectcategory=organizationalUnit)"</i>
<b>Observable 8</b>	<i>Anomalous Command-Line: adfind.exe -sc trustdmp</i>
<b>Observable 9</b>	<i>Anomalous Command-Line: adfind.exe -subnets -f (objectCategory=subnet)</i>
<b>Observable 10</b>	<i>Anomalous Command-Line: adfind.exe -f "(objectcategory=group)"</i>
<b>Observable 11</b>	<i>Anomalous Command-Line: adfind.exe -gcb -sc trustdmpobjectcategory=group)"</i>
<b>Observable 12 †</b>	<i>Anomalous Command-Line: nltest /domain_trusts /all_trusts</i>
<b>Observable 13 †</b>	<i>Presence of Anomalous Binary: C:\Windows\Temp\adf\AdFind.exe</i>
<b>Observable 14 †</b>	<i>Presence of Anomalous Script: C:\Windows\Temp\adf\adf.bat</i>
<b>Observable 15 †</b>	<i>Execution of Anomalous Binary: C:\Windows\Temp\adf\AdFind.exe</i>
<b>Observable 16 †</b>	<i>Execution of Anomalous Script: C:\Windows\Temp\adf\adf.bat</i>

Observables Associated with Service Stop Technique (T0881)	
<b>Observable 1 †</b>	<i>Anomalous Host Activity: Windows Service Stop (Event ID 6006)</i>

Observables Associated with Service Stop Technique (T0881)	
Observable 2 †	Anomalous Host Activity: Windows Service Stopped: avpsus
Observable 3 †	Anomalous Host Activity: Windows Service Stopped: McAfeeDLPAgentService
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 †	<i>Presence of Anomalous Script: kill.bat</i>
Observable 2 †	<i>Anomalous Increase in System Resource Utilization: Increase in CPU Utilization</i>
Observable 3 †	<i>Anomalous Increase in System Resource Utilization: Increase in Hard Drive Activity</i>
Observable 4 †	<i>Anomalous Command Line: vssadmin Delete Shadows /all /quiet</i>
Observable 5 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB</i>
Observable 6 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded</i>
Observable 7 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB</i>
Observable 8 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded</i>
Observable 9 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB</i>
Observable 10 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded</i>
Observable 11 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB</i>
Observable 12 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded</i>
Observable 13 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB</i>
Observable 14 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded</i>
Observable 15 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB</i>
Observable 16 †	<i>Anomalous Command Line: vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded</i>
Observable 17 †	<i>Anomalous Command Line: vssadmin Delete Shadows /all /quiet</i>
Observable 18 †	<i>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</i>
Observable 19 †	<i>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</i>
Observable 20 †	<i>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</i>
Observable 21 †	<i>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</i>
Observable 22 †	<i>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</i>

Observables Associated with Data Destruction Technique (T0809)	
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
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 (.bkf)
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 †	<i>Anomalous Loss of Revenue: \$67 Million</i>



## APPENDIX B: ARTIFACTS LIBRARY

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

Artifacts Associated with User Execution Technique (T0863)	
<b>Artifact 1</b>	Command Execution
<b>Artifact 2</b>	Service Termination



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

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

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

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

Artifacts Associated with Scripting Technique (T0853)	
<b>Artifact 1</b>	Startup Menu Modification
<b>Artifact 2</b>	OS Service Installation

Artifacts Associated with Scripting Technique (T0853)	
<b>Artifact 3</b>	Registry Modifications
<b>Artifact 4</b>	Network Services Created
<b>Artifact 5</b>	External Network Connections
<b>Artifact 6</b>	Prefetch Files Created
<b>Artifact 7</b>	Executable Files
<b>Artifact 8</b>	System Processes Created
<b>Artifact 9</b>	OS Timeline Event
<b>Artifact 10</b>	System Event Log Creation
<b>Artifact 11</b>	Files Dropped into Directory
<b>Artifact 12</b>	Windows API Event Log

Artifacts Associated with Native API Technique (T0834)	
<b>Artifact 1</b>	Alert Generated
<b>Artifact 2</b>	System Resource Usage Management Changes
<b>Artifact 3</b>	.dll Modifications
<b>Artifact 4</b>	Imports Hash Changed
<b>Artifact 5</b>	Files Created
<b>Artifact 6</b>	Processes Initiated
<b>Artifact 7</b>	Services Initiated
<b>Artifact 8</b>	SYSMON Events Created
<b>Artifact 9</b>	Performance Degradation
<b>Artifact 10</b>	Blue Screen
<b>Artifact 11</b>	Configuration Change
<b>Artifact 12</b>	Command Execution
<b>Artifact 13</b>	Industrial Protocol Command Packet
<b>Artifact 14</b>	Host Device Failure
<b>Artifact 15</b>	Industrial Network Traffic
<b>Artifact 16</b>	Device Reads
<b>Artifact 17</b>	Device I/O Image Table Manipulated
<b>Artifact 18</b>	Device Failure
<b>Artifact 19</b>	Systems Calls
<b>Artifact 20</b>	Device Performance Degradation
<b>Artifact 21</b>	Device Memory Modification
<b>Artifact 22</b>	Device Alarm

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

Artifacts Associated with Remote System Discovery Technique (T0846)	
<b>Artifact 1</b>	Protocol Header Enumeration
<b>Artifact 2</b>	Protocol Content Enumeration
<b>Artifact 3</b>	Virtual Network Computing (VNC) Port 5900 Calls
<b>Artifact 4</b>	TCP ACK Scan
<b>Artifact 5</b>	TCP XMAS Scan
<b>Artifact 6</b>	Recurring Protocol SYN Traffic
<b>Artifact 7</b>	TCP FIN Scans
<b>Artifact 8</b>	Device Failure
<b>Artifact 9</b>	TCP Reverse Ident Scan
<b>Artifact 10</b>	Sequential Protocol SYN Traffic
<b>Artifact 11</b>	Scans Over Industrial Network Ports with Target IPs
<b>Artifact 12</b>	Industrial Network Traffic Content Containing Logical Identifiers
<b>Artifact 13</b>	SMTP Port 25 Traffic
<b>Artifact 14</b>	Device Reboot
<b>Artifact 15</b>	Bandwidth Degradation
<b>Artifact 16</b>	Host Recent Connection Logs
<b>Artifact 17</b>	IEC 101 Traffic to Serial Devices
<b>Artifact 18</b>	IEC 102
<b>Artifact 19</b>	IEC 104
<b>Artifact 20</b>	Open Platform Communications (OPC) Network Traffic
<b>Artifact 21</b>	Statistical Anomalies in Network Traffic
<b>Artifact 22</b>	DNS Port 53 Zone Transfers
<b>Artifact 23</b>	Industrial Network Traffic
<b>Artifact 24</b>	Common Network Traffic
<b>Artifact 25</b>	IEC 103 Traffic (For North America)
<b>Artifact 26</b>	IEC 61850 Manufacturing Message Specification (MMS)
<b>Artifact 27</b>	Controller Proprietary Traffic
<b>Artifact 28</b>	Echo Type 8 Traffic
<b>Artifact 29</b>	ICMP Type 7 Traffic

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

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

Artifacts Associated with Commonly Used Port Technique (T0885)	
<b>Artifact 1</b>	Unexpected Process Usage of Common Port Observed via Firewall Logs
<b>Artifact 2</b>	Unexpected Process Usage of Common Port Observed via OS Commands (netstat)
<b>Artifact 3</b>	Unexpected Process Usage of Common Port Observed via Memory

Artifacts Associated with Commonly Used Port Technique (T0885)	
<b>Artifact 4</b>	Unexpected Process Usage of Common Port Observed via OS Logs
<b>Artifact 5</b>	Unexpected Host Communicating with Common Port on Industrial Asset

Artifacts Associated with Command-Line Interface Technique (T0807)	
<b>Artifact 1</b>	Command Execution
<b>Artifact 2</b>	Application Log
<b>Artifact 3</b>	HTTP Traffic
<b>Artifact 4</b>	Telnet Traffic
<b>Artifact 5</b>	SSH Traffic
<b>Artifact 6</b>	VNC Traffic Port
<b>Artifact 7</b>	Process Creation
<b>Artifact 8</b>	Remote Connections
<b>Artifact 9</b>	Process Ending
<b>Artifact 10</b>	Script Execution
<b>Artifact 11</b>	User Account Logon
<b>Artifact 12</b>	User Account Privilege Change
<b>Artifact 13</b>	Logon Event
<b>Artifact 14</b>	Event Log Type
<b>Artifact 15</b>	Event Log Type
<b>Artifact 16</b>	Failed Logon Event
<b>Artifact 17</b>	Command Line Memory Data
<b>Artifact 18</b>	cmd.exe Application Execution
<b>Artifact 19</b>	RDP Traffic
<b>Artifact 20</b>	Industrial Application Execution
<b>Artifact 21</b>	POWERSHELL Cmdlet Application Execution
<b>Artifact 22</b>	Event ID 4103 POWERSHELL Command
<b>Artifact 23</b>	Event ID 4688 Command Line Execution
<b>Artifact 24</b>	NTUSER Application Execution Entries
<b>Artifact 25</b>	External Network Connection

Artifacts Associated with Lateral Tool Transfer Technique (T0867)	
<b>Artifact 1</b>	Remote Network Traffic
<b>Artifact 2</b>	File Metadata Changes
<b>Artifact 3</b>	User Information Changes

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

Artifacts Associated with Valid Accounts Technique (T0859)	
<b>Artifact 1</b>	Logon Session Creation
<b>Artifact 2</b>	User Account Creation
<b>Artifact 3</b>	Logon Type Entry
<b>Artifact 4</b>	Logon Timestamp
<b>Artifact 5</b>	Failed Logons Event
<b>Artifact 6</b>	Successful Logon Event
<b>Artifact 7</b>	System Logs
<b>Artifact 8</b>	Default Credential Use
<b>Artifact 9</b>	Authentication Creation
<b>Artifact 10</b>	Prefetch Files Created After Execution
<b>Artifact 11</b>	Logons
<b>Artifact 12</b>	Application Log
<b>Artifact 13</b>	Domain Permission Requests

Artifacts Associated with Valid Accounts Technique (T0859)	
<b>Artifact 14</b>	Permission Elevation Requests
<b>Artifact 15</b>	Application Use Times
<b>Artifact 16</b>	Configuration Changes

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

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

Artifacts Associated with Device Restart/Shutdown Technique (T0816)	
<b>Artifact 1</b>	Logon Events
<b>Artifact 2</b>	Process Alarm



Artifacts Associated with Device Restart/Shutdown Technique (T0816)	
<b>Artifact 3</b>	Memory Corruption
<b>Artifact 4</b>	Unauthorized Input
<b>Artifact 5</b>	Command Prompt Opened
<b>Artifact 6</b>	Hardware Failure
<b>Artifact 7</b>	Logoff Events
<b>Artifact 8</b>	Local Network Connections
<b>Artifact 9</b>	Significant Operational Data Changes
<b>Artifact 10</b>	Blue Screen
<b>Artifact 11</b>	Reboot Screen
<b>Artifact 12</b>	Network Command Packets
<b>Artifact 13</b>	Loss of Network Connection
<b>Artifact 14</b>	Process Environmental Changes
<b>Artifact 15</b>	Process Failure
<b>Artifact 16</b>	Process Application Event
<b>Artifact 17</b>	External Network Connections

Artifacts Associated with Data Destruction Technique (T0809)	
<b>Artifact 1</b>	Command Line Arguments
<b>Artifact 2</b>	Files Moved to Recycle Bin
<b>Artifact 3</b>	Missing Files
<b>Artifact 4</b>	Host System Reboot Failure
<b>Artifact 5</b>	Process Logic Failure
<b>Artifact 6</b>	Event Log Creation
<b>Artifact 7</b>	System Call
<b>Artifact 8</b>	System Application Interruption
<b>Artifact 9</b>	Device Failure
<b>Artifact 10</b>	Recovery Attempt Failure
<b>Artifact 11</b>	Trivial File Transfer Protocol (TFTP) Port
<b>Artifact 12</b>	SFTP Port
<b>Artifact 13</b>	Memory Corruption
<b>Artifact 14</b>	Use of File Transfer Protocols
<b>Artifact 15</b>	Secure Copy Protocol (SCP) Port
<b>Artifact 16</b>	File Encryptions
<b>Artifact 17</b>	Non-Native Files

Artifacts Associated with Data Destruction Technique (T0809)	
<b>Artifact 18</b>	External Network Connections
<b>Artifact 19</b>	Transient Device Connections
<b>Artifact 20</b>	Program Execution
<b>Artifact 21</b>	Telnet Port
<b>Artifact 22</b>	FTPS Port
<b>Artifact 23</b>	HTTP Port
<b>Artifact 24</b>	HTTPS Port
<b>Artifact 25</b>	Local Network Connections
<b>Artifact 26</b>	FTP Port
<b>Artifact 27</b>	SMB Port

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

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

<b>Engineering</b>  <ul style="list-style-type: none"><li>• Process Engineer</li><li>• Electrical, Controls, and Mechanical Engineer</li><li>• Project Engineer</li><li>• Systems and Reliability Engineer</li><li>• OT Developer</li><li>• PLC Programmer</li><li>• Emergency Operations Manager</li><li>• Plant Networking</li><li>• Control/Instrumentation Specialist</li><li>• Protection and Controls</li><li>• Field Engineer</li><li>• System Integrator</li></ul>	<b>Support Staff</b>  <ul style="list-style-type: none"><li>• Remote Maintenance &amp; Technical Support</li><li>• Contractors (engineering)</li><li>• IT and Physical Security Contractor</li><li>• Procurement Specialist</li><li>• Legal</li><li>• Contracting Engineer</li><li>• Insurance</li><li>• Supply-chain Participant</li><li>• Inventory Management/Lifecycle Management</li><li>• Physical Security Specialist</li></ul>
<b>Operations Technology (OT) Staff</b>  <ul style="list-style-type: none"><li>• Operator</li><li>• Site Security POC</li><li>• Technical Specialists (electrical/mechanical/chemical)</li><li>• ICS/SCADA Programmer</li></ul>	<b>Information Technology (IT) Cybersecurity</b>  <ul style="list-style-type: none"><li>• ICS Security Analyst</li><li>• Security Engineering and Architect</li><li>• Security Operations</li><li>• Security Response and Forensics</li><li>• Security Management (CSO)</li><li>• Audit Specialist</li></ul>
<b>Operational Technology (OT) Cybersecurity</b>  <ul style="list-style-type: none"><li>• OT Security</li><li>• ICS/SCADA Security</li></ul>	<ul style="list-style-type: none"><li>• Security Tester</li></ul>
<b>Management</b>  <ul style="list-style-type: none"><li>• Plant Manager</li><li>• Risk/Safety Manager</li><li>• Business Unit Management</li><li>• C-level Management</li></ul>	<b>Information Technology (IT) Staff</b>  <ul style="list-style-type: none"><li>• Networking and Infrastructure</li><li>• Host Administrator</li><li>• Database Administrator</li><li>• Application Development</li><li>• ERP/MES Administrator</li><li>• IT Management</li></ul>

## REFERENCES

- <sup>1</sup> [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]
- <sup>2</sup> [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]
- <sup>3</sup> [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]
- <sup>4</sup> [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]
- <sup>5</sup> [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]
- <sup>6</sup> [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]
- <sup>7</sup> [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]
- <sup>8</sup> [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]
- <sup>9</sup> [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]
- <sup>10</sup> [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]
- <sup>11</sup> [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]
- <sup>12</sup> [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]
- <sup>13</sup> [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]

---

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]

<sup>14</sup> [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]

<sup>15</sup> [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]

<sup>16</sup> [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]

<sup>17</sup> [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]

<sup>18</sup> [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]

<sup>19</sup> [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]

<sup>20</sup> [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]

<sup>21</sup> [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]

<sup>22</sup> [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]

<sup>23</sup> [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]

<sup>24</sup> [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]

<sup>25</sup> [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]

- 
- <sup>26</sup> [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]
- <sup>27</sup> [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]
- <sup>28</sup> [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]
- <sup>29</sup> [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]
- <sup>30</sup> [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]
- <sup>31</sup> [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]
- <sup>32</sup> [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]
- <sup>33</sup> [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]
- <sup>34</sup> [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]
- <sup>35</sup> [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]
- <sup>36</sup> [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]
- <sup>37</sup> [TrendMicro | “What Is RYUK Ransomware?” | [https://www.trendmicro.com/en\\_us/what-is/ransomware/ryuk-ransomware.html](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]
- <sup>38</sup> [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]
- <sup>39</sup> [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]

<sup>40</sup> [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]

<sup>41</sup> [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]

<sup>42</sup> [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]

<sup>43</sup> [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]

<sup>44</sup> [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]

<sup>45</sup> [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]

<sup>46</sup> [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]

<sup>47</sup> [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]

<sup>48</sup> [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]

<sup>49</sup> [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]

<sup>50</sup> [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]

<sup>51</sup> [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]

<sup>52</sup> [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]