PRECURSOR ANALYSIS REPORT: WANNACRY RANSOMWARE ATTACK ON RENAULT-NISSAN 2017

Cybersecurity for the Operational Technology Environment (CyOTE)

31 MARCH 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-67339

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

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: WANNACRY RANSOMWARE ATTACK ON RENAULT-NISSAN 2017

1. EXECUTIVE SUMMARY

The WannaCry Ransomware Attack on Renault-Nissan 2017 Precursor Analysis Report leverages publicly available information about the attack and catalogues anomalous observables for each technique employed by the adversary. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

On 12 May 2017, Renault-Nissan, an international car manufacturing company, was the victim of a WannaCry ransomware attack that resulted in the shutdown of five manufacturing plants. WannaCry displayed ransom notes on infected machines, demanding a payment of $300 in Bitcoin, which would double to $600 in three days, to recover encrypted files per machine. The company decided to halt operations and isolate communications for the infected manufacturing facilities, which were in France, Slovenia, Romania, and India. The losses Renault-Nissan suffered, both from any ransom payments and lost revenues, were not made public. For purposes of comparison, Taiwan Semiconductor Manufacturing Company (TSMC) lost 3 percent of its quarterly revenues from a WannaCry attack in 2018 that resulted in a disruption of a similar duration. In Renault-Nissan's case, the company restarted its manufacturing operations on 15 May, three days after the ransomware was triggered.[1]

Renault-Nissan, however, was not the only victim of the May 2017 WannaCry campaign. The ransomware had widespread impact, compromising 200,000 systems throughout 100,000 organizations in over 150 countries worldwide.[2] While Symantec estimated that WannaCry inflicted $4 billion in financial losses worldwide,[3] the CyOTE analysts assess the true cost of this campaign was likely much greater after the cost of infrastructure changes and actions taken to return to normal operations are considered.

Researchers and analysts identified 12 unique techniques (used in a sequence of 14 steps) utilized during the attack with a total of 87 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. Nine of the identified techniques used during Renault-Nissan's 2017 cyber attack were precursors to the triggering event. Analysis identified 69 observables associated with these precursor techniques, 50 of which were assessed to have an increased likelihood of being perceived in the 60 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

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

2. INTRODUCTION

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

2.1. APPLYING THE CYOTE METHODOLOGY

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

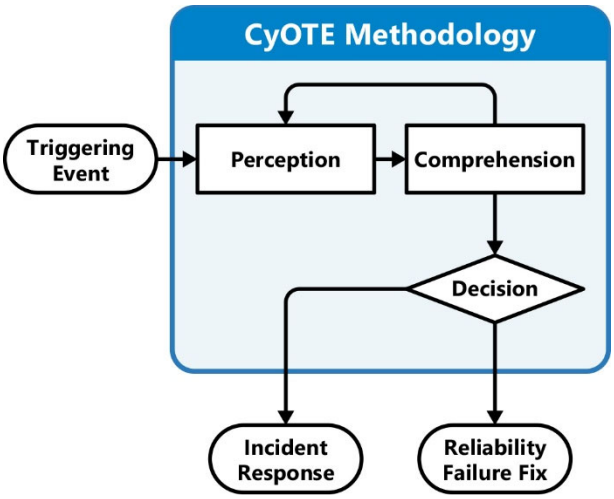


Figure 1. CyOTE Methodology

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

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

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

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

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

2.2. BACKGROUND ON THE ATTACK

On 12 May 2017, adversaries triggered the WannaCry malware that reportedly resulted in Renault-Nissan shutting down five of their manufacturing plants in India, Romania, Slovenia, and France. While not confirmed in publicly available information, the triggering event was likely the use of the Service Stop technique that could have impacted devices within the OT network if the ransomware had spread from the IT network. Operators would have observed a ransom note on the displays of infected systems, demanding a ransom of $300 in Bitcoin; whether Renault-Nissan paid the ransom was not publicly disclosed. The affected plants remained offline until 15 May when they resumed operations.

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.

On 14 March 2017 (D-60), Microsoft identified and provided a patch for the MS17-010 vulnerability that enabled the EternalBlue exploit used in the WannaCry attack. The initial release of information regarding the EternalBlue exploit occurred on 14 April.[4] As a result, the initial access vector for WannaCry is assessed to have occurred on that day, 26 days (D-26) before the Service Stop triggering event on 12 May (D-0).[5,6]

The first detailed report on the WannaCry malware campaign was released by Poland's Computer Emergency Response Team (CERT) on 15 May (D+3) and is assessed as the comprehension date for the campaign.[7,8,9,10]

The WannaCry malware campaign included a ransomware component that leverages operating system level exploits in Windows, allowing it to affect enterprise assets. WannaCry had limited criminal success due to the discovery of a kill switch domain by security researchers. The researchers redirected the propagation of the malware within hours of the triggering event to a sinkhole and dampened the impact of the cyber-attack.

The WannaCry malware also created and executed new services, opened backdoors to The Onion Router (TOR) servers, and encrypted dynamic link library files (DLLs). The malware inhibited response efforts by quickly encrypting vulnerable service data and spreading to other vulnerable devices within the

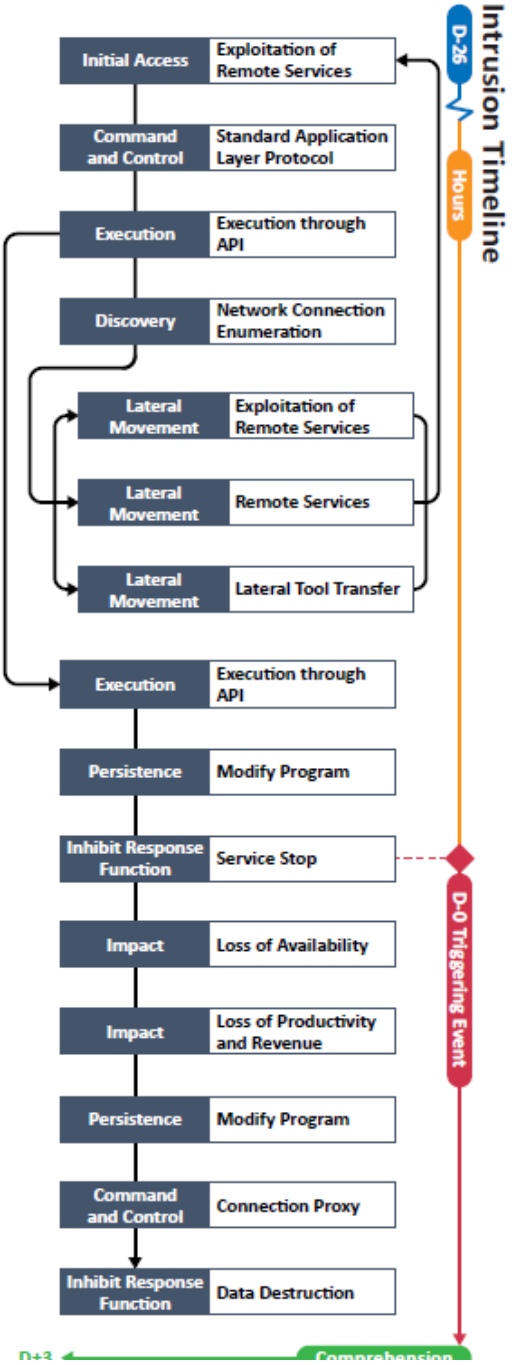


Figure 2. Intrusion Timeline

network. These actions directly impacted Renault-Nissan's ability to function and operate by rendering victim system data inaccessible for a total of three days.[11,12,13,14]

Analysis identified 12 unique techniques (used in a sequence of 14 steps) 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 Industrial Control Systems framework.

Table 1. Techniques Used in the WannaCry Ransomware Attack on Renault-Nissan 2017

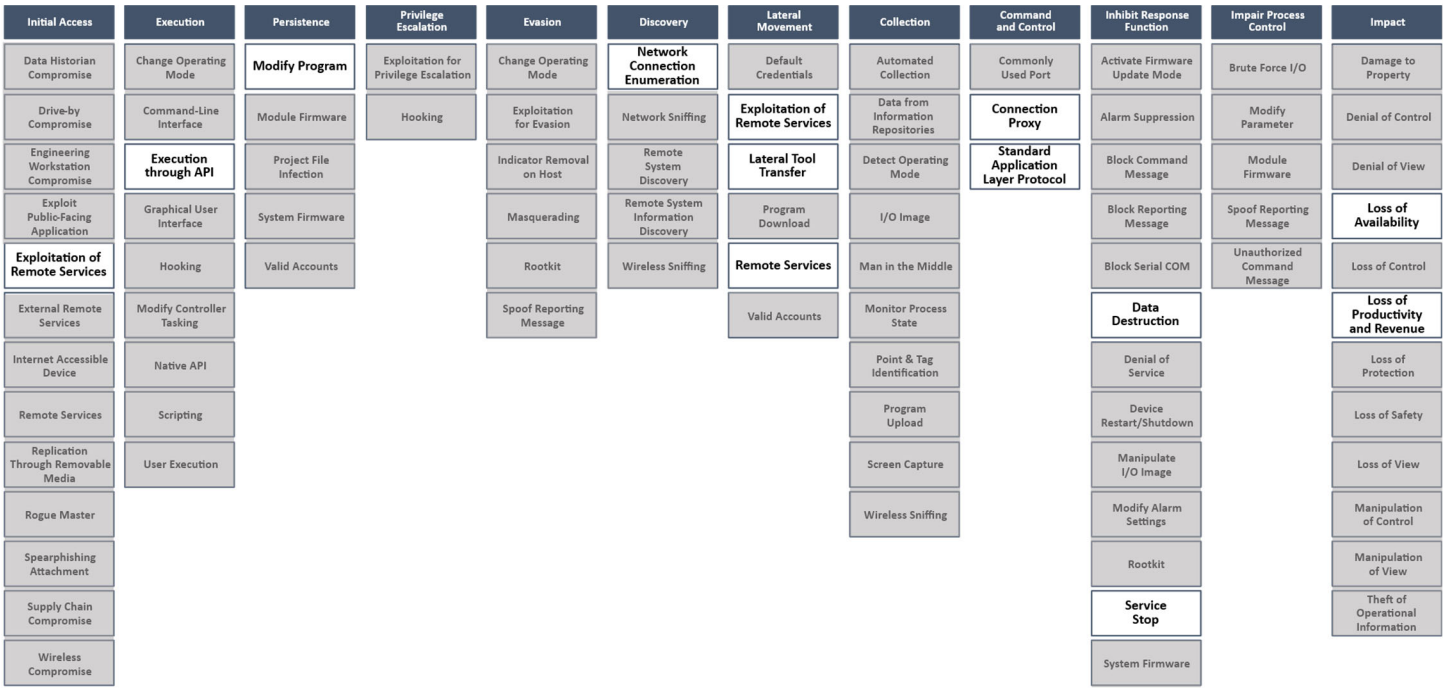


Table 2. Precursor Analysis Report Quantitative Summary

Case Study Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	14
Technique Observables	87
Precursor Techniques	9
Precursor Technique Observables	69
Highly Perceivable Precursor Technique Observable	50

3. OBSERVABLE AND TECHNIQUE ANALYSIS

The following analysis may assist organizations 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. EXPLOITATION OF REMOTE SERVICES TECHNIQUE (T0866) FOR INITIAL ACCESS

Adversaries may leverage vulnerabilities within remote services to move between assets or network segments. The adversaries leveraged the EternalBlue exploit in the Exploitation of Remote Services technique to gain initial access to Renault-Nissan systems on 12 May 2017. Renault-Nissan personnel would have witnessed observables associated with the Exploitation of Remote Services technique within the enterprise and OT environments throughout the entire intrusion.

As part of this technique, WannaCry leverages a vulnerability within the Server Message Block Version 1.0 (SMBv1) protocol, documented in Microsoft Security bulletin MS 17-010, to gain access to a host. Observers likely would have witnessed initiation of SMB requests via Port 445 on hardcoded IP addresses (192[.]168[.]56.20\IPC$ and 172[.]16[.].99.IPC$). WannaCry sets unique values on fields using the SMB protocol, including a Multiplex ID of 81. Failed SMB authentication events could be observed in network traffic.[15]

OT Staff, OT Cybersecurity, Support Staff, IT Cybersecurity, and IT Staff personnel may have been able to observe SMB traffic from anomalous, external IP addresses. They may have also observed specific facets of SMB packets, including access of named pipes as well as an increase in failed SMB authentication events. If these items were identified early in the attack, comprehension time would be reduced.

A total of six observables were identified with the use of the Exploitation of Remote Services technique (T0866). This technique is important for investigation because it presents noticeable effects, such as generation of system log entries and anomalous network traffic. This technique also allows a malicious actor access to systems beyond the host in question, potentially compromising additional hosts. This technique occurs earlier in the timeline and an early response can effectively halt all future events. Terminating the chain of techniques at this point would prevent the use of subsequent techniques.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 31 artifacts could be generated by using the Exploitation of Remote Services technique
Technique Observers[a]	OT Staff, OT Cybersecurity, Support Staff, IT Cybersecurity, IT Staff

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

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

WannaCry also used the EternalBlue exploit to initiate a two-way communication channel via SMB and leveraged the DoublePulsar implant tool to create a backdoor into the victim network from the Internet using TOR. To determine whether to infect a host, the malware would attempt to connect to a kill switch domain. If a connection succeeded, the malware would stop propagating; if the connection failed, the malware would continue to propagate through the victim network.

Observables for this technique have significant overlap with those of the previous technique (T0866). One difference, however, is upon gaining access to a machine, the May 2017 version of WannaCry attempted to connect to this specific kill switch domain, and would continue to propagate until a successful connection could be made:

http[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

OT Staff, OT Cybersecurity, Support Staff, IT Cybersecurity, and IT Staff personnel may have been able to observe anomalous SMB traffic as well as anomalous network connections using the TOR protocol. Additionally, anomalous DNS requests may have been observed. Rapid identification and investigation would have reduced comprehension time.

A total of five observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation because it presents noticeable effects, such as generation of system log entries and anomalous network traffic. This technique occurs earlier in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would limit system damage to anomalous network traffic and system logs. This technique modifies the host operating system files via the creation of anomalous services and modification of user accounts, placing the host into a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the five observables associated with this technique, four are assessed to be highly perceivable. They are italicized and marked † in Appendix A.[16]

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

3.3. EXECUTION THROUGH API TECHNIQUE (T0871) FOR EXECUTION

When executed, WannaCry runs as a Windows service (mssecsvc.exe) on the host, executing a function that registers with service handlers to execute as a legitimate service within the Microsoft operating system.

Specific observables that IT cybersecurity or network administrators might recognize include the presence of a specific executable invoked binary path name:

BinaryPathName="%currentdirectory%5bef35496fcbdbe841c82f4d1ab8b7c2.exe -msecurity

This registers the mssecsvc.exe executable (MD5 db349b97c37d22f5ea1d1841e3c89eb4) as a service and generates corresponding events (e.g., Event 7036) in the Windows System Log.[17]

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe the registration of anomalous executables as well as anomalous Windows Event log entries. Additionally, anomalous running services may have been observed.

A total of five observables were identified with the use of the Execution Through API technique (T0871). This technique is important for investigation because it presents noticeable effects, such as modified settings within the victim's operating system, generation of system log entries, and generation of anomalous network traffic. This technique occurs earlier in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would limit the adversaries' access, as well as prevent the installation and execution of ransomware. This technique modifies the host operating system files via the creation of anomalous services and modification of user accounts, placing the host into a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the five observables associated with this technique, four are assessed to be highly perceivable. They are italicized and marked † in Appendix A.[18,19]

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 19 artifacts could be generated by using the Execution Through API technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity

3.4. NETWORK CONNECTION ENUMERATION TECHNIQUE (T0840) FOR DISCOVERY

Once the WannaCry malware executes, it starts a service named mssecsvc2.0 (Microsoft Security Center 2.0 Service). This service attempts to create and scan a list of IP ranges on the local network and tries to connect to these discovered IP addresses over UDP Ports 137 and 138 and over TCP Ports 139 and 445.[20,21] This behavior allows WannaCry to enumerate and subsequently propagate among devices throughout the local network.

The malware identifies the subnet on which the system resides, scans IP ranges, connects via SMB, and scans for new file shares every few seconds. WannaCry also enumerates active RDP sessions running on the infected host via the taskse.exe executable:

MD5 2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d

WannaCry will attempt to propagate via RDP in parallel with SMB; the enumeration of network drives will result in artifacts related to the SMB protocol. At this stage, the malware, by consuming extra host or network-level resources, may produce latencies in operational and enterprise devices that could be observable by users.[22]

Engineering, OT Staff, OT Cybersecurity, IT Staff, Support Staff, and IT Cybersecurity may have been able to observe anomalous SMB network traffic as well as repeated traffic associated with network scanning. Additionally, anomalous services and processes may be observed running.

A total of 12 observables were identified with the use of the Network Connection Enumeration technique (T0840). This technique is important for investigation because it presents noticeable effects, such as generation of system log entries, increased resource utilization, and generation of anomalous network traffic. This technique also occurs earlier in the timeline and responding to it will effectively halt all future events. This technique enables future techniques access to systems beyond the host in question, resulting in the potential compromise of additional hosts. Terminating the chain of techniques at this point would prevent the malware from propagating from the initially compromised host to additional hosts.

Of the 12 observables associated with this technique, seven are assessed to be highly perceivable. They are italicized and marked † in Appendix A.[23]

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 33 artifacts could be generated by using the Network Connection Enumeration technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, IT Staff, Support Staff, IT Cybersecurity

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

For each host in the scanned network identified by WannaCry as having an open SMB service or active RDP session, the malware will create an additional thread to propagate. In the former case, WannaCry leverages the EternalBlue exploit. In the latter, the malware will execute over the RDP session. Specific observables lateral to this technique are like those of the previous technique (T0840), although increased network traffic may also be associated with malware propagation and not just network enumeration.

Engineering, OT Staff, IT Staff, Support Staff, OT Cybersecurity, and IT Cybersecurity personnel may have been able to observe an increase in failed as well as successful authentication attempts via RDP.

A total of 10 observables were identified with the use of the Exploitation of Remote Services technique (T0866). This technique is important for investigation because it is the mechanism by which malware can propagate to additional hosts. This technique appears midway in the timeline and responding to it will limit further exploitation and propagation. If system backups occur on other systems within the enterprise after this technique is executed, data recovery and disaster recovery efforts will be impaired. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 31 artifacts could be generated by using the Exploitation of Remote Services technique
Technique Observers	Engineering, OT Staff, IT Staff, Support Staff, OT Cybersecurity, IT Cybersecurity

3.6. REMOTE SERVICES TECHNIQUE (T0886) FOR LATERAL MOVEMENT

The WannaCry malware will spawn a second thread to propagate to hosts running on networks other than that of the currently infected host. The second thread generates random IPs and attempts to connect to them on Port 445. If the connection is successful, the malware then attempts to exploit the SMBv1 vulnerability mentioned previously. Existing RDP sessions on devices located within external networks are a secondary means through which the malware can propagate outside of its current host's subnet.

Different artifacts would be observable to IT and cybersecurity professionals, depending upon whether the lateral movement was achieved via SMB or RDP. In either case, increases in network traffic for each of these protocols would be visible as the malware simultaneously attempts to connect to multiple external hosts. In the latter case, creating an active RDP session would result in the generation of an Event 4624 in the Windows Event Log along with an unencrypted RDP cookie containing the username. Event 7036, corresponding to changes to services, would also likely appear in the Windows System Log.

Support Staff, IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe anomalous volumes network traffic related to the SMB or RDP protocols.

A total of eight observables were identified with the use of the Remote Services Technique (T0886). This technique is important for investigation as it is often leveraged to facilitate lateral movement in a victim's environment, allowing for further malicious activity. This technique appears midway through 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 to the infected host and prevent the malware from spreading to additional vulnerable hosts. If system backups occur on other systems within the enterprise after this technique is executed, data recovery and disaster recovery efforts will be impaired.

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

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

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

According to CyOTE analysts, WannaCry leverages both SMB and RDP to move laterally through affected networks. SMB and RDP are commonly used components within industrial networks and enable the malware to copy itself over to uninfected hosts. Several of these observables overlap with the previous two techniques, including increased network traffic over the SMB and RDP protocols, the transmission of login credentials, and potential artifacts of creating active sessions (e.g., Event 4624 in the Windows Event Log).

Engineering, OT Staff, OT Cybersecurity, Support Staff, IT Cybersecurity, and IT Staff personnel may have been able to observe anomalous network traffic associated with SMB and RDP, as well as an increase in anomalous successful and failed authentication attempts.

A total of 11 observables were identified with the use of the Lateral Tool Transfer technique (T0867). This technique is important for investigation because it enables the malware to propagate to additional hosts and spread throughout the operating environment. It modifies the host operating system files of other hosts via the manipulation of system configuration settings and associated system registry entries, placing the host into a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired. This technique appears in the middle of the timeline and responding to it will likely prevent malware from accessing other hosts within the enterprise. Terminating the chain of techniques at this point would prevent malware from compromising additional systems.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 21 artifacts could be generated by using the Lateral Tool Transfer technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Support Staff, IT Cybersecurity, IT Staff

3.8. EXECUTION THROUGH API TECHNIQUE (T0871) FOR EXECUTION

According to CyOTE analysts, after execution, the WannaCry malware carries out an encryption component within the device itself by installing and extracting a PE32 binary (decryptor) from its resource section named “R”.

Once executed, the malware creates and runs tasksche.exe, initiating the following process with the CreateProcess API:

BinaryPathName=”C: \WINDOWS\tasksche.exe / i”

This generates Windows System Log Event 4688 in the event log and Event 7068 in the service log. If the initiated process is run without the “/i” argument, the WannaCry malware loads an XIA resource and decompresses multiple files. Next, the malware evades detection and obfuscates files by setting hidden attributes for the malware “%CD%” directory. [24]

Engineering, OT Staff, OT Cybersecurity, Support Staff, IT Cybersecurity, and IT Staff personnel may have been able to observe the addition of anomalous scheduled tasks, running services, and windows system log entries. Additionally, the presence of anomalous directories and files may be detected. Finally, the absence of files and the presence of anomalously encrypted files within the OT and IT environment may be detected.

A total of eight observables were identified with the use of the Execution through API technique (T0871). This technique is important for investigation because it allows the encryption of data within the victim environment. This technique appears in the middle of the timeline and responding to it will likely prevent malicious encryption and potential loss of data, as well as critical business services. This technique modifies files within the enterprise, via encryption of files, placing data into a modified state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired. Terminating the chain of techniques at this point will prevent the malware from encrypting files as well as exfiltrating data.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 19 artifacts could be generated by using the Execution through API technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Support Staff, IT Cybersecurity, IT Staff

3.9. MODIFY PROGRAM TECHNIQUE (T0889) FOR PERSISTENCE

The WannaCry malware adds a registry key to "tasksche.exe" which modifies the registry.[26] To ensure persistence is maintained, the malware creates two registry run keys:

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Randomvalue1>:
<Full_path>\tasksche.exe

and

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Randomvalue2>:
<Full_path>\tasksche.exe

Once created, the registry run keys are executed in the task scheduler.

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe the creation and execution of anomalous scheduled tasks, services, and processes. Additionally, the modification of registry keys may be detected.

A total of four observables were identified with the use of the Modify Program technique (T0889). This technique is important for investigation because it modifies the host and enables persistent adversarial access to victim operating environments. This technique appears in the middle of the timeline and responding to it will limit persistence of the malware. This technique modifies the host operating system files, via the manipulation of processes and modification of registry files, resulting in the host being placed into a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired. Terminating the chain of techniques at this point will limit persistence of malware within operational environments.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 3 artifacts could be generated by using the Modify Program technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity

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

At this point, the WannaCry malware would stop the MS Exchange and Structured Query Language (SQL) servers, potentially impacting any data server (e.g., data historian). As a result, all services would have been shut down manually by operators due to an inability to control or change operations or functions.[28] In addition, the process for the decryptor (WanaDecryptor) would spawn.

Engineering, Management, IT Staff, IT Cybersecurity, Support Staff, OT Cybersecurity, and OT Staff personnel may have been able to observe the anomalous absence of SQL-based database services as well as Exchange-based email services. Additionally, the anomalous stoppage of critical services may be observed.

A total of three observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation because it prevents victims from delivering products or services. This technique modifies the host operating system files, via the manipulation of host services and modification of registry files, resulting in the host being placed into a modified or compromised state. This technique occurs late in the timeline and represents the triggering event. Terminating the chain of techniques at this point would limit the disablement of mission-critical services.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 13 artifacts could be generated by using the Service Stop technique
Technique Observers	Engineering, Management, IT Staff, IT Cybersecurity, Support Staff, OT Cybersecurity, OT Staff

3.11. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

At this stage along the attack timeline, the victim will start to lose access to files and functionality within the system (e.g., Human Machine Interface [HMI], historian, Programmable Logic Controllers [PLCs], Remote Terminal Units [RTUs], share drive, etc.), resulting in a loss of host and network availability. This could affect industrial applications resulting in a loss of availability, loss of control, and loss of ability to operate. Operators will likely note an initial increase in alarms while simultaneously experiencing a sudden loss of system availability. As industrial applications become unavailable due to the malware encrypting of file shares and/or drives, remote services become unavailable. While operators and engineers work to re-establish process control, a ransom note is identified within the OT environment, providing confirmation of a cyber attack.

Engineering, Management, Support Staff, IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe the loss of access to and functionality of systems within the OT and IT environments. Additionally, the loss of access to files and folders within both environments may be observed.

A total of seven observables were identified with the use of the Loss of Availability technique (T0826). This technique is important for investigation because it prevents owners and operators from delivering products or services. This technique also presents noticeable effects, resulting in unresponsive equipment and limited network functionality. This technique appears late in the timeline and responding to it has the potential to limit the impact to responsiveness and functionality. Terminating the chain of techniques at this point would limit the ability of WannaCry to maintain C2 connectivity, as well as limit the deletion of critical data.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 8 artifacts could be generated by using the Loss of Availability technique
Technique Observers	Engineering, Management, Support Staff, IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity

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

Immediately following the loss of availability of operational systems, the user has lost all access to files and functionality within the system (e.g., HMI, historian, PLCs, RTUs, share drive, etc.), resulting in a loss of trust and confidence in the control and safety systems. Operators experiencing a loss of operational process control will likely be required to troubleshoot the issue by resetting/restarting processes. Operators would find industrial applications inaccessible due to the encryption of file shares and/or drives and a loss of access to remote services.

Engineering, Management, Support Staff, IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe the loss of access to files, drives, and business systems within the OT and IT environments.

A total of two observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation because it involves a direct loss of revenue and productivity for the victim. Additionally, this technique may present an impact for the end users or consumers of products and services. This technique appears at the end of the timeline and responding to it will include efforts to regain operational functionality and to resume normal operation. Terminating the chain of techniques at this point would not limit destruction or business impacts.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 5 artifacts could be generated by using the Loss of Productivity and Revenue technique
Technique Observers	Engineering, Management, Support Staff, IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity

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

With operations effectively stopped, the WannaCry malware would continue to maintain its Command-and-Control connections through a TOR proxy.[29] Once the ransom is paid, the attackers would use the TOR proxy to deliver the decryption key using traffic via TCP Port 9050 within the infected environment. The individuals who would see this activity are network administrators and cyber defenders.

IT Staff, IT Cybersecurity, OT Cybersecurity, and OT Staff personnel may have been able to observe anomalous DNS, HTTP, and/or HTTPS traffic being sent over a non-standard port, as well as increased overall network traffic.

A total of three observables were identified with the use of the Connection Proxy Technique (T0884). This technique is important for investigation because it enables continued monitoring of the victim's operating environment via command and control of the host environment. This technique appears late in the timeline and responding to it will include efforts to regain operational functionality and resume normal operation. Terminating the chain of techniques at this point would disable adversary C2 communications.

All three 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 6 artifacts could be generated by using the Connection Proxy technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity, OT Staff

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

In the event the ransom is not paid, the attackers could delete the locations where Windows operating systems store copies of files (i.e., Volume Shadow Copy files). The volume shadow copies used for back-ups would be “present” but “unavailable” due to the lack of data, denying the victim the ability to restore files.

Engineering, Management, Support Staff, OT Staff, OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe the anomalous deletion of files and data, including critical operating system files. Additionally, Windows-based machines would likely be observed anomalously failing and unable to reboot.

A total of three observables were identified with the use of the Data Destruction Technique (T0809). This technique is important for investigation because it renders files crucial to business and other enterprise operations unusable. This technique appears late in the timeline and responding to it at this point in the timeline is unlikely to minimize the impact of WannaCry. Terminating the chain of techniques at this point would prevent the deletion of sensitive files as well as critical operating system files.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 27 artifacts could be generated by using the Data Destruction technique
Technique Observers	Engineering, Management, Support Staff, OT Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

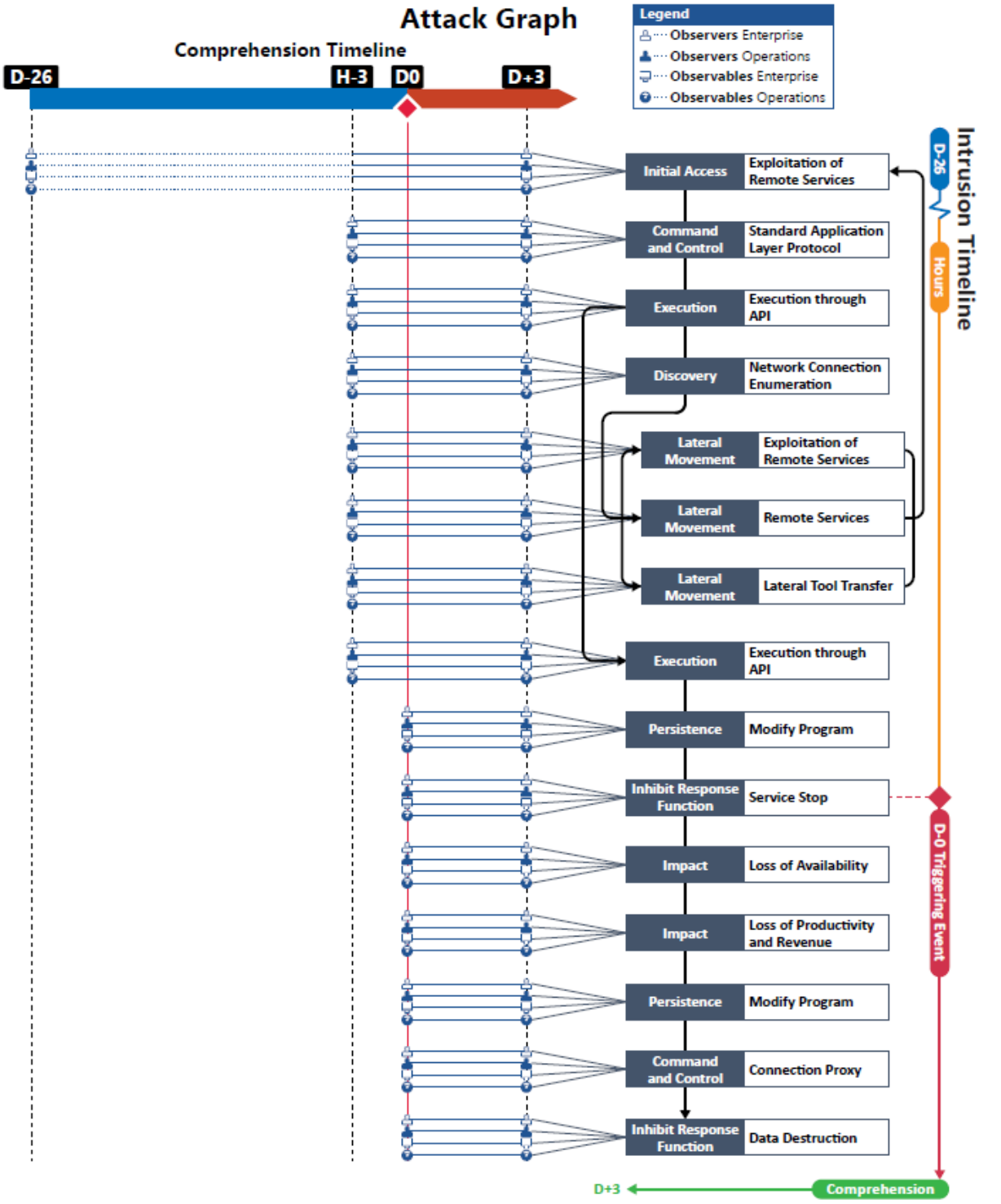


Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

Observables Associated with Exploitation of Remote Services Technique (T0866)	
Observable 1	Usage of Remote Services Protocols Between Assets and Network Segments
Observable 2 †	*MS 17-010 Vulnerability Within Environment*
Observable 3 †	*Initiation of SMB Requests via 445 to Hardcoded IPs 192.168.56.20\IPC$ and 172.16.99.IPC$*
Observable 4 †	*Unique Values in SMB Fields with Multiplex ID Of 81*
Observable 5 †	*Failed SMB Authentication.*
Observable 6 †	*Increase In SMB Authentication Requests*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1	SMBv1 Connections
Observable 2 †	*Backdoor Created Using DoublePulsar in Host Memory*
Observable 3 †	*Infected Host Connecting to Internet via TOR*
Observable 4 †	*Outgoing DNS Requests to Kill Switch Domain http[:]//Www[.]luqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com*
Observable 5 †	*Connection Attempts to Malicious URI Across Victim Environment*

Observables Associated with Execution Through API Technique (T0871)	
Observable 1 †	*Malicious Program Runs as Windows Service (mssecsvc.exe) on Host*
Observable 2	Malicious Program Executes Service Handlers as Legitimate Service on Host OS
Observable 3 †	*Malicious Program Executable BinaryPathName="%currentdirectory%5bef35496fcbdbe841c82f4d1ab8b7c2.exe -msecurity."*
Observable 4 †	*mssecsvc.exe Registered Service as MD5 db349b97c37d22f5ea1d1841e3c89eb4*
Observable 5 †	*Windows System Log Event 7036 Entries*

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 1	Increase in Threads Running
Observable 2 †	*Malicious Program Starts Service mssecsvc2.0*
Observable 3 †	*Service Starts Scanning Local Subnet for Lists of IP Ranges Over UDP Ports 137, 138 and TCP Ports 139, 445*
Observable 4 †	*Internal Network Connections Over SMB Created Every Few Seconds*

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 5	Enumeration of Active RDP Sessions
Observable 6	Scheduled Task Executable taskse.exe Will Attempt to Move to Hosts Sharing RDP Connections
Observable 7	Increase in Host Resource Usage
Observable 8	Increase in Network Resources Usage
Observable 9 †	*Host Latency*
Observable 10 †	*Network Latency*
Observable 11 †	*Attempts to Connect to Random IPs via 445 SMB and 3389 RDP*
Observable 12 †	*Host System Log Entries for Session Creation*

Observables Associated with Exploitation of Remote Services Technique (T0866)	
Observable 1	Exploitation of MS 17-010 Vulnerability Using EternalBlue
Observable 2	Connections on TCP Port 445 SMB
Observable 3 †	*Unique Values in SMB Fields*
Observable 4 †	*Failed SMB Connections*
Observable 5	Remote Session Connection on TCP 3389 RDP
Observable 6 †	*Remote Session Failures*
Observable 7 †	*Host Latency*
Observable 8 †	*Network Latency*
Observable 9 †	*Host System Log Entries*
Observable 10 †	*Attempts to Connect to Random IPs via Port 445 SMB and 3389 RDP*

Observables Associated with Remote Services Technique (T0886)	
Observable 1	A Second Thread Is Created on Hosts
Observable 2 †	*Second Thread Generates Random IPs*
Observable 3 †	*Random IPs Attempt to Connect on Port 445 Over SMB*
Observable 4	Existing RDP Sessions Connect to Current Host Subnet
Observable 5	Increase in Network Traffic
Observable 6 †	*Generation of Windows Event ID: 4624*
Observable 7 †	*Unencrypted Cookie Attached to Authentication*
Observable 8 †	*Windows System Log Event ID: 7036*

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 1	Use of Login Credential via File Share and Remote Session Services
Observable 2	Host Event ID 4624 Logs for Successful Logons
Observable 3	Connections on TCP Port 445 SMB
Observable 4 †	*Unique Values in SMB Fields*
Observable 5 †	*Failed SMB Connections*
Observable 6	Remote Session Connection on TCP 3389 RDP
Observable 7 †	*Remote Session Failures*
Observable 8 †	*Host Latency*
Observable 9 †	*Network Latency*
Observable 10 †	*Host System Log Entries*
Observable 11 †	*Attempts to Connect to Random IPs via Port 445 SMB and 3389 RDP*

Observables Associated with Execution Through API Technique (T0871)	
Observable 1 †	*Malicious Software Executes Encryption Component*
Observable 2 †	*Installation of PE32 Binary (Decryptor)*
Observable 3	Creates and Runs Schedule Task tasksche.Exe
Observable 4 †	*Initiates Process: BinaryPathname="C: \WINDOWS\tasksche.exe / L" with the createprocess API*
Observable 5 †	*Windows System Log Event ID: 4688*
Observable 6 †	*Windows Service Log Event ID: 7068*
Observable 7 †	*Hidden Attribute Set for Malware Directory*
Observable 8 †	*Host System Resource Utilization Increases*

Observables Associated with Modify Program Technique (T0889)	
Observable 1 †	*Host System Registry Modification*
Observable 2 †	*Host System Registry Key Added*
Observable 3 †	*Registry Key Added: "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Randomvalue1>: <Full_path>\tasksche.exe"*
Observable 4 †	*Registry Key Added "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Randomvalue2>: <Full_path>\tasksche.exe"*

Observables Associated with Service Stop Technique (T0881)	
Observable 1 †	*MS Exchange Server Services Killed*
Observable 2 †	*SQL Server Services Killed*
Observable 3 †	*WanaDecryptor Process Spawn*

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1 †	*Loss of Access to Files*
Observable 2 †	*Loss of Functionality Within System*
Observable 3 †	*Loss of Access to Share Drive*
Observable 4 †	*Loss of Host in Network Availability*
Observable 5 †	*Increase in Alarms*
Observable 6 †	*Remote Services Become Unavailable*
Observable 7 †	*Ransom Note Appears on Workstations*

Observables Associated with Loss of Productivity And Revenue Technique (T0828)	
Observable 1 †	*Operations Halted*
Observable 2 †	*Plant Output Diminished*

Observables Associated with Connection Proxy Technique (T0884)	
Observable 1 †	*Connections with TOR Server via Port 9050*
Observable 2 †	*File Decryption Key Delivered via TCP Port 9050, if victim paid*
Observable 3 †	*Increase in CPU Resource Usage*

Observables Associated with Data Destruction Technique (T0809)	
Observable 1 †	*Deletion of Volume Shadow Copies*
Observable 2 †	*Failed Restorations Attempts*
Observable 3 †	*Missing Files*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Exploitation of Remote Services Technique (T0866)	
Artifact 1	Application Logs
Artifact 2	Connection to HMI End Points
Artifact 3	Connection to EWS End Points
Artifact 4	Connection to Data Historian End Points
Artifact 5	Connection to Controller End Points
Artifact 6	Manipulation of Process
Artifact 7	Manipulation of Set Points
Artifact 8	Misconfigurations of End Points
Artifact 9	Process Failure
Artifact 10	Controller Failure
Artifact 11	Code Injections into Application
Artifact 12	Application Log On Event
Artifact 13	Code Injection into the OS
Artifact 14	OPC Code Injection
Artifact 15	Database Command Executions
Artifact 16	User Events Across Multiple Devices
Artifact 17	Host System Registry Changes
Artifact 18	Security Events Across Multiple Devices
Artifact 19	Kernel Level Events
Artifact 20	System Reboots
Artifact 21	Blank Screens
Artifact 22	Safemode Reboot
Artifact 23	Application Log Off Event
Artifact 24	Alarm Events
Artifact 25	Absence of Alarm Events
Artifact 26	Common Network Traffic
Artifact 27	Remote Network Traffic
Artifact 28	Vendor Specific Network Traffic
Artifact 29	Industrial Protocol Network Traffic
Artifact 30	SQL Protocol
Artifact 31	SMB Protocol

Artifacts Associated with Standard Application Layer Protocol Technique (T0869)	
Artifact 1	External Network Connections
Artifact 2	DNS Autonomous System Number
Artifact 3	Increase in the Number of External Connections
Artifact 4	Network Content Metadata
Artifact 5	Network Connection Times
Artifact 6	HTTP Traffic Port 80
Artifact 7	DNS Traffic Port 53
Artifact 8	SMB Traffic Port 445
Artifact 9	HTTPS Traffic Port 443
Artifact 10	RDP Traffic Port 3389
Artifact 11	HTTP Post Request
Artifact 12	External IP Addresses

Artifacts Associated with Execution Through API Technique (T0871)	
Artifact 1	Process Failure
Artifact 2	Reboot
Artifact 3	Module Load
Artifact 4	Control Logic Change
Artifact 5	Timestamps Associated with Activity
Artifact 6	IP Addresses from Network Traffic
Artifact 7	API Log Event (if enabled)
Artifact 8	SCADA Protocol Network Traffic
Artifact 9	Data Sent with Large File Size
Artifact 10	Data Received with Large File Size
Artifact 11	Network Traffic with Command Execution Content
Artifact 12	State Change in the Process
Artifact 13	Function Execution
Artifact 14	Common Network Traffic
Artifact 15	Industrial Network Traffic
Artifact 16	Vendor Specific Network Traffic
Artifact 17	Remote Connections
Artifact 18	Controller Failure

Artifacts Associated with Execution Through API Technique (T0871)	
Artifact 19	Controller Configuration Change

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 1	Common Network Traffic
Artifact 2	Polling Network Traffic from Abnormal IP Sender Addresses
Artifact 3	NetBIOS Name Services Port 137
Artifact 4	LDAP Port 389
Artifact 5	Active Directory Calls
Artifact 6	Email Server Calls
Artifact 7	SMTP Port 25 Traffic
Artifact 8	DNS Lookup Queries
Artifact 9	ARP Scans
Artifact 10	TCP Connect Scan
Artifact 11	TCP SYN Scans
Artifact 12	Industrial Network Traffic
Artifact 13	TCP FIN Scans
Artifact 14	TCP Reverse Ident Scan
Artifact 15	TCP XMAS Scan
Artifact 16	TCP ACK Scan
Artifact 17	VNC Port 5900 Calls
Artifact 18	Protocol Content Enumeration
Artifact 19	Protocol Header Enumeration
Artifact 20	Recurring Protocol SYN Traffic
Artifact 21	Sequential Protocol SYN Traffic
Artifact 22	Statistical Anomalies in Network Traffic
Artifact 23	Echo Port 8 Traffic
Artifact 24	Device Failure
Artifact 25	Device Reboots
Artifact 26	Bandwidth Degradation
Artifact 27	Host Recent Connection Logs
Artifact 28	ICMP Port 7 Traffic
Artifact 29	SNMP Port 162 Traffic

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 30	SNMP Port 161 Traffic
Artifact 31	Command Line Dialog Box Open
Artifact 32	Operating System Queries
Artifact 33	DNS Port 53 Zone Transfers

Artifacts Associated with Exploitation of Remote Services Technique (T0866)	
Artifact 1	Application Logs
Artifact 2	Connection to HMI End Points
Artifact 3	Connection to EWS End Points
Artifact 4	Connection to Data Historian End Points
Artifact 5	Connection to Controller End Points
Artifact 6	Manipulation of Process
Artifact 7	Manipulation of Set Points
Artifact 8	Misconfigurations of End Points
Artifact 9	Process Failure
Artifact 10	Controller Failure
Artifact 11	Code Injections into Application
Artifact 12	Application Log On Event
Artifact 13	Code Injection into the OS
Artifact 14	OPC Code Injection
Artifact 15	Database Command Executions
Artifact 16	User Events Across Multiple Devices
Artifact 17	Host System Registry Changes
Artifact 18	Security Events Across Multiple Devices
Artifact 19	Kernel Level Events
Artifact 20	System Reboots
Artifact 21	Blank Screens
Artifact 22	Safemode Reboot
Artifact 23	Application Log Off Event
Artifact 24	Alarm Events
Artifact 25	Absence of Alarm Events
Artifact 26	Common Network Traffic

Artifacts Associated with Exploitation of Remote Services Technique (T0866)	
Artifact 27	Remote Network Traffic
Artifact 28	Vendor Specific Network Traffic
Artifact 29	Industrial Protocol Network Traffic
Artifact 30	SQL Protocol
Artifact 31	SMB Protocol

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 1	Remote client connection
Artifact 2	Logon Event
Artifact 3	Logoff
Artifact 4	Logoff Event
Artifact 5	Registry Changes
Artifact 6	Registry Connection Change
Artifact 7	Mouse Movement
Artifact 8	Unexpected I/O
Artifact 9	Desktop Prompt Windows Created
Artifact 10	Session Cache
Artifact 11	Application Log
Artifact 12	RDP Traffic 3389
Artifact 12	System Log Event
Artifact 13	Authentication Logs
Artifact 14	GUI Modifications
Artifact 15	Data File Size in Network Content
Artifact 16	File Movement
Artifact 17	MSSQL Traffic 1422 Port
Artifact 18	SSH Traffic 22
Artifact 19	SMB Traffic 139, 445
Artifact 20	VNC Traffic 5800, 5900
Artifact 21	Process Creation
Artifact 22	Remote Session Creation Timestamp
Artifact 23	Network Traffic Content Creation

Artifacts Associated with Lateral Tool Transfer Technique (T0867)	
Artifact 1	Command Execution
Artifact 2	File Location Change
Artifact 3	File Metadata Changes
Artifact 4	User Information Changes
Artifact 5	Process Creation
Artifact 6	System Resource Usage Management Events
Artifact 7	Data Sent from One Location to Another
Artifact 8	Data Received from One Location to Another
Artifact 9	SQL Commands
Artifact 10	SQL Create Commands
Artifact 11	SQL Insert Commands
Artifact 12	Command Prompt Dialog Box Open
Artifact 13	SMB Traffic
Artifact 14	.dll Injection into File Directory
Artifact 15	.dll Execution
Artifact 16	Powershell Dialog Box Open
Artifact 17	Common Network Traffic
Artifact 18	Remote Network Traffic
Artifact 19	Industrial Network Traffic
Artifact 20	File Creation
Artifact 21	File Modification
Artifact 22	File Deletion

Artifacts Associated with Execution Through API Technique (T0867)	
Artifact 1	Process Failure
Artifact 2	Reboot
Artifact 3	Module Load
Artifact 4	Control Logic Change
Artifact 5	Timestamps Associated with Activity
Artifact 6	IP Addresses From Network Traffic
Artifact 7	API Log Event (If Enabled)
Artifact 8	SCADA Protocol Network Traffic

Artifact 9	Data Sent with Large File Size
Artifact 10	Data Received with Large File Size
Artifact 11	Network Traffic with Command Execution Content
Artifact 12	State Change in The Process
Artifact 13	Function Execution
Artifact 14	Common Network Traffic
Artifact 15	Industrial Network Traffic
Artifact 16	Vendor Specific Network Traffic
Artifact 17	Remote Connections
Artifact 18	Controller Failure
Artifact 19	Controller Configuration Change

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

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

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

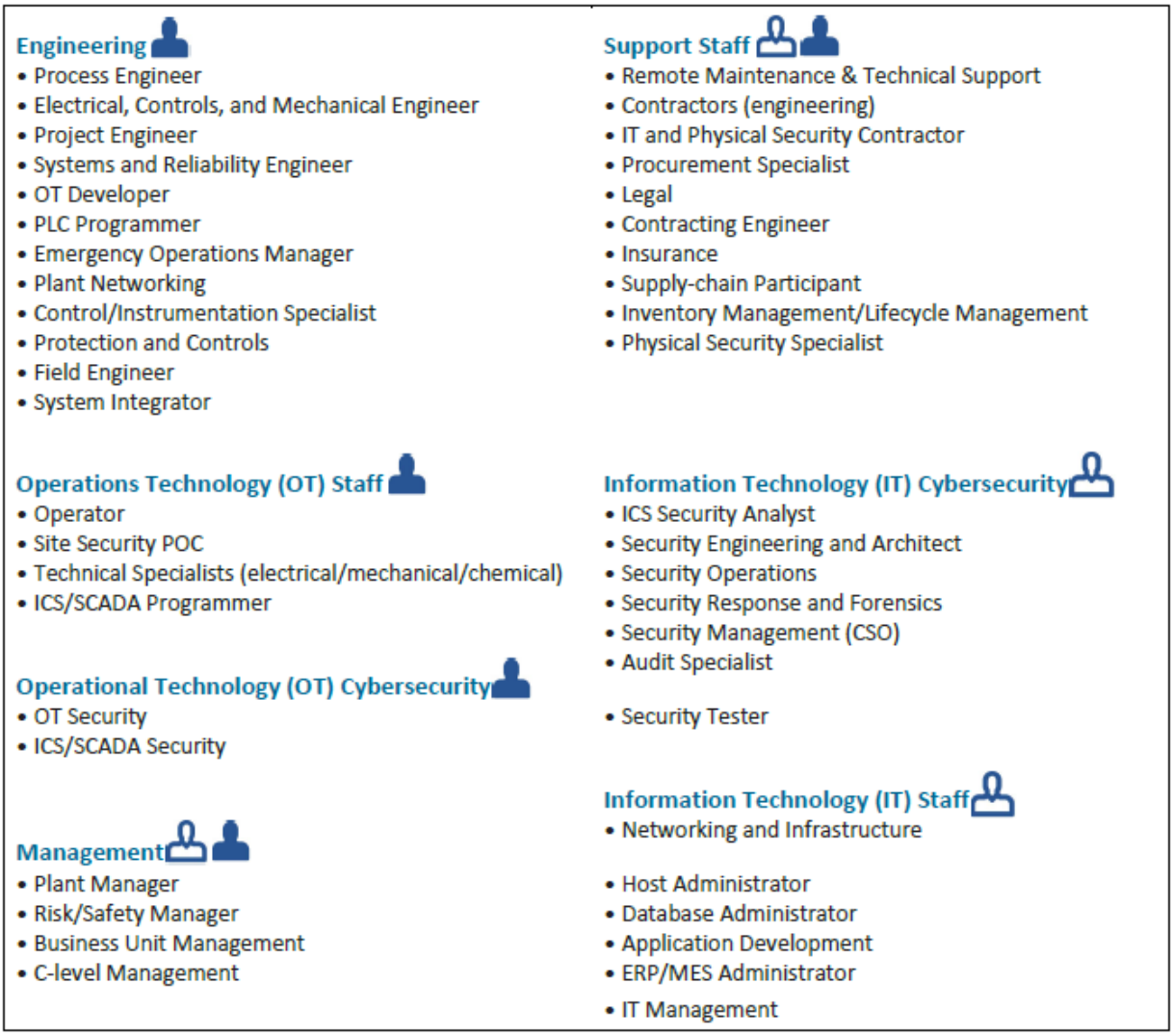
Artifacts Associated with Loss of Productivity and Revenue Technique (T0828)	
Artifact 1	Loss of Confidence in a Safety System Due to Unreliability Might Result in a Risk Management Driven Shutdown of a Plant
Artifact 2	Wormable or Other Highly Propagating Malware Might Result in the Shutdown of a Plant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

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

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 1	Program Execution
Artifact 2	Telnet Port 23
Artifact 3	SFTP Port 22
Artifact 4	FTPS Port 990
Artifact 5	SMB Port 139, 445
Artifact 6	HTTP Port 80
Artifact 7	HTTPS Port 443
Artifact 8	Command Line Arguments
Artifact 9	SCP Port 22
Artifact 10	Memory Corruption
Artifact 11	Files Moved to Recycle Bin
Artifact 12	Non-Native Files
Artifact 13	Transient Device Connections
Artifact 14	External Network Connections
Artifact 15	Local Network Connections
Artifact 16	Host System Reboot Failure
Artifact 17	Process Logic Failure
Artifact 18	Event Log Creation
Artifact 19	System Call
Artifact 20	System Application Interruption
Artifact 21	Device Failure
Artifact 22	Recovery Attempt Failure
Artifact 23	File Encryptions
Artifact 24	Missing Files
Artifact 25	Use of File Transfer Protocols
Artifact 26	FTP Port 20, 21
Artifact 27	TFTP Port 60

APPENDIX C: OBSERVERS

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



REFERENCES

[1] [Industrial Cybersecurity Pulse | Gary Cohen | “Throwback Attack: WannaCry ransomware takes Renault-Nissan plants offline” | https://www.industrialcybersecuritypulse.com/throwback-attack-wannacry-ransomware-takes-renault-nissan-plants-offline/ | 22 April 2021 | Accessed on 16 March 2022 | The source is publicly available information and does not contain classification markings]

[2] [Nick Ismail | “The Real Damage of a Ransomware Attack is Felt in the Downtime” | https://www.information-age.com/real-damage-ransomware-attack-felt-downtime-123466541/ | 1 June 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[3] [Broadcom | Charles Cooper | “WannaCry: Lessons Learned 1 Year Later” | https://symantec-enterprise-blogs.security.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later | 15 May 2018 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[4] [Trend Micro | “Shadow Brokers Leaks Hacking Tools: What it Means for Enterprises” | https://www.trendmicro.com/vinfo/mx/security/news/vulnerabilities-and-exploits/shadow-brokers-leaks-hacking-tools-what-it-means-for-enterprises | 18 April 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[5] [Cybersecurity and Infrastructure Security Agency | “Multiple Ransomware Infections Reported” | https://www.cisa.gov/uscert/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported | 15 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[6] [Poland CERT | Kamil Frankowicz | “WannaCry” | https://www.cert.pl/posts/2017/05/wannacry-ransomware/ | 15 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[7] [Poland CERT | Kamil Frankowicz | “WannaCry” | https://www.cert.pl/posts/2017/05/wannacry-ransomware/ | 15 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[8] [Washington Post | Ellen Nakashima and Craig Timberg | “NSA officials worried about the day its potent hacking tool would get loose, then it did” | https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html | 16 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[9] [The Atlantic | Bruce Schneier | “Who are the Shadow Brokers” | https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/ | 23 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[10] [Kamil Frankowicz | “WannaCry Ransomware” | https://frankowicz.me/wannacry-ransomware/ | 15 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[11] [Cybersecurity and Infrastructure Security Agency | “Alert TA17-132A: Indicators Associated With WannaCry Ransomware” | https://www.cisa.gov/uscert/ncas/alerts/TA17-132A | 12 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[12] [Industrial Cybersecurity Pulse | Gary Cohen | “Throwback Attack: WannaCry ransomware takes Renault-Nissan plants offline” | https://www.industrialcybersecuritypulse.com/throwback-attack-wannacry-ransomware-takes-renault-nissan-plants-offline/ | 22 April 2021 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[13] [Reuters | “Renault-Nissan resumes nearly all production after cyber attack” | https://www.reuters.com/article/us-cyber-attack-renault/renault-nissan-resumes-nearly-all-production-after-cyber-attack-idUSKCN18B0S5 | 15 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[14] [France24 | “France’s Renault hit in worldwide ‘ransomware’ cyber attack” | https://www.france24.com/en/20170512-cyberattack-ransomware-renault-worldwide-british-hospitals | 14 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[15] [LogRhythm | Erika Noerenberg, Andrew Costis, and Nathanial Quist | “A Technical Analysis of WannaCry Ransomware” | https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/ | 16 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[16] [LogRhythm | Erika Noerenberg, Andrew Costis, and Nathanial Quist | “A Technical Analysis of WannaCry Ransomware” | https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/ | 16 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[17] [Mandiant | Alex Berry, Josh Homan, and Randi Eitzman | “WannaCry Malware Profile” | https://www.mandiant.com/resources/wannacry-malware-profile | 23 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[18] [Vipre | “WannaCry Technical Analysis” | https://support.threattracksecurity.com/support/solutions/articles/1000250396-wannacry-technical-analysis | 26 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[19] [Mandiant | Alex Berry, Josh Homan, and Randi Eitzman | “WannaCry Malware Profile” | https://www.mandiant.com/resources/wannacry-malware-profile | 23 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[20] [LogRhythm | Erika Noerenberg, Andrew Costis, and Nathanial Quist | “A Technical Analysis of WannaCry Ransomware” | https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/ | 16 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[21] [Mandiant | Alex Berry, Josh Homan, and Randi Eitzman | “WannaCry Malware Profile” | https://www.mandiant.com/resources/wannacry-malware-profile | 23 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[22] [LogRhythm | Erika Noerenberg, Andrew Costis, and Nathanial Quist | “A Technical Analysis of WannaCry Ransomware” | https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/ | 16 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[23] [Mandiant | Alex Berry, Josh Homan, and Randi Eitzman | “WannaCry Malware Profile” | https://www.mandiant.com/resources/wannacry-malware-profile | 23 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[24] [Mandiant | Alex Berry, Josh Homan, and Randi Eitzman | “WannaCry Malware Profile” | https://www.mandiant.com/resources/wannacry-malware-profile | 23 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[25] [Vipre | “WannaCry Technical Analysis” | https://support.threattracksecurity.com/support/solutions/articles/1000250396-wannacry-technical-analysis | 26 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[26] [Mandiant | Alex Berry, Josh Homan, and Randi Eitzman | “WannaCry Malware Profile” | https://www.mandiant.com/resources/wannacry-malware-profile | 23 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[27] [Mandiant | Alex Berry, Josh Homan, and Randi Eitzman | “WannaCry Malware Profile” | https://www.mandiant.com/resources/wannacry-malware-profile | 23 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[28] [Mandiant | Alex Berry, Josh Homan, and Randi Eitzman | “WannaCry Malware Profile” | https://www.mandiant.com/resources/wannacry-malware-profile | 23 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]

[29] [Vipre | “WannaCry Technical Analysis” | https://support.threattracksecurity.com/support/solutions/articles/1000250396-wannacry-technical-analysis | 26 May 2017 | Accessed on 1 March 2022 | The source is publicly available information and does not contain classification markings]