PRECURSOR ANALYSIS REPORT: NOTPETYA MALWARE ATTACK ON AP MOLLER-MAERSK 2017

Cybersecurity for the Operational Technology Environment (CyOTE)

30 JUNE 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-69495

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: NOTPETYA MALWARE ATTACK ON AP MOLLER-MAERSK 2017

1. EXECUTIVE SUMMARY

The NotPetya Malware Attack on AP Moller-Maersk 2017 Precursor Analysis Report leverages publicly available information about the attack and catalogs anomalous observables for each technique employed by the adversary. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

NotPetya is a destructive malware that targeted Windows systems and masqueraded as a ransomware. It irreversibly encrypted computer systems in at least 65 countries and caused an estimated $10 billion in damages.[1,2,3]

Advesaries deployed the malware through a compromised software update for MEDoc tax accounting software that was released on 22 June 2017 for customers to download.[4,5,6,7,8]

NotPetya lay dormant until 27 June, when it began to propagate across networks that had installed the infected MEDoc update. Ukraine was the epicenter of the attack, with Ukrainian organizations suffering 75 precent of the total reported infections.[9,10]

One of the early victims was AP Moller-Maersk (Maersk), a Danish container shipping company that transports 20 percent of the world's trade. Maersk's Ukrainian office downloaded the infected MEDoc update to a server when the update was released on 22 June. When NotPetya was triggered on 27 June, it spread throughout Maersk's networks in seven minutes and then encrypted the infected systems, taking down the company's entire global computer infrastructure within an hour and forcing Maersk to resort to manual operations.[11,12,13]

While Maersk was able to restore global applications and some business functions in 13 days, it was several weeks before all systems were fully restored. The company had to rebuild its entire computing infrastructure, replacing 49,000 computers and 3,500 of 6,200 servers.[14,15,16,17]

NotPetya also impacted Maersk's operational technology (OT) infrastructure, which controls the automated processes for vessels, cranes, warehouse systems, and ports. Seventeen of Maersk's port terminals experienced operability problems with cranes and terminal scanning gates. Shipping, tugboat, and oil tanker operations also suffered after the malware spread to vessel computer systems used to communicate with ports.[18,19,20,21,22]

In terms of financial losses, Maersk's former Chief Technical and Information Officer reported in 2019 that the NotPetya attack cost the company $350 million, including $30 million in recovery costs.[23]

Researchers and analysts identified 19 unique techniques (used in a sequence of 31 steps) likely utilized during the attack with a total of 112 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Twenty-three of the identified techniques used during the Maersk cyber attack were precursors to the triggering event. Analysis identified 102 observables associated with these precursor techniques, 22 of which were

assessed to have an increased likelihood of being perceived in the 5 days preceding the triggering event. Due to the speed and nature of this attack, reducing response and comprehension time is challenging; however, it underscores the importance of maintaining situational awareness of network changes and effective incident response capabilities. 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 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, 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.

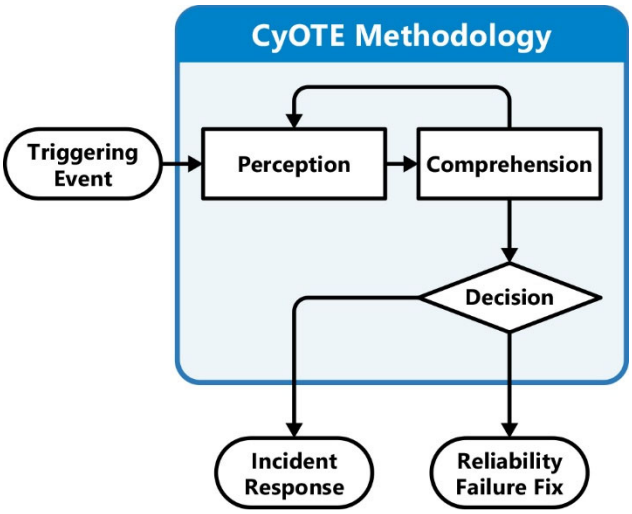


Figure 1. CyOTE Methodology

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 case study's 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 to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

The Danish global shipping company AP Moller-Maersk (Maersk) was among the many victims of the NotPetya malware campaign that began in late June 2017. NotPetya is a destructive malware designed to encrypt Windows systems and render them inoperable while masquerading as a ransomware. NotPetya infected systems in at least 65 countries and caused an estimated $10 billion in damages.[24,25]

NotPetya infected Maersk and other victims through an update of MEDoc tax softare released on 22 June 2017 (D-5), when the infected update was downloaded to a server in Maersk's Ukrainian office.[26,27]

When the global NotPetya attack was triggered at around 5:00 AM EDT on 27 June (D-0), the malware spread through Maersk's network in seven minutes (M+7) and encrypted infected systems in about an hour (H+1).[28,29] By 06:21 EDT, Maersk's global IT infrastructure, as well as many operational technology (OT) systems essential to operations, had been disabled.[30,31]

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 initial infection vector was the installation of the infected MEDoc software update, which was installed on a server in Maersk's Ukrainian office on 22 June (D-5). An administrator accessed the server on 26 June, the day prior to the triggering event (D-0), which allowed NotPetya to harvest their credentials, facilitating the malware's propagation through Maersk's network.[32,33]

Maersk personnel likely first became aware of the attack during the triggering event (D+0) when NotPetya rebooted computer systems and, after rebooting, displayed a fake CHKDSK screen, indicating disk errors were being repaired. This masquerade was intended to fool users into believing a legitimate process was underway, buying the malware time to propagate and then encrypt infected systems before a cybersecurity response could be mounted. As its final act while infected systems were encrypted, NotPetya displayed a fake ransom note.[34]

In addition to disabling the company's IT systems, NotPetya had a severe impact on Maersk's OT

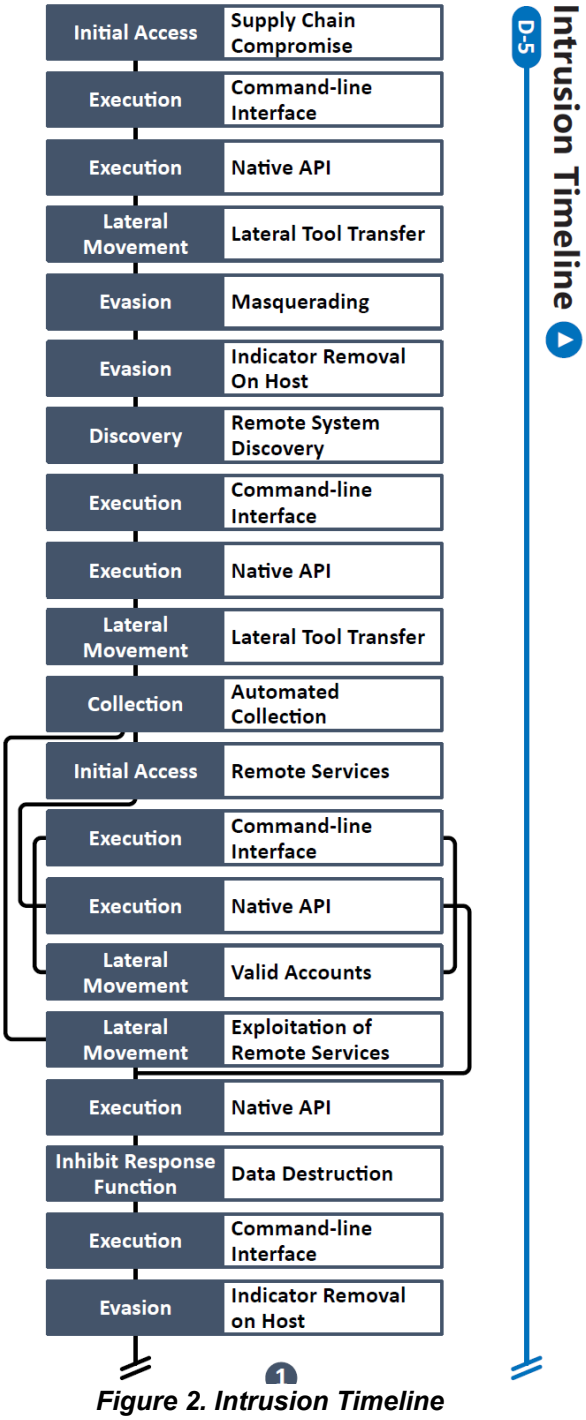


Figure 2. Intrusion Timeline

systems. The company relies heavily on automated processes for vessel, crane, warehouse, and port operations, and 17 of the company's port terminals suffered operability impacts to cranes and terminal scanning gates. Maersk's shipping, tugboat, and oil tanker operations also experienced problems after the malware spread to vessel computer systems used to communicate with ports.[35,36,37,38]

Maersk did not gain full comprehension of the attack until three days later (D+3), when company staff and cyber forensics experts from a local security company reverse engineered NotPetya to understand how the malware worked. Thirteen days after the triggering event (D+13), the company was able to restore all global applications and some business functions, although it was several weeks before all systems were fully restored.[39,40]

NotPetya's financial impact on Maersk was severe: in 2019, Maersk's former Chief Technical and Information Officer (CTIO) reported that NotPetya cost the company $350 million, including $30 million in recovery costs.[41] The attack forced Maersk to rebuild its entire network infrastructure, replacing 49,000 computers and 3,500 of 6,200 servers that could not be restored.[42,43,44]

Analysis identified 19 unique techniques (used in a sequence of 31 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 ICS framework.

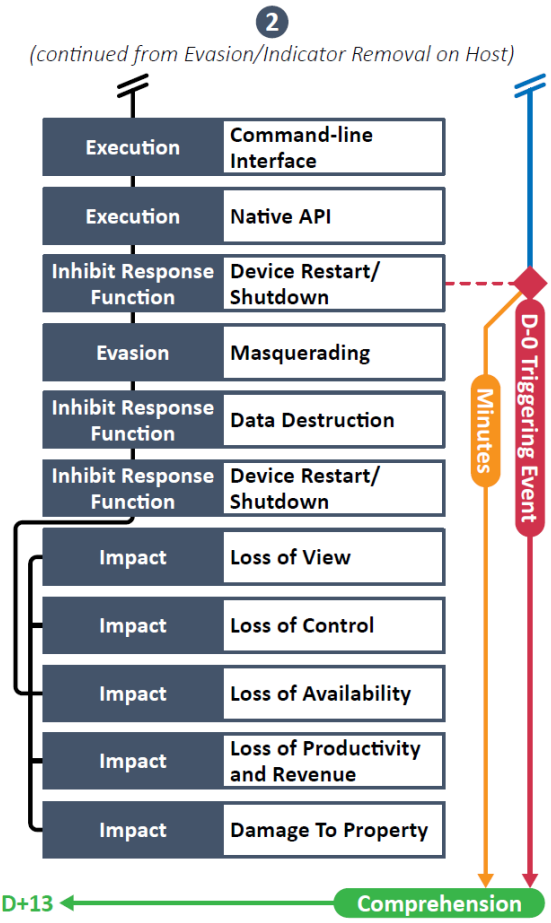


Figure 3. Intrusion Timeline (CONTD.)

Table 1. Techniques Used in the NotPetya Malware Attack on AP Moller-Maersk 2017

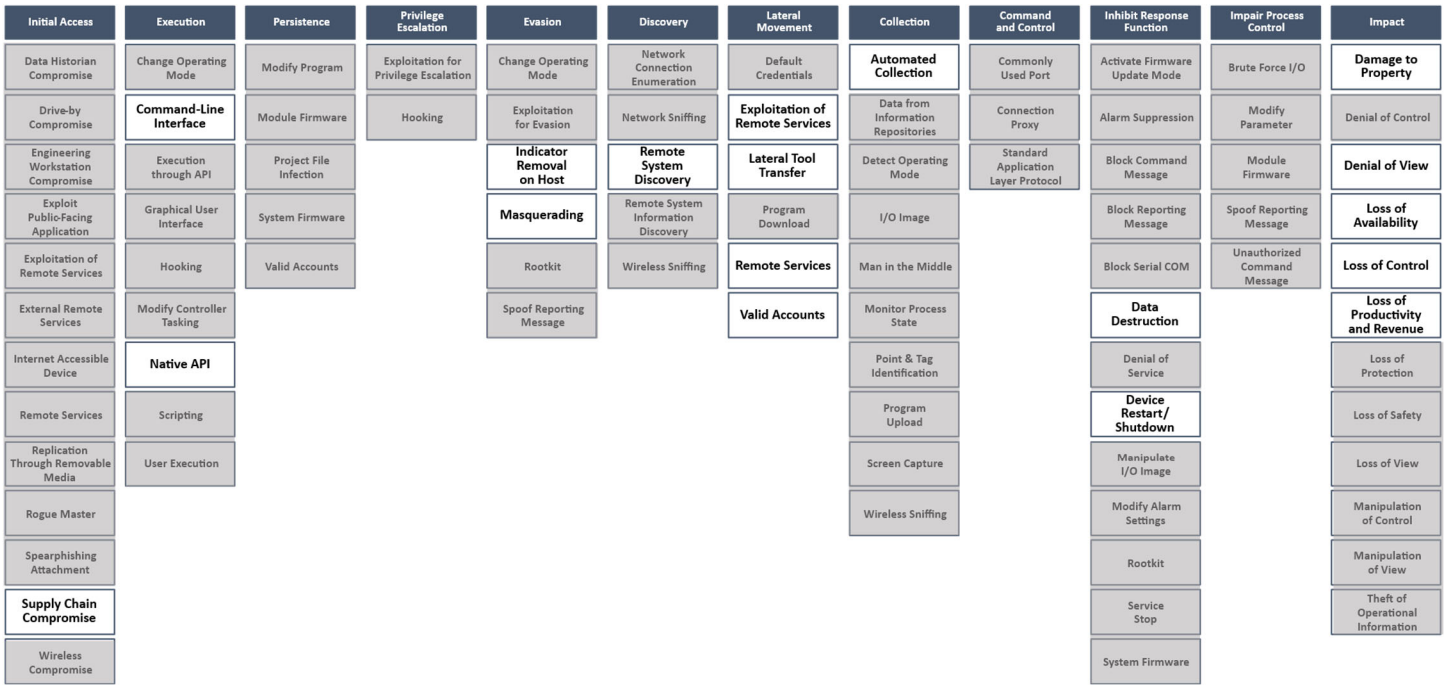


Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	31
Technique Observables	112
Precursor Techniques	23
Precursor Technique Observables	102
Highly Perceivable Precursor Technique Observable	21

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. SUPPLY CHAIN COMPROMISE TECHNIQUE (T0862) FOR INITIAL ACCESS

The initial infection vector for NotPetya was via the Supply Chain Compromise technique (T0862) targeting MEDoc's software update process. The adversary compromised multiple MEDoc systems and installed a backdoor in a DLL of the MEDoc software update that could be used to gather data and execute arbitrary code. The update was released on 22 June 2017.[45,46,47,48,49]

The adversary also gained control of MEDoc's update server, which appeared to be the initial mechanism for delivering the NotPetya malware.[50] Microsoft Security Response and Forensics experts observed telemetry data around 6:30 AM EDT on 27 June that contained a command to execute a process in the MEDoc software to load and execute the malicious file, perfc.dat, which ultimately led to the NotPetya infections.[51]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of six observables were identified with the use of the Supply Chain Compromise technique (T0862). This technique is important for investigation, as it identifies the initial infection vector. This technique appears early in the attack timeline. Terminating the chain of techniques at this point would likely prevent the malware from spreading to local systems and encrypting infected hosts.

Of the six observables associated with this technique, two are assessed as highly perceivable. They are italicized and marked † in Appendix A.[52]

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 31 artifacts could be generated by the Supply Chain Compromise technique
Technique Observers[a]	OT Cybersecurity, IT Cybersecurity, Engineering, 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. COMMAND-LINE INTERFACE TECHNIQUE (T0807) FOR EXECUTION

Microsoft observed the MEDoc software issue, a malicious command, via the Command-Line Interface technique (T0807) from telemetry data collected on the morning of the attack. A command-line interface was used to call a Windows API to install the malicious DLL, perfc.dat, on the victim's system.[53,54]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of five observables were identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation because it provides a record of actions taken during the initial infection. This technique appears early in the attack timeline. Terminating the chain of techniques at this point would likely invalidate two of NotPetya's four initial infection vectors (PsExec, WMIC, EternalBlue, and EternalRomance), as PsExec and Windows Management Instrumentation Command-line (WMIC) use command-lines to issue API calls to access and infect systems on local networks.[55] This technique modifies the host operating system files, resulting in the host being placed into a modified or compromised state. If system backups are created after this technique is executed, then data recovery and disaster recovery efforts will be impaired.

Of the five observables associated with this technique, two are assessed as highly perceivable. They are italicized and marked † in Appendix A.[56,57]

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 25 artifacts could be generated by the Command Line Interface technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

3.3. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

The adversary used a command line to call the Windows API, rundll32.exe, to install and run the malicious DLL on the victim's system.[58,59]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of four observables were identified with use of the Native API technique (T0834). This technique is important for investigation because it enables changes to the underlying operating system and enables interaction between the malware and native resources on the host. This technique appears early in the attack timeline. Terminating the chain of techniques at this point would likely invalidate two of NotPetya's initial infection vectors, as PsExec and WMIC use API calls to access and infect systems on the local network.[60]

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 25 artifacts could be generated by the Native API technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

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

The malicious DLL, perfc.dat, was installed and executed on the victim's system via the Lateral Tool Transfer technique (T0867).[61] Malicious DLL delivery and execution for the NotPetya malware could occur in five different ways: by initial network infection, resulting from supply chain infection; by infection from the local network via PsExec; by infection from the local network via WMIC; by infection from the local network via EternalBlue; or by infection from the local network via EternalRomance.[62] Once perfc.dat is installed, it drops the PsExec utility, dllhost.dat, but under a different name.[63]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of five observables were identified with use of the Lateral Tool Transfer technique (T0867). This technique is important for investigation to understand some aspects of the initial infection vector. This technique is employed early in the attack timeline. Terminating the chain of techniques at this point, prior to the installation of perfc.dat, would likely prevent initial infection, system encryption, and prevent the malware from spreading.[64,65,66]

Of the five observables associated with this technique, two are assessed to be highly perceivable. They are italicized and marked † in Appendix A .[67]

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 22 artifacts could be generated by the Lateral Tool Transfer technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

3.5. MASQUERADING TECHNIQUE (T0849) FOR EVASION

Once the main DLL, perfc.dat is installed, it drops the PsExec utility under the name dllhost.dat. The adversary's use of the file name dllhost.dat is likely an attempt at masquerading the identity of the PsExec utility by naming it something else. The file name dllhost.dat is similar in name to the legitimate file, dllhost.exe.[68,69,70]

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of one observable was 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 early in the attack timeline. Terminating the chain of techniques at this point after the initial infection would likely limit the spread of the malware and prevent the victim's system from being encrypted.

The one observable associated with this technique is not highly perceivable. It is located in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 15 artifacts could be generated by the Masquerading technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

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

The NotPetya malware employs the Indicator Removal on Host technique (T0872) shortly after installation. The malware reads itself into process memory before overwriting the original DLL, perfc.dat, with null bytes and removing itself from disk. The adversary likely removed the original DLL file for evasion purposes.[71,72]

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of five observables were identified with the use of the Indicator Removal on Host technique (T0872).[73] This technique is important for investigation because it obscures adversarial activity and limits recovery of compromised assets by defenders. This technique appears early in the attack timeline. Terminating the chain of techniques at this point would likely prevent the malware from spreading to other systems and encrypting critical files. This technique modifies the host operating system files, resulting in the host being placed into a modified or compromised state. If system backups are created after this technique is executed, then data recovery and disaster recovery efforts will be impaired.

The five observables associated with this technique are not highly perceivable. They are located in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 23 artifacts could be generated by the Indicator Removal on Host technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

3.7. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

The NotPetya malware employed the Remote System Discovery technique (T0846) by using a command-line interface to call Windows APIs and collect information about the victim's environment. The collected data includes network connection addresses, privileges assigned to the host's account, and running processes on the host system.[74,75]

The malware used data collected from the victim's environment to establish an operating procedure for spreading to other systems on the local network. For example, the malware would not employ the use of EternalBlue or EternalRomance exploits if, during system discovery, the malware detected specific antivirus solutions actively running on the system.[76,77]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of 13 observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation to identify how the malware collects information about the host's system and uses this data to tailor its operating procedure, as well as to spread to other systems on the local network. This technique appears early in the attack timeline. Terminating the chain of techniques at this point would likely prevent the malware from spreading to other systems and encrypting critical files.

The 13 observables associated with this technique are not highly perceivable. They are located 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	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

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

The malware used the Command-Line Interface technique (T0807) to call Windows APIs to collect information about the victim's system.[78]

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of one observable was identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation as it shows the types of information the malware was focused on collecting, as well as how the data was collected. This technique appears early in the attack timeline. Terminating the chain of techniques at this point would likely limit the spread of the malware to other systems and prevent encryption of critical files.

The one observable associated with this technique is assessed to be highly perceivable. It is italicized and marked † in Appendix A.[79]

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 25 artifacts could be generated by the Command-Line Interface technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

3.9. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

NotPetya employed the Native API technique (T0834) to collect data about the victim's environment, including network connection addresses, privileges assigned to the host's account, and running processes on the host system.[80,81]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of 13 observables were identified with the use of the Native API technique (T0834).[82,83,84,85,86] This technique is important for investigation because it enables adversary access of victim networks as well as persistence. This technique appears early in the attack timeline. Terminating the chain of techniques at this point would likely limit system discovery efforts and challenge the malware's ability to infect other systems and encrypt critical files.

The 13 observables associated with this technique are not highly perceivable. They are located in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 25 artifacts could be generated by the Native API technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

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

NotPetya used data collected during system discovery for the Lateral Tool Transfer technique (T0867). The malware evaluates user privileges to determine if the variant of the Mimikatz tool it employs would be dropped onto victim systems. The Mimikatz variant is only dropped if NotPetya inherits a sufficient level of privileges based on access granted to the user account the malware has coopted. The Mimikatz variant harvests credentials and tokens, typically stored in the form of hashes or clear text, to facilitate authenticated connections to other systems on the local network.[87,88]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of four observables were identified with the use of the Lateral Tool Transfer technique (T0867). This technique is important for investigation to understand how the malware collects data to facilitate propagation through local networks. This technique appears early in the attack timeline. Terminating the chain of techniques at this point would likely prevent the malware from dropping the Mimikatz variant. The malware's ability to spread without the Mimikatz variant would be dependent on other environmental factors, such as the victim's patch status against the EternalBlue and EternalRomance exploits.[89,90]

The four observables associated with this technique are not highly perceivable. They are located in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 22 artifacts could be generated by the Lateral Tool Transfer technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

3.11. AUTOMATED COLLECTION TECHNIQUE (T0802) FOR COLLECTION

NotPetya employed the Automated Collection technique (T0802) by using the Mimikatz variant to steal credentials via a piped command that automated data transfer, facilitating unauthorized authenticated connections to systems on the local network.[91,92]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of three observables were identified with the use of the Automated Collection technique (T0802). This technique is important for investigation because it enables data collection as well as persistence. This technique appears early in the attack timeline. Terminating the chain of techniques at this point would likely invalidate two of the methods NotPetya uses to spread to other systems on the local network. The malware's ability to spread without the Automated Collection technique would be dependent on other environmental factors, such as the victim's patch status against the EternalBlue and EternalRomance exploits.[93,94]

The three observables associated with this technique are not highly perceivable. They are located in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 23 artifacts could be generated by the Automated Collection technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

3.12. REMOTE SERVICES TECHNIQUE (T0886) FOR LATERAL MOVEMENT

NotPetya employed the Remote Services technique (T0886) by using the Windows command-line interface to call remote services, PsExec and WMIC, leveraging stolen credentials to access local systems on the network.[95,96]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of six observables were identified with the use of the Remote Services technique (T0886). This technique is important for investigation because it enables persistence and enables the access of additional hosts within victim networks. This technique occurs near the mid-point of the attack timeline. Terminating the chain of techniques at this point would likely invalidate these two methods used by the malware to spread locally.[97,98,99,100,101]

Of the six observables associated with this technique, three are assessed to be highly perceivable. They are italicized and marked † in Appendix A.[102,103]

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 24 artifacts could be generated by the Remote Services technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

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

NotPetya employed the Command-Line Interface technique (T0807) to access and spread to systems on the local network using data collected from the host's environment, including IP addresses and user credentials. Commands were issued from PsExec and WMIC utilities to remotely access local systems on the network.[104,105,106]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel might have been able to observe this technique.

A total of three observables were identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation because it enables adversaries to control compromised hosts, spreading malware to additional hosts within the victim's operating environment. This technique is used near the mid-point of the attack timeline. Terminating the chain of techniques at this point would likely invalidate these two methods the malware used to spread locally.[107,108]

Of the three observables associated with this technique, two are assessed as highly perceivable. They are italicized and marked † in Appendix A.[109,110,111]

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 25 artifacts could be generated by the Command-Line Interface technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

3.14. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

NotPetya employed the Native API technique (T0834) to call Windows API, rundll32.exe, to load and run the malicious DLL via remote services PsExec and WMIC on local systems.[112,113,114,115]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of one observable was 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 malware. This technique appears near the mid-point of the attack timeline. Terminating the chain of techniques at this point would likely inhibit the malware's ability to issue commands to the PsExec and WMIC utilities. This would limit two of the four methods used by the malware to spread locally.[116,117]

The one observable associated with this technique is not highly perceivable. It is located in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 25 artifacts could be generated by the Native API technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

3.15. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

NotPetya employs the Valid Accounts technique (T0859) to gain access and spread to other systems on local networks. Command-lines are used to pass stolen credentials to local systems to gain unauthorized authenticated remote access, with the WIMC and PsExec utilities issuing commands to load and execute malicious code on local network systems.[118,119,120]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of two observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation to understand how the malware rapidly spreads across local networks. This technique occurs at the mid-point of the attack timeline. Terminating the chain of techniques at this point would likely invalidate these two methods used by NotPetya to access and spread to systems on the local network.[121,122]

Of the two observables associated with this technique, both are assessed to be highly perceivable They are italicized and marked † in Appendix A.[123,124]

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	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

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

NotPetya employed the Exploitation of Remote Services technique (T0866) by using EternalBlue (CVE-2017-0144) and EternalRomance (CVE-2017-0145) exploits to gain initial access to vulnerable systems and deliver NotPetya's malicious DLL.[125]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel might have been able to observe this technique.

A total of ten observables were identified with the use of the Exploitation of Remote Services technique (T0866). This technique is important for investigation to understand how the malware spreads through local networks. This technique appears near the end of the attack. Terminating the chain of techniques at this point would essentially prevent the malware from using the EternalBlue and EternalRomance exploits, which would invalidate these two methods used by the malware to spread locally.[126,127]

Of the ten observables associated with this technique, six are assessed to be highly perceivable. They are italicized and marked † in Appendix A.[128,129]

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

3.17. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

NotPetya employed the Native API technique (T0834) to encrypt files by overwriting existing files using Windows APIs after attempting to spread to other systems on the local network. The malware used Salsa20 for Master Boot Record (MBR) encryption and AES-128 for file encryption.[130,131,132]

OT Cybersecurity, IT Cybersecurity, Engineering, and IT Staff personnel may have been able to observe this technique.

A total of two observables were identified with the use of the Native API technique (T0834). This technique is important for investigation to understand how the malware encrypts system files. This technique appears at the end of the attack timeline. Terminating the chain of techniques at this point in the attack would terminate the process used to encrypt system files, reducing the impact of the malware. This technique modifies the host operating system files, resulting in the host being placed into a modified or compromised state. If system backups are created after this technique is executed, the data recovery and disaster recovery efforts will be impaired.

The two observables associated with this technique are not highly perceivable. They are located in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 25 artifacts could be generated by the Native API technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff

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

NotPetya employed the Data Destruction technique (T0809) by encrypting system files in two phases. The first phase of the encryption process overwrote user files and part of the MBR with a custom boot loader program that activated upon reboot of the infected system.[b] The custom boot loader program, which uses BIOS interruption calls to execute tasks, would boot the system without using Windows, encrypt the master file table, display a fake CHKDSK screen during the final step in the encryption process, and display a fake ransom note.[133]

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of eight observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because it encrypts victim files, rendering systems inoperable and effectively destroying data. This technique appears late in the attack timeline. Terminating the chain of techniques at this point, before the first sector of the MBR is overwritten, would likely prevent the compromise of the MBR booting process and the encryption of other files on the system, ultimately preventing data destruction.

The eight observables associated with this technique are not highly perceivable. They are located in Appendix A.

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

[b] It is important to note that NotPetya could employ different encryption methods depending on the victim environment and would execute encryption protocols based on inherited permissions and antivirus solutions running on the system.

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

NotPetya employed the Command-Line Interface technique (T0807) to spawn a cmd.exe via command-line interface to issue a command to delete Windows Event Logs.[134,135]

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of one observable was 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 and destroy evidence of malicious activity. This technique appears late in the attack timeline. Terminating the chain of techniques at this point would likely prevent the malware from executing the deletion command to erase Windows Event Logs. This technique modifies the host operating system files, resulting in the host being placed into a modified or compromised state. If system backups are created after this technique is executed, the data recovery and disaster recovery efforts will be impaired. Responding to this technique would likely not prevent system encryption without prior mitigation efforts, since the first sector of the MBR would already have been overwritten with a custom boot program and the final phase of the encryption process would initiate upon restart.[136,137]

The one observable associated with this technique is assessed to be highly perceivable. It is italicized and marked † in Appendix A.[138]

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 25 artifacts could be generated by the Command-Line Interface technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

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

NotPetya employed the Indicator Removal on Host technique (T0872) to delete Windows Event Logs via the command-line interface. Windows Event Logs include Setup logs, System logs, Security logs, Application logs, and an update sequence number (USN) change journal.[139] The adversary likely used this technique to hide some of the malware's activities in case encryption was not successful.

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of one observable was identified with the use of the Indicator Removal on Host technique (T0872). This technique is important for investigation because it limits detection and recovery of victim assets by defenders. This technique appears late in the attack timeline. Terminating the chain of techniques at this point would likely prevent the malware from executing the deletion command to erase Windows Event Logs. Terminating the attack prior to deletion would make forensic or incident response easier, as evidence would remain intact on the host system. However, it is unlikely that terminating the attack here would prevent system encryption without some prior mitigation efforts, since the first sector of the MBR has already been overwritten with a custom boot program. The final phase of the encryption process would initiate upon restart.[140,141]

The one observable associated with this technique is not highly perceivable. It is located in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 23 artifacts could be generated by the Indicator Removal on Host technique
Technique Observers	Cybersecurity, IT Cybersecurity, IT Staff

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

NotPetya employed the Command-Line Interface technique (T0807) to call a Windows API to reboot the host system.[142,143]

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of three observables were identified with the use of the Command-Line Interface technique (T0807). This technique is important for investigation because it allows adversaries to control victim hosts and remove indicators, thwarting detection and recovery attempts. because it allows adversaries to control victim hosts and remove indicators, thwarting detection and recovery attempts. This technique appears late in the attack timeline. Terminating the chain of techniques at this point may prevent the command-line interface, which is used to reboot the host system, from spawning. However, this would not guarantee the host system would not be rebooted via other methods.[144,145]

Of the three observables associated with this technique, one is assessed to be highly perceivable. It is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 25 artifacts could be generated by the Command-Line Interface technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

3.22. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

NotPetya employed the Native API technique (T0834) by calling a Windows API via command-line interface to restart the victim's system.[146] In the event the system fails to restart, the malware can issue a different, undocumented Windows API to help ensure a restart.[147]

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of three observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because it enables adversary control of victim devices. This technique appears late in the attack timeline. Terminating the chain of techniques at this point may prevent Windows APIs from being called to restart the victim's system, which in theory could delay the final phase of the encryption process.[148,149] It is unlikely that terminating the attack chain here would prevent system encryption without incident response efforts to fix the corrupted MBR, since the final encryption method would initiate immediately following a reboot.[150]

The three observables associated with this technique are not highly perceivable. They are located in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 25 artifacts could be generated by the Native API technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

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

Upon restart, the victim's system would load the modified boot program and initiate the final stage of the encryption process via the Device Restart/Shutdown technique (T0816).[151,152,153] The unscheduled shutdown of infected hosts is assessed to be the Triggering Event, which is the first obvious indication to victims that there is a problem with their systems.

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of two observables were 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. This technique appears late in the timeline and responding to it may halt the execution and spread of NotPetya. Terminating the chain of techniques at this point in the attack may prevent the victim's system from being restarted, which could delay the final phase of the encryption process. It is unlikely this intervention would prevent system encryption without incident response efforts to fix the corrupted MBR, since the final encryption method would initiate immediately following a reboot.[154,155]

Both 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 17 artifacts could be generated by the Device Restart/Shutdown technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

3.24. MASQUERADING TECHNIQUE (T0849) FOR EVASION

NotPetya employs the Masquerading technique by displaying a fake CHKDSK screen (error screen) after a forced reboot, instructing the user to not shutdown the system in hopes of preventing the user from power cycling the system during the final phase of the encryption process. During this time, the malware's custom boot program encrypts the infected system's master file table.[156,157]

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of one observable was identified with the use of the Masquerading technique (T0816). This technique is important for investigation because it circumvents critical security tools that can alert a victim of malicious cyber activity. This technique appears late in the attack timeline. Terminating the chain of techniques at this point would interrupt the final stage of the encryption process; however, it is unclear what impact this would have on the overall encryption process.[158,159]

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 15 artifacts could be generated by the Masquerading technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

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

NotPetya employs the Data Destruction technique (T0809) during the final phase of the encryption process, when the initially modified MBR code directs the encryption of the master file table on the victim's system.[160] During final encryption, a fake CHKDSK screen (error screen), associated with the Masquerading technique (T0849), is displayed until the victim's system is restarted for a second and final time.[161,162]

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

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 at the very end of the attack timeline. Terminating the chain of techniques at this point would interrupt the final stage of the encryption process; however, it is unclear what impact this would have on the overall encryption process.[163,164]

The three observables associated with this technique are not highly perceivable. They are located in Appendix A.

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

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

The last step in the master file table encryption process is the Device Restart/Shutdown technique (T0816). Following a second and final system reboot, NotPetya displays its fake ransom note.[165,166]

OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have been able to observe this technique.

A total of one observable was identified with the use of the Device Restart/Shutdown technique (T0816). This technique is important for investigation because it renders victim operating assets unusable and destroys critical data. This technique appears at the end of the attack timeline. Terminating the chain of techniques at this point would likely have no impact on malware operation. Security researchers agree that following the final reboot, decrypting infected systems is not feasible, as the decryption key is overwritten during the encryption process.[167,168,169,170]

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 17 artifacts could be generated by the Device Restart/Shutdown technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

3.27. LOSS OF VIEW TECHNIQUE (T0829) FOR IMPACT

The Loss of View technique (T0829) leaves NotPetya victims with inoperable systems that no longer boot to Windows because critical system files have been encrypted without a decryption mechanism.[171,172]

OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff, and OT Staff personnel may have been able to observe victim reports of inoperable systems.[c]

A total of one observable was identified with the use of the Loss of View technique (T0829). This technique is important for investigation because it prevents owners and operators from delivering products or services. This technique appears at the end of the timeline, beyond the point at which a defender could take action to disrupt the attack. Terminating the chain of techniques at this point would not limit destruction or business impacts.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 4 artifacts could be generated by the Loss of View technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff, OT Staff

[c] For at least the techniques covered in sections 3.27 through 3.29, most or all company personnel would likely perceive the effects of the malware encrypting infected systems and the resulting impact on company operations. However, for the purposes of this case study, only IT, OT, and Engineering staff who could directly observe system or network activity related to the attack, and in some situations potentially respond to it are specifically listed.

3.28. LOSS OF CONTROL TECHNIQUE (T0827) FOR IMPACT

The Loss of Control technique (T0827) leaves victims with inoperable systems that no longer boot to Windows because critical system files have been encrypted without a decryption mechanism, and impacted systems can no longer execute applications, send commands, or receive commands.[173,174]

OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff, and OT Staff personnel may have been able to observe victim reports of inoperable systems.

A total of one observable was identified with the use of the Loss of Control technique (T0827). This technique is important for investigation because it prevents owners and operators from issuing commands to equipment. This technique appears at the end of the timeline, beyond the point at which a defender could take action to disrupt the attack. Terminating the chain of techniques at this point would not limit destruction or business impacts.

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

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

3.29. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

The Loss of Availability technique (T0826) leaves victims with systems that no longer boot to Windows because critical system files have been encrypted without a decryption mechanism, and files and operations associated with impacted systems can no longer be accessed.[175,176]

OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff, and OT Staff personnel may have been able to observe victim reports of inoperable systems.

A total of one observable was identified with the use of the Loss of Availability technique (T0826). This technique is important for investigation because it prevents victims from utilizing business and operational assets. This technique appears at the end of the timeline, beyond the point at which a defender could take action to disrupt the attack**.** Terminating the chain of techniques at this point would not limit destruction or business impacts.

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

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

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

Maersk suffered significant financial losses under the Loss of Productivity and Revenue technique (T0828) as a result of the NotPetya cyber attack. The company's business volume dropped by 20 percent after the attack, as personnel had to manually perform their jobs for several weeks until all systems could be restored.[177,178,179] The financial loss was estimated at $350 million, including $30 million in recovery costs.

All company staff, including OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff, OT Staff, and Management personnel may have been able to observe victim reports of lost productivity and revenue.

A total of one observable was identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation because it involves a direct loss of revenue and productivity for the victim. This technique appears at the end of the timeline, beyond the point at which a defender could take action to disrupt the attack. Terminating the chain of techniques at this point would not limit destruction or business impacts.

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

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

3.31. DAMAGE TO PROPERTY TECHNIQUE (T0879) FOR IMPACT

The Damage to Property technique (T0879) typically leaves the victim with systems that are effectively destroyed, as the NotPetya malware does not provide for decryption of infected systems. In the case of Maersk, the company had to rebuild its entire infrastructure, replacing 49,000 computers and 3,500 of 6,200 servers over the course of several weeks.[180,181,182,183,184]

All company staff, including OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff, OT Staff, and Management personnel may have been able to observe victim reports of unrecoverable systems.

A total of one observable was identified with the use of the Damage to Property technique (T0879). This technique is important for investigation because it causes damage to IT and OT assets, interrupts business processes, and extends recovery time. This technique appears at the end of the timeline, beyond the point at which a defender could take action to disrupt the attack. Terminating the chain of techniques at this point would not limit destruction or business impacts.

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

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 18 artifacts could be generated by the Damage to Property technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, Engineering, IT Staff, OT Staff, Management

APPENDIX A: OBSERVABLES LIBRARY

Observables Associated with Supply Chain Compromise Technique (T0862)	
Observable 1	Malicious Command Observed by Microsoft Leading to NotPetya Infection: C:\\Windows\\system32\\rundll32.exe\" \"C:\\ProgramData\\perfc.dat\",#1 30
Observable 2	Malicious Backdoor in MEDoc Software Update: ZvitPublishedObjects.dll
Observable 3	Size of MEDoc's Malicious Update: 333Kb
Observable 4	Version Number of MEDoc's Malicious Update, Issued on 22 June 2017: 10.01.188-10.01.189
Observable 5 †	*Microsoft Task Manger, Showing Active Process: perfc.dat*
Observable 6 †	*Microsoft Task Manger, Showing Active Process: rundll32.exe*

Observables Associated with Command Line Interface Technique (T0807)	
Observable 1	EzVit.exe Process from MEDoc Executed the Following Command Line: C:\\Windows\\system32\\rundll32.exe\" \"C:\\ProgramData\\perfc.dat\",#1 30
Observable 2	cmd.exe Used to Spawn Command-Line Interface
Observable 3 †	*The Following Command Was Issued via PsExec:* *exe %s /node:"%ws" /user:"%ws" /password:"%ws" process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\%s\" #1*
Observable 4 †	*The Following Command Was Issued via WMIC:* *Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1 60"*
Observable 5	Hash for psexec.exe: f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5

Observables Associated with Native API Technique (T0834)	
Observable 1	Windows API Was Used to Execute a Dynamic Link Library: rundll32.exe
Observable 2 †	*Command Issued via PsExec:* *exe %s /node:"%ws" /user:"%ws" /password:"%ws" process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\%s\" #1*
Observable 3 †	*Command Issued via WMIC:* *Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1 60"*
Observable 4	Hash for psexec.exe: f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 1	Malicious DLL Used to Infect Systems: perfc.dat
Observable 2	Perfc.dat Drops dllhost.dat, Which is a Pseudonym for PsExec
Observable 3 †	*rundll32.exe Shows Up in Microsoft Task Manger as Active Process*
Observable 4 †	*perfc.dat Shows Up in Microsoft Task Manger as Active Process*
Observable 5	Command Line to Install Malicious file: C:\\Windows\\system32\\rundll32.exe\" \"C:\\ProgramData\\perfc.dat\",#1 30

Observables Associated with Masquerading Technique (T0849)	
Observable 1	Dllhost.dat is a Pseudonym for PsExec Utility

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 1	Malware Reads Itself into Process Memory Prior to Removing Itself from Host
Observable 2	Malware Copies Itself to Another Buffer as Part of the Process of Removing Itself from Host
Observable 3	Malware Calls Freelibrary to Unmap the Original Notpetya DLL from Process Memory as Part of the Process of Removing Itself from Host
Observable 4	Malware Overwrites the Original DLL File with Null Bytes as Part of the Process of Removing Itself from Host
Observable 5	Malware Deletes the Original Notpetya DLL from the File System as Part of the Process of Removing Itself From Host

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1	Malware Called Function GetExtendedTcpTable
Observable 2	Malware Called Function GetIpNetTable
Observable 3	Malware Called Function NetServerEnum
Observable 4	Malware Called Function NetServerGetInfo
Observable 5	Malware Called Function DhcpEnumSubnets
Observable 6	Malware Called Function DhcpGetSubnetInfo
Observable 7	Malware Called Function DhcpEnumSubnetClients
Observable 8	Malware Called Function GetTempPathW
Observable 9	Malware Called Function GetTempFileNameW.
Observable 10	Malware Called Function WNetOpenEnumW
Observable 11	Malware Called Function WNetEnumResourceW
Observable 12	Malware Called Function CredEnumerateW

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 13	Malware Called Function SeDebugPrivilege

Observables Associated with Command-Line Interface Technique (T0807)	
Observable 1 †	*Command-Line Interface Spawned to Issued Commands*

Observables Associated with Native API Technique (T0834)	
Observable 1	Malware Called Function GetExtendedTcpTable
Observable 2	Malware Called Function GetIpNetTable
Observable 3	Malware Called Function NetServerEnum
Observable 4	Malware Called Function NetServerGetInfo
Observable 5	Malware Called Function DhcpEnumSubnets
Observable 6	Malware Called Function DhcpGetSubnetInfo
Observable 7	Malware Called Function DhcpEnumSubnetClients
Observable 8	Malware Called Function GetTempPathW
Observable 9	Malware Called Function GetTempFileNameW.
Observable 10	Malware Called Function WNetOpenEnumW
Observable 11	Malware Called Function WNetEnumResourceW
Observable 12	Malware Called Function CredEnumerateW
Observable 13	Malware Called function SeDebugPrivilege

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 1	MD5 and SHA256 Hashes for 32-bit Mimikatz Variant: MD5: 2813D34F6197EB4DF42C886EC7F234A1 SHA256: EAE9771E2EEB7EA3C6059485DA39E77B8C0C369232F01334954FBAC1C186C998
Observable 2	MD5 and SHA256 Hashes for 64-bit Mimikatz Variant: MD5: 7E37AB34ECDCC3E77E24522DDFD4852D SHA256: 02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f
Observable 3	Mimikatz Variant Created Named Pipe for Passing Harvested Credentials
Observable 4	Malware Drops Mimikatz Variant in a Random Value.tmp File in Windows Tmp Folder

Observables Associated with Automated Collection Technique (T0802)	
Observable 1	Main Executable Uses Named Pipe C:\WINDOWS\TEMP\561D.tmp, \\.\pipe\{C1F0BF2D-8C17-4550-AF5A-65A22C61739C}
Observable 2	MD5 and SHA256 Hashes for the 32-bit Mimikatz Variant: MD5: 2813D34F6197EB4DF42C886EC7F234A1 SHA256: EAE9771E2EEB7EA3C6059485DA39E77B8C0C369232F01334954FBAC1C186C998
Observable 3	MD5 and SHA256 Hashes for the 64-bit Mimikatz Variant: MD5: 7E37AB34ECDCC3E77E24522DDFD4852D SHA256: 02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f

Observables Associated with Remote Services (T0886)	
Observable 1 †	*Command Issued via PsExec:* *Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1 60"*
Observable 2 †	*Command Issued via WMIC:* *C:\WINDOWS\dllhost.dat \\w.x.y.z -accepteula -s -d C:\Windows\System32\rundll32.exe C:\Windows\perfc.dat,#1 60*
Observable 3	Dllhost.dat is a Pseudonym Given to PsExec Utility
Observable 4 †	*rundll32.exe Shows Up in Microsoft Task Manager as an Active Process*
Observable 5 †	*perfc.dat Shows Up in Microsoft Task Manager as an Active Process*
Observable 6	Hash for psexec.exe: f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5

Observables Associated with Command-Line Interface (T0807)	
Observable 1 †	*Command Issued via WMIC:* *Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1 60"*
Observable 2 †	*Command Issued via PsExec:* *C:\WINDOWS\dllhost.dat \\w.x.y.z -accepteula -s -d C:\Windows\System32\rundll32.exe C:\Windows\perfc.dat,#1 60*
Observable 3	Cmd.exe Spawns Command-Line Interface

Observables Associated with Native API (T0834)	
Observable 1	Windows API rundll32.exe Executes Dynamic Link Library

Observables Associated with Valid Accounts (T0859)	
Observable 1 †	*Command Issued via WMIC:* *Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1 60"*
Observable 2 †	*Command Issued via PsExec:* C:\WINDOWS\dllhost.dat \\w.x.y.z -accepteula -s -d C:\Windows\System32\rundll32.exe C:\Windows\perfc.dat,#1 60

Observables Associated with Exploitation of Remote Services (T0866)	
Observable 1 †	*Four-byte XOR Key 9EC8253D Sent via EternalBlue*
Observable 2 †	*Four-byte XOR Key 3D9EC825 Sent via EternalBlue*
Observable 3 †	*Four-byte XOR Key 253D9EC8 Sent via EternalBlue*
Observable 4 †	*Four-byte XOR Key C8253D9E Sent via EternalBlue*
Observable 5	Binary Signature Over Port 445 9EC8253D9EC8253D9EC8253D9EC8253D
Observable 6	Binary Signature Over Port 445 3D9EC8253D9EC8253D9EC8253D9EC825
Observable 7	Binary Signature Over Port 445 253D9EC8253D9EC8253D9EC8253D9EC8
Observable 8	Binary Signature Over Port 445 C8253D9EC8253D9EC8253D9EC8253D9E
Observable 9 †	*EternalBlue Operated via SMB port 445*
Observable 10 †	*EternalRomance Operated via SMB Ports 139 and 445*

Observables Associated with Native API (T0834)	
Observable 1	Malware Called Function MapViewOfFile
Observable 2	Malware Called Function CreateFileMappingW

Observables Associated with Data Destruction (T0809)	
Observable 1	Sector 0 of the MBR is Overwritten with Custom Boot Loader
Observable 2	Sectors 1-31 of the MBR are Overwritten with 16-bit code
Observable 3	Part of Sector 32 of the MBR Includes Bitcoin Wallet and Personal Installation Key 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
Observable 4	Part of Sector 32 of the MBR Includes Generated Salsa20 Encryption Key

Observables Associated with Data Destruction (T0809)	
Observable 5	Sector 33 of the MBR is Overwritten with All 0x7 or 0x7h, Depending on Source
Observable 6	As Part of the Malware's Overwriting Procedure, Sector 34 Overwritten with XOR Encoded Original MBR with 0x7
Observable 7	User Files with These Extensions Were Encrypted: .3ds, .7z, .accdb, .ai, .asp, .aspx, .avhd, .back, .bak, .c, .cfg, .conf, .cpp, .cs, .ctl, .dbf, .disk, .djvu, .doc, .docx., .dwg, .eml, .fdb, .gz, .h, .hdd, .kdbx, .mail, .mdb, .msg, .nrg, .ora, .ost, .ova, .ovf, .pdf, .php, .pmf, .ppt, .pptx, .pst, .pvi, .py, .pyc, .rar, .rtf, .sln, .sql, .tar, .vbox, .vbs, .vcb, .vdi, .vfd, .vmc, .vmdk, .vmsd, .vmx, .vsdx, .vsv, .work, .xls, .xlsx, .xvd, and .zip
Observable 8	CRYPT_FLAG in Sector 32 Is Set to 0 Before the Master File Table Is Encrypted

Observables Associated with Command-Line Interface (T0807)	
Observable 1 †	*Cmd.exe Spawns Command-Line Interface*

Observables Associated with Indicator Removal on Host (T0872)	
Observable 1	Command to Delete Windows Event Logs wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c:

Observables Associated with Command-Line Interface (T0807)	
Observable 1 †	*Windows API Used to Reboot Host System* */c schtasks /Create/SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST <HH:MM>*
Observable 2	Windows API Used to Shutdown Host System NTRaiseHardError
Observable 3	Cmd.exe Is Used to Spawn a Command-Line Interface to Issue Commands

Observables Associated with Native API technique (T0834)	
Observable 1	Malware Called Windows API shutdown.exe
Observable 2	Malware Called Windows API system32
Observable 3	Malware Called Windows API NTRaiseHardError

Observables Associated with Device Restart/Shutdown (T0816)	
Observable 1 †	*Victim Reports of System Shutdowns Have Been Reported*

Observables Associated with Device Restart/Shutdown (T0816)	
Observable 2 †	*The Following Command Is Used by the Malware to Shut Down the System: /c schtasks /Create/SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST <HH:MM>*

Observables Associated with Masquerading (T0849)	
Observable 1 †	*Fake CHKDSK Screen Is Displayed to Victims*

Observables Associated with Data Destruction (T0809)	
Observable 1	CRYPT_FLAG in Sector 32 Is Set to 1 After Master File Table Encrypted
Observable 2	Malware Drops README.txt
Observable 3	Master File Table Is Encrypted with Salsa20

Observables Associated with Device Restart/Shutdown (T0816)	
Observable 1	Windows APIs Were Used to Shut Down the System

Observables Associated with Loss of View (T0829)	
Observable 1 †	*Maersk Personnel Reported a Loss of View to Network Systems*

Observables Associated with Loss of Control (T0827)	
Observable 1 †	*Maersk Personnel Reported a Loss of Control of Network Systems*

Observables Associated with Loss of Availability (T0826)	
Observable 1 †	*Maersk Personnel Reported a Loss of Availability to Network Systems*

Observables Associated with Loss of Productivity and Revenue (T0828)	
Observable 1 †	*Maersk's Business Volume Dropped by 20% After the Notpetya Attack. The Drop in Business Volume Shows a Measured Drop in Productivity.*

Observables Associated with Damage to Property (T0879)	
Observable 1 †	*Maersk Replaced 49,000 Computers and 3,500 Servers as a Result of Notpetya Attack*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Supply Chain Compromise Technique (T0862)	
Artifact 1	DNS Queries Traffic Port
Artifact 2	MAC Address
Artifact 3	Source IP Address
Artifact 4	Destination IP Address
Artifact 5	Network Discover Protocols
Artifact 6	SMB Port
Artifact 7	SNMP Port
Artifact 8	LLDP Requests
Artifact 9	HTTP Port
Artifact 10	Ping Echo Port
Artifact 11	Static Source IP Address
Artifact 12	Usage of Default Account
Artifact 13	Usage of Vendor Maintenance Account
Artifact 14	Domain Name
Artifact 15	Domain Registrant Data
Artifact 16	Domain IP Resolution
Artifact 17	Domain Autonomous System Number
Artifact 18	Hardware Serial Number Missing
Artifact 19	Additional Hardware Inserted On Devices
Artifact 20	Mismatched Software Hashes
Artifact 21	Device Failures
Artifact 22	Device Incompatibility Issues
Artifact 23	Hardware Tampering Evidence
Artifact 24	Hardware Failed Site Acceptance Test
Artifact 25	Physical Defects to Hardware
Artifact 26	Unscheduled Firmware Updates
Artifact 27	Manipulation of Signature on Digital Certifications
Artifact 28	Inconsistencies In Software Bill of Materials
Artifact 29	Inconsistencies In Hardware Bill of Materials
Artifact 30	Factory Acceptance Test Failure
Artifact 31	Inaccurate Delivery Based on Design Documents

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

Artifacts Associated with Native API Technique (T0834)	
Artifact 1	Industrial Network Traffic
Artifact 2	Industrial Protocol Command Packet
Artifact 3	Device Reads
Artifact 4	Device I/O Image Table Manipulated

Artifacts Associated with Native API Technique (T0834)	
Artifact 5	Device Failure
Artifact 6	Alter Process Logic
Artifact 7	Device Performance Degradation
Artifact 8	Device Memory Modification
Artifact 9	Device Alarm
Artifact 10	Device Live Data Changes
Artifact 11	Systems Calls
Artifact 12	Alert Generated
Artifact 13	Memory Corruption
Artifact 14	Host Device Failure
Artifact 15	Blue Screen
Artifact 16	Performance Degradation
Artifact 17	SYSMON Events Created
Artifact 18	Services Initiated
Artifact 19	Processes Initiated
Artifact 20	Files Created
Artifact 21	Imports Hash Changed
Artifact 22	.dll Modifications
Artifact 23	System Resource Usage Management Changes
Artifact 24	Command Execution
Artifact 25	Configuration Change

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

Artifacts Associated with Lateral Tool Transfer Technique (T0867)	
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 Masquerading Technique (T0849)	
Artifact 1	File Creation with Common Name
Artifact 2	Additional File Directories Created
Artifact 3	Scheduled Job Modification
Artifact 4	Service Creation
Artifact 5	Services Metadata
Artifact 6	Scheduled Job Metadata
Artifact 7	Leetspeak User Metadata
Artifact 8	Common Application with Non-Native Child Processes
Artifact 9	Process Metadata Changes
Artifact 10	Command Line Execution
Artifact 11	File Modification
Artifact 12	Warez Application Use
Artifact 13	Leetspeak File Creation
Artifact 14	Applications Causing Unintended Actions
Artifact 15	Additional Functionality In Applications

Artifacts Associated with Indicator Removal on Host Technique (T0872)	
Artifact 1	Command Execution
Artifact 2	User Logon Event
Artifact 3	User Logoff Event
Artifact 4	Windows Registry Key Deletion
Artifact 5	Windows Registry Key Modification
Artifact 6	HMI Dialog Box Open
Artifact 7	HMI Dialog Box Close
Artifact 8	HMI Screen Changes
Artifact 9	Process Creation
Artifact 10	HMI Interface Manipulation
Artifact 11	API System Calls
Artifact 12	File Creation
Artifact 13	Missing Log Events
Artifact 14	Memory Writes
Artifact 15	Unexpected Reboots
Artifact 16	Windows Security Log 1102 for Cleared Events
Artifact 17	File Deletion
Artifact 18	File Modification
Artifact 19	Sdelete Executable Loaded
Artifact 20	Sdelete Executable Executed
Artifact 21	File Metadata Changes
Artifact 22	Timestamp Inconsistencies
Artifact 23	User Authentication

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 1	Common Network Traffic
Artifact 2	IEC 103 Traffic (For North America)
Artifact 3	IEC 61850 MMS and
Artifact 4	Controller Proprietary Traffic
Artifact 5	Echo Type 8 Traffic
Artifact 6	ICMP Type 7 Traffic
Artifact 7	SNMP Port 162 Traffic

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 8	SNMP Port 161 Traffic
Artifact 9	Command Line Dialog Box Open
Artifact 10	Operating System Queries
Artifact 11	DNS Port 53 Zone Transfers
Artifact 12	Industrial Network Traffic Content About Hostnames
Artifact 13	Polling Network Traffic from Unauthorized IP Sender Addresses
Artifact 14	NETBIOS Name Services Port
Artifact 15	LDAP Port
Artifact 16	Active Directory Calls
Artifact 17	Email Server Calls
Artifact 18	SMTP Port 25 Traffic
Artifact 19	DNS Lookup Queries
Artifact 20	ARP Scans
Artifact 21	TCP Connect Scan
Artifact 22	TCP SYN Scans
Artifact 23	Scans Over Industrial Network Ports with Target IPS
Artifact 24	TCP FIN Scans
Artifact 25	TCP Reverse Ident Scan
Artifact 26	TCP XMAS Scan
Artifact 27	TCP ACK Scan*
Artifact 28	VNC Port 5900 Calls
Artifact 29	Protocol Content Enumeration
Artifact 30	Protocol Header Enumeration
Artifact 31	Recurring Protocol SYN Traffic
Artifact 32	Sequential Protocol SYN Traffic
Artifact 33	Statistical Anomalies in Network Traffic
Artifact 34	Industrial Network Traffic Content Containing Logical Identifiers
Artifact 35	Device Failure
Artifact 36	Device Reboot
Artifact 37	Bandwidth Degradation
Artifact 38	Host Recent Connection Logs
Artifact 39	Industrial Network Traffic

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 40	OPC Network Traffic
Artifact 41	IEC 104
Artifact 42	IEC 102
Artifact 43	IEC 101 Traffic to Serial Devices

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

Artifacts Associated with Native API Technique (T0834)	
Artifact 1	Industrial Network Traffic
Artifact 2	Industrial Protocol Command Packet
Artifact 3	Device Reads
Artifact 4	Device I/O Image Table Manipulated
Artifact 5	Device Failure
Artifact 6	Alter Process Logic
Artifact 7	Device Performance Degradation
Artifact 8	Device Memory Modification
Artifact 9	Device Alarm
Artifact 10	Device Live Data Changes
Artifact 11	Systems Calls
Artifact 12	Alert Generated
Artifact 13	Memory Corruption
Artifact 14	Host Device Failure
Artifact 15	Blue Screen
Artifact 16	Performance Degradation
Artifact 17	SYSMON Events Created
Artifact 18	Services Initiated
Artifact 19	Processes Initiated
Artifact 20	Files Created
Artifact 21	Imports Hash Changed
Artifact 22	.dll Modifications
Artifact 23	System Resource Usage Management Changes
Artifact 24	Command Execution
Artifact 25	Configuration Change

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

Artifacts Associated with Lateral Tool Transfer Technique (T0867)	
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 Automated Collection Technique (T0802)	
Artifact 1	Network Read Request
Artifact 2	OPC Read Requests
Artifact 3	Local Memory Read Requests
Artifact 4	Database Read Request
Artifact 5	POWERSHELL Command Arguments
Artifact 6	User Account Logs
Artifact 7	SMB Traffic Port
Artifact 8	File Transfer
Artifact 9	Application Log
Artifact 10	Service Log
Artifact 11	Native Tool Use
Artifact 12	External Network Connections
Artifact 13	Command Line Arguments

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 14	File Creation
Artifact 15	File Execution
Artifact 16	Command Execution
Artifact 17	Internal Network Connections
Artifact 18	IP Addresses
Artifact 19	MAC Addresses
Artifact 20	Operational Data Exfiltration
Artifact 21	User Account Creation
Artifact 22	User Account Privilege Change
Artifact 23	SQL Read Requests

Artifacts Associated with Remote Services (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
Artifact 9	Desktop Prompt Windows Created
Artifact 10	Session Cache
Artifact 11	Application Log
Artifact 12	RDP Traffic
Artifact 13	System Log Event
Artifact 14	Authentication Logs
Artifact 15	GUI Modifications
Artifact 16	Data File Size in Network Content
Artifact 17	File Movement
Artifact 18	MSSQL Traffic 1433 Port
Artifact 19	SSH Traffic
Artifact 20	SMB Traffic

Artifacts Associated with Remote Services (T0886)	
Artifact 21	VNC Traffic
Artifact 22	Process Creation
Artifact 23	Remote Session Creation Timestamp
Artifact 24	Network Traffic Content Creation

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

Artifacts Associated with Native API Technique (T0834)	
Artifact 1	Industrial Network Traffic
Artifact 2	Industrial Protocol Command Packet
Artifact 3	Device Reads
Artifact 4	Device I/O Image Table Manipulated
Artifact 5	Device Failure
Artifact 6	Alter Process Logic
Artifact 7	Device Performance Degradation
Artifact 8	Device Memory Modification
Artifact 9	Device Alarm
Artifact 10	Device Live Data Changes
Artifact 11	Systems Calls
Artifact 12	Alert Generated
Artifact 13	Memory Corruption
Artifact 14	Host Device Failure
Artifact 15	Blue Screen
Artifact 16	Performance Degradation
Artifact 17	SYSMON Events Created
Artifact 18	Services Initiated
Artifact 19	Processes Initiated
Artifact 20	Files Created
Artifact 21	Imports Hash Changed
Artifact 22	.dll Modifications
Artifact 23	System Resource Usage Management Changes
Artifact 24	Command Execution
Artifact 25	Configuration Change

Artifacts Associated with Valid Accounts (T0859)	
Artifact 1	Logons
Artifact 2	Default Credential Use
Artifact 3	Application Log
Artifact 4	Domain Permission Requests
Artifact 5	Permission Elevation Requests

Artifacts Associated with Valid Accounts (T0859)	
Artifact 6	Application Use Times
Artifact 7	Configuration Changes
Artifact 8	Prefetch Files Created After Execution
Artifact 9	Logon Session Creation
Artifact 10	User Account Creation
Artifact 11	Authentication Creation
Artifact 12	System Logs
Artifact 13	Successful Logon Event
Artifact 14	Failed Logons Event
Artifact 15	Logon Timestamp
Artifact 16	Logon Type Entry

Artifacts Associated with Exploitation of Remote Services (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 Logon Event
Artifact 13	Code Injection into the Operating System
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

Artifacts Associated with Exploitation of Remote Services (T0866)	
Artifact 20	System Reboots
Artifact 21	Blank Screens
Artifact 22	Safe Mode Reboot
Artifact 23	Application Logoff 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 Native API Technique (T0834)	
Artifact 1	Industrial Network Traffic
Artifact 2	Industrial Protocol Command Packet
Artifact 3	Device Reads
Artifact 4	Device I/O Image Table Manipulated
Artifact 5	Device Failure
Artifact 6	Alter Process Logic
Artifact 7	Device Performance Degradation
Artifact 8	Device Memory Modification
Artifact 9	Device Alarm
Artifact 10	Device Live Data Changes
Artifact 11	Systems Calls
Artifact 12	Alert Generated
Artifact 13	Memory Corruption
Artifact 14	Host Device Failure
Artifact 15	Blue Screen
Artifact 16	Performance Degradation
Artifact 17	SYSMON Events Created
Artifact 18	Services Initiated

Artifacts Associated with Native API Technique (T0834)	
Artifact 19	Processes Initiated
Artifact 20	Files Created
Artifact 21	Imports Hash Changed
Artifact 22	.dll Modifications
Artifact 23	System Resource Usage Management Changes
Artifact 24	Command Execution
Artifact 25	Configuration Change

Artifacts Associated with Data Destruction (T0809)	
Artifact 1	Program Execution
Artifact 2	Telnet Port
Artifact 3	SFTP Port
Artifact 4	FTPS Port
Artifact 5	SMB Port
Artifact 6	HTTP Port
Artifact 7	HTTPS Port
Artifact 8	Command Line Arguments
Artifact 9	SCP Port
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

Artifacts Associated with Data Destruction (T0809)	
Artifact 24	Missing Files
Artifact 25	Use of File Transfer Protocols
Artifact 26	FTP Port
Artifact 27	TFTP Port

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

Artifacts Associated with Indicator Removal on Host Technique (T0872)	
Artifact 1	Command Execution
Artifact 2	User Logon Event
Artifact 3	User Logoff Event
Artifact 4	Windows Registry Key Deletion
Artifact 5	Windows Registry Key Modification
Artifact 6	HMI Dialog Box Open
Artifact 7	HMI Dialog Box Close
Artifact 8	HMI Screen Changes
Artifact 9	Process Creation
Artifact 10	HMI Interface Manipulation
Artifact 11	API System Calls
Artifact 12	File Creation
Artifact 13	Missing Log Events
Artifact 14	Memory Writes
Artifact 15	Unexpected Reboots
Artifact 16	Windows Security Log 1102 for Cleared Events
Artifact 17	File Deletion
Artifact 18	File Modification
Artifact 19	Sdelete Executable Loaded
Artifact 20	Sdelete Executable Executed
Artifact 21	File Metadata Changes
Artifact 22	Timestamp Inconsistencies
Artifact 23	User Authentication

Artifacts Associated with Command-Line Interface Technique (T0807)	
Artifact 1	Remote Connections
Artifact 2	Script Execution
Artifact 3	User Account Logon
Artifact 4	External Network Connection
Artifact 5	User Account Privilege Change
Artifact 6	Command Execution
Artifact 7	Logon Event

Artifacts Associated with Command-Line Interface Technique (T0807)	
Artifact 8	Event Log Type
Artifact 9	Event Log Type
Artifact 10	Failed Logon Event
Artifact 11	cmd.exe Application Execution
Artifact 12	RDP Traffic
Artifact 13	Industrial Application Execution
Artifact 14	POWERSHELL Cmdlet Application Execution
Artifact 15	Event ID 4103 POWERSHELL Command
Artifact 16	Event ID 4688 Command Line Execution
Artifact 17	NTUSER Application Execution Entries
Artifact 18	Command Line Memory Data
Artifact 19	VNC Traffic Port
Artifact 20	SSH Traffic
Artifact 21	Telnet Traffic
Artifact 22	HTTP Traffic
Artifact 23	Application Log
Artifact 24	Process Creation
Artifact 25	Process Ending

Artifacts Associated with Native API Technique (T0834)	
Artifact 1	Industrial Network Traffic
Artifact 2	Industrial Protocol Command Packet
Artifact 3	Device Reads
Artifact 4	Device I/O Image Table Manipulated
Artifact 5	Device Failure
Artifact 6	Alter Process Logic
Artifact 7	Device Performance Degradation
Artifact 8	Device Memory Modification
Artifact 9	Device Alarm
Artifact 10	Device Live Data Changes
Artifact 11	Systems Calls
Artifact 12	Alert Generated

Artifacts Associated with Native API Technique (T0834)	
Artifact 13	Memory Corruption
Artifact 14	Host Device Failure
Artifact 15	Blue Screen
Artifact 16	Performance Degradation
Artifact 17	SYSMON Events Created
Artifact 18	Services Initiated
Artifact 19	Processes Initiated
Artifact 20	Files Created
Artifact 21	Imports Hash Changed
Artifact 22	.dll Modifications
Artifact 23	System Resource Usage Management Changes
Artifact 24	Command Execution
Artifact 25	Configuration Change

Artifacts Associated with Device Restart/Shutdown (T0816)	
Artifact 1	Process Application Event
Artifact 2	Process Environmental Changes
Artifact 3	Loss of Network Connection
Artifact 4	Network Command Packets
Artifact 5	Reboot Screen
Artifact 6	Blue Screen
Artifact 7	Significant Operational Data Changes
Artifact 8	Logon Events
Artifact 9	Logoff Events
Artifact 10	Process Failure
Artifact 11	Hardware Failure
Artifact 12	Command Prompt Opened
Artifact 13	Unauthorized Input
Artifact 14	Memory Corruption
Artifact 15	Process Alarm
Artifact 16	External Network Connections
Artifact 17	Local Network Connections

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

Artifacts Associated with Data Destruction (T0809)	
Artifact 1	Program Execution
Artifact 2	Telnet Port
Artifact 3	SFTP Port
Artifact 4	FTPS Port
Artifact 5	SMB Port
Artifact 6	HTTP Port
Artifact 7	HTTPS Port
Artifact 8	Command Line Arguments
Artifact 9	SCP Port
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

Artifacts Associated with Data Destruction (T0809)	
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
Artifact 27	TFTP Port

Artifacts Associated with Device Restart/Shutdown (T0816)	
Artifact 1	Process Application Event
Artifact 2	Process Environmental Changes
Artifact 3	Loss of Network Connection
Artifact 4	Network Command Packets
Artifact 5	Reboot Screen
Artifact 6	Blue Screen
Artifact 7	Significant Operational Data Changes
Artifact 8	Logon Events
Artifact 9	Logoff Events
Artifact 10	Process Failure
Artifact 11	Hardware Failure
Artifact 12	Command Prompt Opened
Artifact 13	Unauthorized Input
Artifact 14	Memory Corruption
Artifact 15	Process Alarm
Artifact 16	External Network Connections
Artifact 17	Local Network Connections

Artifacts Associated with Loss of View (T0829)	
Artifact 1	Application Logic Hooks or Modifications Might Prevent Proper Reporting to/from an Industrial Application
Artifact 2	Blocking Communications Paths and Channels (Comms, Network Infrastructure, Host Packet Routing) Might Occur via an OS or Device Modification
Artifact 3	Masked Reconfiguration of Alarm Thresholds or Other Configuration Settings Might Result in Unexpected Lack of Situational Awareness
Artifact 4	File System Modification Artifacts Might Be Associated with The Loss of View Attack Might Be Present on Disk

Artifacts Associated with Loss of Control (T0827)	
Artifact 1	Process Alarms
Artifact 2	Machine State Change
Artifact 3	Configuration Change
Artifact 4	Set Point Failure
Artifact 5	Service Request Increases
Artifact 6	Runaway Conditions
Artifact 7	Failed Input Commands
Artifact 8	Process Environment Changes
Artifact 9	Device Failure
Artifact 10	Network Connection Loss
Artifact 11	Unresponsive I/O Conditions
Artifact 12	Process Failure
Artifact 13	Repeated Maintenance Reports

Artifacts Associated with Loss of Availability (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

Artifacts Associated with Loss of Availability (T0826)	
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

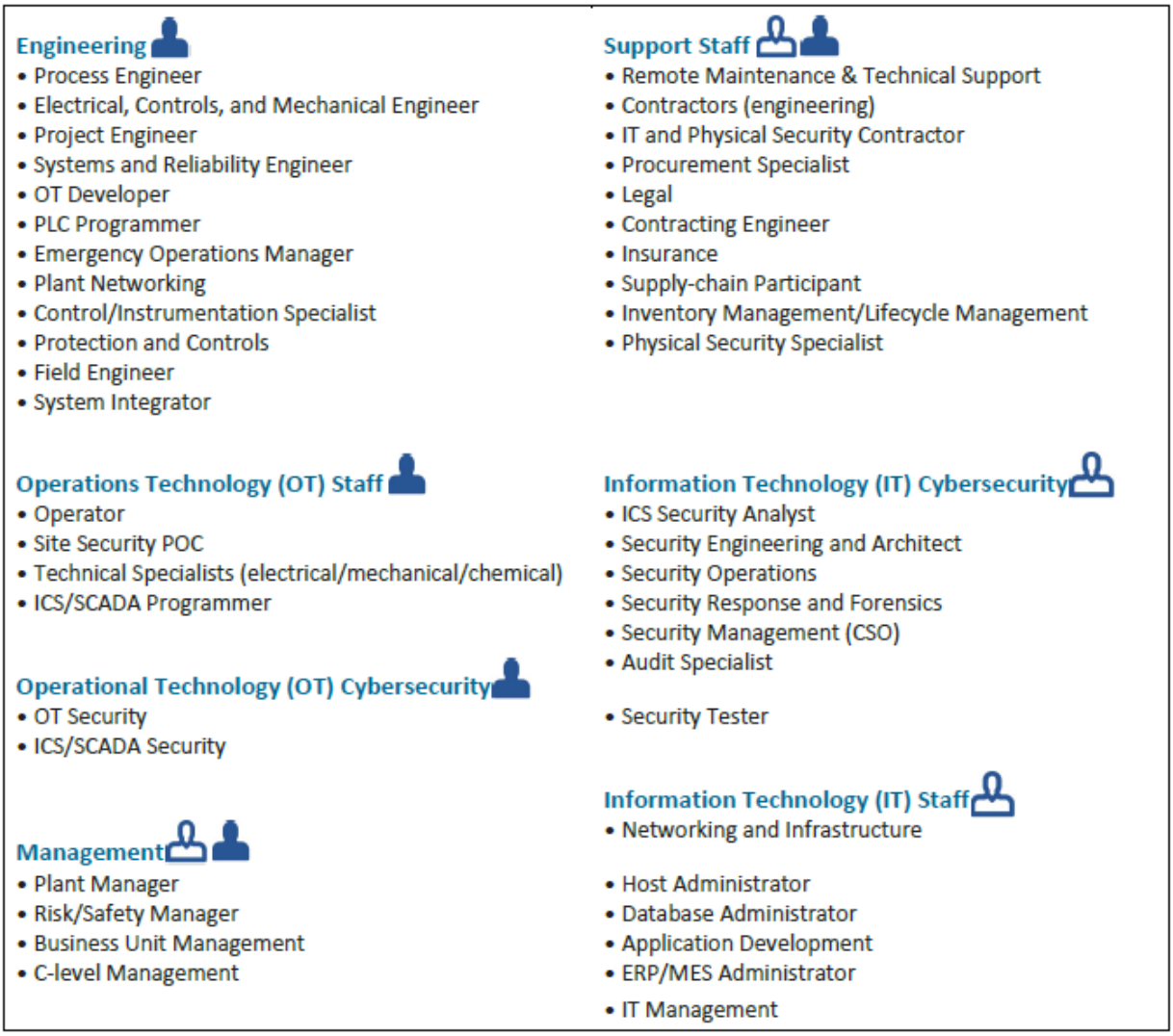
Artifacts Associated with Loss of Productivity and Revenue (T0828)	
Artifact 1	Loss of Confidence in a Safety System Due to Unreliability Might Result in a Risk Management Driven Shutdown of a Plant
Artifact 2	Wormable or Other Highly Propagating Malware Might Result in The Shutdown of a Plant to Prevent 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 Damage to Property (T0879)	
Artifact 1	Damage to Property Due to Equipment Malfunction
Artifact 2	Frequent Maintenance Failures
Artifact 3	Process Trip
Artifact 4	Alarms
Artifact 5	Smoke
Artifact 6	Liquid Spills
Artifact 7	Pressure Relief
Artifact 8	Loud Vibrations
Artifact 9	Safety Systems Engaged
Artifact 10	Breakers Closing and Opening Rapidly
Artifact 11	Damage to Property Due to Malicious Network Traffic
Artifact 12	Damage to Property Due to Equipment Degradation
Artifact 13	Reduction In Traffic Volume to Device
Artifact 14	Increase In Connecting Errors to Device
Artifact 15	Catastrophic Failure
Artifact 16	Surges in Power

Artifacts Associated with Damage to Property (T0879)	
Artifact 17	Ladder Logic Configuration Changes
Artifact 18	Industrial Network Traffic

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] [Microsoft | Microsoft Defender Security Research Team | “New ransomware, old techniques: Petya adds worm capabilities” | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[2] [Forbes | Jonathan Ponciano | “‘Extremely Destructive’ Russian Cyberattacks Could Cost U.S. Billions Of Dollars In Economic Damage, Goldman Warns” | https://www.forbes.com/sites/jonathanponciano/2022/03/07/extremely-destructive-russian-cyberattacks-could-cost-us-billions-of-dollars-in-economic-damage-goldman-warns/?sh=1a00fe92dc09 | 7 March 2022 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[3] [CISCO Blog – Talos | David Maynor, Aleksandar Nikolic, Matt Olney, and Yves Younan | “The MeDoc Connection” | https://blog.talosintelligence.com/2017/07/the-medoc-connection.html | 5 July 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[4] [Microsoft | Microsoft Defender Security Research Team | “New ransomware, old techniques: Petya adds worm capabilities” | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[5] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[6] [ESET | ““Petya” Ransomware: What we know now” | https://web.archive.org/web/20220408104100/https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/ | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[7] [CISCO Blog – Talos | David Maynor, Aleksandar Nikolic, Matt Olney, and Yves Younan | “The MeDoc Connection” | https://blog.talosintelligence.com/2017/07/the-medoc-connection.html | 5 July 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[8] [ESET | Anton Cherepanov | “Analysis of TeleBots’ cunning backdoor” | https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ | 4 July 2017 | Accessed 6 April 2022 | The source is publicly available information and does not contain classification markings]

[9] [ESET | ““Petya” Ransomware: What we know now” | https://web.archive.org/web/20220408104100/https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/ | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[10] [Microsoft | Microsoft Blog | “Windows 10 platform resilience against the Petya ransomware attack” | https://www.microsoft.com/security/blog/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/ | 29 June 2017 | Accessed 30 March 2022 | The source is publicly available information and does not contain classification markings]

[11] [YouTube | Black Hat Europe 2019 - Andy Powell | “Implementing the Lessons Learned From a Major Cyber Attack” | https://www.youtube.com/watch?v=wQ8HIjkEe9o | 18 March 2020 | Accessed 23 March 2022 | The source is publicly available information and does not contain classification markings]

[12] [YouTube | Andrey Gubarev | “Maersk 's CTIO Adam Banks about NotPetya ransomware attack I Information Security Europe 2019” | https://www.youtube.com/watch?v=_MwsxIS3tG8 | 8 July 2019 |

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

[13] [YouTube | Pol Bothuan channel | “CyberSecurity Davos 2017 - Maersk - Business Impact - with EN subtitles” | https://www.youtube.com/watch?v=VaqIYlYmDbA | 11 June 2018 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[14] [YouTube | Andrey Gubarev’s channel – Adam Banks | “Maersk 's CTIO Adam Banks about NotPetya ransomware attack I Information Security Europe 2019” | https://www.youtube.com/watch?v=_MwsxIS3tG8 | 8 July 2019 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[15] [YouTube | Pol Bothuan | “CyberSecurity Davos 2017 - Maersk - Business Impact - with EN subtitles” | https://www.youtube.com/watch?v=VaqIYlYmDbA | 11 June 2018 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[16] [YouTube | Black Hat Europe 2019 - Andy Powell | “Implementing the Lessons Learned From a Major Cyber Attack” | https://www.youtube.com/watch?v=wQ8HIjkEe9o | 18 March 2020 | Accessed 23 March 2022 | The source is publicly available information and does not contain classification markings]

[17] [Maarten van Hees | “The 2017 MAERSK Cyber Incident - Learning from and applying the Lessons of a Major Cyber Incident” | https://fhi.nl/app/uploads/sites/75/2020/10/201029-FHI_Maersk.pdf | October 2020 | Accessed 13 April 2022 | The source is publicly available information and does not contain classification markings]

[18] [Synopsys | Taylor Armerding | “Air gaps in ICS going, going … and so is security” | https://www.synopsys.com/blogs/software-security/smart-shipping-ics-air-gap/ | 28 November 2018 | Accessed 13 April 2022 | The source is publicly available information and does not contain classification markings]

[19] [MoreThanShipping | Irmak Aktan | “More Cyber Attacks: Sharks in the Water for the Shipping World” | https://www.morethanshipping.com/more-cyber-attacks-sharks-in-the-water-for-the-shipping-world/ | 5 October 2020 | Accessed 13 April 2022 | The source is publicly available information and does not contain classification markings]

[20] [Organization of American States | “Maritime in the Western Hemisphere” | https://www.oas.org/en/sms/cicte/docs/Maritime-cybersecurity-in-the-Western-Hemisphere-an-introduction-and-guidelines.pdf | Accessed 13 April 2022 | The source is publicly available information and does not contain classification markings]

[21] [YouTube | ieeeComputerSociety - Andy Powell | “Episode 438: Andy Powell on Lessons Learned from a Major Cyber Attack” | https://www.youtube.com/watch?v=Hu5BR2vt-Uw | 11 December 2020 | Accessed 23 March 2022 | The source is publicly available information and does not contain classification markings]

[22] [Organization of American States | “Maritime in the Western Hemisphere” | https://www.oas.org/en/sms/cicte/docs/Maritime-cybersecurity-in-the-Western-Hemisphere-an-introduction-and-guidelines.pdf | Accessed 13 April 2022 | The source is publicly available information and does not contain classification markings]

[23] [CSO | Dan Swinhoe | “Rebuilding after NotPetya: How Maersk moved forward” | https://www.csoonline.com/article/3444620/rebuilding-after-notpetya-how-maersk-moved-forward.html | 9 October 2019 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[24] [Microsoft | Microsoft Defender Security Research Team | “New ransomware, old techniques: Petya adds worm capabilities” | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[25] [Forbes | Jonathan Ponciano | "'Extremely Destructive' Russian Cyberattacks Could Cost U.S. Billions Of Dollars In Economic Damage, Goldman Warns" | https://www.forbes.com/sites/jonathanponciano/2022/03/07/extremely-destructive-russian-cyberattacks-could-cost-us-billions-of-dollars-in-economic-damage-goldman-warns/?sh=1a00fe92dc09 | 7 March 2022 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[26] [YouTube | Andrey Gubarev | "Maersk 's CTIO Adam Banks about NotPetya ransomware attack I Information Security Europe 2019" | https://www.youtube.com/watch?v=_MwsxIS3tG8 | 8 July 2019 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[27] [YouTube | Black Hat Europe 2019 - Andy Powell | "Implementing the Lessons Learned From a Major Cyber Attack" | https://www.youtube.com/watch?v=wQ8HIjkEe9o | 18 March 2020 | Accessed 23 March 2022 | The source is publicly available information and does not contain classification markings]

[28] [Microsoft | Microsoft Defender Security Research Team | "New ransomware, old techniques: Petya adds worm capabilities" | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[29] [CISCO Blog – Talos | David Maynor, Aleksandar Nikolic, Matt Olney, and Yves Younan | "The MeDoc Connection" | https://blog.talosintelligence.com/2017/07/the-medoc-connection.html | 5 July 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[30] [YouTube | Andrey Gubarev | "Maersk 's CTIO Adam Banks about NotPetya ransomware attack I Information Security Europe 2019" | https://www.youtube.com/watch?v=_MwsxIS3tG8 | 8 July 2019 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[31] [YouTube | Black Hat Europe 2019 - Andy Powell | "Implementing the Lessons Learned From a Major Cyber Attack" | https://www.youtube.com/watch?v=wQ8HIjkEe9o | 18 March 2020 | Accessed 23 March 2022 | The source is publicly available information and does not contain classification markings]

[32] [YouTube | Andrey Gubarev | "Maersk 's CTIO Adam Banks about NotPetya ransomware attack I Information Security Europe 2019" | https://www.youtube.com/watch?v=_MwsxIS3tG8 | 8 July 2019 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[33] [YouTube | Black Hat Europe 2019 - Andy Powell | "Implementing the Lessons Learned From a Major Cyber Attack" | https://www.youtube.com/watch?v=wQ8HIjkEe9o | 18 March 2020 | Accessed 23 March 2022 | The source is publicly available information and does not contain classification markings]

[34] [Crowdstrike | Karan Sood and Shaun Hurley | "NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft" | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[35] [Synopsys | Taylor Armerding | "Air gaps in ICS going, going … and so is security" | https://www.synopsys.com/blogs/software-security/smart-shipping-ics-air-gap/ | 28 November 2018 | Accessed 13 April 2022 | The source is publicly available information and does not contain classification markings]

[36] [MoreThanShipping | Irmak Aktan | "More Cyber Attacks: Sharks in the Water for the Shipping World" | https://www.morethanshipping.com/more-cyber-attacks-sharks-in-the-water-for-the-shipping-world/ | 5 October 2020 | Accessed 13 April 2022 | The source is publicly available information and does not contain classification markings]

[37] [Organization of American States | “Maritime in the Western Hemisphere” | https://www.oas.org/en/sms/cicte/docs/Maritime-cybersecurity-in-the-Western-Hemisphere-an-introduction-and-guidelines.pdf | Accessed 13 April 2022 | The source is publicly available information and does not contain classification markings]

[38] [YouTube | ieeeComputerSociety - Andy Powell | “Episode 438: Andy Powell on Lessons Learned from a Major Cyber Attack” | https://www.youtube.com/watch?v=Hu5BR2vt-Uw | 11 December 2020 | Accessed 23 March 2022 | The source is publicly available information and does not contain classification markings]

[39] [YouTube | Andrey Gubarev | “Maersk 's CTIO Adam Banks about NotPetya ransomware attack I Information Security Europe 2019” | https://www.youtube.com/watch?v=_MwsxIS3tG8 | 8 July 2019 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[40] [Maarten van Hees | “The 2017 MAERSK Cyber Incident - Learning from and applying the Lessons of a Major Cyber Incident” | https://fhi.nl/app/uploads/sites/75/2020/10/201029-FHI_Maersk.pdf | October 2020 | Accessed 13 April 2022 | The source is publicly available information and does not contain classification markings]

[41] [CSO | Dan Swinhoe | “Rebuilding after NotPetya: How Maersk moved forward” | https://www.csoonline.com/article/3444620/rebuilding-after-notpetya-how-maersk-moved-forward.html | 9 October 2019 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[42] [YouTube | Andrey Gubarev | “Maersk 's CTIO Adam Banks about NotPetya ransomware attack I Information Security Europe 2019” | https://www.youtube.com/watch?v=_MwsxIS3tG8 | 8 July 2019 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[43] [YouTube | Pol Bothuan | “CyberSecurity Davos 2017 - Maersk - Business Impact - with EN subtitles” | https://www.youtube.com/watch?v=VaqIYlYmDbA | 11 June 2018 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[44] [YouTube | Black Hat Europe 2019 - Andy Powell | “Implementing the Lessons Learned From a Major Cyber Attack” | https://www.youtube.com/watch?v=wQ8HIjkEe9o | 18 March 2020 | Accessed 23 March 2022 | The source is publicly available information and does not contain classification markings]

[45] [CISCO Blog – Talos | David Maynor, Aleksandar Nikolic, Matt Olney, and Yves Younan | “The MeDoc Connection” | https://blog.talosintelligence.com/2017/07/the-medoc-connection.html | 5 July 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[46] [Microsoft | Microsoft Defender Security Research Team | “New ransomware, old techniques: Petya adds worm capabilities” | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[47] [Cynet | Noam Zweig | “A Technical Analysis of NotPetya” | https://www.cynet.com/blog/a-technical-analysis-of-notpetya/ | 28 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[48] [ESET | Anton Cherepanov | “Analysis of TeleBots’ cunning backdoor” | https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ | 4 July 2017 | Accessed 6 April 2022 | The source is publicly available information and does not contain classification markings]

[49] [ESET | Anton Cherepanov | ““Petya” Ransomware: What we know now” | https://web.archive.org/web/20220408104100/https://www.eset.com/us/about/newsroom/corporate-

blog/petya-ransomware-what-we-know-now/ | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[50] [CISCO Blog – Talos | David Maynor, Aleksandar Nikolic, Matt Olney, and Yves Younan | "The MeDoc Connection" | https://blog.talosintelligence.com/2017/07/the-medoc-connection.html | 5 July 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[51] [Microsoft | Microsoft Defender Security Research Team | "New ransomware, old techniques: Petya adds worm capabilities" | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[52] [Microsoft | Microsoft Defender Security Research Team | "New ransomware, old techniques: Petya adds worm capabilities" | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[53] [Crowdstrike | Karan Sood and Shaun Hurley | "NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft" | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[54] [Microsoft | Microsoft Defender Security Research Team | "New ransomware, old techniques: Petya adds worm capabilities" | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[55] [Crowdstrike | Karan Sood and Shaun Hurley | "NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft" | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[56] [Crowdstrike | Karan Sood and Shaun Hurley | "NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft" | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[57] [Microsoft | Microsoft Defender Security Research Team | "New ransomware, old techniques: Petya adds worm capabilities" | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[58] [Crowdstrike | Karan Sood and Shaun Hurley | "NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft" | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[59] [Microsoft | Microsoft Defender Security Research Team | "New ransomware, old techniques: Petya adds worm capabilities" | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[60] [Microsoft | "Attack surface reduction rules reference" | https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-process-creations-originating-from-psexec-and-wmi-commands | 11 April 2022 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[61] [Microsoft | Microsoft Defender Security Research Team | "New ransomware, old techniques: Petya adds worm capabilities" | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-

techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[62] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[63] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[64] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[65] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[66] [Microsoft | Microsoft Defender Security Research Team | “New ransomware, old techniques: Petya adds worm capabilities” | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[67] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[68] [Microsoft | D_A_Renoir | “How to tell if dllhost.exe is real or virus” | https://answers.microsoft.com/en-us/windows/forum/all/how-to-tell-if-dllhostexe-is-real-or-virus/e7ba27e9-acc2-4d2a-ad56-9fc960a85c46 | 14 May 2020 | Accessed 29 April 2022 | The source is publicly available information and does not contain classification markings]

[69] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[70] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[71] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[72] [Crowdstrike | Shaun Hurley and Karan Sood | “NotPetya Technical Analysis Part II: Further Findings and Potential for MBR Recovery” | https://www.crowdstrike.com/blog/petrwrap-technical-analysis-part-2-further-findings-and-potential-for-mbr-recovery/ | 3 July 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[73] [Crowdstrike | Shaun Hurley and Karan Sood | “NotPetya Technical Analysis Part II: Further Findings and Potential for MBR Recovery” | https://www.crowdstrike.com/blog/petrwrap-technical-analysis-part-2-further-findings-and-potential-for-mbr-recovery/ | 3 July 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[74] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[75] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[76] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[77] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[78] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[79] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[80] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[81] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[82] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[83] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[84] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[85] [CISA | “Malware Initial Findings Report (MIFR) – 10130295” | https://www.cisa.gov/uscert/sites/default/files/publications/MIFR-10130295.pdf | 30 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[86] [Cynet | Noam Zweig | “A Technical Analysis of NotPetya” | https://www.cynet.com/blog/a-technical-analysis-of-notpetya/ | 28 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[87] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-

technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[88] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[89] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[90] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[91] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[92] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[93] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[94] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[95] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[96] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[97] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[98] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[99] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[100] [CISA | “Malware Initial Findings Report (MIFR) – 10130295” | https://www.cisa.gov/uscert/sites/default/files/publications/MIFR-10130295.pdf | 30 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[101] [Cynet | Noam Zweig | “A Technical Analysis of NotPetya” | https://www.cynet.com/blog/a-technical-analysis-of-notpetya/ | 28 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[102] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[103] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[104] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[105] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[106] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[107] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[108] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[109] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[110] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[111] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[112] [Microsoft | “rundll32” | https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/rundll32 | 3 March 2021 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[113] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[114] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[115] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[116] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[117] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[118] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[119] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[120] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[121] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[122] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[123] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[124] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[125] [Microsoft | Microsoft Defender Security Research Team | “New ransomware, old techniques: Petya adds worm capabilities” | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[126] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[127] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[128] [CISA | “Malware Initial Findings Report (MIFR) – 10130295” | https://www.cisa.gov/uscert/sites/default/files/publications/MIFR-10130295.pdf | 30 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[129] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[130] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[131] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[132] [Microsoft | Microsoft Defender Security Research Team | “New ransomware, old techniques: Petya adds worm capabilities” | https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[133] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[134] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[135] [Cynet | Noam Zweig | “A Technical Analysis of NotPetya” | https://www.cynet.com/blog/a-technical-analysis-of-notpetya/ | 28 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[136] [Trendmicro | Brian Cayanan and Anthony Melgarejo | “Petya Ransomware Attack In Progress, Hits Europe” | https://www.trendmicro.com/en_us/research/17/f/large-scale-ransomware-attack-progress-hits-europe-hard.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[137] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[138] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[139] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[140] [Trendmicro | Brian Cayanan and Anthony Melgarejo | “Petya Ransomware Attack In Progress, Hits Europe” | https://www.trendmicro.com/en_us/research/17/f/large-scale-ransomware-attack-progress-hits-europe-hard.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[141] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[142] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[143] [Cynet | Noam Zweig | “A Technical Analysis of NotPetya” | https://www.cynet.com/blog/a-technical-analysis-of-notpetya/ | 28 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[144] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[145] [Cynet | Noam Zweig | “A Technical Analysis of NotPetya” | https://www.cynet.com/blog/a-technical-analysis-of-notpetya/ | 28 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[146] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[147] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[148] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[149] [Cynet | Noam Zweig | “A Technical Analysis of NotPetya” | https://www.cynet.com/blog/a-technical-analysis-of-notpetya/ | 28 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[150] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[151] [Trendmicro | Brian Cayanan and Anthony Melgarejo | “Petya Ransomware Attack In Progress, Hits Europe” | https://www.trendmicro.com/en_us/research/17/f/large-scale-ransomware-attack-progress-hits-europe-hard.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[152] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-

technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[153] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[154] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[155] [Cynet | Noam Zweig | “A Technical Analysis of NotPetya” | https://www.cynet.com/blog/a-technical-analysis-of-notpetya/ | 28 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[156] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[157] [Trendmicro | Brian Cayanan and Anthony Melgarejo | “Petya Ransomware Attack In Progress, Hits Europe” | https://www.trendmicro.com/en_us/research/17/f/large-scale-ransomware-attack-progress-hits-europe-hard.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[158] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[159] [Trendmicro | Brian Cayanan and Anthony Melgarejo | “Petya Ransomware Attack In Progress, Hits Europe” | https://www.trendmicro.com/en_us/research/17/f/large-scale-ransomware-attack-progress-hits-europe-hard.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[160] [CISA | “Malware Initial Findings Report (MIFR) – 10130295” | https://www.cisa.gov/uscert/sites/default/files/publications/MIFR-10130295.pdf | 30 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[161] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[162] [Trendmicro | Brian Cayanan and Anthony Melgarejo | “Petya Ransomware Attack In Progress, Hits Europe” | https://www.trendmicro.com/en_us/research/17/f/large-scale-ransomware-attack-progress-hits-europe-hard.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[163] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[164] [Trendmicro | Brian Cayanan and Anthony Melgarejo | “Petya Ransomware Attack In Progress, Hits Europe” | https://www.trendmicro.com/en_us/research/17/f/large-scale-ransomware-attack-progress-hits-europe-hard.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[165] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[166] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[167] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[168] [CISA | “Malware Initial Findings Report (MIFR) – 10130295” | https://www.cisa.gov/uscert/sites/default/files/publications/MIFR-10130295.pdf | 30 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[169] [Crowdstrike | Karan Sood and Shaun Hurley | “NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft” | https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ | 29 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[170] [CISCO Blog – Talos | “New Ransomware Variant "Nyetya" Compromises Systems Worldwide” | https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html | 27 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[171] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[172] [CISA | “Malware Initial Findings Report (MIFR) – 10130295” | https://www.cisa.gov/uscert/sites/default/files/publications/MIFR-10130295.pdf | 30 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[173] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[174] [CISA | “Malware Initial Findings Report (MIFR) – 10130295” | https://www.cisa.gov/uscert/sites/default/files/publications/MIFR-10130295.pdf | 30 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[175] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[176] [CISA | “Malware Initial Findings Report (MIFR) – 10130295” | https://www.cisa.gov/uscert/sites/default/files/publications/MIFR-10130295.pdf | 30 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[177] [YouTube | Andrey Gubarev | “Maersk 's CTIO Adam Banks about NotPetya ransomware attack I Information Security Europe 2019” | https://www.youtube.com/watch?v=_MwsxIS3tG8 | 8 July 2019 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[178] [YouTube | Pol Bothuan | “CyberSecurity Davos 2017 - Maersk - Business Impact - with EN subtitles” | https://www.youtube.com/watch?v=VaqIYlYmDbA | 11 June 2018 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[179] [YouTube | Black Hat Europe 2019 - Andy Powell | “Implementing the Lessons Learned From a Major Cyber Attack” | https://www.youtube.com/watch?v=wQ8HIjkEe9o | 18 March 2020 | Accessed 23 March 2022 | The source is publicly available information and does not contain classification markings]

[180] [YouTube | Andrey Gubarev | “Maersk 's CTIO Adam Banks about NotPetya ransomware attack I Information Security Europe 2019” | https://www.youtube.com/watch?v=_MwsxIS3tG8 | 8 July 2019 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[181] [YouTube | Pol Bothuan | “CyberSecurity Davos 2017 - Maersk - Business Impact - with EN subtitles” | https://www.youtube.com/watch?v=VaqIYlYmDbA | 11 June 2018 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]

[182] [YouTube | Black Hat Europe 2019 - Andy Powell | “Implementing the Lessons Learned From a Major Cyber Attack” | https://www.youtube.com/watch?v=wQ8HIjkEe9o | 18 March 2020 | Accessed 23 March 2022 | The source is publicly available information and does not contain classification markings]

[183] [Symantec Security Response | Security Response Team | “Petya ransomware outbreak: Here’s what you need to know” | https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper | 24 October 2017 | Accessed 19 April 2022 | The source is publicly available information and does not contain classification markings]

[184] [CISA | “Malware Initial Findings Report (MIFR) – 10130295” | https://www.cisa.gov/uscert/sites/default/files/publications/MIFR-10130295.pdf | 30 June 2017 | Accessed 22 March 2022 | The source is publicly available information and does not contain classification markings]