PRECURSOR ANALYSIS REPORT: CONFICKER INFECTION OF GUNDREMMINGEN NUCLEAR POWER PLANT 2016

Cybersecurity for the Operational Technology Environment (CyOTE)

30 JUNE 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-69466

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: CONFICKER INFECTION OF GUNDREMMINGEN NUCLEAR POWER PLANT 2016

1. EXECUTIVE SUMMARY

The Conficker Infection of Gundremmingen Nuclear Power Plant 2016 Precursor Analysis Report leverages publicly available information about the global Conficker malware outbreak and catalogs anomalous observables for each technique employed in the attack against Gundremmingen. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

Conficker initially appeared in November 2008, and throughout its evolution has acquired several different names including Downup, Downadup, and Kido. Conficker is a worm-type malware that self-propagates across vulnerable systems. However, the Conficker Working Group, a coalition of cybersecurity researchers, was able to shut down all the domains associated with the Conficker command and control servers in 2009, eliminating the malware's extant ability to execute malicious code against infected systems.[1]

In the case of the Gundremmingen Nuclear Power Plant in Gundremmingen, Germany a routine security check on 24 April 2016 discovered Conficker malware on 18 systems within the plant's IT network that oversees the fuel handling system.[2] Upon detection of the malware, Gundremmingen shut down for two days to follow security procedures, including wiping the malware from all infected systems and scanning all other systems to ensure the malware was no longer present. Gundremmingen officials said they suspected someone brought in the malware by accident on a USB thumb drive, either from home or computers in the facility.[3] The plant's internal network was isolated from the Internet, obstructing the Conficker malware from further propagation to external machines or otherwise enabling adversary access to the infected internal machines.[4]

CyOTE researchers and analysts identified 22 techniques utilized during the attack, generating a total of 78 observables using MITRE's ATT&CK® for Industrial Control Systems framework. 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, then earlier comprehension of malicious activity can take place. Eighteen of the identified techniques used during the Conficker cyber attack were precursors to the triggering event. Case study analysis identified 66 observables associated with these precursor techniques, 41 of which were assessed to have an increased likelihood of being perceived preceding the triggering event of the malware. The response and comprehension time likely could have been reduced by four hours if these highly perceivable observables had been identified before the triggering event occurred.

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

2. INTRODUCTION

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

2.1. APPLYING THE CYOTE METHODOLOGY

The CyOTE methodology, as shown in Figure 1 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® for Industrial Control Systems (ICS) framework as a common lexicon to assess triggering events. By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables, which could represent a faint signal of an attack requiring investigation. CyOTE can assist organizations in prioritizing their OT environment visibility investments.

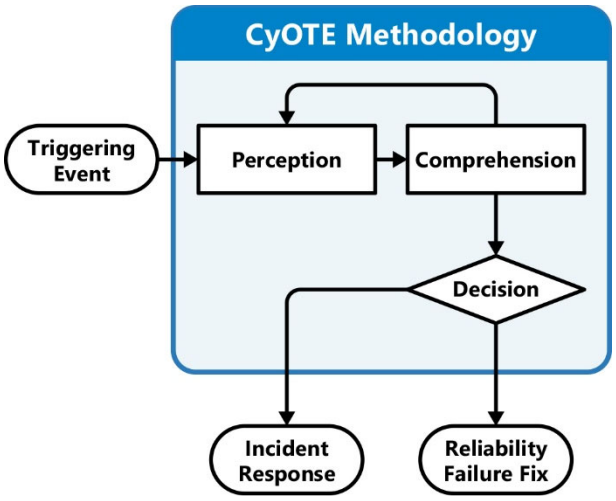


Figure 1. CyOTE Methodology

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

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

Each technique has an assessed perceivability. Perceivability is a function of the number of observables and the potential for personnel to detect those observables. If a technique includes

effects which personnel may detect, such as deletion or modification of system files or required user execution, then the technique would be more perceivable.

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

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

2.2. BACKGROUND ON THE ATTACK

The Microsoft Malware Protection Center identified the first iteration of Conficker malware (Conficker A) in November 2008. Conficker is a worm-type malware which infects unpatched Windows operating systems by utilizing three different methods of initial access to propagate and worm into connected systems. Conficker connects these machines to a remote server that allows the adversaries to execute remote code on infected systems, although this functionality was never used in a way that caused significant impact on victims. Conficker has at least five different variants (A through E), which researchers identified between November 2008 and April 2009. Information from researchers and victims indicated the different Conficker variants had infected 25 million machines as of 25 October 2011.[5] Despite software security responses, Conficker infections have continued to propagate in older systems years after the malware's introduction.

In the case presented in this study, a routine security check revealed a Conficker infection at the Gundremmingen Nuclear Power Plant on 24 April 2016.[6] Among the infected systems was a computer network containing data visualization software associated with the equipment the plant utilized for moving nuclear fuel rods.[7]

A timeline of adversarial techniques for a generic Conficker attack is shown in Figure 2. The timeline includes the estimated number of hours prior to and after the triggering event. The timeline after the triggering event includes the assessed victim comprehension timeline.

The Conficker malware replicates in three different ways: by removable media, network shares, or by exploitation of remote services. The malware at Gundremmingen was most likely introduced to the plant's machines by a USB storage device (H-4.5). When a Conficker-infected removable device connects to a machine and Conficker is installed, the malware sleeps for 30 minutes to decrease risk of detection (H-4).[8] In the case of Gundremmingen, the malware was unable to propagate beyond the plant's network or otherwise call back to adversary command and control (C2) servers because the plant's network was isolated from the Internet.[9]

After its sleep period, Conficker executes a multitude of evasive steps to avoid detection, including embedding itself in the form of a rootkit.[10] Immediately upon execution of the evasive steps, Conficker attempts to contact the adversary's domain to download any updates or further instructions. In the case of isolated networks such as Gundremmingen's, even though Conficker is unable to connect with the adversary's domain, it continues its execution process using peer-to-peer (P2P) user

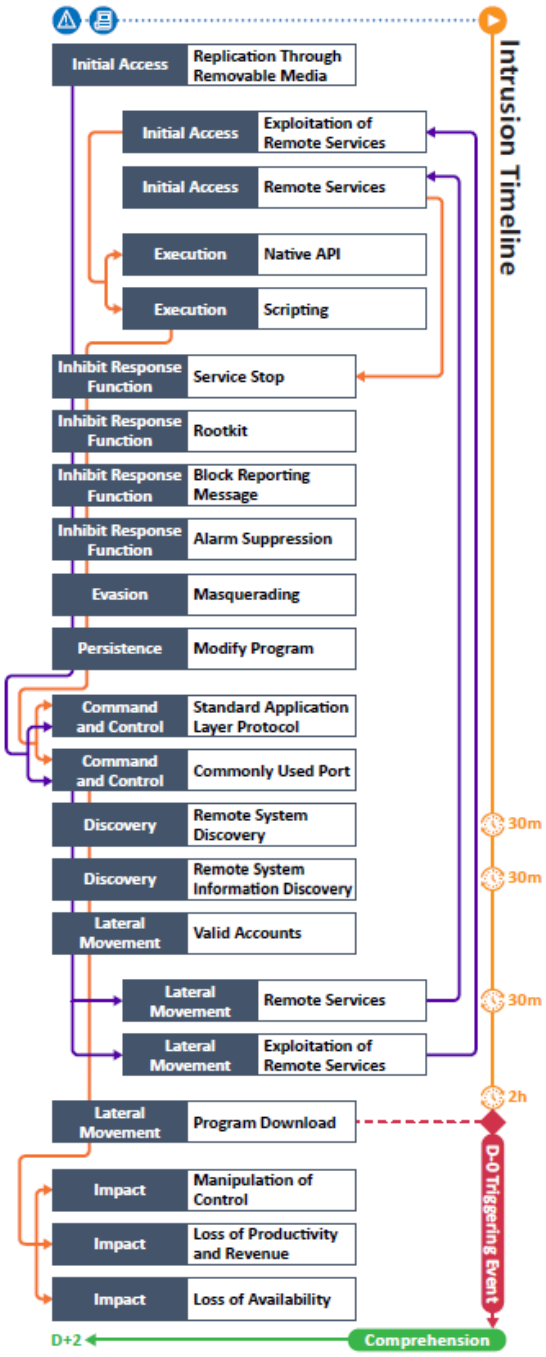


Figure 2. Intrusion Timeline

datagram protocol (UDP) scans to identify other machines on the network, after which Conficker again sleeps for 30 minutes (H-3).[11]

Next, Conficker uses an HTTP server created earlier as part of the adversary's domain connection process to communicate with machines found in the P2P scan and determine if those machines are already infected.[12] Once this process is completed, Conficker sleeps for another 30 minutes (H-2.5) before attempting to infect any uninfected machines by utilizing network shares to replicate. The malware then sleeps for a fourth time for 30 minutes (H-2) before attempting to infect any remaining uninfected machines through vulnerability exploitation and brute-force.[13,14]

Finally, the malware installs W.32 Waledac and SpywareProtect2009 and sleeps for two hours before executing any further impact steps, including execution of arbitrary code from a connected C2 server, toward a triggering event (D-0).[15]

Upon detection of the malware at Gundremmingen, personnel shut down operations for two days (D+2) to wipe the malware from infected systems and scan other systems to ensure they were clean.

Conficker was never utilized by threat actors to execute any further impact steps, despite being available for remote code execution. The malware was thwarted by a group that shut down all the domains associated with the C2 servers, leaving Conficker impotent beyond its inherent propagation capability. The Conficker malware could have caused further impact to Internet-connected machines assuming adversaries were able to leverage its capabilities.

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

Table 1. Techniques Used in the Gundremmingen Cyber-Attack

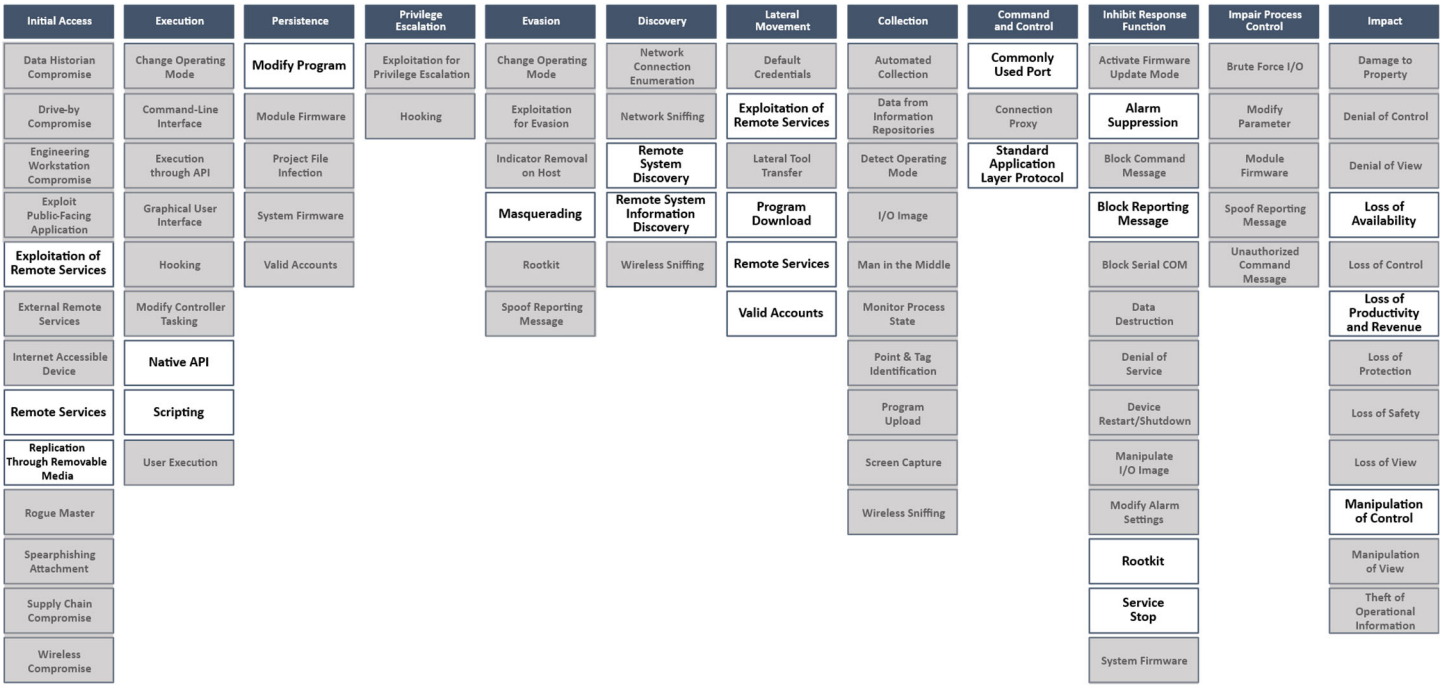


Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	22
Technique Observables	78
Precursor Techniques	18
Precursor Technique Observables	66
Highly Perceivable Precursor Technique Observables	41

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. REPLICATION THROUGH REMOVABLE MEDIA TECHNIQUE (T0847) FOR INITIAL ACCESS

The Conficker malware uses the Replication Through Removable Media technique (T0847) by leveraging the default autorun feature (autorun.inf) of Windows.[16] The autorun.inf function enables Conficker to automatically run executables whenever a removable drive is inserted into a system.[17] To increase its chance of success, the malware sets the "shell execute" prompt in the autorun.inf file to be "Open folder to view files". The prompt is created with social engineering tactics in mind to interact with users unaware of the malware executing the autorun program, furthering its propagation across the network. Once the Conficker malware has its initial foothold, it listens for the WM_DEVICECHANGE message. The WM_DEVICECHANGE signals a new removable device or drive has been mapped to the compromised system and initiates an immediate attempt to infect the new device.[18]

Observers of this technique would include all computer users being requested to initiate the propagation (OT Cybersecurity, IT Cybersecurity, and IT Staff). Observers would likely see a notification in the Windows Event Log when a Universal Serial Bus (USB) or other removeable media device connects to the system. The newly attached device would automatically assign a drive signature.

A total of six observables were identified with the use of the Replication Through Removeable Media technique (T0847). This technique is important for investigation due to its autorun feature and its direct execution by a user. This technique modifies the host operating system files via the installation of the Conficker Malware, resulting in the host being commanded into a modified / compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired. This technique is used early in the attack timeline and responding to it will disrupt further infection of a network. Terminating the chain of techniques at this point would limit operational impact to an attempted malware infection.

Of the six observables associated with this technique, five are assessed to be highly perceivable (Drive Creation; File Creation; autorun.inf Execution Feature; Autoplay Alert, Windows Event Log entries).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 48 artifacts could be generated by the Replication Through Removable Media technique
Technique Observers[a]	IT Cybersecurity, IT Staff, OT Cybersecurity

[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. EXPLOITATION OF REMOTE SERVICES TECHNIQUE (T0866) FOR INITIAL ACCESS

Once Conficker has gained initial access, the malware uses the Remote Procedure Call (RPC) communication protocol as its primary access point for propagation. This exploit utilizes the Microsoft Windows Server Service RPC Handling Remote Code Execution (RCE) Vulnerability (BID 31874), which Microsoft announced in October of 2008 and has since patched (MS08-067).[19] This vulnerability makes legacy Windows systems (e.g., Windows 2000, XP, Server 2003, Vista, and Server 2008) viable targets. Conficker exposes the RPC Vulnerability and targets TCP Port 445 using the Server Message Block (SMB) network file sharing protocol to execute arbitrary code without prior authentication. The malware proceeds to create an HTTP server on a random port. It exploits shared drive connections to other remote systems, directing them to connect and download the Conficker malware, further spreading the infection.[20]

Observers of this technique would include IT Staff, IT Cybersecurity and OT Cybersecurity with varying levels of awareness. Cybersecurity and IT Staff would require a network baseline in order to observe a new locally sourced HTTP server within the domain. OT Cybersecurity may notice latency and an increase in TCP 445 traffic within Windows Event Logs.

A total of five observables were identified with the use of the Exploitation of Remote Services technique (T0866). This technique is important for investigation due to its main vector of infection through a patched vulnerability (MS08-067). This technique appears early in the attack chain timeline and responding to it will prevent further damaging effects present in the malware itself. Terminating the chain of techniques at this point would prevent further intrusion.

Of the five observables associated with this technique, three are assessed to be highly perceivable (RPC Traffic; TCP 445 (SMB) Network File; Windows Event Log Entries).

Please see Appendix A for the list of observables.

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

3.3. REMOTE SERVICES TECHNIQUE (T0886) FOR INITIAL ACCESS

Conficker's persistence and ability to infect systems relies on multiple pathways to continually spread into system networks. The malware does this by using the Remote Services technique (T0886) to attempt to copy additional instances to other machines through the administrative network share (ADMIN$). The NetServerEnum request returns all visible Windows machines found on the network and the malware attempts to infect each of the identified machines.[21]

Conficker then harvests locally logged-on user credentials, copying itself to network connected machines. If the user credentials prove ineffective, Conficker will attempt authentication with all user names found on the local machine, leaving as an observable Windows Event ID 4624: Login, attempting brute-force authentication using nearly 250 common passwords.[22] Login failure will be reflected in Event ID 4625: Login Failures, and lead to user accounts being locked from too many invalid login attempts if standard security policy rules are applied.

The ability to observe this technique depends on the number of attempts made to breach user accounts and if locally logged-on user credentials are valid. If Conficker successfully uses harvested credentials to provide access across the ADMIN$ drive, then users have little chance of observing the technique. Conficker's brute-force of username and password feature would cause users to be locked out after too many invalid login attempts. OT Cybersecurity, IT Cybersecurity, or IT Staff would be notified of login disruption by security alert policies focusing on Event ID 4625: Login Failures.

A total of four observables were identified with the use of the Remote Services technique (T0886). This technique is important for investigation as access to various accounts allows adversaries to move between assets and network segments, resulting in the ability to configure systems. This technique appears early on the attack timeline and terminating the chain of techniques at this point would limit the adversaries to initial access points, resulting in a halt of attack execution. Additionally, terminating the chain of techniques at this point would likely prevent the malware from spreading to other systems.

Of the four observables associated with this technique, two are assessed to be highly perceivable (Windows Event ID 4624; Windows Event ID 4625).

Please see Appendix A for the list of observables.

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

3.4. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

Conficker disables access to vulnerabilities within the netapi32.dll and prevents access to this vector from other adversaries. The malware provides an in-memory patch to the RPC vulnerability (MS08-067) within the netapi32.dll, which removes the buffer overflow vector used to compromise the system. However, while the Conficker patch of the buffer overflow vector does protect against other adversaries, the malware authors specifically crafted the patch to allow other Conficker hosts to reinfect the victim. Conficker parses incoming RPC requests to search for a specific string within the Conficker shellcode, allowing remote access to victims when adversaries encounter the string.

A total of six observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because it presents noticeable effects, such as the generation of anomalous HTTP traffic, anomalous DNS requests, and the insertion of new domains into the environment. This technique appears early in the timeline and responding to it will effectively halt all future events, including modification of host OS files and access to additional Conficker-infected hosts. This technique modifies the host operating system files, leaving the host in a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired.

OT Cybersecurity, IT Cybersecurity, or IT Staff would perceive these network-based observables if a network baseline is established, and network traffic security protocols actively monitor outbound/inbound traffic.

Of the six observables associated with this technique, five are assessed to be highly perceivable (RPC Logs Potentially in Windows Event Logs; Visible on Network if SMB is not Encrypted; Connection to external IPs via HTTP; DNS Request Associated with Bad Domain; New Domain Inserted into the Environment).

Please see 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. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

After gaining initial access, Conficker further propagates by initiating a SMB session on Port 445/TCP with the targets discovered by the NetServerEnum execution. The infected host binds to the SRVSVC pipe and sends a NetPathCanonicalize request embedded with the exploit payload. The exploit prompts the target victim to contact the infected host on a connect-back port to download a portable executable (PE) DLL file. The exploit issues a Windows API call, so the service executes as a svchost.exe.[23]

This technique would require a network baseline to observe, limiting the number of observers who would be able to perceive the malware within their network. Due to its complexity, the observers, including IT Staff, IT Cybersecurity, and OT Cybersecurity, would have limited visibility.

A total of one observable was identified with the use of the Scripting technique (T0853). This technique is important for investigation due to its ability to assist with the propagation of malware across networks. This technique appears after initial access is achieved and assists with access to other connected devices. Responding to it will effectively halt an infection vector used by the malware. Terminating the chain of techniques at this point would result in minimal impact within an environment and stop the proliferation of the malware across similarly connected devices.

None of the observables are assessed to be highly perceivable.

Please see 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

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

To limit response capabilities, the malware worm monitors domain name system (DNS) requests to domains containing anti-Conficker strings, antivirus resources, and malware support. When an applicable DNS is found, user access appears as if the network request timed out and DNS is retransmitted, resulting in a blocked site.[24] This technique inhibits global census or distributing new binary updates to infected systems.[25]

OT Cybersecurity, IT Cybersecurity, and IT Staff may observe backups, deletion of restore points, and disabling of automatic backup settings.

A total of five observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation because malware worm authors typically generate new variants (e.g., Conficker A, Conficker B, Conficker C). This technique appears early in the timeline and responding to it allows infected machines to have access to sites to update security software. Terminating the chain of techniques at this point would limit the widespread effects of the malware worm. This technique modifies the host operating system files, via the modification of backup images and restore points, resulting in the host placing the device into a modified or compromised state. If system backups are created after this technique is executed, then data recovery and disaster recovery efforts will be impaired. Additionally, due to the deletion of backup images and restore points, this technique impairs data recovery and disaster recovery efforts.

Of the five observables associated with this technique, four are assessed to be highly perceivable (DNS Request Time Out; Increase in DNS Retransmissions; Disables Automatic Backup Settings; Deletes Backup/Restore Points).

Please see Appendix A for the list of observables.

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

3.7. ROOTKIT TECHNIQUE (T0851) FOR INHIBIT RESPONSE FUNCTION

To limit response capabilities, Conficker implements a rootkit. This step ensures connections to remote security sites are prevented and appear to users to time out in order to evade security software.[26] The worm's embedded rootkit blocks access to domain requests containing any of the strings depicted below. After the DNS retransmissions, the DNS request times out, creating the appearance of a connection failure.[27]

This increase in DNS retransmissions would show a slight increase in network latency. IT Staff, IT Cybersecurity, and OT Cybersecurity would receive alerts built on a network baseline if one had been established.

Activescan	Adware	Agnitum	Ahnlab	Anti-	Antivir
Arcabit	Avast	Avg	Avgate	Avrira	Avp.
Ac-sc	Bdtools	Bit9	Bothunter	Ca	Castlecops
Ccollomb	Centralcommand	Cert	Clamav	Comodo	Computerassociates
Confick	Coresecure	Cpsecure	Cyber-ta	Defender	Downad
Doxpara	Drweb	Dslreports	Emsisoft	Enigma	Esafe
Eset	Etrust	Ewido	Fortinet	F-prot	Freeav
Free-av	Fsecure	F-secure	Gdata	Gmer	Grisoft
Hackerwatch	Hackersoft	Hauri	Honey	Ikarus	Insecure
iv.cs.uni	Jotti	K7computing	Kaspersky	Kav	Kido
Llnw	Llnwd.	Malware	Mcafee	Microsoft	Mirage
Mitre	Msdn.	Msft	Msftncs	Ms-mvp	Msmvps
Mtc.sri	Nai	Ncircle	Networkassociates	Nmap	Nod32
Norman	Norton	Onecare	Panda	Pctools	Precisesecurity
Prevx	Ptsecurity	Qualys	Quickheal	Removal	Rising
Rootkit	Safety.live	Sans	Secunia	Secure computing	Secureworks
Snort	Sophos	Spamhaus	Spyware	Staysafe	Sunbelt
Symantec	Technet	Tenablese	Threat	Threatexpert	Trendmicro
Trojan	Vet	Virscan	Virus	Wilderssecurity	windowsupdate

A total of three observables were identified with the use of the Rootkit technique (T0851). This technique is important for investigation due to its noticeable user account lockdown effects and password security alerts, increasing awareness from the average user to the IT Department. This technique appears toward the end of the malware's infection phase and responding to it will alert IT of the malware's presence inside a network. Terminating the chain of techniques at this point

would increase the effectiveness of actions taken to limit further spreading within a given network. This technique modifies the host operating system files via the implementation of the rootkit, resulting in rootkit executables placing the host into a modified or compromised state. If system backups are created after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the three observables associated with this technique, all three are assessed to be highly perceivable (Network Request Timeouts from Security Related Websites; Increase in DNS Retransmissions; Blocking of Predetermined DNS Requests).

Please see 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 Rootkit technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

3.8. BLOCK REPORTING MESSAGE TECHNIQUE (T0804) FOR INHIBIT RESPONSE FUNCTION

To further disguise its activities, Conficker disables Window Security notifications, preventing the system from alerting the user that the malware is modifying registries. Access to SafeMode is prevented in the malware modified windows environment.[28]

Observers likely to see anomalous entries in the Event Viewer Log include OT Cybersecurity, IT Cybersecurity, and IT Staff.

A total of three observables were identified with the use of the Block Reporting Message technique (T0804). This technique is important for investigation because adversaries blocking report messages from the end user can lead to disabling a response function. This technique appears further along in the timeline and responding to it allows users to observe the current state of equipment. Terminating the chain of techniques at this point would allow users to respond in a proper or timely manner to an event, such as a dangerous fault. This technique modifies the host operating system files via the manipulation of system configuration settings and associated system registry entries, placing the host into a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the three observables associated with this technique, two are assessed to be highly perceivable (Prevents Access to Safe Mode; Event Viewer Log Entry).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 18 artifacts could be generated by the Block Reporting Message technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

3.9. ALARM SUPPRESSION TECHNIQUE (T0878) FOR INHIBIT RESPONSE FUNCTION

As an additional attempt to obscure evidence, Conficker modifies registries, disabling most mainstream security software programs from notifying staff of subsequent events. This step also prevents access to Safe Mode and disables Windows Security Alert notifications.[29]

OT Cybersecurity, IT Cybersecurity, and IT Staff may have observed modification within Event Viewer Log entries.

A total of three observables are identified with the use of the Alarm Suppression technique (T0878). This technique is important for investigation because it suppresses alerts built into security systems intended to alert staff of potential risks. This technique appears early in the timeline, and responding to it will limit operational impact, as staff would be aware of anomalous behavior in a system, allowing for earlier response. This technique modifies the host operating system files via the manipulation of system configuration settings and associated system registry entries, placing the host into a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the three observables associated with this technique, two are assessed to be highly perceivable (Disabling of Security Software; Event Viewer Log Entries).

Please see Appendix A for the list of observables.

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

3.10. MASQUERADING TECHNIQUE (T0849) FOR EVASION

Conficker uses a simple but effective mechanism to cloak its runtime presence. Although the service starts through svchost.exe, it is not visible in the service manager because its DisplayName is set to be empty, and type is set to be invisible. Then, unlike well-behaved DLLs, the Conficker DLL initialization function never returns, hence it is not added to the DLL list of the given process. Since the DLL is added as part of a group that includes other normal services in the netsvcs group, the instance of svchost.exe is not terminated, allowing Conficker to run behind the scenes. Another masquerading capability of Conficker is to remove an offensive registry key, reboot the system, and delete the corresponding DLL file from the system32 directory.[30]

OT Cybersecurity, IT Cybersecurity, and IT Staff could observe DLL creation, renaming, and deletion.

A total of two observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation as adversaries purposely disguise files so staff may not suspect malicious applications or executables. This technique appears further along the attack timeline and responding to it would allow staff to stop execution of malicious files. Terminating the chain of techniques at this point would limit adversaries to reconnaissance activity. This technique modifies the host operating system files via the manipulation of system configuration settings and associated system registry entries, placing the host into a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the two observables associated with this technique, one is assessed to be highly perceivable (Registered DLLs with DisplayName Set to Empty and Type Set to Invisible).

Please see Appendix A for the list of 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

3.11. MODIFY PROGRAM TECHNIQUE (T0889) FOR PERSISTENCE

After the malware has ensured it will remain undetected on the system, it connects to one of its predetermined external IP address domains to see if it needs to update itself. If it does, then the malware will connect, and a HTTP server is created on the infected machine. This HTTP server is leveraged later for lateral movement. Meanwhile, as the files download, the Conficker malware updates to the most recent version.[31]

OT Cybersecurity, IT Cybersecurity, and IT Staff may observe anomalous entries within an Event Viewer Log.

A total of four observables were identified with the use of the Modify Program technique (T0889). This technique is important for investigation as modifying programs and ensuring proper updates are installed affects how the malware interacts with the different systems. This technique appears further along in the timeline and responding to it will prevent malware updates from occurring. This technique modifies the host operating system files via creation of the HTTP server and modification of system registry entries, placing the host into a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the four observables associated with this technique, two are assessed to be highly perceivable (Download of Files; Event Viewer Log Entries).

Please see Appendix A for the list of 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

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

Conficker queries a list of random domains, checking for ones that are live. The malware then attempts to resolve each generated domain name to an IP address. If it succeeds, it sends an HTTP request to the resolved domain. Data from the HTTP request is parsed and saved to memory. Conficker verifies the signature of any data received from this HTTP request, determining if the bytes returned are authentic and signed. If the signature is valid, then the data received is decrypted and executed. This step updates Conficker using only "authentic" sources, as determined by the signature of the returned bytes.

OT Cybersecurity, IT Cybersecurity, or IT Staff would perceive these network-based observables if a network baseline is established, and network traffic security protocols actively monitor outbound/inbound traffic. The unauthorized outbound HTTP request would alert Cybersecurity personnel and IT Staff that anomalous activity was occurring in the network, prompting a cyber incident investigation.

A total of five observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation due to its outbound connection and development of adversary-generated domains within a network. This technique appears before the proliferation stage and responding to it will limit the outbound traffic and connection to malicious URL domains. Terminating the chain of techniques at this point would stop the connection to malicious domains and therefore not allow for further adversary activity. This technique potentially modifies the host operating system files via the potential download and installation of signed data, placing the host into a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the five observables associated with this technique, three are assessed to be highly perceivable (Targeting TCP 445 (SMB); Connection to Malicious URL Domains for C2C; Windows Event Log Entries).

Please see 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 Standard Application Layer Protocol technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

3.13. COMMONLY USED PORT TECHNIQUE (T0885) FOR COMMAND AND CONTROL

The Conficker malware abuses the RPC vulnerability (MS08-067) through the use of the commonly used Port 445/TCP to initiate an SMB session. The malware can then bind to the SRVSVC pipe and issue the NetPathCanonicalaize request, which houses the exploit payload.[32]

Windows Event Log entries indicate the creation of an HTTP Server and an increase in RPC traffic would be observable to those with an established baseline. Observers of this technique would primarily be those associated with the monitoring of network traffic and endpoint monitoring, namely through anomalous RPC and SMB traffic, as well as Windows Log entries and HTTP server creation. Observers of this technique would include IT staff, IT Cybersecurity and OT Cybersecurity personnel.

A total of five observables were identified with the use of the Commonly Used Port technique (T0885). This technique is important for investigation as adversaries may communicate over a commonly used port to bypass firewalls or network detection systems. This technique appears relatively late in the timeline and may alert personnel to abnormal activity, prompting a cyber incident response. Terminating the chain of techniques at this point would allow personnel to investigate unusual network traffic, decreasing comprehension time.

Of the five observables associated with this technique, three are assessed to be highly perceivable (RPC Traffic; Targeting TCP 445 (SMB); Windows Event Log Entries).

Please see Appendix A for the list of observables.

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

3.14. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

Conficker utilizes the HTTP server created in the Modify Program technique (T0889) to perform peer-to-peer (P2P) UDP scans. These scans are conducted on Port 53/UDP to identify other machines on the network by targeting random IP addresses. This scanning is the initial P2P setup routine for W32.Downadup.C.[33]

If traffic monitoring is executed properly, OT Cybersecurity, IT Cybersecurity, and IT Staff should observe an increase in UDP traffic compared to baseline activity.

A total of two observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation as discovering a list of other systems on a network by IP address, hostname, or other logical identifiers could allow adversaries to laterally move throughout a network. This technique appears late in the timeline, close to the triggering event, and responding to it will effectively prevent the spread of Conficker throughout machines on a network.

Of the two observables associated with this technique, one is assessed to be highly perceivable (High UDP Traffic).

Please see 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

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

Conficker uses the Remote System Information Discovery technique (T0888) in multiple ways. The malware includes a P2P mechanism, enabling machines infected with Conficker variants C through E to communicate, instructing them to download W32.Waledac.[34] Conficker can act as both a client and a server to share content, both distributing to and receiving from other Conficker-infected computers. Conficker includes an algorithm to deterministically generate a set of domain names each day and contact those domains throughout the day to check if an updated version of the worm is available for download.

Four scanning threads generate a random list of IP addresses for the hosts to contact. The same IP-to-port mapping is used to help determine which ports on which IPs could be targeted. Conficker then uses an HTTP server to communicate with another device and determine whether it is already infected. A Conficker host can have up to 32 Conficker server instances running, with each IP address generating a server instance. Conficker simultaneously checks the binary updates of the infected computers to see if the Conficker-only content is digitally signed by Conficker authors to distribute between peers. Terminating the chain of techniques at this point would likely prevent the malware from spreading to other systems.

Observers of this technique may include OT Cybersecurity, IT Cybersecurity, and IT Staff.

There were three observables identified with the use of the Remote System Information Discovery technique (T0888). This technique is important for investigation since adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifiers on a network that is used for lateral movement or discovery techniques.

Of the three observables associated with this technique, one is assessed to be highly perceivable (HTTP request (getmyip.org, getmyip.co.uk, checkip.dyndns.org)).

Please see Appendix A for the list of observables.

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

3.16. REMOTE SERVICES TECHNIQUE (T0886) FOR LATERAL MOVEMENT

The Remote Services technique (T0886) occurs as Conficker uses network shares to further spread itself throughout a given network. In doing this, Conficker runs rundll32.exe to copy itself through the system and will sleep after this technique is performed to prevent itself from being detected. It also identifies admin share drives or Inter-process Communication (IPC).[35]

OT Cybersecurity, IT Cybersecurity, and IT Staff may observe the use of this technique.

A total of two observables were identified with the use of the Remote Services technique (T0886). This technique is important for investigation as it allows adversaries to move between assets and network segments, resulting in the ability to configure systems. This technique appears both early on the attack timeline with initial access while later being used for lateral movement into another systems. Terminating the chain of techniques at this point would limit the malware's spread throughout the network.

Of the two observables associated with this technique, none are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

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

3.17. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

The next step in Conficker's attack chain is to query valid user accounts on a target remote server. To authenticate with the target, Conficker tries the credentials of the locally logged-on user first. If these credentials do not work, then the malware begins trying different username and password pairs.[36] The malware attempts to brute-force these accounts by using a table of 240 common passwords.[37]

With security policy best practices implementation, OT Cybersecurity, IT Cybersecurity, and IT Staff could observe network traffic associated with this activity, such as sending password lists, querying users, and communication between targets.

A total of two observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because compromised credentials are used to bypass access controls to various resources within a network or grant an adversary increased privileges to specific systems and devices. This technique appears later in the timeline for this case and responding to it will effectively limit access to protected machines. Terminating the chain of techniques at this point would likely prevent the malware from spreading to other systems.

Of the two observables associated with this technique, one is assessed to be highly perceivable (Network Traffic Associated with Work (Sending of Password List, Querying of Users, Communication Between Targets).

Please see 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

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

The Exploitation of Remote Services technique (T0866) is seen in Conficker's use of MS08-067, otherwise known as CVE-2008-4250, to attack other uninfected machines.[38] This exploit makes use of a RCE Vulnerability present in the RPC component of Microsoft Windows Server Service.[39] This technique is only effective against computers that have not applied the patch for the Microsoft Windows Server Service RPC Vulnerability (BID 31874). By targeting TCP Port 445, this exploit allows an adversary to trigger an overflow in the path canonicalization functionality of RPC and execute arbitrary code on a remote machine via use of a crafted RPC request.[40] If the malware successfully exploits the issue, the worm then creates an HTTP server on the compromised computer on a random port.[41]

If a network baseline is properly setup and monitoring capabilities are in place, OT Cybersecurity, IT Cybersecurity, and IT Staff may observe Event Viewer Log Entries.

A total of five observables were identified with the use of the Exploitation of Remote Services technique (T0866). This technique is important for investigation as software vulnerabilities are a common way for adversaries to take advantage of a programming error to enable remote service abuse. This technique appears late in the timeline and responding to patches released with vulnerabilities will limit spread to other networks.

Of the five observables associated with this technique, three are assessed to be highly perceivable (RPC Traffic; Targeting TCP (445); Event Viewer Log Entries).

Please see Appendix A for the list of observables.

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

3.19. PROGRAM DOWNLOAD TECHNIQUE (T0843) FOR LATERAL MOVEMENT

Before the download of scareware software, Conficker reads 0x400 bytes, and if the buffer is null-terminated, the malware passes the message to the function thread_download_file_from_url using Port 80/TCP (HTTP).[42] The message is interpreted as a string representing a URL (https://trafficconverter.biz/4vir/antispyware/) used to download an executable, loadadv.exe. Conficker then downloads two malicious files within this executable, W.32 Waledac and SpywareProtect2009.[43] Waledac is used to send spam via email, download and execute arbitrary files, harvest email addresses from the infected machine, proxy network traffic, sniff passwords, and perform denial of service attacks.[44] SpyProtect2009 is a form of scareware that provides users with false indication that their computers were infected with malware.[45] It then encourages users to pay for the product to remove these phantom threats from the machine.[46]

If proper configurations are in place, OT Cybersecurity, IT Cybersecurity, and IT Staff may observe Event Viewer Log Entries.

A total of four observables were identified with the use of the Program Download technique (T0843). This technique is important for investigation since it allows adversaries to transfer a malicious program to end user devices. This technique appears later in the timeline and responding to it will prevent malicious payloads from propagating to additional machines. This technique modifies the host operating system files via the installation of Waledac and SpyProtect2009, and modifies system registry entries, resulting in the host being placed into a modified or compromised state. If system backups are created after this technique is executed, data recovery and disaster recovery efforts will be impaired.

Of the four observables associated with this technique, three are assessed to be highly perceivable (File download: loadadv.exe; Web Connection to https://trafficconverter.biz/4vir/antispyware/; Event Viewer Log Entries).

Please see Appendix A for the list of observables.

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

3.20. MANIPULATION OF CONTROL TECHNIQUE (T0831) FOR IMPACT

Conficker uses the Manipulation of Control technique (T0831) after its infection phase is complete. The Conficker malware connects to an external domain to add the newly infected computer to a list among several linked botnets. Once Conficker establishes a foothold it creates a bi-directional pipe (CreateNamedPipe API) where both the server and clients can write and read streams of messages limited to 0x400 bytes. The attacker could execute arbitrary code at this point or make changes to set point values, tags, or other parameters. The malware can also manipulate and disable Windows services related to updates, security, and removal products by denying users web access. This technique can be observed by logging and log analysis at both the network and host levels. Firewall, router, and host logs (including server logs) could all produce indicators of attack.

IT staff, OT Cybersecurity, and IT Cybersecurity personnel could observe this technique by establishing a network baseline and monitoring network traffic.

Two observables were identified with the Manipulation of Control technique (T0831). This technique is important for investigation as it may present an impact for the end-users or consumers of products and services. Terminating the chain of techniques at this point would likely limit the ability of the malware to spread and cause negative impacts to other systems, as well as limit the overall utility of the malware campaign by limiting individual nodes from executing unauthorized commands.

The two observables associated with this technique are assessed to be highly perceivable (Execution of Arbitrary Code through Botnet Configuration; CreateNamedPipe API).

Please see 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 Manipulation of Control technique
Technique Observers	OT Cybersecurity, IT Cybersecurity, IT Staff

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

The Loss of Productivity and Revenue technique (T0828) represents the computer system shutdown required to contain and sanitize the malware. Gundremmingen was taken offline for two days after the discovery of the Conficker infection to perform scanning and mitigating security operations. This shutdown resulted in a loss of $2.6 million in revenue.[47]

Because of the magnitude and global proliferation of Conficker impacts, the potential worldwide cost of finding and mitigating the malware is estimated at $9.1 billion or more.[48] If the malware is not mitigated, Conficker could be leveraged by additional adversaries with potentially catastrophic results. For example, in 2011, a hacking gang from Ukraine used Conficker to trick people into buying fake anti-virus products, costing victims a total of $72 million dollars.[49]

OT Cybersecurity, IT Cybersecurity, IT Staff, Engineering, OT Staff, Management, and Support Staff would perceive this technique through its impact on productivity and revenue loss.

Three observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation as it may present an impact for the end-users or consumers of products and services.

The three observables associated with this technique are assessed to be highly perceivable (Loss of Two Days of Productivity; Cost of “Spyware” Antivirus; Estimated Global Cost of $9.1 Billion).

Please see Appendix A for the list of 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	OT Cybersecurity, IT Cybersecurity, IT Staff, Engineering, OT Staff, Management, Support Staff

3.22. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

The Loss of Availability technique (T0826) occurred during a routine security audit that discovered the malware in the IT network of the Block B fuel IT computers.[50] Though it never reached the SCADA systems of the plant, officials decided to follow their predetermined security procedures and shut down the affected systems for two days. They used antivirus software to scan the plant's other systems and rolled systems to their last safe backup. All staff would have been able to observe the emergency shutdown system initiation.

OT Cybersecurity, IT Cybersecurity, IT Staff, Engineering, OT Staff, Management, and Support Staff would perceive this technique through its impact on system access and availability.

Three observables were identified with the use of the Loss of Availability technique (T0826). This technique is important for investigation as it prevents owners and operators from delivering products or services. This technique appears after the triggering event.

All three observables associated with this technique are assessed to be highly perceivable (Anti-virus Alerts; Two-day Downtime Due to Reconfiguration; Rollback to Last Safe Backup).

Please see Appendix A for the list of observables.

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

APPENDIX A: OBSERVABLES LIBRARY

The observables listed here were associated or believed to be associated with the use of Conficker at Gundremmingen Nuclear Power Plant.

Observables Associated with Replication Through Removable Media Technique (T0847)	
Observable 1	Autorun.inf Execution Feature
Observable 2	Drive Creation
Observable 3	File Creation
Observable 4	Process Access
Observable 5	Autoplay Alert
Observable 6	Windows Event Log Entries

Observables Associated with Exploitation of Remote Services Technique (T0866)	
Observable 1	Remote Procedure Call (RPC) Traffic
Observable 2	Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874)
Observable 3	TCP Port 445 SMB Network File
Observable 4	Creation of HTTP Server on a Random Port
Observable 5	Windows Event Log Entries

Observables Associated with Remote Services Technique (T0886)	
Observable 1	Use of Admin Network Share (ADMIN$)
Observable 2	NetServerEnum Request
Observable 3	Windows Event ID 4624: Login
Observable 4	Event ID 4625: Login Failures

Observables Associated with Native API Technique (T0834)	
Observable 1	Netapi32.dll and Zeek dcerpc.log
Observable 2	Remote Procedure Call (RPC) Logs in Windows Event Logs
Observable 3	Visible on Network if SMB is not Encrypted
Observable 4	Connect Back HTTP Connection
Observable 5	DNS Request Associated with Bad Domain
Observable 6	New Domain into the Environment

Observables Associated with Scripting Technique (T0853)	
Observable 1	Portable Executable (PE) Dropped to Disk

Observables Associated with Service Stop Technique (T0881)	
Observable 1	Denial of DNS Requests to Domains Containing Conficker Antivirus
Observable 2	DNS Request Timeout
Observable 3	Increase in DNS Retransmissions
Observable 4	Disables Automatic Backup Settings
Observable 5	Deletes Backup/Restore Points

Observables Associated with Rootkit Technique (T0851)	
Observable 1	Network Request Time out from Security Related Websites
Observable 2	Increase in DNS Retransmissions
Observable 3	Blocking of Predetermined DNS Requests

Observables Associated with Block Reporting Message Technique (T0804)	
Observable 1	Disable Windows Security Alert Notifications
Observable 2	Prevents Access to Safe Mode
Observable 3	Event Viewer Log Entries

Observables Associated with Alarm Suppression Technique (T0878)	
Observable 1	Disabling of Security Software
Observable 2	Prevent Access to Safe Mode
Observable 3	Event Viewer Log Entries

Observables Associated with Masquerading Technique (T0849)	
Observable 1	DLL Creation, Renaming, and Deletion
Observable 2	Registered DLLs with DisplayName Set to Empty and Type Set to Invisible

Observables Associated with Modify Program Technique (T0889)	
Observable 1	External IP Address Connection
Observable 2	HTTP Server Creation
Observable 3	File Download to Update Conficker Malware Form
Observable 4	Event Viewer Log Entries

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1	Microsoft Windows Server Service Remote Procedure Call (RPC) Handling Remote Code Execution Vulnerability (BID 31874)
Observable 2	Targeting TCP Port 445 (SMB)
Observable 3	External Network Connections
Observable 4	Connection to Malicious URL Domains for C2C
Observable 5	Windows Event Log Entries

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 1	Remote Procedure Call (RPC) Traffic
Observable 2	Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874)
Observable 3	Targeting TCP Port 445 (SMB)
Observable 4	Creation of HTTP Server
Observable 5	Windows Event Log Entries

Observables Associated with Remote System Discovery Technique (T0846)	
Observable 1	High UDP Traffic
Observable 2	Port 53/UDP (DNS)

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 1	HTTP Request
Observable 2	Binary Updates Check
Observable 3	File Signature Check

Observables Associated with Remote Services Technique (T0886)	
Observable 1	Execution of rundll32.exe
Observable 2	Identification of Admin Share or Interprocess Communication (IPC)

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Brute-Force Password Attempts
Observable 2	Associated Network Traffic

Observables Associated with Exploitation of Remote Services Technique (T0866)	
Observable 1	Remote Procedure Call (RPC) Traffic
Observable 2	Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874)
Observable 3	Targeting TCP Port 445
Observable 4	Creation of HTTP Server
Observable 5	Event Viewer Log Entries

Observables Associated with Program Download Technique (T0843)	
Observable 1	Port 80/TCP (HTTP)
Observable 2	Web Connection to https://trafficconverter.biz/4vir/antispyware/
Observable 3	File Download loadadv.exe
Observable 4	Event Viewer Log Entries

Observables Associated with Manipulation of Control Technique (T0831)	
Observable 1	Execution of Arbitrary Code through Botnet Configuration
Observable 2	CreateNamedPipe API

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1	Loss of Two Days Productivity
Observable 2	Estimated Global Cost of $9.1 Billion
Observable 3	Cost of “Spyware” Antivirus

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1	Two-day Downtime Due to Reconfiguration
Observable 2	Antivirus Alerts
Observable 3	Rollback to Last Safe Backup

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Replication Through Removable Media Technique (T0847)	
Artifact 1	ARP Connections
Artifact 2	FTP Port 21
Artifact 3	FTPS Port 990
Artifact 4	HTTPS Port 443
Artifact 5	HTTP Port 80
Artifact 6	USB Make
Artifact 7	USB Model
Artifact 8	USB Version
Artifact 9	USB Serial Number
Artifact 10	Mass Storage Class (MSC) Connections
Artifact 11	Picture Transfer Protocol (PTP) Connections
Artifact 12	MAC Address
Artifact 13	Media Transfer Protocol (MTP) Connections
Artifact 14	.LNK File
Artifact 15	Network Discovery Protocols Traffic
Artifact 16	Changes to System Registry SYSTEM\CurrentControlSet\Enum\USBSTOR
Artifact 17	Drive Letter Creation
Artifact 18	Changes to System Registry SYSTEM\MountedDevices
Artifact 19	Bytes sent from System Resource Usage Manager (SRUM)
Artifact 20	Bytes Received from SRUM
Artifact 21	Device User (USB)
Artifact 22	Last Time Device Connected (USB)
Artifact 23	Source IP Address
Artifact 24	First Time Device Connected (USB)
Artifact 25	Device Disconnected Time (USB)
Artifact 26	Wireless Transmission
Artifact 27	Plug and Play Log File setupapi.log
Artifact 28	System Log Plug and Play Driver Installed Event 20001
Artifact 29	Security Log Attempt to Access Removable Storage Object Event (4663)
Artifact 30	Security Log Failure to Access Removeable Device (4656)
Artifact 31	Network Connections with Honeypot
Artifact 32	Honey Pot Logs
Artifact 33	User Agents

Artifacts Associated with Replication Through Removable Media Technique (T0847)	
Artifact 34	DNS Queries Traffic
Artifact 35	File Access Created
Artifact 36	File Access Removed
Artifact 37	Process Creation
Artifact 38	Process Termination
Artifact 39	Device Failure
Artifact 40	Device Reboot
Artifact 41	Performance Degradation
Artifact 42	Command Line Dialog Box Opened
Artifact 43	Recent Connections Metadata Change
Artifact 44	RDP Traffic Port 3389
Artifact 45	VNC Traffic Port 5900
Artifact 46	SSH Traffic Port 22
Artifact 47	Telnet Traffic
Artifact 48	TFTP Port 69

Artifacts Associated with Exploitation of Remote Services Technique (T0866)	
Artifact 1	Application Logs
Artifact 2	Connection to HMI End Points
Artifact 3	Connection to EWS End Points
Artifact 4	Connection to Data Historian End Points
Artifact 5	Connection to Controller End Points
Artifact 6	Manipulation of Process
Artifact 7	Manipulation of Set Points
Artifact 8	Misconfigurations of End Points
Artifact 9	Process Failure
Artifact 10	Controller Failure
Artifact 11	Code Injections into Application
Artifact 12	Application Log on Event
Artifact 13	Code Injection into the OS
Artifact 14	OPC Code Injection
Artifact 15	Database Command Executions
Artifact 16	User Events Across Multiple Devices
Artifact 17	Host System Registry Changes

Artifacts Associated with Exploitation of Remote Services Technique (T0866)	
Artifact 18	Security Events Across Multiple Devices
Artifact 19	Kernel Level Events
Artifact 20	System Reboots
Artifact 21	Blank Screens
Artifact 22	Safemode Reboot
Artifact 23	Application Log off Event
Artifact 24	Alarm Events
Artifact 25	Absence of Alarm Events
Artifact 26	Common Network Traffic
Artifact 27	Remote Network Traffic
Artifact 28	Vendor Specific Network Traffic
Artifact 29	Industrial Protocol Network Traffic
Artifact 30	SQL Protocol
Artifact 31	SMB Protocol

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 1	Remote Client Connection
Artifact 2	Logon Event
Artifact 3	Logoff
Artifact 4	Logoff Event
Artifact 5	Registry Changes
Artifact 6	Registry Connection Change
Artifact 7	Mouse Movement
Artifact 8	Unexpected I/O
Artifact 9	Desktop Prompt Windows Created
Artifact 10	Session Cache
Artifact 11	Application Log
Artifact 12	RDP Traffic Port 3389
Artifact 13	System Log Event
Artifact 14	Authentication Logs
Artifact 15	GUI Modifications
Artifact 16	Data File Size in Network Content
Artifact 17	File Movement
Artifact 18	MSSQL Traffic Port 1433

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 19	SSH Traffic Port 22
Artifact 20	SMB Traffic Ports 139, 445
Artifact 21	VNC Traffic Ports 5800, 5900
Artifact 22	Process Creation
Artifact 23	Remote Session Creation Timestamp
Artifact 24	Network Traffic Content Creation

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

Artifacts Associated with Scripting Technique (T0853)	
Artifact 1	Files Dopped into Directory
Artifact 2	System Event Log Creation
Artifact 3	OS Timeline Event
Artifact 4	Startup Menu Modification
Artifact 5	System Processes Created
Artifact 6	Windows API Event Log
Artifact 7	Executable Files
Artifact 8	Prefetch Files Created
Artifact 9	External Network Connections
Artifact 10	Network Services Created
Artifact 11	Registry Modifications
Artifact 12	OS Service Installation

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

Artifacts Associated with Rootkit Technique (T0851)	
Artifact 1	Drive Modification
Artifact 2	Industrial Network Traffic for Remote Code Execution
Artifact 3	Remote Network Traffic for Remote Code Execution
Artifact 4	Modified Reporting
Artifact 5	Failed Reporting

Artifacts Associated with Rootkit Technique (T0851)	
Artifact 6	Blue Screen on Workstation
Artifact 7	System Resource Usage Monitor (SRUM) Metadata Changes
Artifact 8	Performance Mismatched with Performance Reporting
Artifact 9	Packet Mismatch Between Network and Host Sources
Artifact 10	Unusual Protocol Field Values
Artifact 11	Increased Maintenance Without Faults Reported
Artifact 12	Firmware Number Modification
Artifact 13	Blocked Read Requests at OS Level
Artifact 14	Blocked Delete Requests at OS Level
Artifact 15	Blocked Create Requests at OS Level
Artifact 16	Blocked Write Requests at OS Level
Artifact 17	Firmware Flash Update
Artifact 18	Device Reboot
Artifact 19	Device Failure
Artifact 20	Dropped API Calls
Artifact 21	Application Logs
Artifact 22	Dialog Box Requesting Update
Artifact 23	Common Network Traffic for Remote Code Execution

Artifacts Associated with Block Reporting Message Technique (T0804)	
Artifact 1	Application Modification
Artifact 2	Physical Process Changes without Data Received
Artifact 3	Conflicting Device Status Reports
Artifact 4	I/O Values Mismatched with Process Current State
Artifact 5	Delayed Operational Process Status Change
Artifact 6	Application Log Event Absent
Artifact 7	Historian Database Missing Data
Artifact 8	I/O Server Nonresponsive
Artifact 9	Real-Time Operational Data Missing
Artifact 10	Supervisory Application Logs Mismatch Current State
Artifact 11	Process Status Modification
Artifact 12	Network Traffic Changes
Artifact 13	Network Connections Creation
Artifact 14	Operational Device Failure

Artifacts Associated with Block Reporting Message Technique (T0804)	
Artifact 15	Operational Database Data Modification
Artifact 16	Operational Database Configuration Change
Artifact 17	Operational Process Termination
Artifact 18	Operational Process Alarm Failures

Artifacts Associated with Alarm Suppression Technique (T0878)	
Artifact 1	Modification of Alarm Set Points
Artifact 2	Runaway Process State
Artifact 3	Catastrophic Failures
Artifact 4	Configuration Change Logs
Artifact 5	Increased Number of Output Quality Assurance Failures
Artifact 6	Insertion of Malicious Industrial Protocol to Suppress True Process Values
Artifact 7	Modification of SQL Database Inputs
Artifact 8	SQL Protocol Network Traffic
Artifact 9	External Connection to Operational Database
Artifact 10	Mismatch Between Sensor Reporting and Physical Process
Artifact 11	Change in Process Output
Artifact 12	Increased Maintenance Issues
Artifact 13	Control System Degradation

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

Artifacts Associated with Masquerading Technique (T0849)	
Artifact 14	Applications Causing Unintended Actions
Artifact 15	Additional Functionality in Applications

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

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

Artifacts Associated with Commonly Used Port Technique (T0885)	
Artifact 1	Unexpected Process Usage of Common Port Observed via OS Commands (Netstat)
Artifact 2	Unexpected Process Usage of Common Port Observed via Memory
Artifact 3	Unexpected Process Usage of Common Port Observed via OS Logs
Artifact 4	Unexpected Process Usage of Common Port Observed via Firewall Logs
Artifact 5	Unexpected Host Communicating with Common Port on Industrial Asset

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 1	Common Network Traffic
Artifact 2	IEC 103 Traffic (for North America)
Artifact 3	IEC 61850 MMS and GOOSE

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 4	Controller Proprietary Traffic
Artifact 5	Echo Type 8 Traffic
Artifact 6	ICMP Type 7 Traffic
Artifact 7	SNMP Port 162 Traffic
Artifact 8	SNMP Port 161 Traffic
Artifact 9	Command Line Dialog Box Open
Artifact 10	Operating System Queries
Artifact 11	DNS Port 53 Zone Transfers
Artifact 12	Industrial Network Traffic Content about Hostnames
Artifact 13	Polling Network Traffic from Unauthorized IP Sender Addresses
Artifact 14	NetBIOS Name Services Port 137
Artifact 15	LDAP Port 389
Artifact 16	Active Directory Calls
Artifact 17	Email Server Calls
Artifact 18	SMTP Port 25 Traffic
Artifact 19	DNS Lookup Queries
Artifact 20	ARP Scans
Artifact 21	TCP Connect Scan
Artifact 22	TCP SYN Scans
Artifact 23	Scans over Industrial Network Ports with Target IPs
Artifact 24	TCP FIN Scans
Artifact 25	TCP Reverse Ident Scan
Artifact 26	TCP XMAS Scan
Artifact 27	TCP ACK Scan
Artifact 28	VNC Port 5900 Calls
Artifact 29	Protocol content Enumeration
Artifact 30	Protocol Header Enumeration
Artifact 31	Recurring Protocol SYN Traffic
Artifact 32	Sequential Protocol SYN Traffic
Artifact 33	Statistical anomalies in network traffic
Artifact 34	Industrial Network Traffic Content Containing Logical Identifiers
Artifact 35	Device Failure
Artifact 36	Device Reboot
Artifact 37	Bandwidth Degradation

Artifacts Associated with Remote System Discovery Technique (T0846)	
Artifact 38	Host Recent Connection Logs
Artifact 39	Industrial Network Traffic
Artifact 40	OPC Network Traffic
Artifact 41	IEC 104
Artifact 42	IEC 102
Artifact 43	IEC 101 Traffic to Serial Devices

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

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 1	Logons
Artifact 2	Default Credential Use
Artifact 3	Application Log
Artifact 4	Domain Permission Requests
Artifact 5	Permission Elevation Requests
Artifact 6	Application Use Times
Artifact 7	Configuration Changes
Artifact 8	Prefetch Files Created After Execution
Artifact 9	Logon Session Creation
Artifact 10	User Account Creation
Artifact 11	Authentication Creation
Artifact 12	System Logs
Artifact 13	Successful Logon Event ID: 4624
Artifact 14	Failed Logons Event ID: 4625

Artifact 15	Logon Timestamp
Artifact 16	Logon Type Entry

Artifacts Associated with Program Download Technique (T0843)	
Artifact 1	Controller in Stop State
Artifact 2	Operational Process Restart
Artifact 3	Operational Database Data Modification
Artifact 4	Device Alert
Artifact 5	Device Alarm
Artifact 6	Controller Application Log Event
Artifact 7	Supervisory Workstation Program Download Popup
Artifact 8	Controller Application Log Type
Artifact 9	Controller Application Log Timestamp
Artifact 10	Controller Network Connections via Management Protocol
Artifact 11	Controller Connection to External Website
Artifact 12	Controller in Program State
Artifact 13	Controller Connected to External Networks
Artifact 14	Network Traffic Creation
Artifact 15	Network Metadata
Artifact 16	External Domain Connection
Artifact 17	External IP Address
Artifact 18	Controller State Change
Artifact 19	Operational Process Shutdown

Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 1	HMI Input Manipulation
Artifact 2	Command Execution
Artifact 3	Event Log Creation
Artifact 4	Application Log Event
Artifact 5	Altered Command Sequences
Artifact 6	Application File Modification
Artifact 7	Operational Data Modification
Artifact 8	I/O Modification
Artifact 9	Engineering Workstation Mouse Movement
Artifact 10	Controller Set Point Change

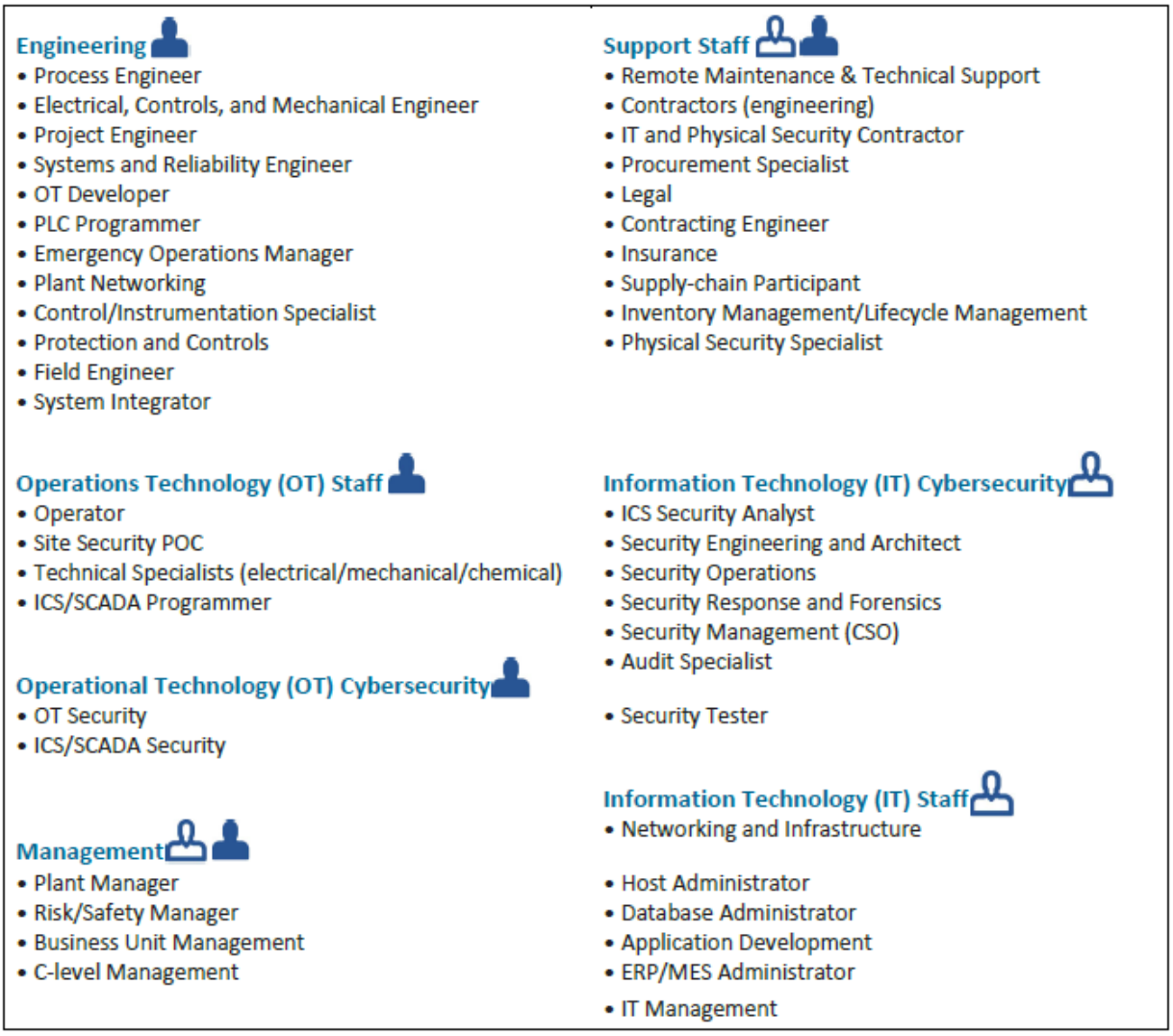
Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 11	Controller Parameter Change
Artifact 12	Controller Tag Change
Artifact 13	Process State Change
Artifact 14	Process Shutdown
Artifact 15	Process Restart
Artifact 16	Process Initiated

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

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

APPENDIX C: OBSERVERS

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



REFERENCES

[1] [SENKI | The Rendon Group | “Conficker Working Group: Lessons Learned” | https://www.senki.org/wp-content/uploads/2020/11/Conficker-Working-Group-Lessons-Learned-June-2010-Published-January-2011-whitepaper_76813745321.pdf|January 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[2] [Reuters | Christoph Steitz and Eric Auchard | “German nuclear plant infected with computer viruses, operator says” | https://www.reuters.com/article/us-nuclearpower-cyber-germany-idUKKCN0XN2OS | 26 April 2016 | Accessed 1 July 2022 | The source is publicly available information and does not contain classification markings]

[3] [Softpedia | Catalin Cimpanu | “Malware Shuts Down German Nuclear Power Plant on Chernobyl’s 30th Anniversary” | https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml | 26 April 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[4] [Reuters | Christoph Steitz and Eric Auchard | “German nuclear plant infected with computer viruses, operator says” | https://www.reuters.com/article/us-nuclearpower-cyber-germany-idUKKCN0XN2OS | 26 April 2016 | Accessed 1 July 2022 | The source is publicly available information and does not contain classification markings]

[5] [IEEE Xplore| Seungwon Shin, Guofei Gu, Narasimha Reddy, and Christopher P. Lee | “A Large-Scale Empirical Study of Conficker” | https://ieeexplore.ieee.org/document/6060910 | 25 October 2011 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[6] [Softpedia | Catalin Cimpanu | “Malware Shuts Down German Nuclear Power Plant on Chernobyl’s 30th Anniversary” | https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml | 26 April 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[7] [Reuters | Christoph Steitz and Eric Auchard | “German nuclear plant infected with computer viruses, operator says” | https://www.reuters.com/article/us-nuclearpower-cyber-germany-idUKKCN0XN2OS | 26 April 2016 | Accessed 1 July 2022 | The source is publicly available information and does not contain classification markings]

[8] [Usenix | “A Foray into Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/ | 7 April 2017| Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[9] [Softpedia | Catalin Cimpanu | “Malware Shuts Down German Nuclear Power Plant on Chernobyl’s 30th Anniversary” | https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml | 26 April 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[10] [Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics” | https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[11] [Symantec | Jarrad Shearer | “W32.Downadup” | https://web.archive.org/web/20190930212315/https:/www.symantec.com/security-center/writeup/2008-112203-2408-99 | 30 Sep. 2019 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[12] [Symantec | Jarrad Shearer | “W32.Downadup” | https://web.archive.org/web/20190930212315/https:/www.symantec.com/security-center/writeup/2008-112203-2408-99 | 30 Sep. 2019 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[13] [Usenix | “A Foray into Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/ | 7 April 2017| Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[14] [SRI International | Philip Porras, Hassen Saidi, and Vinod Yegneswaran | “An Analysis of Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/index2.html | 4 February 2009 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[15] [SRI International | Philip Porras, Hassen Saidi, and Vinod Yegneswaran | “An Analysis of Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/index2.html | 4 February 2009 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[16] [Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics” | https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[17] [Usenix | “A Foray into Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/ | 7 April 2017 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[18] [Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics” | https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[19] [Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics”| https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[20] [Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics”| https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[21] [Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics” | https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[22] Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics”| https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[23] [SRI International | Philip Porras, Hassen Saidi, and Vinod Yegneswaran | “An Analysis of Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/index2.html | 4 February 2009 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[24] [Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics”| https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[25] [Usenix | “A Foray into Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/ | 7 April 2017 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[26] [Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics” | https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[27] [Symantec | Jarrad Shearer | “W32.Downadup” | https://web.archive.org/web/20190930212315/https:/www.symantec.com/security-center/writeup/2008-112203-2408-99 | 30 Sep. 2019 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings

[28] [Symantec | Jarrad Shearer | “W32.Downadup” | https://web.archive.org/web/20190930212315/https:/www.symantec.com/security-center/writeup/2008-112203-2408-99 | 30 Sep. 2019 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[29] [Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics” | https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[30] [Symantec | Jarrad Shearer | “W32.Downadup” | https://web.archive.org/web/20190930212315/https:/www.symantec.com/security-center/writeup/2008-112203-2408-99 | 30 Sep. 2019 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[31] [Symantec | Jarrad Shearer | “W32.Downadup” | https://web.archive.org/web/20190930212315/https:/www.symantec.com/security-center/writeup/2008-112203-2408-99 | 30 Sep. 2019 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[32] [Usenix | “A Foray into Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/ | 7 April 2017 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[33] [Symantec | Jarrad Shearer | “W32.Downadup” | https://web.archive.org/web/20190930212315/https:/www.symantec.com/security-center/writeup/2008-112203-2408-99 | 30 Sep. 2019 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[34] [Microsoft Security Intelligence | “Win32/Waledac” | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=win32%2Fwaledac | 13 Apr. 2009 | Accessed 02 Jun. 2022 | The source is publicly available information and does not contain classification markings]

[35] [Symantec | Kelly Burton | “The Downadup Codex- A comprehensive guide to the threats mechanics” | https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20The%20Downadup%20Codex%20v2.0.pdf | 8 May 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[36] [Symantec | Jarrad Shearer | “W32.Downadup” | https://web.archive.org/web/20190930212315/https:/www.symantec.com/security-center/writeup/2008-112203-2408-99 | 30 Sep. 2019 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[37] [Usenix | “A Foray into Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/ | 7 April 2017 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[38] [SRI International | Philip Porras, Hassen Saidi, and Vinod Yegneswaran | “An Analysis of Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/index2.html | 4 February 2009 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[39] [SRI International | Philip Porras, Hassen Saidi, and Vinod Yegneswaran | “An Analysis of Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/index2.html | 4 February 2009 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[40] [SRI International | Philip Porras, Hassen Saidi, and Vinod Yegneswaran | “An Analysis of Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/index2.html | 4 February 2009 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[41] [Microsoft | “Win32/Conficker worm” | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=win32%2fconficker | 7 January 2009 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[42] [Usenix | “A Foray into Conficker’s Logic and Rendezvous Points” | https://www.usenix.org/legacy/event/leet09/tech/full_papers/porras/porras_html/ | 7 April 2017 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[43] [FireEye | “FireEye Event Description: Bot.Conficker” | https://mil.fireeye.com/edp.php?sname=Bot.Conficker | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[44] [Microsoft Security Intelligence | “Win32/Waledac” | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=win32%2Fwaledac | 13 Apr. 2009 | Accessed 02 Jun. 2022 | The source is publicly available information and does not contain classification markings]

[45] [Microsoft Security Intelligence | “Rogue:Win32/FakeSpypro” | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Rogue:Win32/FakeSpypro | 17 Aug. 2010 | Accessed 02 Jun. 2022 | The source is publicly available information and does not contain classification markings]

[46] [Microsoft Security Intelligence | “Rogue:Win32/FakeSpypro” | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Rogue:Win32/FakeSpypro | 17 Aug. 2010 | Accessed 02 Jun. 2022 | The source is publicly available information and does not contain classification markings]

[47] [Fauske & Associates | “Cost Benefit Analysis of Nuclear Power Plants” | https://www.fauske.com/blog/cost-benefit-analysis-of-nuclear-power-plants | 11 May 2017 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]

[48] [ZDNet | “Conficker estimated economic cost? $9.1 billion” | https://www.zdnet.com/article/confickers-estimated-economic-cost-9-1-billion/ | 23 April 2009 | Accessed 04 Jun. 2022 | The source is publicly available information and does not contain classification markings]

[49] [KrebsonSecurity | “$72M Scareware Ring Used Conficker Worm” | https://krebsonsecurity.com/2011/06/72m-scareware-ring-used-conficker-worm/ | 23 Jun. 2011 | Accessed 04 Jun. 2022 | The source is publicly available information and does not contain classification markings]

[50] [Softpedia | Catalin Cimpanu | “Malware Shuts Down German Nuclear Power Plant on Chernobyl’s 30th Anniversary” | https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml | 26 April 2016 | Accessed 23 May 2022 | The source is publicly available information and does not contain classification markings]