CASE STUDY: EKANS RANSOMWARE ATTACK ON HONDA

Cybersecurity for the Operational Technology Environment (CyOTE)

31 MARCH 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-67338

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

CASE STUDY: EKANS RANSOMEWARE ATTACK ON HONDA

1. EXECUTIVE SUMMARY

The EKANS Ransomware Attack on Honda case study leverages publicly available information about the attack to catalogue anomalous observables for each technique employed by the adversaries. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology (CyOTE) program.

EKANS ransomware was created and used in an intrusion campaign against at least five critical infrastructure asset owners, including Honda Motor Co. (Honda), operating in Europe, Asia, and South America from December 2019 through July 2020. EKANS is the first known ransomware designed to impact systems that run Operational Technology vendor products, and the victim asset owners suffered a loss of production and revenue due to these attacks. While public statements issued by victims did not describe the length of downtime nor any details of response operations, the EKANS codebase displays common ransomware behavior such as stopping system services, encrypting data, and displaying a ransom note. The adversaries were also very deliberate in choosing their victims: EKANS is tailored to only target specific companies by their internal network domain name.[1]

Using the MITRE ATT&CK® for Industrial Control Systems framework, researchers and analysts identified eight techniques utilized during the EKANS attack on Honda, aligning to six tactics, with a total of 40 observables. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the four precursor techniques believed to have been employed in the attack on Honda had been perceived and investigated prior to the triggering event, earlier comprehension of malicious activity would likely have taken place. Case study analysis identified 20 observables associated with these precursor techniques, the most significant of which were those associated with the abuse of remote service and valid accounts.

Due to EKANS' small signature and evasive characteristics, the victim can do very little to defend their systems if the adversaries are successful in implanting the malware; therefore, precursor comprehension is of paramount importance. To date, no victim organization has provided public information about triggering events, adversary tactics and techniques, or associated timelines. However, initial access, persistence on the targeted systems, and loading of the EKANS ransomware clearly occurred before execution of the attack.

The information gathered in this case study contributes to a library of observables tied to a repository of artifacts, data sources, technique detection capabilities, and procedural recipes 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 asset owners and operators (AOOs) 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), CyOTE is a partnership with energy sector owners and operators whose goal is to tie the impacts of a cyber-attack to anomalies in the OT environment to determine whether the anomalies have a malicious cyber cause.

2.1. APPLYING THE CYOTE METHODOLOGY

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

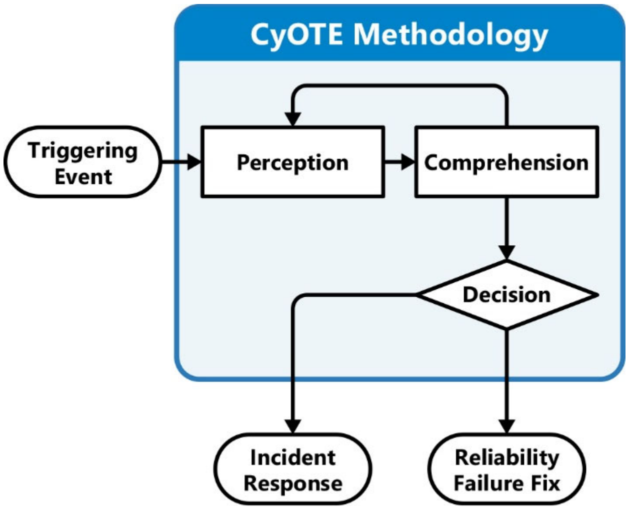


Figure 1. CyOTE Methodology

Case studies such as this one support continued learning through analysis of historical incidents that have impacted OT. This case study 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 AOOs 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 AOO. The point on this timeline when each technique appears is critical to the AOO'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 AOOs to detect those observables. If a technique includes effects which AOOs 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 AOOs with a library of observables reported in each historical case. The library can be used in conjunction with a repository of artifacts, data sources, technique detection capabilities, and procedural recipes to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

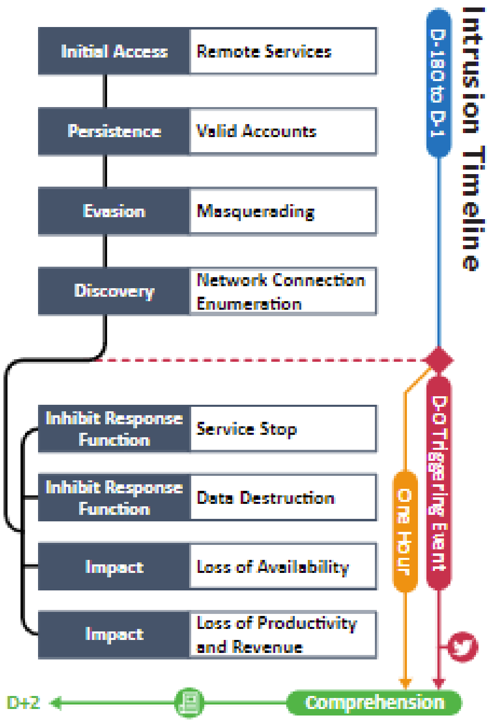


Figure 2. Honda Cyber-Attack Timeline

EKANS ransomware emerged in mid-December 2019. Over the course of the campaign through June 2020, multiple unknown parties uploaded EKANS malware samples to VirusTotal. Numerous security researchers conducted forensic analysis of EKANS and published technical characteristics and analytical results.[2,3] Based on analysis of this information, Adversaries targeting Honda likely initiated access between January 2020 and 7 June 2020 (D-180 to D-1).

On the morning of 8 June 2020 (D-0), Honda announced technical difficulties with their manufacturing operations. Information security experts later determined one of the company's servers had very likely been infected with EKANS ransomware, and that it was specifically targeting OT system processes. This was the first known instance of ransomware designed to impact systems that run OT vendor products, and EKANS inflicted loss of availability, production, and revenue on Honda and the other victims during this attack campaign.[4]

The adversaries employed four precursor techniques through the initial phases of the intrusion: Remote Services, Valid Accounts, Network Connection Enumeration, and Masquerading. The adversaries likely achieved initial access at some point between six months and the day prior to attack execution (D-180 to D-1) and the triggering event (D-0).[5]

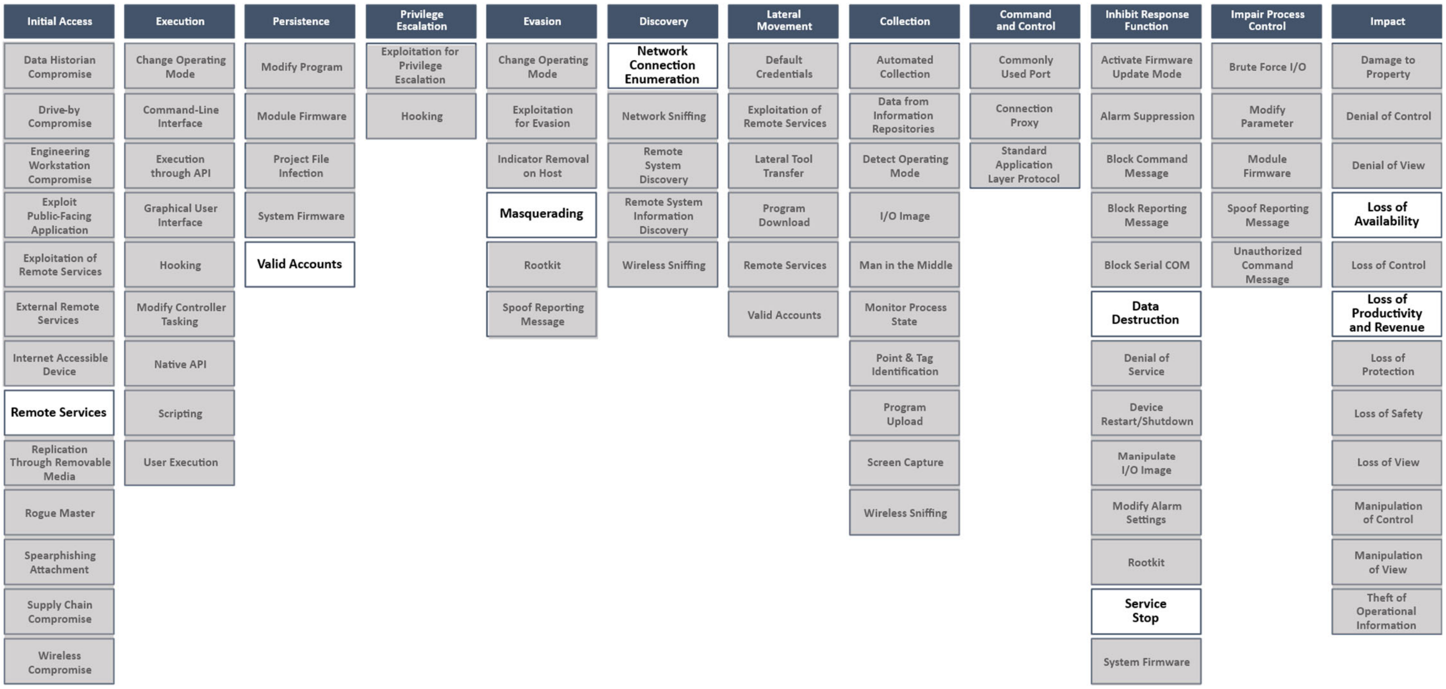
The adversaries likely achieved persistence using the Valid Accounts technique, conducted discovery using the Network Connection Enumeration technique, and masqueraded using an "update.exe" file for the Masquerading technique.

Finally, the adversary initiated a service stop, which killed systems that included data historians and Human Machine Interface (HMI) OT products (D-0), resulting in a loss of availability for affected systems.

Honda's first announced the attack in a message on social media at 11:47 AM on 8 June 2020 (D+1). The first public reporting on the incident was two days later, on 10 June 2020 (D+2), and is assessed to signify comprehension of the intrusion.

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

Table 1. Techniques Used in the Honda Cyber-Attack



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

Table 2. Case Study Quantitative Summary

Case Study Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	8
Technique Observables	40
Precursor Techniques	4
Precursor Technique Observables	20
Highly Perceivable Precursor Technique Observable	11

3. OBSERVABLE AND TECHNIQUE ANALYSIS

The following analysis may assist AOOs and identify malicious cyber activity earlier and more effectively. There are no first-hand accounts from Honda or other EKANS victims describing incident response efforts and characteristics of unauthorized network access techniques or lateral movement techniques used by the adversaries. As such, the following techniques and observables were compiled from publicly available sources and correlated with subject matter expert analysis.

3.1. REMOTE SERVICES TECHNIQUE (T0886) FOR INITIAL ACCESS

Adversaries may leverage remote services to move between assets and network segments. In the case of the cyber-attack on Honda, the adversary very likely loaded EKANS ransomware to victim systems after establishing initial access via a Microsoft Remote Desktop Protocol (RDP) network connection in the enterprise or operations environment. Affected companies had RDP connections exposed to the public Internet and we assess that the adversaries likely used a file sharing service to deliver the EKANS industrial ransomware.

The Remote Services Technique (T0886) is responsible for six observables that likely occurred in the IT and OT environments. These observables would have been visible to the IT staff, IT cybersecurity, OT staff, and OT cybersecurity. If the observers identified and investigated observables earlier in the attack this could have reduced comprehension time. This technique is important for investigation because it presents perceivable effects, such as generation of system log entries and suspicious network traffic to the victim's RDP service. This technique occurs early in the timeline and responding to this technique will effectively halt all future events.

Of the six observables associated with this technique, four are assessed to be highly perceivable (RDP Authentication Log, RDP Activity Timestamp, System Log Entries, Usage of File Sharing Services).

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 Remote Services technique
Technique Observers[a]	IT Staff, IT Cybersecurity, OT Staff, and 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. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

Two of the execution requirements for EKANS are the use of administrator credentials and distribution via the domain controller. The adversaries likely utilized authentic credentials of administrators and accessed domain controllers in both the IT and OT environments.

The Valid Accounts Technique (T0859) is responsible for four observables in the IT and OT environments. These observables likely would have been visible to the IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Support Staff. If this technique had been identified and investigated earlier in the attack, comprehension time likely would have been reduced. This technique is important for investigation because it presents perceivable effects, such generation of system log entries and anomalous network traffic to the victim's domain controller using RDP services. This technique occurs earlier in the timeline, and responding to it could effectively halt all future events.

Of the four observables associated with this technique, two are assessed to be highly perceivable (Usage of Administrative Account on Domain Controller, Domain Controller Activity Timestamp).

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	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Support Staff

3.3. MASQUERADING TECHNIQUE (T0849) FOR EVASION

EKANS ransomware is loaded on the victim systems as a file named ‘update.exe’, a very common name.[6] EKANS is believed to have impacted Honda and other victim systems in both the IT and OT environments.

This technique has some inherent challenges related to detection, as it will evade typical antivirus scans, as well as some Endpoint Detection and Response (EDR) capabilities. However, the use of Tripwire, reverse engineering techniques, or system hashing can increase the perceptibility of the Masquerading technique.

EKANS is written in the Go programming language and leverages features of Go-derived executable binaries to hinder forensic analysis and avoid detection by antivirus monitoring. Go binaries are noticeably larger in size than binaries derived from other programing languages. To combat bulky file sizes, Go allows a programmer to strip binaries during compilation. Most of the information removed is typically used by debuggers. Analysis of EKANS files indicates they are stripped and offer no clues for the malware analyst.

With stripped Go binaries, Interactive Disassembler (IDA) is unable to recognize normal library files. This is an example of an adversary masquerading to disguise a malicious application or executable as another file, to avoid operator and engineer suspicion.

The Masquerading Technique (T0849) is responsible for six observables in the IT and OT environments. These observables likely would have been visible to the IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity, Support Staff, and if identified and investigated earlier in the attack would have reduced comprehension time. This technique is important for investigation because it presents perceivable effects, such as loading of anomalous executables with stripped debug information. This technique also occurs earlier in the timeline, and responding to this technique could effectively halt all future events. This technique modifies the victim operating system files, resulting in the host being placed into a modified state. System backups taken after this technique is executed will impact data recovery and disaster recovery efforts.

Of the six observables associated with this technique, two are assessed to be highly perceivable (Loading of File Named ‘update.exe’, Files with Stripped Binaries).

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	IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity, Support Staff

3.4. NETWORK CONNECTION ENUMERATION TECHNIQUE (T0840) FOR DISCOVERY

Domain Name System (DNS) queries are most likely to be the network discovery technique used by the adversary to deploy the EKANS ransomware in the victim's IT and OT environment. EKANS is designed to discover the domain controller and ensure the targeted victim's internal domain (example: *@honda.org) is present.

The Network Connection Enumeration technique (T0840) is responsible for four observables in the IT and OT environments. These observables likely would have been visible to the IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity, Support Staff, and if identified and investigated earlier in the attack would have reduced comprehension time. This technique is important for investigation because it presents perceivable effects, such as internal hosts performing unusual DNS queries and suspicious network traffic. This technique also occurs right before the execution of the ransomware in the timeline. If the victim does not perceive this technique and respond to it, EKANS will execute.

Of the four observables associated with this technique, three are assessed to be highly perceivable (Invalid Responses in Network Lookup Responses in Network Traffic, Suspicious Network Statistics, Internal Host Performing Domain Query that Normally Doesn't).

Please see Appendix A for the list of observables.

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

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

EKANS has a static list of services it interrupts or “kills.” This kill list includes numerous antivirus products, data historians, HMI applications, and other security services, including EventLog, which otherwise would interfere with encryption of the victim system's data. This technique would also result in the loss of remote management capabilities.

The Service Stop Technique (T0881) is responsible for seven observables in the IT and OT environments. These observables likely would have been visible to the IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Support Staff. If the observers identified and investigated the observables earlier in the attack, then comprehension time could have been reduced. This technique is important for investigation because it presents perceivable effects, such as generation of system log entries, interruption of services, and increased system resource utilization rates associated with file encryption. This technique does modify the victim operating system files and will result in a loss of access to encrypted files, as well as loss of access to the halted victim services.

This technique occurs later in the timeline and there are limited options for effective impact prevention. This technique is extremely critical for perception as it is the last perceivable technique before data destruction and loss of availability occurs.

Of the seven observables associated with this technique, all are assessed to be highly perceivable (Interruption of HMI Application Use, Specific Windows Services Killed, Missing or Failed System Log Entries, Antivirus Products Killed, Business Process Interruptions, Interruption of Various Application Use, Interruption of Data Historian Use).

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 using the Service Stop technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, and Support Staff

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

EKANS ransomware blocks communications to render applications unable to communicate in both the IT and OT environments. This mechanism, which uses legitimate Windows firewalls to block network communication during encryption, is a unique phenomenon of this ransomware. As such, this feature continued to be included in the EKANS variant released in June 2020 and later.

EKANS first encrypts all files without changing the file extensions. Once all files are encrypted, it changes all file extensions at the same time. Since the file extension is not changed while the ransomware is being encrypted, the behavior mirrors the normal renaming process, and it is difficult for the user to notice the file is being encrypted. EKANS encrypts certain files to be ransomed thus preventing access to mission critical data and impacting physical processes. EKANS encrypts files and removes Volume Shadow Copy backups on the victim. EKANS ransomware likely affects systems in both the IT and OT environments.

EKANS executes when the host system is a domain controller. EKANS does not present a ransom on the targeted domain controller. If EKANS determines the infected host is a domain controller, it distributes the ransom message to the Windows desktops of users in the domain under the root directory of C drive.[7]

A total of eight observables are associated with the use of the Data Destruction technique (T0809). Five of these observables are assessed to be highly perceivable (Legitimate Windows Firewalls Block Communications with Applications, Encryption of Critical System Files, Encryption and Removal of Volume Shadow Copy, Sends Ransom Note to Domain Controller, Creates Ransom Letter on Windows Desktops of Public Users Under the Root Directory of C: Drive).

Please see Appendix A for the list of observables.

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

3.7. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

EKANS interrupts running processes for control systems applications then encrypts data required for effective use, resulting in Loss of Availability. Multiple legitimate processes are forcibly terminated, which may interfere with decryption and recovery activities. EKANS ransomware was designed to create an impact in both the IT and OT environments.

A total of four observables were identified with the use of the Loss of Availability Technique (T0826). All four of these observables are assessed to be highly perceivable (Processes Halted; Resulting in Inability to Access Processes and Services; Encryption of Files; Resulting in Inability to Access Files; Loss of HMI Application Use; Loss of Data Historian Use).

Please see Appendix A for the list of observables.

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

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

EKANS causes loss of productivity and revenue through disruption and possible damage to the availability and integrity of control system operations, devices, and related processes.

A total of one observable was identified with the use of the Loss Productivity and Revenue (T0828). This one observable is assessed to be highly perceivable (Inability to Execute Business Processes).

Please see Appendix A for the list of observables.

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

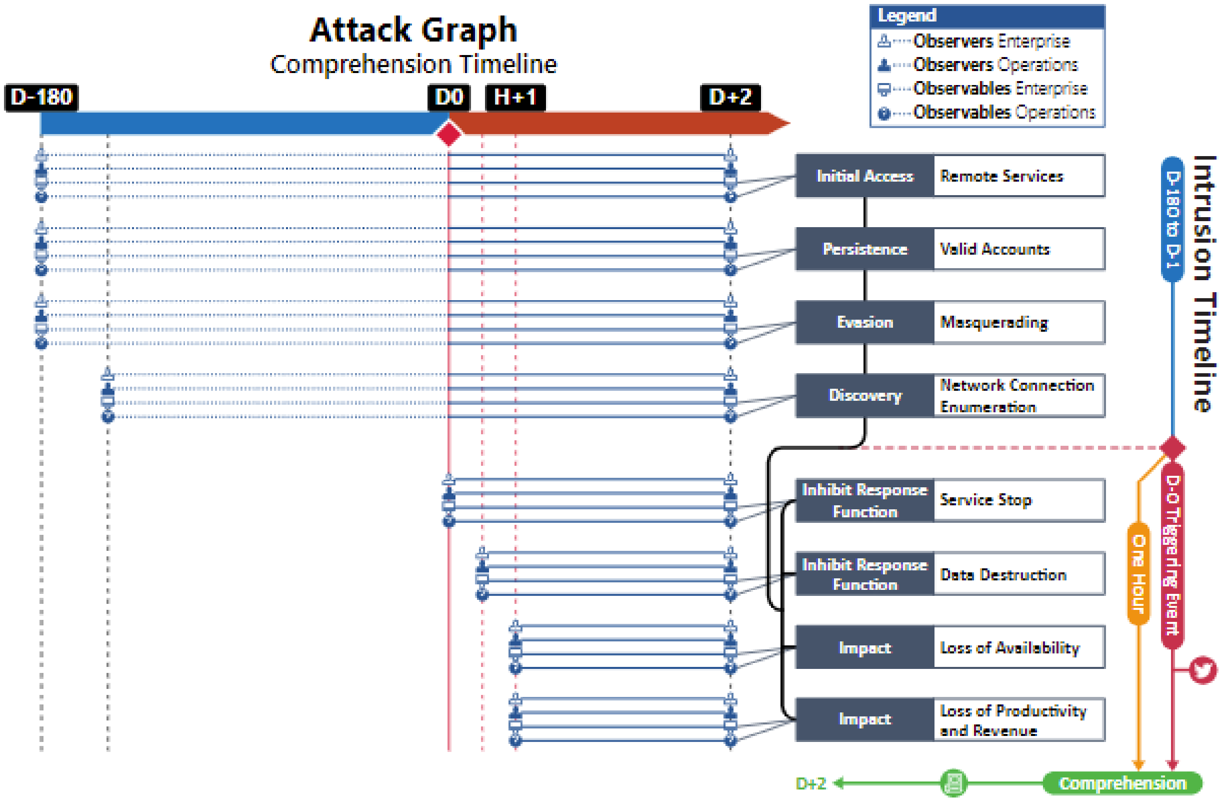


Figure 3. Honda Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

The observables found in this appendix are specific to those assessed to have been used in the EKANS ransomware attack on Honda.

Observables Associated with Remote Services Technique (T0886)	
Observable 1	RDP Authentication Log
Observable 2	RDP Connections to Internal Network
Observable 3	RDP Activity Timestamp
Observable 4	Internet-Facing RDP Connections
Observable 5	System Log Entries
Observable 6	Usage of File Sharing Services

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Usage of Remote Desktop Protocol (RDP) to Domain Controller
Observable 2	Usage of Administrative Account on Domain Controller
Observable 3	Admin Authentication Log on Domain Controller
Observable 4	Domain Controller Activity Timestamp

Observables Associated with Masquerading Technique (T0849)	
Observable 1	Loading Of File Named “update.exe”
Observable 2	Malware Developed Using Go Programming Language
Observable 3	Large Binaries
Observable 4	Bulky Files
Observable 5	Files with Stripped Binaries
Observable 6	Failure of Antivirus to Detect Suspicious Executable

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 1	Application of DNS Lookup of Internal Victim Domain Name
Observable 2	Invalid Responses in Network Lookup Responses in Network Traffic
Observable 3	Suspicious Network Statistics
Observable 4	Internal Host Performing Domain Query That Normally Does Not

Observables Associated with Service Stop Technique (T0881)	
Observable 1	Interruption of HMI Application Use

Observables Associated with Service Stop Technique (T0881)	
Observable 2	Specific Windows Services Killed
Observable 3	Missing or Failed System Log Entries
Observable 4	Antivirus Products Killed
Observable 5	Business Process Interruptions
Observable 6	Interruption of Various Application Use
Observable 7	Interruption of Data Historian Use

Observables Associated with Data Destruction Technique (T0809)	
Observable 1	Legitimate Windows Firewalls Block Communications with Applications
Observable 2	File Encryption
Observable 3	File Extensions Change
Observable 4	Encryption of Critical System Files
Observable 5	Encryption and Removal of Volume Shadow Copy
Observable 6	Checks to See if Host Is a Domain Controller
Observable 7	Sends Ransom Note to Domain Controller
Observable 8	Creates Ransom Letter on Windows Desktops of Public Users Under the Root Directory of C: Drive

Observables Associated with Loss of Availability Technique (T0826)	
Observable 1	Processes Halted, Resulting in Inability to Access Processes and Services
Observable 2	Encryption of Files, Resulting in Inability to Access Files
Observable 3	Loss of HMI Application Use
Observable 4	Loss of Data Historian Use

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1	Inability to Execute Business Processes

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Remote Services Technique (T0886)	
Artifact 1	Remote Client Connection
Artifact 2	Logon Event
Artifact 3	Logoff
Artifact 4	Logoff Event
Artifact 5	Registry Changes
Artifact 6	Registry Connection Change
Artifact 7	Mouse Movement
Artifact 8	Unexpected I/O
Artifact 9	Desktop Prompt Windows Created
Artifact 10	Session Cache
Artifact 11	Application Log
Artifact 12	RDP Traffic 3389
Artifact 13	System Log Event
Artifact 14	Authentication Logs
Artifact 15	GUI Modifications
Artifact 16	Data File Size in Network Content
Artifact 17	File Movement
Artifact 18	MSSQL Traffic 1433 Port
Artifact 19	SSH Traffic 22
Artifact 20	SMB Traffic 139, 445
Artifact 21	VNC Traffic 5800, 5900
Artifact 22	Process Creation
Artifact 23	Remote Session Creation Timestamp
Artifact 24	Network Traffic Content Creation
Artifact 25	Logon

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

Artifacts Associated with Valid Accounts Technique (T0859)	
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 Masquerading Technique (T0849)	
Artifact 1	File Creation with Common Name
Artifact 2	Additional File Directories Created
Artifact 3	Scheduled Job Modification
Artifact 4	Service Creation
Artifact 5	Services Metadata
Artifact 6	Scheduled Job Metadata
Artifact 7	Leetspeak User Metadata
Artifact 8	Common Application with Non-Native Child Processes
Artifact 9	Process Metadata Changes
Artifact 10	Command Line Execution
Artifact 11	File Modification
Artifact 12	Warez Application Use
Artifact 13	Leetspeak File Creation
Artifact 14	Applications Causing Unintended Actions
Artifact 15	Additional Functionality in Applications

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 1	Common Network Traffic
Artifact 2	Polling Network Traffic from Abnormal IP Sender Addresses
Artifact 3	NetBIOS Name Services Port 137
Artifact 4	LDAP Port 389
Artifact 5	Active Directory Calls

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 6	Email Server Calls
Artifact 7	SMTP Port 25 Traffic
Artifact 8	DNS Lookup Queries
Artifact 9	ARP Scans
Artifact 10	TCP Connect Scan
Artifact 11	TCP SYN Scans
Artifact 12	Industrial Network Traffic
Artifact 13	TCP FIN Scans
Artifact 14	TCP Reverse Ident Scan
Artifact 15	TCP XMAS Scan
Artifact 16	TCP ACK Scan
Artifact 17	VNC Port 5900 Calls
Artifact 18	Protocol Content Enumeration
Artifact 19	Protocol Header Enumeration
Artifact 20	Recurring Protocol SYN Traffic
Artifact 21	Sequential Protocol SYN Traffic
Artifact 22	Statistical Anomalies in Network Traffic
Artifact 23	Echo Port 8 Traffic
Artifact 24	Device Failure
Artifact 25	Device Reboots
Artifact 26	Bandwidth Degradation
Artifact 27	Host Recent Connection Logs
Artifact 28	ICMP Port 7 Traffic
Artifact 29	SNMP Port 162 Traffic
Artifact 30	SNMP Port 161 Traffic
Artifact 31	Command Line Dialog Box Open
Artifact 32	Operating System Queries
Artifact 33	DNS Port 53 Zone Transfers

Artifacts Associated with Service Stop Technique (T0881)	
Artifact 1	Process Failure
Artifact 2	Alarm Event
Artifact 3	Sysmon Logs
Artifact 4	Application Error Messages

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

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

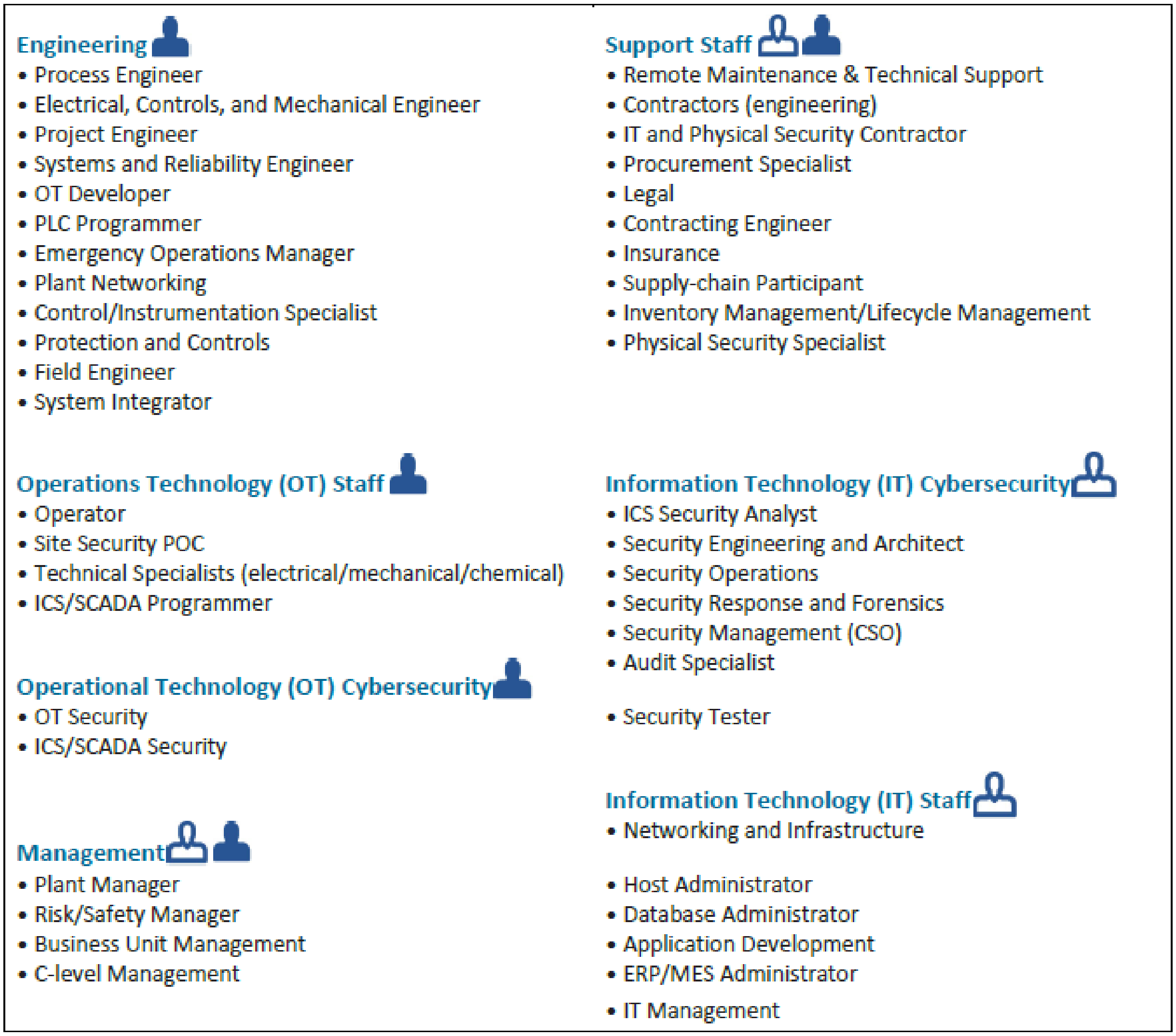
Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 24	Missing Files
Artifact 25	Use of File Transfer Protocols
Artifact 26	FTP Port 20, 21
Artifact 27	TFTP Port 60

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 Present on Disk

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

APPENDIX C: OBSERVERS

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



Engineering

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

Operations Technology (OT) Staff

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

Operational Technology (OT) Cybersecurity

- OT Security
- ICS/SCADA Security

Management

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

Support Staff

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

Information Technology (IT) Cybersecurity

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

- Security Tester

Information Technology (IT) Staff

- Networking and Infrastructure

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

- IT Management

REFERENCES

[1] [Kaspersky ICS CERT | “Targeted Attacks on Industrial Companies Using Snake Ransomware” | https://ics-cert.kaspersky.com/media/Kaspersky_ics_cert_alert_Snake_EN.pdf | 17 June 2020 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[2] [HowToFix.guide | Robert Bailey | “What is Ransom.Ekans infection?” | https://howtofix.guide/ransom-ekans/ | July 2019 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[3] [Malwarebytes Labs | “Honda and Enel Impacted by Cyber Attack Suspected to be Ransomware” | https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/ | 9 June 2020 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[4] [Threat Post | Tara Seals | “Snake Ransomware Delivers Double-Strike on Honda, Energy Co.” | https://threatpost.com/snake-ransomware-honda-energy/156462/ | 10 June 2020 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[5] [International Journal of Critical Infrastructure Protection | Thomas Miller, and others | “Looking Back to Look Forward: Lessons Learnt from Cyber-Attacks on Industrial Control Systems” | https://www.sciencedirect.com/science/article/abs/pii/S1874548221000524?via%3Dihub | December 2021 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[6] [Dragos | “EKANS Ransomware and ICS Operations” | https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/ | 3 February 2020 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]

[7] [GitHub | VK_Intel | “open_mal_analysis_notes” | https://github.com/sysopfb/open_mal_analysis_notes/blob/master/e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.md | 7 January 2020 | Accessed 1 March 2022 | The source is publicly available information and does not contain classification markings]