CyOTE CASE STUDY: TARDIGRADE

FEBRUARY 21, 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

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

INL Idaho National Laboratory

Table of Contents

CYOTE CASE STUDY: TARDIGRADE 1

INTRODUCTION 1
METHODOLOGY 1
BACKGROUND ON THE ATTACK 2
MAP OF ATTACK TTPS 2
APPLICATION OF CYOTE METHODOLOGY AND TECHNIQUES TO THE ATTACK PATH 3
Event Perception *5*
Event Comprehension *5*
Event Decision *6*
CONCLUSION 6
SCENARIO CONSIDERATIONS 6

CYOTE CASE STUDY: TARDIGRADE

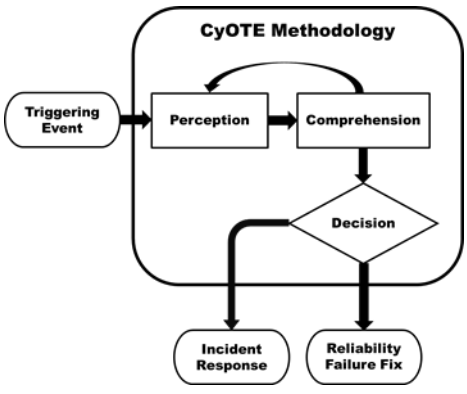
INTRODUCTION

The CyOTE methodology developed capabilities for energy sector asset owners and operators (AOOs) to independently identify adversarial tactics, techniques, and procedures (TTPs) 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. CyOTE seeks to tie effects of a cyber-attack to anomalies—as detected by commercial or in-house solutions—in the OT environment to determine if it has a malicious cyber cause.

Case Studies support continued learning through analysis of incidents and events. Some of the richest and most detailed Case Studies are expected to be produced by AOOs who have employed the CyOTE methodology to perceive and comprehend actual triggering events in their OT environments, with the benefit of complete access to all data and full context. To bootstrap the learning process and complement anticipated AOO-generated Case Studies, the CyOTE team has begun compiling Case Studies of historical OT attacks and OT-related incidents.

This historical Case Study is based on publicly available reports of the incident from media outlets and cybersecurity firms instead of the full context and data that an AOO would have. This Case Study is not, nor is it intended to be, completely comparable in detail or structure, nonetheless it provides examples of how key concepts in the CyOTE methodology look in the real world. Perhaps more importantly, evaluating this historical incident through the CyOTE methodology provides a learning opportunity from the perspective of "how could this have been detected?" instead of "why was this missed?" to grow the body of knowledge on perception, comprehension, and organizational capabilities.

METHODOLOGY



The CyOTE methodology applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. MITRE's ATT&CK® Framework for Industrial Control Systems (ICS)[1] is used as a common lexicon to assess triggering events related to three Use Cases – Alarm Logs, Human-Machine Interface (HMI), and Remote Logins – which together account for 87 percent of the techniques commonly used by adversaries. The CyOTE methodology is also appropriate for OT-related anomalies perceived outside the three Use Cases, such as through the energy system itself.

The Case Study highlights the CyOTE methodology for an AOO to use, starting from the point in time and space an anomalous event or condition meriting investigation – a triggering event – is perceived, and continues to the point where the anomaly is comprehended with sufficient

[1] https://collaborate.mitre.org/attackics/index.php/Main_Page

confidence to make a business risk decision on the appropriate resolution. If sufficient evidence of a malicious nexus is found, then the situation is addressed through existing organizational incident response procedures. Failure to find sufficient evidence of malicious activity defaults to the situation addressed through existing organizational corrective maintenance and work management procedures.

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. Over time, AOOs' triggering events will move towards fainter signals, detected earlier, to interdict incidents before more significant harms are realized in the face of infrastructure changes, new technologies, and determined and sophisticated adversaries.

BACKGROUND ON THE ATTACK

In spring of 2021, the Tardigrade advanced persistent threat (APT) was first reported within the biomanufacturing sector, resulting in the loss of productivity, revenue, information, and availability for organizations operational technology (OT). Bioeconomy Information Sharing and Analysis Center (BIO-ISAC) reports that artifacts associated with Tardigrade were discovered in the OT environment of a bio-manufacturing asset owner in Spring of 2021.[2] The event was initially detected with presence of a ransomware note in the biomanufacturing facility systems. The exact nature of the system experiencing ransomware was not reported. Incident response was conducted across the entire enterprise. In addition to addressing the ransomware issues, during the malware reverse engineering stage, sophisticated techniques and Indicators of Compromise were extracted. In October 2021, further presence of this malware was noted at a second facility.

Tardigrade represents a high risk to the AOO's OT environments due to its ability to operate undetected, allowing the adversary privileged access to move and operate uninhibited within the victim environment. This malware is autonomous, allowing the ability to decide on lateral movement based on internal logic and the ability to selectively identify files for modification. BIO-ISAC and other incident response organizations continue to study the technical characteristics of Tardigrade to develop observable characteristics for more effective network and system monitoring and protection.

MAP OF ATTACK TTPS

By mapping the techniques, tactics, and procedures an attacker used to gain access, CyOTE researchers examined where greater monitoring and detection could provide the visibility needed to connect the dots on attacker activity. Figure 1 demonstrates pivot points used by the adversary and does not indicate linear use of techniques within a given timeline. Tardigrade used stealthy and sophisticated techniques across the range of MITRE ATT&CK for ICS tactics spanning from initial access to impact. The main role of this malware is to download, manipulate files, send main.dll library, if possible, deploy other modules, and remain hidden. AOOs can utilize this

[2] https://www.isac.bio/post/tardigrade

information in their own environments to quickly identify potential attacks and take mitigative actions.

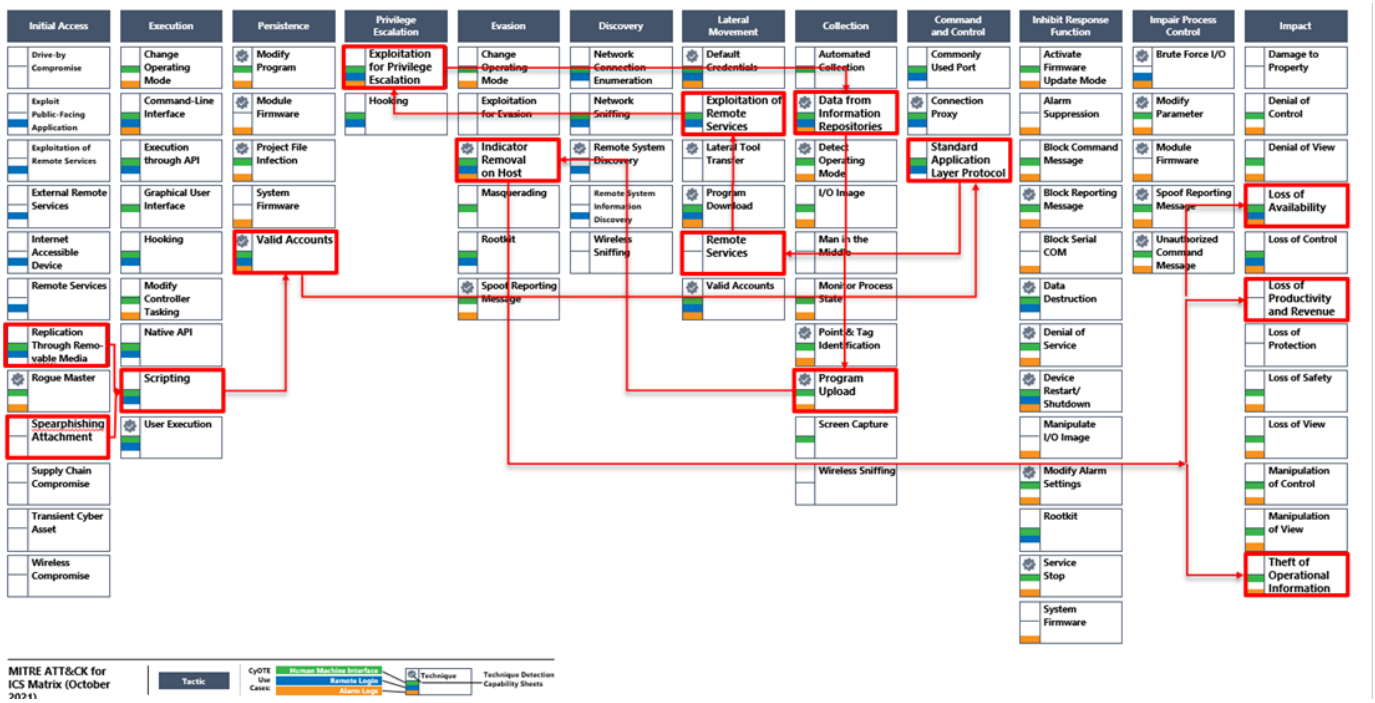


Figure 1. Tardigrade Incident Adversary Techniques Chain

APPLICATION OF CyOTE METHODOLOGY AND TECHNIQUES TO THE ATTACK PATH

Anomalies, possible related adversary techniques, and perception methods for the anomalies are broken down by general adversary campaign steps below.

The chart shown in Figure 2 clearly lays out the multiple techniques on a timeline to demonstrate the series of techniques utilized throughout the entirety of the Tardigrade attack. Once adversaries gained access via the Spearphishing Attachment and initiated the compromise technique, they were able to cause impactful and damaging changes, including theft of information (intellectual property), loss of productivity and revenue, and loss of availability (failure to meet process requirements). The AOOs did not perceive the intrusion activity until impact occurred, approximately four months after initial access.[3]

[3] https://www.isac.bio/post/tardigrade

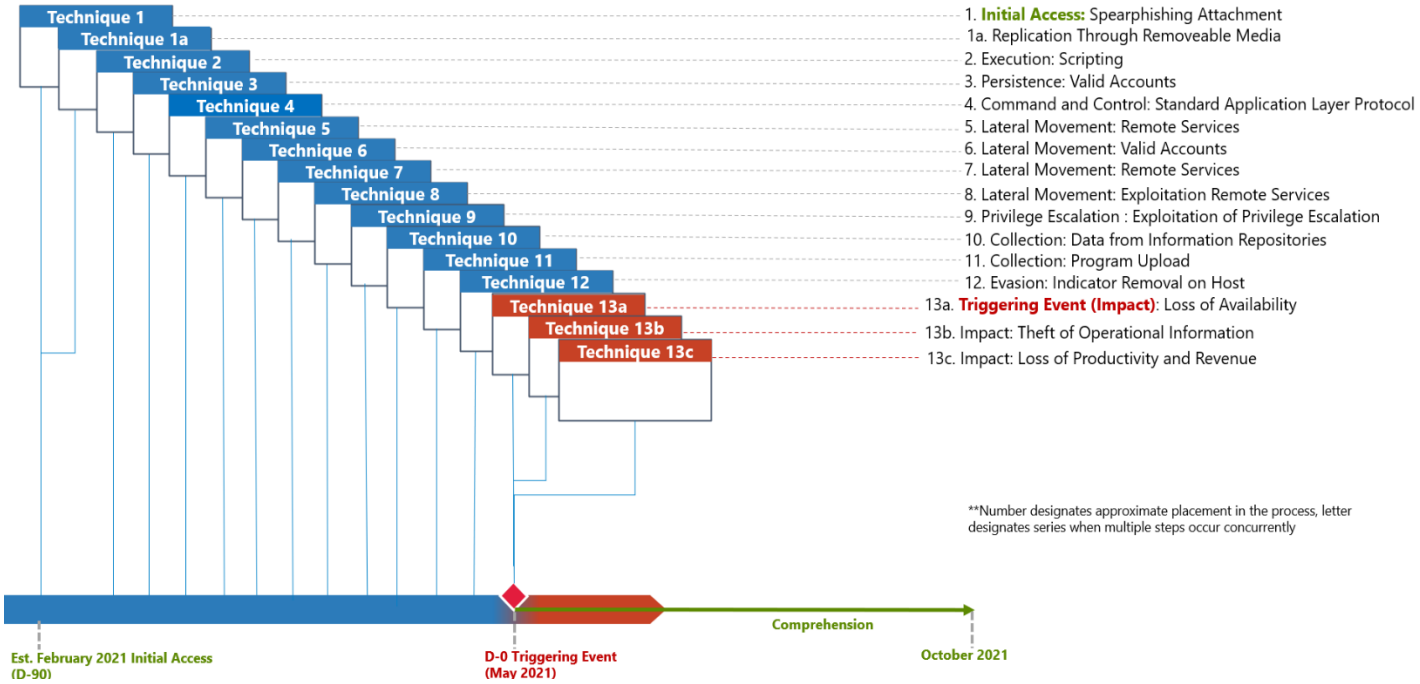


Figure 2. Tardigrade Technique Timeline

By employing the CyOTE methodology, an AOO could begin the comprehension process earlier to reach a decision point with decreased impacts. Because perception requires the recognition of normal vs. anomalous activity, identifying this attack prior to impact requires purposeful monitoring placement early in the attack chain. Several techniques may have been comprehended earlier, had relevant data sources been identified:

- T859 Valid Accounts - Adversaries may steal the credentials of a specific user or service account using credential access techniques.[4]
- T811 Data from Information Repositories - Adversaries may target and collect data from information repositories.[5]
- T0845 Program Upload - Adversaries may attempt to upload a program from a PLC to gather information about an industrial process.[6] [7]
- T0872 Indicator Removal on Host - Adversaries may attempt to remove indicators of their presence on a system in an effort to cover their tracks. [8] [9]

[4] *CyOTE Technique Detection Capability Sheet available for T859 Valid Accounts*
[5] *CyOTE Recipe available for T811 Data from Information Repositories*
[6] *CyOTE Recipe available for T845 Program Upload*
[7] *CyOTE Technique Detection Capability available for T845 Program Upload*
[8] *CyOTE Recipe available for T872 Indicator Removal on Host*
[9] *CyOTE Technique Detection Capability available for T872 Indicator Removal on Host*

Event Perception

As demonstrated on the timeline, event perception identifies anomalies during the cyberattack, D-90 through D-0, that could have triggered earlier investigation. The following are example anomalies associated with each technique above that could have potentially been perceived prior to impact:

T859 Valid Accounts –

- Unusual time stamps on use of application
- Changing passwords and account creation
- Users account usage on server and client hosts
- Unusually high number of failed Host Logon attempts
- Multiple instances of account being opened and used

T811 Data from Information Repositories –

- Changes in data location, type, and file
- Access, read, write, modify and copy files
- Application log associated with user
- Network traffic with data exfiltration
- Modification or movement of .dll objects

T0845 Program Upload –

- .dll objects
- Changing of log content and network traffic content
- Changing of folders for lateral movement via network share
- Program upload to workstations/servers/interface devices

T0872 Indicator Removal on Host –

- Removal or change of host logs, connection logs
- Deletion of .dll objects
- File and registry deletion
- Process creation
- Registry key modification

Event Comprehension

Though each anomaly may be perceived and comprehended by different observers, typically admins, IT personnel, cyber defenders, forensic analysts, network administrators, and operators are roles needed to comprehend the techniques used in the Tardigrade attack. To comprehend if observed anomalies correlate with use of a known adversary technique, observers must build context. The following are examples of questions the different roles may have used to build context around potential anomalies for each of the techniques identified above:

- T859 Valid Accounts – Admins, IT personnel, and cyber defenders should evaluate if an account is inactive due to leave, if there is an unusual number of login attempts, if a login is coming from an unexpected location, or if the login is occurring at an unexpected time.

- T811 Data from Information Repositories – Operators, IT personnel, and admins should determine what information is moving, who authorized the move of information, why the information is being moved, and if it is part of a planned update.
- T0845 Program Upload – Cyber defenders, IT personnel, admins, and network administrators should ask what the program being uploaded is, if the program is authorized, and did the upload originate externally.
- T0872 Indicator Removal on Host – IT personnel, cyber defenders, admins, and forensic analysts should determine if the logging being turned off was part of a planned outage and who could authorize the logging changes.

Additional observables could have been monitored to identify anomalous behavior leading to the cyber-attack. The modification of specific files, exporting of functions from dynamic link libraries, flushing of registries and loss of intellectual property, product and revenue are all anomalies related to the triggering event.

Event Decision

By acting on perceived anomalies and building comprehension, an AOO can reach a decision point to either initiate cyber event incident response or reliability failure fix procedures. Operators observing Spearphishing attachments or identifying dynamic link library file replacement signaled suspicious behavior. By reporting anomalies through the correct channels, an AOO could quickly identify triggering events, build comprehension, and make a better risk-informed decision to respond to a security event earlier in the attack chain.

CONCLUSION

The Tardigrade malware demonstrates a sophisticated level of cyber intrusion capabilities impacting an OT environment, with relevance to asset owner operators within critical infrastructure sectors, including the Energy sector. The CyOTE methodology can be applied even in non-energy subsector systems to result in deeper comprehension of the OT environment and enable identification and mitigation of cybersecurity incidents. Using the CyOTE methodology, an AOO can filter signals from noise to identify interconnected anomalies, triggering further investigation, and escalated response procedures. AOOs can use commercial tools and/or CyOTE capabilities to increase visibility and comprehension. Deeper comprehension will allow AOOs to successfully identify and comprehend indicators of attack earlier in the campaign in order to respond to and resolve incidents with ever decreasing impacts. Furthermore, deeper comprehension of the OT environment provides AOOs sufficient confidence to make risk-informed decisions on whether or not to declare a cybersecurity incident and begin response procedures in the OT environment when anomalies occur outside the OT environment.

SCENARIO CONSIDERATIONS

After reviewing this Case Study, AOOs should consider how a similar scenario could unfold in their operating environment, determine the level and location of visibility necessary for them to perceive the triggering event and other anomalies, and identify accessible information sources to build comprehension. The following questions for reflection and discussion can help AOOs prepare to employ the CyOTE Methodology in their organization.

- Could you perceive a similar triggering event in your organization? How would it be perceived, and by whom?
- What anomalies exist that could have been perceived earlier than the triggering event was? How would each be perceived, and by whom?
- Who will you contact from the System Operations, Engineering, and Cybersecurity departments to build comprehension? Would they be willing and able to assist today?
- How much evidence would you need to confidently reject the null hypothesis of a reliability failure, and initiate cybersecurity incident response procedures?
- Who else in your organization needs to be aware of the outcome?

AOOs can refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov