CyOTE CASE STUDY: OLDSMAR WATER TREATMENT FACILITY

SEPTEMBER 23, 2021

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.

Idaho National Laboratory

Table of Contents

CYOTE CASE STUDY: OLDSMAR WATER TREATMENT FACILITY 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
Valid Accounts 3
External Remote Services 4
Graphical User Interface 4
Modify Parameter 4
CONCLUSION 5
SCENARIO CONSIDERATIONS FOR AOOS USING CYOTE CASE STUDIES 5

CyOTE CASE STUDY: OLDSMAR WATER TREATMENT FACILITY

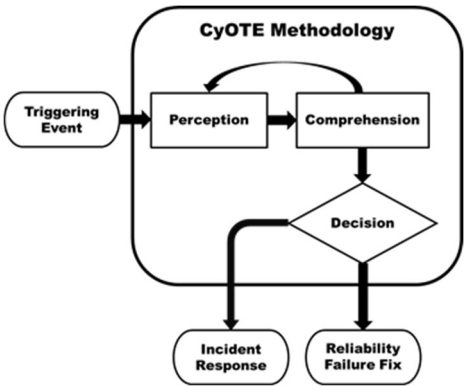
INTRODUCTION

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 delivery 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

On February 5, 2021, a hacker gained control access to change chemical concentrations of the water supply for nearly 15,000 people at the Oldsmar, Florida water treatment facility. The attacker gained access to a TeamViewer account, which allows remote use of the computer controlling chemical content of an underground water reserve.[2]

The attack occurred in between employee maintenance periods and was discovered when an operator noticed unusual mouse movement on the computer screen from a remote user. An employee had noticed similar remote activity earlier in the day, but did not recognize it as anomalous. Availability of open-source information on plant engineering and automation, including the HMI, such as a list of chemicals operators can add to the process allowed threat actors easier access.

The triggering event for this incident was the operator perceiving un-commanded and unusual mouse cursor movement that changed a critical process setting. In this incident, an individual human operator actually perceived abnormal mouse cursor movement twice, but it was not recognized as abnormal and thus a triggering event until the mouse movement resulted in an inappropriate change to sodium hydroxide levels. Reportedly, in that organization it was not uncommon for an authorized remote user to briefly take control of the HMI to check readings without notifying the operator beforehand, so the addition of inappropriate actions elevated the mouse movement from an event to a triggering event. This highlights the fact that individual baselines of what constitutes normal activity will vary from organization to organization.

MAP OF ATTACK TTPS

The Oldsmar incident involved the use of adversary techniques from two of the three CyOTE Use Cases – Remote Login and Human Machine Interface. Four techniques, used in series, were identified as part of this relatively simple incident. These techniques, in chronological sequence as employed by the adversary and not in order of detection by the victim, are shown in Figure 1.

[2]https://www.msn.com/en-us/news/us/lye-poisoning-attack-in-florida-shows-cybersecurity-gaps-in-water-systems/ar-BB1dxMlI?mc_cid=1287406bbd&mc_eid=33e049eacb%E2%80%8B

By mapping the techniques, tactics, and procedures an attacker used to gain access, CyOTE researchers examine where greater monitoring and detection could provide the visibility needed to connect the dots on attacker activity. AOOs can utilize this information in their own environments to quickly identify known attacks and take mitigative actions.

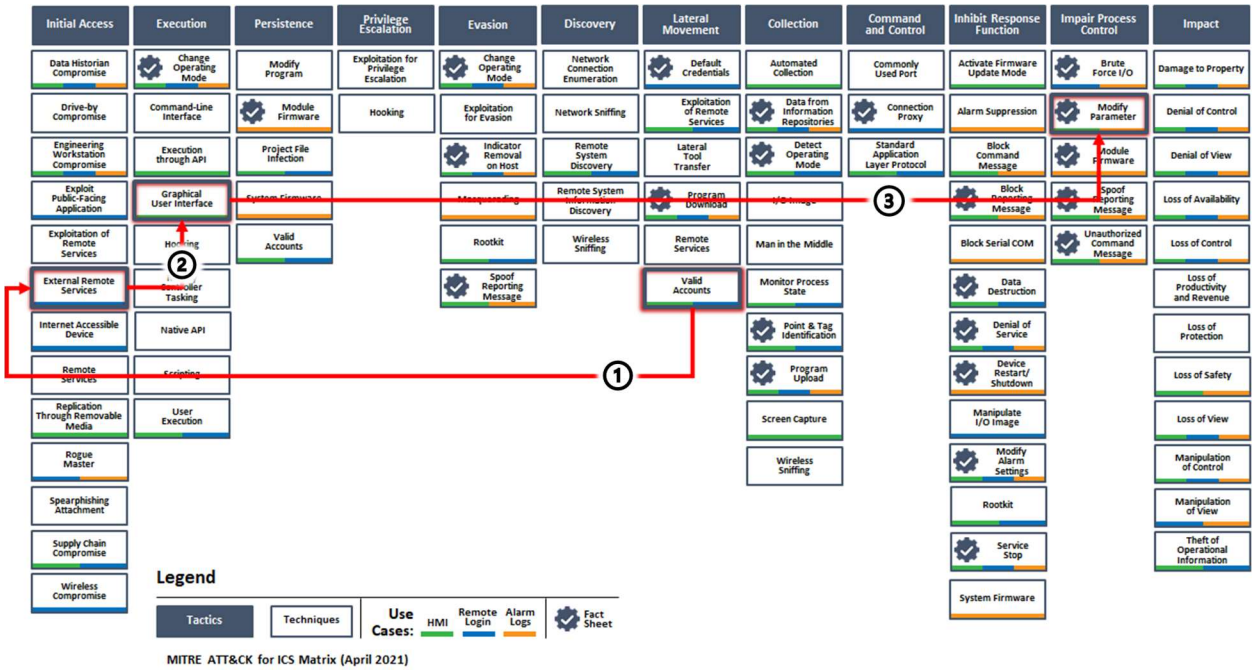


Figure 1. Oldsmar Incident Adversary Techniques Chain

APPLICATION OF CyOTE METHODOLOGY AND TECHNIQUES TO THE ATTACK PATH

Anomalies, possible related adversary techniques, and example perception methods for the anomalies are detailed below.

Valid Accounts

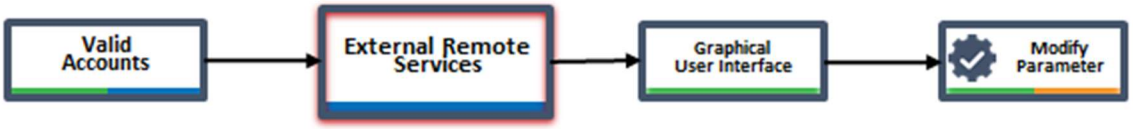
Anomaly: Oldsmar passwords were discovered in a password data leak that occurred days prior to the attack.[3] A security audit could also have revealed password sharing between employees and services.

Technique: An attacker gained access to the HMI system using valid user credentials.

Perception Opportunities: Account breach detection services could have alerted the utility to compromised credentials, which could then have been used to alert operators to intrusion attempts if used.

[3] https://cybernews.com/news/oldsmar-florida-water-facility-credentials-contained-in-comb-data-leak/

External Remote Services



Anomaly: With a valid credential, remote access may not appear anomalous on its own. Anomalous behavior may be revealed as an unknown source IP, multiple users from the same source IP, one user from multiple source IPs, or a user with valid access pivoting to use the control network in ways not intended or authorized.

Technique**:** The attacker used the stolen credential to remotely access the system.

Perception Opportunities: Remote service logging & monitoring and VPN Host Scan/Health Check could be observed.

Graphical User Interface

Anomaly: Equipment operation from the HMI that impacts the OT system and that is not initiated by the control room operator or by a known/expected remote access user.

Technique: The attacker used remote access to gain control of the HMI system.

Perception Opportunities: Operator identified an uninitiated change on the HMI by observing mouse movement. However, a more sophisticated attacker may operate the system using keyboard and minimize mouse movement to avoid detection.

Modify Parameter

Anomaly: Operational parameter modified outside of safe limits.

Technique: The hacker raised the levels of lye in the water from 100 to 11,100 parts per million.

Perception Opportunities: The change could be detected by an operator (as in this event), a redundant system, alarms from the HMI or historian indicating an out-of-bounds change, or downstream alarms from the physical environment detecting unsafe chemical levels in the water.

CyOTE Proof of Concept Tool: The CyOTE T836 Modify Parameter Proof of Concept tool could have been used to alert on this attack as it uses the ConfigEngine to monitor directories and files for modifications. ConfigEngine, one of the Structured Threat Observable Tool Set (STOTS) tools, and monitors directories and files for modifications. ConfigEngine uses a custom script to periodically remotely connect to a device, download a user-defined file, and compare it for any changes. If a change is identified, ConfigEngine will generate a Structured Threat Information Expression (STIX™) object and transmit it to the STIX™ monitor.

Decision: Oldsmar's water treatment facility leadership decided that this was a cybersecurity incident and initiated their response procedures. In this case, comprehension and the decision point were reached as soon as the triggering event was perceived due to the obvious malicious nature of this particular triggering event.

CONCLUSION

Even in non-energy subsector systems, the CyOTE methodology can be applied to result in deeper comprehension of an AOO's OT environment, enabling identification and mitigation of cybersecurity incidents. In the Oldsmar Case Study, failure to recognize anomalous activity including visual cues and out-of-bound threshold changes early in the attack delayed response procedures until a malicious operation was already well underway. Without sufficient comprehension, an AOO may fail to filter out signal from noise in order to successfully identify similar anomalies and initiate investigation in their own OT environment. By correlating anomalies with known techniques and stringing together observables, an AOO could identify and comprehend indicators of attack earlier in order to respond and resolve incidents with ever decreasing impacts. Furthermore, deeper comprehension of the OT environment allows AOOs sufficient confidence to make risk-informed decisions on whether to declare a cybersecurity incident and begin response procedures in the OT environment when anomalies occur outside the OT environment.

SCENARIO CONSIDERATIONS FOR AOOs USING CyOTE CASE STUDIES

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 observables 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
DOE Senior Technical Advisor	Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557