CyOTE CASE STUDY: DARKSIDE

FEBRUARY 8, 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: DARKSIDE 1

INTRODUCTION 1
METHODOLOGY 1
BACKGROUND ON THE THREAT ACTOR 2
Threat Actors that have Worked with DarkSide *2*
MAP OF ATTACK TTPS 3
BACKGROUND ON THE ATTACK 3
APPLICATION OF CYOTE METHODOLOGY AND TECHNIQUES 4
CONCLUSION 5
SCENARIO CONSIDERATIONS FOR AOOS USING CYOTE CASE STUDIES 5

CyOTE CASE STUDY: DARKSIDE

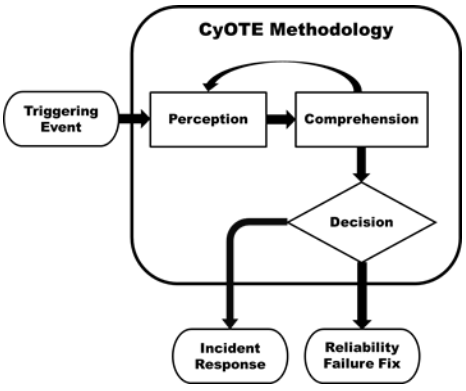
INTRODUCTION

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 the 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 confidence to make a business risk decision on the appropriate resolution. If sufficient evidence

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

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 THREAT ACTOR

DarkSide is a cybercrime group believed to be based in eastern Europe that offers Ransomware as a Service (RaaS), striving to provide full or partial service, depending on the threat actor. DarkSide provides configurable capabilities, builds for Windows and Linux, and an administrative panel to manage builds, blogposts, communications with victims, payment, and automated test decryption. DarkSide has a full process from "initial compromise" to "complete mission." After the initial compromise, the process begins by "establish foothold, escalate privileges," "internal reconnaissance," and "complete mission." In other attacks that utilized DarkSide, adversaries have been seen hopping around in the environment. At the end of the process, the threat actor can deploy the DarkSide ransomware and execute, stealing the data and encrypting it. To ensure the data is not released, the victim must pay to decrypt the data. DarkSide also has the capability to blackmail for distributed denial-of-service (DDoS).[2]

Threat Actors that have Worked with DarkSide

Although threat actors using DarkSide RaaS are generally unattributable, investigating clusters of threat activity involved in deployment of DarkSide sheds light on common attack lifecycles.[3] Uncategorized threat actors deploying DarkSide are referred to using UNC (unclustered) designation, clustered by cyber intrusion activity including observables such as adversary tools and infrastructure.[4]

UNC2628

Intrusions progress relatively quickly, going from initial access to data encryption in two to three days. There is a correlation between early suspicious authentication attempts and the start of interactive intrusion operations for initial access. Initial access is generally gained through corporate VPN structure using legitimate credentials captured during precursor activity. Tools used to interact with the victim environment include Cobalt Strike and BEACON.

UNC2659

[2] https://krebsonsecurity.com/wp-content/uploads/2021/05/darkside20.txt
[3] https://www.mandiant.com/resources/shining-a-light-on-darkside-ransomware-operations
[4] https://www.mandiant.com/resources/how-mandiant-tracks-uncategorized-threat-actors

This threat actor takes more time, but still generally moves through the entire attack lifecycle in under 10 days. Initial entry is gained through a VPN exploit.

UNC2465

These threat actors take the longest, potentially months. After the initial access, they live in the environment, often with month-long gaps with only intermittent activity. After a few months—perhaps due to suspicions of being detected or getting what they can—they deploy the ransomware.[5]

Because DarkSide ransomware is likely distributed by multiple actors, TTPs used across incidents associated with it will vary, as demonstrated in Figure 1.

MAP OF ATTACK TTPS

By mapping techniques, tactics, and procedures used in past attacks attributed to DarkSide, CyOTE researchers examine where greater monitoring and detection could provide visibility needed to detect a similar attacker in the OT environment with ever-decreasing impact. AOOs can utilize this information in their own environments to quickly identify known attacks and take mitigative actions. Figure 1 shows TTPs used across incidents by DarkSide threat actors, highlighted in red.

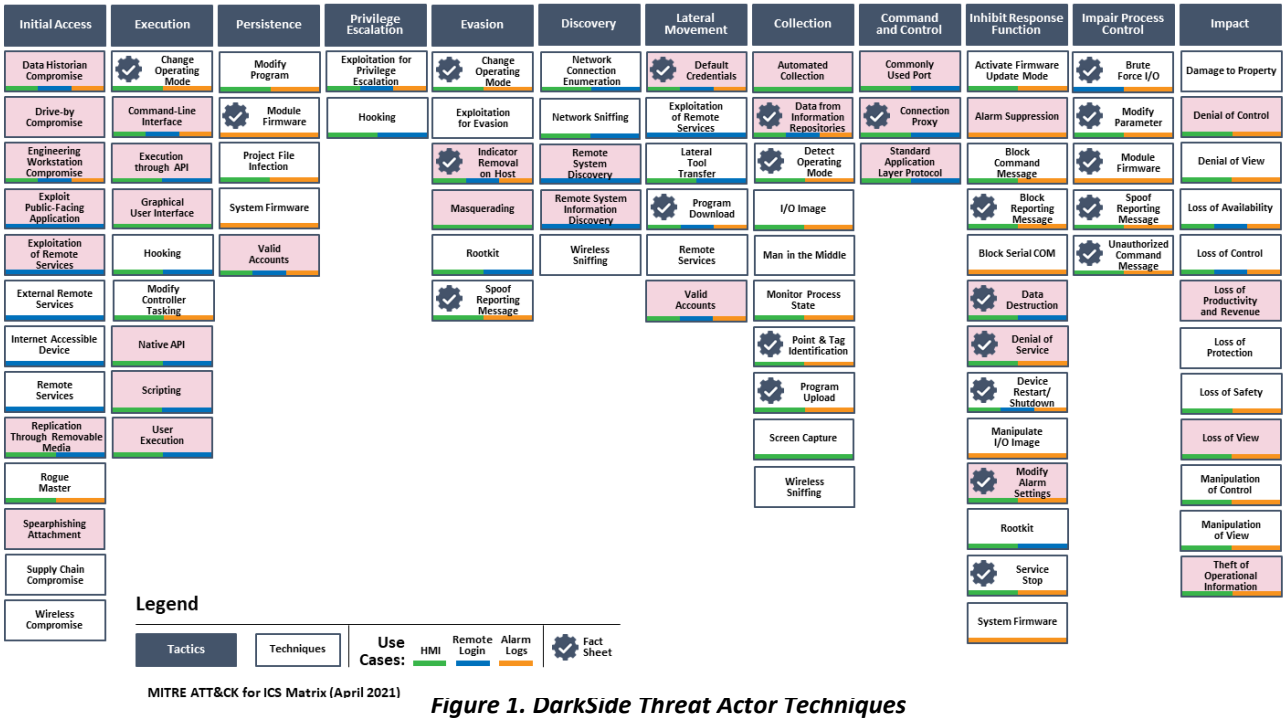


Figure 1. DarkSide Threat Actor Techniques

BACKGROUND ON THE ATTACK

DarkSide most recently gained media traction for their involvement in the 2021 Ransomware attack on the Colonial Pipeline. In the Colonial attack, Darkside may have used all, some, or none of the techniques highlighted in Figure 1. Initial access occurred on April 29 following a data leak which likely contained login credentials used to gain initial entry through an outdated VPN.

[5] https://www.mandiant.com/resources/shining-a-light-on-darkside-ransomware-operations

Although Colonial had two-factor authentication on most of their access points, some were missed.[6]

Forensic analysis identified that once inside, the attacker moved laterally within the network, although very limited information was provided on how. Lateral movement allowed the attacker to gain Active Directory access, which was likely used to acquire valuable assets for data exfiltration and move through the system to deploy the ransomware to connected machines.[7]

An employee in a control room discovered a Ransomware note notifying Colonial that over 140GB of data including accounting and research and development files had been uploaded and would be automatically published upon failure to pay. The employee brought the note to the attention of management. Although the attack occurred in the IT environment, this triggered the decision to shut down the pipeline and conduct further investigation of OT environment.

Although, at the time of this report writing, insufficient information is publicly available to determine specific adversary techniques and CyOTE Use Cases involved in the Colonial incident, DarkSide is known to use techniques from all three CyOTE Use Cases – Alarm Logs, Remote Login, and HMI.[8] The following information demonstrates how an AOO would leverage the CyOTE methodology based on the information publicly available.

APPLICATION OF CYOTE METHODOLOGY AND TECHNIQUES

Perception - Potential Observables:

The following observables could have been perceived as anomalies within the organization prior to receipt of the ransomware note, however, there is a lack of information to determine if all the observables identified represent a deviation from normal. Regardless, some observables would, by their very nature, generate additional analysis to be initiated by the AOO.

- Use of an account which was dormant
- Old VPN usage
- Data Exfil (100GB+)
- Ransomware Note

Comprehension Opportunities:

To comprehend a triggering event, it is important for the AOO to increase their understanding and determine if a triggering event is due to a cyberattack or physical failure. By using the CyOTE methodology, an AOO could begin the process of understanding the observables present based on the relevant context across operations to include OT, IT, business, and cybersecurity domains. These observables include:

- Account Login, Usage
- Anti-Virus Alert
- Data Exfil (100GB+)

[6] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[7] https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

[8] https://www.varonis.com/blog/darkside-ransomware/

- Service stop
- Increased hard drive/Network Share activity
- Document Management System/Canary File

After collecting information, the AOO will need to comprehend what was received and attempt to make sense of perceived information. Additional information such as antivirus alerts could also be investigated.

Decision:

The next step is to make a risk-informed decision based on the results of the investigation. If there is clear indication of a cyber event, the AOO acts, declares a cyber incident, and initiates response action. How an AOO responds is based on their risk appetite and where cybersecurity falls within the prioritization. For many AOOs, response is based on their emergency response plan for how to work through the event and who to contact. This could include:

- Consult Emergency Response Plan
- Shut down Process
- Initiate investigation

In the case of Colonial, based on their risk appetite, the action was to shut down the process and then initiate the investigation based on this being prioritized as a security event to the business response of maintaining the pipeline.

CONCLUSION

While the OT and IT realms are generally considered to be unique and separate environments, this ransomware attack demonstrates how an IT attack can impact the OT environment in a novel way. Although there was uncertainty as to whether the threat actor itself could directly impact the OT environment, productivity and revenue were ultimately impacted as a result of incident response procedures.

While the CyOTE methodology was created to improve security of the operational technology environment, there is value in using the same methods to evaluate any anomaly in the enterprise information technology environment as well. By using the CyOTE methodology, an AOO can gain better visibility and comprehension of anomalies, thereby enabling a shift in threat detection capability to identify attacks 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.

- Is there an anomaly that could have been perceived and triggered investigation earlier? 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