TECHNIQUE T811: DATA FROM INFORMATION REPOSITORIES

CyOTE Use Case(s)[1]	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI, Remote Login	Collection
Data Sources	
Potential Data Sources	Application Logs, Authentication Logs, Data Loss Prevention, NetFlow Logs, Third-party Application Logs
Historical Attacks	Colonial Pipeline; ACAD/Medre.A, Duqu, and Flame malware[2]

TECHNIQUE DETECTION

The Data from Information Repositories technique (Figure 1) may be detected when there are unauthenticated connections to information repositories in a network and indications that sensitive files in these repositories are being accessed.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools[3] and Recipes[4] for asset owners and operators (AOO) to identify indicators of attack for techniques like Data from Information Repositories within their operational technology (OT) networks. Referencing CyOTE Case Studies[5] of known attacks, AOOs in both small and large organizations can utilize CyOTE's Use Case analyses to tie operational anomalies and observables to cyber-attack campaigns resulting in ever-decreasing impacts.

PERCEPTION: OBSERVABLES FROM HISTORICAL ATTACKS

The Data from Information Repositories technique has been used by the Dragonfly 2.0 threat

[1] CyOTE Use Cases (Alarm Logs, Human-Machine Interface [HMI], and Remote Login) were identified by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and validated by Idaho National Laboratory (INL) as situations where OT log data may have a high likelihood of containing attack indicators. More information on Use Cases and how they apply to Technique Detection Capability Sheets can be found in the Technique Prioritization Report: https://inl.gov/wp-content/uploads/2021/12/CyOTE-Technique-Prioritization-Report-2021.pdf

[2] This Technique Detection Capability Sheet focuses on this technique's use in one historical attack. See the MITRE page on T811: Data from Information Repositories for additional historical attacks that have used this technique: https://collaborate.mitre.org/attackics/index.php/Technique/T0811

[3] A Proof of Concept tool is a representative implementation of a set of steps and methods for identifying techniques. A Proof of Concept tool is defined as a script(code) or using capabilities of existing tools (e.g., Splunk, Gravwell), to demonstrate the capability to identify adversarial activity for a selected technique. A Proof of Concept tool is not ready for implementation in an AOO's environment as its major focus is to a specific instance (device, vendor, protocol, scenario) in order to prove a concept.

[4] A Recipe is a set of steps and methods for identifying techniques. Recipes can be used to develop a Proof of Concept or operational tool in an AOO's OT environment.

[5] Visit https://inl.gov/cyote/ for all CyOTE Case Studies.

actor[6] and by the DarkSide threat actor in the Colonial Pipeline incident.[7] In the Colonial Pipeline attack, the following observables were identified:

- Victim data collection via DLL execution
- Execution of 32-bit DLL named "encryptor2.dll"
- Encryptor2.dll calls the Volume Shadow Service (vssvc.exe) to remove all volume shadow copies
- Ransomware gathers victim system information and other identifiable information
- Ransomware checks victim language and halts if language is Russian

Disclaimer: Past occurrences are not guaranteed to occur in future attacks.

COMPREHENSION

In the Colonial Pipeline attack, DarkSide ransomware collected data about the infected environment by loading the libraries instructed by the dynamic-link library (DLL). The ransomware harvests standard information on the system—such as OS, username, hostname, domain, and OS architecture—then encrypts the data and sends it to the Command and Control (C2) server. By understanding the nature and possible origins of this attack, as well as how the adversary used the Data from Information Repositories technique to execute the attack, an AOO can better comprehend how this technique is used with others and enhance their capabilities to detect attack campaigns using this technique and decrease an attack's impacts.

CURRENT CAPABILITY

The CyOTE T811 Recipe describes a process to implement deep packet inspection to parse out individual bytes in messages meant to detect access to sensitive information. It detects types of information being sought, repository details, and looks for login events for databases. It scans for common information technology (IT) protocols such as File Transfer Protocol (FTP), Postgres/SQL, Telnet, Secure Shell (SSH), and operational technology (OT) protocols such as Schweitzer Engineering Laboratories (SEL) and Inter-Control Center Communications Protocol (ICCP). This provides an AOO and the industry insight into the nature of the data access and alerts on sensitive data access. CyOTE Recipes demonstrate how to apply the CyOTE methodology[8] to gain a better understanding of identified anomalies and make better risk-informed decisions.

POTENTIAL ENHANCEMENTS

Additional research is needed to build an operational tool from the T811 Recipe to scan messages commonly seen in the AOO's network, any additional protocols, and be customized to fit a network traffic profile unique to an AOO. The operational tool should have the ability to find the aforementioned commands and network activity in live traffic.

---

[6] MITRE, *Group: Dragonfly 2.0, Berserk Bear, DYMALLOY,* https://collaborate.mitre.org/attackics/index.php/Group/G0006

[7] CyOTE Case Study: DarkSide. https://inl.gov/wp-content/uploads/2021/09/DarkSide-CyOTE-Case-Study.pdf

[8] Methodology for Cybersecurity in Operational Technology Environments, 2021. https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf

ASSET OWNER DEPLOYMENT GUIDANCE

To deploy this capability, the CyOTE T811 Recipe recommends to fully develop and deploy parsers in an asset owner's infrastructure. The logs will then need to be sent to a log analysis tool such as Splunk or Gravwell. Example queries and dashboards will be provided in the plugin documentation specific to the Data from Information Repositories technique.

When complete, the operational tool should be deployed on a host capable of processing the desired amount of traffic. This host will either need access to live traffic or storage for Packet Capture (PCAP) files to be processed.

AOOs can refer to the CyOTE Technique Detection Capabilities report (visit https://inl.gov/cyote/) for more information on the background and approach of CyOTE's technique detection capabilities, and to the other historical Case Studies available at the CyOTE website for information on other historical cyberattacks.

AOOs can also 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

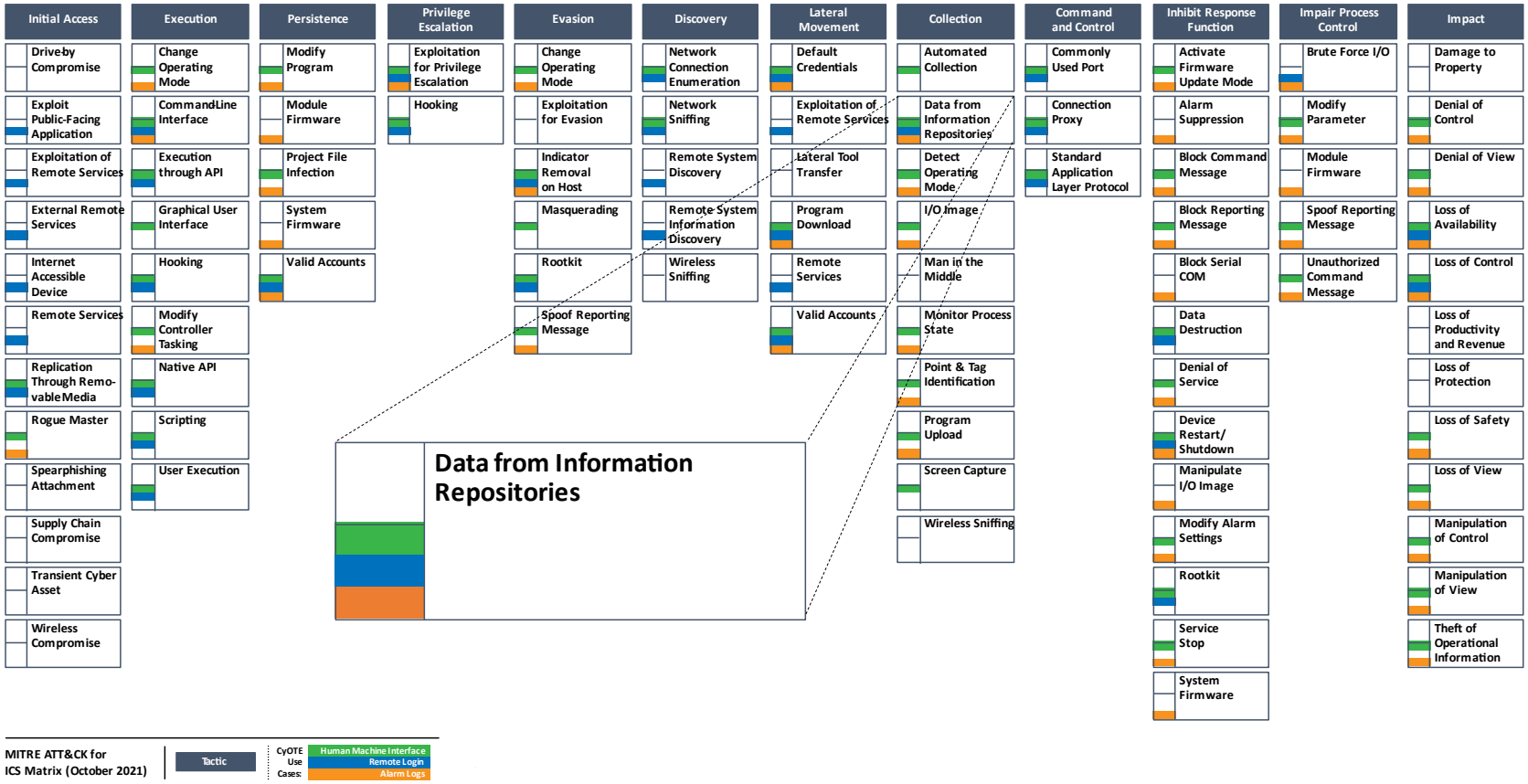

Figure 1: ICS ATT&CK Framework[9] – Data from Information Repositories Technique

[9] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.