TECHNIQUE T859: VALID ACCOUNTS

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI, Remote Login	Persistence, Lateral Movement
Data Sources	
Potential Data Sources	Packet Captures, Process Command-line Parameters, Network Protocol Analysis, OS Logs, Application Logs
Historical Attacks	Oldsmar Water Facility Breach

TECHNIQUE DETECTION

The Valid Accounts technique[1] (Figure 1) may be detected when there are unnecessary or unexpected connections to systems from known user accounts or accounts with default credentials. Connections from one user with multiple IP addresses, or multiple users from the same IP address, can also indicate the malicious use of valid credentials.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools[2] and Recipes[3] for asset owners and operators (AOO) to identify indicators of attack for techniques like Valid Accounts within their operational technology (OT) networks. Referencing CyOTE Case Studies[4] 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 Valid Accounts technique was used in the Oldsmar water facility breach in Florida in 2021.[5] In this attack, the following observables were identified:

- Unfamiliar IP addresses
- Unexpected login sessions
- New accounts being created (seen in authentication logs)

---

[1] MITRE ATT&CK for ICS, T859: Valid Accounts, https://collaborate.mitre.org/attackics/index.php/Technique/T0859

[2] 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.

[3] 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.

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

[5] 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

- Restricted areas of the network being accessed

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

COMPREHENSION

In the Oldsmar incident, the adversary gained access to the human-machine interface (HMI) system using valid user credentials, which had been leaked days prior to the attack.[6] Having breached the system, the adversary modified parameters of the machines to increase the amount of lye in the water. The Oldsmar leadership determined that a cybersecurity incident was occurring and initiated response procedures.[7] By understanding the nature and possible origins of this attack, as well as how the adversary used the Valid Accounts 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 Recipe describes a process to build capabilities to assist perception for identifying anomalies, looking into triggers to provide context, and assisting the decision-making process. A potential capability is suggested which monitors and analyzes host and application logs across various systems to identify anomalies in user activity, such as logging into a new high value system or at an unusual time.

POTENTIAL ENHANCEMENTS

Additional research is needed to tailor this capability to monitor operating and application logs for abnormal or unexpected behavior. Potential synergy could be had combining this detection capability with the Default Credentials technique.

ASSET OWNER DEPLOYMENT GUIDANCE

The CyOTE Recipe may be leveraged to develop an operational tool in a state of continuous monitoring. The tool will need to collect authentication logs from operating systems, applications, and network domains. Analysis of the logs may benefit from machine learning applications. The capability will log when variances are identified and alert when those variances are suspected to be malicious. Alerts can be customized to output to a syslog entry or a STIX 2.1 format.

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.

[6] https://cybernews.com/news/oldsmar-florida-water-facility-credentials-contained-in-comb-data-leak/
[7] CyOTE Case Study: Oldsmar Water Treatment Facility, https://inl.gov/wp-content/uploads/2021/09/Oldsmar-CyOTE-Case-Study.pdf

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

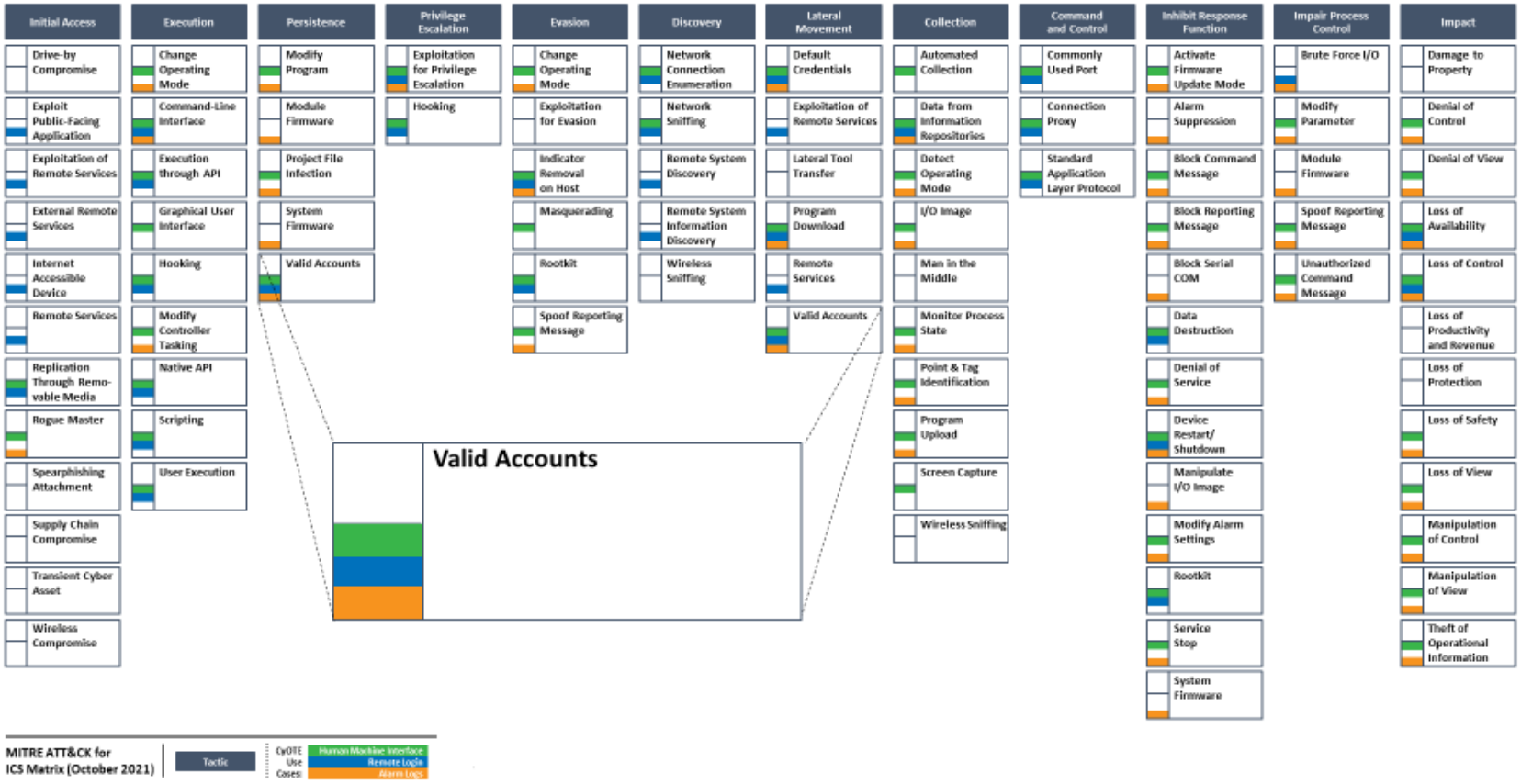

Figure 1: ICS ATT&CK Framework[8] – Valid Accounts Technique

[8] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.