TECHNIQUE T836: MODIFY PARAMETER

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI	Impair Process Control
Data Sources	
Potential Data Sources	Device/Application/System Logs, Network Protocol Analysis, Packet Capture
Historical Attacks	Oldsmar Water Facility Breach

TECHNIQUE DETECTION

The Modify Parameter technique[1] (Figure 1) may be detected when logs indicate changes made to programs instructing devices how to operate.

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 within their operational technology (OT) networks. However, for the Modify Parameter technique, the CyOTE program recommends the use of the ConfigEngine tool to develop a capability for identifying Modify Parameter in an AOO's OT environment. Additionally, by 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 Modify Parameter technique was used in the Oldsmar water facility breach in Florida in 2021.[5] In this incident, the following observables were identified:

- Increased internet traffic
- Device logs or alarms indicating changes to parameters
- Lye levels in water increased from 100 to 11,100 parts per million

[1] MITRE ATT&CK for ICS, T836: Modify Parameter, https://collaborate.mitre.org/attackics/index.php/Technique/T0836

[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.nbcnews.com/tech/security/lye-poisoning-attack-florida-shows-cybersecurity-gaps-water-systems-n1257173

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

COMPREHENSION

In the Oldsmar incident, the adversary first 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 Modify Parameter 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

As previously noted, the CyOTE program recommends the use of ConfigEngine to develop a capability for identifying Modify Parameter in an AOO's OT environment. ConfigEngine, one of the Structured Threat Observable Tool Set (STOTS)[8] tools, monitors directories and files for modifications. ConfigEngine uses a custom written script to remotely connect to a device and download a user defined file on a periodical basis to identify if the file has changed. If a change is identified, ConfigEngine will generate a STIX object and transmit it to the STIX monitor.

POTENTIAL ENHANCEMENTS

Additional research is needed to tailor ConfigEngine into an operational tool that will leverage multiple methods to identify parameters being modified on supported devices. These methods will include monitoring traffic to the device and additional methods of querying a device which can be used to classify a malicious parameter modification. When a parameter modification is detected, the tool will provide a customizable alert(s) (e.g., outputting a syslog entry).

ASSET OWNER DEPLOYMENT GUIDANCE

The operational tool can be configured to include information regarding a device to be monitored, including device vendor, version, and connection information.

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.

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.

[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
[8] https://github.com/idaholab/STOTS

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

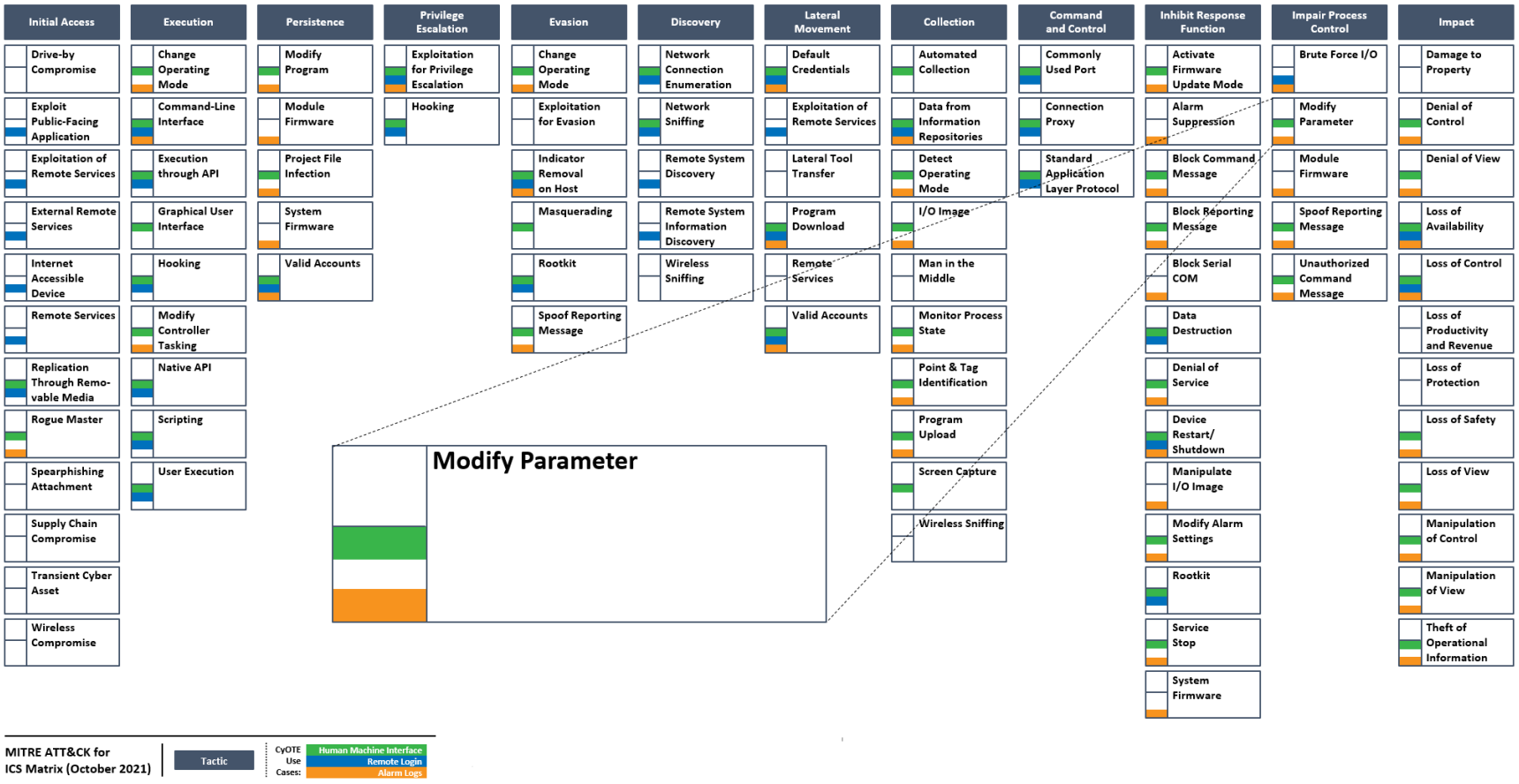

Figure 1: ICS ATT&CK Framework[9] – Modify Parameter Technique

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