TECHNIQUE T875: CHANGE PROGRAM STATE – IMPAIR PROCESS CONTROL

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI, Remote Login	Impair Process Control
Data Sources	
Potential Data Sources	Packet Captures, Network Protocol Analysis, OS Stack Logs, Application Logs
Historical Attacks	Triton Attack at Petro Rabigh[1]

TECHNIQUE DETECTION

The Change Program State technique[2] (Figure 1) may be detected when a device's program state is changed without warning or reason.

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 Change Program State 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 Change Program State technique was used in the Triton attack at Petro Rabigh in 2017.[6] In this attack, the following observables were identified:

- Increased internet traffic
- Increased DMZ traffic between information technology (IT) and OT networks

[1] MITRE, *Software: Triton, TRISIS, HatMan,* https://collaborate.mitre.org/attackics/index.php/Software/S0013
[2] MITRE ATT&CK for ICS, T875: Change Program State, https://collaborate.mitre.org/attackics/index.php/Technique/T0875. Note that this technique has been deprecated, and its content merged into T858, Change Operating Mode: https://collaborate.mitre.org/attackics/index.php/Technique/T0858
[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.
[6] https://www.eenews.net/stories/1060123327

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

COMPREHENSION

In the Triton attack at Petro Rabigh, the adversary first gained access through an engineering workstation to map the network; once they gained control of the workstation, they moved through the network and deployed the malware, changing program states and device logic to issue malicious command messages that shut down part of the plant.[7] By understanding the nature and possible origins of this attack, as well as how the adversary used the Change Program State 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 capability that reads and analyzes network traffic captures based upon set criteria, which are located in a separate configuration file. The criteria compare protocol layer fields to static values (e.g., MAC and statically defined IP addresses of hosts). It alerts on trusted IP lists for unauthorized traffic detection, monitors for PLC program download commands from unauthorized host(s), and controllers' running programs forced to a new state (e.g., reset, start, halt) from an operator or engineering workstation. The capability's output provides statistics about observables (i.e., number of times triggered, which packets caused the trigger, data about network streams, and which streams include the full or a portion of the protocol cycle).

POTENTIAL ENHANCEMENTS

Additional research is needed to tailor this capability to monitor network traffic for connections from non-authorized devices, download program commands outside scheduled maintenance windows (integration with group calendar), identify remote shutdown commands from authorized/unauthorized workstations, and alert when a controller is forced to a different state. The capability will rely on a user-defined list of hosts permitted to communicate with and provide commands to a device (e.g., human-machine interface [HMI], engineering workstation). The capability's configuration file will detail what protocols to monitor for commands and state changes.

ASSET OWNER DEPLOYMENT GUIDANCE

Deploying this capability in a continuously monitoring state will require connection to a span port of the desired network. This capability can also be used offline by ingesting network traffic in a Packet Capture (PCAP) file. The capability will alert when hosts not on the *allowlist* issue commands or send reporting messages. Alerts can be customized to output to a JSON log or a STIX 2.1 format.

[7] CyOTE Case Study: Triton in Petro Rabigh. https://inl.gov/wp-content/uploads/2021/09/Triton-CyOTE-Case-Study.pdf

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.

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

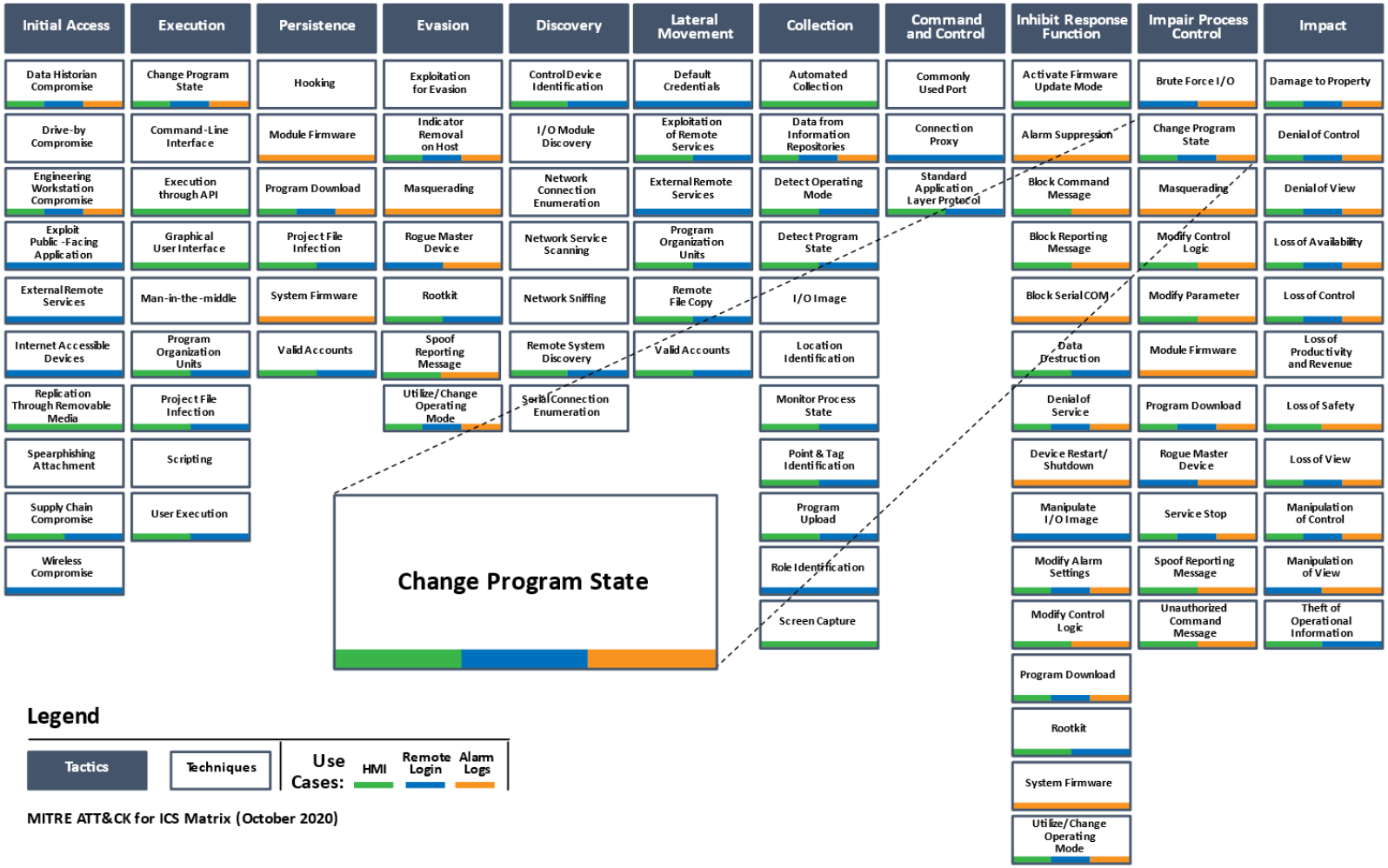

Figure 1: ICS ATT&CK Framework[8] – Change Program State Technique – Impair Process Control

[8] © 2020 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.