TECHNIQUE T868: DETECT OPERATING MODE

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
HMI, Remote Login	Collection
Data Sources	
Potential Data Sources	Device Logs, Network Protocol Analysis, Packet Capture
Historical Attacks	Triton Attack at Petro Rabigh[1]

TECHNIQUE DETECTION

The Detect Operating Mode technique[2] (Figure 1) may be detected when there are unrecognized connections to the network, or when there are unfamiliar files on the network with information about device operating modes.

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 Detect Operating Mode 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 Detect Operating Mode 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

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

---

[1] MITRE, *Software: Triton, TRISIS, HatMan,* https://collaborate.mitre.org/attackics/index.php/Software/S0013
[2] MITRE ATT&CK for ICS, T868: Detect Operating Mode, https://collaborate.mitre.org/attackics/index.php/Technique/T0868
[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

COMPREHENSION

In the Triton attack at Petro Rabigh, the adversary first gained access through an engineering workstation to deploy the malware. The adversary had obtained the IP addresses of Triconex safety instrumented system (SIS) controllers, allowing them to gather information on device operating modes. They continued moving through the network and modified operating modes 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 Detect Operating Mode 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 Proof of Concept tool performs deep packet inspection of Modbus protocols to alert when a "read register" command is identified for the operating mode register. An "allow/deny" configuration file is used to filter alerts from approved hosts and flag unapproved host commands.

POTENTIAL ENHANCEMENTS

Further development may include a dynamic list of "allowed" queries and hosts and support for various hardware and protocols. This will reduce the work of generating the configuration file and improve the anomaly detection capabilities of the tool.

ASSET OWNER DEPLOYMENT GUIDANCE

An operational tool should be deployed by a network team, in conjunction with cyber defenders and operators, to a host capable of processing the desired amount of traffic in an acceptable time frame. This host will either need access to a span port for live traffic or stored Packet Capture (PCAP) files awaiting to be processed. The operational tool can be configured by populating it with supporting information regarding approved hosts.

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

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

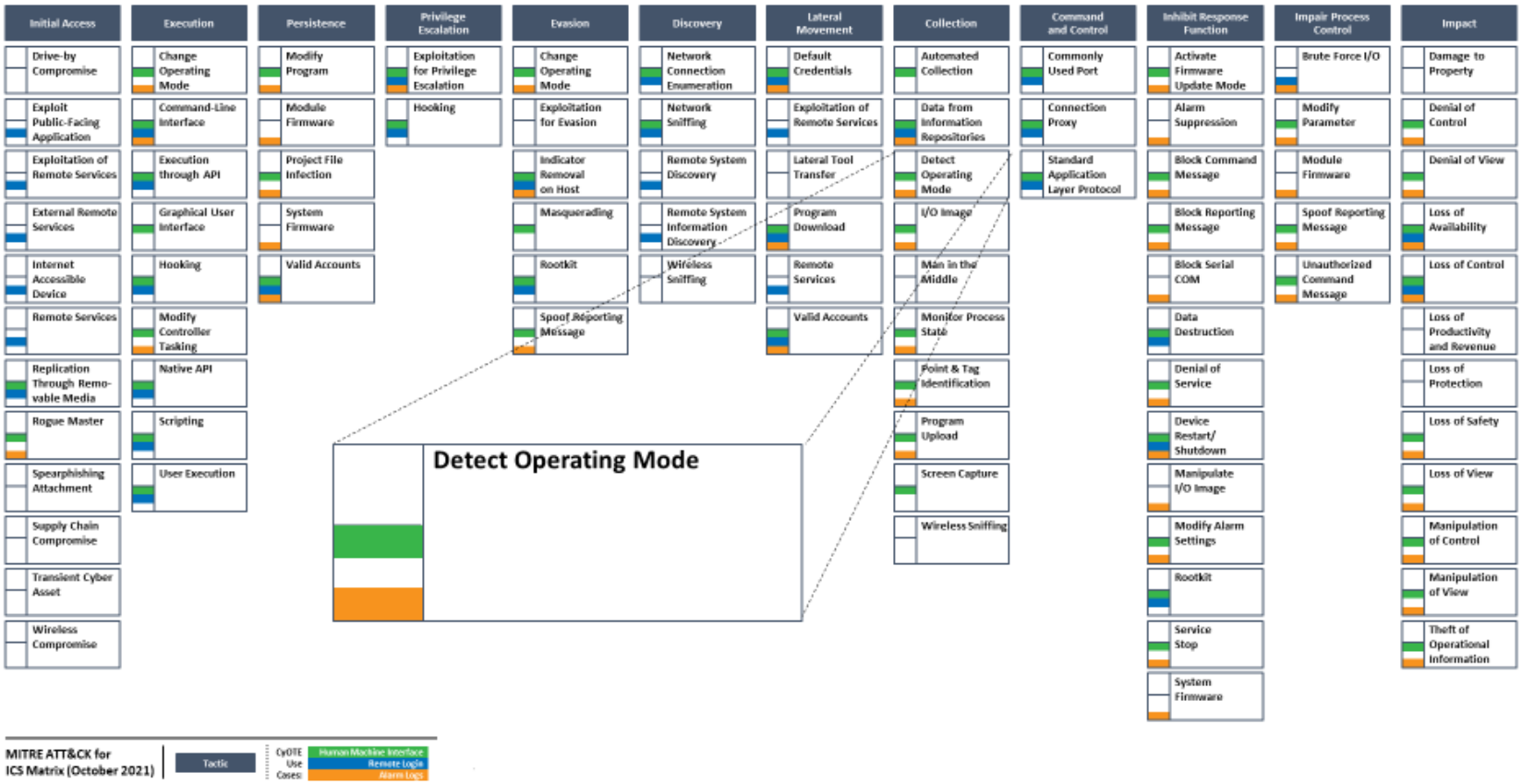

Figure 1: ICS ATT&CK Framework[8] – Detect Operating Mode Technique

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