TECHNIQUE T843: PROGRAM DOWNLOAD

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI, Remote Login	Lateral Movement
Data Sources	
Potential Data Sources	Packet Captures, Operating System Stack Logs, Data Historian, Netflow Logs, Application Logs
Historical Attacks	Triton Attack at Petro Rabigh[1]

TECHNIQUE DETECTION

The Program Download technique[2] (Figure 1) may be detected when new and unknown programs are downloaded to a network, or if a device operating mode is changed to accept a program download.

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

- Increased internet traffic
- Unfamiliar IP addresses noted in NetFlow logs
- Device operating mode change
- Software being installed

---

[1] MITRE, *Software: Triton, TRISIS, HatMan,* https://collaborate.mitre.org/attackics/index.php/Software/S0013
[2] MITRE ATT&CK for ICS, T843: Program Download, https://collaborate.mitre.org/attackics/index.php/Technique/T0843
[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 used the TriStation protocol to download programs onto devices. They then moved 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 Program Download 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 outlines a process to analyze OT network traffic and use deep packet inspection to identify potential indicators arising from an attempted program download.

POTENTIAL ENHANCEMENTS

This process can be enhanced by leveraging device logs to trigger network traffic capture and assist network capture analysis.

ASSET OWNER DEPLOYMENT GUIDANCE

The CyOTE Recipe can be leveraged to develop an operational tool. This tool should be deployed by the 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 and populated 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

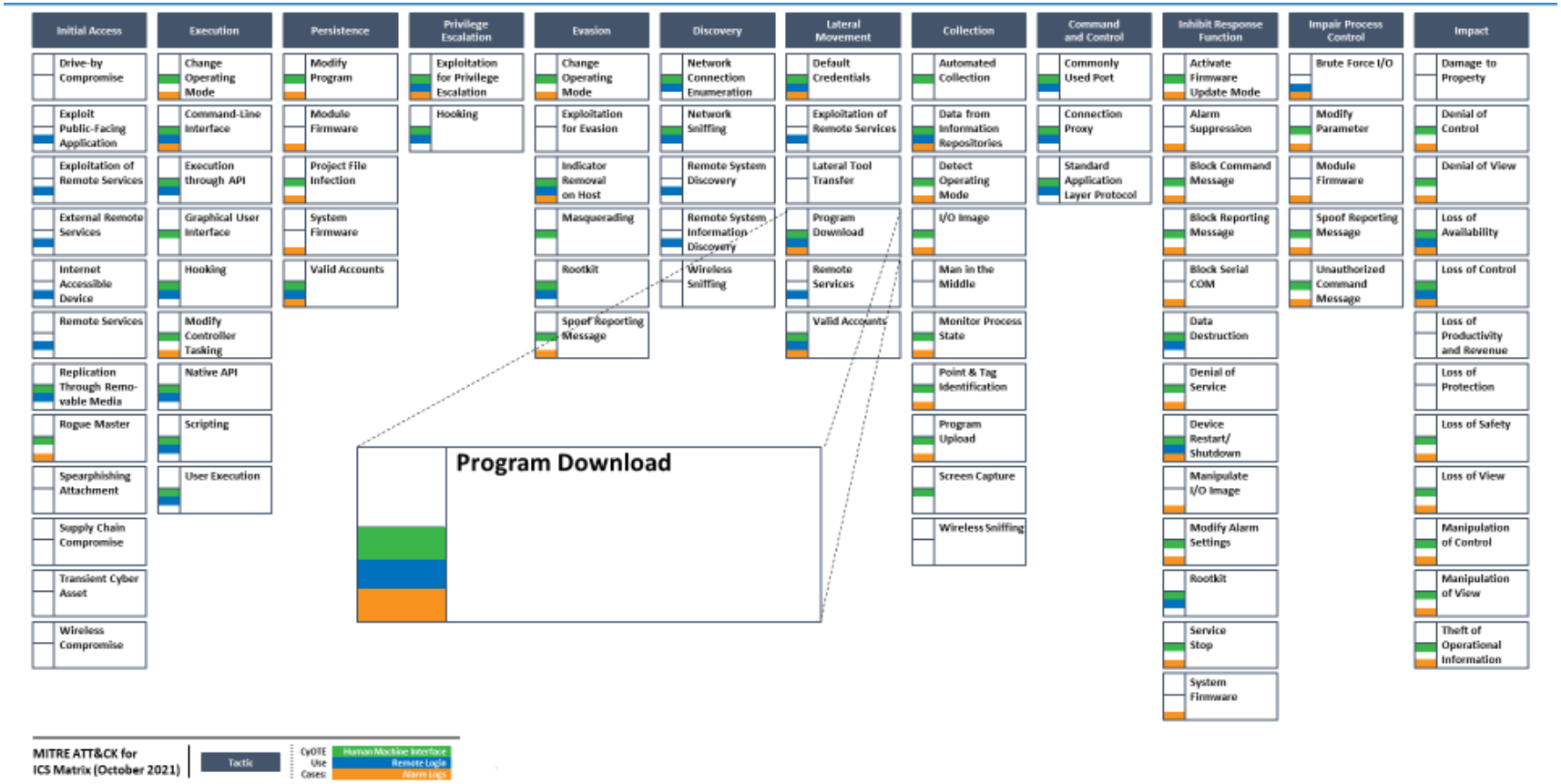

Figure 1: ICS ATT&CK Framework[8] – Program Download Technique

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