TECHNIQUE T848: ROGUE MASTER

CyOTE Use Case(s)[1]	MITRE ATT&CK for ICS® Tactic
Alarm Logs, Remote Login	Initial Access
Data Sources	
Potential Data Sources	Packet Captures, Network Protocol Analysis, OS Stack Logs, Application Logs
Historical Attacks	Ukraine 2015[2]

TECHNIQUE DETECTION

The Rogue Master technique[3] (Figure 1) may be detected via network traffic logs and application logs if they indicate unauthenticated messages or unrecognized IP addresses connecting into the system.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools[4] and Recipes[5] for asset owners and operators (AOO) to identify indicators of attack for techniques like Rogue Master within their operational technology (OT) networks. Referencing CyOTE Case Studies[6] 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.

OBSERVABLES FROM HISTORICAL ATTACKS

There are multiple historical attacks where this technique was used to impact operations. One example where this technique was used is the 2015 attack on Ukrainian power companies, in

[1] CyOTE Use Cases (Alarm Logs, Human-Machine Interface [HMI], and Remote Login) were identified by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and validated by Idaho National Laboratory (INL) as situations where OT log data may have a high likelihood of containing attack indicators. More information on Use Cases and how they apply to Technique Detection Capability Sheets can be found in the Technique Prioritization Report: https://inl.gov/wp-content/uploads/2021/12/CyOTE-Technique-Prioritization-Report-2021.pdf

[2] This Technique Detection Capability Sheet focuses on this technique's use in one historical attack. See the MITRE page on T848: Rogue Master for additional historical attacks that have used this technique: https://collaborate.mitre.org/attackics/index.php/Technique/T0848

[3] MITRE ATT&CK for ICS, T848: Rogue Master, https://collaborate.mitre.org/attackics/index.php/Technique/T0848

[4] 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) to validate a recipe.

[5] 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.

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

which threat actors took control of the OT environments via control systems.[7] In this attack, the following observables could have been identified:

- Control commands issues from distribution management system
- System changes
- Technical artifacts generated through the use of the rogue master

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

COMPREHENSION

In the Ukraine 2015 attack, the adversaries started with a successful spearphishing campaign that started at least six months prior to a cyber-induced power outage, which occurred on 23 December 2015. The attack resulted in adversaries compromising three power distribution utilities in Ukraine and opening breakers at more than 50 substations, causing a loss of power for approximately 225,000 customers. Adversaries took steps to inhibit response efforts by carrying out telephonic denial of service attacks against some utility call centers, shutting down backup power systems at control centers, uploading malicious firmware to damage devices used to remotely control substations, and using a wiper malware to damage servers and workstations.[8] By understanding the nature and possible origins of this attack, as well as how the adversary used the Rogue Master 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 T848 Recipe describes a capability, based on the CyOTE methodology,[9] to read and analyze network traffic capture and analyze it based upon a set of criteria defined in a separate configuration file. The criteria compare protocol layer fields to static values, alert on trusted IP lists for unauthorized traffic detection, and conduct protocol validating. The T848 Recipe identifies outputs that will provide statistics about triggered criteria (i.e., number of times triggered, which packets caused the trigger, data about the network streams) and which network streams included the full protocol cycle or only a part. The protocol validation summary identifies the packets associated with validation (or lack thereof).

POTENTIAL ENHANCEMENTS

Further development by an AOO can involve monitoring network traffic for commands issued from non-authorized devices. The capability can leverage a user-defined list of allowed hosts (in the configuration file) which are permitted to communicate with and provide commands to a device (i.e., human-machine interface [HMI], engineering workstation(s)).

---

[7] https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)

[8] Contact CyOTE.Program@hq.doe.gov for more information.

[9] Methodology for Cybersecurity in Operational Technology Environments, 2021. https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf

ASSET OWNER DEPLOYMENT GUIDANCE

AOOs may leverage the T848 Recipe to develop an operational tool in a state of continuous monitoring. The tool will need to connect to a span port of the desired network. This tool may be used offline by ingesting network traffic in a Packet Capture (PCAP) file. The capability will alert when hosts that are not on the allowed hosts list issue commands. The command list can be reduced by providing a list of authorized hosts. 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.

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

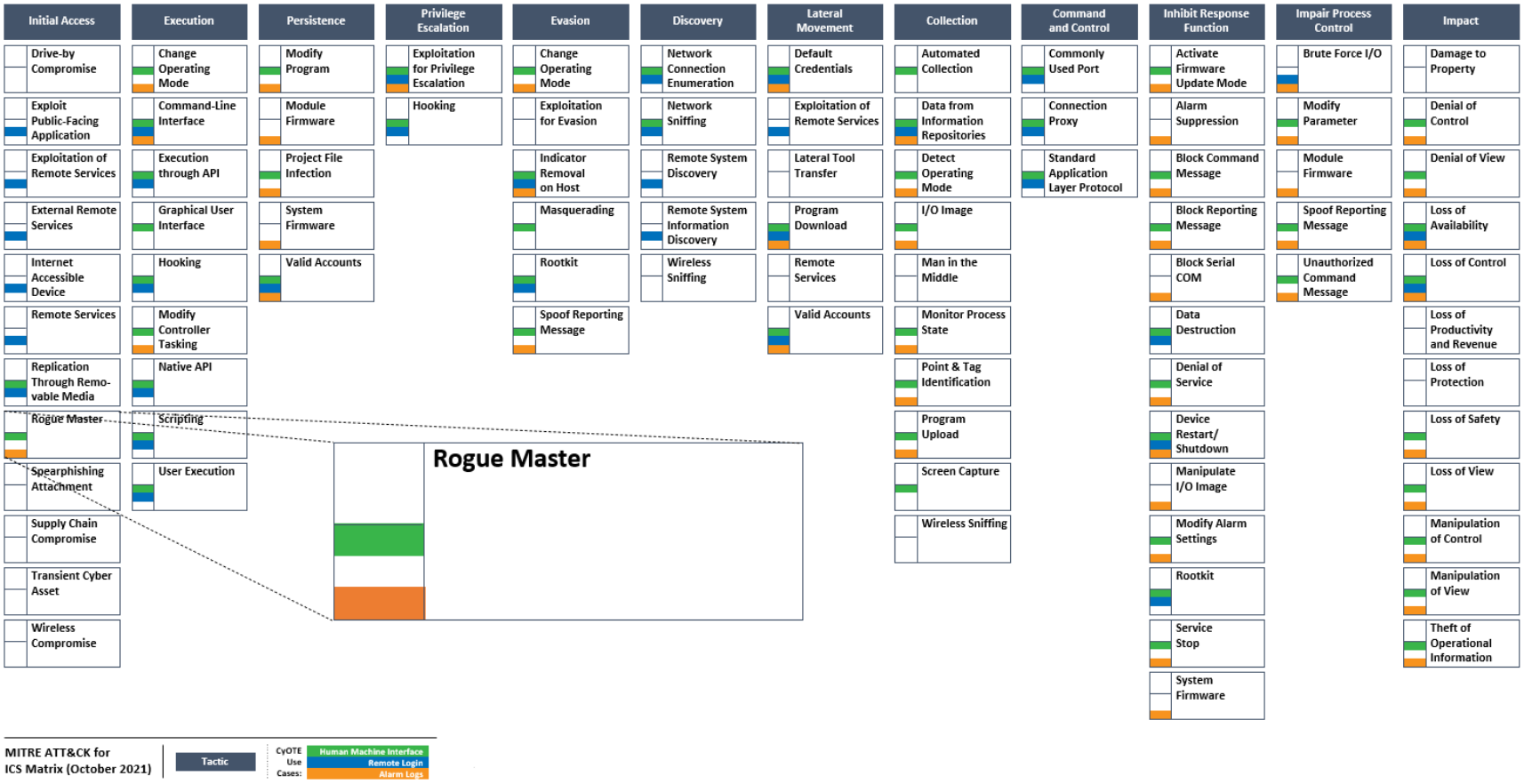

Figure 1: ICS ATT&CK Framework[10] – Rogue Master Technique

[10] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.