TECHNIQUE T872: INDICATOR REMOVAL ON HOST

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI, Remote Login	Evasion
Data Sources	
Potential Data Sources	File Monitoring, Process Monitoring, Process Command-line Parameters, API Monitoring, Windows Event Logs
Historical Attacks	Triton Attack at Petro Rabigh[1]

TECHNIQUE DETECTION

The Indicator Removal on Host technique[2] (Figure 1) may be detected when changes made to a device are overwritten or deleted from logs.

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 Indicator Removal on Host 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 Indicator Removal on Host technique was used in the Triton attack at Petro Rabigh in 2017.[6] In this attack, the following observables were identified:

- Anti-virus software alert writing of false program
- Event logs, scripts, registry keys, and other data being deleted
- Software being uninstalled

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, T872: Indicator Removal on Host, https://collaborate.mitre.org/attackics/index.php/Technique/T0872
[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 took several actions to hide the attack. Once they had accessed the network and deployed the malware via an internet-connected engineering workstation, they removed indicators of the attack from the controllers by reverting them to a previous operating state. If this failed, the malware overwrote the malicious program with a dummy one. Hiding these actions allowed the adversary to gain deeper access to the network, modifying controller logic and operating modes 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 Indicator Removal on Host 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 uses industry standard remote process monitoring, remote log aggregation, and best practice host-based access control configuration. Host systems are configured manually or through group policy to use best practice access controls for protecting local log files and executables. The Recipe provides remote process and log monitoring via a SYSLOG messaging service or a host-based agent, depending on the host's capabilities. A LOGSTASH server receives remote process and log updates hosts and stores this information in an Elasticsearch database. The Recipe describes how to analyze the collected data using Elasticsearch and provide alerts resulting from finding indicators of compromise using Kibana messaging.

POTENTIAL ENHANCEMENTS

The capability could provide integrity hardening through Mandatory Access Control (MAC) or Discretionary Access Control (DAC) policies (the use of MAC or DAC is dependent on capabilities of the host). This CyOTE Recipe could also remotely monitor system processes and log files for real-time detection and store this data for forensic analysis.

ASSET OWNER DEPLOYMENT GUIDANCE

Deploying the capability in the CyOTE Recipe in a continuously monitoring state will require modification of host devices and provide network access from each host to a log server. The log server will need sufficient storage to keep log files for forensic analysis. Additionally, the log server or a separate server will need to be established to analyze the collected logs and send alerts. Ideally, this recipe would be integrated as part of an existing SIEM.

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.

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

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

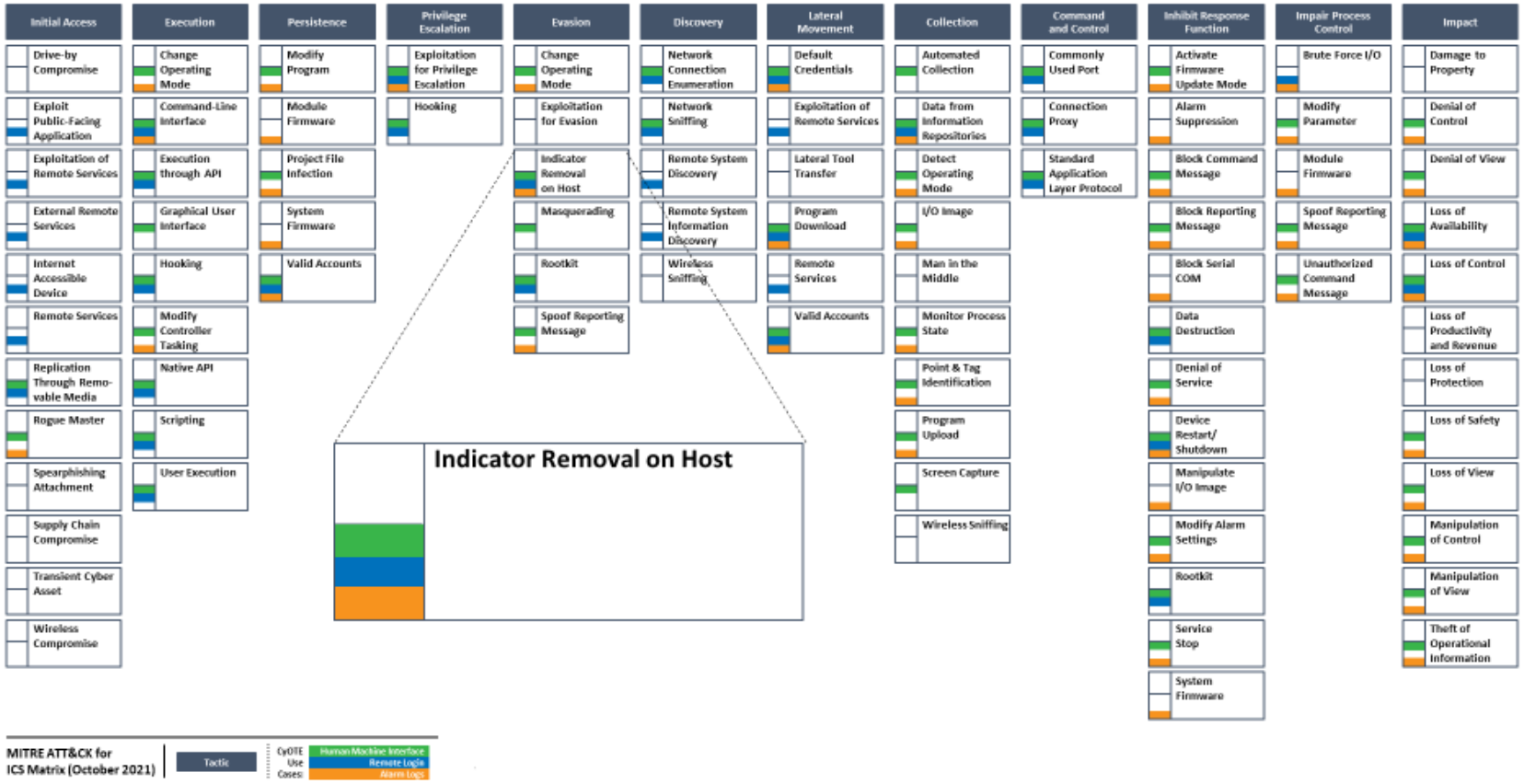

Figure 1: ICS ATT&CK Framework[8] – Indicator Removal on Host Technique

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