TECHNIQUE T809: DATA DESTRUCTION

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
HMI, Remote Login	Inhibit Response Function
Data Sources	
Potential Data Sources	File Monitoring, Process Command-Line Parameters, Process Monitoring
Historical Attacks	Industroyer/CRASHOVERRIDE[1]

TECHNIQUE DETECTION

The Data Destruction technique[2] (Figure 1) may be detected if there are non-native files and data on a system, or if data backups or other files are deleted 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 within their operational technology (OT) networks. However, for the Data Destruction technique, the CyOTE program recommends the use of the ConfigEngine and FileEngine tools to develop a capability for identifying Data Destruction in an AOO's OT environment. Additionally, by 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 Data Destruction technique was used in the Industroyer attack in the Ukraine in 2016.[6,7] In this attack, the following observables were identified:

- File monitoring systems detecting file deletion
- Process command-line parameters changing or not accepting certain commands

---

[1] MITRE, Software: Industroyer, CRASHOVERRIDE, https://collaborate.mitre.org/attackics/index.php/Software/S0001
[2] https://collaborate.mitre.org/attackics/index.php/Technique/T0809
[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.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
[7] https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

- Process monitoring systems picking up on unknown processes running or installing files

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

COMPREHENSION

In the Industroyer attack, the adversary was able to destroy crucial data once they had gained enumerated connected network devices and learned system information and device communication patterns. They then were able to access the Data Historian and initiate the compromise, causing impactful and damaging changes through the use of other techniques, including Device Restart/Shutdown, Service Stop, Manipulation of Control, and Manipulation of View.[8] By understanding the nature and possible origins of this attack, as well as how the adversary used the Data Destruction 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

As previously noted, the CyOTE program recommends the use of ConfigEngine and FileEngine to develop a capability for identifying Data Destruction in an AOO's OT environment. ConfigEngine and FileEngine, two detection tools in the Structured Threat Observable Tool Set (STOTS),[9] monitor directories and files for modifications. ConfigEngine uses a custom written script to remotely connect to a device and download a user-defined file on a periodic basis to identify if the file has changed. If a change is identified, ConfigEngine will generate a Structured Threat Information Expression (STIX) object and transmit it to the STIX monitor. FileEngine remotely connects to a device using SSH and saves the output of a directory listing for a user-defined folder. If a change is identified in the directory listing, FileEngine will generate a STIX object and transmit it to the STIX monitor.

POTENTIAL ENHANCEMENTS

Additional research will be necessary to tailor this capability to leverage multiple methods and identify Data Destruction on supported devices. The documentation provided with the tools will give example lists of potential directories and files to monitor on supported systems. When Data Destruction is detected, the tools should provide a customizable alert (e.g., outputting a syslog entry).

ASSET OWNER DEPLOYMENT GUIDANCE

To deploy an operational tool, directories and files will need to be configured so they can be monitored. Additionally, details will be needed on how to remotely connect to device(s) to be monitored, and alerts will need to be configured.

[8] CyOTE Case Study: CRASHOVERRIDE/Industroyer. Visit https://inl.gov/cyote/ for more information.
[9] https://github.com/idaholab/STOTS

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

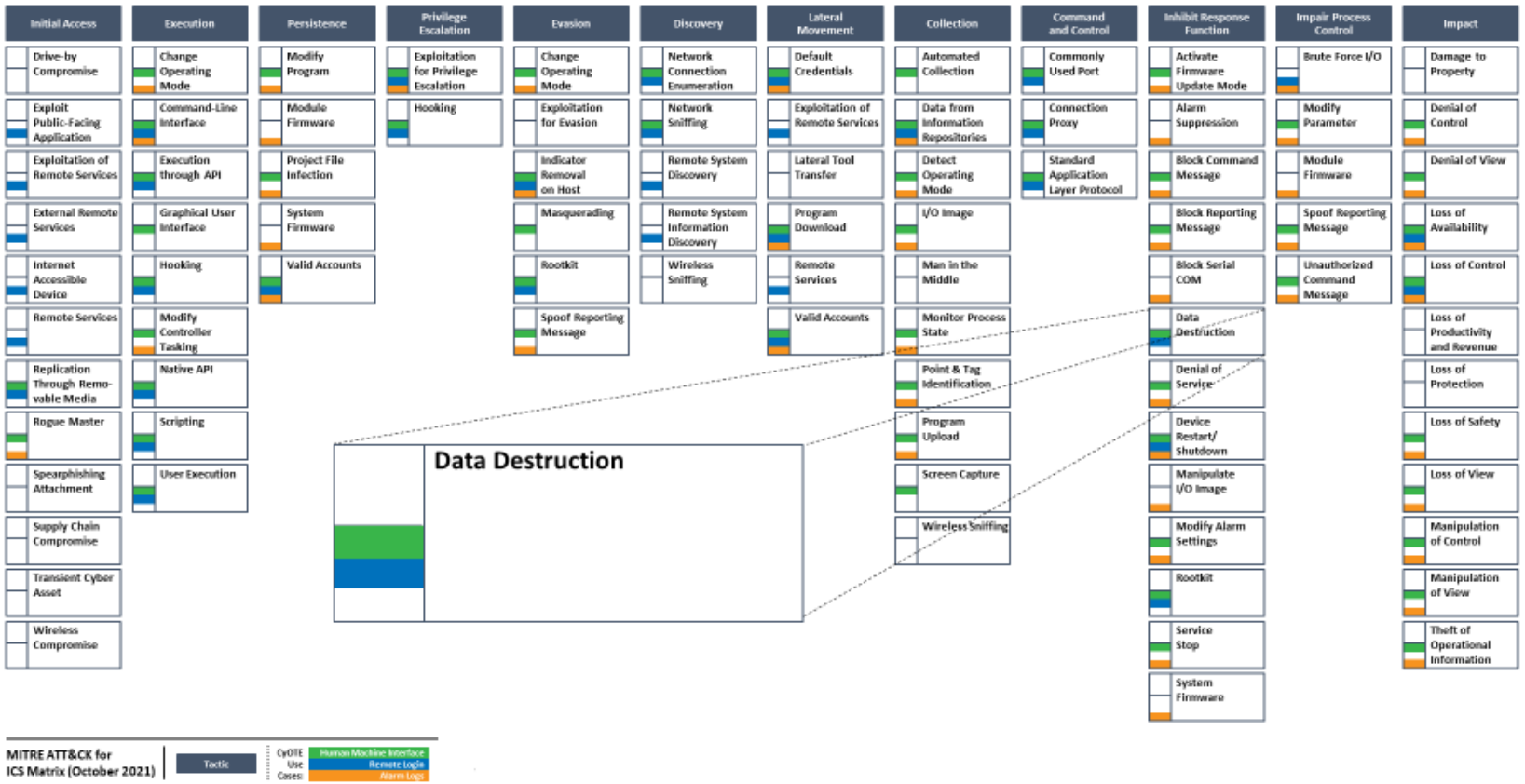

Figure 1: ICS ATT&CK Framework[10] – Data Destruction Technique

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