TECHNIQUE T889: MODIFY PROGRAM

CyOTE Use Case(s)[1]	MITRE ATT&CK for ICS® Tactic
HMI, Alarm Logs	Persistence

Data Sources	
Potential Data Sources	Device/Application/System Logs, Network Protocol Analysis, NetFlow Logs, Packet Capture, Zeek Logs, Data Historian
Historical Attacks	WannaCry Ransomware Attack on Renault-Nissan[2]

TECHNIQUE DETECTION

The Modify Program technique (Figure 1) may be detected when there are indications of modified or added programs found in logs from the Potential Data Sources identified above.

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 Modify Program 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 Modify Program technique is found in Stuxnet[6] and PLC-Blaster[7] and was used in the WannaCry attack on Renault-Nissan.[8] In the WannaCry attack, the following observables were

[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 T889: Modify Program for additional historical attacks that have used this technique: https://collaborate.mitre.org/attackics/index.php/Technique/T0889

[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] MITRE, Software: Stuxnet, https://collaborate.mitre.org/attackics/index.php/Software/S0010

[7] MITRE, Software: PLC-Blaster, https://collaborate.mitre.org/attackics/index.php/Software/S0009

[8] Cybersecurity & Infrastructure Security Agency (CISA), Alert (TA17-132A), Indicators Associated with WannaCry Ransomware, https://www.cisa.gov/uscert/ncas/alerts/TA17-132A.

identified:

- Host system registry modification
- Host system registry keys added

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

COMPREHENSION

In the WannaCry ransomware attack in 2017, the adversary added two registry keys to “tasksche.exe” which modified the registry to enable the malware to continue to run without needing to leverage the initial exploit again. The initial exploit that the adversaries employed was the EternalBlue exploit in the Exploitation of Remote Services technique, which they used to gain initial access to Renault-Nissan systems.[9] By understanding the nature and possible origins of this attack, as well as how the adversary used the Modify Program 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 T889 Recipe outlines general guidance to help AOOs develop a capability to analyze operational technology (OT) network traffic and identify indicators used to modify a device’s program. This capability focuses on inconsistencies in the services that a device provides. CyOTE Recipes demonstrate how to apply the CyOTE methodology[10] to gain a better understanding of identified anomalies and make better risk-informed decisions.

POTENTIAL ENHANCEMENTS

Taking proactive and preventive measures to reduce the risk of a modified program occurring may likely deter attackers from using this attack path. Further development may leverage device logs to trigger network traffic capture and assist network capture analysis and system logs to trigger device monitoring.

ASSET OWNER DEPLOYMENT GUIDANCE

To deploy this capability, the CyOTE T889 Recipe recommends to develop an operational tool to be deployed by the network team, in conjunction with cyber defenders and operators, to a host capable of processing the desired amount of traffic and system logs in an acceptable time frame. This host will either need access to a span port for live traffic or stored Packet Capture (PCAP) files waiting to be processed. The host will also need access to system logs. The tool will need to be configured and populated initially with supporting information on 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

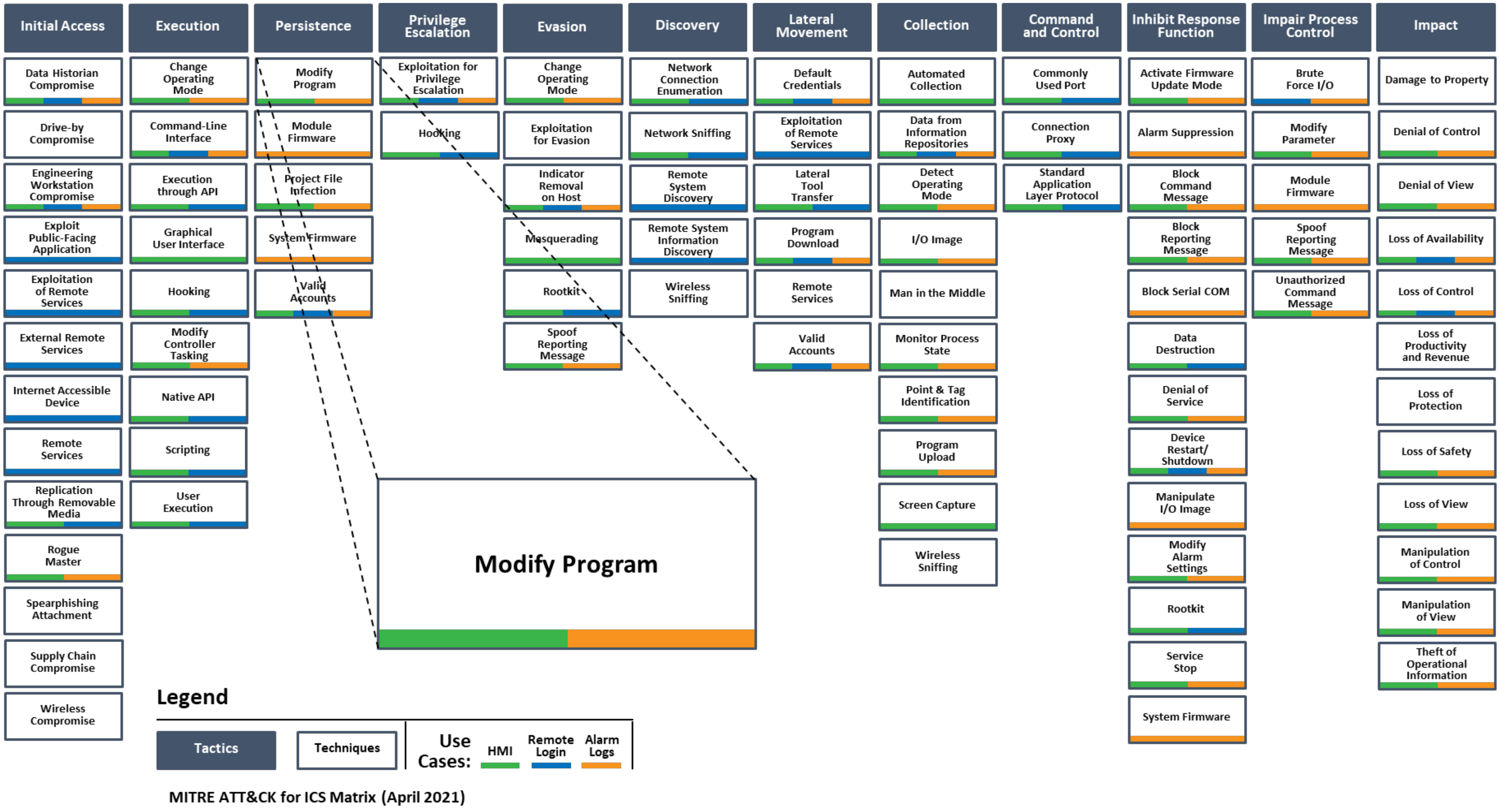
[9] CyOTE Case Study: WannaCry. Contact CyOTE.Program@hq.doe.gov for more information.

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

capabilities, and to the other historical Case Studies available at the CyOTE website for information on other historical cyberattacks.

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



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

Modify Program

Legend

Tactics	Techniques	Use Cases:	HMI	Remote Login	Alarm Logs

MITRE ATT&CK for ICS Matrix (April 2021)

Figure 1: ICS ATT&CK Framework[11] – Modify Program Technique

[11] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.