TECHNIQUE T849: MASQUERADING

CyOTE Use Case(s)[1]	MITRE ATT&CK for ICS® Tactic
HMI	Evasion
Data Sources	
Potential Data Sources	Command Execution, File Metadata, File Modification, Process Metadata, Scheduled Job Metadata, Scheduled Job Modification, Service Creation, Service Metadata
Historical Attacks	Industroyer/CRASHOVERRIDE, EKANS, REvil, Stuxnet, and Triton[2]

TECHNIQUE DETECTION

The Masquerading technique (Figure 1) may be detected when there are indications of unexpected or disguised files found in the file directory or common service programs running from unexpected parent processes or locations.

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 Masquerading 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 Masquerading technique has been used in several different historical attacks. One example

[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 T849: Masquerading for additional historical attacks that have used this technique: https://collaborate.mitre.org/attackics/index.php/Technique/T0849.

[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.

where this technique was used is the 2020 EKANS attack on Honda.[6] In this attack, the following observables were identified:

- Unexpected "update.exe" file in directory

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

COMPREHENSION

In the 2020 EKANS attack on Honda, adversaries used the Masquerading technique to disguise malicious content as "Update.exe."[7] Engineers then ran this anomalous executable under the assumption that it was a legitimate update. By understanding the nature and possible origins of this attack, as well as how the adversary used the Masquerading 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 T849 Recipe outlines general guidance to help AOOs confirm suspicion of the use of Masquerading in their OT environment and provides recommendations on ways to improve their detection capabilities for this technique. CyOTE Recipes demonstrate how to apply the CyOTE methodology[8] to gain a better understanding of identified anomalies and make better risk-informed decisions.

POTENTIAL ENHANCEMENTS

Taking proactive and preventive measure to reduce the risk of a masquerading attempt may likely deter attackers from attempting to use this attack path. Potential enhancements to current monitoring capabilities could include: developing a comprehensive analysis of network behaviors associated with service stop commands; identifying which particular processes may be susceptible to malicious modification/masquerading; implementing network segmentations and block actions to prevent unauthorized file changes from unauthorized subnets; clarifying what normal file metadata should look like to determine if it was manipulated; using code signing to verify digital signatures; leveraging application control to limit code executions on a system; enforcing file system access controls to restrict access to files/directories; and auditing accounts to validate permissions levels and to review access logs.

ASSET OWNER DEPLOYMENT GUIDANCE

To deploy this capability, the CyOTE T849 Recipe recommends to identify logging data required to perform alerting (e.g., network traffic captures, endpoint process execution logs), opportunities to include logging data into an alerting platform, and equipment that will allow for feasible implementation of log and data collection. Additionally, alerts will need to be created to

[6] https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/
[7] Ibid.
[8] Methodology for Cybersecurity in Operational Technology Environments, 2021. https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf

monitor activity and protection/prevention capabilities, and configurations will need to be selected that fit the parameters of the asset environment without interfering with operations.

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, 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

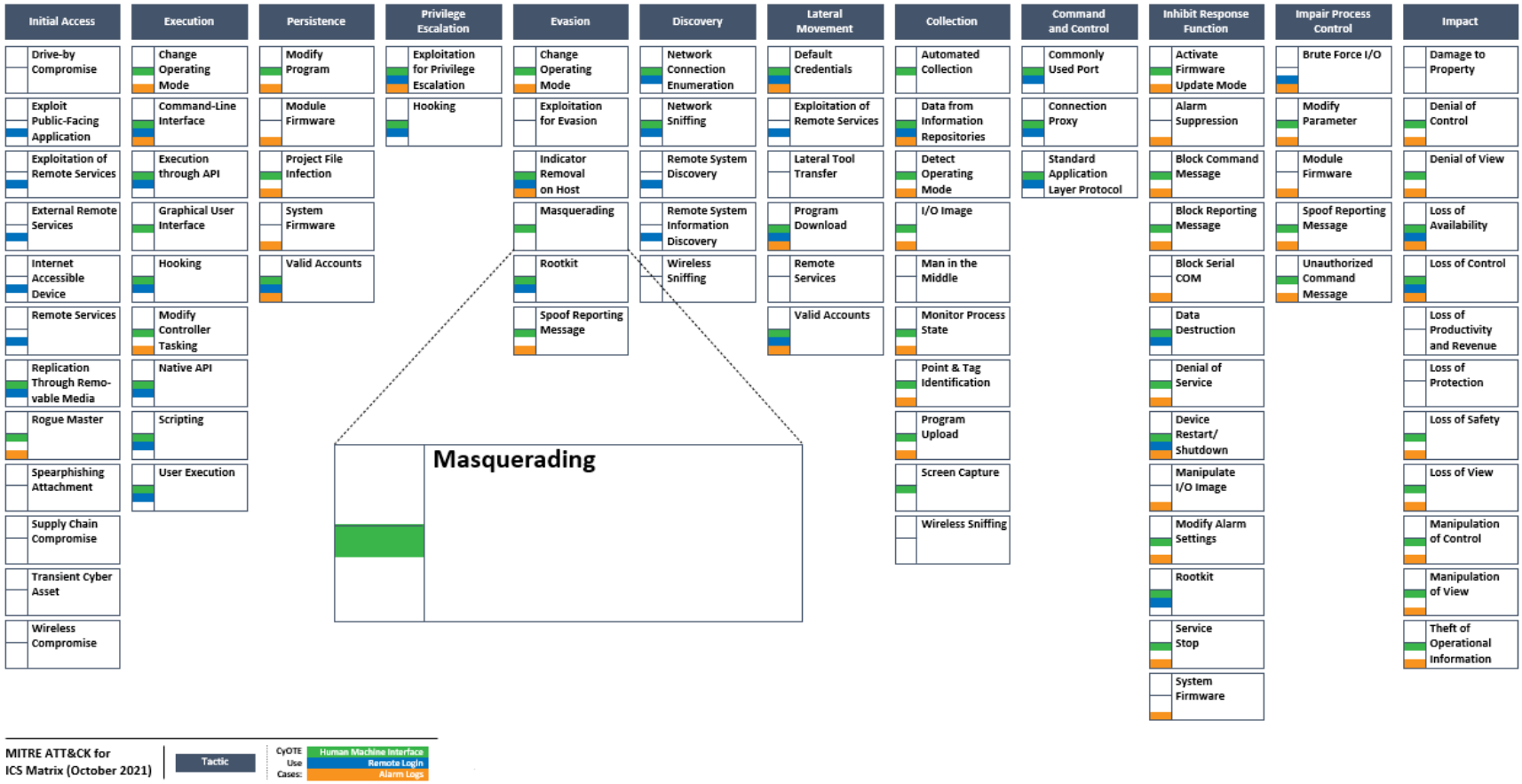

Figure 1: ICS ATT&CK Framework[9] – Masquerading Technique

[9] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.