TECHNIQUE T840: NETWORK CONNECTION ENUMERATION

CyOTE Use Case(s)[1]	MITRE ATT&CK for ICS® Tactic
HMI, Remote Login	Discovery
Data Sources	
Potential Data Sources	Command Execution, OS API Execution, Process Creation
Historical Attacks	EKANS software[2]

TECHNIQUE DETECTION

The Network Connection Enumeration technique (Figure 1) may be detected by using system baseline activity to determine if there are anomalous applications and processes. In limited cases, anomalous network activity may also indicate the existence of this technique. A baseline or knowledge of a baseline is required to be able to detect the use of this technique.

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 Network Connection Enumeration 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 Network Connection Enumeration technique is used by the EKANS software.[6] The following observables can be identified:

---

[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 T840: Network Connection Enumeration for additional historical attacks that have used this technique: https://collaborate.mitre.org/attackics/index.php/Technique/T0840

[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.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

- Invalid DNS responses

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

COMPREHENSION

EKANS performs a DNS lookup of an internal domain name associated with its target network to identify if it was deployed on the intended system. If EKANS attempts to reach a DNS connection that does not exist, it receives an invalid DNS response. Once the malware is deployed on the intended system, the software first masquerades itself as a valid executable with the filename "update.exe," which is similar to how other valid programs perform background software updates.[7] By understanding the nature and possible origins of this attack, as well as how the adversary used the Network Connection Enumeration 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 T840 Recipe outlines general guidance to help AOOs confirm suspicion of the use of Network Connection Enumeration 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 measures to reduce the risk of a network connection enumeration occurring may likely deter attackers from using this attack path. Potential enhancements to current monitoring capabilities could include: monitoring and analyzing process spawns and arguments for detecting various enumeration-performing tools; identifying enumeration parent processes and establishing context through additional process spawn analysis; monitoring DNS requests to identify hosts performing potentially malicious queries; monitoring for new domain activity which may be part of an enumeration; and deploying honeypots, honeynets, or decoy resources to detect network enumeration.

ASSET OWNER DEPLOYMENT GUIDANCE

To deploy this capability, the CyOTE T840 Recipe recommends to identify logging data required to perform alerting (e.g., DNS queries, response logs, network traffic captures, endpoint command/process execution and network connection logs), opportunities to include logging data into an alerting platform, and equipment that will allow for feasible implementation of log and data collection. Alerts will need to be created to monitor activity, and protection/prevention

[7] https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

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

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

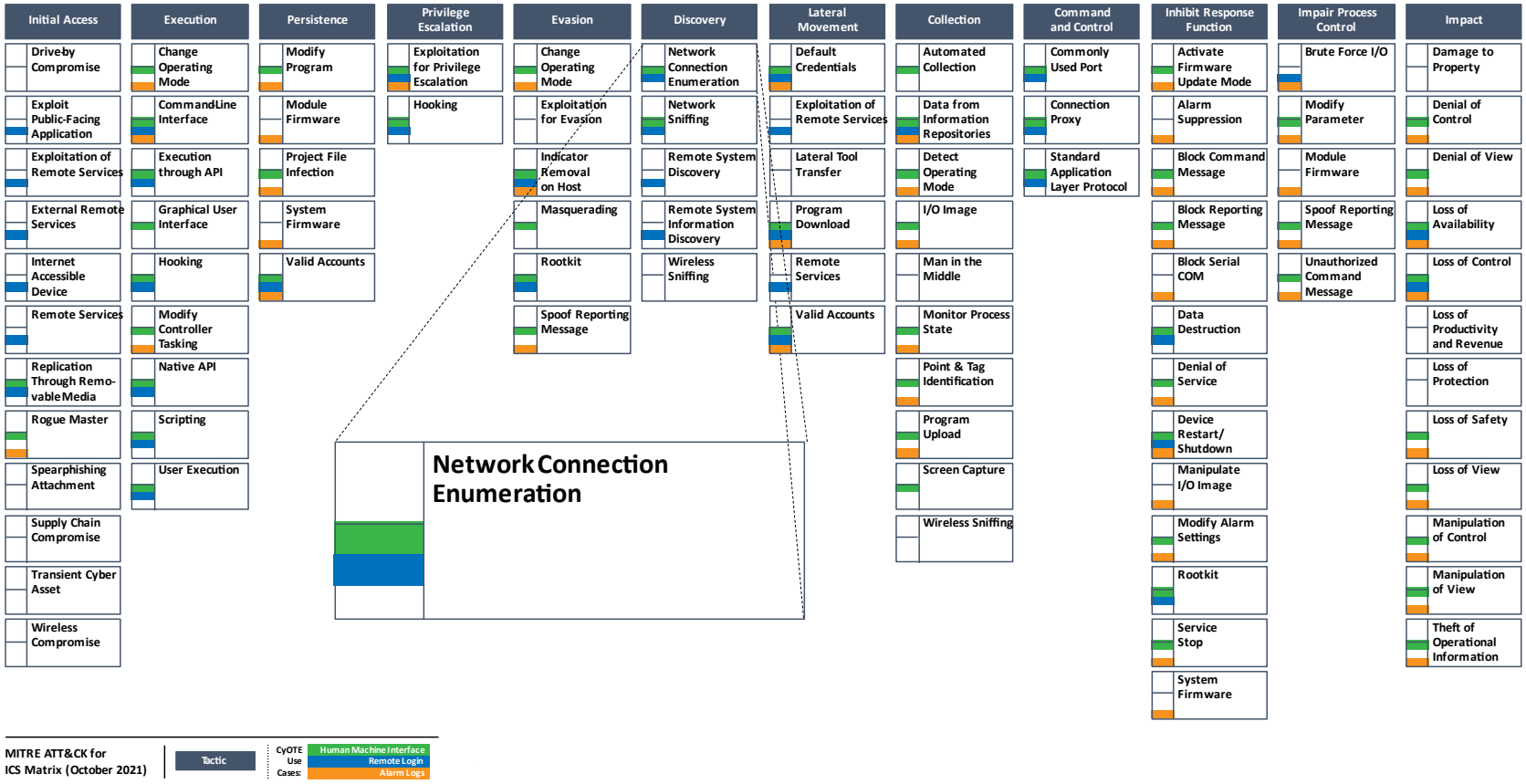

Figure 1: ICS ATT&CK Framework[9] – Network Connection Enumeration Technique

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