TECHNIQUE T846: REMOTE SYSTEM DISCOVERY

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Remote Login	Discovery
Data Sources	
Potential Data Sources	Packet Captures, Process Monitoring, Process use of Network, Process Command-line Parameters, Network Protocol Analysis, OS Stack Logs, Application Logs
Historical Attacks	Industroyer/CRASHOVERRIDE,[1] Triton Attack at Petro Rabigh[2]

TECHNIQUE DETECTION

The Remote System Discovery technique[3] (Figure 1) may be detected if there are unauthorized connections or packets sent across a network to scan for information.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools[4] and Recipes[5] for asset owners and operators (AOO) to identify indicators of attack for techniques like Remote System Discovery within their operational technology (OT) networks. Referencing CyOTE Case Studies[6] 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 Remote System Discovery technique was used in the Industroyer/CRASHOVERRIDE attack in the Ukraine in 2016[7,8] and in the Triton attack at Petro Rabigh in 2017.[9] In these attacks, the following observables were identified:

- Industroyer/CRASHOVERRIDE: Increased internet traffic from potentially malicious IP

[1] MITRE, Software: Industroyer, CRASHOVERRIDE, https://collaborate.mitre.org/attackics/index.php/Software/S0001
[2] MITRE, Software: Triton, TRISIS, HatMan, https://collaborate.mitre.org/attackics/index.php/Software/S0013
[3] MITRE ATT&CK for ICS, T846: Remote System Discovery, https://collaborate.mitre.org/attackics/index.php/Technique/T0846
[4] 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.
[5] 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.
[6] Visit https://inl.gov/cyote/ for all CyOTE Case Studies.
[7] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
[8] https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf
[9] https://www.eenews.net/stories/1060123327

addresses; logs within the control process
- Triton: Process monitoring; process use of network; process command-line parameters; increased internet traffic from potentially malicious IP addresses

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

COMPREHENSION

In the Industroyer attack, the adversary began discovering the system once they had inspected the state of the network to determine device roles and unique details (Network Connection Enumeration). They were able to issue unauthorized commands to cause impactful and damaging changes through the use of other techniques, including Device Restart/Shutdown, Service Stop, Manipulation of Control, and Manipulation of View.[10]

In the Triton attack, the adversary leveraged a poorly configured firewall to access the network, after which they accessed a remote engineering workstation to deploy the malware. This allowed them to discover devices on the system and carry out the attack into the system firmware, eventually modifying the control logic of the controllers to either shut down unexpectedly or to continue running in unsafe conditions. This shut down a portion of the Petro Rabigh plant.[11]

By understanding the nature and possible origins of these attacks, as well as how the adversaries used the Remote System Discovery technique to execute the attacks, 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 process to build capabilities to assist perception for identifying anomalies, looking into triggers to provide context, and assisting the decision-making process. A potential capability could read and analyze network traffic captures based upon set criteria, which are in a separate configuration file. The criteria compare protocol layer fields to static values (e.g., MAC and statically defined IP addresses of hosts). It alerts on trusted IP lists for unauthorized traffic detection, monitors for abnormal traffic typically used for detecting remote systems. The Recipe identifies outputs that will provide statistics about triggered criteria (i.e., number of times triggered, which packets caused the trigger, data about the network streams) and which network streams included the full protocol cycle or only a part.

POTENTIAL ENHANCEMENTS

Additional research is needed to tailor capabilities to monitor network traffic for connections from non-authorized devices, or abnormal connections from authorized devices. A capability will rely on a user-defined list of hosts permitted to communicate with and provide commands to a device (e.g., human-machine interface [HMI], engineering workstation). A capability's configuration file will detail what protocols to monitor for commands and state changes.

[10] CyOTE Case Study: CRASHOVERRIDE/Industroyer. Visit https://inl.gov/cyote/ for more information.
[11] CyOTE Case Study: Triton in Petro Rabigh, https://inl.gov/wp-content/uploads/2021/09/Triton-CyOTE-Case-Study.pdf

ASSET OWNER DEPLOYMENT GUIDANCE

An operational tool can be developed from these capabilities for use in a continuously monitoring state by connecting it to a span port of the desired network. The tool may be used offline by ingesting network traffic in a Packet Capture (PCAP) file. It will alert when hosts send traffic typically associated with system identification. Alerts can be customized to output to a syslog entry or a STIX 2.1 format.

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

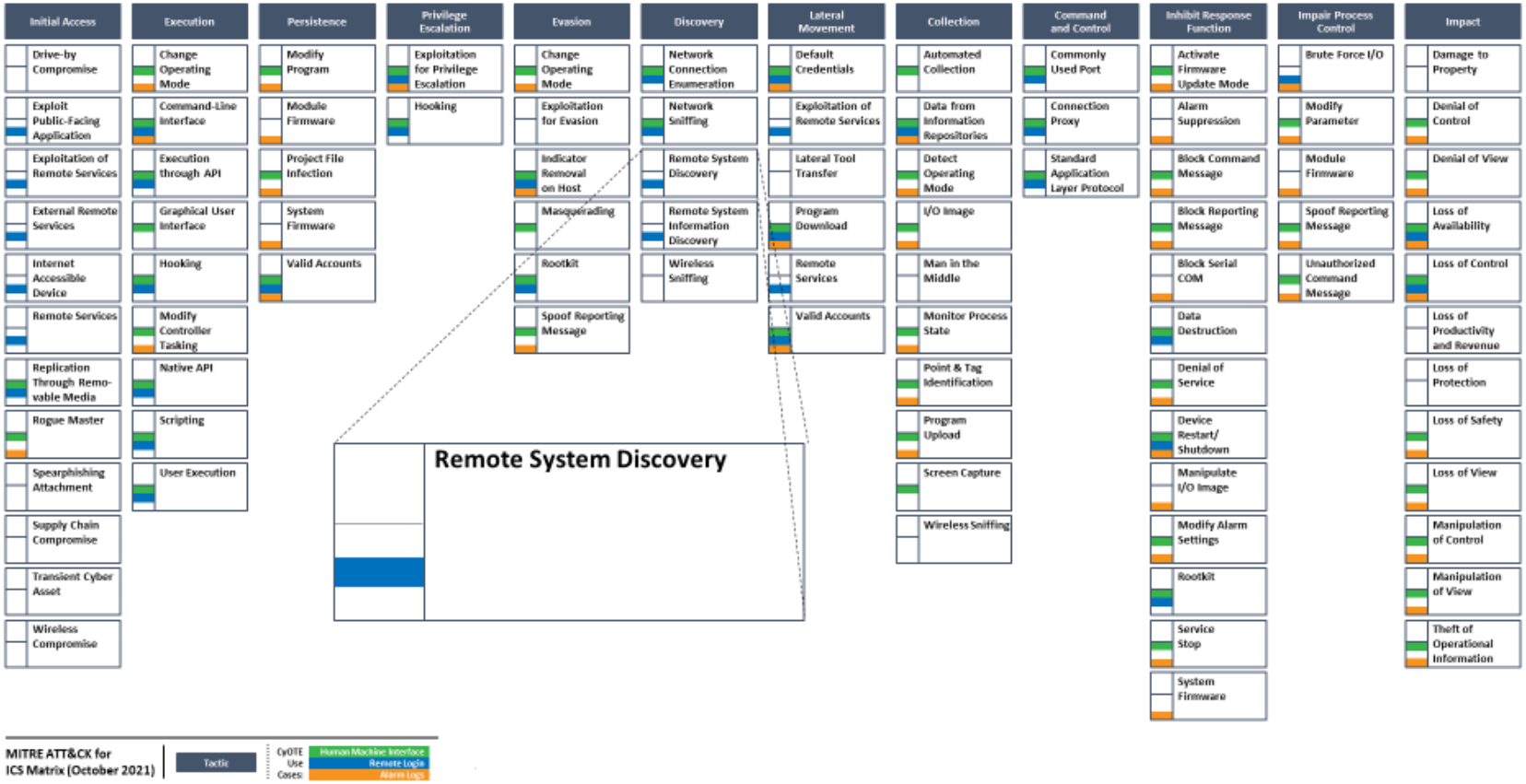

Figure 1: ICS ATT&CK Framework[12] – Remote System Discovery Technique

[12] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.