TECHNIQUE T886: REMOTE SERVICES

CyOTE Use Case(s)[1]	MITRE ATT&CK for ICS® Tactic
Remote Login	Lateral Movement, Initial Access
Data Sources	
Potential Data Sources	Command Execution, Logon Session Creation, Network Share Access, Network Connection Creation, Network Traffic Flow, Network Traffic Content, NetFlow logs, Process Creation
Historical Attacks	Industroyer/CRASHOVERRIDE, TRISIS, REvil, Stuxnet, Ukraine 2015[2]

TECHNIQUE DETECTION

The Remote Services technique (Figure 1) may be detected when there are indications of remote access, data transmission, authentication, name resolution, and/or other remote functions 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 Remote Services 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 Remote Services 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 T886: Remote Services for additional historical attacks that have used this technique: https://collaborate.mitre.org/attackics/index.php/Technique/T0886

[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 Ukraine 2015 incident.[6] In this attack, the following observables were identified:

- Log data

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

COMPREHENSION

In the 2015 Ukraine incident, attackers employed the Remote Services technique by using remote access tools within the environment to take control of operator workstations and open individual breakers across substations. They first gained access approximately 183 days (estimated to be June 2015) prior to the unauthorized manipulation of controls on December 23, 2015 through a spearphishing attachment technique targeting three Ukrainian power distribution companies.[7] By understanding the nature and possible origins of this attack, as well as how the adversary used the Remote Services 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 T886 Recipe outlines general guidance to help AOOs confirm suspicion of the use of Remote Services 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 opportunities for remote services to be used in malicious attacks 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; properly segmenting networks to establish functional boundaries that can be properly monitored and have block actions implemented; establishing a strong password policy to prevent attackers from abusing weak credentials to compromise accounts; requiring frequent password changes to reduce the validity of harvested credentials; leveraging strong authentication methods for both users and devices/processes/API calls; and auditing accounts to validate permissions levels and to review access logs to provide a host-based baseline for monitoring.

[6] https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108

[7] CyOTE Case Study: Ukraine 2015. Contact CyOTE.Program@hq.doe.gov for more information.

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

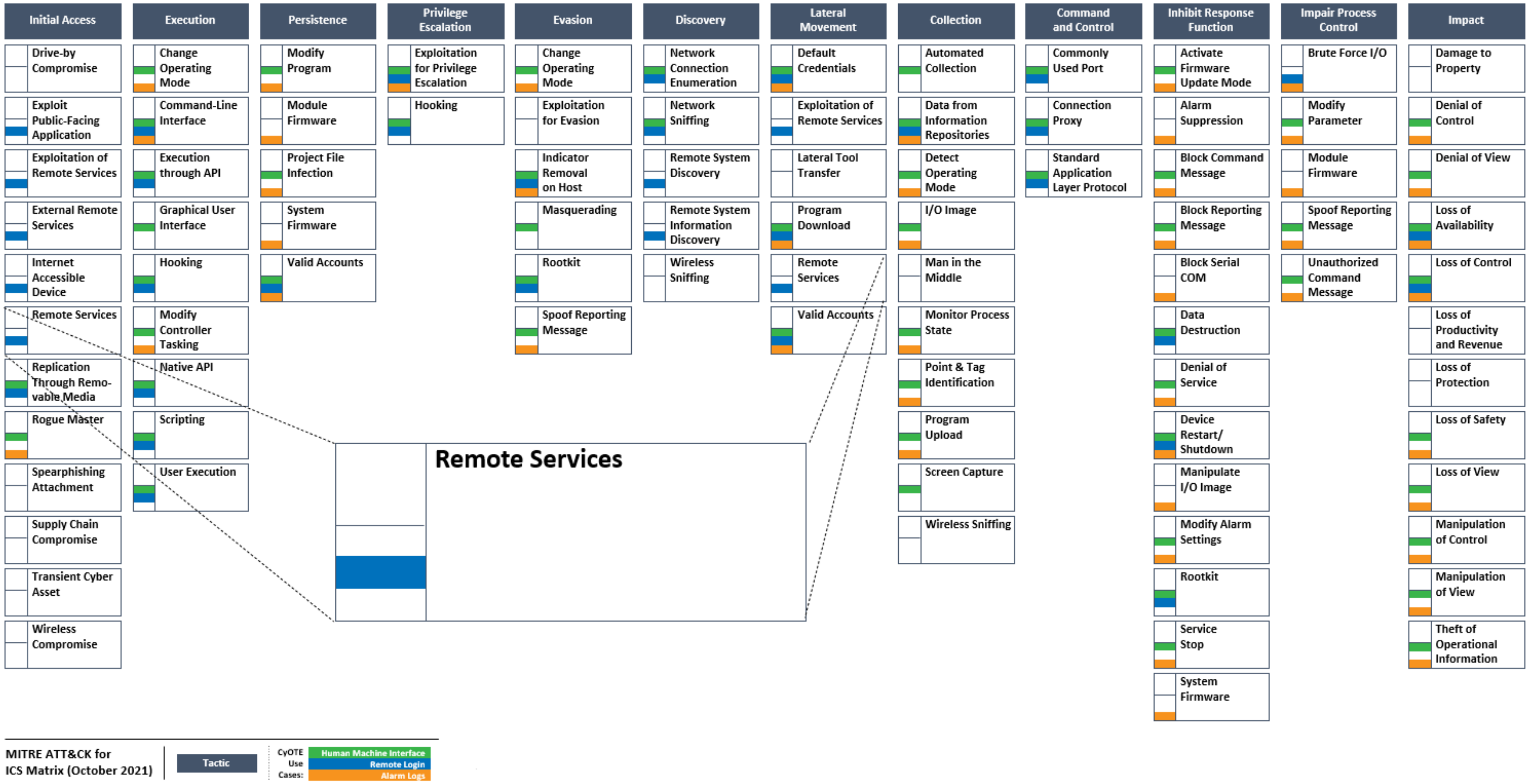
ASSET OWNER DEPLOYMENT GUIDANCE

To deploy this capability, the CyOTE T886 Recipe recommends to identify logging data required to perform alerting, 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 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



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by 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
Exploit Public-Facing Application	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
Exploitation of Remote Services	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
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

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

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