MITRE ATT&CK FOR ICS - TENABLE'S TAKE

INTRODUCTION

Guides and frameworks published by leading global security bodies play an important role in engaging the cyber security community in professional debate and in helping security professionals prioritize tasks in a systematic manner, so they can track their progress and assess security gaps. In the area of ICS security this includes the **NIST framework**, **NERC-CIP standards** and many other industry specific standards.

The variety of standards reflect different approaches and enables security professionals to choose which standard emphasizes best what they consider to be most critical in cyber security. While some frameworks focus on increasing network hygiene to mitigate the chances and impact of a cyber attack, others may focus on threat detection or quick recovery.

Recently, the **MITRE Corporation** published ATT&CK® for ICS, which is "a knowledge base useful for describing the actions an adversary may take while operating within an ICS network". It is a recent addition to the already established ATT&CK® framework originally published for general purpose networks.

FRAMEWORK DIFFERENCES

MITRE advises that the differences between the two frameworks are:

- *ATT&CK for ICS focuses on adversaries who have a primary goal of disrupting an industrial control process, destroying property or c[1]ausing temporary or permanent harm or death to humans by attacking industrial control systems.*

- *ICS operations require continuous work as a stated target of adversaries in the ICS world.*

- *ICS networks are very heterogeneous environments. There are many software/hardware platforms, applications and protocols present in these environments.*

Typical devices and architectures in ICS environments are considerably different from those of IT networks, thus requiring an ICS specific variant.

EVALUATING MITRE ATT&CK FOR ICS

Tenable encourages the ICS security community to review this knowledge base and become familiar with the attack methods. This is the first step to stimulating the process of taking protective measures to address OT threats.

At the same time, it is important to note that the guide states its goal is "to better characterize and describe post-compromise adversary behavior". Tenable posits that a blanket statement of evaluating the entire security posture of an organization based on compromises can miss important threats. Furthermore, professionals that only consider security solutions and practices to systematically address specific threats or compromise techniques and only them will likely miss more effective and available security measures that can reduce the attack surface in the first place. This would comprehensively eliminate weak spots and reduce risk as a continuous "peace time" process.

ANALYSIS OF TENABLE.OT CAPABILITIES

ATT&CK for ICS comprises eleven tactics which include 81 different techniques. Below is a summary of the Tenable's capabilities to detect the use of specific techniques as noted.

[1] https://collaborate.mitre.org/attackics/index.php/Overview

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

Teal — Fully Supported | Blue — Supported Through Integration

Tenable.ot provides defensive measures that effectively address attack tactics.

Examples include:

1. Policy Based Threat Detection: By applying the right policies, either the out-of-the-box or customized, Tenable.ot alerts on unauthorized or anomalous behavior that may appear in most of the tactics, including: **Initial access, Lateral Movement, Command & Control, Impair Process Control.**

2. Deep Situational Awareness: Tenable.ot's deep visibility into OT protocols and ability to query in their native protocols identifies changes in configuration and logic of the industrial process. This is typical when executing ICS attacks and include techniques such as: **Execution, Persistence, Evasion.**

3. Anomaly Detection: Tenable.ot's network baseline and reconnaissance activity detection secures from tactics including **Execution, Discovery, Collection, Command and Control.**

4. Active Querying: Tenable.ot patented and proven active querying technology exposes many attack flow aspects including: **Initial access, Evasion, Inhibit Response Function.**

The **Impact** tactic is a highlighted example of the difference in perspectives:

- For the **attacker,** impact defines the goals
- For the **defender,** impact doesn't provide detail into measures taken to address other tactics

OTHER CONSIDERATIONS

It is important to understand the tactics and techniques which are outlined in MITRE's ATT&CK for ICS knowledge base. Tenable advises ICS security professionals to further add the following considerations to your ICS security strategy:

1. Ensure that vulnerabilities are identified and mitigated as part of a continuous process, unrelated to any specific attack. Solutions should include identification of relevant vulnerabilities in the OT environment with as few false positives as possible.

2. The strategy should be risk driven and solutions should address the organization's specific situation that include what is identified as weak aspects of the security posture.

3. The strategy should emphasize the importance of asset management as the basis of vulnerability management and incident response. This will be key to mitigate the impact of materialized attacks.

4. Because attackers use several techniques that may change PLC programming as part of their attack, configuration control of controllers is critical in order to identify deviations from the operational set up.

SUMMARY

MITRE's ATT&CK for ICS is an important framework for the entire ICS security community to map and analyze different techniques used by adversaries. While tenable.ot covers many security aspects to detect these techniques, it is important to understand that the security task is wider than defensively countering these techniques as they arise, and should be considered accordingly.

For More Information: Please visit **tenable.com**
Contact Us: Please email us at **sales@tenable.com** or visit **tenable.com/contact**