TRAPX
SECURITY

WHITE PAPER

Simplifying MITRE ATT&CK Adoption with DECEPTION TECHNOLOGY

The MITRE ATT&CK™ framework is a comprehensive matrix of tactics and techniques used by defenders to better classify attacks and assess an organization’s risk. The goal of the framework is to improve detection of adversaries by illustrating the actions an attacker may have taken. *(How did the attacker get in? How are they moving within the network?)*

The knowledge base of tactics, techniques and sub-techniques is designed to help answer those questions while contributing to the overall awareness of an organization’s security posture. Organizations can then use the framework to identify gaps, and prioritize remediation based on risk.

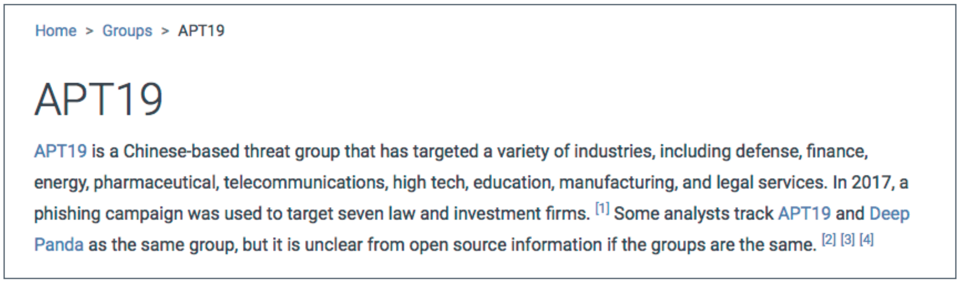
The MITRE ATT&CK framework has gained increasing prominence as a tool for planning, building, and testing the ability of security teams. The layout of ATT&CK Matrices makes this possible, but challenges persist.

Keys to Success: Focus on Relevant Techniques

The greatest challenge with adopting MITRE ATT&CK is finding a way to practically apply the overwhelming amount of information contained within the framework. To help ease the burden of adoption and integration, MITRE has released extensive documentation as well as a handbook with suggested strategies. One of the key recommendations included in the guide is limiting adoption to techniques specific to the organization’s industry and environment. Typically this requires researching several threat reports of the previous year’s attacks. Threat groups are then laid out according to the industries they target as seen in the figure below. This exercise may deliver a subset of more relevant techniques, however, insight to assist in actually prioritizing this subset of tactics may still be lacking.

EXAMPLE: **ONE TECHNIQUE USED BY APT19 IS REGISTRY RUN KEYS/STARTUP FOLDER**

SEARCH FOR “PHARMACEUTICAL”



Home > Groups > APT19

APT19

APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. [1] Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same. [2] [3] [4]

DESCRIPTION OF APT19 GROUP

From there, you can bring up that group’s page to look at the techniques they’ve used (based solely on open source reporting we’ve mapped) so you can learn more about them. If you need more info on the technique because you’re not familiar with it, no problem—it’s right there on the ATT&CK website. You could repeat this for each of the software samples that we’ve mapped the group using, which we track separately on the ATT&CK website.

Visibility Through Deception

Deception technology immerses real IT assets in a "mirror maze" of fake applications, databases, domain controllers, routers, printers, etc. that are invisible to legitimate users and applications but completely authentic to an attacker. This is a highly effective form of defense that makes the attackers path to lateral movement treacherous, time-consuming and risky. (For more information on deception as a strategy, click here.)

Deception takes a fundamentally different approach to cybersecurity, and offers unique benefits for those looking for insight to support ATT&CK prioritization. Unlike other security controls, deception draws the attacker in. The moment an attacker interacts with a trap, they reveal themselves and their tactics, techniques, and procedures.

1

ACTIVE INTERNAL TECHNIQUES

In short, TrapX reveals techniques that are actively used in the network today. For those in search of effective ways to prioritize MITRE ATT&CK adoption, TrapX, together with MITRE provides clear, risk-based criteria for Priority 1 remediation.

2

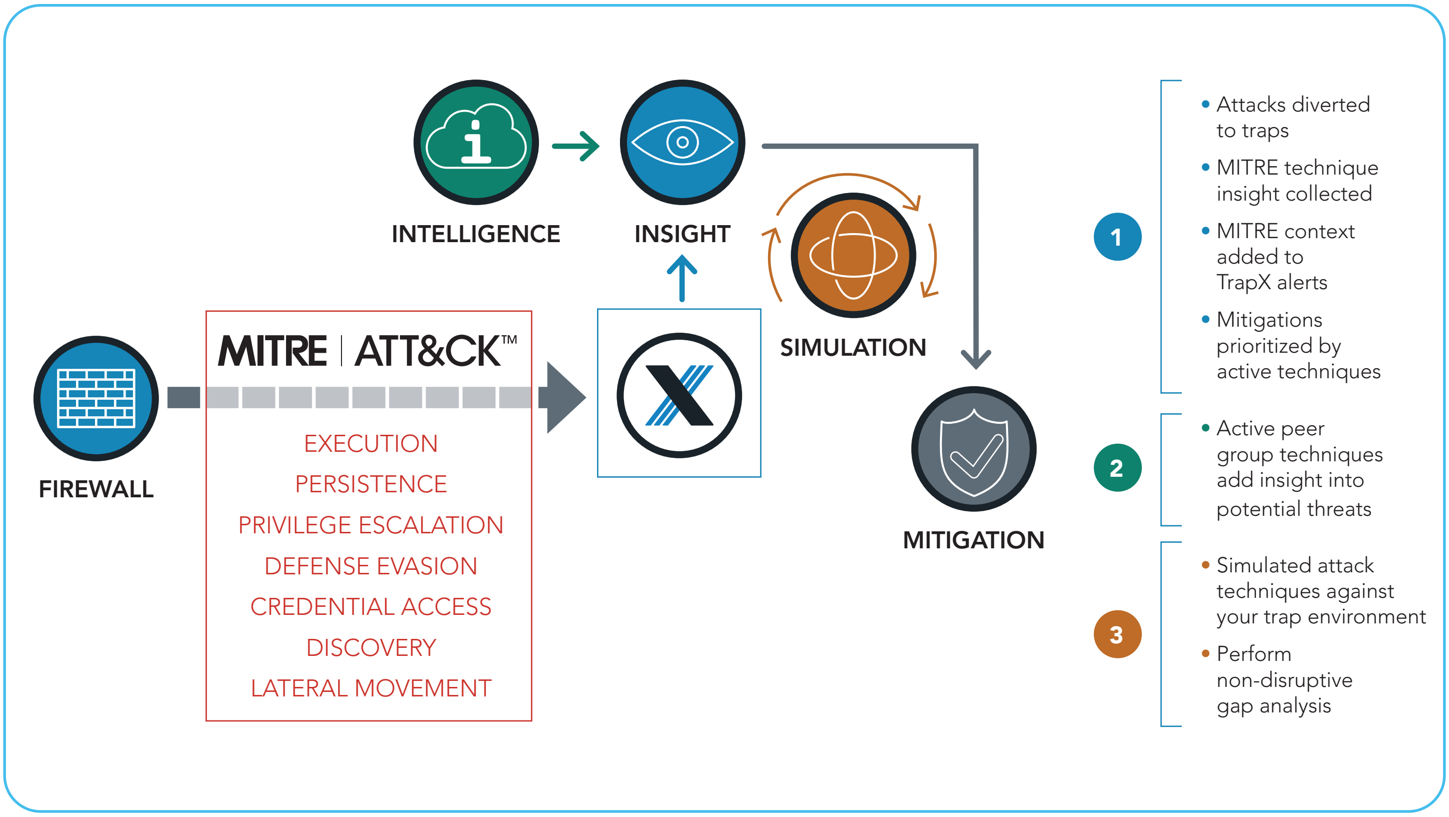
ACTIVE COHORT TECHNIQUES

Once the most immediate risk has been addressed, the scope can be broadened to include vulnerability to anticipated attacks. MITRE ATT&CK provides tools to search and analyze attacks within specific industries. TrapX complements this resource with peer insights, a dynamic anonymized feed of data into active techniques within TrapX customer cohorts. This unique capability enables the SOC to proactively adjust their deception strategy as the attack landscape changes.

3

NON-DISRUPTIVE TESTING

TrapX runs in a shadow network that is invisible to legitimate users and systems, therefore it generates virtually no false positives when properly configured. In addition, TrapX traps do not touch endpoints so simulated attacks can be run against emulated traps in this environment without disrupting security operations.


INTELLIGENCE
INSIGHT
SIMULATION
MITIGATION
FIREWALL
MITRE | ATT&CK™
EXECUTION
PERSISTENCE
PRIVILEGE ESCALATION
DEFENSE EVASION
CREDENTIAL ACCESS
DISCOVERY
LATERAL MOVEMENT
1
- Attacks diverted to traps
- MITRE technique insight collected
- MITRE context added to TrapX alerts
- Mitigations prioritized by active techniques
2
- Active peer group techniques add insight into potential threats
3
- Simulated attack techniques against your trap environment
- Perform non-disruptive gap analysis

MITRE and IoT

An important first step in employing threat data is ensuring visibility and proper logging of attacks. But organizations like John Muir Health need visibility from critical IoT devices; however this is not always feasible since the FDA governs medical devices, and logging agents cannot be deployed. The solution for John Muir Health was to implement smart, deceptive traps provided by TrapX. These traps mirrored the activity of medical devices, drawing attackers towards a device that did provide proper logging of techniques. The deception technology gave this organization a better source of threat intelligence because it was not generalized for their industry, but specific to the adversaries in their unique environment. This immediately led to remediation steps that stopped these attacks and provided the security team with a clear view of challenges to come.

Mapping to MITRE

TrapX DeceptionGrid™ alerts provide powerful criteria for ATT&CK prioritization with alerts that provide telemetry that maps attacks to the MITRE Framework. Using a tool called the ATT&CK Navigator, the information collected by DeceptionGrid can be mapped to the exact ATT&CK technique and tactics required to understand the actions an adversary will take.

The TrapX report entitled, "Anatomy of an Attack: Medical Device Highjack (Medjack)," provides an exact play-by-play of the tools used by adversaries during an attack against a hospital's infrastructure. The report is a combination of a fully simulated environment and anonymized case studies. Using the detailed alerts from DeceptionGrid, the tools recorded can be matched with their given techniques. Creating a layer on ATT&CK Navigator then makes it possible to create an intuitive graphic that can be shared amongst teams. The figure on page 6 is an example of such a mapping based on the Medjack report series.

The importance of being able to highlight the exact techniques used in a confirmed attack are monumental. It can be easy for security teams to become overwhelmed with the number of techniques covered by ATT&CK, but creating these specific mappings provides a much smaller set of potential threats that can streamline prioritization and reduce adoption complexity. The mapping process is quite simple using the detailed information gathered by DeceptionGrid. Examples from the Medjack report include DLL injection, lateral movement using SMB, and creating hidden processes. With these logs, it becomes possible to highlight each of these boxes on the ATT&CK Navigator. After this has been done, the layer can be rendered to SVG (Scaled Vector Graphic) for inclusion in reports. Multiple layers can even be created to break down mappings in any way the security team might desire.

FIGURE 1A: **TRAPX COVERAGE OF THE MITRE ATT&CK ENTERPRISE FRAMEWORK**

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
11 Items	34 Items	62 Items	32 Items	69 Items	21 Items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force
Hardware Additions	Complied HTML File	AppCert DLLs	AppInit DLLS	Bypass User Account Control	Credential Dumping
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credentials Access
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Promot	Compiled HTML files	Forced Authentication
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking
Valid Accounts	Graphical User Interface	Change Default File Association	Exploration for Privilege Escalation	Component Object Model Hijacking	Input Capture
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification	
	Service Execution	Image File Execution Options Injection	Process Injection	File Deletion	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets	
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass	
	Source	Launch Daemon	Setuid and Setgid	Group Policy Modification	
	Space after Filename	Launchctl	SID-History Injection	Hidden Files and Directories	
	Third-party Software	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users	
	Trap	Local Job Scheduling	Sudo	Hidden Windows	
	Trusted Developer Utilities	Login Item	Sudo Caching	HISTCONTROL	
	User Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection	
	Windows Management Instrumentation	LSASS Driver	Web Shell	Indicator Blocking	
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools	
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host	
		New Service		Indirect Command Execution	
		Office Application Startup		Install Root Certificate	
		Path Interception		InstallUtil	
		Plist Modification		Launchctl	
		Port Knocking		LC_MAIN Hijacking	
		Port Monitors		Masquerading	
		PowerShell Profile		Modify Registry	
		Rc.common		Mshta	
		Re-opened Applications		Network Share Connection Removal	
		Redundant Access		NTFS File Attributes	
		Registry Run Keys /Startup Folder		Obfuscated Files or Information	
		Scheduled Task		Parent PID Spoofing	
		Screensaver		Plist Modification	
		Security Support Provider		Port Knocking	
		Server Software Component		Process Doppelgänging	
		Service Registry Permissions Weakness		Process Hollowing	
		Setuid and Setgid		Process Injection	
		Shortcut Modification		Redundant Access	
		SIP and Trust Provider Hijacking		Regsvcs/Regasm	
		Startup Items		Regsvr32	
		System Firmware		Rootkit	
		Systemd Service		Rundll32	
		Time Providers		Scripting	
		Trap		Signed Binary Proxy Execution	
		Valid Accounts		Signed Script Proxy Execution	
		Web Shell		SIP and Trust Provider Hijacking	
		Windows Management Instrumentation Event Subscription		Software Packing	
		Winlogon helper DLL		Space after Filename	
				Template Injection	
				Timestomp	
				Trusted Developer Utilities	
				Valid Accounts	
				Virtualization/Sandbox Evasion	
				Web Services	
				XSL Scrip Processing	

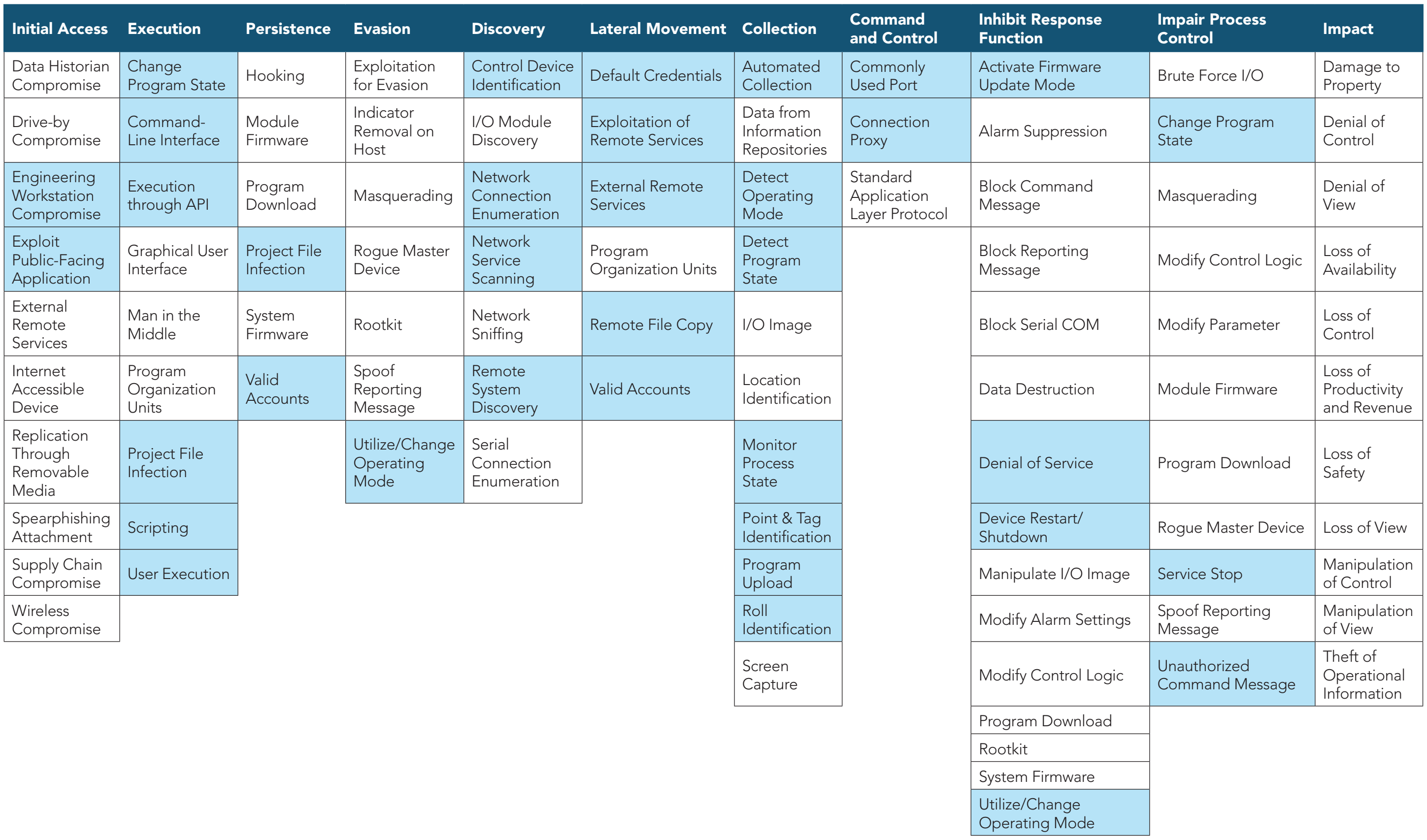
FIGURE 1B: **TRAPX COVERAGE OF THE MITRE ATT&CK ENTERPRISE FRAMEWORK**

Discovery	Lateral Movement	**Collection**	**Command and Control**	**Exfiltration**	**Impact**
23 Items	18 Items	13 Items	22 Items	9 Items	16 Items
Account Discovery	Applescript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
File and Directory Discovery	Internal Spearfishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Peripheral Device Discovery	Remote File Copy	Input Capture	Failback Channels		Network Denial of Service
Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
System Information Discovery	Windows Admin Shares		Remote File Copy		
System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
System Network Connections Discovery			Standard Cryptographic Protocol		
System Owner/User Discovery			Standalone Non-Application Layer Protocol		
System Service Discovery			Uncommonly Used Port		
System Time Discovery			Web Service		
Virtualization/Sandbox Evasion					

MITRE & Industrial Control Systems

MITRE ATT&CK has recently highlighted the dangers found in Industrial Control Systems (ICS) as a severe risk environment that warrants its own matrix of techniques. TrapX has always focused on the specific problems associated with securing an ICS environment by overcoming the lack of logging visibility using deception. The TrapX threat intel paper, "Anatomy of Attack: Industrial Control Center Under Siege," gives a detailed case study of the techniques used by adversaries when attacking manufacturing plants. DeceptionGrid provided detailed logs of the attacks made against traps that can then be mapped on the ATT&CK Navigator as demonstrated in the figure below. In this particular attack, initial access was achieved by an outside USB device unknowingly introducing malware into a control system. Discovery methods including network scanning for specific services was used, followed by the execution of the malware using the command line interface. The ability to map the techniques used by adversaries during an attack significantly lowers the risk faced by corporate assets. Without DeceptionGrid the intel that made this mapping possible would not have been available.

FIGURE 2: **TRAPX COVERAGE OF THE MITRE ATT&CK FOR INDUSTRIAL CONTROL SYSTEMS**



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						Roll 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		

Conclusion

The MITRE ATT&CK Framework is an important and powerful resource. However, with a growing list of more than 260 techniques, it is becoming more challenging to synthesize the framework into a strategic plan. TrapX DeceptionGrid draws attacks toward traps and away from critical assets such as IoT and ICS systems. In doing so, TrapX enables MITRE to integrate into these environments while providing new protection and new insight into attacker tradecraft that is mapped back to the ATT&CK Framework. This powerful combination eliminates blind spots, while simplifying and prioritizing ATT&CK adoption.

To learn more about TrapX and how Deception technology can accelerate and simplify adoption of the MITRE ATT&CK Framework, visit our web site or schedule a call with a solution specialist today.

TrapX Security, Inc.
303 Wyman Street
Suite 300
Waltham, MA 02451

+1–855–249–4453
www.trapx.com

sales@trapx.com
partners@trapx.com
support@trapx.com

About TrapX Security

TrapX has created a new generation of deception technology that provides real-time breach detection and prevention. Our proven solution immerses real IT assets in a virtual minefield of traps that misinform and misdirect would-be attackers, alerting you to any malicious activity with actionable intelligence immediately. Our solutions enable our customers to rapidly isolate, fingerprint and disable new zero day attacks and APTs in real-time. TrapX Security has thousands of government and Global 2000 users around the world, servicing customers in defense, health care, finance, energy, consumer products and other key industries.