l agree.

To make Medium work, we log user data and share it with processors. To use Medium, you must agree to our <u>Privacy Policy</u>, including cookie policy.



Sep 20, 2018 · 5 min read

This post was originally published May 3, 2018 on mitre.org.

ATT&CK

Why ATT&CK was Created

ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge. MITRE started this project in 2013 to document common tactics, techniques, and procedures (TTPs) that advanced persistent threats use against Windows enterprise networks. ATT&CK was created out of a need to document adversary behaviors for use within a MITRE research project called FMX. FMX's objective was to investigate use of endpoint telemetry data and analytics to improve post-compromise detection of adversaries operating within enterprise networks. Much of that work is documented here: <u>Finding Threats with ATT&CK-based</u> <u>Analytics</u> and the <u>Cyber Analytics Repository</u>.

Based on our research, we decided we needed a framework to address four main issues:

- 1. Adversary behaviors. Focusing on adversary tactics and techniques allowed us to develop analytics to detect possible adversary behaviors. Typical indicators such as domains, IP addresses, file hashes, registry keys, etc. were easily changed by adversaries and were only useful for point in time detection—they didn't represent how adversaries interact with systems, only that they likely interacted at some time.
- 2. Lifecycle models that didn't fit. Existing adversary lifecycle and Cyber Kill Chain concepts were too high-level to relate behaviors to defenses—the level of abstraction wasn't useful to map TTPs to new types of sensors.
- 3. Applicability to real environments. TTPs need to be based on observed incidents to show the work is applicable to real environments.
- 4. Common taxonomy. TTPs need to be comparable across different types of adversary groups using the same terminology.

We strongly believe that offense is the best driver for defense. An organization's ability to detect and stop an intrusion improves greatly by maintaining strong offense and defense teams that work together. Within FMX, ATT&CK was the framework used to build adversary emulation scenarios. The emulation team used these scenarios to inject real-world inspired activity into the network. Then the team used the tests to verify that the sensors and analytics were working to detect adversarial behavior within a production network. The approach resulted in a rapid improvement in detection capability, and, most importantly, in a measured and repeatable way.

ATT&CK became the go-to tool both for the adversary emulation team to plan events and for the detection team to verify their progress. This was such a useful process for MITRE's research program that we felt it should be released to benefit the entire community, so MITRE released ATT&CK to the public in May 2015. ATT&CK has since expanded significantly to incorporate techniques used against macOS and Linux, behaviors used by adversaries against mobile devices, and adversary strategies for planning and conducting operations pre-exploit.

What is ATT&CK?

ATT&CK is largely a knowledge base of adversarial techniques—a breakdown and classification of offensively oriented actions that can be used against particular platforms, such as Windows. Unlike prior work in this area, the focus isn't on the tools and malware that adversaries use but on how they interact with systems during an operation.

ATT&CK organizes these techniques into a set of tactics to help explain to provide context for the technique. Each technique includes information that's relevant to both a red team or penetration tester for understanding the nature of how a technique works and also to a defender for understanding the context surrounding events or artifacts generated by a technique in use.

Tactics represent the "why" of an ATT&CK technique. The tactic is the adversary's tactical objective for performing an action. Tactics serve as useful contextual categories for individual techniques and cover standard, higher-level notations for things adversaries do during an operation, such as persist, discover information, move laterally, execute files, and exfiltrate data.

Techniques represent "how" an adversary achieves a tactical objective by performing an action. For example, an adversary may dump credentials to gain access to useful credentials within a network that can be used later for lateral movement. Techniques may also represent "what" an adversary gains by performing an action. This is a useful distinction for the Discovery tactic as the techniques highlight what type of information an adversary is after with a particular action. There may be many ways, or techniques, to achieve tactical objectives, so there are multiple techniques in each tactic category.

The ATT&CK Matrix[™]

The relationship between tactics and techniques can be visualized in the ATT&CK Matrix. For example, under the tactic <u>Persistence</u> (this is the adversary's goal—to persist in the target environment), there are a

series of techniques including <u>AppInit DLLs</u>, <u>New Service</u> and <u>Scheduled Task</u>. Each of these is a single technique that adversaries may use to achieve the goal of persistence.

Initial Access	Execution 31 items	Persistence 56 items	Privilege Escalation 28 items		Credential Access 20 items		Lateral Movement 17 items	Collection 13 items		Command And Control 21 Items
Exploit Public-Facing	CMSTP	Accessibility Features	Manipulation	Binary Padding	Bash History	Application Window	Application Deployment	Automated Collection	Data Compressed	Communication Through
Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Discovery	Software	Clipboard Data	Data Encrypted	Removable Media
Hardware Additions	Control Panel Items	Appinit DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Data from Information	Data Transfer Size	Connection Praxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Bunnes Henry Account	Clear Command History	Credentials in Files	File and Directory	Exploitation of Remote Services System	Repositories	Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package		CMSTP	Credentials in Registry Discovery				Exfiltration Over Alternative Protocol Exfiltration Over	Custom Cryptographic
	Execution through Module	BITS Jobs		Code Signing	Exploitation for			Data from Network		Protocol
Spearphishing Link	Load	Bootkit	DLL Search Order	Component Firmware	Credential Access		Pass the Hash	Shared Drive	Command and Control	Data Encoding
Spearphishing via	Exploitation for Client Execution	Browser Extensions	Hjacking	Component Object Model	Forced Authentication	Network Share Discovery	Pass the Ticket	Data from Removable	Channel	Data Obfuscation
Service Supply Chain Compromise		Change Default File	Dylib Hjacking	Hijacking	Hooking	Password Policy	Remote Desktop Protocol	Media Data Staged	Exfiltration Over Other Network Medium	Domain Fronting
	Installuti	Association	Exploitation for Privilege Escalation	Control Panel Items	Input Capture	Discovery			Exfiltration Over Physical Medium	Fallback Channels
Trusted Relationship	Launcheti	Component Firmware		DCShadow	Input Prompt	Peripheral Device	Remote File Copy	Email Collection		Multi-hop Proxy
Valid Accounts	Launchoti Local Job Scheduling	Component Object Model Hijacking	Extra Window Memory Injection File System	Deobfuscate/Decode Files or Information	Kerberoasting	Permission Groups	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver				Keychain		Replication Through Removable Media	Man in the Browser		Multiband Communication
	LSASS Driver Mishta	Create Account DLL Search Order	Permissions Weakness	Disabling Security Tools DLL Search Order Hilacking	LLMNR/NBT-NS	MNR/NBT-NS Process Discovery isoning Query Registry etwork Sniffing Query Registry Remote System Discovery	Shared Webroot	Screen Capture Video Capture		Multilayer Encryption
		Hijacking	Hooking		-		SSH Hiacking			Port Knocking
	PowerShell	Dylib Hijacking	Image File Execution	DLL Side-Loading			Taint Shared Content			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Options Injection	Exploitation for Defense Evasion			Third-party Software Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions	Launch Daemon New Service	Extra Window Memory Injection	Private Keys Security Software Replication Through Removable Media System Information Securityd Memory Discovery	Discovery				Standard Application Layer Protocol
	Rundli32	Weakness		File Deletion						
	Scheduled Task	Hidden Files and	Path Interception	File System Logical Offsets		Windows Remote Management			Standard Cryptographic Protocol	
	Scripting	Directories	Plist Modification	Gatekeeper Bypass	Two-Factor Authentication Interception	System Network Configuration Discovery				Protocol Standard Non-Application Lawer Protocol
	Service Execution	Hooking	Port Monitors	Hidden Files and Directories Hidden Users						
	Signed Binary Proxy Execution	Hypervisor	Process Injection			System Network				Uncommonly Lised Port
	Signed Script Proxy	Image File Execution Options Injection	Scheduled Task	Hidden Window		Connections Discovery				Web Service
	Execution		Service Registry	HISTCONTROL		System Owner/User Discovery				
	Source		Permissions Weakness Setuid and Setgid	Image File Execution Options Injection		System Service Discovery				
	Space after Filename	Launch Agent		rector						

The ATT&CK Matrix is probably the most widely recognizable aspect of ATT&CK because it's commonly used to show things like defensive coverage of an environment, detection capabilities in security products, and results of an incident or red team engagement.

Cyber Threat Intelligence

Another important aspect of ATT&CK is how it integrates cyber threat intelligence (CTI). Unlike previous ways of digesting CTI that were used primarily for indicators, ATT&CK documents adversary group behavior profiles, such as <u>APT29</u>, based on publicly available reporting to show which groups use what techniques.

Usually, individual reports are used to document one particular incident or group, but this makes it difficult to compare what happened across incidents or groups and come to a conclusion on what types of defenses were most effective. With ATT&CK, analysts can look across groups of activity by focusing on the technique itself. When deciding how to focus defensive resources, analysts might want to start with techniques that have the highest group usage.

Examples of how particular adversaries use techniques are documented in its ATT&CK page, which represents that group's procedure for using the technique. The procedure is a particular instance of use and can be very useful for understanding exactly how the technique is used and for replication of an incident with adversary emulation and for specifics on how to detect that instance in use.

Where ATT&CK is Today

ATT&CK has expanded quite significantly over the past five years, from Windows to other platforms and technologies. It's in use by many different government organizations and industry sectors, including financial, healthcare, retail, and technology. The public adoption and use has led to significant contributions back to ATT&CK to keep it upto-date and useful for the community. We want to continue this trend, so <u>MITRE has big plans</u> to keep growing ATT&CK to ensure its future as a valuable public resource.

Continuing This Series

Now that we've covered some of the basics, you can look forward to future blog posts that go into more detail on topics covered within this post. We'll discuss the use of ATT&CK with cyber threat intelligence, behavior-based detection analytics, and adversary emulation, as well as additional areas.