ATT&CK 101

Blake Strom Follow
Sep 20, 2018 · 5 min read

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

Why ATT&CK was Created

MITRE started ATT&CK 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: Finding Threats with ATT&CK-bas

Based on our research, we decided we n

1. Adversary behaviors. Focusing on ac develop analytics to detect possible a domains, IP addresses, file hashes, r 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 a
classification of offensively oriented acti
platforms, such as Windows. Unlike pric
and malware that adversaries use but or
operation.

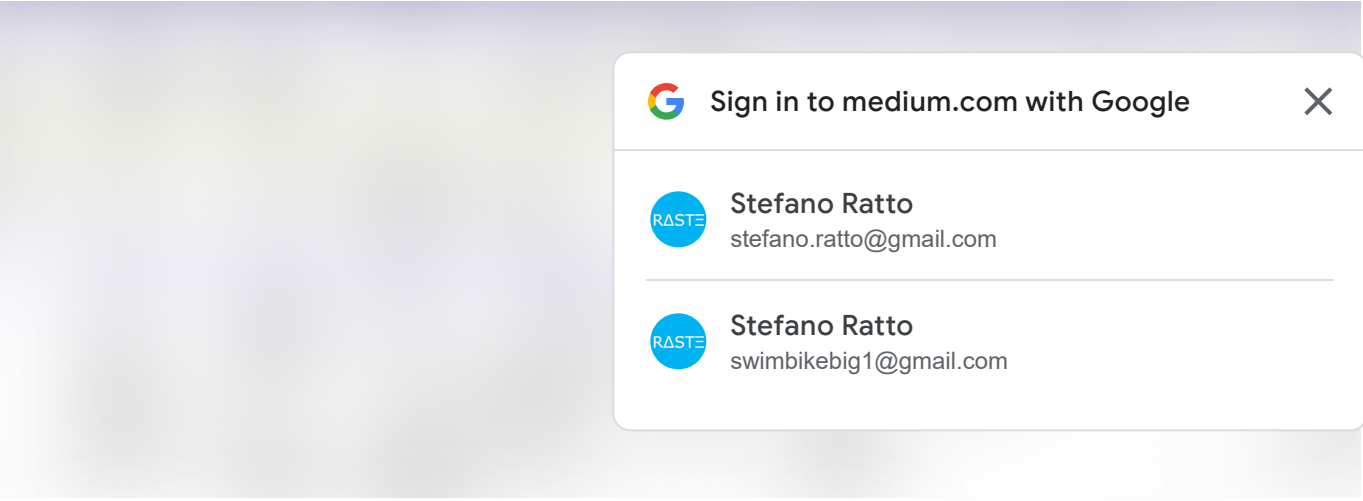
ATT&CK organizes these techniques into
context for the technique. Each technique includes information that's relevant to both a red team or penetration tester for understanding the nature of how a technique works and also to a defender for understanding the context surrounding events or artifacts generated 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 Persistence (this is the adversary's goal — to persist in the target environment), there are a series of techniques including AppInit DLLs, New Serviceand Scheduled Task. Each of these is a single technique that adversaries may use to achieve the goal of persistence.



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 APT29, 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
organizations and industry sectors, inclu
technology. The public adoption and use
ATT&CK to keep it up-to-date and usefu
trend, so MITRE has big plans to keep gr
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.

Cybersecurity Mitre Attack Information Security Threat Hunting Threat Intelligence