MITRE ATT&CK®: What Is It?

The MITRE ATT&CK database contains detailed information about the dangerous behaviors advanced persistent threat (APT) groups have utilized at various points in actual hacks. Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) provides in-depth accounts of known techniques, methods, and processes used by adversarial parties to accomplish their technological goals.

Which Organizations Rely on MITRE ATT&CK, and Why

Because it's available for no cost, ATT&CK has been widely embraced by businesses and government agencies of all sizes and across many different sectors. Any internal teams concerned with constructing secure systems, applications, and services are users. These groups include security defenders, penetration testers, red teams, and cyberthreat intelligence teams. Thanks to the abundance of information it includes on attacks (and attackers), it can help businesses assess whether they are gathering sufficient information to detect assaults and measure the efficacy of their present defenses. (Walkowski, 2021)

Strategic Words for Attack

Since these terms might have various meanings in other settings, it is crucial to first understand how MITRE ATT&CK defines tactics, techniques, and procedures before delving into the matrix.

The "what" of an attack, in technical terms, is described by the tactic, which may be, for example, acquiring Initial Access, sustaining Persistence, or establishing Command and Control. Attempts at attack almost always necessitate the adoption of more than one strategy.

Attackers' techniques detail the "how" they execute a tactic. Each tactic in the two matrices has corresponding methods, and in the Enterprise matrix, some techniques are further subdivided. Attack methods such as Phishing, used to get Initial Access, are an illustration of this (a tactic). Spearphishing Attachment, Spearphishing Link, and Spearphishing via [a] Service are the three linked sub-techniques of phishing. (Walkowski, 2021)

Procedures: Describes the exact malware or other tools that APTs have used to accomplish certain tactics and sub-techniques (often in creative or new ways).

Analyzing Information using ATT&CK Navigator

ATT&CK Navigator simplifies the process of analyzing threats, assessing defenses, designing attack simulations, and comparing the various factors that ATT&CK monitors, all of which would otherwise require a spreadsheet or other tool. Both the Dridex and ZeusPanda banking trojans' techniques are shown in Figure 17 on separate tabs. Both can be compared side-by-side in the current tab. Dridex-specific methods are shown in yellow, ZeusPanda-specific methods in red, and common methods in green. (Walkowski, 2021)

Conclusion

MITRE ATT&CK is a database that collects, organizes, and cross-references information about real-world adversary groups, including their known behavior, the tactics, techniques, and procedures they employ, specific instances of their activities, and the software and tools (both legitimate and malicious) they use to aid in their attacks. Since it was designed from the standpoint of an attacker, MTRE ATT&CK is one of a kind among threat modeling and cyberattack lifecycle models. This makes it a one-of-a-kind tool for shedding light on how cybercriminals operate, which in turn helps companies fine-tune their own security measures. (Walkowski, 2021)

References:

(Walkowski, 2021) https://www.f5.com/labs/learning-center/mitre-attack-what-it-is-how-it-works-who-uses-it-and-why