Journal: Consider the Motive for Attack

Nathaniel Madore

Considering the motives for adversaries could help determine what types of attacks to watch out for. This is helpful to develop a layered defense approach to stop these common adversaries from achieving maximum damage. By knowing the motivations behind the attack, the organization can establish a better footing for dealing with those attacks. This could even be preventatively changing aspects of the business to avoid being a juicy target for these threat actors. Although this does not resolve the problem of being a target for any number of reasons these threat actors might be motivated from. It does help to understand whether they are motivated by money, recognition or political reasons. The meaning behind these motivations can affect the incident response teams plan for dealing with the crisis.

The best way to explain this to a new developer is to think with the mindset of the attacker. From our point of view a systemic approach to dealing with an adversary only will reveal data that provides a less complete set of information that can enhance the analysis. Hence the need to understand the adversarial mindset. New developers should try to understand the attack from the point of view of the attacker. This helps provide more complete information about the incident including the why behind the attack. By explaining the connection between the bigger picture and the event. A new developer can understand why it is important that they practice their adversarial mindset in order to obtain a higher level of detail within a computer forensic analysis.

One concept that can be included in the final reflection is not to leave security to the end. By explaining the adversarial mindset to new developers, we can adopt security practices into the development of a system from the start. This will help challenge the team to provide solutions that have not been encountered yet in the real world. Like for example thinking of security measures that reduce the impact of threat actors in the seven categories most commonly found in a real time operating environment. Using this as a part of the reflection will help explain how best practices implemented early on will improve the applications security posture in the end.