FOUR TIERS OF ATTACKS

GLANC, LTD.

Adversary capability model

Realistic adversary model is essential in establishing effective cyber defense strategies. A typical adversary model for Security Operations Centers (SOC) and “threat hunting” is complex and multifaceted, making it unsuitable for other objectives like high-level risk assessment and proactive defense resource management. To resolve this issue, we have developed a straightforward model centered around a single factor: the level of adversarial capability. There are four tiers and their corresponding attacks.

A1: OPPORTUNISTIC ADVERSARY

A1 is an opportunistic adversary, it is main goal to do a wide sweep for easy prey and gain a quick advantage. It does not imply, contrary to typical misconception, that the attack is to be non-sophisticated; it means that the adversary capability is mostly limited by the availability of automation tools at hand. An example of A1 adversary would be a hacktivist, a script kiddie or a regular ransomware operator. To leverage the vulnerability, opportunistic attackers may use exploits, exploit packs and even write simple exploits when it does not require significant effort.

A2: TARGETED HACKERS

A2 may carry out targeted attacks and have capabilities for some fine tailoring and limited persistence. Skilled hackers and advanced ransomware operators exemplify A2 adversaries. Their capabilities go beyond A1’s, creating custom exploits for known vulnerabilities when feasible, but their main difference is determination rather than skill.

A3: ORGANIZATIONAL ADVERSARY

A3 is organizational/persistent adversary. A3 type can allocate significant resources, manage and reuse it when deemed necessary, optimize the effort, and carry out attacks that require coordination among participants. Ransomware creators and most “regular” nation state actors, that do not qualify for A4, are A3. Thus, A3 actors are the primary source for “weaponized” exploits, attack tools and ransomware in thew black market, and they use it with impressive creativity. Zero day vulnerabilities start gaining some relevance on this level, but for A3 they are scarce and short-lived.

A4: APEX PREDATOR

A4 is an apex predator aiming for no less than strategic dominance in cyber , an entity that has capability to manage adversarial resources long-term not being restricted by demands of immediate profit. A4 are major nation state agencies and cyber weapon dealers on government contracts. Unlike A3, A4 attackers are typically limited not by adversarial capability, but rather by strategic justification to allocate appropriate resources to a given attack. Key characteristics include deniability (operations designed to look like lower-level adversaries’ actions unless there is a strategic advantage in open demonstration) and synergy (using advanced non-cyber means such as SIGINT, HUMINT, or kinetic to achieve targets).

Underestimating attackers and sticking to “best practices” not adherent to elevated requirements may have devastating effects. The success of StuxNet operation was guaranteed by the fact that the attackers were A4, and the defenders prepared for A2 at most. Overthinking the protection would make you run out of the budget, deprioritize important things and finally, to have a cyber security management program that does not work and never will. The vast majority of all attacks out there are A1, and a “regular” business most likely will never see a single A3 or higher attack in its lifetime; however, a government agency or a Fortune 1000 company is almost guaranteed to face the necessity to counter A3 or even A4.

+359878830030
arkenoi@glanc.ltd
facebook.com/glancltd
glanc.ltd

GLANC, LTD.