1 Attackers: Motivations and Patterns

1.1 The Attacks and the Attackers

Before talking about the attackers, let's talk about what they do: attacks. An attack means exploiting something to gain access to a system, usually sensitive data. These attacks can be active when attempting to alter system resources or passive which means not affecting any of the system resources. They can also be done from the inside (this is the most common case) if the attack is carried by someone inside the security perimeter or from the outside if it's carried by an unauthorized user [1]. Now that we know how an attack can be executed, an Attacker is the person who does this operation. An attacker may be an individual person or a group (sometimes working worldwide) and can be one of different types, such as [2]:

- Hacktivists, usually worldwide groups, who stand against what they don't agree with or believe in
- Script Kiddies, the less skilled. They normally use automated tools made by other attackers
- Phishermen, a specific type of Cybercriminals, who send infected emails to different users to steal their credentials
- Cyberterrorists, the most dangerous type of attackers, they target governments or companies that run critical infrastructures like hospitals or power grids

1.2 Common Motivations

The motivations, normally, are directly related to the types of attackers. For example, it is known that the motivations of script kiddies are almost always to have fun, that's why sometimes they are called joy hackers. On the other hand, the people who do phishing want financial gain or, in some cases, to steal intellectual property. Besides these motivations we can see many more, such as: espionage (stealing confidential information to gain advantage over some company or country - e.g. China and Russia installed malware to spy on Barack Obama before his election), sabotage (e.g. Russia influenced the U.S. elections), political (e.g. the group of hacktivists called Anonymous stands against several governments) or economical/competition (companies can target and steal ideas/products from one another).

1.3 Patterns

By analysing different attacks, we can find their most common patterns, i.e. understand what attackers most commonly do in their attacks and get advantage from that to develop our security. A study conducted in 2007, meant to profile the common attacker behaviours following the SSH compromises [3], shows that the most common sequence is to gain access, then download and run automated software. Therefore, we know what is the first thing to protect our system against to. Seeing the results of this or similar studies, we can find the most common credential attempts and make sure we don't use anything similar to those. Even though this study had great results, it was aimed only at low skilled hackers. The main difficulty on this topic is to discover patterns on the advanced ones. One possible solution to this problem is to hire high skilled hackers and analyse their common actions.

1.4 Conclusion

There are so many motivations (enormous amount of attack vectors), that all data in some system/company must be protected, mostly against the common attackers patterns. Although studying the motivations and the patterns of the attackers can help improving security, it is impossible to make a 100% secure system. There will always be different people that will do different than the common patterns already studied. Because of that, the defender needs to put himself in the attacker position, understand their possible motivations, and imagine all the different attacks that can be done against the company assets.

References

[1] ANTUNES, N. *Lecture 02 CSAM*. 2019.

[2] BLOG, S. *Types of Cyber Attackers and their Motivations*. 2015.

[3] CUKIER, D. R. R. B. M. *Profiling Attacker Behavior Following SSH Compromises*. 2007.