Advanced Persistent Threats | Andreia and Rodrigo

Intro

For today's presentation, we're going to discuss Advanced Persistent Threats (or APT's, for short). We'll be using CrowdStrike as our main source of information, since it is a trusting source in threat investigation.

(Slide: Objectives)

Our goal is to give more insight into this often misunderstood topic. As such, we'll be going over what an APT is, how to identify one, what common methods they use to attack their targets and how we can protect ourselves against such gigantic threats.

We will also be providing some examples of notable APT attacks and to finish off, we'll be taking a look at the top 10 adversaries of 2022, including what groups we should be aware of going into 2023 in specific countries, including Portugal.

(Slide: What is an Advanced Persistent Threat?)

An Advanced Persistent Threat is a sustained cyberattack in which the intruder hides inside the victim's network in order to steal sensitive data. These types of attacks tend to be targeted at high-value organizations (such as Fortune 500 companies and governmental agencies), and they are often performed by nation-state threat actors, composed of teams of the best cybercriminals in their particular countries.

(Slide: Goals)

You might be wondering: "What is the goal of these attacks?" - Well, there's a couple reasons why an APT attack might take place:

- Espionage, like spying on another country to find out state secrets
- Financial gain (This is quite common specifically for North Korean groups)
- Socio-political reasons, such as fighting against dictatorships and internet censorship
- Just plain destruction

(Slide: Stages)

Although there is a more intricate "Kill Chain", APT attacks usually consist of 3 stages:

1. Infiltration, where the attackers will try everything to get inside their target's network. This includes using multiple types of Social Engineering attacks, like phising through all possible methods of communication.

2. Escalation, in which the attacks spread malware through the network and use that as a queue to expand, as a use to map the network and attempt to gather important credentials - like Administrator privileges - along the way. At this stage, they usually install multiple backdoors. In other words, many ways to get back into the network to perform more operations.

3. And exfiltration, where the attacks actually take the data they have gathered and extract it, while trying to not get detected. It usually involves distracting the target's security team and systems with something else, like a DoS (Denial of Service) attack, or even a "fake backdoor" being suddently exposed.

(Slide: Chracteristics)

For system administrators and CISSO's (System Security Officers)`, there are ways to identify when an APT attack is (or has been) taking place. These include:

- Strange behaviour on certain accounts, such as late night activity
- The presence of multiple backdoors
- Unexpected data bundles (an indication that data has been amassed to be exfiltrated)
- Unusual network and database activity, like large amounts of data being searched

(Slide: Codenames)

Like we mentioned near the start of the presentation, APT's are usually sponsored nation-state actors. Funnily enough, CrowdStrike categorizes these threats by country and give them animal codenames. Here's some examples:

- China (Panda)
- India (Tiger)
- Iran (Kitten)
- North Korea (Chollima, a Pegasus-like creature in North Korean mythology)
- Pakistan (Leopard)
- Russia (Bear)
- Syria (Jackal)
- Vietnam (Buffalo)
- Worldwide/Unknown (Spider)

(Website time!)