What is APT1?

APT1 is believed to be a bureau of the People's Liberation Army that is responsible for cyberattacks in which they stole intellectual property from other nations. The victims that they targeted were involved in industries that China has identified as vital to its growth as a country. Stealing this information and intellectual property would take away any edge an adversary might have over them by evening the playing field.

What are the tactics, techniques, and procedures deployed by ATP1?

APT1 has stolen hundreds of terabytes of data from over a hundred organizations that we know of. They are not limited to attacking one target at a time and have demonstrated the ability to attack multiple at once. They have a specific attack methodology that they employ to steal data. These attacks have been found to include the following methods:

- **Credential Dumping**
- **Masquerading**
- **Pass the Hash**
- **Remote Desktop Protocol**
- **Email Collection**
- **Scripting**
- **Command Line Interface**
- **Data from Local System**
- **Data Compressed**

What would be the first thing you do when you are hired onto a company as a Hunt Analyst? Why did you choose this first thing?

On my first day with a company seeking to protect themselves from attacks by entities such as APT1 is to first identify if they are likely to be a target of attack from a state run agency. For example, if they are a healthcare system, they would be unlikely to be victims of APT1. On the other hand, if they are working on defense contracts, it would be vital to be prepared for threats like this as they are very likely to be under attack from state level threats.

Assuming I knew this going into work on my first day, I would evaluate the system and what kind of hardening I would need to do to protect them from these kinds of attacks. To protect against credential dumping attacks, I would ensure that users were limited to the principle of least privilege to prevent a successful attack from being as successful. I would also ensure that password protections were in place. If the company has no policies regarding passwords, it would be very likely that they would be successfully attacked.

My first day as a Hunt analyst would mostly be about checking the system for flaws and doing what I could to make management aware of ways to prevent them. The reason that I would be so focused on this on day one is that it would be vital to my job to know what kind of defenses and policies the company had in place to prevent attacks in the first place.

Observation is the first step of the OODA loop so that would be my focus on day one, most likely moving into the orientation phase very quickly.

Bibliography

SecureSet. (2020). SCA HUN200-1 APT1 Case Study.