Adversary Archetype

Basic

Type of Adversary: Hacker for hire.

Size: One person.

Structure: They operate independently and are hired for specific contracts.

Targets

This is dependent on their contract but their targets tend to fall within the following groups:
- Social activists
- Political leaders
- Human rights defenders
- Journalists

Motivation

The main motivation is money, although there may at times also be an ideological affinity with the contractor.

Intent

- Obtain sensitive information that can be used to blackmail the victim.
- Delete files and documents on an investigation that compromises the contractor from the cloud.
- Stealing access to the victim's email and social media accounts to affect their ability to communicate and disseminate information.

Technical Capabilities

They have formal technical training and are extremely adept in hacking and social engineering. They have access to state-of-the-art hardware and are experts in creating fake email and social media accounts.

Favored Means of Attack

- Phishing via email, SMS and WhatsApp to obtain access credentials for their victims' accounts.
- Social engineering executed through fake social media accounts to obtain sensitive personal information about the victim.

Resources

- Money and time are abundant given that they are contracted and paid for the specific purpose of carrying out this work.
- Lack of a legal framework and rule of law have further eased this individual's ability to carry out attacks.

Constraints & Limitations

- Conditions of use of the platforms used to contact victims.
- Until the attacker can gain access into closed sites and accounts the information they have is limited to what is publicly available online.