ANOMALI™
Hacker Persona

Courtesy of Anomali Labs

Cyber Mercenaries

These are the arms dealers of the cyber world, but in some cases are lumped in with the loosely defined "APT" bucket.

Script Kiddies

1. The Common Criminals of the Cyber world.
2. These are actors who are hanging out on message boards, might try to write a RAT once,
3. or engage in a DDoS with Anonymous here and there, but often can't monetize their gains.
4. The old web defacement hackers focused on getting their name out there would fall into this category.

The Insider Threat

Malicious Insiders - Employees with a grudge.

Whitehat Hackers

These are security researchers and operators. They actively track and monitor threats. They may sinkhole domains and seize or takedown botnets. They may or may not operate completely within the law, but their intent is to stop malicious hackers. Those that operate outside the law are sometimes referred to as "Greyhats".

Organized Criminals

These are groups that are much more efficient with monetizing their gains. They have a well established supply chain where different tasks are often supplied by different individuals (spam operations, backdoor operations, carding operations, hosting operations). The "Business Club" that includes the ZeuS author Slavik (Evgeney Bogachev) and PCI intrusion actor Dmitri Smilanets, fall into this group.

Nationalist Hackers

State Allowed and Enabled Hackers - These actors may not be nation states themselves, but are not prosecuted for their activities which often further their states agenda. Some of this groups intrusions are lumped into the "APT" bucket.

Repeat Offenders

These are people or groups like LulzSec and Sabu, or actors like th3J3st3r. They've gained some skill and have some connections to loosely monetize their gains, but they don't have the well oiled criminal connections that other groups have.

Hacktivists

These are the larger groups that want to make a statement through common techniques such as DDoS attacks or Web Defacements, like the various Anon-sects. They are motivated by ideology, politics, etc.

Disorganized Criminals

These are people like the ShadowCrew, with Gonzalez and Stephen Watt. They have some skills, are loosely organized, and they have some capability to monetize their gains.

Nation State Actors

These are the true Military and Intelligence Apparatus. They have giant budgets and long running persistent programs, but are usually focused on true intelligence and military objectives. The tools used by these groups can be extremely complex, but may be simple since these groups play to the level of their victim, not wanting to burn expensive tools and exploits unnecessarily. These are often the truly advanced or extremely persistent attacks in the "APT" bucket.