**CYBERCRIME LANDSCAPE**

**Cybercriminals**

Cybercriminals usually work in organised groups, named cybercriminal organizations.

**Main targets and motivations:**

* Financial gain: The main target of cyberciminals is to obtain profit with their actions. They can use many different attacks to obtain profit such as Ransomware, trojans…
* Espionage: Some groups such as political groups, militar groups and other entities are targets of espionage. Information is an important source of money.
* Attack on reputation: Cybercriminals may want to benefit their beliefs or harm others. This may be for their own ideology or their services may be requested by other organizations. This is also called Hacktivism.

**Modus operandi:**

* Ransomware attacks: They encrypt the data of other organizations and ask for money to get the information back.
* Phishing and social engineering: They manipulate individuals to reveal sensitive information or trick them to give themselves access to valuable information.
* Malware deployment: They use viruses, worms or trojans.
* DDoS attacks: They use this attacks to disrupt services, this usually has great impact on the victim's reputation,
* Credential stuffing: Using automated scripts to try stolen credentials on various sites, exploiting the tendency of users to reuse passwords across platforms.

**Organizations against cybercrime**

**Public entities:**

* Interpol and Europol: These entities have dedicated cybercrime units and they. Their main operations are taking down dark web marketplaces, arresting important cybercriminals and they are responsible for acting against major cybercrime operations.
* FBI: The FBI has a cybersecurity division that collaborates with private entities to tackle global cyberthreats.
* Cybersecurity and Infrastructure Security Agency (CISA): Their goal is to protect critical infrastructure from cyberattacks. They offer guidance, share threat intelligence, and help to respond to cyber incidents.
* National Cybersecurity centers: Many countries have their own cybersecurity centers for their own country. These entities are also responsible for doing public awareness campaigns.

· In Spain we have the INCIBE (Instituto Nacional de Ciberseguridad)

**Private entities:**

* Anti-Phishing Working Group (APWG): It tracks and dismantle phishing operations. It also tries to educate the public on phishing attacks in order to avoid them so it works on both, fighting against existing threats and avoiding new ones.
* Telefonica Tech: Is the cybersecurity branch of Telefonica. They offer their services to other companies specially in Spain. They also collaborate with law enforcement and public organizations against cybercrime.
* Hispasec: A consultancy that provides specialized services such as penetration testing, vulnerability analysis, and incident response. They created VirusTotal, a well-known malware analysis service.

**Sources:**

<https://www.crimrxiv.com/pub/onzk3jbg/release/1>

<https://www.recordedfuture.com/threat-intelligence-101/threat-actors/cybercriminals>

<https://www.interpol.int/en/Crimes/Cybercrime>

<https://cybersixgill.com/resources/the-state-of-the-underground-2023/>

<https://threat.technology/these-are-the-top-cyber-security-companies-in-spain-2021/>