Cybercriminal Ecosystem

Cybercrime is no longer a one man operation. Within the cybercrime underground an attacker can find a wealth of tools and services that can be bought or rented to facilitate different aspects of the attack lifecycle.*

Fraud as a service is constantly changing and adapting to new security solutions, offering end to end technologies, multiple SLA levels and low prices for everything a cybercriminal might need.

Malware

Cost: Free - $20k (license based)

Trojan designed to steal data, manipulate online banking sessions, inject screens and more.

Exploit Kits

Cost: $2K (monthly rental)

Toolkits designed to exploit system and software vulnerabilities resulting in a malicious download.

Droppers

Cost: Free - $10K

Software designed to download malware to an infected device, evading antivirus and research tools.

Infrastructure

Cost: $50 - $1,000 (Rental per month)

Hosting services for malware update, configuration and command and control servers. Some are fast flux or TOR based.

Money Mules

Cost: Up to 60% of account balance

A person who receives thestolen money from a hacked account and transfers the funds via an anonymous payment service to the mule operator.

Spammers

Cost: $1 - $4 per 1000 emails

Spam botnet operators that spread emails with attachments or links leading to a Trojan infection.

* This infographic shows one possible scenario of a cybercriminal attack lifecycle. Prices for this scenario are estimates.