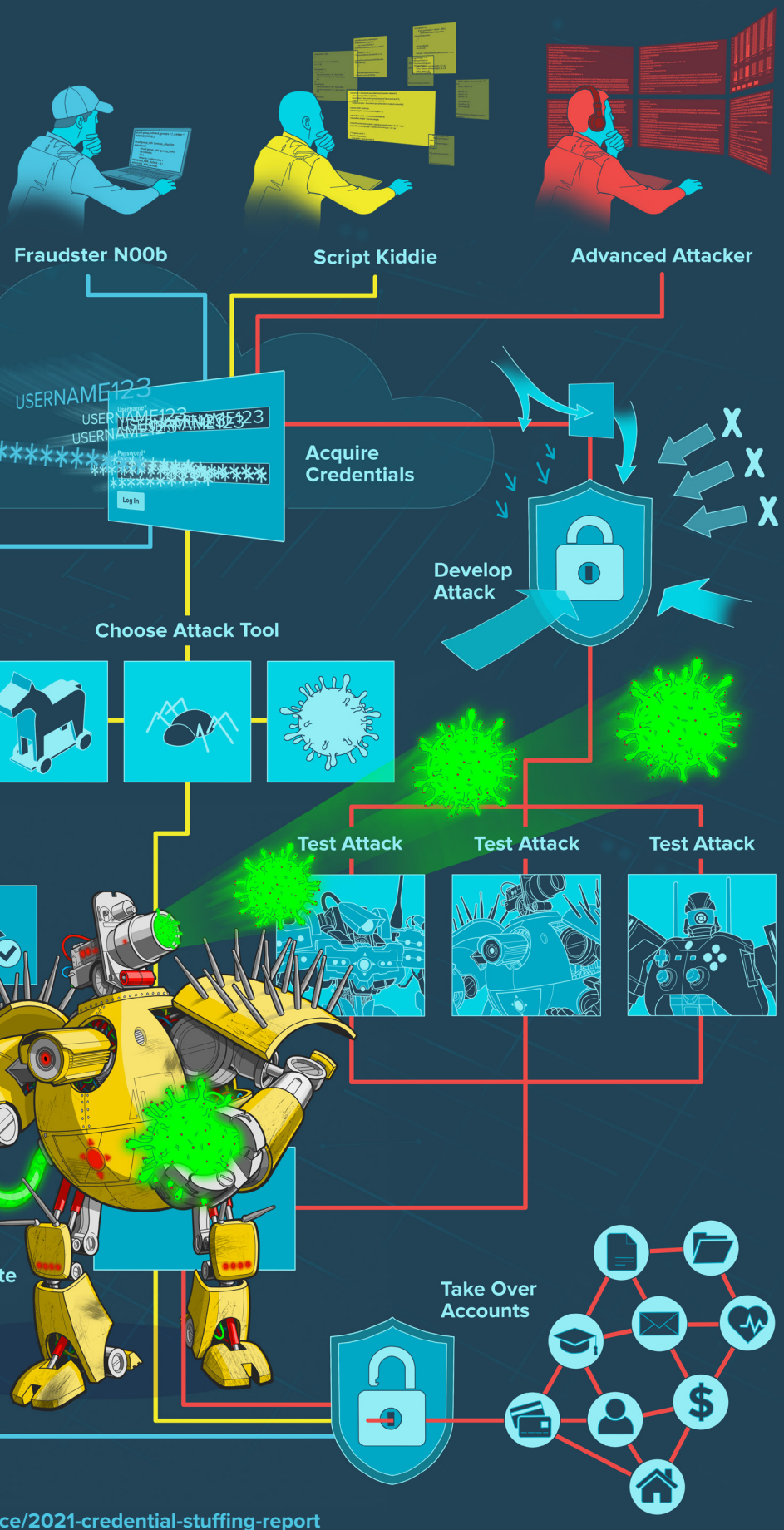
2021 Credential Stuffing Report Infographic

Credential stuffing methods depend on the attacker skill level.

Most attackers start off with the cheapest, and therefore least sophisticated, attack to maximize profits. Advanced attackers will only increase sophistication (resemble and blend-in with genuine users) if their target has implemented countermeasures that detect their original attack, and the rewards outweigh the increasing attack cost.

How advanced attackers develop and test their attacks with common tools:

- **Simulate Network Traffic** using a tool like Sentry MBA to craft HTTP requests along specified parameters and pass them along to the target (not emulating human behavior or higher-level browser activity).
- **Simulate Browsers and Native Apps** with tools like Puppeteer, Headless Chrome, PhantomJS.
- **Simulate Human Behavior** with a tool like Browser Automation Studio that produces slow and random mouse and keyboard behavior that standard automation checks fail to detect.
- **Use Microwork Services** to scale up real human behavior, like CAPTCHA solving, with services like Amazon Mechanical Turk (MTurk), Microworkers, Minijobz, and RapidWorkers.



F5 LABS

SHAPE Part of F5

Read the full report on F5Labs:
https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report