

Break the Account Takeover Kill Chain

Would you recognize a cyber kill chain as it's happening?

Explore the **Account Takeover Kill Chain** cyberattack stages and learn how to stop them.

1



RECONNAISSANCE

What to Expect

Data breach; credentials stolen



HOW TO DEFEND

Implement:

- Web application firewall
- Encryption
- Credential checks against known breaches
- Strong security policies



POSSIBLE ATTACKER REACTION

Attackers may try another site or buy credentials, since billions are available on the dark web.

2



WEAPONIZATION

What to Expect

Small spike in failed logins



HOW TO DEFEND

Confirm:

- Whether logins are legitimate users
- Bot management software is tuned
- Login endpoints are protected with MFA



POSSIBLE ATTACKER REACTION

Attackers may tune bot software if bot is detected.

3



DELIVERY

What to Expect

Spike in traffic; excessive login requests



HOW TO DEFEND

Validate:

- Rate controls
- MFA
- User behavior anomalies
- Advanced detections from bot management software



POSSIBLE ATTACKER REACTION

Attack is stopped. Kill chain is disrupted. Very sophisticated bots **may** temporarily evade detection.

4



EXPLOITATION

What to Expect

Single request coming from a human; small increase in logins



HOW TO DEFEND

Inspect:

- User behavior anomalies



POSSIBLE ATTACKER REACTION

Attackers can't do anything at scale. For individual attempts, criminals **may** search for the account owner on social networks.

5



ACTION

What to Expect

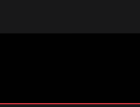
Spike in customer reports of accounts being taken over



HOW TO DEFEND

Monitor:

- User risk continuously until user logs out



POSSIBLE ATTACKER REACTION

Account protection software blocks the attempt. Attackers give up.

Learn how Akamai can help you **prevent account takeover**

[Learn more](#)

