CYBEREDGE GROUP

THREAT BRIEF

Understanding Fake Account Creation and Defense Requirements

WHAT IS FAKE ACCOUNT CREATION?

An attack in which cyber criminals deploy bot networks to automate the creation of hundreds, even thousands, of counterfeit user accounts in a short amount of time.

Companies leverage user accounts for a variety of purposes. In addition to providing access to web-based services, user accounts—and the associated information—are used for tracking user behavior, to deliver personalized offers, and to create additional revenue (for example, by selling email lists). Naturally, companies want to make it as easy as possible for users to register for an account. Some companies, like cloud computing providers, offer free services just for signing up.

Unfortunately, it's just as easy for cyber criminals to sign up for a fake account as it is for a user to sign up for a legitimate account.

WHAT'S AT RISK

- Productivity of your security and fraud analysts, customer service, and IT
- Brand reputation
- Company devaluation
- Fake news and disinformation
- Data quality
- Financial fraud
- Consumer and stakeholder trust

HOW IT WORKS

Fake account creation exploits the business logic of a website or application, specifically the registration form. Attackers create illegitimate accounts, which they then use to conduct other criminal acts, such as financial fraud, money laundering, or to spread rumors, fake news, spam or malware.

Cybercriminals can create fake accounts manually, but using botnets allows them to scale their efforts. Cybercriminals assemble an attack script that inputs data into a registration form. They then use bot networks to distribute the script and create many fake accounts.

FAKE ACCOUNT CREATION DEFENSE CHALLENGES

Several challenges come into play when addressing fake account creation. Not the least of which is the issue of the customer experience. Prevention techniques like adding strong authentication, CAPTCHA, or challenge questions can create user friction at a critical point in the customer journey. If the account creation process is too cumbersome, companies risk losing potential customers.

The sophistication of bots also poses a challenge when it comes to stopping fake account creation. Some bots can overcome CAPTCHA, and all the inputs from bots are within the expected parameters for a registration form—so accounts look legitimate when they're being created. Transaction analysis tools only detect fake accounts after the fact. By then, the criminals may have already used the accounts to commit other attacks.

Finally, security organizations are already strapped for resources. Configuring JavaScript and SDKs to gain more visibility into client-side behaviors is time-intensive and increasingly ineffective.

According to Facebook, the social media giant disabled

583 MILLION

fake accounts between January and March of 2018.

REQUIREMENTS FOR FAKE ACCOUNT CREATION DEFENSE

An effective solution for detecting and stopping fake account creation must:

- Be a software-only solution; no need for expensive, purpose-built appliances
- Be deployable on-premises, in the cloud, across any number of locations
- Not rely on in-line detection, which is limited and adds network latency
- Automatically discover all application assets across the organization
- Not require use of time-consuming JavaScript or mobile SDK modifications
- Use an AI engine with machine learning to provide attack detection/analysis in real-time
- Provide effective attack defense against all channels — web, mobile, and API apps
- Integrate with existing security tools, providing security teams with insight into attack details
- Stop attacks fast with customizable, automated mitigation policies
- Reduce infrastructure costs, financial loss, business disruption

THREE KEY REQUIREMENTS FOR A BOT ATTACK:

1) Attack Tools

- Sentry MBA
- SNIPR
- Hitman
- Hydra
- Medusa
- Phantom JS
- CURL & WGET

2) Infrastructure Access

- Compromised devices
  - Business and personal computers
  - Home routers
  - IoT
- Underground VPNs
- Unscrupulous Internet Service Providers

3) Credentials (username–password pairs)

- Where are credentials acquired?
  A sampling of breaches in 2018 includes:
  - Under Armour, 150M records
  - MyHeritage, 92M records
  - Facebook, 50M records
  - British Airways, 380K records
  - T-Mobile, 2M records
- How are breached credentials sourced?
  - Dark Web supplier/seller e-commerce applications

Any organization that encourages users to sign up for an account via a registration form is at risk of fake account creation. Traditional infrastructure security tools or first-generation bot defense solutions can't prevent these attacks. Fake account creation is a specialized, automated attack that requires innovative, advanced detection and mitigation technology.