Understanding Account Takeover Attacks and Defense Requirements

WHAT IS AN ACCOUNT TAKEOVER (ATO)?

An attack in which cyber criminals deploy bot networks to test real usernames and passwords at consumer-facing websites for the purposes of gaining authorized access to a legitimate account.

A data breach can result in hundreds of thousands of user credentials landing on the dark web.

Once the breach is discovered, the target company typically responds by forcing customers to reset their passwords. Nevertheless, the risk remains because people often reuse their usernames and passwords to access work applications, social media networks, e-commerce sites, or streaming media services. The tendency to reuse passwords combined with the availability of user credentials on the dark web create a ripe opportunity for cybercriminals to commit massive account takeover attacks.

WHAT'S AT RISK

- Productivity of your security and fraud analysts, customer service, and IT
- Over-provisioning infrastructure to compensate for degrading performance
- Customer and stakeholder trust
- Confidential and sensitive data
- Brand reputation
- Financial fraud

HOW IT WORKS

An ATO attack begins with credential harvesting. Cybercriminals either purchase usernames, email addresses, and/or passwords on the dark web or harvest them from a previous data breach. Criminals then test the credentials to determine which username/password combinations are valid. The process is automated using massive, often geo-distributed bot armies that emulate human behavior. When a valid username and password combination is discovered, the cybercriminal uses it to gain access to the account.

Once cybercriminals have legitimate access to an account, they can generally move about freely and without generating suspicion. At this point, criminals can commit financially motivated downstream attacks such as:

- Financial fraud by carrying out unauthorized transfers or withdrawals from bank accounts, or using stored credit cards to make fraudulent purchases
- Spam by posting user-generated content from the victim's account
- Phishing by attacking the victim's colleagues

ATO DEFENSE CHALLENGES

ATO attacks are uniquely difficult to defend against for two reasons:

1.) The keyboard clicks and mouse moves executed by sophisticated bots look like typical human behavior

2.) Cybercriminals obtain seemingly authorized access via legitimate user credentials

Because of these two factors, traditional detection and prevention tools are unlikely to detect an ATO attack. Infrastructure-level detection is oblivious to legitimate transactions. Transaction analysis tools detect criminal activity after the attack is over and the damage is done. While multi-factor authentication may be used to help thwart ATO attacks, it's not foolproof and requiring customers to present a second form of authentication impacts the user experience.

To further complicate matters, 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. Complicated websites, like those for e-commerce, offer login capability from multiple pages. It's important to discover all of these entry points to protect them. JavaScript simply can't do that. Plus, as first-generation technologies, JavaScript and SDKs don't always function as intended.

REQUIREMENTS FOR ATO DEFENSE

An effective solution for detecting and stopping ATO attacks should provide these capabilities:

- A software-only solution; no need for expensive, purpose-built appliances
- Deployable on-premises, in the cloud, across any number of locations
- Passive, off-line deployment, allowing more time for accurate detection
- Automatic discovery of all application assets across the organization
- No need for time-consuming JavaScript or mobile SDK modifications
- AI engine with machine learning to provide attack detection/analysis in real time
- Effective attack defense against all channels – web, mobile, and API apps

WEB APPLICATION ATTACKS ACCOUNT FOR

21%

OF BREACHES,

according to the 2018 Verizon Data Breach Investigations Report.

- Integration with existing security tools, providing security teams with insight into attack details
- Help customers right-size their infrastructure and avoid over-provisioning due to bot traffic
- Minimize risk of data/financial loss, business disruption, damaged reputation

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

If your organization relies on web, mobile, and API applications, you may be the target of an ATO attack right now without your knowledge. These specialized, automated attacks require innovative, advanced detection and mitigation technology that you won't find in traditional infrastructure security tools or first-generation bot defense solutions.