HUMAN

Are You Prepared for ACCOUNT TAKEOVER ATTACKS?

What Are Account Takeover Attacks?

Account takeover (ATO) is an attack in which criminals take unauthorized ownership of online accounts using stolen usernames and passwords.

Username: cjerry78
Password: *********
LOGIN

- Email Account
- Online Bank Account
- Online Retail Account
- Any Account or Service with a Login

Value Stored in Accounts

Consumer accounts hold more **personal information** and **payment data** than ever before, making them a rich **target for cybercriminals**.

- Credit and debit card numbers
- Gift card balances
- Loyalty points
- Personally identifiable information (PII)

45% of consumers prefer using **stored credit card information** for easier checkout

80% of U.S. adults belong to **at least one loyalty program**

How Can Cybercriminals Monetize Accounts?

There are growing opportunities for cybercriminals to **monetize compromised accounts** and the identity information they contain. They can:

- Make fraudulent purchases with stored payment information
- Drain gift card balances, loyalty points and account credits
- Submit fake credit applications
- Create fake accounts
- Submit fake warranty claims
- Post fake reviews

ATO Attacks Are On the Rise

April 2020 → June 2021: ATO attempts **rose 307%** from April 2020 to June 2021

ATO attacks averaged **82% of all login attempts** in the **second half** of 2021 (up from **75%** in the **first half** of 2021)

Malicious login attempts make up to **94% of total login attempts** during attack peaks

ATO and the Digital Attack Lifecycle

Cybercrime has become more integrated, continuous and cyclical than ever before. Data breaches fuel credential stuffing attacks, which in turn fuel ATO attacks. **Attackers only need to buy a list of stolen credentials and unleash an army of bots to do the rest**.

Login Databases Breached

- Facebook 533,000,000
- MGM Grand 10,600,000
- EasyJet 9,000,000
- Experian Brazil 220,000,000
- Dubsmash 162,000,000
- Syniverse 500,000,000
- Twitter 330,000,000
- Microsoft 250,000,000
- WordPress 76,500,000
- Uber 57,000,000
- Marriott Hotels 383,000,000
- DoorDash 4,900,000
- T-Mobile 2,200,000
- Quora 100,000,000

Credential Stuffing Attack — Automated login attempts to validate credentials

→ **Valid Email/Password Pairs for This Site** — **8% success** (varies based on databases) — **Validated account ~$3**

→ **Account Takeover Attack**
- Account abuse
- Identity theft
- Stolen PII

Why ATO Attacks Are So Difficult to Detect

It is **very easy to launch a highly distributed campaign with bots** that pretend to be browsers. Because the number of requests from a single source is small and doesn't exceed the limit of requests from an IP address, **ATO attacks fly under the radar**.

- **366,000** login attempts
- **>1,000** different IP addresses
- **10,000** attempts per hour

77% of these attacks would go **undetected** by volumetric detection

ATO Attacks Cause Financial Losses

ATO losses are up **72% year over year**

U.S. businesses lose nearly **$7 billion** annually due to **ATO attacks**

Up to **80%** of e-commerce operational costs are **negatively affected by bad bots**

Malicious bots **negatively impact 18–23%** of e-commerce revenue

Business Impact of ATO Attacks

- **High operational costs** for infrastructure and bandwidth
- **Increased demand** for customer resources
- **Damage to brand** reputation and consumer trust
- **Burden on IT** to manage bad bots
- **Refunds**, chargebacks and make goods
- Lawsuits and regulatory **fines**
- **Dive** in stock prices

How Can You Stop Account Takeover Attacks?

Advanced bot detection and mitigation services can reduce the negative impact of malicious bots by more than **50% at times of peak bot traffic**.

The key to preventing ATO attacks is to switch from profiling environments to focusing on behavioral anomalies and characteristics. HUMAN Bot Defender leverages machine learning, behavioral analysis and predictive analytics to detect and stop sophisticated account takeover attacks with unparalleled accuracy.

> "I found HUMAN to be the ultimate vendor with [an] amazing support team, great vision, and an ever-growing hunger for success."
>
> — Reference Customer from the Forrester Wave™: Bot Management, Q2 2022

SOURCES: Aberdeen Strategy & Research: Quantifying the Impact of Bad Bots on E-commerce Merchant Profitability; Forrester: The Forrester Wave™: Risk-Based Authentication; Ipsos: ING International Mobile Banking Survey; Javelin Strategy & Research: Identity Fraud Report; PerimeterX: Automated Fraud Benchmark Report; Reuters: Loyalty Programs Poll; Sift: Q3 2021 Digital Trust & Safety Index.

Learn more at www.humansecurity.com