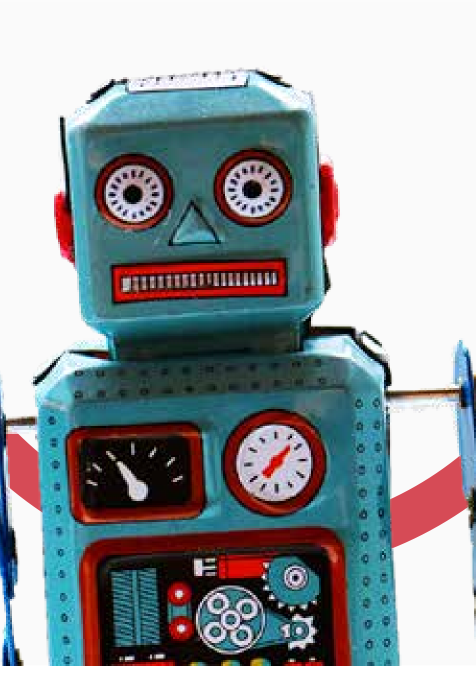
perimeterx | Infographic

Are You Prepared for Account Takeover Attacks?



What are Account Takeover (ATO) Attacks?

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

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

Username
cjerry78
Password
****
LOGIN

Account Takeover is Exploding

Because it is relatively easy to break into online accounts and monetize them, **websites have become the new banks for attackers**. They use automated bots to gain access to credit card or bank account details, and steal credit card reward points, gift cards, loyalty points, airline miles and marketplace credits. ATO is trending up a staggering 72 percent over the prior year.

ATO Attacks Are Up

$7 Billion
Loss due to ATO in 2019

+72%
year-over-year ATO attacks in 2019

137 Million
Mobile malware detections in 2019, up 22 percent

Bot Attacks Are Up

$16.9 Billion
Overall fraud losses grew 15% in 2019

60% – 70%
of traffic to checkout pages is malicious bots

40% – 80%
of retail login attempts are by malicious bots

What's Driving ATO Attacks?

Web App Breaches Fuel ATO
2x
Web Application Attacks Doubled in 2019

$$$
$40 – $392 Million
cost of mega-breaches

Organized Fraud Ecosystem
4.1 Billion
Records exposed in 2019 as a result of a 54% increase in breaches the prior year

45%
of breaches in 2019 involved **stolen credentials**

59%
of people **reuse passwords**; average 6 passwords total

29%
Increase in attacks between February and March 2020, influenced by COVID

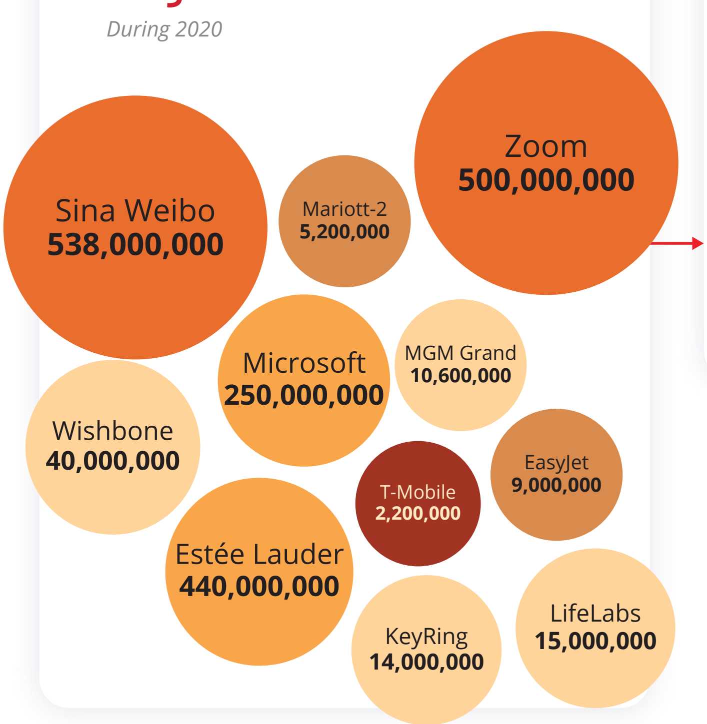
> "PerimeterX can track user fingerprints across web, mobile, and API channels, making it a good choice for organizations looking to understand behavior regardless of how the user accesses the site."
>
> Forrester, New Wave: Bot Management, Q1 2020

Automated Bot ATO Vector

All attackers have to do is buy a list of stolen credentials and launch an army of bots across multiple sites to test user name and password combinations. In the end, they get a list of validated credentials that they can use for account takeover or sell to others.

Login Databases Stolen

During 2020



ATO Attack

Bot Attack
Automated testing against site

Site Fraud

Bot Attack
- Account abuse
- Identity theft
- Stolen PII

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

Why Bot 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, **bot 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

Lasting Impacts of ATO

ATO attacks can be devastating to both users and the organizations that support them.

For users, the result, invariably, is **a horrible experience** stemming from one or more of the following:

- Inability to access personal accounts
- Loss of personal data
- Unauthorized purchases
- Depleted gift card and loyalty point balances

For organizations, it means:

- High operational costs
- Warranty fraud
- Burden on IT to manage bad bots
- Loss of consumer confidence
- Impact on revenue
- Dive in stock prices
- Risk of massive fines

What Can You Do?

The key to stopping account takeover and account abuse attacks is to switch from profiling environments to focusing on behavioral anomalies and characteristics. **PerimeterX Bot Defender protects online accounts** from unauthorized access and **averts account takeover attempts** before they can cause damage.

Eliminate Account Takeover

With its sophisticated machine learning, **PerimeterX Bot Defender** detects malicious behavior on websites in real-time, **stopping the most advanced account takeover attacks**.

Stop Fake Account Creation

With **PerimeterX Bot Defender** you can detect fake account creation attempts in real-time, **automatically blocking bots** from registering for your service, while **performing automated analysis** for continuously updated protection.

> "Bad bots make it easy for malicious attackers to quickly roll through countless login / password combinations, which can lead to account takeover. Blocking bots prevents automated credential stuffing and application hacks."
>
> Forrester

Learn more at www.perimeterx.com

SOURCES
Forrester, New Wave: Bot Management, Q1 2020
2020 Global Identity and Fraud Report by Experian
The 2020 Identity Fraud Report, released today by Javelin Strategy & Research
Web Application Attacks Double from 2019: Verizon DBIR Verizon's annual data breach report shows most attackers are external, money remains their top motivator, and web applications and unsecured cloud storage are hot targets.
Today's 'mega' data breaches now cost companies $392 million to recover from.
Identity Force