What Are ATO Attacks?
ATO attacks occur when someone gains unauthorized access to one or more online accounts.

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

ATO is Exploding
Because it is relatively easy to break into online accounts and discover them, websites have become the most prominent attack vector in breaches. Authenticated account attacks are by malicious bots.

ATO Attacks Are Up

$5.1 Billion
1.4 billion stolen email and password combinations found on Dark Web database

65% of all ATO attempts
+79% year-over-year mobile ATO attacks in 2018

79% of all ATO attempts
+65% year-over-year ATO attacks in 2018

$1 Billion
Malicious bot attacks on websites in real-time

50% – 70% at traffic to checkout pages is malicious bots

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

What’s Driving ATO Attacks?

Why Bot ATO Attacks Are So Difficult to Detect
ATO attacks can be devastating. With its sophisticated machine learning, PerimeterX can detect malicious behavior on any account or service with a login. In the end, they get a list of validated credentials that can be used for ATO or sold to others.

Bot Attack

Valid email/password pairs for this site (varies based on databases)

8% success rate

366,000 login attempts

10,000 attempts per hour

> 1,000 different IP addresses

For banks, the result, in most cases, is a fraudulent transaction. For retail websites, the result is a fraudulent purchase. For online communities, the result is a compromised community. For organizations, the result is a fraud and liability that can result in: patient deidentified • Stolen PII • Account abuse • Warranty fraud • High operational costs • Risk of massive fines • Dive in stock prices • Impact on revenue • Loss of consumer confidence • Burden on IT to manage bad bots

What Can You Do?
Eliminate ATO
PerimeterX can detect bots and automate analysis to perform automated analysis for your data.

Stop Fake Account Creation
PerimeterX can detect bots and automate analysis to perform automated analysis for your data.

Login Databases Stolen

Organizations
Email
Marketing
Travel
Healthcare
Financial Services
Retail
Professional Services
Wellness
Information Security
Consumer Goods
Automotive
Consumer Services
Automated Bot ATO Attack Vector
With automated bot attacks, attackers launch armies of bots to gain access to credit card or bank account details, test user name and password combinations, and perform automated analysis to test user name and password combinations.

1,000,000,000
1.4 billion stolen email and password combinations found on Dark Web database

500,000,000
366,000 login attempts

20,000
> 1,000 different IP addresses

10,000
10,000 attempts per hour

366,000
366,000 login attempts

10,000
10,000 attempts per hour

> 1,000
> 1,000 different IP addresses

Lasting Impacts of ATOs
ATO attacks can be devastating. They can use for ATO or sell to others.

For users, the result, in most cases, is a horrible experience stemming from one or more of the following:

Unauthorized access to one or more online accounts:

Email
Online Bank
Any Account or Service with a Login

What Are ATO Attacks?
ATO attacks occur when someone gains unauthorized access to one or more online accounts.

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

ATO is Exploding
Because it is relatively easy to break into online accounts and discover them, websites have become the most prominent attack vector in breaches. Authenticated account attacks are by malicious bots.

ATO Attacks Are Up

$5.1 Billion
1.4 billion stolen email and password combinations found on Dark Web database

65% of all ATO attempts
+79% year-over-year mobile ATO attacks in 2018

79% of all ATO attempts
+65% year-over-year ATO attacks in 2018

$1 Billion
Malicious bot attacks on websites in real-time

50% – 70% at traffic to checkout pages is malicious bots

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

What’s Driving ATO Attacks?

Why Bot ATO Attacks Are So Difficult to Detect
ATO attacks can be devastating. With its sophisticated machine learning, PerimeterX can detect malicious behavior on any account or service with a login. In the end, they get a list of validated credentials that can be used for ATO or sold to others.

Bot Attack

Valid email/password pairs for this site (varies based on databases)

8% success rate

366,000 login attempts

10,000 attempts per hour

> 1,000 different IP addresses

For banks, the result, in most cases, is a fraudulent transaction. For retail websites, the result is a fraudulent purchase. For online communities, the result is a compromised community. For organizations, the result is a fraud and liability that can result in: patient deidentified • Stolen PII • Account abuse • Warranty fraud • High operational costs • Risk of massive fines • Dive in stock prices • Impact on revenue • Loss of consumer confidence • Burden on IT to manage bad bots

What Can You Do?
Eliminate ATO
PerimeterX can detect bots and automate analysis to perform automated analysis for your data.

Stop Fake Account Creation
PerimeterX can detect bots and automate analysis to perform automated analysis for your data.

Login Databases Stolen

Organizations
Email
Marketing
Travel
Healthcare
Financial Services
Retail
Professional Services
Wellness
Information Security
Consumer Goods
Automotive
Consumer Services
Automated Bot ATO Attack Vector
With automated bot attacks, attackers launch armies of bots to gain access to credit card or bank account details, test user name and password combinations, and perform automated analysis to test user name and password combinations.

1,000,000,000
1.4 billion stolen email and password combinations found on Dark Web database

500,000,000
366,000 login attempts

20,000
> 1,000 different IP addresses

10,000
10,000 attempts per hour

> 1,000
> 1,000 different IP addresses

Lasting Impacts of ATOs
ATO attacks can be devastating. They can use for ATO or sell to others.

For users, the result, in most cases, is a horrible experience stemming from one or more of the following:

Unauthorized access to one or more online accounts: