Bot and ATO Attacks: How They're Related and What You Can Do

CNP CARD NOT PRESENT®
NEWS, EDUCATION AND EVENTS
DECODING DIGITAL PAYMENTS & FRAUD

Radial
a bpost company

There are faceless armies of robots arrayed against you. They are legion, they are tireless and, if they overwhelm your defenses, they can be lethal—to your business. Bots are not the minions of an evil super-intelligence in a science fiction film bent on dominion over mankind. They are simply tools that can be used by anyone who picks them up. And, the people picking them up these days often are criminals employing them to take over or create online accounts.

While account takeover (ATO) fraud used to concern mainly bankers and insurance companies, the range of online accounts being illegally accessed and monetized is exploding. E-commerce sites frequently allow consumers to store their payment credentials to make subsequent visits easier or to make recurring purchases automatic. Media companies are storing card numbers to enable streaming video services. Telecommunications companies are providing direct-carrier billing for online purchases. Digital wallets, funded by bank accounts or payment cards, store value that can be accessed online.

> *When a fraudster gains access to a victim's personal online account, they are able to leverage that customer's trusted history and loyalty built over the life of the account. And, a customer who is the victim of an ATO may not even realize they have been compromised if the account has not been accessed for an extended period of time.*

And, not only do fraudulent transactions associated with ATO result in higher average loss, according to Towhidul Hoque, senior manager of fraud decision analytics at Radial, they are also more difficult to spot than other types of fraud because they raise fewer red flags.

"When a fraudster gains access to a victim's personal online account, they are able to leverage that customer's trusted history and loyalty built over the life of the account," Hoque explains. "And, a customer who is the victim of an ATO may not even realize they have been compromised if the account has not been accessed for an extended period of time."

The number and variety of online accounts that contain stored value or to which consumers are attaching payment credentials has proliferated significantly, and nearly all of them are currently secured with the ubiquitous user id/password combination. With too many passwords to remember, consumers reuse them frequently, creating a vulnerability that is leveraged by stolen data—data that's available to bad actors via ubiquitous network security breaches reported in the news.

One review noted that publicly disclosed data breaches in the first six months of 2019 exposed 4.1 billion records[1]. Hundreds of millions of those records included usernames and passwords.

That's where bots come in.

BOTS SUPERCHARGING ATO

Overall, fraudulent transactions fell from 2018 to 2019, but losses due to account takeover fraud continued to surge. In 2019, ATO cost businesses $6.8 Billion in direct fraud losses—72 percent more than the year before[2]. Generally speaking, bots are the engine driving that growth through a process called "credential stuffing."

With billions of stolen records up for sale on the Dark Web, there is no shortage of raw material. Fraudsters understand that stolen username/password combos will likely get them access to multiple online accounts. But, how do they know which login credentials will enable them to access which sites?

Growth in direct account takeover fraud losses from 2018 to 2019

72%

Bots are simply software scripts that automate a process. When the primary data stolen in breaches was payment card information, bots were used mainly for card testing. Fraudsters directed bots to make hundreds or thousands of low-dollar purchases at various e-commerce sites to verify the validity of credit card information. As breaches began to yield different information, however, the bots' targets changed.

Now, you're more likely to find bad actors using bots to automate the login process for websites—something they can do at a scale that makes ATO simple. A bot can take billions of usernames and passwords and try them at thousands of websites. When a certain credential set is validated for a specific site, it can then be packaged and sold with other valid credentials to fraudsters who specialize in extracting value from an online account before they are detected.

With a valid login, a fraudster appears to be the legitimate user and, therefore, is extremely difficult to identify. Once logged in, they can monetize their illegal access in several ways. They can purchase physical products with the account's card on file and resell them, drain an account of any stored value (e.g., cash, store credit, gaming credits or loyalty points), and so on.

ATTACKING BOTS UPSTREAM TO HEAD OFF ATO DOWNSTREAM

While an unauthorized account takeover is difficult to spot with traditional fraud detection technology (the fraudulent user was authenticated by supplying the right username and password, after all), there are some indicators. Higher average order values, multiple changes to an account at one time (e.g., shipping address, password, and email address), or the transfer of many reward points are examples of red flags that may indicate ATO.

Companies are investing significantly in technology solutions that attempt to identify which accounts are legitimate and which have been accessed using stolen login credentials. In one study, credit card issuers cited retail ATO fraud as the biggest reason for investing in machine learning-based antifraud technology[3]. Other tools also are available that organizations can employ as part of a layered defense against ATO.

> *...the best practice for handling ATO attacks is to prevent the attack at the account login stage, not the order checkout stage*

Effective bot detection, which companies might not connect with ATO, should form an important layer in that defense. Traditional fraud detection solutions are not sufficient. Nearly all of these solutions are focused on catching criminals *after* they have accessed the accounts—completely understandable, given the way online fraud departments developed.

"But, the best practice for handling ATO attacks is to prevent the attack at the account login stage, not the order checkout stage," Hoque says. "Monitoring keystroke velocity and device identification sensors allows the ATO to be detected well before the transaction is executed. Knowing the customer's behavioral data is also critical in preventing these types of attacks. Having some form of insight to the customers previous and current geographic location, IP address, device, and browser details gives the ability to create a standard that if not properly met, would prevent the attack altogether by denying the transaction."

Companies that have visibility into bot-delivered credential stuffing attacks and effective solutions to mitigate those attacks are preventing account takeover before it happens.

CONSIDER BOTS AS PART OF A LAYERED DEFENSE

Merchants focused on fraud in their digital channels may not come into direct contact with bots and the ways they attack a company's systems. But, for those who operate downstream from a business's main security architecture, the effect of bots on the most pernicious types of fraud they face is clear. And, employing resources to combat bots should be a vital part of any e-commerce merchant's layered defense against fraud.

Just like the fraud they are used to commit, bot attacks are becoming more sophisticated and difficult to detect. Just as antifraud solutions are evolving to meet that sophistication, so are solutions designed to identify and manage malicious Web traffic generated by bots. And, while bot management generally is seen as an IT or security initiative, hence, outside the purview and control of the fraud department, solutions that employ technology to intercept malicious login attempts before they occur translate directly into a reduction in the number of stolen credentials validated and sold to fraudsters to monetize.

Despite their power and speed, bots are not unstoppable. By digging into your data, you can spot recurring patterns or unusual formatting that will point to bot activity. But this activity occurs quickly, so once it's spotted a counter-response needs to be put into place just as quickly.

Fraud departments are vital to the bottom line of card-not-present merchants and account takeover fraud is not going away. But a reduction in the overall number of compromised accounts will likely result in the number of fraudulent transaction attempts and the attendant customer impact. For online sellers increasingly suffering from account takeover fraud, initiating an organizational dialogue about how bot management can benefit multiple areas of a business could result in the addition of an important layer of defense.

> *"Companies that have visibility into bot-delivered credential stuffing attacks and effective solutions to mitigate those attacks are preventing account takeover before it happens."*

1 - 2019 MidYear QuickView Data Breach Report, Risk Based Security
2 - 2020 Identity Fraud Study, Javelin Strategy and Research
3 - Machine Learning: Fraud is Now a Competitive Issue, Aite Group

ABOUT RADIAL

Radial Inc., a bpost company, is the leader in omnichannel commerce technology and operations. Premier brands around the world confidently partner with Radial to deliver their brand promises, anticipate and respond to industry disruption, and compete in a rapidly evolving market. Radial's innovative solutions connect retailers and customers through advanced omnichannel technologies, intelligent payments and fraud protection, efficient fulfillment, supply chain services, and insightful customer care services – especially where high-value customer experiences are critical. We are flexible, scalable, and focused on our clients' business objectives. Learn how we deliver today's retail for you at radial.com.

ABOUT CARD NOT PRESENT®

Card Not Present, part of the RELX Group, is an independent voice generating original news, information, education and inspiration for and about the companies and people operating in the card-not-present space—one of the only sources of content focused solely on this growing segment of the payments industry. Our only product is information. Our only goal is to provide it in an unbiased manner to our subscribers. For more information, visit CardNotPresent.com.

This document was produced as a joint effort between Card Not Present® and Radial.

CNP CARD NOT PRESENT®
NEWS, EDUCATION AND EVENTS
DECODING DIGITAL PAYMENTS & FRAUD

Radial
a bpost company