PROTECT YOUR ONLINE BUSINESS FROM CREDENTIAL STUFFING

STAY AHEAD OF THREATS WITH ADVANCED BOT MANAGEMENT TECHNOLOGY
When someone logs into your site, how do you tell the difference between legitimate use and credential stuffing? Not knowing if a login is coming from a real user or a software program imitating one makes your business vulnerable to fraud.

With the proliferation of online applications, most users don’t practice good Internet hygiene — often repurposing the same login credentials across multiple accounts. That makes every online business with a login page a potential target for credential stuffing, whether you’ve had a data breach or not.

The higher the transaction value, the more that is at risk. A fraudster can purchase goods from an online store, take out bank loans from a financial institution, or steal medical information from a healthcare site. Credential stuffing can hurt your business, customers, and brand — and it is a problem so stealthy that you need specialized tools to detect and defend against it.

Understanding credential stuffing threats, their increasing sophistication, and the best approaches for stopping them can help you safeguard your business.

Source: The Cost of Credential Stuffing, Ponemon Institute, 2017
Recent industry estimates put the number of stolen credentials – user names, passwords, and email addresses – currently circulating in the billions. According to a 2017 report by Frost & Sullivan, “For attackers, it’s simply a numbers game; a 1% success rate of 1 billion attempts will result in 10 million breaches.”

Customer credentials are typically compromised by break-ins elsewhere. That information is then sold on the black market as single or multi-pack sets at prices ranging from under a dollar for premium content to thousands for high-balance bank accounts. FTC research found that it took only nine minutes for hackers to start accessing published stolen credentials once these were available.

Your network and data can be properly secured, but your business is still exposed to fraud if you can’t see and stop credential stuffing before a successful combination is found. In a recent survey by the Ponemon Institute, more than half of respondents reported credential stuffing as a significant security challenge for their companies. Additionally, nearly 70% of respondents said they did not feel (or were unsure if) their companies had adequate visibility into these attacks.
Credential stuffing begins with an attacker trying to verify stolen user information against your website login systems. Once a subset of valid logins is confirmed, the attacker will either resell that list to another fraudster or engage in an account takeover directly – draining online accounts of anything monetizable.

Unlike other web application attacks, such as an SQL injection, login requests resulting from credential stuffing do not have patterns you can easily identify and block. Verified credentials are valid requests – the login information is legitimate, but the entity attempting to authenticate into an account is not – making them nearly impossible to spot.

Fortunately, the process of verifying stolen credentials – or credential stuffing – is not likely to be accomplished manually. This is your opportunity to intervene. Validation is typically automated, which makes credential stuffing a bot problem from the start.
Your ability to stop credential stuffing attacks depends on how well you can detect and mitigate bots. Putting a stop to this activity before account takeovers occur allows you to:

- More easily identify abuse, since login requests generated by bots are easier to catch than account takeovers involving humans.

- Lower the incidence of account takeover attempts by reducing the number of validated credentials available to fraudsters.

- Make your website less attractive to fraudsters, who often move on to less protected targets.

Simply put, a bot is a piece of software running on a server connected to the Internet that interacts with other online entities, such as your website. Multiple bots strung together form a network referred to as a botnet, which can make quick work of an otherwise time-consuming process such as entering hundreds, thousands, or tens of thousands of login credentials. And behind this software is the bot operator – the individual or organization that created the script.

Source: Top Ten Considerations for Bot Management
Once a bot is detected, your response can impact the sustainability of a solution. If an operator notices that you’ve found the bot, it will try to figure out how, and update its software to avoid detection. With profitable account takeover opportunities, credential stuffing attracts some of the most sophisticated bot operators and has a higher rate of bot evolution.

Bots come in many shapes and sizes, ranging from simple scripts to complex automation tools – and continuously change over time. You can gauge the sophistication behind a credential stuffing threat by measuring the pattern of login traffic or the technologies and capabilities utilized.

If you’re only looking for login spikes, much more serious activity can go undetected. Most websites interact with a range of threats every day – from obvious automation to the most evasive bot behavior. A brute-force attack from a handful of IP addresses requires a different strategy than a bot using recorded human behavior with few and sporadic requests per IP address.
Looking at bot sophistication by traffic pattern with a variety of levels detected in a 24-hour period.
Looking at bot technologies and capabilities in escalating sophistication
As detection technologies improve, so do the evasion techniques available to bot operators. An effective bot management strategy isn’t static and must consider the current and future bot landscape to stay ahead of threats. Let’s look at each threat by low, medium, and high sophistication to determine which bot management approach is right for your business.

**LOW SOPHISTICATION**

- Generates large spikes of login requests from a single IP address or multiple addresses, peaking several times higher than legitimate human traffic
- Utilizes randomized user agent generators, browser impersonation, and session replay
- Triggers alerts from traffic management and security tools without specialized bot detection capabilities

The simplest form of credential stuffing begins with one bot making repeated login attempts. The increase in requests coming from a single IP address is easy to catch and block with standard traffic management tools. If only it stayed that way.
Next, operators move to botnets with multiple IP addresses ranging from a few to hundreds, with the amount of login requests from each IP address a fraction of before. Blocking is still possible, but starts getting tedious with the rising number of IPs. Rate limiting can automatically block individual IP addresses that exceed a threshold for the maximum number of requests within a given time. However, operators will likely reduce the request rate to go undetected yet again.

To better mimic traffic generated by a browser, operators then update programs to spoof various request header fields, such as the user agent. A web application firewall (WAF) or in-house tools may stop these still simple bots using custom rules to identify and block specific header fields. However, these solutions quickly become unsustainable as threats evolve.

For example, if you detect a botnet sending login requests from a common user agent, you can create rules that identify and prevent them from passing – but the operator may change the user agent once blocked, and you will need to find it again. Without a specialized bot management solution, you’ll reach a point – usually at rate limiting – where you just don’t have the expertise or resources to keep up.
MEDIUM SOPHISTICATION

- Generates a concentration of requests that stand out, usually occurring overnight, but peaking at a level similar to legitimate traffic
- Utilizes JavaScript and full cookie support
- Requires a bot management technology partner or solution to detect and prevent

Dynamic IPs – hundreds or thousands of bots cycling through IP addresses – can reduce the effectiveness of rate controls. Injecting a JavaScript challenge is often the first step against these harder-to-detect, but still relatively simple bots. But JavaScript is just a programming language – the way you use it in automated attacks determines its effectiveness. Introducing the language to bots that don’t understand it can stop some threats, but not more sophisticated ones.

More developed tools support JavaScript and can get around a challenge. Enter browser fingerprinting – injecting JavaScript not to present a challenge, but to collect identifying information. With browser fingerprinting, the JavaScript collects a variety of characteristics such as screen resolution, browser type, plug-ins and fonts. These details identify if the client is built on an automated or headless browser as well as the unique combination of characteristics that reveal the source.
Once you have the fingerprint, you can analyze the characteristics for anomalies, such as if a browser doesn’t support a specific plug-in – details you can use to identify and respond to the threat. You can also save the fingerprint, so if you see it repeatedly doing the same thing from different devices, such as part of a credential stuffing attack, there’s a much higher likelihood of it being a bot.

Browser fingerprinting is one of the most widely used detection technologies, but nowadays mainstream browser fingerprint spoofing tools exist that are easy to acquire and deploy. A sophisticated bot operator or persistent fraudster can evade browser fingerprinting, making it a less effective deterrent against those attracted to the more lucrative business of credential stuffing.
KEEP PACE WITH INCREASING BOT SOPHISTICATION.

HIGH SOPHISTICATION

- Generates low and slow activity in a 24-hour period from a massively distributed botnet, consisting of thousands or tens of thousands of bots, sending just a few login requests each
- Utilizes disposable IP addresses, browser fingerprint spoofing, and recorded human behavior
- Demands specialized bot detection with advanced behavior anomaly analysis to uncover

With the less sophisticated bot operator, HTTP anomaly detection, JavaScript challenges, and browser fingerprinting can be enough to catch activity. But an operator capable of assembling a massively distributed botnet is likely to get around those strategies. Managing this highly sophisticated threat involves advanced bot detection that can track and analyze anomalies in behavior.

The latest bot management technologies collect behavioral telemetry to distinguish between humans and bots. Behavior anomaly analysis uses measurements from user input devices, such as keyboard strokes and mouse movements from a computer or accelerometer, and gyroscope readings from a mobile phone or tablet. For example, a human cannot physically move a mouse in a perfectly straight line, so a mouse interacting with a website in that manner can’t be a human. When analyzed together, this telemetry can provide a highly accurate assessment of whether a user is a human or a bot.
Of course, bot operators can develop telemetry that appears random to make differentiation more difficult. And when a set of telemetry works, it can be replayed across multiple bots. The key to outsmarting these techniques is in the telemetry analysis.

Since the most sophisticated bots can change their patterns to better mimic human users, the success of behavior anomaly analysis depends on how well it identifies the minute differences that expose activity as non-human. This requires a machine-learning algorithm highly tuned to variances between human and bot behavior.

The key press pattern of a human is sporadic with irregular intervals between each press, compared to the pattern of a bot, which has regular intervals between presses.
The number of login attempts made by humans and bots to a login page for a leading fashion retailer over an 8-day period.

CASE STUDY

After a large attack peaking at more than 131,000 requests per hour, a leading fashion retailer began to block bot traffic with Akamai Bot Manager Premier. Not only did the detected bot login traffic fall to a statistically insignificant amount, but the level of human login traffic did not change.
When it comes to credential stuffing, minimizing false positives is paramount. This is especially true with highly sophisticated bot activity that mimics human behavior. Misidentifying a human visitor as a bot can block your users from their accounts, creating unhappy customers and lost business opportunities.

More than 70% of Ponemon Institute survey respondents agreed that preventing credential stuffing attacks is difficult because fixes that curtail criminals may diminish the web experience of legitimate users.

Advanced machine-learning technology and behavior anomaly analysis used against these more sophisticated threats leads to better accuracy. The more finely tuned the algorithm, the more precise the analysis to minimize performance impact and false positives that can inadvertently block legitimate user logins.
The money you invest in a bot management solution — whether it’s in-house or outsourced, basic or advanced — should be proportionate to the potential financial or brand impact that credential stuffing can have on your business. Usually your interest in this area aligns with fraudsters: The more you have to lose, the more they stand to gain.

You can estimate the impact by quantifying the scope of activity and tying it to known metrics such as:

- **Money lost to fraud.** The average value of fraudulent transactions using stolen credentials — metrics will vary between industries, but include average order value or account balance.

- **Cost of prevented fraud.** Many organizations have anti-fraud solutions priced by the number of lookups — reducing the incidence of compromised accounts lowers the cost of these solutions.

- **Remediation costs.** Catching fraud attempts early reduces remediation expenses — notifying customers to change credentials costs less than assigning a representative to a fraud investigation.

- **Value of lost customer.** Fraudulent transactions can lead to lost customers — most industries have a metric for customer lifetime value.
Here’s an example.

Assumptions:

- 1,000,000 fraudulent login attempts / month
- 20 compromised accounts / month
- $0.01 per lookup for anti-fraud solutions
- $500 average fraudulent transaction value
- $1,000 remediation costs per account
- $2,000 average customer lifetime value
- 20% attrition rate attributed to compromised accounts

\[
\begin{align*}
1,000,000 \times $0.01 &= $10,000 \text{ reduced fraud prevention cost/ month} \\
20 \times $500 &= $10,000 \text{ prevented fraud costs / month} \\
20 \times $1,000 &= $20,000 \text{ prevented remediation costs / month} \\
20 \times 20\% \times $2,000 &= $8,000 \text{ lost customer value/month} \\
$10,000 + $10,000 + $20,000 + $8,000 &= $48,000 \text{ total value/month}
\end{align*}
\]

Add in the cost of potential application downtime from spikes in login requests, and the financial impact can be even higher.
To successfully manage and mitigate the latest bot threats — such as credential stuffing — you need an advanced, purpose-built bot solution with the latest and most advanced detections. Today, that means behavior anomaly analysis and machine-learning algorithms with the lowest possible false positives.

But your bot problems probably extend beyond credential stuffing — web scraping, content aggregation, and good bot management, to name a few — requiring a broader bot management strategy. Key requirements in a comprehensive bot management solution include:

- Dedicated bot detection technology that can meet increasingly sophisticated threats
- The latest, most advanced detections to continue catching bots as they evolve
- Cloud support to handle spikes in traffic that might otherwise overwhelm the login infrastructure
- Highly accurate detection algorithms to preserve legitimate user experiences
- Protection against bots for login pages as well as your entire website
- Advanced and conditional actions that allow you to manage bot traffic, not just mitigate it
- Insight into bot traffic as new methods develop to evade detection

CREDENTIAL STUFFING IS JUST ONE OF MANY BOT PROBLEMS.
For more visibility into online threats, bot management tools should also easily integrate into your overall web security strategy. A complete security solution that includes a WAF, protection from distributed denial of service (DDoS) attacks, and bot management will help you better identify the true nature of threats against your website.

For example, a traffic spike that takes down your login server may first appear to be a DDoS attack. If you only have DDoS protection, stopping the attack may give you the false impression that you’ve mitigated the risk. However, combining DDoS protection with bot management allows you to maintain availability while identifying the root cause – a spike in login requests from credential stuffing.

In addition, integrated user interfaces for DDoS protection, WAF, and bot management solutions allow you to see suspicious activity across applications. And a single destination to whitelist helpful bots, such as search engine crawlers, will help you more efficiently manage online activity. Should a security event occur, you can access a central source to view all attack vectors for faster resolution.
With up to 30% of all web traffic traversing its network daily, including some of the largest and most frequently attacked sites in the world, Akamai is uniquely positioned for deep visibility into legitimate application use as well as the constantly evolving attack behaviors of malicious bots. It has the latest bot detection technologies that are proven to identify the most sophisticated bots today—even those conducting credential stuffing and account takeovers.

Its complete online security portfolio is designed to help customers manage bot traffic on the Akamai cloud delivery platform at the network edge, before reaching their websites and infrastructure. With a wide array of advanced and conditional actions to help control the good bots, the bad bots, and the spectrum of bots in between, Akamai can help enterprises manage the business and IT impacts of bot traffic to protect customers, business, and brand.

CASE STUDY

A Global 500 financial services group found its pensions site, which typically processes 20,000 invalid login attempts per day, began receiving 50,000 invalid login attempts every five minutes. During the attack, the infrastructure struggled as users received session timeouts or were unable to log into their accounts. Quick deployment of Akamai Bot Manager Premier immediately halted the attack and prevented the bot operator from taking out fraudulent loans against actual customer accounts.
In one credential abuse attack, Akamai observed a botnet of nearly 13,000 IP addresses, with each member averaging one login attempt every two hours. Altogether, the botnet sent 167,039 login attempts over 24 hours, and 123,909 unique accounts were targeted.

Source: Improving Credential Abuse Threat Mitigation
Learn more about how to manage and mitigate bot threats such as credential stuffing at www.akamai.com/bots.

Contact us to find out how Akamai’s new advanced bot management technologies can enhance your online security strategy.