WHITE PAPER

Credential Stuffing: How to Keep Criminals from Impacting Your Customers

PRESENTED BY

AMERICAN BANKER

SPONSORED CONTENT FROM

Akamai

Experience the Edge

Is that a customer logging into your website or a bot? Is that a good bot engaged in essential tasks or a bad bot consuming so many resources that it impacts your customers' ability to access your site?

Credential stuffing makes those questions difficult to answer. Credential stuffing is a targeted attack against an organization's website or an application. Criminals use bots – a string of connected computers coordinated together – or scripted applications to automate login attempts with compromised usernames and passwords in order to gain access to accounts.

Credential stuffing is a distinct part of the cybercrime economy, and for criminals, it's a lucrative one. For financial institutions, credential stuffing attacks are incredibly costly. In a 2017 study done with Ponemon Institute, Akamai found that a single credential stuffing campaign could cost a financial institution between $550,000 to $55 million USD including initial account remediation costs, customer notifications, and regulatory fines.[1]

When financial services organizations notify their customers about an incident that requires a change of password, it can create such a negative experience that some customers choose to take their business elsewhere, resulting in lost revenue.

As criminals continue to improve their attack methods, it's more difficult for financial institutions to protect against credential stuffing.

According to the Akamai 2019 State of the Internet / Security Report, financial services is one of the most highly targeted verticals for credential abuse attacks.[2]
The 2020 report found that nearly 20% of the 85,422,079,109 credential abuse attacks observed between December 2017 and November 2019 target clearly identified APIs. Of those targeted APIs, 473,518,955 were in the financial services industry, representing a shift in criminal tactics.

For example, in just one massive credential stuffing campaign, a financial institution was bombarded with 55,141,782 malicious login attempts. This attack was the largest spike in targeted credential abuse Akamai has seen against a financial services organization since we've started tracking such attacks.

As criminals continue to improve their attack methods, it's more difficult for financial institutions to protect against credential stuffing. Distinguishing a bot from a human requires specialized, intelligent security tools to detect credential stuffing attacks and keep the bad guys out, while letting the good guys – your customers – in with as little friction as possible.

Billions of stolen and leaked data records help feed credential stuffing since these compromised data records – with their associated passwords – are easy and cheap for criminals to access on the dark web.

How Credential Stuffing Works

Credential stuffing is a multi-step process:

1. **The attacker picks targets,** most likely based on popularity, brand reputation, and what credentials are available on the dark web.
2. **Armed with a list of stolen username and password combinations,** the attacker uses a botnet or automated tool to repeatedly attempt to login until they are successful.
3. **Once the attacker determines which credentials work,** they either login to the accounts and take them over for financial gain or resell the validated credentials as individual accounts on the dark web.

A key issue leading to the growth of credential stuffing is the reuse of login credentials, or password recycling. Customers often use the same credentials across multiple accounts, such as using the same username and password for banking, email, loyalty programs, streaming media services, and retail shopping – all of which are popular targets for criminals. A criminal possessing a valid reused credential combination has the virtual keys to the customer's kingdom, thus making every business susceptible to credential stuffing, regardless of whether or not the targeted company has been breached.

Credential Stuffing: Tough to Detect

Credential stuffing is done stealthily, and since attackers often change the methods used to bypass defenses and impersonate authorized customers, it's difficult to detect. In a 2017 Ponemon Institute report sponsored by Akamai, 32% of respondents say that they lack visibility into credential stuffing attacks and 30% say they were unable to detect and mitigate attacks. Seventy percent (70%) say their organization lacks credential stuffing defenses.[3] The percentage of organizations vulnerable to credential stuffing continues to rise.

However, it is fair to say that protecting against credential stuffing is a balancing act. What if the customer simply mistyped a password? Customers who are mistakenly shut out of their accounts understandably get frustrated and angry. False positives are a very real concern; it's difficult to protect against attacks without increasing customer friction and possibly losing revenue.

Indeed, the Ponemon study reports that 71% of respondents say that preventing credential stuffing attacks is difficult because the fixes might diminish the web experience for legitimate customers.[4]

Bots are only part of the problem. Criminals also use automated tools for attacks. In fact, Akamai detects tools like Snipr, STORM, or Sentry MBA as part of our defenses. These automated tools vary in sophistication. Some – such as a single bot making repeated login attempts from a single IP address – are easy to catch with standard IP traffic management tools. Others are more difficult to catch since the login attempts come from hundreds or thousands of IP addresses.

During an attack, criminals will conduct reconnaissance and testing to determine the victim's detection thresholds, and modify attack rates as needed, such as sending a few login requests over a 24-hour period, to stay below the radar.

During an attack, criminals will conduct reconnaissance and testing to determine the victim's detection thresholds, and modify attack rates as needed, such as sending a few login requests over a 24-hour period, to stay below the radar. Other tactics include using disposable IP addresses, browser fingerprint spoofing, and recorded human behavior to avoid detection. These techniques evolve daily.

How Bots Outsmart Traditional Tools

Since login information is legitimate, but a machine and not a person is attempting to login to the account, traditional tools such as web application firewalls (WAF) focused on network or web-based attacks won't catch credential stuffing. Instead, financial institutions need specialized intelligent bot detection and management tools to defend against credential stuffing.

While financial institutions have long used CAPTCHA in an attempt to limit credential stuffing success, CAPTCHA increases customer friction. Customers are not enamored with typing out the distorted text that appears on their screen or selecting all the boxes containing road signs to pass a test. In addition, criminals can successfully trick CAPTCHA.[5]

Another protection method financial institutions use is rate limiting, which blocks IP addresses that exceed a threshold for the maximum number of requests within a time frame. However, criminals figure out the threshold and operate below it. If the financial institution limits login attempts to five, criminals will attack in series of four attempts to avoid detection.

The Two-Pronged Solution: Detecting Credential Stuffing at Login Combined with Customer Education

The most prudent credential stuffing protection is to prevent an attacker from validating credentials by implementing defenses in front of consumer login endpoints and APIs. This approach, combined with educating customers about good password hygiene, is a critical part of a strong foundation to prevent credential stuffing.

At Login: A Bot Management Solution

A bot management solution that protects against credential stuffing should complement your other enterprise fraud management tools already in place, and easily integrate into the overall security strategy. This provides defense in depth: if one security capability fails, the next capability in the chain will stop it.

The most effective bot detection tools combine advanced behavior anomaly analysis and behavioral telemetry with machine learning. For example, measurements from user input devices (i.e., mouse movements, keyboard strokes, touch screen events, and gyroscope/accelerometer readings), can distinguish between automated tools and humans. If the mobile device moves – ever so slightly – it's likely handled by a human. A perfectly straight mouse movement? This could be one of several indicators pointing to a bot or automated access attempt.

The bot management solution should include both a WAF and protection from distributed denial of service (DDoS) attacks. A traffic spike that appears to be a DDoS attack to take down your server, may actually be a spike in login requests from credential stuffing. Comprehensive tools offering good monitoring are the only way to determine the root cause.

Customer Education

Another proactive way to decrease credential stuffing attempts starts with your customers. Educate customers about the dangers of reusing passwords or using weak or easily guessed passwords.[6] *PCMag* found that 35% of users don't change their passwords unless prompted. Google found that 52% of users reuse passwords for multiple accounts–and an additional 13% use the same password for all their accounts.[7]

Educate customers about the dangers of reusing passwords or using weak or easily guessed passwords.[6] *PCMag* found that 35% of users don't change their passwords unless prompted. Google found that 52% of users reuse passwords for multiple accounts–and an additional 13% use the same password for all their accounts.[7]

And it's not just customers. There have been media reports about phone providers and other organizations – and even the U.S. government – using 0000 or other easily guessed passwords for their default router passwords.

Stop Cybercrime from Credential Abuse:
11 Questions to Ask a Potential Vendor

Use these questions to find a bot management provider that can effectively protect your financial institution from credential stuffing attacks:

1. How do you work with existing security and fraud teams?
2. Can you detect fraud across constantly changing attack vectors and geographies?
3. How does your tool scale to meet global demand?
4. What is the typical implementation timeline for your products and what integration support do you offer?
5. Do you provide centralized management and situational awareness?
6. What security expertise and talent services do you offer?
7. Do you support customization and DevOps?
8. Do you meet financial industry compliance and privacy regulatory requirements?
9. How does your solution minimize customer friction and reduce false positives?
10. What is your innovation road map and your success rate in delivering on it?
11. How do you leverage threat intelligence and invest in research to optimize discovery?

Stop Credential Stuffing in Its Tracks

Credential stuffing is difficult to detect, but that doesn't mean financial institutions should sit back, wait for an attack, and attempt to minimize the damages. Instead, financial institutions can stop credential stuffing in its tracks at the point of login with a bot management tool that uses advanced behavior anomaly analysis and behavioral telemetry–based tools.

Cybercrime such as credential stuffing continues to evolve – and a shortage of security talent makes it difficult for financial institutions to find or afford the security expertise they need in-house. A better approach is to work with an outside partner that has insights into constantly changing attack vectors and the expertise to stop bots and automated tools before criminals can even attempt to login.

SOURCES

1) https://content.akamai.com/us-en-pg10079-the-cost-of-credential-stuffing.html

2) https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-a-year-in-review-report-2019.pdf

3) https://content.akamai.com/us-en-pg10079-the-cost-of-credential-stuffing.html

4) https://content.akamai.com/us-en-pg10079-the-cost-of-credential-stuffing.html

5) https://www.wired.co.uk/article/google-captcha-recaptcha

6) https://www.pcmag.com/news/35-percent-of-people-never-change-their-passwords

7) http://services.google.com/fh/files/blogs/google_security_infographic.pdf

Akamai

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 05/20.