Debevoise & Plimpton | Data Blog

CYBERSECURITY

Credential Stuffing Continues: Practical Guidance to Protect Customer Information

BY: AVI GESSER, MICHAEL R. ROBERTS AND SUCHITA MANDAVILLI BRUNDAGE - JANUARY 31, 2022

In September 2020, we wrote about the risks of credential stuffing attacks following the New York Attorney General's (NYAG) settlement with Dunkin' Donuts. Since then, these attacks have continued, and regulators' expectations of companies' efforts to reduce the risk of credential stuffing attacks for their customers' online accounts have increased. On January 5, 2022, the NYAG's Bureau of Internet and Technology published a *Business Guide for Credential Stuffing Attacks*, which was the result of a months-long investigation uncovering widespread failures of

companies to effectively combat credential stuffing attacks on their customers. In this Debevoise Data Blog post, we discuss why credential stuffing attacks continue to be a significant risk for some companies and ways to reduce that risk.

What Is Credential Stuffing?

In order to remember the passwords for our ever-increasing number of online credentials, most of us reuse the same or similar credentials across multiple websites and apps. As a result, if attackers compromise one set of our online credentials, they can use automated tools to see if those same (or very similar) credentials work for other accounts and websites.

Threat actors can acquire valid customer credentials through phishing and hacking, or by purchasing bulk credentials on the dark web that were stolen by others. As more companies fall victim to data breaches, the pool of compromised credentials that can be used for these attacks grows and the overall risk increases.

Like phishing, credential stuffing is often not an attack by itself, but a means to gain access to an online account to launch another attack (e.g., obtain additional sensitive or personal information, load ransomware, send phishing emails, make purchases using the compromised account, transfer funds to the attackers' account, exfiltrate confidential personal or company data, etc.).

Credential stuffing can be hard to defend against because the attackers are using valid credentials to access an account. Companies therefore need to distinguish between logins by authorized users and logins by threat actors, when both look identical in terms of the credentials used.

Account Takeovers

Credential stuffing attacks are often used by attackers to take over a customer's online banking or investment account, with the goal of transferring assets to an account controlled by the attacker or making purchases with debit or credit card information. Attackers also cancel purchases or return items, and direct the company to issue a refund to the attacker's account.

Ways to Protect Customers' Accounts and Combat Credential Stuffing

Because of these risks, regulators expect companies to take proactive steps to protect customers' accounts from credential stuffing attacks. In the press release accompanying the issuance of its *Business Guide*, NYAG Letitia James stated that businesses "have the responsibility to take appropriate action to protect their customers' online accounts and this guide lays out critical safeguards companies can use in the fight against credential stuffing." Below are several measures discussed in the NYAG *Business Guide*, as well as regulatory guidance from the New York State

Department of Financial Services ("DFS") and the Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") to combat credential stuffing attacks.

Multifactor Authentication ("MFA")

MFA requires users to provide at least two separate authentication factors to access their online account. These factors typically fall into three categories: (1) something you know (like a username and password), (2) something you have (like a one-time passcode sent to a user's mobile phone or obtained from an app) or (3) something you are (like a fingerprint).

Implementing MFA greatly reduces the risk of credential stuffing because the attacker can no longer access an account with just a valid username and password, and it is difficult for the attacker to obtain the second factor without direct access to the customer's phone. That said, attackers can obtain second-factor codes. For example, if a customer's email credentials are among those that have been compromised, then the attacker can obtain the second-factor code when it is sent to the customer's compromised email account. Because of this vulnerability, some companies have stopped sending second-factor passcodes via email, and only send them by SMS or through apps. Even passcodes sent via SMS can be vulnerable due to SIM swapping or SIM jacking, which is when the threat actor obtains control of a victim's phone number by activating a new SIM card connected to the victim's phone number on a phone that the threat actor controls—but this kind of attack requires a lot of work by the threat actor. Finally, attackers can trick users into giving up the second-factor code that has been sent to them through phishing scams and the use of fake websites that look like the company's real website.

Although two-factor authentication is common for employees who are logging into their work environment remotely, it is a less common requirement for customers logging into online accounts because of the friction that it can create in getting access to a website or app. And even when MFA is employed for customer accounts, the *Business Guide* notes that many hackers were able to circumvent preexisting MFA controls because these controls were not implemented correctly, rendering them ineffective. Businesses who have employed MFA for either customer or employee accounts should review DFS's recent MFA guidance explaining common MFA pitfalls and ways to avoid them.

Trusted Devices

A true MFA program requires the use of a second factor every time that users log into their online accounts. Given the lost time that this can add to a user experience, some companies have opted for a "trusted device" program, which only requires users to use a second factor when they log in with a new device (or in some cases, from a new location). Once a device is recognized by the company, it becomes "trusted," and users only need their credentials (without a second factor) to sign into their account from that device going forward. Some companies also require customers to confirm that the device they are logging in from should in fact be trusted going forward, and automatically un-

trust a device when it has not been used to log into the account for a set period of time.

Password Controls

Companies should periodically review and update their password requirements to ensure that customer passwords are consistent with industry standards for strength, length, type and frequency of changing passwords. Some companies have moved to a "passwordless" authentication model by avoiding the "something you know" factor entirely, and instead relying on a factor that "you have" (e.g., an email address, telephone number or device that is known to be associated with a specific individual) and/or a factor that "you are" (e.g., biometrics such as facial recognition, fingerprint or voice signature). While passwordless authentication can significantly reduce the risk of credential stuffing in some circumstances, it can also create new challenges in terms of the collection and use of biometric data, which can create onerous legal obligations in terms of consents, storage, disposal and use.

Detecting Suspicious Logins

Another way to stop credential stuffing is to detect suspicious logins. For example, if a person logs into the same account from two locations that are thousands of miles apart in a short period of time (i.e., impossible travel), then the company can temporarily disable access to that account because one of those logins is likely fraudulent. Other suspicious login detection measures involve identifying IP addresses that have been associated with fraud or with a location that is unlikely to be connected to the authorized user and blocking them. Many companies create an IP address "allow list" and "block or deny list." Businesses can also subscribe to third-party intelligence feeds to stay up-to-date on external IP "deny lists," and block activity from these IP addresses.

Login Attempt Monitoring, Bot Detection and Rate Limiting

Because threat actors conduct their credential stuffing using automated tools, these attacks often involve large spikes in login attempts, which can be monitored and detected. Automated customer activity monitoring tools conduct 24/7 surveillance, provide accurate real-time and baseline measurements of customer activity, and can alert security personnel if key activity metrics exceed pre-set thresholds. Companies can also implement IP-address-based rate limiting, which limits the number of times that a single IP address can take certain actions, like attempts to log into an account. If a single IP address exceeds a set limit of login attempts, then the company can block it for a period of time.

Bot-detection tools can identify and block bot-generated traffic, even when that traffic has been disguised to mirror human login behavior. One common bot-detection system is CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart. The SEC OCIE recommended deploying some form of CAPTCHA, which requires users to perform a task that is relatively easy for humans, but hard for bots (e.g., identifying a particular object within a grid

of pictures, or wavy letters that appear against a background of noise), to combat automated scripts used in credential stuffing attacks. CAPTCHA systems are often limited to situations where customers log in from a new device or enter an incorrect password more than once. With CAPTCHA solutions becoming more advanced as time goes on, companies may want to periodically review whether their CAPTCHA solutions remains in step with market practice and are configured to operate in a way proportionate to the companies' risk of credential stuffing. That said, even the most sophisticated CAPTCHA solutions can struggle to tackle the risk of software-sourced and crowd-sourced CAPTCHA puzzle solving, where attackers pay humans to solve them and help attackers fly under the radar.

Web Application Firewalls ("WAFs") protect applications from malicious activity by serving as a traffic "checkpoint" between the application and the Internet. WAFs operate through a set of rules to filter information flow. The Bureau's *Business Guide* specifically noted that WAF features like rate limiting (discussed above) and HTTP request analysis are helpful to prevent credential stuffing attacks. HTTP request analysis involves identifying potentially malicious traffic from header information and other metadata, and blocking access accordingly. WAFs can block requests that originate from malicious networks or IP addresses, requests made from unusual locations outside the expected customer geographic area, requests originating from browsers with common credential stuffing tool attributes, and more. WAFs also provide helpful monitoring functions that can assist businesses in early and efficient detection of credential stuffing attacks, as discussed above.

Preventing Suspicious Account Activity

Companies can also implement additional controls for online activity that is highly associated with account takeovers, such as changing the phone number or password associated with the account, and transfers of funds to certain banks, countries or financial apps. These controls may include sending the user a second-factor code that must be authenticated before the requested activity is allowed to proceed.

Online Monitoring and Threat Intelligence

Attackers often use fraudulent company websites to capture the credentials of customers of that company. To protect against these kinds of social engineering attacks, companies can work with vendors to identify and take down fraudulent websites posing as the company's website. Companies can also purchase URLs likely to be used for such cybersquatting.

Companies can conduct dark web monitoring and password testing programs. This involves searching the dark web for lists of leaked usernames/passwords and performing tests to see whether any current customer accounts are susceptible to credential stuffing attacks. Additionally, companies can reference lists of known exposed passwords and create password "block lists" to discourage or prevent customers from using weak passwords.

Customer Education

One final tool that companies can use to prevent credential stuffing is alerting users to the latest threats and reminding them about best practices to protect their online accounts.

Conclusion

Credential stuffing and account takeovers remain a significant cyber threat for many companies, for which is there no one-size-fits-all solution. To successfully reduce this risk without significantly impacting customers' user experience, companies usually have to experiment with several of the measures discussed above, and based on their risk and testing experience, deploy a bespoke multi-prong strategy.

To subscribe to the Data Blog, please click here.

The authors would like to thank Debevoise law clerks Jacob Apkon and Elise Coletta for their contribution to this article.

Avi Gesser

Avi Gesser is Co-Chair of the Debevoise Data Strategy & Security Group. His practice focuses on advising major companies on a wide range of cybersecurity, privacy and artificial intelligence matters. He can be reached at agesser@debevoise.com.

Michael R. Roberts

Michael R. Roberts is a senior associate in Debevoise & Plimpton's global Data Strategy and Security Group and a member of the firm's Litigation Department. His practice focuses on privacy, cybersecurity, data protection and emerging technology matters. He advises clients on regulatory investigations, incident response, crisis management strategies, privacy and information security program development and management, as well as compliance counseling regarding evolving laws and regulations, such as the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), and the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation. He can be reached at mrroberts@debevoise.com.

Suchita Mandavilli Brundage

Suchita Mandavilli Brundage is an associate in Debevoise's Litigation Department. She can be reached at smbrundage@debevoise.com.

PREV POST

Webcast – AI Benefits and Risks for the Insurance Industry: A Regulator's View

NEXT POST

CCPA Enforcement Update: California AG Announces a New Enforcement Sweep Targeting Customer Loyalty Programs

Related Posts

Four Takeaways from the SEC's Proposed Cybersecurity Rules

FEBRUARY 16, 2022

Webcast – Fireside Chat with NYDFS Cyber Chief Justin Herring

FEBRUARY 5, 2022

SEC Cybersecurity Update: Ch Gensler Offers Insight into Upcoming Regulation

JANUARY 25, 2022