CARLTON FIELDS

Credential Stuffing: Where Passwords Go When They Are Stolen and Some Strategies for Defense and Incident Response

August 24, 2021

Credential stuffing is a growing cyberattack method in which cybercriminals use a set of thousands of compromised user credentials, stolen from one company, to attempt a breach into another company's secured system. It is enabled by both automated bots (used to "stuff" credentials into online login pages) and the increasing supply of stolen usernames and passwords, known as credential pairs. This article describes this fraud and provides some guidance for corporate counsel and security professionals on addressing it in the context of state data breach law.

The Scheme

As an example, let us assume there was a hack of the corporate systems of an email service provider, "Company Alpha," which compromises a database of a few thousand credential pairs for users of Company Alpha's email service. The threat actor may use that database in at least two nefarious ways.

First, the threat actor may try to use those credential pairs against Company Alpha's users by hacking directly into the users' email accounts. These exploits can be lucrative in the short term, until Company Alpha or its users discover the hack and (hopefully) reset the accounts to lock out the threat actors from these secondary breaches.

Second, the threat actor may sell that database on the dark web, either as a set of credentials of Company Alpha's users or simply as a generic database of usernames and passwords. The value of this database to hack Alpha's user accounts plummets once the breach is disclosed, for the reason stated above. But there is still value to the generic database of possible credential pairs to hack other organizations. This market thrives solely because of consumers' tendency — even in 2021, with all we know about cybersecurity — to reuse passwords across multiple websites.

The criminals who bought the generic database will then create or use a bot to run these credential pairs from Company Alpha against other companies' secured systems. Common targets include online commerce sites, social media sites, and banks — all of which will be referred to here as "Company Beta." This new threat actor then either directly accesses individual consumer accounts at Company Beta or monetizes the "new" database by advertising that they have credential pairs verified to match Company Beta's user accounts.

Strategies

Multifactor Authentication. Company Alpha combats the scheme with traditional perimeter and in-depth defenses, including encryption of credential pairs at rest on the corporate system, to prevent the credential pairs from getting stolen in a batch in the first place. But Company Beta's approach requires some more nuance, as the threat is not to the credential pairs in the back-office system but to the consumer-facing portion of its services, through the login screens. One basic approach is simply to warn consumers to use a unique password, and not reuse old passwords, when setting up the original relationship. As might be expected, such warnings vary in effectiveness. A more robust approach is to turn on or require multifactor authentication (MFA) for consumers so that a compromised credential pair alone is insufficient to access the account.

Login and User Monitoring. Some companies go further and have defense systems designed to monitor login attempts from a single IP address across accounts, login attempts into an account at unusual times of the day, or from foreign IP addresses. This approach can be effective at detecting credential stuffing attacks in real time. Certain variations of this monitoring require tracking user behavior information, and for states that have privacy statutes, some exceptions may help avoid privacy compliance problems.

Company Beta may see network activity that a bot is simply testing credential pairs. If this happens, its security personnel might attempt to block that activity. Additionally, the company might next examine this "testing" to determine if this was just a test or if the successful login resulted in an actual account compromise. If the latter, the company will then determine whether "personal information" was accessed or leaked, potentially triggering notice obligations under state data breach laws.

Dark Web Monitoring. Another technique is to actively monitor the dark web, typically through a third-party service provider, to find credential pairs that are advertised as accessing the company's website. That approach is becoming more common as such vendor services proliferate, although it can raise hard legal and practical questions about what a company like Company Beta should do once it learns that credential pairs are out there that may match those of consumers on its own systems.

The law on Company Beta's obligations here is evolving, and a response will be highly fact-dependent. A risk-based approach is common. But with more dark web monitoring becoming available, companies should have a clear plan on what to do if they find potential credential databases, which might include escalating the discovery to their legal department or risk professionals.

A common approach with a dark web alert is to reset the vulnerable accounts, if knowable, and then assess the system for suspicious login activity to determine whether disclosure notification under state data breach law is required. There are wrinkles, though. Most state data breach laws cover usernames and passwords, but those are addressed to Company Alpha's scenario, where a hack of one company exposes credential pairs to access consumer accounts with that same company. Those state data breach laws are not clearly applicable to Company Beta's posture, where a second company (Beta) learns that thousands of credential pairs (stolen from Alpha or otherwise) may include one or more pairs that could match Beta's consumers' accounts or that are being advertised as such. That is, Company Beta has not had credential pairs taken from its system. Company Alpha was breached, and so Company Alpha has the immediate obligation to disclose this to its consumers. Beta, on the other hand, could argue that it does not have any obligation until it confirms a compromise of one or more of its user accounts and access to personal information, regardless of what it finds on the dark web.

Significance

Once a company suspects a breach of its users' accounts, the legal risk of taking no action is substantial. For example, about a year ago, the New York attorney general announced a settlement of an enforcement action against Dunkin' Brands Inc., franchisor of Dunkin' Donuts. The AG alleged that Dunkin's online customer accounts were targeted in a credential stuffing attack whereby threat actors gained access to customers' stored-value cards, which the attacker could then use or sell online. The AG alleged that a third-party app developer had notified Dunkin and provided a list of nearly 20,000 accounts compromised in just five days. Despite this, Dunkin reportedly failed to investigate, determine if personal information was acquired, notify customers, or reset accounts.

The takeaway from all this is that if a company is aware of a possible compromise to its systems — regardless of whose fault it is or how it occurred — it should take some action to investigate, protect consumers, and, if needed, notify the consumers. Companies are best suited to think strategically about how to protect their data and to include their legal counsel in discussions about dark web monitoring and consider including these concerns in their incident response planning.

Authored By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology