SpyCloud

INDUSTRY: Travel & Hospitality

CASE STUDY

Top 10 **Travel Booking Site** Discovers Up to 11,000 Exposed Customer Credentials per Hour with SpyCloud

CHALLENGE

Preventing account takeover begins with monitoring the dark web, but without the ability to match user accounts with a database of exposed credentials, a top 10 travel booking site was vulnerable to attack.

SOLUTION

The booking company uses the SpyCloud API to continually monitor and protect customer accounts against SpyCloud's massive database of exposed emails and plaintext passwords.

RESULT

With automated dark web monitoring, the company discovers thousands of exposed customer accounts every hour, enabling the company to better protect their customers from account takeover.

CHALLENGE: PREVENTING ACCOUNT TAKEOVER AFTER A BREACH

Account takeover (ATO) is a growing problem that impacts virtually every industry, particularly those organizations with an e-commerce capability. When cyber criminals steal usernames and passwords or purchase them from breach data on the dark web, both consumer and company can suffer.

The risk of ATO keeps security leaders up at night. Beyond the financial loss, ATO is often the dreaded aftermath of a security breach and can continue to cause damage for years. For one of the top 10 travel site's Account Security Group, keeping constant watch over their user accounts is a full-time job that would greatly benefit from automation.

"It has always been our goal to prevent, detect and remediate any account security threat," says a security leader at the online travel company. "We wanted a solution that would enable us to continually evaluate our security stack and if we detect any gaps in our strategy, take immediate action to protect our customers and our brand, starting with ATO prevention."

SOLUTION: IDENTIFY EXPOSED CREDENTIALS EARLY AND RAPIDLY

SpyCloud always has its ear to the ground in the deep and dark web. Through proprietary tools, techniques and technologies, SpyCloud is able to detect corporate breaches earlier than any other company. The earlier exposed credentials are discovered, the more likely a future breach can be prevented.

To prevent a breach, ATO and ongoing fraud from happening, this top 10 travel booking site turned to SpyCloud, recognizing the value of the detailed, real-time, accurate data SpyCloud provides. They chose to work with SpyCloud to launch a new initiative to automatically detect exposed customer credentials and alert security leaders early in the process, before criminals have the opportunity to take over the account and cause damage.

The company uses SpyCloud data as part of their account stuffing attack monitoring. For each login attempt to their domains, they initiate an out-of-band SpyCloud check for an account match. They then check match alerts against SpyCloud's recorded spikes in account stuffing attacks to identify any correlations.

> *The SpyCloud data reveals which accounts are compromised so we can force the account down an alternate road that includes a second step in the verification process. This is typically requiring the account owner to answer security questions or engage in two-step multi-factor authentication.* ***Without the SpyCloud data, we would be in constant risk for attacks we never saw coming.***

"We use SpyCloud to detect the ATO storms - when an attacker targets our system with a list of breached credentials," says the security leader at the company. "The SpyCloud data reveals which accounts are compromised so we can force the account down an alternate road that includes a second step in the verification process. This is typically requiring the account owner to answer security questions or engage in two-step multi-factor authentication. Without the SpyCloud data, we would be in constant risk for attacks we never saw coming. We may not be able to stop every breach, but we feel we are being more proactive and have dramatically improved our security stance."

RESULT: THOUSANDS OF EXPOSED CREDENTIALS DISCOVERED EVERY HOUR

One of the unique aspects of SpyCloud is the ability to discover direct matches with emails and passwords. Identifying exposed emails is not enough and doesn't indicate the account has been compromised. With SpyCloud's proprietary password cracking methodology, more passwords can be cracked, unencrypted and operationalized. In fact, SpyCloud owns the largest database of emails and plaintext passwords, eight billion and counting.

"SpyCloud allows us to see where we are vulnerable in order for us to fortify those potential entry points," says the security leader. "With the SpyCloud database constantly updated, we can continually monitor our customer base with the freshest, most usable data available. Using the SpyCloud data, we discover anywhere from 3,000 to 11,000 direct matches per hour. Every one of those exposed accounts could have led to account takeover. "

While the SpyCloud solution does include the capability for users to automatically remediate accounts with matches to breach records, typically forcing a password reset, the travel company prefers to go down the PII route for now. It's mission to reduce friction in the booking process presents unique challenges.

By forcing a password reset during the login process, customers are faced with what the company believes is potential friction. "For now, we are using SpyCloud simply for monitoring, but we are aware the solution can do much more," says the security leader. "We are evaluating our options and are considering moving towards being more proactive without compromising our mission. The fact that SpyCloud is customizable to our needs now but also scalable to where we may go in the future is one of the reasons we chose their solution."

> *"Using the SpyCloud data, we discover anywhere from **3,000 to 11,000 direct matches per hour.** Every one of those exposed accounts could have led to account takeover.*