SpyCloud

Case Study

SpyCloud Protects Active Domain Users from Account Takeover

Global Networking Company

Overview

The global IT and networking company profiled is a recognized technology leader with approximately 75,000 employees and annual revenue of nearly $50 billion. Security is a primary focus of its digitization strategy and the company uses a multi-pronged approach to ensure its systems, employees and customers are protected.

Challenge

Discovering exposed user credentials across the global networking company's many domains proved to be challenging using old, redundant, and undecrypted password data from an incomplete solution.

Solution

The technology company automatically monitors domain user accounts using fresh data pulled from the SpyCloud database via an API, giving the company time to remediate before accounts are compromised.

Result

With the SpyCloud exposure data at their fingertips, the company generates detailed reports that enable earlier remediation as well as justifying the value of their investment in account takeover prevention technology.

SpyCloud

Discovering Compromised User Accounts Early

The technology company is well-aware of security risks that seem to never end. Its focus on protecting its assets and users motivates security leaders to continually implement modern solutions to combat the threats.

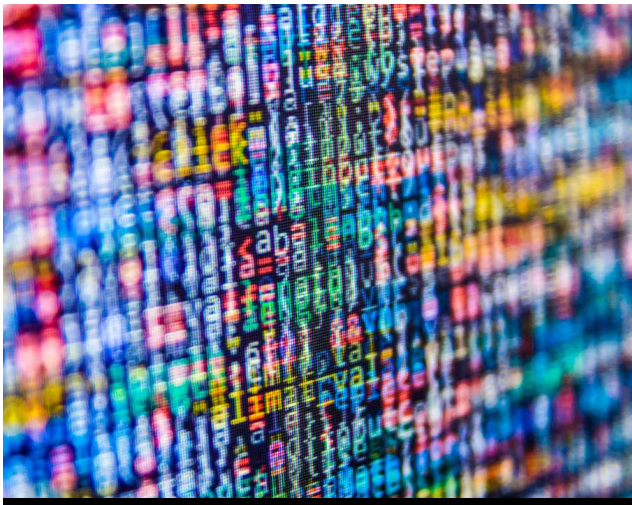
One of the growing challenges is protecting usernames and passwords from being compromised. When users select a password to log into internal company domains, they establish a connection point that criminals are all too quick to leverage.

The primary problem is directly linked to reused passwords. When employees use the same or slightly varied password across multiple accounts, it's like a neon light flashing for criminals. While this introduces risk for every organization, this particular company has more than their share of corporate domains to protect. Through acquisitions, they have accumulated multiple domains, each with its own user base.

The existing security products they were using were intended to monitor the dark web and notify security leaders of any compromised accounts. What they received instead was old and redundant data that was discovered well after the credentials had already been stolen and sold on underground markets. Further, the previous vendor was only able to provide exposed encrypted password hashes much of the time, making the data inactionable. For a company who takes security seriously, a better solution had to be found.

Detailed Exposure Data that Triggers Automated Remediation

The technology company was intrigued by the quality and quantity of data that SpyCloud curates, particularly with the number of plaintext passwords that are directly matched to a username. SpyCloud has recovered the largest database of compromised accounts, has cracked the most amount of encrypted password hashes into plaintext, and is constantly ingesting more breach data sooner after a breach than any other company.



> "Great data is wonderful, but the way SpyCloud operationalizes it for us has been invaluable in our efforts to justify our investment in this security technology."

When compromised credentials are discovered earlier in the account takeover lifecycle, companies like this one can take action before criminals use the credentials in stuffing attacks to gain access into the organization.

"The SpyCloud data has proven to be of very high quality and we saw instant value," says a security manager within the technology company.

"The SpyCloud model lends itself well to driving the level of automation required for our use cases."

For the technology company, automation is key to efficiency, accuracy and speed. They have automated most of the discovery and remediation process using the SpyCloud API to pull breach records across all of their domains to form a watchlist that is forwarded to the security manager. The security team separates external and internal account holders of their main domain, and external account users are notified directly of compromised credentials.

Another process is initiated for internal account holders. For these accounts, answers to a series of questions direct the type of remediation effort: has the breach record been seen before? Is the account still active? Does the account belong to an executive, administrator or service account?

The technology company has also built their own internal "Credentials Leak Notification Dashboard" that monitors the value SpyCloud is providing. This dashboard contains monthly reports of the leaks as well as the victims who were notified, the notification timeline, and the specific accounts that have experienced more than one breach.

More Exposures Discovered Than Ever Before

In just one quarter, the IT and technology company was able to use the SpyCloud data to notify more than 3,600 users that their credentials had been exposed These are active user accounts that were threatening the enterprise without users realizing they were playing a role in security risk. Today, the company is confident they are catching exposures and using the data to educate users on ways to fortify their passwords going forward.

Using the API, the reports in the company's dashboard contain all of the relevant data pulled directly from the SpyCloud database, giving the company the information they need to take appropriate and immediate action.

"The SpyCloud data provides us with the details of not only the exposures but how we are distilling the data and deriving value from the SpyCloud solution," says the manager. "Great data is wonderful, but the way SpyCloud operationalizes it for us has been invaluable in our efforts to justify our investment in this security technology."

SpyCloud

About SpyCloud

SpyCloud transforms recaptured data to protect businesses from cyberattacks. Its products leverage a proprietary engine that collects, curates, enriches and analyzes data from the criminal underground, driving action so enterprises can proactively prevent account takeover and ransomware, and protect their business and consumers from online fraud. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to over 150 cybersecurity experts who aim to make the internet a safer place.

Enterprise Protection

Prevent account takeover that can lead to ransomware.

Learn More

Consumer Protection

Combat account takeover and online fraud.

Learn More

Investigations

Unmask criminals attempting to harm your business.

Learn More

Data Partnerships

Enhance your solution with SpyCloud's data.

Learn More