SpyCloud

Case Study

Protecting a Fortune 100 Financial Services Company

Investigating the Global Threat Landscape

Overview

One of the many large customers using the full set of SpyCloud data and research tools is a Fortune 100 financial services provider. This organization agreed to anonymously share details of their strategy for investigating and determining the credibility of threats to their consumers, employees, partners, and acquisition targets. For this security team, SpyCloud's solutions have become key among the complex set of tools used to alert customers to threats, evaluate the risk of new business opportunities, understand the plans of cybercriminals, and hunt down fraudsters.

Challenge

With high-value customer accounts on the line, this financial services company wanted to sharpen their account takeover prevention program to prevent more online fraud, as well as enhance their threat intelligence team's investigations with breach data beyond what they could collect on their own.

Solution

SpyCloud enables this firm to identify and remediate compromised consumer passwords at scale to lock out criminals. SpyCloud's robust dataset also enriches the information the threat intelligence team can use to investigate fraud – which is important given that they typically start with only a few pieces of information.

Result

Today, the firm protects millions of consumers around the world from account takeover fraud with SpyCloud. In their fraud investigations, SpyCloud data facilitates connections that weren't possible before, helping the threat intel team get more out of their other data sources and deliver their findings with a higher degree of confidence.

SpyCloud

Threat Hunting

The financial services organisations worldwide threat intel team uses a two-pronged approach to identifying, classifying and responding to threats. A tactical analysis team tracks the tactics, techniques, and procedures (TTPs) threat actors are using to target the organization, then determines response strategies depending on the type of threat, be it ransomware, malware, phishing, or credential stuffing.

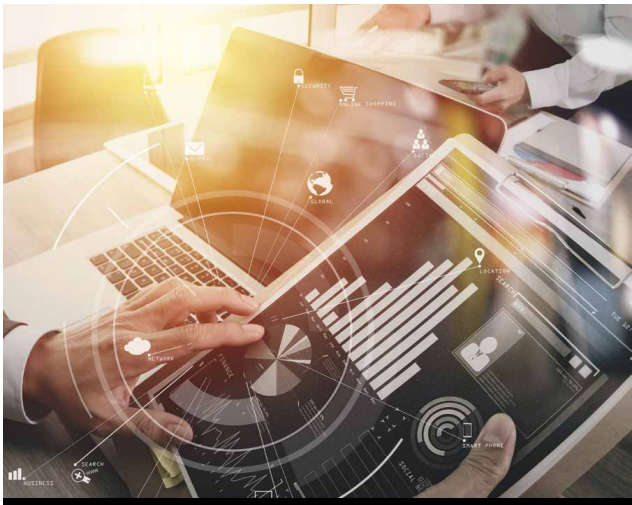
A strategic analysis team investigates the perpetrators behind these attacks. The strategic analysis team identifies the individuals or groups who carry out attacks or share information related to the organization's protections with other cybercriminals.

SpyCloud's data helps these teams:

- Protect consumer accounts from fraud by detecting and remediating exposed credentials.
- Attribute threats to specific individuals or groups of actors and gather evidence for law enforcement.
- Develop risk profiles on partners, vendors, and acquisition targets to protect the organization from inheriting risks through third parties.

Fraud Prevention and Investigation

Preventing fraud is the primary objective for this financial services firm, and SpyCloud helps by giving the fraud team reliable and fast access to breach data that can help prevent account takeovers. In these attacks, criminals use lists of known username and password pairs, often obtained from breaches, to attempt to log into financial accounts. Once in, they may change key account information to lock out the rightful owner and siphon funds elsewhere. Other tools and tactics are used depending on the criminals' ultimate plan to monetize these stolen accounts – for example, some may be resold on the underground market – but stopping account takeovers in the first place is the best way to prevent financial fraud.



> "If you're an organization that's not running on a Zero Trust model, then you have no idea what threats you're allowing into your environment."

Among companies monitoring the dark web and cybercriminal underground, SpyCloud typically recovers, curates, and gets breach data into customers' hands the fastest, thanks to its human intelligence-driven approach. This means customers like this Fortune 100 financial services organization can act on SpyCloud data quickly, alerting compromised customers before cybercriminals can monetize their information.

The task of protecting consumers for this organization is huge. Each day, the security team sees a massive volume of credential stuffing attacks against customer accounts. Many are low-level threats, in which attackers simply automate lists of password and username combinations to see if they manage to find a successful login. To prevent that success, the organization regularly checks their entire customer database against SpyCloud's breach data to identify exposed credentials and force customers to reset them.

Pro Tip: *Scanning your entire customer database and forcing credential resets for compromised users is a tactic SpyCloud recommends for all its customers, and the benefits extend beyond preventing fraud or providing peace of mind for security teams. Companies who proactively monitor and remediate for password exposures are more likely to retain customers. A PWC study of U.S. adults found that 87% of consumers say they will take their business elsewhere if they don't trust that a company is handling their data responsibly. Most consumers do trust financial organizations with their data, and by being proactive in helping consumers avoid fraud, organizations can prove their commitment to responsible data handling.*

Other account takeover attempts are more dangerous, carried out by motivated, adaptive threat actors who are specifically targeting the firm's customer accounts. As the team explains, "We see actors that are very unsophisticated that just don't care…and then we have actors who will respond within a certain time frame to a given control being introduced that specifically blocks their activity. Sometimes it's 8 hours, sometimes it's 24 hours, sometimes it's a few days, but we can always tell which actors are targeting us and we notice certain patterns."

Particularly for these targeted attacks, resetting compromised passwords quickly is essential. A consumer's account is vulnerable the moment a new data breach exposes their login. SpyCloud's fast access to new breach data enables the firm to shorten that exposure window by resetting exposed passwords quickly to head off this type of attack.

Reducing Outside Risk

Today's enterprises rely on hundreds of partners, vendors, and other third parties to deliver products and services to consumers around the world. Each outside group with access to the network presents a multitude of cybersecurity risks. This financial services organization uses SpyCloud's investigation solution and breach data to see deeper into third parties' overall risk profile, which is especially helpful in understanding the potential risks posed by acquisition targets.

At the beginning of an M&A process, the security team uses SpyCloud to investigate whether the target company has had any data breaches that they haven't disclosed, whether because they have chosen not to inform the acquiring company or because they don't know that they have been breached.

SpyCloud

Confidence is the Key to Intelligence Value

As a global organization serving many millions of customers and interacting with thousands of third parties, this financial services organization relies on SpyCloud as a critical part of its collection of intelligence-gathering tools. In this industry, security professionals know that confidence in the credibility of intelligence sources simplifies the difficult task of identifying threat actors, preventing their attacks from infecting consumers, and, hopefully, leading law enforcement to make arrests.

When reporting to internal stakeholders or to law enforcement, SpyCloud's customer knows that their assessments of threats and threat actors are made with a higher degree of confidence because of the reliability and credibility of SpyCloud's data.

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