Global Fintech Company Protects Users from Botnets, Financial Fraud, and Other Threats with SpyCloud

SpyCloud helps protect thousands of vulnerable accounts representing tens of millions of dollars.

About the Customer

This case study covers an anonymous SpyCloud customer – a fintech platform used by merchants, consumers, and traders all over the world. The company also provides merchant payment processing systems and tools supporting some of the most highly trafficked websites. Due to the valuable and sensitive nature of its users' information and assets, threat actors are continuously looking for ways to exploit them.

Combating Automated and Targeted Account Takeover (ATO) Attacks

With so much at stake for its business and customers, this company invests heavily in cybersecurity. It goes to great lengths to not only protect customers and employees, but also to educate them on how to protect themselves and why it matters. Despite warnings for the last several years, many consumers continue to reuse passwords across multiple websites and services. When one site is breached, threat actors apply those stolen credentials to access consumer accounts on other sites.

"We know that password reuse and compromised credentials are still the number one way that people get themselves hacked," explained the head of the organization's security operations team. "We're one of the few major consumer-facing platforms that requires two-factor authentication for all of our users. But even with 2FA, a stolen or lost password is still a really bad security situation."

The company uses SpyCloud to check users' credentials proactively, identifying logins that appear in SpyCloud's breach data, and taking action to secure vulnerable accounts as soon as possible after an exposure. In addition to protecting users from account takeover by locking out potential attackers, this also helps to reduce the confusion caused when users receive unexpected 2FA codes during credential stuffing attempts.

"Since starting to use SpyCloud, we've seen a corresponding drop in partial logins, which might happen if there's a login attempt using a breached login combination that can't bypass two-factor authentication, for example. But that still triggers a login notification to the user and they get confused. For us to be able to get ahead of that curve and know that we can prevent these partial login attempts in the first place adds an extra layer of defense."

High-volume credential stuffing attacks aren't the only concern for this organization. Given the substantial monetary value of the accounts they manage, cybercriminals are very motivated to invest time and effort into targeted, creative attacks against their customers. As a result, the company not only uses SpyCloud data to reset exposed passwords, but also to help model clients' account takeover risk behind the scenes to determine who may be at highest risk of an attack. For example, the company has found that being exposed in a data breach at all—regardless of whether a password was exposed—increases customers' likelihood of being targeted for SIM-swapping.

> We get some predictive data out of SpyCloud that we factor into our risk models. If you have recently appeared in a data breach, you are at elevated risk of SIM-swapping and that's something we can take action on accordingly.

Users' breach exposures can reveal not only risks created by the specific information criminals have access to, but also the ways a user's own habits can put them in danger. By including that information in risk models, the security team can identify accounts that may require additional oversight or even individual outreach for education.

"If you have 30 or 40 passwords exposed, or if 20 of them are the same, it tells us something about your security patterns as an individual. That means we can do some targeted individual outreach with clear recommendations, or factor that information into our ATO risk models. If someone has a higher risk of ATO due to their prominence in the community or the balances they carry, but they don't demonstrate the same security hygiene that we hope for, we might want to put in some countermeasures."

Automating Account Takeover Prevention at Scale

The company's security operations team reviewed several options and chose SpyCloud because of its industry-leading cybersecurity expertise and robust dataset, which provided a match rate of 3-5 percent on customer-facing credentials during their initial data test.

The team was also impressed with the speed of SpyCloud's high-volume, performant API, which is important because if the company opts to gate a user login, verification of the account credentials needs to be instantaneous. The API interface was also easy to work with during implementation, making setup a breeze.

"The SpyCloud API was super easy to integrate. It took a day and a half for our engineers, and then it was just up and running. We've had the integration in place for a year now and had zero issues, zero downtime. On the technology side, it's an enterprise-grade API for us."

With access to high-quality, regularly-updated breach data from SpyCloud, the company was able to eliminate manual sourcing for credential lists, which had been taking about half of a full-time employee's time without coming close to satisfying the organization's needs. In addition, the team was able to create automated workflows using the SpyCloud API that freed them up to work on higher-value projects.

> Our goal is always to automate as much as possible, and in SpyCloud's case, we've been able to automate virtually 100%. That has been a tremendous time saving so we can focus on things that are more targeted, unique, or interesting.

Automation opens up more time for activities that can help the team continually improve their sophisticated account takeover prevention program, such as performing internal investigations to evaluate trends and root cause analysis, and determine if there are additional mitigations they might be able to put into place to protect customers. To help support these activities, the team uses SpyCloud's API to integrate SpyCloud data into their Security Orchestration, Automation and Response (SOAR) tools.

Using SpyCloud data in conjunction with SOAR tools helps the team enrich and pivot on their investigation data, as well as provide additional feedback for their account takeover modeling. For example, SpyCloud data has helped the team correlate credential stuffing botnets to understand the sources of the combolists they're testing and determine if other accounts might be at risk. Using lists of stolen credentials, malicious actors leverage this type of botnet to bombard websites with attempts to gain access using the stolen logins.

"Given the passwords these botnets are trying, we can develop hypotheses about where they're getting their source data and to some extent, what software is being used. This lets us pivot and see what other email addresses were exposed in that particular breach."

Through scenarios like this, SpyCloud helps the team strengthen their defenses proactively in support of their primary objective: "We do everything we can to protect our users and their funds."

Protecting Consumers from Credential-Stealing Botnets

SpyCloud recovers some data collected by botnets – malware infections that siphon credentials and other data from users' systems and send them to an attacker's command and control panel. If a user's credentials appears in a botnet record, it's likely that attackers also have access to a substantial amount of other sensitive data, including their personal information, additional credentials, web history, browser fingerprint, and more. These users are at extremely high risk of account takeover, and criminals often start by targeting valuable accounts such as those belonging to customers of this fintech company.

By using SpyCloud data to identify users whose data has appeared in botnet records, this company has been able to lock cybercriminals out of thousands of highly vulnerable accounts.

> **"With SpyCloud's botnet data, we've protected thousands of accounts representing tens of millions of dollars of funds.**

"They are users we found in SpyCloud's botnet data, where we were able to successfully intervene and force password resets and account recoveries before an attacker was able to do something malicious with those credentials."

Because these users' systems have likely been compromised, the company takes steps to ensure reset passwords don't end up right back in an attacker's hands.

"We assume that if your [customer login] credentials appear somewhere in the botnet data, your email and phone and other mechanisms for proving you are who you say you are, are compromised, too," explained the head of the security operations team. By educating customers about cybersecurity, the team hopes to help users eliminate the malware from their systems and prevent them from falling into similar traps in the future."

"With the botnet data, we saw a very easy way to give a high-signal, highly targeted message to end users where not only can we say that we're going to take more extreme security measures, lock the users' account, and require them to re-verify; but we're also able to send them an email saying, 'it looks like your password was stolen due to malware; before you recover your account, we highly recommend running some sort of antivirus scan, using a password manager…' Otherwise they're just going to end up back in the same position."

With valuable accounts at stake, consumers' reactions to this outreach have been positive. Even better, this approach means the company has not only protected accounts on its own site but likely others as well, preventing immeasurable damage.

Conclusion

Using SpyCloud data to support consumer account takeover prevention enables this company to support one of their guiding principles: maximizing security without sacrificing usability.

"Security and usability are often seen as opposites, as tradeoffs. We strive to make sure they aren't," they explained. "We want to be the most secure and most trusted, but we still want to be the most useful. That's where SpyCloud fits in because it gives us the data we need to intervene when we need to, and then leave users alone when we don't." Rather than forcing users to jump through hoops that might encourage more bad habits, the team strives to provide as much protection as possible without adding friction to the login process.

"We look for ways to make login and authentication as easy for users as possible and still help intervene at key points to prevent them from harming themselves. If we can see that a user has a bad pattern of setting simple, predictable passwords that are going to get them in trouble later, that allows us to do a targeted intervention. SpyCloud gives us another tool in our arsenal to protect our customers without forcing them to try to think like a security team."

Beyond protecting consumer accounts, the team highlighted some additional benefits that are often overlooked, such as the reputational value of investing in account takeover prevention.

"We look at SpyCloud as reputation mitigation as well. You can do everything right and still end up in headlines for the wrong reasons. At a certain volume, ATO is indistinguishable from your platform's security being compromised."

The team also emphasized the bigger picture, pointing out how interconnected financial services accounts have become. Because of integrations between different types of accounts from both fintech and traditional financial accounts, an account compromised on one platform can easily cascade into losses for another provider.

Conversely, companies with strong account takeover practices provide additional protection for providers whose users have connected accounts. Ultimately, the team hopes more financial services organizations start using SpyCloud.

> **As more companies start to use SpyCloud and check for compromised credentials, there are some really powerful network effects that can come out of it. We'll all benefit.**

The SpyCloud Difference

Current, Relevant, Truly Actionable Data

SpyCloud Consumer Account Takeover Prevention draws on the largest repository of recovered breach assets in the world to help you make sure the users logging into your systems are who they say they are.

Using Human Intelligence, SpyCloud goes deeper into the web than any other cybersecurity company, extracting data that's otherwise undetectable. Our database of exposed credentials and PII is not only the largest in the industry—it offers the most current, relevant, and truly actionable data to protect users from account takeover.

More data, along with our substantial investments in password cracking at scale (resulting in billions of plaintext passwords), means more matches and stronger account protection.

Experience the quality of our data for yourself. We invite you to put our data to the test against your own consumer base. Contact us to request a data test.