SpyCloud

Case Study

Global Computer Manufacturer and Retailer Saves Time Identifying and Investigating High-Risk Customers with SpyCloud

Overview

This Fortune 50 computer manufacturer and retailer develops, sells, repairs and supports computers for both enterprises and consumers. The organization's cyber fraud prevention and investigations teams are responsible for identifying high-risk customers and investigating suspect activities. Their primary goal is to protect the enterprise from online fraud and lost revenue.

Challenge

The organization's cyber fraud prevention and investigations teams experience a high volume of requests and wanted to eliminate days of unnecessary investigations by steering their efforts away from low-risk users. They were building an in-house fraud decisioning engine using third-party services to score at-risk users' credentials and personal data available on the criminal underground, but complicated logic and long development times impeded their progress.

Solution

The automatic recapture and correlation of high volumes of darknet exposure data was a critical missing piece in the development of the company's in-house engine. To incorporate automated consumer fraud risk analytics into their security technology stack, the company selected SpyCloud Identity Risk Engine, and for a deeper dive into the highest-risk customers, they use SpyCloud Investigations.

Result

SpyCloud tested over 2 million accounts that were deemed high risk by their existing solutions and sent to manual review. SpyCloud Identity Risk Engine found 82% were low risk, which would have enabled the team to focus resources toward the 18% of medium and high risk accounts. For high risk accounts the organization pivoted to SpyCloud Investigations, which reduced the time spent per fraud investigation by more than one hour.

SpyCloud

Fortune 50 Computer Manufacturer and Retailer Proactively Reduces Manual Review and Bolsters Fraud Investigations with SpyCloud

The company's business deals with both B2B and B2C high-value, high-volume sales. As a result, they are targeted by fraudsters on a regular basis – with each successful instance of fraud costing the company an average of $18,000. The cyber fraud prevention and investigations teams are tasked with identifying potentially fraudulent transactions and investigating high-risk consumers to protect revenue. The teams are also responsible for recognizing and expediting low-risk transactions.

The fraud team monitors suspicious activity, resulting in approximately 100,000 investigation requests daily (35,000 to 40,000 every 4 hours), with time only allowing each team member to perform 30 to 50 incident reviews and an average of 5 to 7 in-depth investigations per day. This workload was completely unsustainable, especially considering how much time was spent on low-risk users. The team knew there was a missing component of their fraud framework and sought solutions to fill the gap.

To help fight against online fraud in a more comprehensive, automated way, the organization began developing their own proprietary in-house fraud decisioning engine that comprises multiple vendor tools and solutions, as well as a blend of external third-party data and historical internal data to help identify high-risk transactions and lessen the number of required fraud investigations.

The team selected SpyCloud Identity Risk Engine and SpyCloud Investigations to incorporate darknet data analytics into their new build via a Splunk integration. For each transaction, a numerical risk score is given, supported by up to 24 key risk indicators, providing a quick and concise snapshot that is used to determine whether or not the attempted transaction could be driven by malicious intent. The organization is provided with exactly what is in criminal hands, allowing them to take multiple data points into consideration, including:

- Did the email show up in a breach? What was the nature of that breach? How recently did the breach occur (i.e. within 30 days)?
- What is the user's password reuse habit? Does the user have good password hygiene?
- Does the user have additional PII exposed like credit card information, address, date of birth, or SSN which could easily aid impersonation?
- Is there a malware infection on the device(s) being used?

The ability to identify malware-infected consumers with SpyCloud is a significant benefit for the company, because infostealer malware actively siphons all of their credentials, browser fingerprints and web session cookies that can be used to bypass MFA and log into accounts, making the criminal indistinguishable from the consumer. In situations where SpyCloud is able to identify that there was an exposure within the last 30 days, the team takes preventative action to monitor the transaction with a higher level of scrutiny.

SpyCloud

The cyber fraud prevention and investigations teams are excited by the potential impact that SpyCloud can have in various steps in the customer journey. In the future, the company plans to incorporate the risk assessment across all transaction and communication channels, including the website, chat functions, and more. For example, when a customer engages in a chat session, the organization's in-house engine will call SpyCloud's API to help determine if the customer is legitimate or if additional context provided by SpyCloud would warrant suspicion of malicious intent.

RESULTS

Quality of Data Tests Solidified Decision to Incorporate SpyCloud into Their Internal Risk Engine

The organization provided SpyCloud with four weeks of data for over 2 million accounts that made contact or transacted and were deemed high risk and sent to manual review. SpyCloud Identity Risk Engine found 82% were low risk, which would have enabled the team to focus on the 7% that were high risk and decide if the 11% medium risk were subject to further review. Additionally, time spent per fraud investigation was reduced by more than an hour.

Of the 2 million tested accounts in question, 70% had poor password hygiene, making them susceptible to account takeover, and 4% were victims of malware infections. These results prompted a separate analysis of the organization's entire customer base, which revealed an alarmingly high password reuse rate of 68%.

Reduced Investigations Cycle Time

As the organization continues to build out and strengthen their in-house engine, they are already seeing the value SpyCloud can bring as post-transaction investigation time has reduced by 30%.

Automated Investigations Steps to Increase Efficiency

Using Identity Risk Engine, the company was able to reduce the number of necessary investigations through automation and detection of low-risk users, focusing efforts on higher risk accounts, as well as get insights on multiple other data points and factors to allow for additional checks and balances in the pursuit of preventing fraud.

"As you move to the right of any transaction and you start to get more proactive in fraud checks, you also start to get a lot more false positives. Having additional information related to a user beyond just an email helps us move beyond assumptions to have better insights on the validity of a transaction," the company's security investigator said.

> **"Not only were we able to focus on the high-risk transactions identified by SpyCloud, we also found that 4% of our users were infected with malware, which alerted the team to an increased need for investigation into their purchases, including customer outreach. Predicting fraud tied to malware is unique to SpyCloud, and the pilot surpassed our expectations and ultimately contributed to the final buying decision."**
>
> **- SECURITY INVESTIGATOR**