SpyCloud

INDUSTRY: Chemical

CASE STUDY

Combining ATO Prevention with Employee Education to Fight Cybercrime

CHALLENGE

Preventing a security breach that impacts their customer data is a top priority for this customer, yet without credential exposure monitoring and reporting, they were at constant risk.

SOLUTION

The company consistently monitors employee credentials against SpyCloud's database of stolen credentials to proactively catch account takeover exposure before criminals have the opportunity to compromise employee accounts.

RESULT

With accurate, real-time exposure data at their fingertips, the team is able to prove risk, helping executives and employees become more aware of the threat of account takeover and be proactive to prevent it.

ABOUT THE CUSTOMER

This case study covers a global specialty chemical company headquartered in the United States. Its innovative solutions are designed for customers in the pulp and paper, leather, plastics, oil and gas, and water treatment industries. Its goal is to help customers improve their operations by boosting productivity, increasing profitability and ensuring safety, compliance and sustainability.

CHALLENGE: VISIBILITY INTO THE REAL THREAT OF EXPOSED CREDENTIALS

One of the company's strategic initiatives is to apply digital technology in the process of not only applying chemicals but helping customers ensure their processes are efficient and effective. With cyber threats front and center, the company is equally invested in taking appropriate protections to mitigate their own risk by protecting sensitive data.

"Much of what we do is not only to gain the trust of our customers with our chemical and process expertise but with how we treat their private information," explained the director of Global IT Infrastructure. "We can't afford to have a security breach that impacts their data."

The company understands that many attackers find entry points into organizations via unsuspecting employees. Whether by using their company credentials on personal accounts or responding to phishing emails that download malware, employees are often the easiest targets for cybercriminals. Many of this company's employees use multiple devices to access systems with corporate or customer information, compounding the risk.

In fact, the company has experienced account takeover of this nature in the past with a phishing attack that made its way to the CEO. "Our CEO had his email account taken over and the cybercriminal sent out a bogus email to a finance associate claiming our financial officer authorized a wire transfer," shared the director. "The email was convincing, even using actual names and private information." Fortunately, the team member was well trained in spotting suspicious emails and went directly to the finance officer to verify the email was a scam.

Even with best practices in place, the IT Infrastructure team recognized the company needed to add credential exposure reporting to its repertoire of security solutions. Many of its executives didn't realize their information was exposed and associates didn't believe their stolen credentials would harm the company or customers. In order to prove the risk to them, the team needed hard data to show them the threat was real, from the CEO to the most entry-level associate.

> *"Our CEO had his email account taken over and the cybercriminal sent out a bogus email to a finance associate claiming our financial officer authorized a wire transfer."*

65 DIFFERENT 3RD PARTY BREACHES SEARCHED

2000 EXPOSED EMPLOYEE RECORDS DETECTED

Since becoming a SpyCloud customer

SOLUTION: REAL-TIME, USABLE DATA FOR IMMEDIATE REMEDIATION

The company already had multiple layers of technology safeguards in place, such as firewalls, automatic security updates, malware prevention, and automatic monitoring of assets. The one thing it lacked was consistent monitoring of employee credentials against a database of stolen credentials. For that, they chose SpyCloud.

"We are a chemical company, not a cybersecurity company. SpyCloud watches multiple areas of the dark web for us, gathers exposed credential data that we never had access to before and presents it in a simple way we can share with associates and corporate leaders to help them understand the level of risk we are facing. The SpyCloud data is more specific and actionable than any other solution we found, giving us employee, account-level and source detail we need to prove the threat and take immediate action. SpyCloud also shared best practices we could immediately employ. Combined with real-time exposure data, our employees are continually improving their cyber-knowledge and skills."

Employee education has been a major focus — and something to which SpyCloud has contributed greatly. Teaching associates and executives about the tactics cybercriminals use and the steps they must take to safeguard their accounts are just as important as the technology in place to protect their information, brand and reputation. Today, all of the company's employees understand they are all potential targets and know what to do to lessen the risk.

RESULTS: CONTINUAL IMPROVEMENT OF CYBER AWARENESS, SKILLS AND PROTECTION

Since implementing SpyCloud as part of its overall technology stack, this customer has dramatically reduced the risk of a breach. Its executives and associates are proactive in contributing to the company's security stance, particularly as they receive data on exposed credentials. Information from SpyCloud empowers them to take control of their corporate credentials, which in turn, helps them protect their personal accounts as well.

The success of the SpyCloud solution has been measurable, so much so, that it enabled the IT infrastructure team to obtain budget for weekly phishing prevention training from industry experts. It has become an expectation that associates continually develop their cyber skills and adhere to best practices, including changing their passwords on a regular basis, choosing strong and unique passwords, multi-factor authentication and not using corporate IDs for personal business.

"Criminals have been doing the same thing they've been doing for centuries. They're just doing it differently now. We can't fight it all with technology alone. We must also transform our habits to reduce the risk. Our security strategy has come a long way, but we are never complacent. I sleep better at night knowing we are doing as much as we can, while at the same time, always have one eye open to what we need to do next."

> *"The SpyCloud data is more specific and actionable than any other solution we've found, giving us employee, account-level and source detail we need to mitigate the threat and take immediate action."*