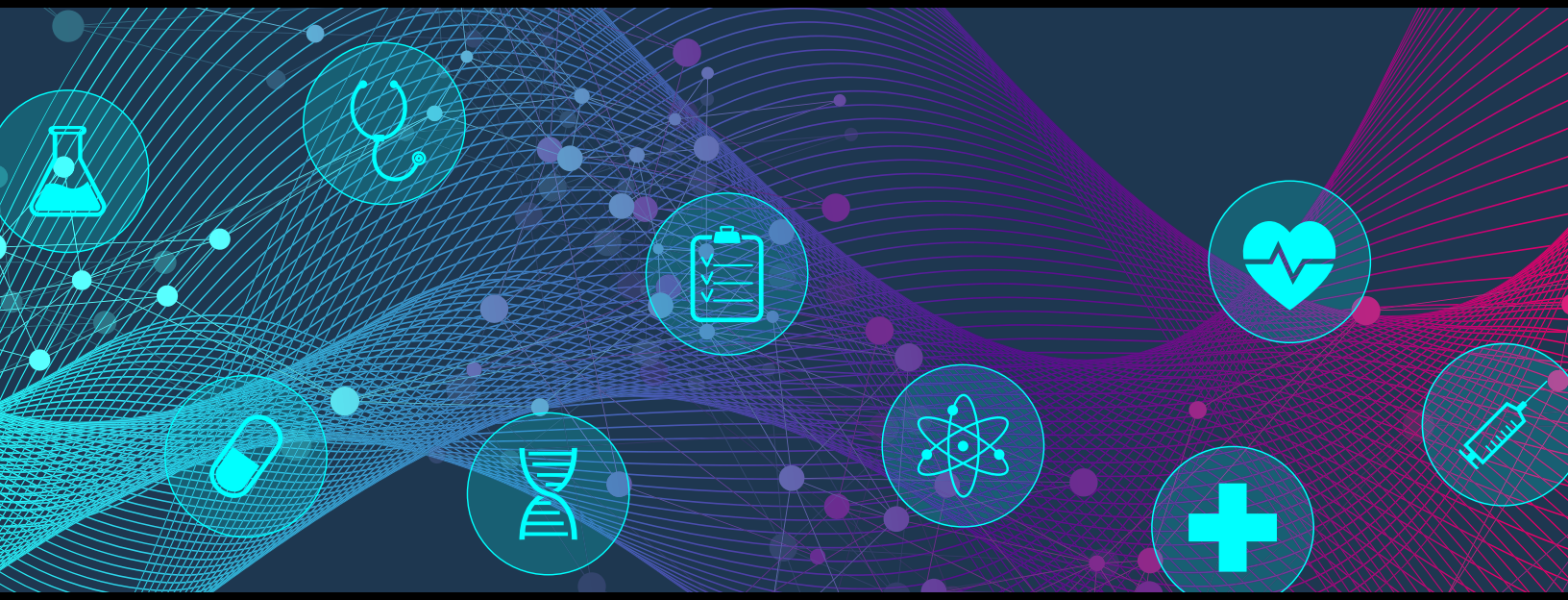
SpyCloud



Case Study

Global Biomedical Research Organization Reduces Cyber Risk in Highly Targeted Industry with SpyCloud Enterprise Protection

Overview

This global biomedical research organization has a mission to reduce emerging infectious diseases through research, development, and delivery of vaccines and other innovative biomedical solutions.

Challenge

In an industry fraught with cyberattacks, this organization must protect sensitive healthcare research from bad actors. The small security team has limited tools and resources to proactively identify employee darknet exposures that put their organization at risk.

Solution

After identifying a high-priority exposure of a malware-infected user accessing their network, the organization chose to incorporate darknet insights into their security framework by implementing SpyCloud's automated Enterprise Protection solutions to reduce the risk of account takeover and ransomware.

Result

With SpyCloud, the organization automatically protects more than 400 employees from account takeover and can quickly act on infected personal and third-party devices accessing their network – all while saving time and resources for their small security team.

SpyCloud

Global Biomedical Research Organization Incorporates Darknet Data into Security Framework to Protect Employee Accounts and Reduce Enterprise Risk of Ransomware

The healthcare industry as a whole continues to be a priority target, with two-thirds of healthcare organizations reporting ransomware attempts in the last year. As such, the organization's small security team is charged with thwarting potential threats despite being spread thin and with limited resources. The team is proactive with their security measures – tasked with not only the usual aspects of safeguarding the network and infrastructure, but also with offering regular cybersecurity awareness training and performing weekly phishing simulation exercises for their employee base.

While researching cybersecurity vendors who could help his team work more efficiently and effectively, the IT Security Manager came across SpyCloud. After signing up for a trial, he found significant value in SpyCloud's Cybercrime Analytics, powered by darknet data, but was not in a position to incorporate it into their security framework at that time.

Due to the nature of their work in healthcare research for vaccines, the organization has doubled in size over the last few years, now with more than 400 employees globally. When the organization received additional funds during the pandemic, the IT Security Manager championed allocating funds to enhance their program with SpyCloud's solutions. Once he re-engaged, SpyCloud detected an exposed password for one of their user's Active Directory accounts. Upon further investigation, it was determined that the user accessed a corporate video communications application from a personal device that was infected with infostealer malware – the source of the password exposure. Armed with this unique insight, the security team quickly remediated the vulnerable device and account with the employee. The incident proved the immediate value SpyCloud solutions would bring in protecting their network and infrastructure.

To protect their enterprise from account takeover, the organization initially implemented:

- SpyCloud Employee ATO Prevention to protect against account takeover that can result from credentials exposed in third-party data breaches
- SpyCloud VIP Guardian to secure executives' online identities
- SpyCloud Active Directory Guardian to prevent, detect, and automate password resets for compromised Active Directory accounts

As cyberthreats to the healthcare industry continue to evolve, the organization turned their attention to SpyCloud's latest enterprise protection solution, Compass, which detects potential entry points for ransomware stemming from stolen credentials and session cookies exfiltrated from malware-infected devices (managed, unmanaged, and under-managed) that are used to access critical workforce applications.

Since implementing Compass, the organization has not experienced a malware infection on one of their corporate-issued, managed devices. However, they were surprised to identify both a third-party contractor who accessed their network using a malware-infected machine, and an employee who accessed the organization's applications from a personal infected device. The team would not have had visibility into these exposures without SpyCloud. Once SpyCloud identified the exposed data, the security team swiftly took Post-Infection Remediation steps, negating the opportunity for follow-on attacks.

SpyCloud provides actionable insights and contextual information that the security team can't get anywhere else, which allows them to highlight the value of the investment in SpyCloud to leadership as part of their overall security program, and also supports the organization's commitment to proactive security.

"SpyCloud always goes above and beyond with eye-opening, powerful information. Not only are they able to identify an exposure, but they provide additional, timely information about the potential impact of a compromise that we would otherwise never be aware of. As a security practitioner, when I think of a malware infection, it's unlikely that just one account is exposed – it's probably hundreds of accounts that are exposed. With SpyCloud, I can see what actually is exposed and what is relevant so I can take quick action."

- CYBERSECURITY OFFICER

Results

PROTECTS ALL EMPLOYEES FROM ACCOUNT TAKEOVER

With the healthcare industry a prime target for cyberattacks, proactive security is of utmost importance to the organization. SpyCloud's Enterprise Protection solutions secure all 400+ employees from account takeover, extending that protection to VIPs' personal accounts.

REDUCES RISK OF RANSOMWARE WITH DARKNET INSIGHTS

Using SpyCloud, the team gets insights about potential risks they wouldn't otherwise have known about, which shows the value of the investment to leadership and affords the security team much-needed intel to prevent cybercrime – even with limited time and resources at their disposal. SpyCloud helps them address a critical blindspot in ransomware defense: detecting infected devices accessing the network and enabling complete Post-Infection Remediation of the resulting exposed corporate applications and credentials that could create the opportunity for further attacks.

"SpyCloud Compass provides amazing information - it gives us another layer of information that we didn't have before."

- CYBERSECURITY OFFICER

Previously, malware-infected device remediation was focused simply on removing the malware and wiping the device, whereas now the security team is able to see the true impact of the threat including the stolen authentication information and affected applications, which they can then help the user address and bolster their remediation efforts.

"You can't really put a number on what was saved by just having this information. Because if you stop something early, you're preventing things down the line you can't even really anticipate. Without SpyCloud data, I wouldn't even have a way to look into this kind of information. I have tapped into other sites, and it's just a different level of service with SpyCloud," the Cybersecurity Officer explained.

SpyCloud

SAVES SUBSTANTIAL TIME & RESOURCES FOR A SMALL TEAM

The ease of use with SpyCloud solutions enables the security team to spend a minimum amount of time reviewing alerts, typically around five minutes per day.

In the event of cyber incident response, SpyCloud solutions save the security team approximately 20 hours of recovery time per device. When it's necessary to further investigate specific alerts, the Cybersecurity Officer leverages his SpyCloud customer success manager and other SpyCloud experts who have become an extension of the team by offering additional resources and insight. Previously cyber investigations could take multiple business days, but using insights from SpyCloud reduces that time to one hour.

> **"The system is intuitive and made as simple as possible, which makes using SpyCloud efficient and easy. It also helps me avoid alert fatigue that most security professionals feel from an abundance of alerts."**
>
> **- CYBERSECURITY OFFICER**

REDUCES ALERT FATIGUE WITH AUTOMATED SOLUTIONS

In a security environment that generates up to 200 alerts a day, the security team must prioritize the most critical issues and determine what is relevant and actionable. Automation plays a key role in helping the team address the most urgent security tickets, specifically alerts from SpyCloud Active Directory Guardian that are deemed critical since exposed passwords could be used on the organization's Active Directory and have a one-to-one correlation with the associated email address – leaving an entry point for criminals to perpetrate ATO.

ENHANCES INTERNAL SECURITY AWARENESS

The IT Security Manager hosts security-focused brown bag lunches to encourage cybersecurity awareness with employees, incorporating the concepts SpyCloud evangelizes, like password security. He promotes strong, complex passwords, recently increasing password character requirements, and implemented a password manager across the organization. He also lets employees know about the opportunity to check their own darknet exposure on the SpyCloud website. Additionally, the team also executes phishing simulations on a weekly basis to further enhance internal security.