CASE STUDY

Global Biotechnology Giant Leverages Phishing Response Service to Thwart Phishing Attacks

Customer Profile

A global Biotechnology giant operating on five continents, with 9,400 employees spread out across 30 countries.

Challenges

The Biotechnology company faced resource constraints, making it challenging to assign or hire full-time employees to optimize email security tools and handle malicious usersubmitted emails efficiently. Securing email communication is vital for maintaining business operations, meeting regulatory requirements, and upholding the company's reputation. Given the rise in advanced phishing attacks, defending against external threats and handling user-generated emails has become increasingly complex for their small team of two to manage.

Solution

Binary Defense Phishing Response Service

Results

- Expanded visibility into potential suspicious or malicious emails
- Improved the organization's security maturity by providing recommendations to enhance internal processes and workflows
- Reduced the day-to-day tactical lift of responding to incidents and user submissions on behalf of the biotechnology security team
- 1,769 User-submissions
- 367 escalations resulted in 277 benign positives and 90 true positives

Challenges

As a global Biotechnology giant operating on five continents, the organization heavily relies on email for communications with partners, providers, and patients. Keeping email correspondence secure is critical to ensure business continuity, staying compliant with ever-changing regulations—and protecting the company's reputation. With the rise of sophisticated phishing attacks, it became increasingly difficult to safeguard against external threats and respond to thousands of user-submitted emails. The global Biotech company knew it had a gap in its phishing controls. Still, with a small security team of two and competing priorities, they could not effectively pull together resources to monitor potential malicious emails. After a failed attempt to augment their limited resources with a MSSP, it was determined that leveraging a trusted Phishing Response partner would be the best solution to help mature their security posture and shore up their email security gaps.

Solution

The global Biotechnology company partnered with Binary Defense to manage its phishing response. This allowed the team to stay focused on high-priority initiatives while giving them peace of mind that potential malicious emails were being thoroughly investigated. Binary Defense's specialized phishing analysts conduct thorough email analysis, leveraging gathered intelligence to proactively prevent attacks early in the lifecycle, enhance the biotechnology company's security protocols, and optimize internal workflows and processes. By leveraging Binary Defense's Phishing Response Service, the biotech giant can successfully address phishing emails reported by their users and their email security tools. This collaboration involves Binary Defense's skilled phishing analyst identifying the strategies used in attacks, documenting their investigation procedures and findings, and offering actionable recommendations to strengthen security measures and detection capabilities to effectively lower risks.

Results

The Biotechnology company decided to improve their email security by hiring dedicated phishing analysts to manage their email security tools and user-submitted emails. They partnered with Binary Defense with the aim of having a trusted advisor to help them improve their email security. After implementation, Binary Defense took swift action and within just over 6 months, they investigated more than 1,769 user submissions, leading to 367 escalations. The collaboration between Binary Defense's phishing analyst and the company's security team helped to significantly advance their maturity levels. This partnership resulted in the company's security team fully embracing recommendations for enhancing internal processes and workflows, leading to improved email security.

Phishing Response in Action

After examining a suspicious email submitted by a user, Binary Defense swiftly initiated an investigation into a phishing campaign involving the spoofing of multiple vendors and specifically aimed at the executive team members using counterfeit DocuSign documents. By investigating and analyzing the tactics, techniques, and procedures leveraged by the attacker, Binary Defense's phishing analysts uncovered a critical pattern in the spoofing attacks, leading to nine additional recipients, six additional sending domains, six additional subjects, six additional malicious URLs, and four additional instances of user interaction. Upon discovering these findings, the dedicated phishing analyst took swift action to block sending domains and malicious URLs, purging emails, and resetting user credentials within 2 hours of the first delivery. These mitigation measures implemented by Binary Defense and the Biotech company allowed them to detect and thwart further intrusion attempts proactively. Additionally, the phishing analyst demonstrated exceptional dedication by uncovering logging discrepancies and offering remedial suggestions. This incident is a prime example of the many phishing attempts that Binary Defense's Phishing Response Service has successfully intercepted, preventing attackers from infiltrating the biotech infrastructure.

20% of all

user-submitted emails required full-scope investigation in the first five months.

In Conclusion

The ongoing partnership between the leading global biotechnology company and Binary Defense continues to prove highly successful in detecting and mitigating cyber-attacks earlier in the attack lifecycle. It efficiently reduces risks for the organization, bolsters its cybersecurity posture, and optimizes workflows and procedures. With cyber threats growing more advanced, organizations need to stay alert and collaborate with trusted partners like Binary Defense to strengthen their defenses. Through Binary Defense's phishing response service, the biotech company proactively protected sensitive data, avoiding potential financial and reputational damage.