Technology Company Improves Threat Visibility with Binary Defense’s Digital Risk Protection Service

Customer Profile

A Technology Company that provides software and services to help corporations gain a true competitive advantage from their IP. With over 1,000 employees, the Technology Company's software is used by over a million customers in corporations all over the world.

Challenges

The Technology Company operated with a small team, each member balancing multiple responsibilities. This internal team faced limitations in both capacity and expertise, which hindered their ability to monitor the clearnet, dark web, and darknet for potential threats to their organization, data, and employees. The Technology Company faced a significant challenge when fraudulent domains began issuing fake job offers. Additionally, the company was entering a phase of potential transactions, such as acquisition or attracting new investors. This situation necessitated a solution to enhance their security posture, ensuring threat notification across various sources to prevent breaches and reassure new buyers and investors.

Solution

Digital Risk Protection Service (DRPS)

Results

- 1,000+ leaked email addresses across various breaches were identified by Binary Defense’s Counterintelligence team
- Improved security posture through customized alerts and reporting provided real-time actionable insights
- Discovery of over 70 potentially harmful domains within a 90-day period
- Increased visibility of exposed digital assets with insights into potential vulnerabilities, risks, and impact.

Challenges

As a Technology Company providing software and services that help corporations gain a true competitive advantage from their IP, this organization needed to take their security program to the next level. With over 1,000 employees, the Technology Company's software is used by over a million customers in corporations all over the world.

The Technology Company operated with a small team, each member balancing multiple responsibilities. This internal team faced limitations in both capacity and expertise, which hindered their ability to monitor the Clearnet and Darknet for potential threats to their organization, data, and employees. They required a provider with profound security expertise, capable of collaborating effectively with their team and utilizing tools to detect threats across various sources.

The Technology Company faced a significant challenge when fraudulent domains began issuing fake job offers, hurting its reputation and causing chaos for internal teams. Additionally, the company was entering a phase of potential transactions, such as acquisition or attracting new investors. This situation necessitated a solution to enhance their security posture, ensuring threat notification across multiple sources were being monitored to prevent breaches and reassure new buyers and investors.

Solution

When a leading organization faced increasing concerns about leaked emails, typosquatting, and hidden threats lurking on the Clearnet and Darknet, they turned to the Binary Defense’s Counterintelligence team for support. With a strong foundation in military and law enforcement expertise, the team quickly went to work, uncovering digital risks that posed a direct threat to the company’s security and reputation.

The Counterintelligence team’s investigation revealed several domains potentially registered by threat actors to impersonate the brand, target employees with phishing schemes, and scam customers into sharing sensitive banking information. Each identified domain was meticulously reviewed, with detailed summaries provided to the client in a clear, actionable format.

Beyond identification, the team offered an additional layer of support: clients with full-time monitoring services could request domain takedowns, allowing the Counterintelligence team to handle the process end-to-end and free up internal resources.

The team also conducted a comprehensive scan of the Darknet, uncovering postings that mentioned the organization and ensuring any compromised data was reported with a full context of its exposure. This proactive approach gave the client's security team peace of mind, knowing that emerging threats were being monitored and mitigated continuously.

By providing actionable insights, removing malicious domains, and regularly delivering updates, the Binary Defense Counterintelligence team empowered the organization to focus on its core mission without the distraction of digital threats. The result was a fortified security posture and confidence in the company's ability to stay ahead of cybercriminals.

Results

Binary Defense developed a customized Digital Risk Protection solution for the Technology Company to address imminent threats and prepare for upcoming mergers and acquisitions. The Counterintelligence team conducted an investigation of the company's domains and related emails against known breaches to determine if any had been compromised. During this deep dive, it was discovered that over 1,000 email addresses were leaked across various breaches. A detailed report, including a .xlsx file with all affected emails and breach names, was provided to the internal security team.

1,000+

leaked emails across various breaches were identified by Binary Defense's Counterintelligence team

Additionally, the Counterintelligence team examined multiple domains to identify any potentially malicious setups targeting the Technology Company, its employees, or customers. This investigation led to the discovery of over 70 potentially harmful domains within a 90-day period, including typo-squatting domains mimicking those of the Technology Company and its subsidiaries. Recommendations to block these domains were escalated, and all findings were shared with the internal security team for further action.

The team also identified a concerning post on a Darknet site operated by a well-known Ransomware-as-a-Service (RaaS) provider. This post mentioned the Technology Company by name, indicating plans to execute a ransomware attack. The Counterintelligence team included screenshots of the document names, alleged to be part of the leaked information, in their report. By monitoring both the Clearnet and Darknet, the technology provided potential investors and buyers with peace of mind. It demonstrated that the security team was proactively addressing security gaps and identifying threats early, all without the need to increase headcount.

About Binary Defense

Binary Defense is on a mission to Make the World a Safer Place by combining Threat Intelligence, Technology, and Analyst Tradecraft with industry-leading processes to provide results-driven cybersecurity services that address the most pressing security challenges facing organizations today.

600 Alpha Parkway
Stow OH 44224
binarydefense.com
sales@binarydefense.com