CASE STUDY

Retailer Restores Customer Trust Through Binary Defense Partnership

Customer Profile

A retail company that offers consumers distinctive outdoor apparel and accessories. They provide both e-commerce and brick-and-mortar shopping options,leading to revenue exceeding 5 million.

Challenges

For this retailer, with an immature security program and a small, overextended team juggling multiple business functions, combating numerous spoofed websites was a challenge. This led to diminished consumer trust, complaints of missing orders, and data theft. Despite efforts to remove these deceptive sites, new ones quickly emerged, overwhelming the team. The retailer realized the need for expert help and sought an advisor to take down existing spoofed sites, monitor for new ones, and assess theirinfrastructure for vulnerabilities.

Solution

Digital Risk Protection Services (DRPS)
Managed Detection & Response (MDR)
Analysis on Demand (AoD)

Results

- Over 23 spoofed websites were identified within a period of 6 months
- Restored customer confidence in the retail brand
- The team gained substantial time savings, enabling them to focus on their primary responsibilities
- Minimized financial losses by preventing malicious entities from stealing consumers' credit card details.
- Provided the team with reassurance that their infrastructure remained secure and uncompromised
- Offered recommendations to strengthen the retailer's security posture

Challenges

While e-commerce has led to ease of purchasing, it also opens the door to potential threats to use tactics to harvest customer credentials, PII, and credit card data. E-commerce site spoofing is a sophisticated tactic that cybercriminals employ to deceive consumers and sabotage legitimate businesses. By mimicking the appearance or functionality of a genuine e-commerce site; bad actors lure unsuspecting customers into providing sensitive information under the guise of a trusted platform. The consequences can be severe, leading to financial losses, identity theft, and erosion of consumer trust in the affected business. In this retailer's case, they had an immature security program and a small team that was overburdened. The retail team had to fulfill many different business functions, stretching themselves thin. The team struggled to combat numerous spoofed websites, leading to diminished consumer trust, complaints of missing orders, and stolen customer data. Despite efforts to take down these deceptive sites, new ones would quickly emerge, posing a constant challenge that was far beyond the skills of the retailer's team. The retail team conducted their own review of the suspicious websites to uncover how targeted the spoofed sites were. They discovered that despite subtle signs of potential illegitimacy, the sites still garnered enough consumer trust to complete transactions. Recognizing that their resources were being over-extended and the need for expert assistance, the team sought a trusted advisor to dismantle existing spoofed sites, monitor for new ones, and thoroughly examine their infrastructure to find any exploited vulnerabilities.

Solution

Bad actors persist in their efforts, especially if their tactics prove effective. Amid rising complaints and the emergence of new websites, the retailer turned to a reliable advisor, Binary Defense, to tackle these ongoing threats to their business, brand, and customers. Binary Defense quickly determined that combining three services, Digital Risk Protection Service (DRPS), Managed Detection and Response (MDR), and Analysis on Demand (AoD), was required to tackle all the retailer's concerns. The counterintelligence team, which is preventive and aims to deter attackers by disrupting their operations, was the ideal solution for working side-by-side with the retailer's team to take down spoofed websites and continuously

monitor new ones that emerged. Binary Defense's MDR, especially the Analysis On Demand service, was the ideal fit to address the retailer's worries about a breach, necessitating an expert analyst to conduct a thorough investigation.

The AoD team, comprised of T3 analysts specializing in digital forensics, malware analysis, and threat intelligence, can effectively handle complex incidents within customer environments. To ensure the company's peace of mind regarding its infrastructure's security, Binary Defense's T3 analyst performed a complete forensic analysis delving into potential security threats. The collaborative efforts of the counterintelligence team and AoD analyst provided a comprehensive solution that went beyond hunting and taking down spoofed websites.

Results

After gaining enough background on the retailer's challenges and concerns, the counterintelligence team swiftly identified and dismantled spoofed websites before they became fully operational within just a few months. The counterintelligence team confirmed the retailer was actively being targeted due to a trend of over 23 new spoofed sites appearing over the course of 6 months. After taking down one after another, the counterintelligence team noticed that the websites targeting the retailer began to slow down. The team's active deterrence was paying off, reducing further financial harm and restoring consumer trust in the retailer's brand.

As the counterintelligence team was monitoring for new sites, the analyst from the Analysis on Demand team had their investigation of the retailer's infrastructure underway. Binary Defense's analyst conducted a complete forensic analysis of the retailer's endpoints and analyzed their website for malicious activity, looking for exploited vulnerabilities or hidden bad actors. Throughout this investigation, the analyst offered the retailer timely responses and maintained consistent communication, ensuring their team remained well-informed. Once the forensic analysis was concluded, the analyst confirmed the retailer's company endpoints, employee user accounts, and website had not been compromised.

The expert analyst also provided detailed strategic and tactical mitigation recommendations to strengthen the business's security posture, taking a proactive strategy to prevent future attacks from occurring.

The partnership with Binary Defense resolved immediate threats and fostered a long-term commitment to maturing the retail company's security posture. With spoofed websites diminishing in frequency after the counterintelligence team's interventions, customer trust began to be restored, and the retailer found itself on the path to a more secure and resilient internal infrastructure. After the collaboration, the retail company acquired a new perspective on cybersecurity, recognizing the value of strategic partnerships in safeguarding its own infrastructure and brand. By prioritizing trust and security and following the advice of Binary Defense's expert analyst to implement an EDR, Vision On Demand, the company showcased its commitment to safeguarding customers. This solidified its standing as a trustworthy and secure platform for online transactions.

23+ spoofed websites were identified within a period of 6 months

In Conclusion

E-commerce site spoofing poses a complex challenge for retailers, spanning from financial loss to the subsequent loss of customer trust. The collaboration between Binary Defense and the retail company doesn't just offer an immediate fix but signifies a deep dedication to long-term security. By staying proactive and nurturing partnerships with leaders in the cyber security space like Binary Defense, businesses can effectively combat emerging threats and position themselves as secure entities in the e-commerce space.