Cybeta

CASE STUDY

Retail Sector

Contact us today to learn how Cybeta can augment your existing security program.

A Fortune 1000 retailer with more than **$3 billion in annual revenues** and substantial cybersecurity investments approached Cybeta to help them understand how **proactive business threat intelligence** could be used to complement their existing information security and risk management efforts.

SOLUTION / ACTION

Cybeta immediately identified current and active threats against the firm that had been previously unknown to them and their managed security service provider. The first of which was an exposed URL from a company webpage that was vulnerable to a cross-site scripting attack. This is a common web application vulnerability where an attacker could steal credentials, harvest employee privacy information, or spread malware. Cybeta uncovered the presence of this vulnerability from a hacker forum on the dark web where an anonymous user left instructions on how the code could inflict damage to the company and where it is located.

The second threat was discovered using proprietary investigative techniques and sources. Cybeta uncovered compromised metadata such as username and passwords belonging to senior management stemming from an unrelated attack on a third-party service. These same techniques unearthed corporate email addresses and privacy information tied to 15 other staff members who were identified on a protected forum as being privileged users of a certain SaaS application used at the company. Cybeta learned this was fueling speculation on the forum of the possibility of staging future attacks against these individuals due to a correct assumption that their privileged access was likely based on their proximity to highly sensitive corporate secrets.

Cybeta found a third threat identifying how a human resources webpage, belonging to one of the manufacturer's overseas joint ventures, was emitting a malware signature previously unknown to both entities. This signature exposed the manufacturer and its entire business ecosystem to potentially significant data loss and reputation damage.

BENEFITS / IMPACT

The impact was immediate. Cybeta was asked by corporate leadership to present their work at the manufacturer's annual board meeting to foster renewed security awareness and usher wholesale change to existing information security efforts. Not only did the firm realize a historical misallocation of its resources relative to the threat but affirmed its commitment to effective enterprise security through a strategic investment in intelligence monitoring, robust JV due diligence, and persistent analysis of threats in a dynamic security landscape.