SEGASEC

Financial Sector
Success Story

Fortune 500 Bank Relies on Segasec to Foil Advanced Phishing Attacks

About Fortune 500 Bank

Our customer is a Fortune 500 multi-channel bank and one of the most respected financial institutions in Europe. The bank serves millions of private clients and small and medium-sized enterprises worldwide via hundreds of branch offices, insurance agencies and electronic channels. Among the bank's services are debt capital, domestic cash equity, corporate banking, private banking, leasing, factoring, reinsurance, private equity and project and trade finance.

The Problem

During the first half of 2018, the average number of cyberattacks per banking institution rose to 520, compared to 207 per bank during the same period last year. "When the bank came to us for a solution, they were under constant phishing attack," said Segasec CEO Elad Shulman. The bank's cyber logs and records showed nearly 1,000 malicious activities each month, targeting bank customers and their financial assets and jeopardizing the bank's reputation and customer trust.

These phishing attacks were not detected in time, and once they were detected, it took the bank days, sometimes weeks to take them down. In the meantime, some customers fell victim to the scams and lost valuable assets. While the bank had deployed anti-fraud and other cyber security tools, these systems were not able to detect advanced phishing schemes or to cope with an attack.

The Solution

"Traditional anti-phishing solutions can only react to an attack in progress, and that's a big limitation," explains Elad Schulman. "At Segasec, we have developed a proactive and preemptive approach that successfully detects and monitors the online preparations for a phishing attack, and is able to disarm the attack within minutes of launch – before users are exposed to the scam," continues Schulman.

With Segasec monitoring the web for phishing activity against this Fortune 500 Bank, phishing attacks are now disarmed and blocked within seconds of launch, before bank customers are exposed.

Using a full list of the bank's URLs and other online assets, the Segasec solution began active and passive monitoring of the web, enabling early detection of phishing attacks involving the bank, and timely take-down of the attack. In addition, Segasec is strengthening the efficacy of existing fraud prevention systems by simulating controlled and evolving attack scenarios that provide vital cyber intelligence for the bank's protective shield strategy.

Results

Now that Segasec's solution is monitoring the web for phishing activity against the bank 24/7, phishing attacks are disarmed within minutes of launch, and at most, within an hour or two. This is a tremendous improvement compared to the days and weeks it used to take to stop an attack. Even though cyberattacks evolve and continue apace, customers are no longer exposed to phishing attacks during their online interactions with the bank, enabling the bank to protect its stellar reputation and customer trust.

Contact us: Info@segasec.com