CASE STUDY

MAJOR FINANCIAL SERVICES COMPANY CHOSES DECEPTION FOR VISIBILITY AND FORENSICS

COMPANY PROFILE: A LARGE FINANCIAL SERVICES COMPANY

Situation

Information Security senior management sought to gain better visibility into their diverse and international network environment and address the often-challenging question of are my security controls working reliably, what threats have by passed these controls, and are they doing anything that could negatively impact operations.

Attivo Deployment

The ThreatDefend™ platform provided this financial services company with global early threat detection and the ability to easily and scalably provide deception into remote locations without requiring additional hardware.

OVERVIEW

The Vice President of Cybersecurity required better visibility into their large and diverse international network that spanned corporate and remote offices. Like many large enterprises, even with a mature and well-implemented security posture, they faced the challenge of fully understanding what threats were within their environment and how likely they were to cause harm. After researching numerous detection security controls, they recognized deception technology as a solution to a range of challenges. Additionally, they saw value in the platform's ability to gather adversary intelligence including TTPs, IOCs, and threat intelligence that provided insight into the attacker's entry point, methods, and motivation.

CHALLENGE

With a diverse infrastructure, and assets in numerous countries that carried a broad range of regulatory and legal requirements, gaining adequate visibility into remote locations and providing consistent data security compliance was especially challenging. The specific restrictions in some regions posed additional challenges requiring unique solutions. The organization needed a solution that would be easy to deploy and manage, even in remote locations, and would not unduly increase their information security team's workload.

SOLUTION

The organization selected the Attivo Networks® ThreatDefend™ platform, utilizing the BOTsink® server to deploy decoys, ThreatDirect™ to project decoys into remote locations, and ThreatStrike® to place deception credentials and other assets on the endpoints. The organization used staged rollouts, to test detection strategies and application of deception techniques. Though a global deployment is a massive undertaking, the customer was pleasantly surprised at how simple the deployment process was with the use of machine learning. This automation feature made it incredibly easy to prepare, deploy, and update deceptions while maintaining environmental authenticity and attractiveness for an attacker.

ROI

The Vice President of Cybersecurity had researched a range of potential technologies and vendors before selecting Attivo Networks Deception Technology as the most effective and efficient way to get the visibility and early detection they needed in their complex international environment. The scalability and ease of deployment, use, and maintenance made the ThreatDefend platform an excellent fit for this organization's environment. Additionally, the reliable, accurate, and actionable alerts and forensic capabilities improved the information security team's efficiency and required no additional operational resources.

OUTCOME

The organization added deception technology in order to proactively achieve visibility, especially in remote locations, and provide improved reporting and forensics capability across their widely varied sites. The organization's experience demonstrates that the ThreatDefend platform is easy to deploy and maintain at scale. Additionally, the solution provides insight into activity at the network and endpoint with high-fidelity, accurate alerts. Deception technology has given them "eyes inside the network" visibility they were not getting from any other solutions. The ability to gather adversary threat intelligence was also powerful in fortifying their defenses.

ATTIVO NETWORKS PRODUCTS

The company focused on visibility and forensics capabilities, installing BOTsink® servers to provide decoys, ThreatDirect™ to allow them to project decoys seamlessly into remote locations, and ThreatStrike™ to place deception credentials and other deceptive assets on endpoints throughout the organization.

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend™ Deception Platform provides a comprehensive platform for proactive security and accurate threat detection within user networks, data centers, clouds, and a wide variety of specialized attack surfaces. The portfolio includes expansive network, endpoint, application, and data deceptions designed to misdirect and reveal attacks from all threat vectors. Advanced machine-learning makes preparation, deployment, and operations fast and simple to operate for organizations of all sizes. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations automate the blocking, quarantine, and threat hunting for accelerated incident response. Attivo has won over 65 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com