CASE STUDY

Attivo NETWORKS

PRIVATE SECTOR BANK IN INDIA CHOOSE ATTIVO NETWORKS TO ADD DECEPTION TECHNOLOGY FOR ENHANCED CYBERSECURITY

ORGANIZATION

A leading private sector bank in India with over four thousand branches and assets valued at nearly 20 billion dollars.

SITUATION

As a large private sector bank in India, this organization is subject to the extensive regulations regarding cybersecurity, privacy, etc. The bank was familiar with deception technology, having deployed a competing solution over two years ago. The use of deception is stipulated as a requirement in the Reserve Bank of India's Cybersecurity Initiative[1]. However, this organization was not seeing the expected value and performance with the solution they had previously deployed. They were not initially looking to deploy additional/ replace their deception technology but were receptive to performing a Proof of Concept (POC) deployment after speaking with the Attivo Networks team.

The local team performed a successful POC and demonstrated the superiority of the Attivo Networks ThreatDefend platform. The bank's security team took note of the ThreatDefend platform's ability to project deception into remote locations and operate seamlessly in a cloud environment. The ability to leverage the "Sinkhole" capability in the Attivo solution for gathering forensic and safely study active attack information was also seen as a measurable advantage over their existing solution.

The bank decided to deploy the ThreatDefend platform to augment their existing solution with a view towards fully replacing it with the Attivo solution.

SOLUTION

The Bank had an existing deception solution to comply with the Reserve Bank of India's security regulations, which specifies that organizations must deploy some form of "Honeypot" technology – from which modern deception technology evolved[2]. While their existing solution technically met the RBI requirements, it did not provide the breadth of coverage the bank required and was not delivering the level of confidence they expected. The ThreatDefend platform delivered the missing pieces and filled in the gaps in their existing solution.

[1] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF

[2] https://attivonetworks.com/documentation/Attivo_Networks-Deception_Technology_Honeypot.pdf

The ThreatDefend solution also offered native 3rd party integration with the other components in their security stack, which made the cybersecurity team more efficient and more effective. As they had noted during the POC, the platform gave them improved visibility and forensic information on adversaries that might penetrate their perimeter.

ATTIVO NETWORKS PRODUCTS

The bank installed a range of Attivo Networks products to implement their ThreatDefend platform deployment. Starting with multiple BOTsink servers as hardware appliances to give full coverage of their environment, and adding a cloud based BOTsink to directly cover their cloud presence. For management, they installed the cloud-based version of Attivo Central Manager (ACM) to manage the entire deployment.

To protect their remote sites and branch offices, the bank selected the ThreatDirect solution to project deception into the remote sites. By creating secure tunnels from the ThreatDirect VM back to a BOTsink server, the bank gets the full deception capabilities granted by the BOTsink without requiring additional hardware or overhead.

For endpoint protection, they deployed the Attivo ThreatStrike solution. The ThreatStrike solution places deceptive credentials and other assets on servers and workstations that will direct an attacker away from production assets and into the deception environment. By directing attacks into the high-interaction decoys, the bank would not only protect their production assets, but would also gain forensic insight into the attacker's methods and what they were targeting.

IMMEDIATE VALUE

During the Proof of Concept phase with the Attivo team, the bank saw the improved performance over their existing solution and where the ThreatDefend platform provided the missing pieces in their deception layer while filling the gaps in their security stack. They also noted that the high-fidelity alerts with no false positives made their incident response team more effective.

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 offers comprehensive and accurate threat detection for user networks, data centers, clouds, and a wide variety of specialized attack surfaces. A deception fabric of network, endpoint, application, and data deceptions efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning simplifies deployment and operations for organizations of all sizes. Automated attack analysis, forensics, actionable alerts, and native integrations accelerate and streamline incident response. The company has won over 100 awards for its technology innovation and leadership.

www.attivonetworks.com