Attivo NETWORKS®

Large Retailer uses Deception for Active Acquisition Strategy

Company	Situation	Solution
A large retail organization.	The organization has an active acquisition strategy and a key priority in their integration strategy is to establish visibility into the acquired networks to understand the vulnerabilities that may exist.	The Attivo ThreatMatrix Deception and Response Platform™ provides needed visibility into the network to determine the presence of active threats. The system is based on interaction and engagement with decoys and traps deployed throughout the enterprise, and alerts on application misconfigurations that may reflect risk exposure.

Overview

This retail organization was actively investigating and assessing the security controls of their broader affiliate organizations. The organization was concerned that the affiliate networks did not have the appropriate level of security maturity and defenses to quickly detect cyber attackers in line with their own enterprise standards. Specifically, they were worried that the acquired networks had hidden or time triggered malware that could move laterally across affiliate networks and potentially breach their corporate network, leading to exfiltration of company and customer data.

Challenge

The acquired organization had basic security but little visibility into any threats that have made their way inside the network. Because of the lack of visibility, the infosec teams lacked confidence that these networks weren't already compromised in some way. A compromised affiliate network posed a risk to not only that subsidiary, but to the broader enterprise as well. Any in-network malware could potentially spread to the larger organization, and create significant risk to customer confidence, revenue, and their brand reputation. The team needed a reliable way to know if the network was compromised, as well as visibility into the acquired organization's overall health and risk associated with its end-points. Beyond gaining this initial visibility, they needed a reliable way to detect any new threats inside the network that could occur in the future.

Solution

The large retail organization deployed the ThreatMatrix Deception and Response Platform across the acquired company's data centers and end user networks. The ThreatMatrix Platform provided them with visibility into lateral movements and reconnaissance actions conducted by malware and malicious actors. The ThreatMatrix BOTsink engagement servers were customized to match the production environment, creating decoys that reflected the same configurations as their counterpart production critical assets. These decoys presented an attacker with an attractive target that could engage, trap, and safely observe the tactics, techniques, and procedures being leveraged against them.

In addition to the ThreatMatrix Platform, the organization has implemented the Attivo ThreatStrike End-point Suite. This solution creates customized deceptive credentials that are deployed to thousands of end points, to identify compromises that rely on credential theft. These agentless, deceptive credentials entice and divert an attacker into engaging with the Attivo engagement servers, thereby revealing themselves, and allowing Attivo to analyze the threat. With deception deployed, the organization gained visibility into threats within the subsidiary's network. In one specific instance, they identified suspected Ransomware that was active in the environment and the ThreatMatrix Platform gave them the detailed attack forensics to remediate the identified threat.

Lastly, the organization utilizes the ThreatMatrix Platform's capabilities for secondary phishing and malware analysis. The Phishing and Malware Analysis Platform automatically executes suspicious files and URLs, providing detailed analysis to the incident response team, ensuring that they have the evidence to determine if the sample can safely be executed, or if it is malicious in nature.

ROI and Outcome

The team efficiently gained knowledge and visibility of the acquired network while adding a much-needed capability for early threat detection to identify any future attacks. By deploying the Attivo solution, the team accelerated their ability to establish visibility into their network, and helped them gain additional insight into the security gaps that exist. They now have real time, highly reliable detection of threats inside the network, and have gained an ability to understand the nature and mechanisms of an attack. They can detect external threat actors, malicious insiders, and advanced malware and APTs. In addition, they have enabled end users, with the click of a button, to submit suspicious emails for automated analysis.

Attivo Products

Attivo ThreatMatrix Deception and Response Platform, ThreatStrike deceptive credentials, the Attivo BOTsink engagement servers for malware analysis and decoys.

About Attivo Networks

Attivo Networks® is the leader in deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber-attacks. The Attivo ThreatMatrix™ Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. Attivo Camouflage dynamic deception techniques and decoys set high-interaction traps to efficiently lure attackers into revealing themselves. Advanced attack analysis and lateral movement tracking are auto-correlated for evidence-based alerts, forensic reporting, and automatic blocking and quarantine of attacks. For more information visit www.attivonetworks.com.