CASE STUDY

LARGE RETAILER USES DECEPTION FOR ACTIVE ACQUISITION STRATEGY

COMPANY

A large retail organization.

SITUATION

The organization has an active acquisition strategy, and a key priority in its integration strategy is to establish visibility into the acquired networks to understand the vulnerabilities that may exist.

SOLUTION

The Attivo Networks ThreatDefend® Detection and Response platform provides needed visibility into the network to determine the presence of active threats. The system detects confirmed interaction and engagement with decoys and traps deployed throughout the enterprise, and alerts on 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 detect cyber attackers quickly, in line with their 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 the exfiltration of company and customer data.

CHALLENGE

The acquired organization had basic security controls but little visibility into any attackers that successfully infiltrated their network. This lack of awareness gave the Infosec teams low confidence that these networks did not already have an active compromise. A breached 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 corporate network and create a significant threat to customer confidence, revenue, and brand reputation. The team needed a reliable way to know if attackers had compromised the network, as well as visibility into the acquired organization's overall health and risk associated with its endpoints. Beyond gaining this initial visibility, they needed a reliable way to detect any new threats inside the network that could surface in the future.

SOLUTION

The sizeable retail organization deployed the ThreatDefend Detection and Response platform across the acquired company's data centers and end-user networks. The ThreatDefend platform provided the organization with visibility into lateral movements and reconnaissance activities from malware and malicious actors.

The BOTsink® engagement servers projected decoys customized to match the production environment, representing the same configurations as their counterpart critical production assets. These decoys presented attackers with an attractive target that would engage, trap, and safely observe the attacker's tactics, techniques, and procedures as well as record Indicators of Compromise (IoC) for additional threat intelligence.

In addition to the ThreatDefend platform, the organization implemented the Endpoint Detection Net (EDN) Suite ThreatStrike®. This agentless solution provides a first line of defense against credential theft, creating customized deceptive breadcrumbs in the form of credentials and lures that deploy to thousands of endpoints. These fake credentials entice and divert attackers into engaging with the decoy engagement environment, thereby revealing themselves and allowing the platform to analyze the threat.

After deploying the platform, 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 ThreatDefend platform provided the detailed attack forensics necessary to remediate the infection before it could spread to the corporate network.

The organization also used the ThreatDefend platform's capabilities for secondary malware analysis and submission of suspicious emails. The built-in malware analysis sandbox automatically executed suspicious files and URLs, providing detailed reports to the incident response team and the evidence to determine if the sample is safe or malicious.

ROI AND OUTCOME

The organization 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 ThreatDefend platform, the organization accelerated its ability to establish visibility into the entire corporate network and helped it gain additional insight into the security gaps that exist.

The organization now has real-time, highly reliable detection of threats inside its environment, and the analysis capabilities to understand the nature and mechanisms of an attack. It can detect external threat actors, malicious insiders, advanced malware, and advanced persistent threats (APT). The organization has also enabled its end-users to submit suspicious emails for automated analysis with a simple click of a button.

ATTIVO PRODUCTS

Attivo ThreatDefend Detection and Response platform, Endpoint Detection Net (EDN) Suite's ThreatStrike® solution, and the Attivo BOTsink® solution for malware analysis and decoys.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com