Semiconductor Company Implements Deception to Stop Man-in-the-Middle Attacks

Company	Situation	Solution
A global semiconductor manufacturer.	The company needed to protect their IP and had already experienced a breach by a Chinese hacker group. Current solution generated high false positives.	Implementing the Attivo ThreatDefend™ Platform gave the team the visibility needed to detect man-in-the-middle attacks, advanced threats, and replace false positves with high-fidelity alerts.

Overview

The organization had been infiltrated by a Chinese hacker group using a man-in-the-middle attack that was able to successfully bypass their prevention systems and exfiltrate critical data. The security organization was instructed to improve their detection capabilities and get more reliable insight into threats that may be using tactics to steal credentials or use social engineering to penetrate the network. They needed a solution that would be able to detect subtle, in-network attacks as well as phishing and advanced threat protection.

Challenge

The biggest challenge this organization was facing was manpower. In addition to the numerous alerts generated by their prevention and other security devices, the infosec team was receiving 45-50 suspicious emails a day. The team was so severely burdened that they were rarely able to go through the backlog and investigate all of the potential threats that they were alerted to.

Solution

To ensure full coverage, the organization deployed the Attivo ThreatDefend Deception and Response Platform on all the VLANs in their network to specifically detect man-in-the-middle and lateral movement attacks. Additionally, the infosec team took full advantage of the analysis engine provided by the ThreatDefend Platform to more efficiently correlate attack information and for forensic reporting. Additionally, they automated the phishing email analysis process, providing a consistent way to analyze suspect emails and ensuring that all submitted samples are analyzed. The team was also able to achieve control of their alert volume since the Attivo solution alerts were all based on engagement and all represented either a threat or a misconfiguration that could become an attacker entry point.

Since the organization has many locations, they needed a solution that would be able to protect their networks that are physically very far apart. Using virtual versions of the ThreatDefend solution, they deployed deception technology across offices in three different countries spanning two continents to cover their manufacturing, design, and management offices. Given the efficiency of this solution, deployment was fast and did not require additional staff to operate a global deployment.

ROI

With the ThreatDefend Deception Platform, the information security team saves critical time through the automation of malware and suspicious email analysis. Moreover, the high-fidelity alerts provided by the ThreatDefend Platform allow the team to focus their attention on substantiated threats rather than false positives generated by other devices.

The infosec team is very pleased with the accurate and high-fidelity alerts and that they now have the visibility into their network that was unachievable previous to their adoption of deception technology. Now, not only can they detect man-in-the-middle and other advanced threats, but they can also detect infected machines in their network and threats that are moving laterally between machines. The detection capabilities they have allows them to focus their attention on accelerated incident response and faster remediation as opposed to analyzing alerts.

Outcome

Adding the ThreatDefend Platform to their suite of security devices fundamentally strengthened the organization's security posture by adding in real-time detection and improving threat analysis and attack remediation. Previously, they were vulnerable and had experienced the impact of man-in-the-middle attacks. The organization now has visibility and early detection coverage across multiple sites, accurate threat alerting, and the ability to report back to management on how they can and will detect threats within their network.

Now, not only can they detect man-in-the-middle and other advanced threats, but they can also detect infected machines in their network.

Attivo Products

The Attivo ThreatDefend Deception and Response Platform with multiple BOTsink engagement servers.

About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com