CASE STUDY

SEMICONDUCTOR COMPANY IMPLEMENTS DECEPTION TO STOP MAN-IN-THE-MIDDLE ATTACKS

COMPANY

A global semiconductor manufacturer.

SITUATION

The company needed to protect their IP and had already experienced a breach by a Chinese "hacker" group. The current solution generated a high rate of false-positives.

SOLUTION

Implementing the ThreatDefend® Platform gave the team the visibility needed to detect Man-in-the-Middle attacks, advanced threats, and replace false positives with high-fidelity alerts.

OVERVIEW

A Chinese "hacker" group infiltrated the organization and used a Man-in-the-Middle (MitM) attack to steal credentials that allowed it to access and exfiltrate critical data. The organization instructed the Infosec team to improve their detection capabilities and get more reliable insight into threats that stole credentials or used social engineering to penetrate the network. They needed a solution that could detect subtle, in-network attacks as well as protect from phishing and advanced threat activity.

CHALLENGE

The organization faced considerable personnel and resources challenges for its Infosec team. In addition to the numerous alerts generated by detection, prevention, and other security controls, the Infosec team received 45-50 suspicious emails a day. The team rarely had the available time or analysts to process the backlog and investigate all of the potential threats for which they received alerts.

SOLUTION

To gain full coverage of its environment, the organization deployed the ThreatDefend® Deception and Response Platform on all the VLANs in their network expressly to detect MitM attacks and other lateral movement activity. Additionally, the Infosec team took full advantage of the platform's attack analysis engine to more efficiently correlate attack information and for forensic reporting. Moreover, they automated the phishing email submission process, providing a consistent way for users to send suspect emails for analysis. The team managed to achieve control of their alert volume since the alerts the ThreatDefend platform generated resulted from direct attacker engagement and represented either a misconfiguration, a policy violation, or an actual security incident.

Since the organization has many locations, it needed a solution that would cover both its on-premises and remote networks equally. Using virtual versions of the ThreatDefend platform, it deployed decoys and deception across offices in three different countries spanning two continents to cover its manufacturing, design, and management offices. Given the efficiency of this solution, deployment was fast and did not require additional staff to operate a global rollout.

ROI

With the ThreatDefend platform, the Infosec team saved critical time by automating malware and phishing email analysis. Moreover, the high-fidelity alerts provided by the ThreatDefend platform allowed the team to focus their attention on substantiated threats rather than false positives generated by other security controls.

The Infosec team is delighted with the accurate and high-fidelity alerts as well as their visibility into the network that they could not achieve before their adoption of deception technology. Now, not only can they detect MitM and other advanced attack activity, but they can also identify infected systems in their network along with laterally moving threats. The detection capabilities they gained allows them to focus their attention on accelerating incident response and remediating incidents faster as opposed to investigating and analyzing alerts.

OUTCOME

Adding the ThreatDefend platform to its suite of security controls fundamentally strengthened the organization's security posture by adding in real-time detection while improving threat analysis and attack remediation. Previously, they were vulnerable and had experienced the consequences of MitM attacks. The organization now has visibility and early detection coverage across multiple sites, accurate threat alerting, and a stronger overall security posture to defend against future attacks.

ATTIVO PRODUCTS

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

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides organizations of all sizes with an active defense for early and accurate threat detection. The Attivo ThreatDefend® Platform delivers comprehensive detection for on-premises, cloud, and specialized attack surfaces with a deception fabric designed to efficiently misdirect and reveal attacks from all threat vectors. High-fidelity alerts are backed with company-centric threat intelligence and automated attack analysis, forensics, native integrations streamline incident response. The company has won over 120 awards for its technology innovation and leadership. Learn more: www.attivonetworks.com