CASE STUDY

MAJOR ENTERTAINMENT ORGANIZATION DEPLOYS DECEPTION FOR INSIDER THREAT VISIBILITY

COMPANY

Major entertainment organization.

SITUATION

The organization is extremely concerned about targeted and stolen credential attacks on its intellectual property from both insiders and external threat actors. Its current solutions were not sufficient and generated a high volume of false positives.

SOLUTION

Deployment of the ThreatDefend® platform on multiple subnets and wide distribution of the ThreatStrike suite deceptive credentials to close visibility gaps and minimize risk.

OVERVIEW

This organization conducts significant product launches and is a leader in an extremely competitive entertainment market that is a prime target for cyberattacks. They consider their intellectual property very valuable, and a leak of data or projects would significantly diminish their competitive advantage in the landscape and, as a nature of the industry, have a tremendous impact on their revenue stream. For this organization, a breach is unacceptable, and avoiding one is a top priority.

The organization is primarily concerned with attacks leveraging stolen credentials. With the right credentials, a malicious actor could easily infiltrate critical assets to steal intellectual property for financial gain. Given the high value of their intellectual property, visibility into malicious activity from insiders in their organization was also of critical importance. They needed a discrete detection tool that would give them real-time visibility into threats within the network and misconfigurations that could lead to an attack. The solution also required that it not be easily detected by insiders within their organization. The company has gone to great lengths to set traps for attackers and limit the number of people within their organization who know of the Attivo solution deployment.

CHALLENGE

The organization's extensive network drove their most significant challenges, and that they had multiple high-traffic locations with little to no visibility into any activity that could be indicative of a stolen credential attack. There was no way to distinguish between an employee using their credentials to access a project and a malicious actor using stolen credentials to take intellectual property. This lack of visibility and clarity proved extremely troublesome for the organization because it forced the Infosec team to try to bridge their visibility gaps with multiple different solutions that generated a high volume of alerts, with a high rate of false positives. Moreover, the team had to spend resources monitoring the solutions, and, given there was not enough capacity to research every alert generated, they had to investigate every incident because they did not have enough actionable information to true positives from false-positive alerts within the noise. The time burden of false positives had a tangible impact on the team's ability to successfully protect their intellectual property and their bottom line.

The Infosec team needed a solution that would not only monitor and thwart stolen credential attacks but also cut through the noise of their network with substantiated, actionable alerts.

SOLUTION

The organization implemented the ThreatDefend Deception and Response Platform throughout their network. The security team deployed multiple devices inside the data center to protect and monitor critical intellectual property as well as on user networks to monitor for stolen credential attacks and visibility into attacker lateral movement. They used the ThreatStrike® endpoint deception suite, placing deceptive credentials throughout their network on end-user devices. These deceptive credentials looked authentic but pointed to network decoys, and acted as alarm bells for attackers stealing usernames and passwords and using them to escalate privileges. If attackers attempted to log in with the deceptive credentials, the team received an alert of the illicit activity, the credentials the attackers used, and the system the activity originate3d fro, enabling the team to act quickly to remediate the situation.

ROI

The information security team gained significant visibility into stolen credential attacks by installing the ThreatDefend platform for continuous threat management. By employing the ThreatStrike suite deceptive credentials, they not only increased visibility but also gained early detection against any potential threat activity through stolen credential use. Visibility and early detection against attacks coupled with reduced false-positive alert noise gave them the means to defend their bottom line efficiently. The awareness provided by the ThreatStrike suite offers the Infosec team early detection of malicious activities in their network long before the attack can have a chance to exfiltrate critical assets. Achieving early detection into insider and external threats with the ability to detect stolen credential attacks has significantly reduced the risk of a breach and has simplified their incident response with actionable alerts and a means to reduce their time to respond and remediate.

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 100 awards for its technology innovation and leadership.
Learn more: www.attivonetworks.com