CASE STUDY

REAL ESTATE INVESTMENT FIRM TESTS ADSECURE

Red Team unaware of redirection into Deception AD environment

ORGANIZATION

A major US-based real estate investment company with over 200 properties.

SITUATION

The organization regularly conducts annual Red team testing to evaluate their security readiness. As part of their next scheduled test, they decided to assess the ThreatDefend® Platform. In addition to the network and endpoint decoys, they tested the ADSecure solution to evaluate its effectiveness in Active Directory (AD) reconnaissance activity that adversaries frequently use. The organization provided the Red Team with a laptop as their entry point.

SOLUTION

The organization configured the deception environment to match their current network assets. They installed the ADSecure agentless solution on the entry laptop to hide all the production domain controllers, administrator accounts, and service accounts, and return nothing but decoy results. They also installed a virtual BOTsink deception appliance to run the decoy environment consisting of network decoys and deceptive credentials. They created an equal amount of decoy AD domain controllers to match their production DCs and did the same for the domain administrator and service account credentials.

The Red Team used a variety of tools and ran queries targeting high-value accounts and objects, such as service accounts, Kerberos tickets, and domain controllers. The team evaluated whether or not the ADSecure module could effectively hide high-value AD objects, seamlessly present deceptive data that would validate against a decoy AD infrastructure, and generate alerts on such activity without affecting the production environment.

ATTIVO NETWORKS PRODUCTS

The organization deployed the ThreatDefend platform with the ADSecure solution for the security evaluation. The deployment consisted of a BOTsink virtual appliance to manage the deception environment, the ThreatStrike endpoint suite, and the ADSecure module. The organization configured one of the decoys as a Windows AD Controller and generated authentic-looking credentials and other objects to fill it.

IMMEDIATE VALUE

The ThreatDefend Platform with the ADSecure solution successfully deceived the Red team without touching the production AD controllers. Regardless of whether the testers used built-in commands, MS PowerShell, or custom tools such as Bloodhound, the solution hid critical accounts and gave decoy information in its place. This false information validated against a decoy AD controller within the ThreatDefend platform deception environment, making them appear authentic. The platform also generated alerts and captured all activity whenever the testers followed the decoy data, whether through account use, connecting to network sessions, or other actions on the decoy. The Red Team spent most of their time breaking into the deceptive AD without ever interacting with the production domain controllers. The organization considered this result a successful validation of the ADSecure capabilities.

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