CASE STUDY

FINANCIAL SERVICES FIRM DEPLOYS ADSECURE DURING RED TEAM EVALUATION

Red team diverted to deception ad servers for over two days

ORGANIZATION

A commercial bank with over $100 billion in total assets.

SITUATION

The bank annually conducts a Red Team test to evaluate their security posture. While they have extensive security controls in place, the Red Team still managed to succeed each year. In preparation for their pending Red Team, the organization installed the Attivo Networks ThreatDefend® platform with the just-released ADSecure® module specifically to address its Active Directory security needs.

SOLUTION

Attivo Networks had recently introduced the ADSecure solution as part of the ThreatDefend platform to help protect Active Directory. In prior security evaluations, the Red Team had successfully leveraged the bank's AD to compromise systems and move laterally throughout the network. Knowing that AD was a high priority target for the Red Team in the next test, the bank deployed the ThreatDefend platform and ADSecure to gauge its effectiveness in protecting critical AD accounts.

ATTIVO NETWORKS PRODUCTS

The bank deployed the ADSecure solution as part of a deception deployment to create an engagement environment with core deception capabilities for their Red Team test. This included the BOTsink deception appliance to provide deception capabilities consisting of network decoy systems and servers, along with the central management and event dashboards. The combined deployment provided full alerting and forensic collection to the Blue Team.

IMMEDIATE VALUE

The Red Team expected deception technology in the environment, so after they collected credentials on the entry systems, they validated the information with Active Directory. Despite their preparation, the authenticity of the ADsecure fake data was so compelling that the Red Team believed the deception and used the fake accounts, which validated the artificial AD environment. They attacked the fake AD controller for over 2.5 days until the organization told them to stop attacking the decoys and go elsewhere. While the Red Team engaged with the decoy environment, the platform captured all of their activity, including dropped payloads and exploit tools. This result validated the effectiveness of the ADSecure module and the ThreatDefend platform as a whole.

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 130+ awards for its technology innovation and leadership.

Learn more: www.attivonetworks.com

ANCS050620
www.attivonetworks.com