CASE STUDY

BFSI ORGANIZATION ADOPTS ATTIVO SOLUTIONS TO DERAIL RANSOMWARE

ORGANIZATION

A large organization from Banking, Financial Services, and Insurance (BFSI) sector

SITUATION

Attivo Networks solutions detected ransomware attacks on several endpoints at the bank delivered via email spam embedded with web links.

SOLUTION

The security team successfully protected the organization from the ransomware attacks using the ThreatDefend platform with the EDN DataCloak function.

OVERVIEW

Banking and financial organizations remain the top target for ransomware attacks by cybercriminals. The organization is one of the large banks in the APAC region that provides a range of financial products and services and has an existing ThreatDefend platform deployment. The bank offers various financial services to its customer base and has many subsidiaries, sponsored institutions, and joint ventures distributed globally. In early January of 2021, endpoints at the bank got hit by a ransomware attack. This payload drop got installed on a victim's endpoint when the user opened a malicious file obtained via Instant Messaging (IM), email, social network, or by visiting a malicious site. The payload drop loaded during system bootup and all targeted Windows-OS-based computer systems.

THE CHALLENGE

Ransomware attacks often targeted vulnerable endpoints at the bank, encrypted files, and accessed shared files, folders, and network drives. This particular ransomware strain also generated Web/DNS queries to several malicious websites and attempted to spread across connected networks via SMB.

- The bank's traditional cybersecurity solutions could not detect the ransomware strain or its payload drops early in the attack chain.
- Their existing endpoint security solutions could not prevent ransomware propagation activities to the local folders, network, or cloud mapped shares.
- The bank's security team did not employ forensic intelligence to analyze domain or web queries generated by the malware payload.

ATTIVO NETWORKS SOLUTION

Attivo Networks solutions enabled the bank's security teams to secure their IT infrastructure while pursuing their new digital business initiatives. The ThreatDefend® platform combats ransomware, and related malware, using a combination of the BOTsink® server hosting decoy systems, Endpoint Detection Net (EDN) suite. These solutions create decoy network file servers and place deceptive assets on the endpoints, including decoy credentials and fake file shares while hiding sensitive or critical data and storage from direct access by unauthorized processes. As ransomware attacks will typically attack local and network files, they will also engage assets stored on the fake mapped network shares on the decoy file servers. Any contact with the decoy assets immediately triggers an alert and engages the attacker within the deception environment that records their activities. Their attack becomes preoccupied within a virtual reality, giving the incident response team time to react.

BENEFITS

- Early detection of ransomware activities
- Blocking ransomware activities and engagement
- Concealing files, folders, and mapped network drives
- High fidelity alerts early in the attack
- Malware intelligence and forensic data collection

IMMEDIATE VALUE

Before the attack, the bank had evaluated its endpoint security strategy and deployed the Attivo Networks ThreatDefend® platform and Endpoint Detection Net (EDN) components to protect the network servers, endpoints, and Active Directory. The Attivo solutions detected the ransomware attack early. Hence, the bank's IT team could take preventative action to mitigate the risks associated with the ransomware payloads dropped on the compromised endpoints. The EDN suite's DataCloak function enabled the security team to prevent malicious activities by hiding and denying access to sensitive or critical data, preventing attackers from exploiting the bank's data. The EDN suite's ADSecure solution enabled the security team to detect attacker attempts to gather data from Active Directory and misdirect them with fake results to the decoys for engagement. The Attivo solutions successfully prevented the ransomware attack.

ATTIVO PRODUCTS USED

ThreatDefend® Deception Platform

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications and MITRE® Shield, and its capabilities tightly align to the MITRE ATT&CK® Framework. Attivo has won over 130 awards for its technology innovation and leadership.
www.attivonetworks.com