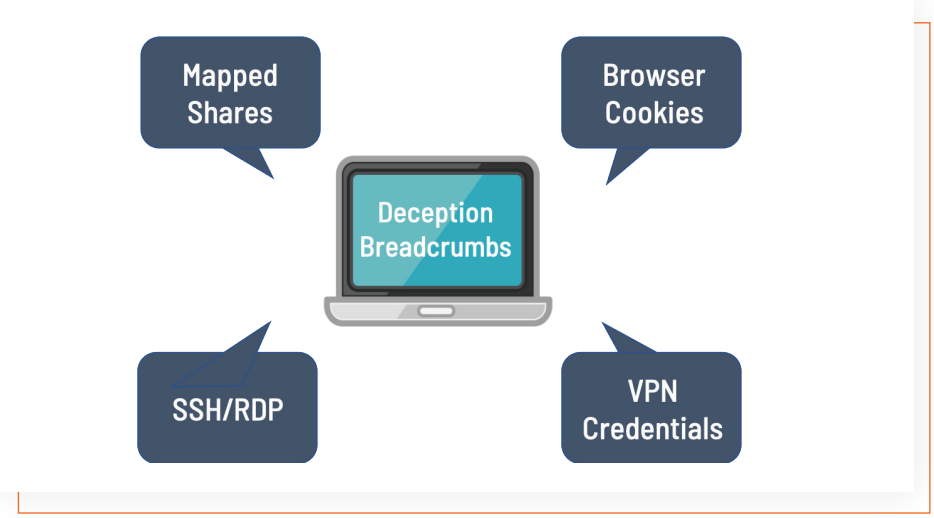
THREATSTRIKE® ENDPOINT DECEPTION SOLUTION

The Attivo ThreatStrike® component of the Endpoint Detection Net (EDN) suite provides early and accurate detection of targeted attacks on endpoints and servers. Customizable and non-intrusive, this deception technology places bait and breadcrumbs that lead to an engagement server, which raises an alert, analyzes attacks, and activates actions to quarantine the infected system.

Attackers will compromise computers to steal passwords and hashes to reach sensitive network data that they can then use to move laterally within the network and escalate privileges to advance their attack. The EDN ThreatStrike component is an endpoint capability that dynamically plants deceptive credentials, lures, and network drives for ransomware detection.



AUTOMATED ATTACK ANALYSIS AND FORENSIC REPORTING

The Attivo EDN ThreatStrike component provides real-time attack analysis and alerts on the use of planted deceptions. Once an attacker takes the bait and tries to use the deceptive credentials, it raises an alert on the standalone EDN Manager or the Attivo BOTsink server. These identify the infected endpoint, analyze the attack, and provide third-party integrations to share information and automate response actions with prevention devices. Additionally, it can query SIEM applications to check and raise alerts based on the failed login use of deception credentials, providing accurate alerts for notifications that would typically be buried and lost in logs of data. The BOTsink analysis engine also goes one step further than typical sandboxes by capturing and analyzing memory forensics as part of the attack analysis. All too often, sandboxes lose this data, and along with it, the attacker's tracks. This unique benefit will often provide the much-needed insight to truly understand and quickly respond to an attack.

RANSOMWARE SOLUTION

Ransomware works by infecting and encrypting the network-attached shares on a device. The Attivo EDN ThreatStrike endpoint lures combat this by mapping hidden SMB shares to the BOTsink decoy engagement VMs. When ransomware infects the device, it encrypts the files in the mapped decoy network shares instead of the production shares. In testing trials of this technology, the Attivo high-interaction deception slowed down the encryption attack cycle by a factor of 25, keeping the ransomware busy encrypting a continuous feed of deception files. Analysis of Petya/NotPetya and WannaCry attacks by Attivo Labs demonstrate the effectiveness of deception technology in detecting and stopping ransomware attacks. Another function of the EDN solution is hiding and denying unauthorized access to real files, folders, shares, and credentials, preventing the ransomware from accessing sensitive data to encrypt.

CONCLUSION

It is critical to detect the attacker the moment they penetrate the network. The EDN ThreatStrike capabilities provide crucial detection for credential-based attacks that anti-virus and other forms of perimeter defense inherently miss. Regardless of the attack vector that an attacker uses to break out from an endpoint, the EDN suite provides a comprehensive detection coverage. Organizations can purchase the EDN suite can as standalone or part of the ThreatDefend platform, which offers network, endpoint, data, and application deceptions to efficiently and accurately reveal attacker presence, analyze the attack, and simplify incident response.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership.
For more information, visit www.attivonetworks.com.