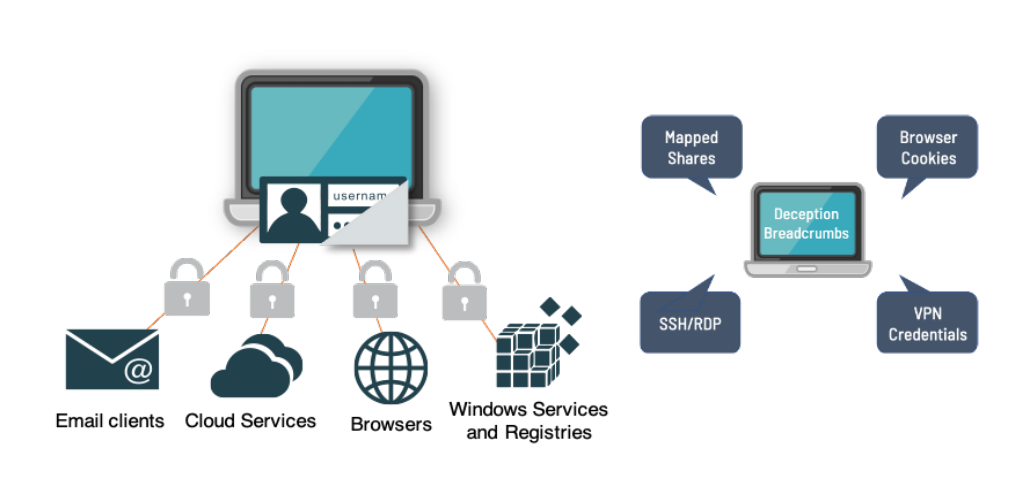
Endpoint Detection Net Suite: ThreatStrike Solution

The Attivo ThreatStrike® component of the Endpoint Detection Net (EDN) suite provides customizable and non-intrusive credential protection and early detection of targeted attacks on endpoints and servers.

Attackers compromise computers to steal passwords and hashes to reach sensitive network data so they can use it to move laterally within the network and escalate privileges to advance their attack.

The EDN ThreatStrike solution hides and denies unauthorized access to credentials by binding them to applications, and dynamically plants deceptive credentials, lures, and network drives. These capabilities stop an attacker's theft of real credentials, mislead and misdirect the attacker for threat intelligence gathering, and detect ransomware attacks.



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 protection against 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 comprehensive credential protection and endpoint 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®, experts in Identity Detection and Response (IDR), provides an innovative defense to protect against identity compromise, privilege escalation, and lateral movement attacks. The company's solutions deliver unprecedented visibility to security exposures and attack paths and prevent and derail attack escalation activities across endpoints, Active Directory, and cloud environments. A combination of patented data cloaking, misdirections, and cyber deception innovations protects identities and comprehensively detects threats. These solutions are an integral part of NIST Special Publications, MITRE Shield, and its capabilities tightly align to the MITRE ATT&CK Framework. Attivo Networks has won 150+ awards for its technology innovation and leadership. www.attivonetworks.com.