USE CASE

Attivo
NETWORKS®

DECEPTION FOR DERAILING RANSOMWARE AND RELATED MALWARE ATTACKS

THE THREAT

Ransomware has proven a particularly destructive threat for organizations of all sizes and industries. This form of attack remains a leading attack vector that presents itself with many complex practical and moral issues when carried out. Its most common variants encrypt on the local system and network shares, then demand some form of ransom to obtain a decryption key. Victims of these attacks may pay the ransom, only to find the provided encryption key doesn't work, or that the attacker had no intention of providing a working key in the first place. The goal in this case may not have been the ransom, so much as disrupting the organization's normal activities.

Related attacks use similar techniques to spread, but do not encrypt the target files. These attacks will delete or corrupt target files, rendering them unusable by the victim. The goal in these attacks are designed more to cause a disruption rather than extract a ransom.

THE CHALLENGE

An initial ransomware or related malware infection often starts with an unsuspecting user opening an email attachment that carries the malicious payload. The malware attacks the victim's system, encrypting or compromising files on the host, and accessible file shares, then spreads to other hosts if possible.

Network file shares can be especially vulnerable, providing both a fertile ground for the malicious code to encrypt or corrupt files, and as a pathway for the infection to spread. An infected host with access to important files can cause significant damage before an organization recognizes the situation.

Mitigation and remediation after a ransomware attack can be time consuming and expensive, making prevention, early detection, and the ability to slow an attacker's progress before it does extensive damage a priority.

ATTIVO NETWORKS® SOLUTION

The Attivo Networks® ThreatDefend platform combats ransomware, and related malware, using a combination of the BOTsink® server hosting decoy systems, including network file shares, and the

ThreatStrike® solution that places deceptive assets on the endpoints, including deceptive credentials and fake file shares.

As these attacks will typically attack both local and network files, they will also engage assets stored on the BOTsink server. Any contact there immediately triggers an alert and engages the attacker within the deception environment so that there attack becomes preoccupied within a virtual reality, giving the incident response team time to react.

IMMEDIATE VALUE

Ransomware attacks can do a great deal of damage very quickly. By giving the malware decoy targets to encrypt or corrupt, the attack is detected and immediately slowed. When the BOTsink server detects a remote host attempting to damage or encrypt a file, it sends an alert while slowing the attacking host's activity. Where it would normally take only seconds for an infected host to encrypt a target file, it now takes minutes or even hours. This capability dramatically slows the attack and interrupts its spread. The incident response team gains additional time to respond and eradicate the threat, minimizing the ransomware's spread and damage. Additionally, a sinkhole port can be opened so that communications with Command and Control can be established. This can be useful for safely gathering time triggered and polymorphic activity and aiding in the complete eradication of a threat.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in network attacks. The Attivo ThreatDefend Deception Platform offers comprehensive and accurate threat detection for user networks, data centers, clouds, and a wide variety of specialized attack surfaces. A deception fabric of network, endpoint, application, and data deceptions efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning simplifies deployment and operations for organizations of all sizes. Automated attack analysis, forensics, actionable alerts, and native integrations accelerate and streamline incident response. The company has won over 100 awards for its technology innovation and leadership.

www.attivonetworks.com