RANSOMWARE MITIGATION

Ransomware has become progressively more advanced. Criminals are moving beyond simple system exploits to using APT-like tactics and techniques to conduct reconnaissance, escalate privileges, and move laterally to find high-value targets, such as production databases, Active Directory controllers, and other critical assets. By encrypting these essential services and waiting until they have a widespread presence in the network, the threat actors can demand higher amounts, and organizations are forced in many cases to pay or suffer extensive recovery efforts and costs. Median ransomware payments have increased by around 150% at the beginning of 2020, showing no sign of slowing or stopping. Organizations must take a different approach to thwart these more aggressive and destructive attackers. The Attivo Networks Endpoint Detection Net (EDN) ransomware mitigation functions arm security teams with the defense they need to detect and derail both common and advanced ransomware attacks quickly.

RANSOMWARE ATTACKS

Typical ransomware spreads through several methods, most often through malicious emails, removable storage drives, or infected links. The ransomware infects the host and then looks for documents, spreadsheets, pictures, or other files and data to encrypt. Once it finishes encrypting the local files and folders, it will often look for network shares mapped to the endpoint and encrypt any files it can access, thus affecting a more significant number of people. It may also look for attached storage devices like USB flash drives to infect as another method of propagation. Once it completes this activity, it will flash a ransom message on the screen with contact information and the amount the attacker is demanding for the unlock code.

Organizations use Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) solutions to detect less-sophisticated ransomware variants and prevent them from infecting endpoints. These endpoint solutions use signature matching or behavioral anomaly detection, identify malicious binaries, and then block their execution to stop the infection. With known malware samples or a good baseline, these systems can effectively prevent endpoint compromise.

> Ransomware is the third most common Malware breach variety and the second most common Malware incident variety. - Verizon DBIR 2020

However, advanced, human-controlled ransomware can bypass these security controls. These threat actors often do not infect the first system they compromise. Instead, they use it as a foothold in the network to launch their attacks, conduct network discovery, probe Active Directory, move laterally to spread around to multiple systems, and identify

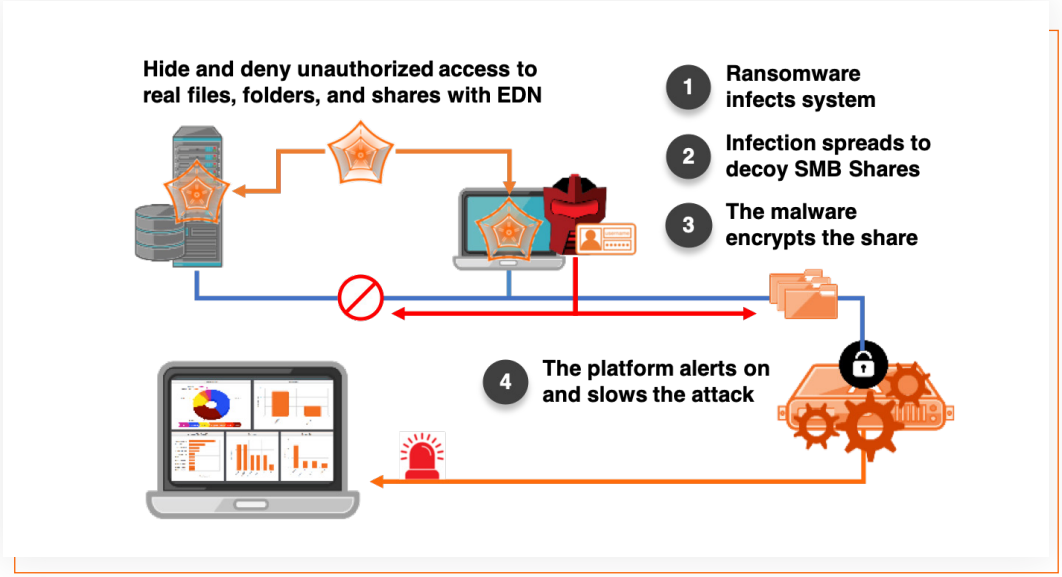
high-value assets to target. At this stage of their attack, they stay hidden from view, unlike commodity ransomware that encrypts any host it infects and then shows the ransom screen as soon as it finishes encrypting files. Only when the attackers have found all the organization's essential assets and encrypted the critical data will they send their ransom demands. They may even threaten to disclose some stolen private data to discourage non-payment. To combat these advanced attackers, organizations are turning to the Attivo Networks EDN solution.

THE EDN SOLUTION

The Attivo Networks® Endpoint Detection Net (EDN) solution, part of the ThreatDefend® platform, includes the ThreatStrike® solution for endpoint deception, the ThreatPath® solution for attack path visibility, and the ADSecure solution for Active Directory defense. Together, they augment existing endpoint defenses, like EPP and EDR, by detecting the tactics and techniques that attackers use to move deeper into the network. Moreover, the solution acts to misdirect, misinform, and deny attackers unrestricted lateral movement from the initially infected system. The EDN suite packages these solutions under one license to simplify the buying process, and is available as a standalone detection solution with the EDN Manager or as part of the ThreatDefend platform, which adds attacker engagement and network reconnaissance detection when used with the BOTsink® deception server decoys.

RANSOMWARE MITIGATION – LIMITING DAMAGE AND MOVEMENT

Included with the EDN solution is a unique technology that is designed to pre-emptively mitigate ransomware attacks. This function prevents attackers from seeing and exploiting production files, folders, and removable media on the endpoint from ransomware discovery, preventing the malware from encrypting user data and limiting its ability to spread via attached storage devices. The solution also hides the production network and cloud mapped shares on the host and only shows decoy file shares to the ransomware as it tries to move around the environment and encrypt files.



In a standalone EDN deployment, the EDN Manager generates alerts for every activity that attempts to enumerate the local files, folders, or tries to move to the shares. Alternatively, when used with the BOTsink server, these mapped file shares lead to network decoy servers populated with fake data. As the ransomware encrypts the files on the phony file shares, the decoys keep feeding the malware a never-ending stream of data to stall and occupy it, delaying the attack while alerting security teams. Additionally, both the EDN Manager and the BOTsink solution have native integrations with existing security solutions that can automatically isolate infected systems to give security teams time to remediate incidents and prevent further spread of infection.

CONCLUSION

The EDN family of products is a powerful solution for adding visibility and detection into both standard and human-controlled ransomware attacks. Whether the adversary is stealing credentials, pulling critical accounts and information from AD, moving laterally, or activating the ransomware to encrypt files, the EDN solution quickly detects and derails these activities. The flexibility of the solution gives security teams an option to deploy it either in standalone mode for detecting attacks or as part of a broader ThreatDefend platform deception fabric. The full platform adds forensic collection, attack analysis, threat intelligence development, native integrations, and the ability to feed the ransomware with unlimited data to stall the attack. By adding the EDN suite to existing EPP and EDR solutions, organizations can strengthen their endpoint ransomware defenses and deny attackers from getting both a foothold into the network and the opportunity to disrupt services.

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