PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH VIRUSTOTAL

Attivo Networks has partnered with VirusTotal to provide advanced threat intelligence sharing and analysis capabilities. With the joint solution, customers gain visibility on attack information and threat intelligence from the Attivo Networks ThreatDefend™ decoy systems, which collect suspicious files that are then fed into VirusTotal for comprehensive analysis. With this integration customers can reduce time and resources required to detect and identify threats and disseminate the information, ultimately reducing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Malware Hunting
- Expedited Incident Response

THE CHALLENGE

Cyberattackers have proven repeatedly that they can, and will, infiltrate the networks of even the most security-savvy organizations. Whether the attacker gets in using stolen credentials, a zero-day exploit, an email-based attack, or simply starts off with insider access, they will establish a foothold and move laterally through the network until they reach their intended target. Attackers have also proven that once inside they can evade the remaining security solutions and traverse the network undetected.

Quickly detecting and shutting down attackers that are already inside the network requires a new security approach that does not rely on typical measures, such as known signatures or attack pattern matching. Deception technology embodies this new approach, tricking attackers into revealing themselves, delivering high fidelity alerts to quickly and efficiently disrupt the attack. It can also capture valuable attack forensics and threat intelligence that organizations can use to bolster their defenses and make future attacks more difficult.

THE ATTIVO THREATDEFEND PLATFORM AND VIRUSTOTAL JOINT SOLUTION

Basic integration between the Attivo ThreatDefend Deception Platform and VirusTotal leverages the VirusTotal public access repository of malware sample hashes. Full integration is easy to set up for organizations that want to leverage VirusTotal's advanced analysis features. In minutes, organizations can have an integrated adaptive security platform that provides effective, real-time detection of cyberattackers with automated threat intelligence sharing and analysis. With native support for file submission and lookups, the integrated solution provides a real-time, non-disruptive way of detecting and blocking threats inside the network. This substantially curtails an attacker's ability to leverage malware, known or unknown, to damage or exfiltrate valuable company assets and information.

ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the Attivo Networks solution provides network, endpoint, and data deception across an organization. The system has proven highly effective in detecting threats from all vectors, including reconnaissance, stolen credentials, Man-in-the-Middle attacks, Active Directory compromise, ransomware, and insider threats.

The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink engagement servers delivering decoys, lures, and breadcrumbs to an attacker, ThreatDirect™ to extend deception into remote locations, the ThreatStrike® endpoint deception suite, ThreatPath® for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM) to coordinate the entire deception suite. Together, these components create a comprehensive early detection and active defense platform against advanced cyber threats.

SUMMARY

The Attivo ThreatDefend Platform plays a critical role in enabling an active defense with in-network threat detection and integrations to dramatically accelerate incident response.

A strategy that depends upon manual intervention may work for low-severity alerts, but high-severity attacks may not give security teams sufficient time to react. Automating malware hunting and file reputation lookups shifts the advantage back to the security team, giving them more lead time to contain an attack, preventing mass damage and data exfiltration. The Attivo Networks ThreatDefend Platform can send malicious file hashes and samples directly to VirusTotal for rapid lookup and analysis. The time saved by automating malware hunting on the network is critical to interrupting malware-based lateral movement and data exfiltration.

The need for this integration is urgent. In a single year, over one billion sensitive records have been stolen with detrimental impact to individuals and enterprises. The resulting damage to the companies' reputations and balance sheets has reached into the billions of dollars. By implementing solutions that detect in-network threats early and having the ability to automatically hunt for additional malware infections, organizations can mitigate the risk of large-scale breaches.

ABOUT ATTIVO NETWORKS

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, ICS-SCADA, POS, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

ABOUT VIRUSTOTAL

VirusTotal was founded in 2004 as a free service that analyzes files and URLs for viruses, worms, trojans and other kinds of malicious content. VirusTotal's goal is to make the internet a safer place through collaboration between members of the antivirus industry, researchers and end users of all kinds. Fortune 500 companies, governments and leading security companies are all part of the VirusTotal community, which has grown to over 500,000 registered users.

www.virustotal.com