Attivo NETWORKS®

Detect Infected Machines and Stop Data Exfiltration with Attivo Dynamic Deception and Juniper SRX Firewalls

Highlights

- Real-time Threat Detection
- Attack TTP Analysis and Forensics
- Automated Quarantine and Blocking
- Expedited Incident Response
- Centralized Threat Intelligence

Attivo NETWORKS®

JUNIPer NETWORKS

Joint Solution Brief

Attivo ThreatDefend® Deception Platform and Juniper SRX® Integration

Through a multitude of cyber attack vectors (stolen credentials, phishing, BYOD, etc.) BOTs and APTs are finding their way onto the corporate networks and datacenters. Once inside the network, the attacker will mount an attack with the goal of stealing valuable company information. In 2014 alone, over one billion records were stolen with personal impact to individuals and in many cases damage to the company's reputation and balance sheet. It is now commonly accepted that a prevention only security strategy is insufficient to defend against cyber attacks. Organizations are now moving to a modernized security strategy that assumes that intrusions will occur and includes systems to detect BOTs and APTs that are inside the network.

Challenge

Most perimeter and end-point security solutions cannot reliably detect the following methods of attacks:

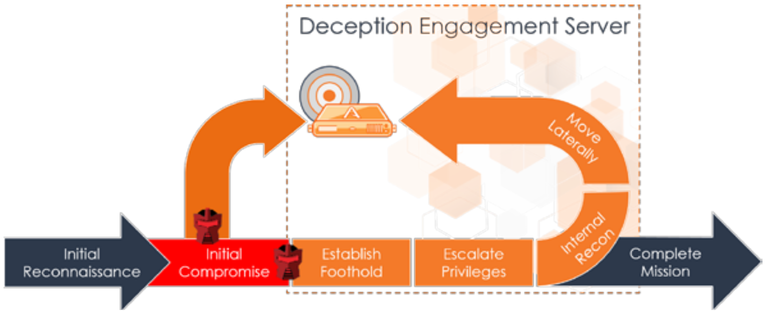
- HTTPS: that bypasses all network security
- Zero-day exploitation
- Stolen employee credentials
- Endpoint/BYOD zero-day infections
- Spear phishing

Solution

Attivo Networks and Juniper have developed an ideal solution that allows customers to quickly discover and dynamically block any infected node on the network, minimizing the risk of a data breach.

Comprehensive Security

A comprehensive security posture needs to include inside the network threat detection as a next layer of defense in today's security infrastructure. The ThreatDefend platform brings a new complementary layer of security by accelerating breach discovery and providing an additional line of defense designed to make it difficult for attackers to reach or compromise valuable assets. The Attivo dynamic deception ThreatDefend Platform is an elegant way to trap the BOTs and APTs that bypass perimeter and endpoint security. Additionally, the platform provides the full Techniques Tactics and Procedures (TTP) with associated forensics (IOC, STIX, CSV & PCAPs) for fast remediation. API access to this data enables it to publish to existing



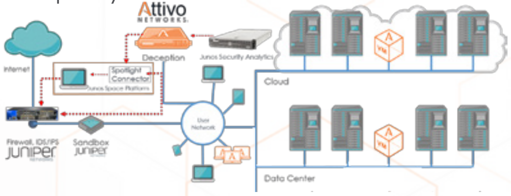
network security infrastructure.

Juniper Networks and Attivo Stop the Attacker

The Attivo BOTsink solution seamlessly integrates with the Juniper Spotlight Connector to provide the SRX Firewall the needed intelligence to block the infected nodes from gaining Internet access and exfiltrating valuable company data. Once the BOTsink platform identifies an infected node, its IP address is sent to the Spotlight Connector through its API for SRX enforcement; quarantining the device, stopping any communication with the Command and Control (CNC) and preventing any data exfiltration.

The BOTsink solution will provide a full coverage attack surface to engage the attack during its discovery and lateral infection phase (as the BOT/APT probes and scans the network looking for high-value targets) or during a targeted attack. The BOTsink decoys are real operating systems based on Windows XP, 7, 2008 Servers, CentOS, and Ubuntu. In addition, the BOTsink decoys host various applications and protocols including Apache, SNMP, SMTP, File Shares, MySQL, etc. The BOTsink solution supports "golden image" customization to match an organization's network or datacenter environment and allow customers to import their virtual machines to deploy as a decoy.
The BOTsink solution will in real-time identify the source of a breach, generate attack intelligence and alerts, and send them to the Juniper Security Analytics system (JSA) to enhance the visibility around the attack and to shorten remediation time.

The integrated solution provides a real-time, non-disruptive way of detecting and blocking BOTs and APTs inside the network, eliminating the opportunity for an attacker to exfiltrate valuable company assets and information.



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, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com

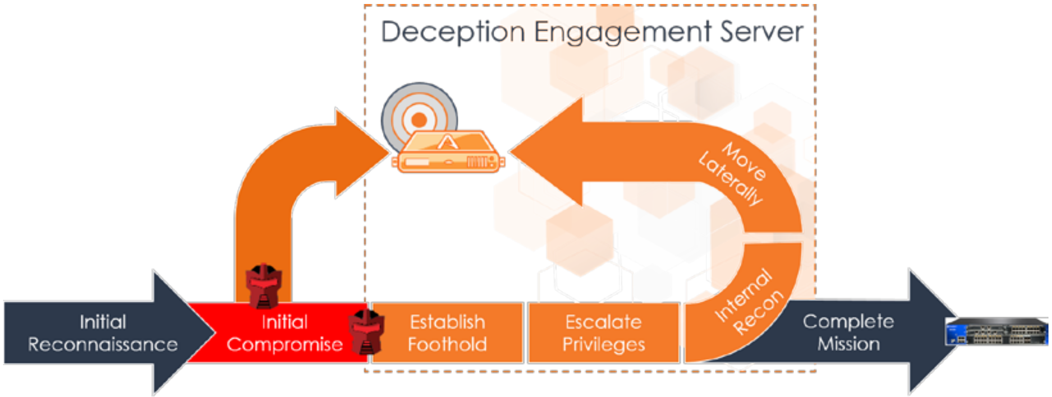
About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Attivo NETWORKS

JUNIPER NETWORKS

Joint Solution Brief



Deception Engagement Server
Initial Reconnaissance
Initial Compromise
Establish Foothold
Escalate Privileges
Internal Recon
Move Laterally
Complete Mission