The Attivo BOTsink Platform Integrates with the Blue Coat ProxySG

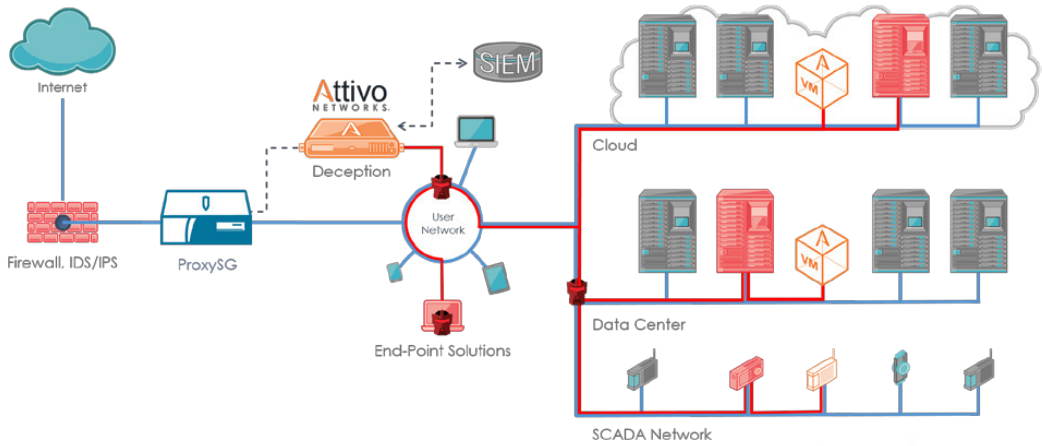
Highlights

- Automatic blocking of attack IP address
- Automatic incident response to stop data exfiltration
- Cross-platform information sharing

Through a multitude of cyber attack vectors (zero-day, unpatched systems, stolen credentials, phishing, BYOD, etc.) BOTs and APTs are by passing prevention systems and are finding ways to get inside corporate networks and datacenters. Once inside-the-network, the attacker will mount an attack with the goal of stealing valuable company information or causing other harm. In 2015 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 has become hard to dispute that a prevention only security strategy is sufficient to defend against cyber attacks. A modern security strategy assumes that intrusions will occur and includes detection systems that quickly reveal BOTs and APTs that are inside the network.

Integrated Solutions

A modern security posture includes prevention and inside-the-network threat detection for a comprehensive defense of one's organization. The Attivo Networks® Deception Platform brings an efficient new approach to accelerating breach discovery in the network, data center and cloud by using deception to make it difficult for attackers to reach or compromise valuable assets. The Attivo BOTsink® solution is based on deception engagement servers, which provide an efficient way to detect and trap attackers 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, significantly improving incident response time. The Attivo BOTsink platform integrates with the Blue Coat ProxySG , which can then promptly block internal end-points from accessing resources outside the corporate environment and the ex-filtration of corporate data.



Joint Solution Brief

About Attivo Networks

Attivo Networks® provides 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, IoT, and POS environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

About Blue Coat

Blue Coat is a leader in advanced enterprise security, protecting 15,000 organizations every day. Through the Blue Coat Security Platform, Blue Coat unites network, security and cloud, providing customers with maximum protection against advanced threats, while minimizing impact on network performance and enabling cloud applications and services. Blue Coat was acquired by Bain Capital in March 2015.

www.bluecoat.com

Attivo NETWORKS

BLUE COAT

Joint Solution Brief

How it Works

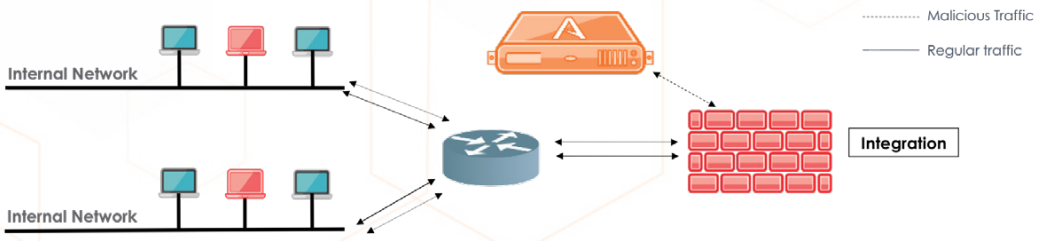
The BOTsink seamlessly integrates with the Blue Coat ProxySG to deliver the addresses of the internal compromised endpoints that need to be blocked from communicating with the command and control (C&C) or any other external communication.

The BOTsink is able to compile the needed information and make it available to the ProxySG through its dedicated connector. As such the Attivo BOTsink is complementing and feeding the ProxySG database so that it can block the compromised endpoints from opening backdoors with the C&C or from ex-filtrating any data.

The BOTsink deception 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 based on real operating systems such as Windows XP, 7, 8, 10, 2008 & 2012 Servers, CentOS, and Ubuntu. In addition, the BOTsink decoys host a wide variety of applications and protocols including but not limited to, Apache, SNMP, SMTP, File Shares, and MySQL. The BOTsink solution will also support the loading of a "golden image"and application customization to use as a decoy and for the highest levels of authenticity to match an organization's network, datacenter or cloud environment.

Key Features and Benefits

Attivo BOTsink integration with Blue Coat ProxySG helps customers to block the infected machine and prevent exfiltration of data or contacting the C&C server thus minimizing the impact of the breach.



Lifecycle of attack detection to blocking

- BOTsink detects attack and raises an alert for a particular attacker IP
- The info about the attacker IP to be blocked is automatically pulled by the SG periodically from the Attivo Appliance in realtime
- SG Proxy blocks all traffic originating from this attacker IP on the perimeter for a time value as configured by TTL seconds.