Solution Brief

Symantec Technology Integration Partner: Attivo

Business Challenge

Through a multitude of cyber attack vectors (zero-day, unpatched systems, stolen credentials, phishing, BYOD, etc.), BOTs and APTs are bypassing prevention systems and finding ways to get inside corporate networks and datacenters. Once inside the network, the intruder 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 not 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 inside the network.

Solution: Symantec and Attivo

A modern security posture includes prevention and inside-the-network threat detection for a comprehensive defense of your 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 Symantec Blue Coat ProxySG, which can then promptly block internal endpoints from accessing resources outside the corporate environment and the ex-filtration of corporate data.

Attivo NETWORKS

Partner: Attivo

Partner Product: BOTsink®

Symantec Product: Blue Coat ProxySG

How it Works

The BOTsink seamlessly integrates with the 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. In this way the Attivo BOTsink is complementing and feeding the ProxySG database to enable it to 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 engagement VM's are based on real operating systems such as Windows XP, 7, 8, 10, 2008 & 2012 Servers, CentOS, and Ubuntu. In addition, the BOTsink engagement VMs 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

Symantec.

application customization to use as an engagement VM and for the highest levels of authenticity to match an organization's network, datacenter or cloud environment.

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, minimizing the impact of the breach.

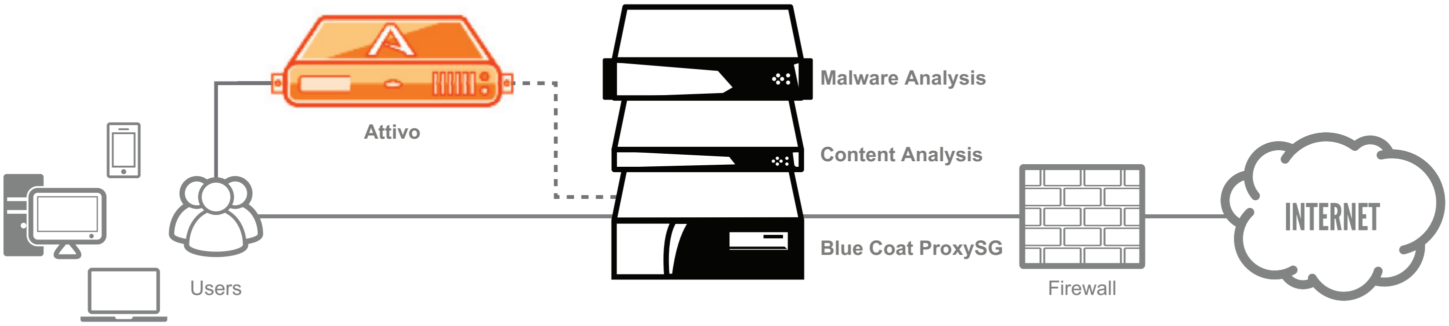
Lifecycle of attack detection to blocking

- 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 real time.
- ProxySG blocks all traffic originating from this attacker IP on the perimeter for a time value as configured by TTL seconds.

About Attivo

Attivo Networks is the leader in dynamic deception technology, which in real-time detects intrusions inside the network, data center, and cloud before the data is breached. Leveraging high-interaction deception techniques, the Attivo BOTsink Solution lures BOTs and APTs to reveal themselves, without generating false positives. Designed for efficiency, there are no dependencies on signatures, database look up or heavy computation to detect and defend against cyber threats. Attivo solutions capture full forensics and provide the threat intelligence to shut down current and protect against future attacks.

For more information visit www.attivonetworks.com.



About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.