Using Inside-the-Network Threat Detection to Stop the Ever Increasing Threat of Advanced Malware Attacks

Today’s corporations are facing an onslaught of cyberattacks. Botnets (BOTs) and advanced persistent threats (APTs) are growing in number and sophistication. Check Point’s Annual Security Report for 2014 noted that over 73% of organizations had at least one bot detected, up 10 points compared to a year ago. In addition, 49% of organizations had 7 or more bot-infected hosts. One of the most alarming discoveries of the report is that 77% of the bots were found to be active for more than 4 weeks AND that the bot attempts to communicate with their Command and Control (C&C) server every 3 minutes!

Active Deception for Threat Detection Solutions

Attivo Networks™ active threat detection solutions detect BOTs and APTs as they move laterally inside an organization’s network and data center.

Deception and Decoy

Designed to augment existing security systems and detect inside the network threats, the Attivo BOTsink family of threat-detection systems uses deception techniques to deceive, detect, and defend against BOTs and APTs as they begin scanning, targeting and probing network clients, servers and services for targets.

Unparalleled Visibility into the Anatomy of Inside-the-Network Attacks

The Attivo BOTsink® Solution uses its patented Multi-Dimensional Correlation Engine (MDCE) to capture and analyze BOT and APT activities to ensure you have the actionable intelligence you need to quickly and effectively shut down inside-the-network threats. The solution will detect and capture actionable information to support remediation and forensics, such as:

- Addresses of infected machines
- Username and password combinations
- Any dropped payloads including location and type of attacks
- Attack activity, including any data it’s trying to download or export data
- Any system/kernel changes, process creation, process injection, registry and network activity Our “smart” solution learns from every engagement to accelerate identification and forensic analysis. The Attivo BOTsink Solution integrates with Log Forwarders and security incident and event management (SIEM) systems seamlessly and can deliver reporting in IOC, UI, Syslog or PCAP files formats
100% Actionable Alerts

The Attivo BOTsink solution provides accurate, actionable alerts, with the intelligence you need to take immediate action to stop BOTs and APTs that have bypassed perimeter security and are propagating inside your network. There are NO legitimate reasons for a user to communicate with the Attivo BOTsink solution, so any scans or attempts to engage it represent an attacker trying to find and target high value network assets.

Attivo Threat Detection Advantages

Attivo delivers a broad set of unique capabilities to its users:

Deception Authenticity
• BOTsink runs real operating systems, services, and applications along with the ability for complete customization, including the ability to import a company’s golden images and applications into its network.

No False Positives
• With a high-efficiency design, Attivo does not send false positives, reducing alert noise and the amount of time and energy required for management.

Scalability
• Attivo solutions are not inline enabling the support of network, data center, and cloud environments including breach detection for east-west data center traffic. Deployment models are VM- or appliance-based and provide global management capability.

Efficient and easy to manage
• Attivo solutions are not reliant on signatures and do not need to maintain a command-and-control database. They integrate seamlessly into existing security environments and can provide threat signatures to other security infrastructure such as firewalls and SIEM devices.
• Deployment options include appliance and VM versions that insert non-disruptively into the network. A typical BOTsink solution can be installed and operational in less than an hour.

Secure
• No data or information ever leaves the user organization’s premises for external (cloud) computation.
• Attivo solutions are highly efficient and scalable since they are not inline and do not need redirection of traffic.

For more information or to schedule a demonstration, contact sales@attivonetworks.com