Attivo Networks and Carbon Black Security Platform Integration

Highlights

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Improved Incident Response
- Infected End-point Detection

Integration between detection and prevention solutions provide the critical infrastructure required for continuous response and protection against cyber attackers. This paper will detail the integration plans between the Attivo Networks BOTsink Deception and Carbon Black Security Platforms and includes the next steps in how Attivo will detect other infected systems based on malware signatures derived from BOTsink attack analysis.

The Challenge

The average dwell time of an attacker currently stands at 201 days, which is then compounded by another 70 days to contain the breach, once it has been identified. Integrating these solutions empowers organizations to reduce time-to-detection and the time required to respond to incidents, ultimately reducing the attacker's ability to complete their ultimate mission.

The Joint Solution

The Attivo BOTsink Deception Platform integrates with Carbon Black Platform solution automating the blocking and quarantine of infected systems in order to curtail any lateral movement and exfiltration attempts.

Quarantining of infected systems.

As the BOTsink solution detects the infected systems, it can be configured to automatically push the infected IP addresses to the Carbon Black server for quarantine. Alternatively, the quarantining action can be initiated manually.

To enable this functionality, the following information needs to be configured in the BOTsink Carbon Black connector:

1. The IP address of the Carbon Black server
2. The authentication Key of the Carbon Black Server (obtained from the carbon black server to authenticate the BOTsink and accept its data)
3. Configuration of the time period the infected systems will be quarantined
4. Select if the system sends the IP addresses automatically as it detects them (auto-quarantine) or not
5. If auto quarantining is selected, then select the severity that will trigger that event

Carbon Black.

Joint Solution Brief

About Carbon Black

Cb Response is the most precise IR and threat hunting solution, allowing you to get the answers you need faster than any other tool. Only Cb Response continuously records and captures all threat activity so you can hunt threats in real time, visualize the complete attack kill chain, and then respond and remediate attacks, quickly.

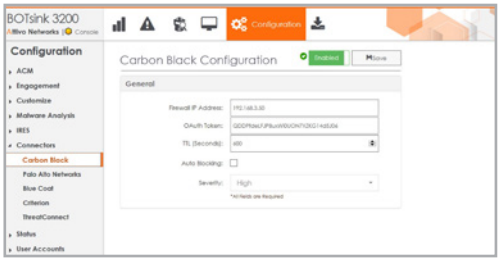
About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo Deception 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

Attivo NETWORKS

Carbon Black.

Joint Solution Brief



To configure the Carbon Black connector you start by enabling it.

- Once the connector is enabled and configured, the user will save the input which will authenticate the BOTsink solution with the Carbon Black server.
- When auto-blocking is selected, the BOTsink solution will send the Carbon Black server the IP addresses of the infected systems to quarantine, the time to quarantine, and the severity of the alert that triggered that event.

If auto-quarantining is not selected, the user can quarantine the infected system by following these steps:

- Go to the event page on the BOTsink
- Select the IP address to quarantine
- Select the quarantine method, in this case Carbon Black
- The same information will be sent to the Carbon Black Server to quarantine the selected system.

The integration and exchange of information are sent using the Carbon Black Server REST API interface.

Summary

The integration between the Attivo Networks BOTsink Deception and Carbon Black Security Platforms will provide joint customers significant improvement in continuous response. By automating the quarantine and blocking of attackers, and automated analysis of suspicious files, organizations will benefit from time and efficiency savings, and improved protection against cyber attackers.