SOLUTION BRIEF

Attivo Networks BOTsink and McAfee Network Security Platform Integration Analyzes Targeted Attacks

Protect networks and data centers against sophisticated threats

The integration of McAfee® Network Security Platform with Attivo BOTsink deception servers empowers organizations with the additional knowledge required to quickly identify and remediate infected devices and prevent cyberattacks. This joint solution:

- Empowers blocking the command and control (C&C) communication from production networks
- Engages the attacker's C&C to gather critical information to remediate the attack
- Provides better insights about the blacklisted domain, as well as the behavior, tactics, and techniques used by the botnet
- Offers BOTsink forensics and alerts that provide full-packet capture of the communication between the engagement virtual machine and the C&C
- Sends substantiated, actionable alerts in Structured Threat Information eXpression (STIX) and OpenIOC formats

McAfee Compatible Solution

- The Attivo BotSink Deception platform 3.3 or higher and McAfee Network Security Platform 8.2
- Attivo Networks BOTsink Deception Platform

The Business Problem

Bots and advanced persistent threats (APTs) are getting more sophisticated and malicious. It is critical to not only detect them, but also to prevent them from attacking again. To accomplish this, organizations need:

- More information on attacker identification and detection of multistage exploit kits
- The ability to identify instructions sent from the C&C server as part of the initial callback mechanism to understand their tools and methods
- The ability to generate Snort signatures, which can be imported into McAfee Network Security Platform and can be used to block attackers based on connection attempts as opposed to signatures

McAfee and Attivo Networks Joint Solution

The Attivo BOTsink solution is based on deception engagement servers that lure attackers to engaging before they can find company production servers through the use of a host of standard and custom applications, endpoint, and server-level deception techniques. The BOTsink solution lures and engages attackers so that forensic information can be gathered to take corrective actions. BOTsink identifies the attacker IP address, understands the effects of the attack on the infected endpoint, and provides full forensics for remediation.

With this integration, users can configure the BOTsink engagement servers as sinkhole addresses in McAfee Network Security Platform. Subsequent traffic from an infected endpoint is then sent to the BOTsink engagement server for attack analysis.

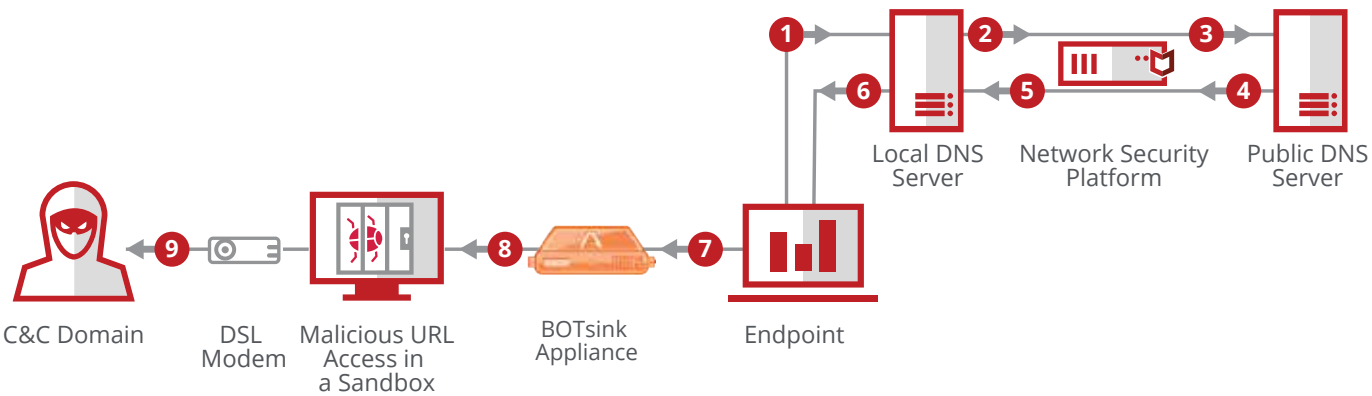

Figure 1. BOTsink Engagement Server and McAfee Network Security Platform Integration

Here's how it works:

1. The user clicks on a malicious link in a spear-phishing email. The endpoint then attempts to connect to the C&C to download a file to exploit a vulnerability and compromise the endpoint.
2. The endpoint sends a DNS query to your enterprise DNS server to resolve the blacklisted C&C. When the enterprise DNS server cannot resolve the blacklisted C&C, it sends the DNS query to a root name server on the internet.
3. The DNS query about the malicious domain goes through McAfee Network Security Platform.
4. The pubic DNS server sends the corresponding DNS response for the request.
5. McAfee Network Security Platform modifies the DNS response so that the resolved IP address is that of an engagement virtual machine.
6. The endpoint connects to the engagement virtual machine and sends the communication, which was actually meant for the C&C server.
7. . The engagement virtual machine launches the URL in a configured browser within the BOTsink sandbox and connects to the C&C. BOTsink will behave as the infected machine and connect to the malicious domain on behalf of the endpoint.
8. If the URL is malicious, the engagement virtual machine gets infected and is allowed to behave like a bot in the sandbox environment. Contained in the sandbox, the BOTsink engages the attacker and extracts the URL and C&C hostname. The BOTsink advanced analytical engine analyzes the botnet traffic and send alerts with the information about the botnet behavior. This allows organizations to understand the intent of the attacker and better defend their networks and data centers against targeted attacks.
9. If an infected file is downloaded, the attack information can be reported to endpoint security applications so they can then be used to check for the presence of the infected file. Similarly, network security applications can see if there have been any other communications with malicious domains that have been detected.

About Attivo Networks

Attivo Networks is an innovator in cybersecurity defense. As the leader in deception-based threat detection technology, Attivo provides dynamic deceptions for the real-time detection of intrusions that have bypassed all other prevention solutions. A modern day defense-in-depth security approach assumes that the organization has been breached and has added inside-the-network detection to its security infrastructure. Attivo uses

high-interaction deception techniques to engage bots and APTs that are inside the network, data center, and cloud. Not dependent on known signatures or attack patterns, the Attivo dynamic deception platform provides the visibility and real-time detection of insider and external threats as the attacker scans or attempts to move laterally in the progression of their attack. Attivo alerts are actionable and are substantiated with detailed attack forensics, which can automatically feed into security information and event management (SIEM) and prevention systems for the prompt blocking, quarantining, and remediation of infected devices—and for the prevention of future cyber attacks. For more information visit **www.attivonetworks.com**.

About McAfee Network Security Platform

The McAfee Network Security Platform is a next-generation intrusion prevention system (IPS) that is built for the accurate detection and prevention of intrusions, denial-of-service (DoS) attacks, distributed denial-of-service (DDoS), malware downloads, and network misuse. McAfee Network Security Platform uses multiple mechanisms to detect advanced botnets. One of the mechanisms inspects DNS traffic to blacklisted domains. When McAfee Network Security Platform detects a blacklisted domain in the DNS traffic, it modifies the DNS packets so that the C&C traffic is sinkholed to a different server of your choice.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com