ATTIVO NETWORKS THREATDEFEND® AND MCAFEE®
NSP INTEGRATION DNS SINKHOLE WITH URL SANDBOXING

Botnets are a complex and pervasive form of cyber attack that has been used by attackers, for over a decade, to compromise millions of endpoints to carry out cyber attacks. Botnets have been the weapon-of-choice for almost all the major finance-related cyber attacks in recent years, and their evolution in terms of strategy, packaging, delivery and distribution continually creates challenges for security administrators worldwide.

The Attivo ThreatDefend Detection and Response Platform improves security in enterprise networks as well as private and public data centers by identifying inside-the-network threats and infected devices in real-time. The Attivo BOTsink® deception server integrates with the McAfee NSP 8.2, taking the DNS sinkhole concept to the next level, by capturing the full intent of the attack, and by providing the forensics required to remediate infected devices.

Together, the McAfee Network Security Platform and Attivo ThreatDefend platform offer a unique method to analyze the tactics, techniques, and procedures of a targeted attack. This knowledge empowers organizations to quickly identify and remediate infected devices and prevent against future cyber attacks.

INTEGRATED PRODUCTS

THREATDEFEND DECEPTION AND RESPONSE PLATFORM

The Attivo ThreatDefend solution uses deception engagement servers that lure attackers to engage before they can find company production servers. The ThreatDefend solution uses a host of standard and custom applications, endpoints, server-level deception techniques, and lures. It engages attackers so that it can gather forensic information to take corrective actions. The ThreatDefend solution identifies the attacker’s IP address, understands the effects of the attack on the infected endpoint, and provides full forensics for remediation. Friction-less in its deployment and highly scalable, the ThreatDefend platform easily detects threats in the enterprise network and within private and public cloud environments. The ThreatDefend deception platform also detects both reconnaissance and targeted attacks.

THE MCAFEE NETWORK SECURITY PLATFORM

The McAfee Network Security Platform is a next-generation IPS, which accurately detects and prevents intrusions, DoS, DDoS, malware download, and network misuse. The Network Security Platform employs multiple mechanisms to detect advanced botnets, one of which is to inspect DNS traffic to blacklisted domains. When the Network Security Platform detects a blacklisted domain in the DNS traffic, it modifies the DNS packets to sinkhole the Command and Control (C2) traffic to a different location of choice.
ATTIVO THREATDEFEND INTEGRATION WITH MCAFEE NETWORK SECURITY PLATFORM (NSP)

For any targeted attack, the first step is to establish a footprint on the network. Attackers employ different methods to develop this footprint. A typical mechanism among attackers is to use phishing emails.

After a user clicks on a URL or opens the payload in the phishing email, malware infects the endpoint and attempts to communicate with Command and Control (C2). This command traffic is vital for the malware to progress through the different stages of the attack until it achieves its goal.

The integration between the Network Security Platform and ThreatDefend detects and blocks the communication between an infected endpoint and a blacklisted C2 by sending the connections to a decoy server that acts as a sandbox environment, to monitor and analyze the characteristics and behavior of the malware and C2.

The McAfee NSP 8.2 analyzes DNS traffic to detect botnets using methods such as DGA (Domain Generation Algorithm), Fast Flex Service Networks (FFSN), and URL/IP blacklist domain database.

The ThreatDefend platform’s BOTsink deception server hosts multiple operating systems and uses dynamic endpoint, server, and application lures to engage attackers. With this integration, users can configure the BOTsink decoys as sinkhole addresses in the NSP. Subsequent traffic from an infected endpoint then goes to the decoys for attack analysis. The ThreatDefend platform deception platforms also save time and energy by providing automated analysis of each attack. It also captures the attacker’s valuable Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOCs), and provides actionable intelligence of the attack for improved incident response and to better fortify the network.

- A BOTsink deception server has many virtual machines that act as decoys, which it uses to engage compromised endpoints. The decoys run on various flavors of Linux and Windows operating systems. These decoys also run multiple services to lure in-network attackers as they attempt to move laterally through the network. ThreatDefend uses its proprietary Analyze, Monitor, and Record (AMR) Engine to provide forensics when it engages with an infected endpoint.

- Instead of sinkholing the C2 traffic to a loopback IP address, the integration redirects the C2 traffic to a decoy, which engages the endpoint and records all the details of the communications. Security personnel can then take the information and network traffic packet captures to extract valuable intelligence for analysis, such as the C2 server IP address, a recording of any commands it sent to C2, and any payloads it requested. The security team can then download the payload to a decoy or any other sandbox technology for analysis.

- The ThreatDefend platform is a secure environment that isolates all attack traffic from the production network, providing a safe environment to defuse and observe the payload activities.
1. The end-user clicks on a link in a malicious email. The endpoint attempts to connect to the C2 to download a file to exploit a vulnerability and compromise the endpoint.

2. The endpoint sends a DNS query to the enterprise DNS server to resolve the blacklisted C2. When the enterprise DNS server cannot resolve the blacklisted C2, it sends the DNS query to a root name server on the Internet.

3. The DNS query about the malicious domain goes through the Network Security Platform.

4. Public DNS Server sends corresponding DNS response for the request.

5. The Network Security Platform modifies the DNS response such that the resolved IP address is that of a decoy.

6. The endpoint connects to the decoy and sends the communication, which it meant to submit to the C2 server.

7. The decoy records all the details of the attack and captures network traffic. The analyst can use the information to investigate the incident, such as extracting the URL, exporting packet captures of the network traffic, recording any encoded commands, or downloading and executing any dropped payloads (in a decoy or sandbox such as McAfee ATD).

---

**USE CASE EXAMPLE DEMONSTRATING VALUE FROM ADDITIONAL FORENSICS**

Malicious email is a popular method used for infecting an endpoint. This type of attack occurs when attackers send malicious domain links in emails, which direct users to malicious sites.

NSP can block access attempts to malicious blacklisted domains; where it drops the packet and crafts a DNS response, which carries Sinkhole address. Since it is not possible to identify every possible malicious domain, attackers can find ways to bypass the NSP block by sending different domain names.
Attackers use tools like Fast-flux and DGA to communicate with the C2 server. NSP detects malicious domains using FFSN and DGA and can send a DNS response pointing to the sinkhole address. Malware from infected systems can generate large numbers of domain requests making it challenging to detect and block every malicious domain request.

Deploying the Attivo ThreatDefend platform integrated with the McAfee NSP will dramatically improve the detection and prevention of an attacker’s ability to complete its mission. The Attivo ThreatDefend platform provides a controlled environment that can sinkhole the C2 traffic and captures all communications from the infected system. Additionally, the ThreatDefend Deception Platform can provide detailed forensics and generate Snort signatures, IOC, PCAP, and STIX reports which users can use to detect additional infected systems in their network.

Essential forensics provided by the ThreatDefend Platform

- Identification and detection of multi-stage exploit kits
- Identification of instructions sent to the C2 server as part of the initial callback mechanism (the ThreatDefend platform captures all network traffic as packet captures to provide forensics)
- Generate Snort signatures which can be imported into NSP and block connection attempts on intent rather than a signature

SOLUTION BENEFIT SUMMARY

Together, the McAfee Network Security Platform and Attivo ThreatDefend deception servers offer a unique method to analyze the tactics, techniques, and procedures of a targeted attack. This knowledge empowers organizations to quickly identify and remediate infected devices and prevent against future cyber attacks.

- Empowers organizations to block the C2 communication from production networks and gathers critical information to remediate the current attack, and prevent against future attacks
- Provides better insight about the blacklisted domain as well as the behavior, tactics, and techniques used by the attacker
- Customized decoys deploy from the ThreatDefend Platform’s BOTsink deception server
- The ThreatDefend platform’s forensics and alerts provide the full packet capture of the communication between the decoy and the C2
- The platform offers substantiated, actionable alerts and can export collected information in STIX and IOC formats or transmit them via Syslog to share the threat information with other security vendors and applications

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in deception technology, provides organizations of all sizes with an active defense for early and accurate threat detection. The Attivo ThreatDefend® Platform delivers comprehensive detection for on-premises, cloud, and specialized attack surfaces with a deception fabric designed to efficiently misdirect and reveal attacks from all threat vectors. High-fidelity alerts are backed with company-centric threat intelligence and automated attack analysis, forensics, native integrations streamline incident response. The company has won over 125+ awards for its technology innovation and leadership. Learn more: www.attivonetworks.com