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 in order 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 packaging, delivery, strategy, and distribution continually creates challenges for security administrators worldwide.

The Attivo ThreatDefend deception 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 ThreatDefend 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 Intel 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.

Integrated Products

ThreatDefend Deception and Response Platform

The Attivo ThreatDefend solution is based on deception engagement servers that lure attackers to engaging before they can find company production servers. Using a host of standard and custom applications, end-point, and server level deception techniques, the ThreatDefend solution will lure and engage attackers so that forensic information can be gathered to take corrective actions. The ThreatDefend solution will identify the attacker IP address, understand the effects of the attack on the infected endpoint, and provide full forensics for remediation. Friction-less in its deployment and highly scalable, the ThreatDefend platform easily detects threats in the enterprise network and in private and public cloud environments. The ThreatDefend deception platform is also designed to detect both reconnaissance and targeted attacks.

The Intel Network Security Platform

The Intel Network Security Platform is a next-generation IPS, which is built for the accurate detection and prevention of intrusions, DoS, DDoS, malware download, and network misuse. The Network Security Platform employs multiple mechanisms to detect advanced botnets. One of the mechanisms 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 such that the C&C traffic is sinkholed to a different server of your choice.

Attivo ThreatDefend Integration with Intel Security 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 establish this footprint. A popular mechanism among attackers is to use phishing emails.

After a user clicks on a URL or opens the payload in the phishing email, the endpoint becomes infected with a bot, which attempts to communicate with the C&C. The C&C communication is key for a bot to progress through the different stages of the attack, until the end goal is achieved.

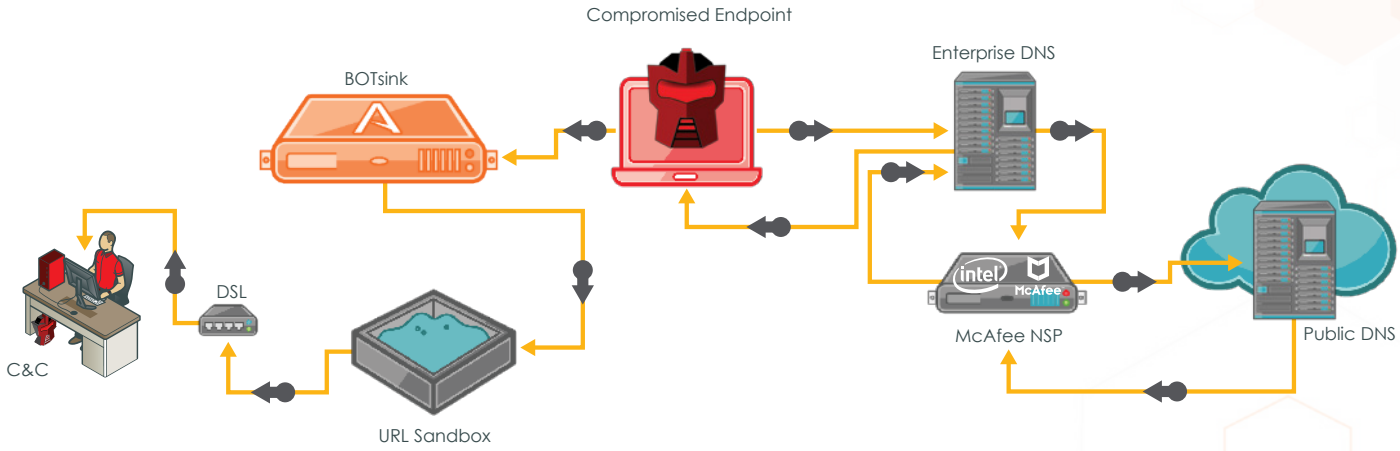
The integration between the Network Security Platform and ThreatDefend detects and blocks the communication between an infected endpoint and a blacklisted C&C by engaging the bot in a simulated C&C, in a sandbox environment, to monitor and analyze the characteristics and behavior of the bot and C&C.

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 Attivo deception platform is designed to host multiple operating systems and use dynamic end-point, server, and application lures to engage attackers. With this integration, users can configure the ThreatDefend engagement servers as sinkhole addresses in the NSP. Subsequent traffic from an infected end-point is then sent to the ThreatDefend engagement server for attack analysis.

- A ThreatDefend appliance has many virtual machines, which are used to engage compromised endpoints. These virtual machines are called decoys. The decoys run on various flavors of Linux and Windows operating systems. These decoys also run multiple services to lure APTs as they attempt to move laterally through the network. ThreatDefend is equipped with its proprietary Analyze, Monitor, and Record (AMR) Engine to provide you the forensics when an infected endpoint is engaged.
- Instead of sinkholing the C&C traffic to a lookback IP address, this integration will redirect the C&C traffic to a decoy which engages the endpoint. From the information collected through this engagement, the decoy communicates with the actual C&C domain masquerading as the infected endpoint. This enables the BOTsink deception server to interact with the C&C and understand the attacker's methodologies and intent.
- The ThreatDefend platform is a secure environment that isolates all attack traffic from the production network, providing a safe environment to defuse and observe APT-related activities.

Diagram: ThreatDefend Engagement Server and Network Security Platform (NSP) Integration Typical Attack Sequence



1. The end user clicks on a malicious link in a spear-phishing email. The endpoint 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 Network Security Platform
4. Pubic DNS Server sends corresponding DNS response for the request
5. 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 was actually meant for the C&C server.
7. The decoy launches the URL in a configured browser within the ThreatDefend sandbox and connects to the C&C. The ThreatDefend will behave as the infected machine and connect to the malicious domain on behalf of the end-point.
8. If the URL is malicious, the decoy gets infected and is allowed to behave like a bot in the sandbox environment. Contained in the sandbox, the ThreatDefend engages the attacker and extracts URL, C&C hostname.
9. The ThreatDefend advanced analytical engine analyses the botnet traffic and raises alerts with the information about the botnet behavior. This allows organizations to understand the intent of the attacker and better defend their network and data center against the targeted attack.
10. If an infected file has been 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.

Use Case Example Demonstrating Value from Additional Forensics

Phishing mail is a popular method used for infecting an endpoint. This 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 C&C server. NSP detects malicious domains using FFSN and DGA and can be configured to send a DNS response pointing to the Sinkhole address. Bots from infected machines can generate large numbers of domain requests making it difficult to detect and block every malicious domain request.

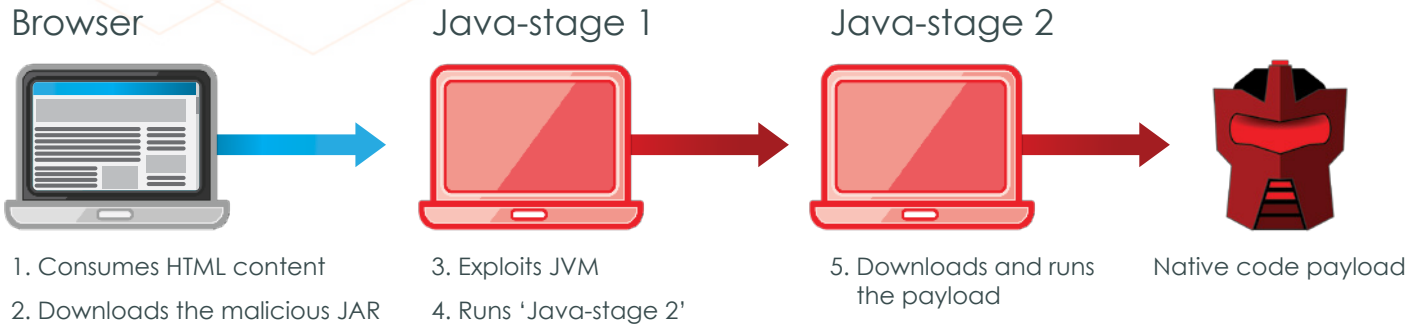
Deploying the Attivo ThreatDefend integrated with the NSP will dramatically improve the detection and prevention of a botnet's ability to complete their mission. The Attivo ThreatDefend provides a controlled environment where the infected machine can be emulated and communications can occur with the C&C on behalf of an infected machine. 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 machines in their network.

Key forensics provided by ThreatDefend

- Identification and detection of multi-stage exploit kits
- Identification of instructions sent from C&C server as part of initial callback mechanism. (ThreatDefend opens up proxy and can do MITM for SSL encrypted sessions provide forensics)
- Generation of Snort signatures which can be imported into NSP and block connection attempts on intent rather then signature

Example: Details of a multi-stage exploit kit

1. Users receive a phishing mail with malicious link
2. User clicks and opens the link browser
3. NSP blocks the request and redirect to ThreatDefend
4. BOTsink continues and emulates as end user
5. Provide detailed forensics of multi-stage attack



Solution Benefit Summary

Together, the Intel 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 C&C communication from production networks and to engage the attackers C&C to gather 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 botnet.
- Customized decoys can be deployed with the ThreatDefend Platform.
- ThreatDefend forensics and alerts provide the full packet capture of the communication between the decoy and the C&C.
- Substantiated, actionable alerts are provided in STIX and Open IOC formats to share the threat information with other security vendors and applications. Alert details can also be shared with a syslog server.

About Attivo Networks

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