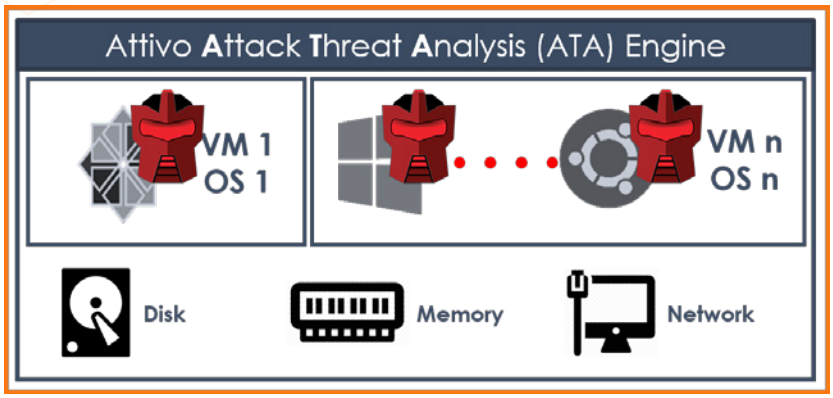
Attivo Networks BOTsink Analysis Functions

The Attivo BOTsink® deception engagement server provides several analysis functions to accelerate incident response. The BOTsink deception server detects active compromises from APTs, malware, ransomware, MiTM, Active Directory, and insider threats in the network based on interaction with the deception platform and provides complete attack analysis and forensic evidence reporting. To help security analysts investigate incidents, gather forensic evidence, and analyze malware, the BOTsink provides the Attack Threat Analysis (ATA) engine and the Malware Analysis Sandbox (MAS).

Attack Threat Analysis

The ATA engine is a primary feature within the BOTsink solution and provides analysis, monitoring, and correlation functions. The ATA engine conducts multi-dimensional correlation on all events on the decoy engagement servers to accurately identify and attribute malicious activities to the source of the attack inside the network. The ATA engine monitors and records all activity inside the decoys at the disk, memory, and network levels. Capturing this information for correlation and analysis, the ATA engine provides full visibility into all attacker actions within the deception environment. As the data is captured, the ATA engine analyzes the events to determine the source of the attack, correlating such data as the source network address, the operating system version, the hostname, and much more. This data is displayed on the BOTsink Dashboard and Analysis tabs, providing the information needed to investigate the malicious activity, and the forensic output to aid in investigation or remediation.

The ATA engine correlates the network traffic, memory activity, and disk activity for session-based forensic output. The ATA engine also outputs forensic evidence based on event analysis and querying from the Analysis tab, giving investigators a robust analysis tool to filter and query on specific activity, source address, time frame, or any other characteristic they choose to focus on, thereby accelerating the investigation. The ATA generates the forensic output as a Mandiant IOC file, a PCAP packet capture file, a memory analysis report based on analysis of the raw memory contents, or as a copy of the files that were dropped onto the decoy. The BOTsink solution uses the information gathered by the ATA to initiate automated incident response via 3rd party integrations with other security tools. The BOTsink solution can also automate incident response with the Attivo Networks ThreatOps solution, which provides the ability to create and define playbooks to sequence repeatable processes, and can automatically block and quarantine attacks through those same 3rd party integrations.



Malware Analysis

The Malware Analysis Sandbox (MAS) is a feature of the BOTsink solution, designed to analyze malicious binaries submissions. Additionally, for suspicious emails, URLs, and email attachments, the MAS analyzes the potential threat and provides detailed forensics to the security team, removing manual review cycles and accelerating their ability to react to malicious binaries or websites.

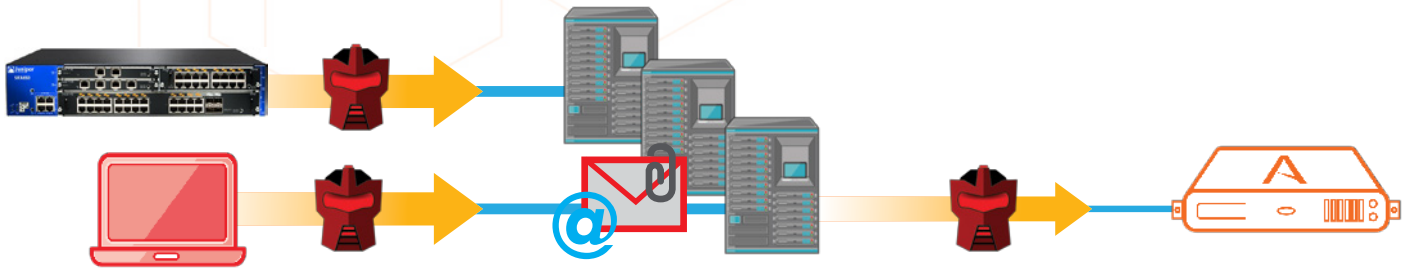
The MAS is a decoy within the BOTsink engagement server that is converted into a dedicated binary analysis VM that analyzes any user-submitted suspicious executable from phishing emails, potential malware, and other threats to capture lateral movement methods, observe malware behavior, and identify attacker IP addresses, such as Command and Control addresses on the Internet. The BOTsink architecture is built on full OS environments, which creates an environment where the malware can execute completely and provide comprehensive attack analysis. This sandbox environment allows exploits to develop without time constraints and can aid in understanding and shutting down sophisticated attacks, such as unrecognized polymorphic malware. The MAS records all threat activity, including payload drops, registry changes, and malware propagation methods. Detailed forensic products provide significant value in addressing and identifying broader vulnerabilities in the environment that may need addressing. Through 3rd party integrations (Firewall, SIEM, NAC, Endpoint), the platform can quickly operationalize with existing security controls to share attack information and remediate vulnerabilities.

For security teams, a dedicated malware analysis tool can be extremely helpful in not only threat intelligence but also in closing the skills gap. Due to the complicated and time-consuming nature of malware analysis, many teams do not have the resources or skills to employ a dedicated malware reverse engineer. By utilizing the MAS, organizations have full analysis capabilities while reducing the need for a manual analysis, which can often consume hours within a day.

Phishing Email Analysis

For phishing email analysis, the MAS provides a forwarding address that employees can forward any suspicious emails to for threat analysis. Once the MAS receives the email, it opens and detonates any attachments, and follows any links in the message. The MAS then produces a detailed analysis report that includes triggered YARA rules, C&C activity, VirusTotal matches, SHA1 signature hashes, and more.

With its ability to analyze numerous emails daily, the MAS saves security teams hours of work that would normally be spent manually checking suspicious emails. This time savings can then be reallocated to other critical projects.



1 Send suspected email to dedicated account

2 Download susptected email and execute in Sandbox

Conclusion

With phishing attacks on the rise, organizations are constantly being targeted by attackers looking to gain access to employee credentials. As these threats increase in frequency and sophistication, employees are experiencing more difficulty determining which messages are real and which are malicious. For already overtaxed security teams, phishing, URL, and email attachment analysis can require significant resources. By using the Attivo Malware Analysis Sandbox, security teams can forward potential threats to a central mailbox for investigation, or upload samples directly to the MAS, saving hours of manual analysis. Additionally, as many teams do not have the resources to analyze all the strains of malware that are detected in their network, the MAS provides this needed automated function. For organizations looking to save time and resources by automating threat analysis, the Malware Analysis Sandbox is an essential piece of the security arsenal.

About Attivo Networks

Attivo Networks® is the leader in dynamic deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber-attacks. The ThreatDefend Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. www.attivonetworks.com