WHITEPAPER

Attivo NETWORKS®

STRENGTHEN DECEPTION AUTHENTICITY WITH MACHINE LEARNING AND DYNAMIC BEHAVIORAL DECEPTION

TABLE OF CONTENT

© 2021 Attivo Networks. All rights reserved.

EXECUTIVE SUMMARY

Malware attacks and data breaches are occurring at an unprecedented rate. Organizations are spending vast amounts of money on security solutions that claim to protect organizations from sophisticated attacks.

The best way to defeat sophisticated attacks is to implement dynamic behavioral deception, a security solution that detects in-network attack techniques and lateral movement activity. Unfortunately, today's next-generation firewalls, IPS, sandboxes, web, and email gateways are not up to that task.

Attivo Networks®, the leader in deception and concealment technology, offers adaptive cybersecurity defense using machine-learning to create deception campaigns that create authentic decoys to address the evolving threat landscape and ever-changing attack surface. The Attivo Networks Artificial Intelligence capabilities extend deception authenticity across the cloud and even into operational networks like SCADA/ICS/IoT/POS networks.

WHAT IS DYNAMIC BEHAVIORAL DECEPTION?

Once inside the network, an attacker starts to move laterally, looking for critical targets with valuable data. Deception for threat detection uses the ability to create an authentic environment of decoys and lures to deceive and attract attackers, thereby misdirecting them from production assets. Decoys matching the production environment include understanding the network and mirroring the systems, operating systems, and services that an endpoint or server uses.

The Attivo Networks solution provides authentic, high-interaction decoy technology to trap attackers into engagement, providing the advantage of early detection and the ability to gather extensive data for attack analysis. A behavioral deception solution's effectiveness depends on its ability to lure an attacker already inside the network. The dynamic engagement feature on the Attivo Networks ThreatDefend Platform attracts in-network attackers quickly and reliably detects them.

The following sections cover the four pillars of behavioral deception built upon machine learning to ensure an organization is least vulnerable to the growing cyber-attacks.

PILLAR I: SELF-LEARNING

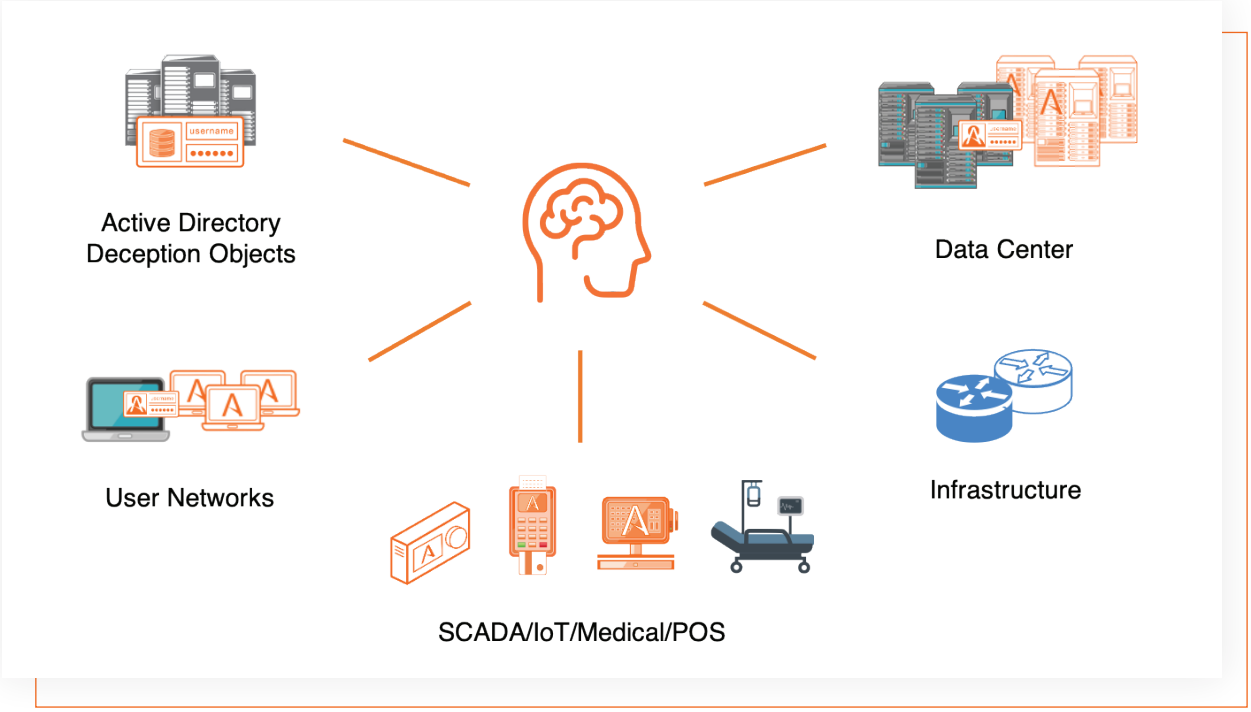
Security teams can use behavioral deception self-learning technology to intelligently auto-discover network behaviors to fingerprint, analyze, profile, and learn every endpoint on the network to circumvent attacker detection further. The Attivo Networks ThreatDefend® Platform's deception authenticity creates a fabric that attackers can't differentiate from production assets, which provides the most comprehensive evidence and analysis of an attacker's behavior upon attacker engagement.

© 2021 Attivo Networks. All rights reserved.

The Attivo solution uses machine-learning algorithms to create network campaigns by analyzing multicast and broadcast network traffic during network discovery. It learns network characteristics such as VLANs, subnets, endpoints, and other network activities automatically and the services, hostnames, MAC addresses, and operating systems of the discovered endpoints. It then creates decoys and assigns production IP addresses to them. When an attacker targets a particular service on an IP address acquired as part of the network campaign configuration, the solution identifies the service and routes this traffic to a relevant decoy VM for engagement.

PILLAR II: INTELLIGENT DEPLOYMENT

The solution gathers data from the production subnets and production endpoints through machine learning algorithms. It configures and adapts the decoys VMs based on the collected data, as discussed below. It then deploys the decoy VMs automatically, customizes them to match the production servers on the network, and generates deceptive tokens to deploy on endpoints.



ADAPTING DECOYS BASED ON ACTIVE DIRECTORY DATA

Attackers often look for the "keys to the kingdom," which frequently means administrative access to the Active Directory. The Attivo Networks Endpoint Detection Net (EDN) suite creates decoy credentials, which can easily fool attacker tools and misdirect them away from the production Active Directory. The EDN suite or the standalone ADSecure solution can also return decoy AD objects to unauthorized or illicit queries. These decoy accounts and query results appear authentic but direct attackers to the decoy VMs rather than production assets.

© 2021 Attivo Networks. All rights reserved.

The solution queries the specified AD Domain Services (DS) to learn the hostnames, usernames, operating systems, and services on production servers. After learning from the AD DS, the solution proposes the best customization and deployment option.

PILLAR III: CONTINUOUS MONITORING

The Attivo Networks solution incorporates machine learning and artificial intelligence into the security fabric. In addition to behavioral deception, the solution offers continuous monitoring and detection of sophisticated tactics and techniques such as ARP Poisoning, MITM (Man-in-the-Middle) attacks, and reconnaissance.

ARP DETECTION

The solution provides various options to detect attacker behavior in the network. It collects and analyzes the ARP requests and replies received. For example, an in-network attacker might attempt ARP cache poisoning attacks. The solution uses its artificial intelligence to automatically send ARP requests to the endpoints discovered in the network. It updates the endpoint ARP cache with entries for decoy VMs, increasing the visibility of decoy VMs as potential targets to attackers who attempt to steal information from a compromised endpoint's ARP cache. The solution investigates further to determine any suspicious ARP poisoning attempts and triggers alerts accordingly.

MITM ATTACK DETECTION

The Attivo solution analyzes NetBIOS Name Service (NBNS) and Link-Local Multicast Name Resolution (LLMNR) queries to detect Man-in-the-Middle attacks. If a MITM attack occurs within the network, the solution provides deceptive credentials to the attacker. The attacker eventually consumes the deceptive username and password, leading to a decoy VM. The decoy then engages the attacker further and raises alerts.

RECONNAISSANCE DETECTION

In-network attackers will attempt to understand the infrastructure and identify any vulnerabilities that might exist. Most recon activity involves identifying the operating systems and open ports on network endpoints. This information enables attackers to move laterally towards the required targets and to compromise more systems. The solution provides a very effective mechanism to customize decoy VMs and detect recon activities. When attackers launch recon activities inside the network, there is a very high chance of targeting decoy VMs and revealing the activity. With behavior deception, the Attivo solution can make the decoy VMs appear vulnerable, but at the same time realistic, luring attackers and disrupt attacks early in the attack cycle.

© 2021 Attivo Networks. All rights reserved.

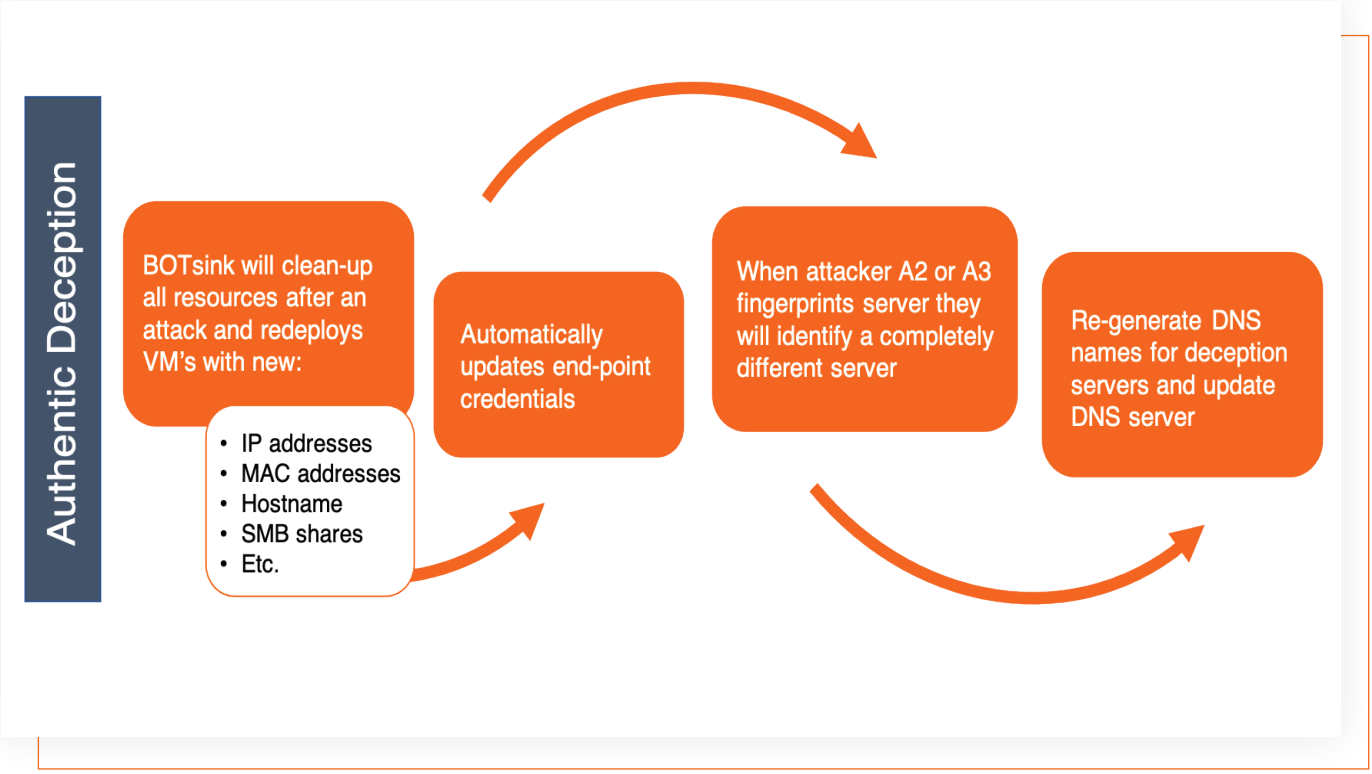
LATERAL ATTACK PATH MACHINE LEARNING

The EDN solution continuously monitors and assesses various vulnerabilities and credential exposures on endpoints. The solution provides intelligence to discover shadow admin accounts, privilege accounts, and other high-value accounts on endpoints. With machine learning capabilities, the solution offers valuable insights into stored, exposed, or orphaned credentials along with misconfigurations that allow attackers lateral movement access.

The solution provides continuous attack path learning and assessments of likely lateral attack paths that attackers would take to compromise a network. The solution exposes and provides visual graphs to these paths through the internal network based on misconfigured systems and misused or orphaned credentials. Within the dashboard, security teams can activate integrations with workflow and incident management systems to automate remediation notifications and processes.

PILLAR IV: SELF-HEALING

The ThreatDefend Platform uses automation and self-healing security models to maintain continuous security. The solution provides authentic deception after every possible attack and redeploys decoy VMs with new IP addresses, MAC addresses, hostnames, SMB shares, etc. This redeployment ensures the freshness of the deception fabric and increases the likelihood of surprising attackers.



© 2021 Attivo Networks. All rights reserved.

BENEFITS OF DYNAMIC BEHAVIORAL DECEPTION

- Ease of deployment
- Early detection of attack vectors
- Continuous assessment
- Better scaling

CONCLUSION

Achieving early detection into the network and adopting the above solutions reduces the risk of a successful attack and the time to remediate significantly. By leveraging machine learning, customers will benefit from increasing an organization's overall security. Self-configurable, self-healing, and automated decoys will lead to securing the network from potential attacks.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications and MITRE® Shield, and its capabilities tightly align to the MITRE ATT&CK® Framework. Attivo has won over 130 awards for its technology innovation and leadership.
www.attivonetworks.com

© 2021 Attivo Networks. All rights reserved.