IST-153 Workshop on Cyber Resilience

Title: **Cyber Resilience through Deception and Decoy**

Primary Author: **Don Woodard**
Address: **Attivo Networks**
47697 Westinghouse Drive
Fremont, CA 94539
Phone: **(703)217-3550**
eMail: **dwoodard@attivonetworks.com**

Attivo Networks introduces a new paradigm in security that complements and augments your existing security infrastructure. The technology deceives, detects, engages, and analyses malware that has bypassed traditional perimeter security and is already inside the network. Attivo's ThreatDefend suite of products help achieve network security by luring, engaging and trapping threats and malware from infected clients and servers in the user network, data center, cloud, SCADA/ICS network, and in the Internet of Things.

The ThreatDefend platform provides a new network security technology with real-time advanced malware detection that targets Advance Persistent Threats (APTs) and BOTs enabling cyber experts to eliminate threats that would previously go undetected. The solution addresses a full array of attacks, including reconnaissance, stolen credentials, ransomware, phishing, man-in-the-middle as well as insider threats.

The ThreatDefend product suite consists of the BOTsink appliance and its embedded software, which includes ThreatStrike, ThreatPath and ThreatOps. Physical and virtual BOTsink appliances are available for on premise and cloud based deployments. Multiple BOTsinks are managed by the Attivo Central Manager (ACM) appliance in a single GUI.

Attivo BOTsink systems are malware detection security tools that complement existing security systems. The ThreatDefend solution securely captures BOTs as they begin scanning the network, client, servers, and services and then tracks all their activity securely. It provides zero false-positive alerts and captures and records all of the malicious communication and propagation activity for future forensic analysis using Attivo's patented Multi-Dimensional Correlation Engine (MDCE).

The Challenge:

Today's cyber-attacks come in a variety of threat vectors, which can include attacks that start with reconnaissance, stolen credentials, phishing or ransomware attacks. Attackers are generally either scanning a network to find hosts with services or applications to compromise or seeking to exfiltrate employee credentials or data. Either way, attackers and their automation tools rely on the responses they receive throughout the attack process. The traditional incident response up to this point has been manual in nature, based on the known threats, but does not address the unknown types of attacks. Resilient technologies are the only platforms that address the ever-changing adversarial threat, remain flexible, easily integrate into other technologies, and recover quickly from adversary engagement. Today's cyber technologies must dynamically change as the threat in the network builds knowledge of the network assets so the adversary cannot complete their mission.

Response:

The Attivo deception and response platform is designed to make the entire network a trap, forcing the attacker to be right 100% of the time or risk being discovered. The solution combines distributed, high-interaction deception lures and decoys designed to provide early visibility into in-network threats, efficient continuous threat management, and accelerated incident response. The solution is based on six pillars, which include visibility, real-time detection, malware and phishing analysis, forensic reporting, incident handling, and response.

Recognized as the industry's most comprehensive deception platform, the Attivo solution provides network and endpoint deceptions and is highly effective in detecting threats from all vectors. These attacks may include advanced persistent threats, stolen credential, Man-in-the-Middle, ransomware, and phishing. Attivo's deception platform allows you to locate threats that are lurking within all types of networks including server, data center, user networks, ROBO, cloud, and specialty environments such as IoT, SCADA, and POS.

The Attivo Deception Platform is comprised of Attivo BOTsink engagement servers, decoys, and deceptions, the ThreatStrike end-point deception suite, ThreatPath for attack path visibility, ThreatOps threat orchestration playbooks, and the Attivo Central Manager (ACM), which together create a comprehensive early detection and continuous threat management defense against cyber threats.

Deception technology is a unique and modern approach that solves the problems organizations are facing in the current cyber climate. These platforms offer the capability to exercise deception-based detection throughout every layer of the network stack, enabling efficient detection for every threat vector. Utilizing high-interaction decoys and lures, deception solutions effectively trick attackers into revealing themselves, thereby closing the "detection deficit". The Attivo platform uses dynamic deception to camouflage itself by changing in an autonomous way which does not allow the attacker to build lists of targets to either avoid or ignore. Attivo dynamic deception also performs transformations on the endpoint using a light weight technology that is not intrusive and does not interrupt daily actions performed by the users of the enterprise. The dynamic deception capability monitors networks for indicators of compromise and automatically deploys more decoys and deception in those segments of the network. Adopting new methods of visibility into potential threat pathways will help agencies proactively deter threats by identifying areas of weaknesses that an attacker can use to maneuver within the network. Attivo Networks embraces this change by enabling the endpoint technology to perform predictive vulnerability analysis of user credentials, SMB shares, and other misconfigured components of the endpoints. Attivo Networks provides early visibility into threats and the evidence based alerts that are required to expedite incident handling. Real-time detection bundled with attack forensic analysis play a critical role changing the playing field against attackers. The hunters now become the hunted, putting the power of control back into an organization's hands.

The industry has been challenged over the years because the adversarial threat has outpaced individual vendor technologies and is forcing the need for cyber technologies to work together and integrate with a common goal to outpace this threat. Removing the "silo's" and building solutions that work together will accomplish this goal.

The lateral movement of sophisticated malware in the core of the network is a very difficult problem to address since the weapon may become polymorphic by changing and adapting to its surroundings. The adversary also builds lists or thumbprints of systems they have already visited or scanned during early reconnaissance activity. These issues cause us to rethink cyber solutions, where the threats exist, and how they act. Today's technologies need the capacity to adapt on the fly when the adversary engages the system. The solutions must identify indicators in the network of an adversary performing early reconnaissance and dynamically push resources to that area of the network to engage the attacker. The defensive and offensive strategies need to change to overcome this challenge and remove the human decision factor within the response to these challenges. Attivo Networks' capabilities are a necessity for your cyber solutions to be effective in addressing today's threats.

Dynamic deception solves this issue in several ways:

(1) By remaining agile in design
(2) By deploying exact copies of production systems
(3) Being resilient upon engagement
(4) Automatic deployment of decoys into suspect areas of the network
(5) Reporting of forensic data to combat threats
(6) Integration of disparate cyber technologies to resolve issues effectively and quickly

Attivo Networks gives the flexibility to the security team to import Gold Disk or STIG images of production systems into the BOTsink to use as decoys to project into the networks being monitored. These systems remain resilient throughout their job of engaging with the threat by changing components of the systems like IP addresses and MAC address to further strengthen the defensive side of dynamic deception. The BOTsink listens to broadcast traffic on the network segments being monitored for early reconnaissance activity and will push decoys out to the network where this activity is taking place. The Attivo Networks deception and decoy product solution will engage the adversary and deliver the forensic data of the Tactics, Techniques and Procedures (TTP's) the attacker is using. These findings are not only important for the integration into other technologies but are also imperative to the incident responder to successfully protect their network. The Attivo platform works in conjunction with the other security platforms and automatically responds immediately to the threat, removing the delay caused by the need for additional human intervention. The current need for cyber specialists to detect and react to threats based on predefined policies only slows the response time and allows the adversary more time to succeed in their mission. This integration of cyber solutions is imperative, enabling the industry to be more adaptive and agile to the ever-changing threat landscape.

The effectiveness of this technology has resulted in organizations across all major industries adopting deception detection technologies for early visibility into threats, improved incident response, and mitigation of risks associated with data and employee credential exfiltration.

Without a fundamental change in our defensive strategies the adversaries will continue to win. By providing a dynamic deception platform to lure attackers, we can more efficiently gain insight into threats and employ the appropriate technology to defend our critical assets. By enabling the ability to change our detection capabilities, industry and government will be able to identify threats faster and enable the SOC team to better utilize their time to respond and remediate the threat.

Attivo Networks is in a unique position to offer these capabilities that have traditionally been very difficult to maintain. Previously, SOC team members have needed to sift through large amounts of data to discover an issue, the goal of this approach is to realign the human resources, help them get ahead of the threat, and respond with precision.

Summary:

Malware is becoming more and more sophisticated by adapting on the fly, and by living in the core of the network, where it is most vulnerable. The Attivo Networks solution and technological approach to cyber threat defense provides visibility into the actions that take place in the core of the network. The solution allows the SOC to run more efficiently through dynamic deception and decoy technologies, identifying threats in their early stages much more quickly than a human team could and provides forensic data that the incident responder needs. This allows the SOC team to concentrate on true threats and work toward understanding the threat in order to remediate it accordingly.

Additionally, change to the approach in defense and offense through harmonious integrations with best of breed cyber security technologies will significantly increase the pace of discovery, response and remediation. To accomplish this, vendor technologies must work in concert to respond without the need of human interaction. Automated services of perimeter and endpoint technologies can be employed for the most immediate response to threats.

To combat the cyber security challenges, the industry must adapt creative ways of addressing threats.   Dynamic deception and decoy is an extremely effective way to gain visibility into adversarial activity and to integrate those findings into the technologies that provide protection to the network automatically. This revolutionary technology provides network-based decoys as well as endpoint based deception which camouflages itself to the attacker and easily adjusts itself when needed. The placement of deception within the user's environment directly engages with the adversary causing them confusion and slowing down their mission. This wasted time gives the incident responder additional time to react by realigning critical resources to more important tasks in protecting their networks. In conclusion, Attivo's cyber deception platform provides a new layer of security for protecting critical assets from threats that have already bypassed traditional perimeter security measures.