GOING ON THE OFFENSIVE WITH ATTIVO NETWORKS ATTACK INTELLIGENCE

THREAT INTELLIGENCE, ADVERSARY INTELLIGENCE, AND COUNTERINTELLIGENCE

Security teams tend to be either defense-based or offense-based organizations, though they may do both in varying degrees. An offensive team would favor bold preemptive measures, whereas a defensive team is more likely to build fortresses to wait and react. Any good security plan must be agile enough to do either as the situation warrants. Organizations will have a tendency to favor one over the other based on style, available information, program maturity, and ability to apply advanced security strategies.

Attackers have traditionally held the offensive advantages of deception, stealth, and surprise in cyber incidents. They leverage many techniques to remain hidden and "under the radar." At the same time, network defenders deal with information and alert overload, an ever-expanding attack surface, and many other challenges, including personnel and resource shortages. Information security teams are turning to deception to address this imbalance and change the asymmetry in cyberwarfare against attackers. The Attivo Networks ThreatDefend platform is ideal for detecting and gathering telemetry on attackers that have evaded perimeter security and are in the network. The ThreatDefend platform's network and endpoint decoys, breadcrumbs, and lures work to mislead attackers, diverting attention and attacks to deceptive assets that alert and record all their activity. Security teams can then apply this information to gain insight into all facets of the attack and obtain rich threat intelligence, adversary intelligence, and counterintelligence. With this level of data, organizations no longer need to wait for the attacker to make a blatant mistake, an exploit, or for a 3rd party to send notification of a breach. Instead, they can apply intelligence collected during attacker tactics of observation or reconnaissance for proactively understand attackers, for enabling them to decipher an attacker's mission better and to fortify their defenses accordingly.

THREAT INTELLIGENCE

Indicators of Compromise (IOCs) are the most common product of threat intelligence collection and development. Upon attacker engagement, the ThreatDefend platform captures all attack activity and provides information and metadata on attack tools, IP addresses, network traffic, and many other facets of the attack. These IOCs provide information that security teams can use to identify potential victims or strengthen existing defenses. The ThreatDefend platform's use of full operating system decoys enables the highest levels of authenticity and interactivity, deceiving attackers into believing they are interacting with a production system instead of a decoy.

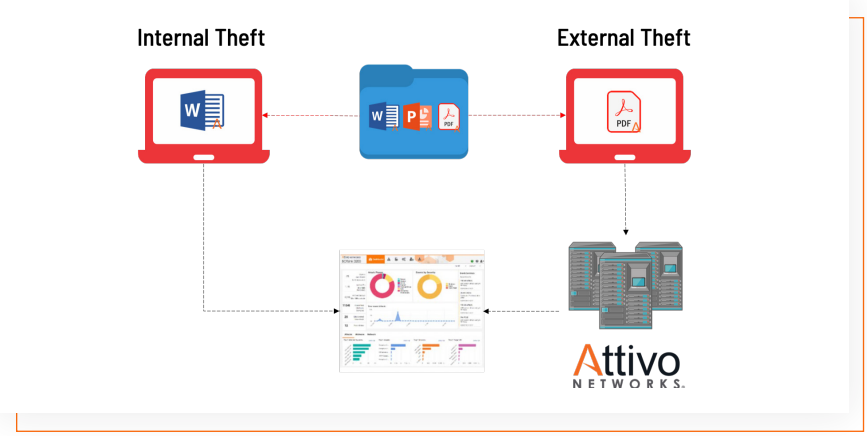
This function allows the attacker to explore the decoy as thoroughly as they wish while unknowingly providing the security team with extensive threat intelligence. At the endpoint, the ThreatDefend platform collects information when attackers attempt to extract data from Active Directory, capturing queries and identifying the critical AD objects they are gathering. It also identifies attempts to probe hosts to fingerprint them and identify ports and services to exploit, providing insight into the targets they are looking to compromise and tactics they are using.

ADVERSARY INTELLIGENCE

Security teams seeking to understand the attacker will look to identify and analyze their Tactics, Techniques, and Procedures (TTPs), patterns of activities or methods associated with a specific threat actor or group of threat actors that identify HOW attackers are attacking. The ThreatDefend platform provides insight into TTPs by capturing all aspects of attacks from start to finish, giving security analyst data they need to develop adversary intelligence while helping with risk management and incident response. These include capturing advanced interactions such as opening lines of communication to command and control servers and recording time-triggered and polymorphic actions.

COUNTERINTELLIGENCE

The ThreatDefend platform provides an inherently offensive counterintelligence function. The solution seeks to disrupt and degrade the information-gathering and attack operations an adversary conducts inside the network, while simultaneously providing collective counterintelligence functions by helping develop threat and adversary intelligence.



DecoyDocs create an alert when opened inside or outside of the network

While IOCs and TTPs help security teams answer how attackers are attacking, there remain the difficult tasks of identifying who is attacking and figuring out what information they are after. The ThreatDefend platform's DecoyDocs function provides the ability to plant decoy files that allow the organization to track documents that attackers exfiltrated. By embedding a tracking callback function into a document, the DecoyDocs solution can provide data on what attackers stole and beaconing data to identify where they opened the files. The DecoyDocs callback provides the externally facing IP address and geolocation of every system that opens the decoy files and

the name of the documents they stole. This information providing data that can help with limited attribution and identification while helping develop or improve proactive security measures.

DecoyDocs are fast and easy to set up. The organization loads decoy Word, PowerPoint, or PDF files into the BOTsink deception servers, which tags them for tracking along with the notification email address they send data to after attackers open them. The Attivo Networks cloud security service then alerts via this email address any DecoyDoc notices arising from any beacons it receives.

Today's modern attacker is making fewer and fewer mistakes, rendering a reactive defense much less effective. By gathering early and detailed threat-, adversary-, and counterintelligence, organizations can take a proactive posture to their security and ultimately call checkmate on the attacker.

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 130+ awards for its technology innovation and leadership.
Learn more: www.attivonetworks.com