Attivo NETWORKS®

Deception Technology—Much more than a Honeypot

Overview

With an increasing number of organizations interested in introducing deception into their multi-layered security defense, it is not uncommon for a prospect to ask, "Isn't deception technology the same thing as a honeypot?" This is an all too common misunderstanding. At the most rudimentary level, yes, they are both fashioned to mislead, perplex, and stall an attacker in their attempt to acquire sensitive data. However, outside of that, the two technologies could not be more dissimilar. This solution brief will detail the origins of honeypots, the logic behind them, and what features ultimately inhibited their universal adoption - followed by a look into what comprises present-day deception technology, how it has evolved, and the functionalities that are catalyzing worldwide deployment and adoption.

The Origin of the Honeypot

Over 15 years ago, the first readily available honeypot, Honeyd, was introduced to the market. This tool provided emulated virtual hosts on a network, crafted to detect the presence of an enemy. Honeypots were designed primarily for research to analyze threats attacking the network. Typically, a honeypot would be placed outside of a network, and it would wait for inbound network connections to see if an attacker would engage with the decoy. The creation of honeypots placed greater focus on gathering general research than it did on fulfilling the essential need for in-network threat detection.

Where Honeypots Fall Short

Attackers today are increasingly more sophisticated, aggressive, and have greater resources at their disposal. It is no longer adequate to merely try to keep attackers out. Becoming overly dependent on prevention infrastructure inevitably leads to a detection gap when an attacker would successfully breach a perimeter. However, relying on a honeypot for this type of detection is limited by the inherent shortcomings of an emulated virtual host. Some of the primary limitations associated with honeypots include:

Authenticity: Human attackers can identify emulated honeypot systems, fingerprint them, and avoid interacting as a result.

Deployment: Honeypots lack centralized deployment/redeployment and require one per network segment.

Ease of operation: Honeypots require the intensive operation of highly skilled security experts and lack a management user interface. Additionally, they are labor-intensive to deploy, scale, and rebuild after attacker engagement.

Scalability: Honeypots cannot scale across any environment, enterprise user network, cloud remote office, or specialized environments such as ICS, IOT, or POS.

Interaction: Low-interaction honeypots can't gather extensive attacker information, which results in alerts without substantiation and as such, will do little to support actionable incident response.

Attack pivot point: Attackers can take advantage of a compromised honeypot system and use it as a pivot point in continuing their attack.

The In-network Threat Detection Gap

In mid 2017, there were 791 organizations breached, a 29% increase over the prior year and it was reported that 60 percent of small companies are unable to sustain their businesses over six months after a cyber-attack.[1] As breaches continue to grow at unprecedented numbers and severity, the public is becoming increasingly frustrated with the current state of security and is demanding tighter security controls or risk losing their business.

Additionally, governments have begun proposing and imposing heftier regulations, fines, and even jail time on organizations who are breached but fail to notify affected parties in a timely manner. Upper-level Non-compliance to GDPR regulation, which will go into effect in May of 2018 could cost an organization up to €20 million, or 4% of the worldwide annual revenue of the prior fiscal year, whichever is higher.[2]

As a result, organizations are being forced to take a new approach and shift their security investments to one that includes not only prevention technology but also includes measures for early detection and response. This shift is driving interest and global adoption of deception technology for early and accurate attack detection and accelerated response to in-network threats.

Deception for Early Detection and Risk Mitigation

Used for decades in warfare, the introduction of deception for cyberwarfare is providing invaluable in changing the asymmetry of an attack. Deception decoys, and lures are placed throughout the network to make the entire network a trap. Additional bread crumbs are positioned throughout the network to proactively lure an attacker into engaging and into revealing their presence. By making the entire network a trap, IT teams gain the offense against attackers, so they can detect them early and derail the attack before any material damage can be done. Deception platforms are also instrumental in attack analysis and remediation as they automate the correlation of attack data and raise only substantiated alerts that are backed by details on attacker's tactics, techniques, and procedures. Indicators of compromise information are also collected to gain adversary intelligence and build better overall security defenses.

Modern-day deception technology goes well beyond what was ever envisioned for honeypots and has eliminated issues of operational functionality, scalability, and deployment limitations. Some of the advancements in deception technology features include:

Authenticity: Deception technology uses full operating systems, services, and applications to create an environment where decoys blend fully into the production environment and are not identifiable as decoys to the attacker. The ability to run the same software (golden image) of production assets takes authenticity to the next level.

Deployment: Advanced deception technology provides flexible deployment options and uses machine-learning to understand the network, simplify deployment, and automatically spin up and refresh the deceptions based on attacker engagement or based on suspicious network activity. Full feature deception is also not limited to network decoys and will also include the ability to detect credential theft, ransomware, and Active Directory attacks based on planted deception lures, shares, and objects.

Ease of operation: Deception platforms are easy to operate and manage via a central console or API integrations and do not come with a need for additional highly skilled security experts to operate.

Scalability: Deception platforms can deploy globally across an evolving attack surface including user networks, data centers, specialized networks (IOT, ICS, POS, SWIFT), and cloud environments.

Interaction: The use of high-interaction decoys, using real operating systems, empowers the deception platform to gather extensive attacker information through engagement. This information is then used to deliver high-fidelity alerts, provide forensic reporting, and automate incident response activity.

Attack pivot point: Deception platform decoys that are not inline are designed so that they are out-of-band and cannot be used as a pivot point to attack the rest of the network.

Knowing What to Look for in your Deception Solution

It is important to note that not all deception is created equal. Essentially, the purpose of deception technology is to detect an unwanted intruder when they carry out reconnaissance or attempt to move laterally from an initially compromised system into another system, or attempt to harvest credentials to escalate privileges. However, different deception players provide varying levels of authenticity and comprehensiveness in how they detect threats.

The modern threat landscape is constantly changing, making it vital for detection technologies to adapt to reliably meet the evolving needs of security teams. Deception plays a unique role in the security stack and closes detection gaps throughout the attack lifecycle. Organizations have struggled with accurate detection of attacker lateral movement and when credentials are used to escalate an attack. A trap and lure-based approach changes the approach to detection and removes any reliance on attack databases, signatures or the need to learn behavior in order to "get good" at detection.

With the use of deception, security teams can also slow down an attack in progress by redirecting that attack away from a production system to a decoy, all while the attacker is led to believe they are escalating their attack. This provides the security team with substantiated alerts and the threat intelligence required to capture and classify attack-related movement and the indicators of compromise on an attack. This information can then be applied to simplify attack analysis, forensic reporting, and to automate incident response actions such as blocking, quarantine, and threat hunting.

Security teams can also gain an advantage against ransomware attackers through the application of high-interaction deception, which can stall an attack by feeding them extensive amounts of fake data and providing the teams an opportunity to isolate the tainted system before the attack can spread widely. Performance testing shows that this technique can slow the attack by a factor of as much as 25x.

Modern deception technology can also be instrumental in validating the resiliency of network security. Authentic deception has proven its effectiveness in tricking highly skilled red team penetration testers into revealing themselves through the use of planted credentials and deception decoys. The detection alerts, attack analysis, and forensic reports can then be used for compliance or ongoing network visibility and risk assessment reporting.

Summary

Deception technology has evolved dramatically from the original concept of honeypots and now plays a critical role in accurately detecting and efficiently responding to in-network threats regardless of the attack vector or attack surface. Distributed detection platforms also present the opportunity create an active defense against attackers that will not only yield early detection, but also network threat visibility, and the automations to dramatically improve incident response.

Whether or not your organization has the most advanced or a less sophisticated set of security controls, everybody needs to know quickly and accurately, what's lurking in their network. Deception is demonstrating that it is the preferred technology for reliably answering this question.

About Attivo Networks

Attivo Networks is an award-winning leader in deception-based threat detection. It's ThreatDefend Deception and Response Platform provides enterprise, mid-market, and government organizations with a flexible and scalable solution for detecting threats across user networks, data centers, cloud and specialty environments such as ICS, IOT, POS, SWIFT, router, and telecom infrastructure. The platform provides high-interaction, authentic decoys for network detection and endpoint credentials and ransomware shares designed to deceive attackers into revealing their presence. The platform's automations for attack analysis and 3rd party integrations simplifying the understanding and incident response to attacks. More information can be found at www.attivonetworks.com

[1] https://www.denverpost.com/
[2] https://www.gdpreu.org/