WHITEPAPER

Attivo NETWORKS®

DECEPTION TECHNOLOGY— MUCH MORE THAN A HONEYPOT

OVERVIEW

As a growing number of organizations investigate deception technology, it is common for them to ask; "Isn't deception technology just a honeypot?" At the most basic level, early honeypots and modern deception technology both rely on setting traps for attackers. However, contemporary deception technology has evolved far beyond its roots in simple honeypots typically used for research. The technology has matured into deception platforms that include decoys, lures, application, data, database and Active Directory deceptions for comprehensive threat detection. Additionally, deception platforms can now provide extensive attack analysis and response automation capabilities. These solutions have removed the management and scalability complexity seen previously with honeypots so that companies, both small and large, can deploy and manage deception environments easily across cloud, on-premises, and operational technology networks.

This white paper will detail the origins of honeypots, the logic behind them, and what ultimately inhibited their universal adoption - followed by a look into what comprises present-day deception technology, how it has evolved, and the advanced functionalities that are behind its current worldwide adoption and deployment.

THE ORIGIN OF THE HONEYPOT

The first "honeypots" in computing are referenced in 1989 in Clifford Stoll's "The Cuckoo's Egg[1] " and built on earlier work at Lawrence Berkeley Laboratory[2] . Initial honeypots were primarily used for research to analyze threats attacking the network and were resource-intensive to set up, maintain, and analyze. These early efforts expanded in 1999 when Lance Spitzner introduced the Honeynet Project[3], which continues even now as a research organization.

In 2007, Niels Provos introduced honeyd[4] as the first effort to create an easily deployed virtual honeypot. This tool provided emulated virtual hosts on a network that were crafted to detect the presence of a malicious actor. Typically, an organization placed a honeypot on the perimeter outside of a production network, and it would wait for inbound network connections to engage with the decoy. The creation of honeypots placed greater focus on gathering general research and threat actor intelligence than it did on fulfilling the role of in-network threat detection.

> Contemporary deception technology has evolved far beyond its roots in simple honeypots typically used for research.

WHERE HONEYPOTS FALL SHORT

Today's threat-actors are more sophisticated, aggressive, and have more significant resources at their disposal than ever before. It is no longer adequate to believe that an organization can keep attackers out. Even with the most sophisticated security controls, mistakes and misconfigurations happen, new types of attacks occur, and no

1 https://www.goodreads.com/book/show/18154.The_Cuckoo_s_Egg
2 http://pdf.textfiles.com/academics/wilyhacker.pdf
3 http://www.honeynet.org/
4 http://www.honeyd.org/

security solution is 100% effective. Organizations that are overly dependent on prevention technologies will inevitably have a detection gap, where an attacker could successfully breach the perimeter and move undetected through the environment for months[5]. However, relying on a honeypot to detect these attackers post-breach is limited by the inherent shortcomings of an emulated virtual host and the logistics of deploying a conventional honeypot.

SOME OF THE PRIMARY LIMITATIONS ASSOCIATED WITH HONEYPOTS INCLUDE:

Authenticity: Human attackers can often identify emulated honeypot systems, fingerprint them, and avoid interacting with them.

Deployment: Honeypots lack a centralized deployment system, and usually require one per network segment. Redeploying honeypots requires as much effort as their initial installation.

Ease of operation: Honeypots are resource-intensive, requiring highly skilled operators to maintain and interpret their results. They also lack a management user interface, and can be very labor-intensive to deploy, scale, and rebuild after an attacker engagement.

Scalability: Honeypots cannot effectively scale across multiple environments, enterprise user networks, 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 does little to support actionable incident response. So-called "live system" honeypots present challenges of their own.

Attack pivot point: A threat actor can take advantage of a compromised honeypot system and use it as a pivot point to continue their attack. This circumstance can happen even with an emulated honeypot and is an even more pronounced issue with a 'live' system.

Lateral Movement: Honeypots do not provide adequate visibility into an attacker's lateral movement throughout the attack life cycle. This problem is pronounced especially with emulated honeypots.

THE IN-NETWORK THREAT DETECTION GAP

While the total number of reported data breaches dropped between 2017 and 2018[6][7], the number of exposed records climbed, and the cost of a breach has risen along with it. Dwell time also remains a prominent issue, with averages reported from several months to over a year, depending on industry and geography. Results from the Attivo Networks 2018 Threat Detection Report showed mixed results from industry professionals as to whether they believed the situation was improving or getting worse.

As data breaches remain at unprecedented numbers and severity, the public is becoming less tolerant of any organization that shows an inability to protect their information and they are increasingly becoming frustrated with the current state of security. Consumers are demanding businesses tighten their security controls or risk losing their business. Additionally, governments have begun proposing stricter regulations and imposing heftier fines, even jail time, on organizations that experience a breach and fail to notify affected parties promptly. Upper-level non-compliance to GDPR,

5 https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
6 https://www.darkreading.com/threat-intelligence/2018-was-second-most-active-year-for-data-breaches/d/d-id/1333875
7 https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

which went into effect in May of 2018, could cost an organization up to €20 million Euro ($22.3 million), or 4% of the worldwide annual revenue of the prior fiscal year, whichever is higher.

New legislation like the California Privacy Protection Act (CCPA) will add hefty fines that include a $7,500 fee for an intentional violation, $2,500 for other violations, as well as $750 or actual damages for each individual, whichever is greater. These penalties would have cost billions of dollars for several of the breaches seen recently. These fines can and will be devastating to many as they go into effect in 2020.

A recent survey by Enterprise Management Associates (EMA) found that users that were highly familiar with deception were not only highly confident in their ability to detect threats but were also able to reduce their dwell times down to 5 days.

As a result, organizations must take a new approach and shift their security investments to one that includes not only prevention technology but also measures for early detection and response. This shift is driving the interest in, and global adoption of, deception technology for early and accurate attack detection and accelerated response to in-network threats. A recent survey by Enterprise Management Associates (EMA) found that users that were highly familiar with deception were not only highly confident in their ability to detect threats but were also able to reduce their dwell times down to 5 days. It is a strong validation of the value that modern deception technology provides.

DECEPTION FOR VISIBILITY, EARLY DETECTION, AND RISK MITIGATION

Generations have used deception techniques in hunting, gaming, law enforcement, and military domains, including playing a crucial part in the largest military operation in history[8]. The introduction of deception technology for cyber defense has added valuable assets that are changing the asymmetry of cyber-attack. Organizations place deceptive decoys, breadcrumbs, and lures throughout the network to make the entire environment a trap, turning the entire environment into a virtual minefield to proactively lure and misdirect an in-network attacker into engaging and revealing their presence. By making the whole network a trap, information security teams can go on the offense against attackers, allowing them to detect an attack early in the cycle, gather company-specific threat intelligence, and derail the attacker before they can do any serious damage.

Deception platforms are also instrumental in attack analysis, forensics, and remediation. Deception systems automate the correlation of attack data and raise only substantiated alerts that are backed by details on the attacker's tactics,

techniques, and procedures. They can also collect accurate Indicators of Compromise (IOC) information to gain enhanced adversary intelligence and build better overall defenses.

8 https://ghostarmy.com/

Modern deception platforms can extend onto the endpoints, where attackers frequently leverage stolen credentials or misconfigurations to expand their foothold across the environment. By inserting deceptive credentials into the host, or even intercepting an attacker's efforts to leverage network authentication systems such as Active Directory, the information security team gains valuable insights and visibility int an attacker's activities while making the task much more complicated for a malicious actor.

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 thoroughly 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. This authenticity extends beyond the computing assets to include deceptive file shares and user credentials that appear identical to production assets. Deception can also include emulations for Industrial Control systems and network assets, covering the entire scope of devices and systems an attacker could encounter.

Deployment: Advanced deception technology provides flexible deployment options and uses machine-learning to learn the network and prepare credible deceptions. This capability simplifies deployment, automatically spinning up and refreshing the deceptive assets based on attacker engagement, suspicious network activity, or ongoing hygiene. Full feature deception is not limited to network decoy assets. Advanced systems can detect credential theft, malware and ransomware attacks, and Active Directory attacks based on planted deceptive credentials, lures, shares, and other objects.

Ease of operation: Modern deception platforms are easy to operate and manage via a central on-premises or cloud console or through SOC API integrations. They do not require additional highly skilled security analysts to operate or maintain. They also integrate natively with existing security controls to add value and simplify incident response operations.

Scalability: Deception platforms can deploy globally in physical, virtual, and cloud environments, protecting an evolving attack surface including cloud, user networks, data centers, remote locations, and specialized networks (IoT, ICS, POS, SWIFT). Advanced deception platforms will also offer forwarder technology to project deception into remote offices and isolated environments without requiring additional full deployments.

Interaction: By using high-interaction decoys, built upon real operating systems, the deception platform can gather extensive attacker information during an engagement. This information delivers high-fidelity alerts, provides forensic reporting, and enables automated incident response activity.

Attack pivot point: Modern deception platforms place decoys out-of-band, rather than in-line on the network. This deployment model prevents an attacker from using them as a pivot point to attack the rest of the environment. Advanced deception platforms also offer the option to route attacker traffic out through a dedicated connection, allowing the incident response team to observe and analyze the activity safely without risking internal assets.

ANWP082919
www.attivonetworks.com

Deception Credentials: Attackers frequently use stolen credentials to move laterally through the environment. Deception technology can place authentic-looking credentials that lead directly to decoy assets rather than production systems. By analyzing the organization's existing credential pathways, a deception platform can identify potential routes an attacker could take through the environment while providing highly authentic deception credentials – a capability that earlier honeypot technologies lacked.

KNOWING WHAT TO LOOK FOR IN YOUR DECEPTION SOLUTION

Many organizations are deploying deception technology as their primary in-network detection system to identify an intruder quickly when they carry out scanning activity, make efforts to move laterally from an initially compromised system, or attempt to harvest credentials to escalate their privileges. Deception for internal, in addition to external, threat detection has also established itself as a primary use case for the technology. Respondents to the EMA survey ranked 12 security tools for detecting insider threats. Thirty percent gave deception technology the highest ranking for being the most effective tool to detect insider threats.

Respondents to the EMA survey ranked 12 security tools for detecting insider threats. Thirty percent gave deception technology the highest ranking for being the most effective tool to detect insider threats.

The threat landscape is continually changing, and modern deception plays a unique role in the security stack to quickly detect threats throughout the attack lifecycle regardless of attack method or threat surface. Organizations have traditionally struggled to identify accurately when an attacker moves laterally and when they use stolen credentials to escalate an attack. Using traps, lures, and decoys change the approach to detection and increase detection accuracy by removing any reliance on attack databases, signatures, or the need to learn behavior to "get good" at detection. It also plays a critical role in reducing alert fatigue by only producing engagement-based alerts that contain the information required to respond decisively.

The information security team can also use high-interaction deception as a valuable tool against ransomware attacks. By feeding the ransomware process large data files that consumes its resources, the incident response team gains an opportunity to isolate the infected system before the attack can spread further. Performance testing shows that this technique can slow the ransomware's progress by a factor up to 25x.

With an advanced platform, security teams can also gain the ability to slow down an attack in progress by redirecting the threat actor away from a production system to a decoy, while leading an attacker to believe they have successfully escalated their attack. This capability provides the security team with substantiated alerts and the threat intelligence required to capture and classify attack-related movement, including indicators of compromise (IoC) from the attack. This company-specific information simplifies attack analysis, forensic reporting, and enables automated incident response actions such as blocking, quarantine, and threat hunting.

Modern deception technology can also be a powerful tool for regulatory compliance, instrumental to validating the effectiveness and resiliency of an organization's network security. Advanced deception has proven effective in detecting and tracking highly skilled red team penetration testers during an engagement, using authentic-looking credential and decoys that tricked them into revealing themselves. Organizations can then use the detection alerts, attack analysis, and forensic reports for compliance certification or ongoing network visibility and risk assessment reporting.

Selecting the best deception solution for a given organization distills down to meeting an organization's needs for operational efficiency, versatility, range of deception, authenticity, and effectiveness. While the prioritization an organization places on a specific threat or use case varies, these selection criteria remain common for any deception technology deployment.

SUMMARY

Deception technology has advanced dramatically from the original concept of honeypots and evolved into a comprehensive security platform that is easy to deploy and manage. Modern deception plays a critical role in accurately detecting, and efficiently responding to, in-network threats regardless of the attack vector or attack surface. Additionally, integrating deception technology with other components of the security stack improves automation and can dramatically improve incident response efficiency and effectiveness.

Whether an organization utilizes the most advanced and mature security platforms or employs less sophisticated security controls, they need to know quickly and accurately what's lurking in their environment. Deception technology has demonstrated that it can reliably and effectively answer this question and is becoming the preferred technology solution for detecting in-network threats.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend Deception Platform offers comprehensive and accurate threat detection for user networks, data centers, clouds, and a wide variety of specialized attack surfaces. A deception fabric of network, endpoint, application, and data deceptions efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning simplifies deployment and operations for organizations of all sizes. Automated attack analysis, forensics, actionable alerts, and native integrations accelerate and streamline incident response. The company has won over 90 awards for its technology innovation and leadership.

www.attivonetworks.com