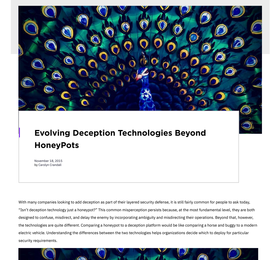
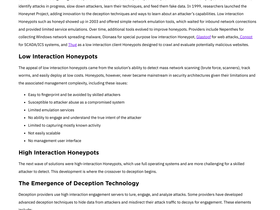


Evolving Deception Technologies Beyond HoneyPots

November 18, 2015
by Carolyn Crandall

With many companies looking to add deception as part of their layered security defense, it is still fairly common for people to ask today, "Isn't deception technology just a honeypot?" This common misperception persists because, at the most fundamental level, they are both designed to confuse, misinform, and delay the enemy by incorporating ambiguity and misdirecting their operations. Beyond that, however, the technologies are quite different. Comparing a honeypot to a deception platform would be like comparing a horse and buggy to a modern electric vehicle. Understanding the differences between the two technologies helps organizations decide which to deploy for particular security requirements.



The History

Let's start from the beginning. Gene Spafford introduced the concept of cyber deception in 1989 when he employed "active defenses" to identify attacks in progress, slow down attackers, learn their techniques, and feed them fake data. In 1999, researchers launched the Honeynet Project, adding innovation to the deception techniques and ways to learn about an attacker's capabilities. Low interaction Honeypots such as honeyd showed up in 2003 and offered simple network emulation tools, which waited for inbound network connections and provided limited service emulations. Over time, additional tools evolved to improve honeypots. Providers include Nepenthes for collecting malware automatically based malware, Dionaea for special purpose low interaction Honeypot, Glastopf for web attacks, Conpot for SCADA/ICS systems, and Thug as a low interaction client Honeypots designed to crawl and evaluate potentially malicious websites.

Low Interaction Honeypots

The appeal of low interaction honeypots came from the solution's ability to detect mass network scanning (brute force, scanners), trach worms, and easily deploy at low costs. Honeypots, however, never became mainstream in security architectures given their limitations and the associated management complexity, including these issues:

- Easy to fingerprint and be avoided by skilled attackers
- Susceptible to attacker abuse as a compromised system
- Limited emulation services
- No ability to engage and understand the true intent of the attacker
- Limited to capturing mostly known activity
- Not easily scalable
- No management user interface

High interaction Honeypots

The next wave of solutions were high-interaction honeypots, which use full operating systems and are more challenging for a skilled attacker to detect. This development is where the crossover to deception begins.

The Emergence of Deception Technology

Deception providers use high interaction engagement servers to lure, engage, and analyze attacks. Some providers have developed advanced deception technologies to hide data from attackers and misdirect their attack traffic to decoys for engagement. These elements include:

- Engagement or deception servers running real or emulated OS and services
- The ability to catch human attackers, not just brute force attacks
- Virtualization support
- Advanced deception techniques:
  - Customization for layer 2-7 deceptions
  - Fully controlled environment (contains infection and can destroy infected VMs)
  - Forensics and reporting
  - Capable of engaging with Command and Control
  - Data Concealment
  - Traffic redirection

There is a fair amount of differentiation even among deception providers. It is essential to note the differences in how authentic the deceptions are and how comprehensive the deception solution is to determine the right fit for one's organization.

Some Things to Consider when Evaluating Deception Solutions:

Platform vs. Elements:

Deception solutions come in several forms, and one must decide how broadly to deploy and what types of attacks to cover. For example, deploying only decoy systems will not reliably detect insider threats and stolen credential attacks.

- Decoy systems – lures and traps
- Endpoint and server deceptions
- Application deceptions

Real vs. Emulated Operating Systems:

Advanced deception providers will use real operating systems to mimic production systems and services. They can also allow organizations to fully customize decoys to appear as production servers by loading "golden images."

Comprehensive deployment: Solutions provide the ability to deploy deception systems alongside production systems in user networks, data centers, and the cloud in a scalable manner. Advanced deception solutions use machine learning to configure the decoys and lures automatically, reducing deployment complexity.

In-line vs. an IP Address Placed on a Trunk Port:

In-line devices will have to process all traffic and require more computing power with more network disruption, installation friction, and cost. Notably, in-line solutions will not scale effectively for east-west traffic detection in data centers.

Concealment and misdirection: Advanced deception solutions can hide local, network, and cloud data from attacker view, preventing attacks from targeting or accessing them. These solutions can also redirect traffic from production assets to decoys, resulting in early alerting and engagement.

Forensic Reporting and Integrations:

One should consider these elements:

- Depth of forensics provided – IPs, type of attack, methods, C2 actions
- Popular report formats: DOC, PCAP, STX, CSV
- Integrations with Firewalls, SIEMS, other devices for blocking, quarantine, and remediation
- Central threat intelligence dashboard with drill-downs

Scalability and Manageability:

These capabilities are necessary for operational efficiency:

- Scales across networks, private, and public data centers
- Central UI for management and threat intelligence aggregation
- Scales to on-premises, the cloud, and remote sites

Conclusion

With deception proving its utility in adding a second line of defense should attackers evade existing security solutions and having addressed the initial limitations of honeypots, deception technology continues to become mainstream in IT security infrastructures.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Alina Network Named a Cool Vendor in Gartner
- Detecting Unconstrained Delegation Exposures in AD Environment
- Top 10 Ways to Protect Your Active Directory
- Protecting Your Active Directory from AdminSDHolder Attacks
- Detecting a Rogue Domain Controller – DCShadow Attack
- Rise in Identity-Based Attacks Drives Demand for a New Security Approach