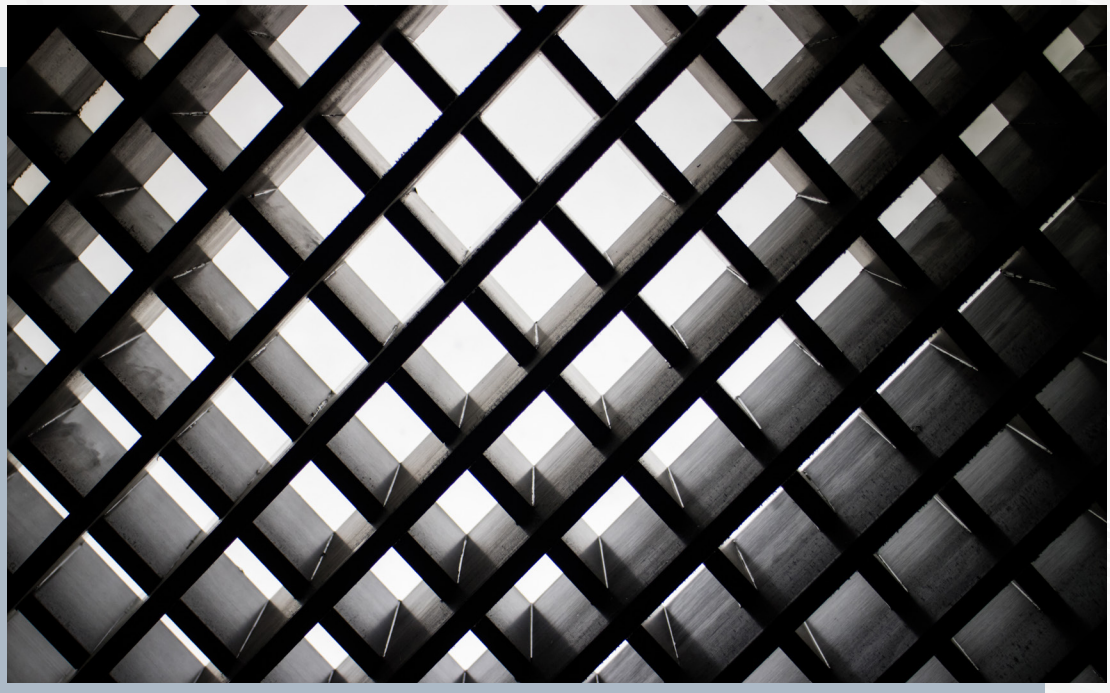
illusive

White Paper

Next Generation Deception Technology Vs. Honeypot Architecture



Deception Technology 101: A Quick Introduction

The idea of deceiving cyber attackers into thinking they've accessed valuable data isn't a new innovation. In 1999, the Honeynet Project, a non-profit dedicated to improving Internet security, developed the first network of honeypot technology.

These decoy computer systems were designed to purposely engage and deceive hackers in order to better understand their tactics and activities. The idea was innovative and effective at the time, but as environments became more sophisticated, deception technology needed to follow suit.

Despite the increasing effort that organizations are putting into keeping intruders out of their networks, once sophisticated attackers zero in on a specific company or information source, there's a good chance they'll find a way in.

Both honeypots and next-gen deception technology have their merits; understanding the key differences between the two is critical for determining which solution can best help an organization defeat the cyber criminals that step into its particular environment.

Perimeter Defenses Aren't Slowing Down Attackers

Despite increasing security investments and best efforts, industry studies and research continues to find that sophisticated malware authors and cyber criminals are innovating at a faster pace than security professionals can react to.

Attackers are increasingly able to slip past network security applications such as IDSs, IPSs, firewalls, and web application firewalls---regardless of how new and comprehensive they are.

Reacting to the attacks is the exact problem. Honeypots and next-gen deceptions are markedly different from traditional cyber security appliances and architectural solutions. Where complicated applications aim to react to a cyber attack and isolate it as soon as possible, honeypot architectures and next-gen deceptions take a more proactive stance to catch cyber criminals in the act.

When It Comes to Deception, Authenticity Matters

The most notable difference between honeypot architectures and a next-gen deceptions approach is their ability to mimic real-world scenarios. Cyber criminals have come to recognize there's something not quite right about honeypots, because they don't behave like a real user-controlled environment. When honeypots are deployed, they are configured to behave in a certain way, and automated to carry out specific tasks to appear authentic to cyber criminals. While this may have proven effective in the past, attackers are no longer deceived as they once were.

Deception Targets Threat Vectors Honeypots Miss

For example, social engineering and spear phishing attacks are an example of how honeypots can be outsmarted. Many attacks today start out with a lure that prompts a user to act in a way that allows malware in to infect the network.

Honeypots can scan for attachments, an old school attack vector, but are incapable of interacting with a spear phishing attack the way end users do, meaning honeypots won't be able to track the criminal or the attack. In contrast, next-gen deception technology is far more adaptive. In fact, it's capable of changing deceptions automatically and not remaining static---like an actual, dynamic network with natural changes in user and network information.

Honeypots are a much more static technology, covering only as much of the network as you can physically integrate with multiple deployments. Next-gen deception technology significantly covers more attack vectors, identifying attackers within three to four lateral movements—even if deceptions aren't deployed on every machine.

Cyber Criminals are Accustomed to Sniffing Out Honeypots

Understanding adversaries is essential for constructing the defenses that will trap them. Here are some of the ways cyber criminals determine whether or not a honeypot is in play:

If access seems too easy, it's probably a fake.

Typically, systems connected to the Internet are devoid of unnecessary ports and services. Any deviation from this configuration could be indicative of a trap.

If the systems still have factory default settings, this increases the chances of a honeypot being present.

If there's a considerable amount of empty hard drive space or very little software installed, it could be a honeypot.

If directories are obviously named (credit card numbers, employee data), the systems are clearly aimed at luring in attackers.

All of these warning signs tell cyber criminals that the system may not be legitimate.

Deception Frustrates Attackers across the Whole Network

In contrast, next-gen deception technology presents the attacker with endless elements of false information that appear genuine, subtly deluding them to the point where the attacker is caught between knowing what is real and what is illusion. This constitutes a more disorienting approach capable of misleading even the most experienced cyber attacker.

Next-gen deceptions provide powerful attacker detection and real-time forensics, with virtually no false positive alerts, and the attacker never knows his movements are being monitored. Honeypots provide value for attacker detainment, but at the cost of more false positive alerts.

Red Teams Agree: Honeypots Fail Where Deception Succeeds

In recent side-by-side Red Team Tests, honeypots provided "comparatively low detection rates with higher maintenance and management costs. These solutions are context-less, one-dimensional, and difficult to scale in a dynamic environment." The ROI isn't compelling for honeynet architectures.

On the other hand, next-gen deception technology was designed for the modern threat landscape. In Red Team Tests, it received high marks across the board:

- Red Teams found the next-gen deception technology extremely difficult to bypass. They set off thousands of alerts as they tried to move laterally through the system. The attack was easily tracked and they were prevented from reaching their ultimate goal.
- Cyber criminals compromise systems by moving laterally between machines. Security deceptions detect this early in the process, keeping track of real time forensic data and complete attacker profiling.
- With a Vector-as-a-Resource (V2R) focus, next-gen deceptions catch attackers off guard by appearing in places that don't coincide with old school methods. V2R can be anywhere and everywhere on a network, making it nearly impossible for attackers to detect false scenarios.

More Honey, Fewer Pots: Lightweight, User-Friendly Deception

Both honeypots and next-gen deception technology set out to proactively deceive and track cyber criminals during the attack phase. That's where the similarities end. Each approach looks very different, from both the enterprise and criminal perspectives.

Honeypots are hardware-based, physical systems that are deployed in the workplace and configured like any other workstation. These static systems act as a sort of sandbox, luring attackers in with the promise of sensitive data and then keeping track of their every move.

On the other hand, next-gen deceptions present a "hall of mirrors." False information is placed in the path of attackers who will use the information in their lateral movement infiltration phase. Attackers are methodical—they collect data, analyze it and calculate their next move as they relentlessly push through a network.

Illusive's next-gen deceptions take advantage of this mindset and cover the entire network in a blanket of finely tuned lures designed to attract cyber criminals, alert network administrators and disrupt the attack.

Not only can companies proactively thwart attacks, they can also gather critical information that can prove useful for future defense.

Conclusion

Honeypot architecture was innovative at its inception. It paved the way for a more proactive approach to cyber security and kept attackers at bay.

Yet, today, cyber criminals are more specialized, targeted and innovative when it comes to seeking new attack vectors and circumventing both perimeter defenses and old school honeypot traps. Cyber security professionals with limited time and resources reported that honeypot solutions were limited in their extensibility, expensive and difficult to manage. Clearly, companies can no longer afford to concentrate all of their resources on firewalls, first line of defense systems and honeypots.

Where honeypots are confined, next-gen deception technology is far more alluring and pervasive.

They also need to incorporate "internally focused" solutions such as next-gen deceptions to help identify a criminal while in attack mode. This type of preemptive technology represents a changing of the guard from old school strategies to more outside-of-the-box thinking that can finally trace and stop professional cyber criminals.

Cyber criminals are taking the time to analyze the human psyche as they craft carefully designed malware lures. It's time for cyber security professionals to take a page out of the attackers' play book and use a more realistic set of illusions to trap, track and thwart their actions from the start. With deceptions placed everywhere throughout the network and on every attack surface, cyber security solutions grow stronger. Essentially, an entire maze of inescapable deceptions can be placed over the network quickly, cost-effectively, and in a way that is scalable for the future.

For those that are serious about detecting attackers post-breach, Illusive's inescapable, next-generation deception technology is a vital step.

The Illusive Active Defense Suite enables organizations to create an environment that is hostile to attacker activities. Active Defense is vital part of a diversified detection strategy, filling an important attacker lateral movement detection gap in existing perimeter defenses. Each of the products in the Illusive Active Defense Suite play an important role in preventing attackers from achieving their objectives by creating a hostile environment and accelerating the time to detection for an attacker that has established a beachhead.

Attack Surface Manager (ASM) continuously analyzes and removes unnecessary credentials and pathways, reducing the attack surface.

Attack Detection System (ADS) makes it impossible for attackers to move laterally by transforming every endpoint into a web of deceptions.

Attack Intelligence System (AIS) delivers human readable on-demand telemetry for current attacker activities to speed investigation and remediation.

Illusive Inc
488 Madison Avenue
11th Floor
New York, NY 10022

Visit us: www.illusive.com
Email us: info@illusive.com
Call us:: US: +1 844.455.8748
EMEA / AsiaPac: +972 73.272.4006
Find us: