Contemporary Cyber Deception Strategies: A Comprehensive Analytical Study of Honeybot Systems and Their Intelligence Applications in 2025

The core philosophy of cyber deception systems and their historical development

In essence, “honeypot” systems represent a radical shift in cyber defense strategies, moving from a passive defense model that relies on building walls and barriers, to an active defense model that relies on proactive intelligence and deception.[1] A honeypot is defined as a security mechanism consisting of information resources (data, servers, or networks) that appear to be a legitimate and valuable part of the network, but are in fact isolated and closely monitored, and have no real productive value.[2] The fundamental value of these systems lies in the fact that they have no legitimate use; therefore, any interaction with them is necessarily considered suspicious activity or an attempted hack.[4]

These systems have evolved from simple detection tools in the late 1990s, such as the Honeyd system, to the integrated "Deception Technology" we see in 2025, which combines artificial intelligence and automation to create fake environments that adapt to the attacker's behavior in real time.[1] These systems act as “zero-noise sensors,” allowing security teams to filter out false alerts and focus only on real threats, thus solving one of the biggest dilemmas for Security Operations Centers (SOCs): “alert fatigue.”[7]

The strategic objective of deploying honeybots goes beyond simply detecting intruders; it aims to distract attackers from vital assets, deplete their resources and time, and gather accurate intelligence about their identities, methods, and tools (TTPs).[2] In the context of the advanced persistent threats (APTs) we are witnessing in 2025, the honeypot has become an indispensable tool for understanding the adversary’s mindset and developing proactive defenses capable of countering previously unknown attacks (zero-day exploits).[9]

Honeypot classifications according to depth of interaction and technical working mechanisms

Honeybot systems are classified based on the level of interaction they allow for the attacker, which in turn determines the quantity and quality of data that can be collected, as well as the level of technical risks associated with each type.[2]

Low-interaction honeypots

Low-reactivity honeypots are the most common in production environments due to their ease of deployment and low resource consumption.[3] These systems operate through limited emulation of certain services and protocols (such as SSH, FTP, or HTTP) without running a fully functional operating system.[2] When an attacker connects to these systems, they interact with software interfaces that mimic system responses, allowing the collection of basic data such as IP addresses, passwords used in brute-force attacks, and simple commands.[12]

These systems are characterized by a high level of security, as the attacker does not have a real operating system that he can exploit to move laterally within the network.[9] However, its limitation lies in its ease of detection by sophisticated attackers, as the typical and simulated responses often lack the depth that an expert would expect.[11]

Medium-interaction honeypots

These systems provide a strategic balance between realism and security, going beyond mere port emulation to include emulation of parts of the operating system or application layer.[15] These systems allow the attacker to execute a wider range of commands, such as browsing fake files or downloading files, while every action is accurately recorded.[15] The Cowrie tool is a classic example of this type, as it simulates an SSH server and allows the attacker to enter a fake "Shell" that logs all keystrokes and uploaded files.[15]

High-interaction honeypots

These systems represent the pinnacle of the "digital trap," where real operating systems and applications are deployed in all their complexity, while deliberately leaving security gaps to lure the attacker.[2] The strength of this type lies in the fact that it provides the attacker with a complete working environment, allowing researchers to monitor his behavior when attempting to escalate privileges, install remote controls, and move laterally.[1]

Despite the quality of intelligence it provides, it carries serious risks; if an attacker manages to break the isolation imposed on the honeybot, he may use it as a platform to launch attacks on the organization’s internal network.[7] Therefore, these systems require a sophisticated "Honeywall" to control traffic and prevent any leakage of damage.[21]

level of interaction	Degree of realism	Risk level	Data type group	Ease of publishing
Low	Simple simulation of services	Very low	Basic data (IP, Credentials)	Very easy[12]
Medium	Interactive simulation of layers	Medium	Session logs, malicious files	Medium[15]
High	Real operating system and applications	high	Complete TTPs, in-depth behavioral analysis	complex[1]
Pure	Complete physical production systems	Very high	100% realistic interaction	Very difficult[3]

Experimental studies in 2024 showed substantial differences in the efficiency of combining different levels; highly interactive systems attracted 76.12% of all attack packets compared to only 23.88% for low-interaction systems, confirming that attackers tend to stay and interact for longer periods in environments that appear more realistic.[11]

Strategic objectives: Honeypot productivity versus research

The objectives of deploying honeypots vary based on the role they play in the organization's overall security strategy.[2]

Production Honeypots

These systems are designed to be part of the day-to-day defenses of commercial and governmental organizations.[2] Its primary goal is to detect active threats within the network and mislead attackers away from sensitive data such as customer data or intellectual

property.[2]These systems are typically of a low-interaction type to reduce the administrative burden and technical risks.[3]

Honeybot productivity provides "high-fidelity" alerts; since no legitimate user is supposed to have access to Honeybot, any alert issued by it represents almost 100% malicious activity.[7]This helps security teams identify insider threats and compromised accounts very quickly.[21]

Research Honeypots

These systems are used by cybersecurity research centers, universities, and government agencies to gather intelligence about the "hacker world".[2]It is not aimed at protecting a specific network, but rather at understanding new tactics, analyzing malware samples, and studying how botnets evolve.[1]

Research honeypots are characterized by being extremely complex, and often consist of entire honeynets designed to record every movement with extreme precision.[3]The data extracted from these systems contributes to the development of new attack signatures, the improvement of artificial intelligence algorithms in defense systems, and the publication of reports on global threat trends.[13]

Functional diversity: Specialized honeypot types in 2025

As the technological landscape has evolved, specialized types of honeybots have emerged, designed to mimic specific digital assets, thus increasing the efficiency of the deception process.[2]

1. **Honeypots (Internet of Things):**With billions of Internet of Things (IoT) devices now in operation, these devices have become a prime target for building botnets.[2]These honeypots mimic surveillance cameras, routers, or smart lighting systems to attract attackers who exploit common vulnerabilities in these devices.[2]
2. **Honeypots Databases:**It aims to attract attackers who target data extraction (exfiltration).[2]These systems appear as databases (SQL or NoSQL) containing fake data that looks sensitive, such as credit card numbers or medical records, allowing for the monitoring of SQL injection techniques.[2]

3. **Web Application Honeypots:**It simulates login portals, e-commerce platforms, or administrator dashboards.[2]These systems help detect cross-site scripting (XSS) attacks and authentication bypass attempts.[2]
4. **Honeypot malware:**Designed to actively attract malware.[3]For example, the (Ghost) system simulates a USB storage device to test software that spreads across physical devices.[24]
5. **Client Honeypots:**It works in reverse; it simulates a human user browsing the internet or opening emails to search for malicious websites and servers that attempt to exploit browser vulnerabilities.[1]
6. **Honeytokens:**These are non-physical "digital traps," such as fake AWS keys, custom email addresses, or Word files containing a "beacon" that triggers an alert when opened.[2]These codes are very effective in detecting data leaks and unauthorized access to sensitive records.[28]

Honeynet architecture and advanced control systems

Honeynet goes beyond the idea of a single device to become a complete network that mimics the infrastructure of an organization, including servers, workstations, and network devices.[5]This architecture aims to study coordinated and complex attacks carried out by advanced threat groups (APTs).[29]

Honeywall: The Trap Keeper

The "Honeywall" is considered the most important component in the Honeynet architecture, as it acts as a gateway that separates the virtual network from the outside world and from the organization's real network.[21]The main tasks of Honeywall are:

- **Data Control:**Ensuring that the compromised honeybot is not used to launch attacks on third parties, by limiting the number of outgoing connections or filtering out malicious content.[1]
- **Data capture:**It logs all data packets passing through the network, logs keystrokes, and analyzes encrypted sessions.[22]
- **Stealth:**Honeywall often operates in "Bridge" mode (Layer 2 Bridge) without an apparent IP address, making it invisible to an attacker who believes they are communicating directly with the target.[22]

Honeynet Generations

The Honeynet architecture has evolved through three technological generations:

- **First Generation (Gen I):**It relied on physical separation and simple traffic control.
- **Second Generation (Gen II):**He integrated virtual technologies and began using more sophisticated tools to capture data.
- **Third Generation (Gen III):**This is the current standard in 2025, as it is based on a source-independent data model and uses "Honeyfarm" techniques for centralized management and analysis.[22]“Honey Farms” allows organizations to deploy hundreds of geographically distributed traps while directing all data to a single analysis center to maximize intelligence utilization.[31]

The AI revolution and large language models in cyber deception (2025)

The year 2025 saw a surge in the use of artificial intelligence (AI) and large language models (LLMs) to transform honeybots from static systems into adaptive entities capable of deceiving even the most cunning attackers.[32]

Adaptive Honeypots

Adaptive honeybots address the classic problem of traditional systems, which is "fingerprinting"; where professional attackers can detect the honeybot through its patterned responses or abnormal network delays.[14]Modern systems, such as HoneyGPT and CogniTrap, use artificial intelligence to change their behavior in real time based on the type of attacker and their skill level.[10]

These systems rely on advanced technologies such as:

- **Persona Induction:**The honeybot impersonates a stressed system administrator or an inexperienced user, tempting the attacker to continue the attack.[32]
- **Dynamic responses:**Instead of responding with static error messages, large language models generate realistic command outputs that include simulated "human errors," making the attacker believe they are inside a real system.[26]
- **Reinforcement Learning:**Frameworks such as ASGuard and CogniTrap use reinforcement learning algorithms to improve the "reward function," which is balancing collecting as much data as possible with ensuring the trap is not detected.[10]

Defense Efficacy Metrics

In advanced environments, quantitative metrics are used to evaluate the adaptive performance of the honeypot.[32]:

1. **Defense Efficacy Rate (DER):**It measures the percentage of attacks that were successfully neutralized or delayed within the trap.
2. **Honeypot Utility Score (HUS):**The quality of intelligence information is measured against cost and risk.[10]

Field studies in late 2024 proved that integrating large language models doubled the attacker's dwell time and increased the diversity of detected attack vectors compared to traditional systems such as (Cowrie).[10]

Deception in the cloud: AWS, Azure, and GCP strategies

As global infrastructure shifts towards the cloud, deception technology has evolved to include cloud-native resources.[34]The Honeybot cloud aims to detect credential theft attempts and lateral movement between accounts.[35]

Best cloud fraud practices in 2025

- **Publishing "Decoy Containers":**Using Docker and Kubernetes to deploy a lightweight, fast-deploying Honeybot that mimics web application services.[6]
- **Identity Decoys:**Create fake users in Active Directory or AWS IAM, granting them seemingly enticing privileges, and monitor any attempts to use these accounts.[34]
- **Storage Decoys:**Placing fake files containing "Honeytokens" inside S3 or Azure Blobs repositories that are ostensibly open to detect intruders.[34]
- **Cloud network isolation:**Use VPC Peering or Private Link to completely isolate the honeybot from the production environment, with native cloud monitoring tools such as AWS CloudTrail to log activity.[6]

cloud component	Trap type (Decoy)	The purpose of deception
(EC2/VM) Computing	Web servers with fake data	Initial hacking attempts revealed[34]

Identity (IAM/AD)	"Administrator" accounts with weak passwords	Attempts to escalate privileges revealed[34]
Storage (S3/Blob)	"trade secret" files are booby-trapped	Data extraction (exfiltration) detection[34]
Artificial Intelligence (GenAI)	Fake proxies and APIs	Uncovering attacks targeting artificial intelligence infrastructure[32]

Honeybots in Industrial Control Systems/OT (ICS/OT) and Cyber Warfare

Industrial Control Systems (ICS) are the critical nerve center of a nation's infrastructure and are a prime target for State-Sponsored Attacks.[38]

Challenges and solutions in an OT environment

Simulating industrial systems (such as power and water plants) is a major challenge because it requires extreme accuracy in simulating complex protocols such as Modbus, S7Comm, and DNP3.[25] In 2025, hybrid honeypots will become the standard, combining software simulation with real hardware (PLCs) to ensure the highest levels of realism.[40]

The Conpot tool is widely used to simulate these environments, and has contributed significantly to the detection of sabotage campaigns targeting the energy sector in Europe and the United States.[27] CISA reports in 2025 showed a 40% increase in the number of industrial devices exposed to the internet, making the deployment of honeybots a critical necessity for identifying threats before they reach real systems.[25]

Case studies: Threat group detection (APTs)

Deception technology in 2024 and 2025 helped expose several major cyber operations:

- **Mustang Panda Collection:**Espionage campaigns targeting diplomatic missions in Southeast Asia have been discovered using Honeybot, which mimics government file-sharing servers.[39]

- **Sandworm Group:**Attempts to disrupt Europe's energy infrastructure through sophisticated industrial traps have been detected, with the use of malware specifically designed for OT systems being recorded.[39]
- **Operation "Spectral Tango":**Security authorities (FBI) used honeybot tactics to infiltrate forums that traded stolen data (such as BreachForums), leading to the dismantling of major criminal networks in mid-2025.[43]

Tools and platforms: Between open source and commercial solutions (2025)

The deception technology market is characterized by great diversity, catering to the needs of various organizations, from individual researchers to large global corporations.[18]

Leading commercial platforms

Commercial companies provide integrated platforms that are easy to manage and capable of large-scale deployment with specialized technical support.[18]

Commercial supplier	basic product	Competitive power
Thinkst Canary	Canary Honeypots	Easy deployment (Plug-and-play) and high-definition alerts with minimal noise.[18]
Fortinet	FortiDeceptor	Deep integration with the "Security Fabric" and coordinated automated response.[18]
SentinelOne	Singularity Hologram	Using behavioral artificial intelligence to create dynamic, real-time deception environments.[28]

Zscaler	Zscaler Deception	Focus on Zero Trust environments and advanced cloud threat detection.[34]
Calvio	ShadowPlex	Leading in managing the deception lifecycle and automation in complex enterprise networks.[28]

Open source ecosystem

Open-source tools remain the preferred choice for researchers and organizations with strong technical teams who want to customize their environments.[27]

- **T-Pot:**An all-in-one platform that brings together more than 20 types of honeypots in one environment, with advanced visual control panels using Kibana.[18]
- **Cowrie:**The most popular tool for simulating SSH and Telnet services, and widely used for collecting brute-force attack data.[17]
- **Dionaea:**Specialized in capturing malware that exploits vulnerabilities in protocols such as SMB, HTTP, and FTP.[18]
- **Intel Owl:**An open-source platform for centrally managing and analyzing threat intelligence extracted from Honeybot and other sources.[27]
- **Honeytrap:**A low-reactivity system that acts as a general sensor for any unauthorized traffic on the network.[27]

Legal and ethical considerations and risk management in 2025

The deployment of the honeypot faces legal complexities that require a delicate balance between security needs and compliance with international and local legislation.[6]

The Entrapment Defense Dilemma

The issue of "entrapment" is one of the most controversial issues in cyber law.[49]

- **Legitimate enticement:**It is the placement of an apparently weak system on the internet to attract attackers who already have criminal intent; this is a legal and ethical practice that is acceptable in most countries.[49]

- **Unlawful enticement (Entrapment):**It is convincing a person to commit a crime that he would not have intended to do were it not for the direct incitement from the trap; this may give the attacker a strong legal defense in court and lead to the exclusion of collected evidence.[48]

Privacy and Compliance (GDPR/CCPA)

Honeybots, by their very nature, collect data about intruders, including IP addresses, behavioral logs, and sometimes personal data if the attacks originate from compromised, innocent user devices.[48]In 2025, organizations must ensure that:

- **Data anonymization:**Remove any personal information not directly related to criminal activity to comply with privacy laws such as (GDPR).[48]
- **Transparency with service providers:**The presence of Honeybot must be disclosed to cloud providers (AWS, Azure, Tencent) to avoid violating Acceptable Use Policies (AUP).[48]
- **Evidence integrity:**Ensuring that the collected records are not tampered with in order to guarantee their acceptance as criminal evidence in the event that the attackers are prosecuted.[6]

Risks of "compromise and pivot"

The biggest technical risk remains the transformation of the honeypot from a defensive tool into a launching point for the attacker.[7]If the system is not adequately isolated using VLANs, strict firewalls, or isolated virtual environments, an attacker may be able to use a honeybot to gain access to the organization's production network.[6]Therefore, it is always advisable to use "Honeywall" and run Honeybot in container environments that can be destroyed and rebuilt immediately upon detection of a breach.[6]

Summary and future recommendations for active defense

Honeypot systems have proven to be not just supplementary tools, but a cornerstone of the modern "Defense-in-Depth" strategy.[5]In a world characterized by automated and AI-powered attacks, deception is the most effective way to turn the tables on attackers.[1]

Strategic recommendations for organizations in 2025:

1. **Integrating deception into the security operations development cycle (DevSecOps):**The deployment of honey tokens and digital traps must be automated as part of building the infrastructure.[6]
2. **Investing in adaptive systems:**Start adopting deception techniques based on large language models to counter intelligent attack agents.[14]
3. **Focus on honeytokens:**Digital tokens (such as fake API keys) are less expensive, less risky, and more efficient at detecting data leaks.[18]
4. **Continuous monitoring and updates:**Attackers are developing their tools to detect traps; therefore, honeypot configurations and their "personalities" must be updated regularly to ensure the opponent is continuously deceived.[6]

In 2025 and beyond, deception technology will continue to evolve towards fully autonomous systems, where networks will be able to create "fake copies" of themselves instantaneously when they sense danger, making cyberspace an inhospitable and very costly environment for any aggressor.[10]