Treacle Tech
Security, Trust, Assurance

What Is Treacle i-Mirage?

Treacle i-Mirage is a next generation Deception platform that does not rely on blocking threats but instead turns the tables by allowing attackers to expose themselves.
It uses Artificial Intelligence to deploy realistic decoy systems that mirror real servers, applications, and user behavior. These decoys appear authentic and attract malicious actors into revealing their tools, methods, and objectives.
Every action taken by an attacker is monitored and analyzed in a fully isolated environment with no exposure to real business systems. This early insight allows defenders to understand and respond before any damage occurs.

What Makes Treacle i-Mirage Unique?

Behavior Based Adaptive Decoys That Learn from the Network

Treacle i-Mirage creates decoys that reflect actual user behavior and live system activity.These are not static simulations. They evolve automatically and stay aligned with the real environment, keeping deception fully believable.

Learning Engine with Artificial Intelligence

The system observes attacker behavior and updates itself over time. It adapts to new methods, learns from past events, and continuously improves its ability to detect threats early.

Only Real Threats Are Flagged

Because only attackers interact with the decoys, every alert is a confirmed malicious action. This removes guesswork and lets security teams focus on real incidents.

Zero Day Threat Discovery

Many of the captured payloads and malware samples were completely unknown at the time of detection. Treacle i-Mirage identified and reported these threats before any antivirus vendor or public source had seen them. This gives organizations early insight into attacks that no other system has yet discovered.

Live Capture of Malware and Payloads

The platform collects all tools, scripts, and malicious files attackers attempt to use. These are preserved for detailed analysis and intelligence gathering.

Clear and Simple Reporting

All technical findings are automatically translated into plain language. Executives and decision makers receive summaries they can understand and act on without needing a technical background.

Real Threats Captured by Treacle i-Mirage

Treacle i-Mirage has uncovered and reported dozens of completely new malware samples that were not found in any antivirus database or global threat feed. Captured directly through deception engagements, these genuine zero day threats represent serious and previously unknown risks to enterprise systems.

Notable Unique Threats Identified

Tailored Ransomware with Embedded Target Markers This malware contained environment specific variables suggesting it was designed for a particular organization. It terminated databases and encrypted critical files while staying undetected.	**GhostLocker** An entirely new ransomware strain that encrypted user data and displayed intimidation images. Only two antivirus engines flagged it initially despite its severe impact and stealth.	**Fense Hybrid Malware** A Linux executable embedded with Python components. It performed encryption service disruption and system alteration while remaining invisible to signature-based tools.	**Lucifer Memory Resident Trojan** A fileless malware that operated within system memory. It leveraged legitimate processes to escalate privileges and remained active without leaving traces on disk.	**SQL Exploited Trojan Installer** Delivered via database interaction this threat used side loading and shell commands to quietly install and run agents while deleting logs and cleaning up evidence.	**Exploit Payload Cluster** Included payloads targeting a variety of known vulnerabilities often disguised to bypass detection. They were delivered in early-stage reconnaissance and setup activity.

Treacle i-Mirage Performance Across Deployments

Category	Approximate Count
Unique zero day malware samples	More than 35
Total malware captured	More than 850
Exploit payloads recorded	More than 200
Attacker IPs identified	More than 5.4 million
VPN and anonymized traffic detected	Over 4 million
High frequency bot based attacks	Around 2 million
Total attacker interactions observed	Around 8.5 million

All of these events were handled without disruption to production networks. Each threat was isolated analyzed and converted into usable threat intelligence.

Strategic Advantages for Stakeholders

- **Proactive Threat Visibility**
  Catch attackers at the very first step instead of discovering incidents after the fact
- **Improved Decision Making**
  Clear executive reports backed by actual threat data support smart investment and policy choices
- **Better Threat Intelligence**
  Captured malware and behavior profiles allow better tuning of defenses and threat hunting
- **No Business Impact**
  Everything takes place in a separate layer so operations continue uninterrupted

Final Takeaway

Treacle i-Mirage changes how security works. It does not wait for threats to happen. It keeps them engaged and learns from them in real time. Every malicious attempt becomes an opportunity to grow stronger. Every sample and tactic become part of your evolving defense. With Treacle i-Mirage your organization gains visibility control and the power to stay ahead of evolving cyber threats.