TAG

USING AI-ENABLED DECEPTION TO STOP AI-POWERED ATTACKS

DR. EDWARD AMOROSO,
CEO, TAG[1]

ACALVIO

USING AI-ENABLED DECEPTION TO STOP AI-POWERED ATTACKS

EDWARD AMOROSO, CEO, TAG

This TAG technical report provides an overview of how AI-enabled deception can be used to counter AI-powered attacks, including adversarial AI. The platform from Acalvio demonstrates that such support is commercially available.

INTRODUCTION

Integrating artificial intelligence (AI) with cyber deception techniques offers a promising strategy to counter emerging AI-powered offensive cyberattacks, including adversarial AI. AI-powered deception leverages machine learning algorithms and rule-based logic to create dynamic, adaptive content that mimics real systems, confusing attackers and redirecting their efforts away from critical assets. Our team at TAG is excited about the prospects of this new application for AI, including for risk reduction of traditional attacks such as ransomware, as well as newer attacks using emerging technologies.

In fact, this new approach, in our view, will be particularly effective against adversarial AI, which uses sophisticated methods such as algorithmic bypass and real-time evasion to target victim systems. As demonstrated by the BlackMamba project, the use of AI enables the generation of polymorphic malware variants that are dynamically modified in each execution cycle, in an attempt to evade detection. By analyzing attacker behavior in real-time, AI-enhanced deception systems can adapt their responses based on collected data, making it increasingly challenging for adversarial tools to achieve their objectives.

An example might involve an AI algorithm analyzing patterns and anomalies in network traffic to identify when adversarial AI tools are probing for vulnerabilities. Once identified, the system could deploy high-fidelity deception with sensitive data in the form of decoys and honey tokens, drawing attackers into a controlled environment. The attackers' methods could be studied, and their actions restricted, thus neutralizing the threat while gathering useful intelligence.

Another practical advantage of combining AI with deception is scalability. Specifically, AI can help automate the deception process, enabling deployment and operation across complex, hybrid environments, including on-premises, cloud, and IoT systems. This dynamic adaptability will be crucial in defending against the fast-evolving nature of AI-powered cyber threats, which we expect to see grow considerably in the coming years, especially from nation-state actors.

Of course, it is not just AI-powered attacks that are countered by the use of AI-enabled deception. We've long believed at TAG that a wide range of cyber incidents could have been avoided had the defenders been more focused on using deceptive methods such as honey token usage to reduce risk. The good news is that commercial tools exist to help practitioners adopt these methods– and in the next section, we explain how Acalvio supports this goal.

ACALVIO ACTIVE DEFENSE

Acalvio's Active Defense Platform employs AI-driven cyber deception to enhance enterprise cybersecurity by proactively detecting and mitigating sophisticated threats. By deploying deceptive assets—such as honey tokens—throughout IT, OT, and cloud environments, Acalvio creates a dynamic security landscape that can confound adversaries and identify malicious activities early in the attack lifecycle.

Acalvio specifically integrates advanced AI techniques that automate and optimize the deployment of deception. Their patented Deception Farm architecture enables centralized management of deception across the enterprise network, ensuring scalability and realism. This architecture is complemented by Fluid Deception technology, which dynamically adjusts the complexity of deception in response to attacker engagement, providing both breadth and depth in threat detection.

Acalvio's AI algorithms automate the configuration and strategic placement of deceptions, creating assets that are enticing for attackers while targeting high-risk areas of interest. For instance, Acalvio's AI automates the configuration of over 100 attributes required to a create a realistic honeytoken user account in Active Directory, placing these accounts in locations most susceptible to exploitation.

Acalvio's platform also addresses emerging AI-powered attacks, including adversarial AI, by leveraging AI to detect and respond to these sophisticated threats. The platform's AI-driven analysis identifies stealthy techniques such as process hollowing and malicious script execution, enhancing the organization's ability to detect and mitigate advanced persistent threats. We view this as essential to handle the most advanced AI-powered attacks.

The company's solutions also align well with the principles of Zero Trust security models by providing comprehensive visibility into the identity attack surface and detecting identity threats with impressive precision. By integrating deception with Identity Threat Detection and Response (ITDR), Acalvio enhances the protection of identity architectures, a critical component in modern cybersecurity strategies.

Acalvio's solutions have demonstrated exceptional effectiveness in defending against advanced threats, including identity attacks, novel ransomware variants, and insider threats with precision. In a recent real-world exploit, Acalvio's strategically deployed honeytokens identified a stealthy insider attack targeting the identity architecture, preventing significant damage to the organization.

ACTION PLAN

We have long recommended at TAG that our Research as a Service (RaaS) customers from enterprise and government pay considerably more attention to the use of deception in their defensive strategies. The proliferation of AI as a means for improving, automating, and accelerating offensive attacks makes the use of deception even more important – and we are bullish on the prospects of combining defensive AI with deception to achieve this goal.

Our advice is that security teams immediately take inventory of how and whether any deception is being used today. Whether this review reveals some existing deployment or nothing at all, we strongly recommend that a discussion be held with Acalvio to better understand the possibilities. In the past, deception was viewed as more of a research task, but we can attest that it has reached production status and that it will improve defensive results for security teams.

Readers interested in more information on Acalvio are encouraged to reach out directly to the company. TAG RaaS subscribers can reach out to a TAG analyst through their TAG RaaS portal account for more guidance on the selection, deployment, and use of deception platforms, including Acalvio's AI-enabled solution. As always, we hope to hear from you as you work to continually optimize your program.

---

[1] TAG Infosphere is a New York-based research and advisory firm founded by former AT&T senior executives, including Dr. Edward Amoroso, former AT&T Chief Information Security Officer (CISO). Since 2016, TAG has focused on the provision of expert insight and tailored guidance for cybersecurity practitioners in hundreds of enterprise teams, government agencies, and commercial vendors located around the world.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence.