AI server attacked



Overview

Security researchers have documented a surge in coordinated attacks targeting artificial intelligence infrastructure, with more than 91,000 malicious sessions recorded between October 2025 and January 2026. GitHub - webpro255/awesome-ai-agent-attacks: A curated timeline of real AI agent security incidents, breaches, and vulnerabilities (2024-2026). Popular open-source AI servers were secretly hijacked for more than a year and turned into a silent army of crypto mining machines. GreyNoise's Ollama honeypot infrastructure captured 91,403 attack sessions during this period. From AI agents leaking internal data to coordinated global malware campaigns — here is everything that happened in AI cybersecurity between April 7 and April 21, 2026, with detailed attack paths for each incident. The fifteen days following April 7, 2026 produced six distinct AI-related security. OWASP just released the Top 10 for Agentic Applications 2026 - the first security framework dedicated to autonomous AI agents. We've been tracking threats in this space for over a year.

© 2026 FD SOLUCIONES OPTICAL SYSTEMS - All rights reserved

Article Content

webpro255/awesome-ai-agent-attacks

Impact: A low-privileged local attacker can bypass Copilot''s user-consent prompts and content filters, inject malicious code suggestions, silently disable telemetry consent, and leak

Hackers turned OpenWebUI AI servers into crypto mining

The researchers found a malware operation that''s been hijacking AI servers to mine cryptocurrency and steal sensitive credentials. The detected infections started by the end of 2024

Hackers Actively Exploit AI Deployments as 91,000+ Attack Sessions

Security researchers have documented a surge in coordinated attacks targeting artificial intelligence infrastructure, with more than 91,000 malicious sessions recorded between October 2025

Hackers Actively Exploiting AI Deployments

Security researchers have identified over 91,000 attack sessions targeting AI infrastructure between October 2025 and January 2026, exposing

6 AI Security Incidents: Full Attack Path Analysis (April 2026)

From AI agents leaking internal data to coordinated global malware campaigns — here is everything that happened in AI cybersecurity between April 7 and April 21, 2026, with detailed attack

The Real-World Attacks Behind OWASP Agentic AI Top 10

OWASP''s new Agentic AI Top 10 highlights real-world attacks already targeting autonomous AI systems, from goal hijacking to malicious MCP

AI Security Incident Tracker

Get updates and analysis on the latest AI security incidents from the PointGuard AI Research Lab.

New Agentjacking Attack Hijacks Your AI Coding Agent to Run Code

New “Agentjacking” attack that hijacks AI coding agents and silently executes attacker-controlled code on developer machines using nothing more than a single injected Sentry error.

AI agent at the wheel: How an attacker used LLMs to move from a

© 2026 FD SOLUCIONES OPTICAL SYSTEMS - All rights reserved

This is the first AI-agent-driven intrusion the Sysdig TRT has captured. The full attack chain — marimo notebook compromise to internal Postgres database dump — ran end-to-end in

Agentjacking Attack Tricks AI Coding Agents Into Running Malicious

Cybersecurity researchers have described what they say is a new class of attack that can trick artificial intelligence (AI) coding agents into running arbitrary code on developer machines.

HTTP/2 Bomb: AI-Discovered DoS Hits Every Major Web Server

HTTP/2 Bomb: AI-Discovered DoS Hits Every Major Web Server Key Takeaways Researcher Quang Luong at offensive security firm Calif, working with OpenAI''s Codex AI model,

Enterprises are racing to secure agentic AI deployments

AI security risks are rising as agentic AI, MCP integrations, and open models expand the enterprise attack surface and supply chain exposure.

JadePuffer ransomware used AI agent to automate entire attack

Researchers identified what they believe is the first documented case of a ransomware operation, JadePuffer, conducted entirely by a large language model (LLM) agent.

AI-Generated Browser Ransomware Abuses Chromium API on

Cybersecurity researchers have flagged a new malware artifact generated using DeepSeek that constructed a novel attack path combining "unrealistic browser-malware concepts with a real

New HTTP/2 Bomb Vulnerability Allows Remote DoS on NGINX,

Cybersecurity researchers have discovered a remote denial-of-service exploit that affects major web servers, including NGINX, Apache HTTPD, Microsoft IIS, Envoy, and Cloudflare Pingora.

Mastodon says its flagship server was hit by a DDoS attack

The DDoS attack against Mastodon''s flagship server comes less than a week after Bluesky was targeted with junk web traffic.

Hackers Can Leverage SQL Server 2025 AI Features

Overview Microsoft''s SQL Server 2025 was designed to bring AI into enterprise databases — but research from SpecterOps shows that these same features can be weaponized for

© 2026 FD SOLUCIONES OPTICAL SYSTEMS - All rights reserved

TechTarget

TechTarget provides purchase intent insight-powered solutions to identify, influence, and engage active buyers in the tech market.

Related Video Reference

This video was associated with the source search result. Verify technical details against current product documentation and project requirements.

Contact Us

Continue your research online:

Website: https://fdsoluciones.es
Technical inquiry: https://fdsoluciones.es/project-enquiry.html

This document is for preliminary research. Verify specifications against current standards, product documentation and project requirements.

© 2026 FD SOLUCIONES OPTICAL SYSTEMS - All rights reserved