AI second-circle server attacked

Overview

According to the South China Morning Post, the assault began with a DDoS attack, followed by brute-force attempts on user IDs and passwords. These efforts potentially allowed the attackers to infiltrate DeepSeek's platform, gaining insights into the AI technology that. Microsoft Incident Response – Detection and Response Team (DART) researchers uncovered a new backdoor that is notable for its novel use of the OpenAI Assistants Application Programming Interface (API) as a mechanism for command-and-control (C2) communications. Instead of relying on more traditional. 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. The analysis reveals two distinct threat campaigns that systematically exploit the expanding. Recent work by Check Point Research has shown how cybercriminals could use AI to enhance an existing attack method. Check Point has dubbed it AI as a C2 Proxy, and it introduces more headaches for anyone with a web supply chain to protect. It can be defended against, but before we get to that. Known for its groundbreaking advancements, DeepSeek has recently found itself in the headlines for a different reason—a cyberattack that has sent ripples through the tech community.

Article Content

Hundreds of Clusters Attacked Due to Unpatched Flaw in Ray AI

Thousands of servers running AI workloads are under attack by threat actors exploiting an unpatched vulnerability in the open-source Ray AI framework – widely used by such companies

OWASP Gen AI Incident & Exploit Round-up, Jan-Feb

Our goal is to provide a clear summary of each reported incident, including its impact, a breakdown of the attack, relevant vulnerabilities from the

Breaking News, World News and Video from Al Jazeera

News, analysis from the Middle East & worldwide, multimedia & interactives, opinions, documentaries, podcasts, long reads and broadcast schedule.

Thousands of servers hacked in ongoing attack targeting

Thousands of servers hacked in ongoing attack targeting Ray AI framework Researchers say it''s the first known in-the-wild attack targeting AI

AI As Malicious C2 Servers Is Almost Here – Reflectiz

The AI as a C2 Proxy technique highlights a broader challenge: as AI tools become embedded in websites and web workflows, they expand your attack surface in ways traditional

Cloudflare''s 2025 Q3 DDoS threat report -

Welcome to the 23rd edition of Cloudflare''s Quarterly DDoS Threat Report. This report offers a comprehensive analysis of the evolving threat

CircleCI MCP server: Natural language CI for AI-driven workflows

CircleCI''s CI-focused MCP server gives AI assistants direct access to your pipelines so they can retrieve logs, analyze failures, and suggest fixes, all in natural language.

ServiceNow Assist AI agents exposed to coordinated attack

A new exploit in ServiceNow''s Now Assist platform can allow malicious actors to manipulate its AI agents into performing unauthorized actions, as detailed by SaaS security firm AppOmni. Default ...

SesameOp: Novel backdoor uses OpenAI Assistants API for

Our investigation uncovered how a threat actor integrated the OpenAI Assistants API within a backdoor implant to establish a covert C2 channel, leveraging the legitimate service rather

Thousands of servers hacked due to insecurely

Ray deployments are not intended to connect to the internet, but AI developers are doing so anyway and leaving their servers vulnerable.

Hackers Breached Hundreds Of Companies'' AI Servers

Cybersecurity researchers have recently uncovered a significant breach involving hundreds of AI compute servers. Hackers exploited an open

DeepSeek''s Cyberattack: A Wake-Up Call for AI Security

According to the South China Morning Post, the assault began with a DDoS attack, followed by brute-force attempts on user IDs and passwords. These

Full report: Disrupting the first reported AI-orchestrated cyber ...

In mid-September 2025, we detected a highly sophisticated cyber espionage operation. We assess with high confidence that it was conducted by a Chinese state-sponsored group we''ve designated GTG

Enormous DDOS attack on Steam went largely unnoticed

Enormous DDOS attack on Steam went largely unnoticed In light of the recent PSN network outage, I''m glad to be a PC gamer and a Steam user. In August 2024, a massive DDOS

Have I Been Pwned: Check if your email address has

Have I Been Pwned allows you to check whether your email address has been exposed in a data breach.

Disrupting malicious uses of AI: June 2025

By using AI as a force multiplier for our expert investigative teams, in the three months since our last report we''ve been able to detect, disrupt and expose abusive activity including social engineering,

Unmasking APT36: How a ''Stealth Server'' C2 Infrastructure Was

The discovery of a new APT36 campaign, leveraging a rare “Stealth Server” command-and-control (C2) panel, highlights the continuous evolution of nation-state espionage tools.

What Security Teams Need to Know About OpenClaw, the AI Super

This demonstrates how security controls specifically designed to detect and prevent AI-based attacks can serve as a critical protective layer between users and AI agents like OpenClaw.

2025 Q4 DDoS threat report: A record-setting 31.4 Tbps

The campaign targeted Cloudflare customers as well as Cloudflare''s dashboard and infrastructure with hyper-volumetric HTTP DDoS attacks

Google Cloud mitigated largest DDoS attack, peaking

Google mitigated a DDoS attack which peaked at 398 million requests per second The most recent wave of attacks started in late August and continue

Arm Comes Full Circle With Homegrown, AI-Tuned Server CPU

The AGI CPU is about getting Arm server CPUs into the hands of large enterprises and companies that do not have their own chip design teams as well as giving those who design their

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

Analyze 6 major AI security incidents from April 2026. Get detailed attack paths on AI agent data leaks, global malware campaigns, and model exploitation.

New ShadowRay Attack Exploit Ray AI-Framework

AI Attacking AI Infrastructure The attack unfolds through multiple coordinated stages, beginning with reconnaissance using interact.sh, an out-of

Adversarial Misuse of Generative AI

Our analysis of government-backed threat actor use of Gemini focused on understanding how threat actors are using AI in their operations and if

AI Security Incident Roundup: April 2026

We track each in the PointGuard AI Security Incident Tracker, and side by side they reveal three patterns: agents are taking actions their operators never sanctioned, identity is the recurring failure

The Untold Story of the Boldest Supply-Chain Hack Ever

The attackers were in thousands of corporate and government networks. They might still be there now. Behind the scenes of the SolarWinds

Hackers Actively Exploit AI Deployments as 91,000

The analysis reveals two distinct threat campaigns that systematically exploit the expanding surface area of AI deployments, ranging from server-side

Aisuru botnet behind new record-breaking 29.7 Tbps

In just three months, the massive Aisuru botnet launched more than 1,300 distributed denial-of-service attacks, one of them setting a new record with

MCP Server Security: The Hidden AI Attack Surface

MCP server security is a critical blind spot in AI integration. Our researchers demonstrated code execution, data theft, and response manipulation

CircleCI warns customers to "immediately rotate all

Updated January 6, 11:00 BST: CircleCI has updated its advisory which deserves revisiting. CircleCI is calling on customers to “immediately rotate

Autonomous validation for the AI era

Deliver production-ready software at AI speed. CircleCI helps modern teams validate, test, and ship every change with intelligent automation.

Internet companies tackle the biggest ever denial of

Leading internet companies including Amazon and Google are taking steps to fight off the biggest distributed denial of service (DDoS) attack ever

Contact Us

For more information, pricing, or custom solutions, please contact us:

Website: https://www.invest-bud.com.pl
Email: sales@ibud-photonics.com
Phone: +33 1 45 62 89 07
Address: 10 Avenue des Champs-Élysées, 75008 Paris, France

This document is for informational purposes only. Specifications subject to change without notice.