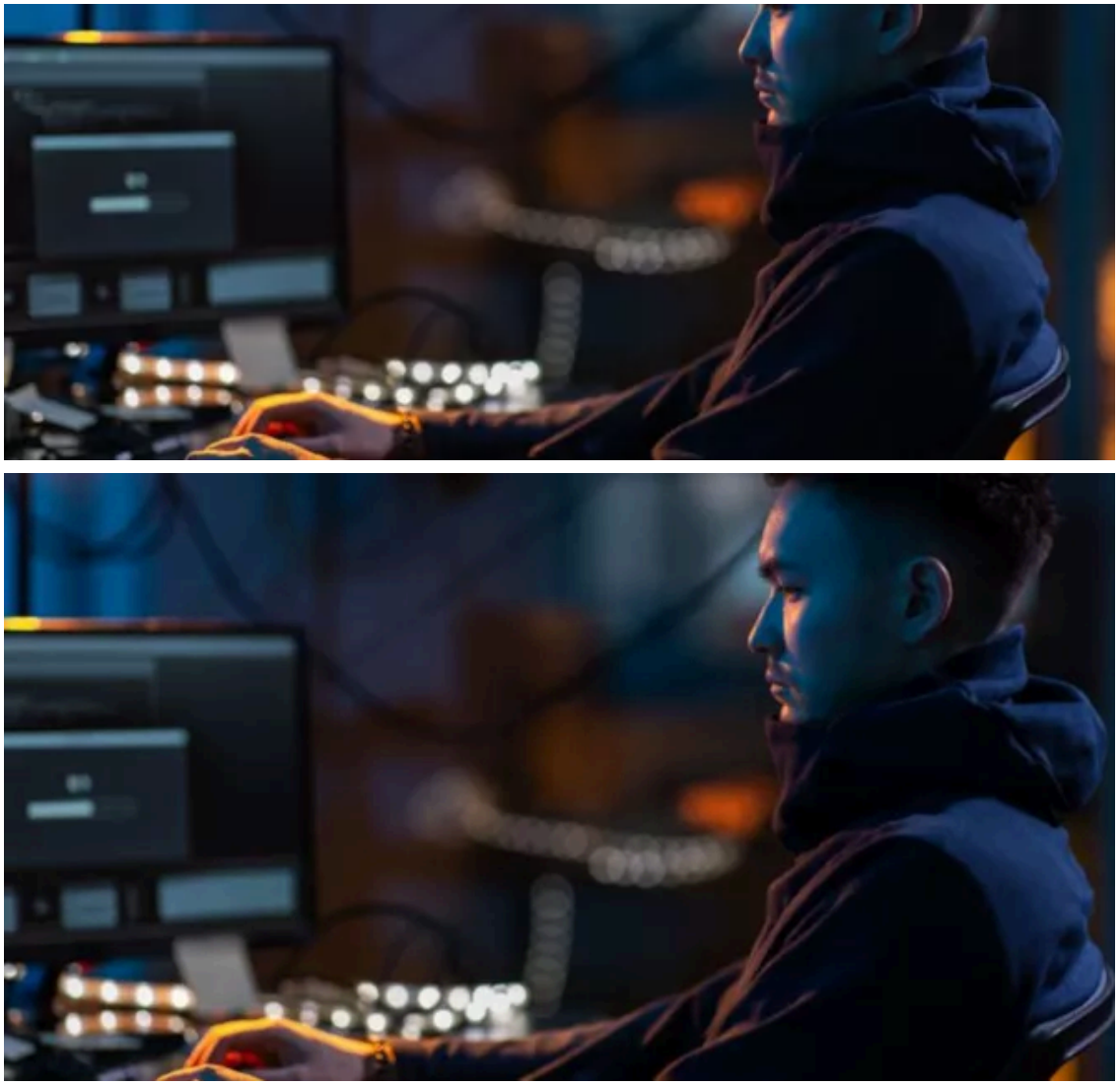
Research, News, and Perspectives

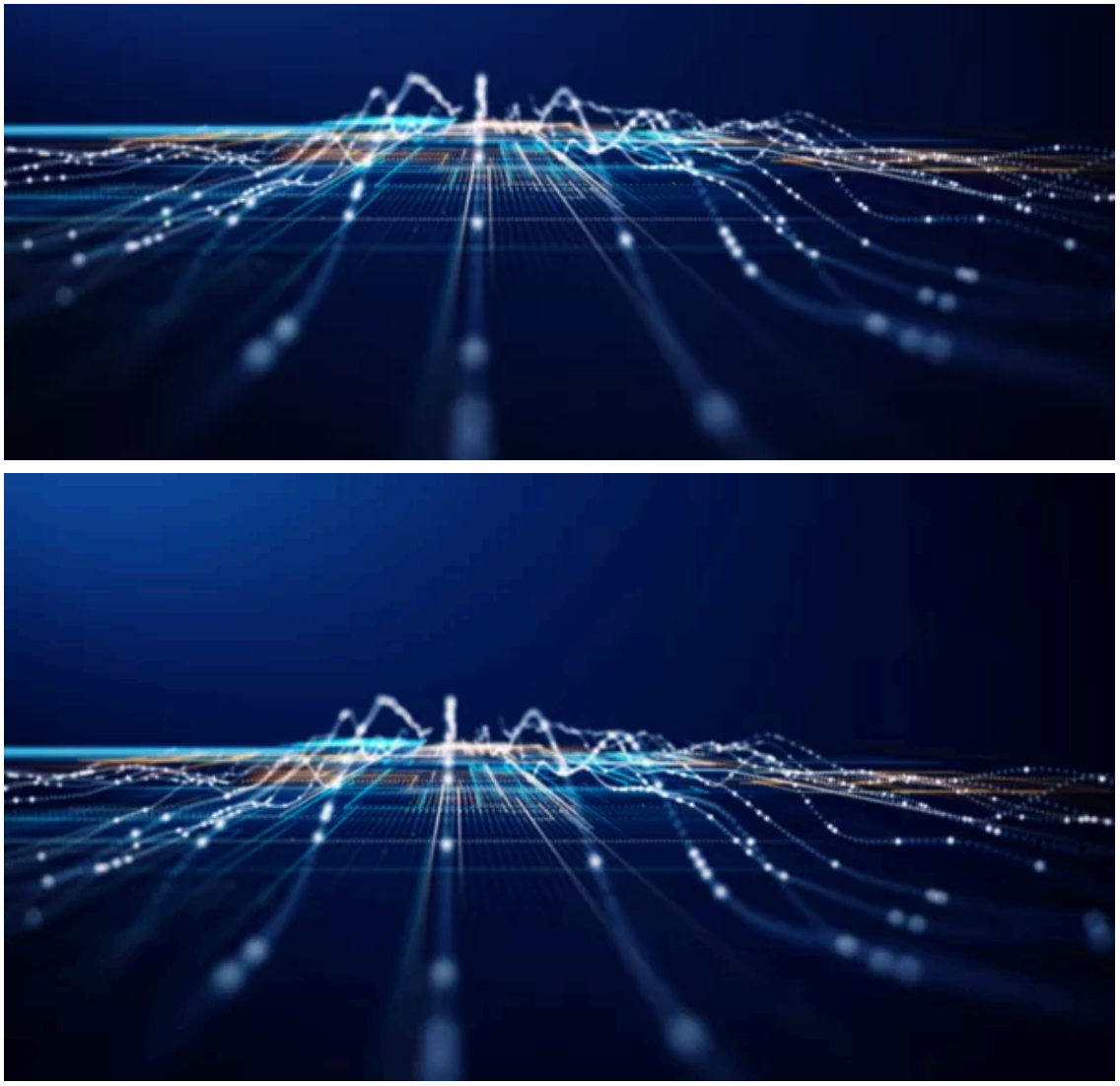
Archived: 2026-04-05 18:37:48 UTC



Artificial Intelligence (AI)

Weaponizing Trust Signals: Claude Code Lures and GitHub Release Payloads

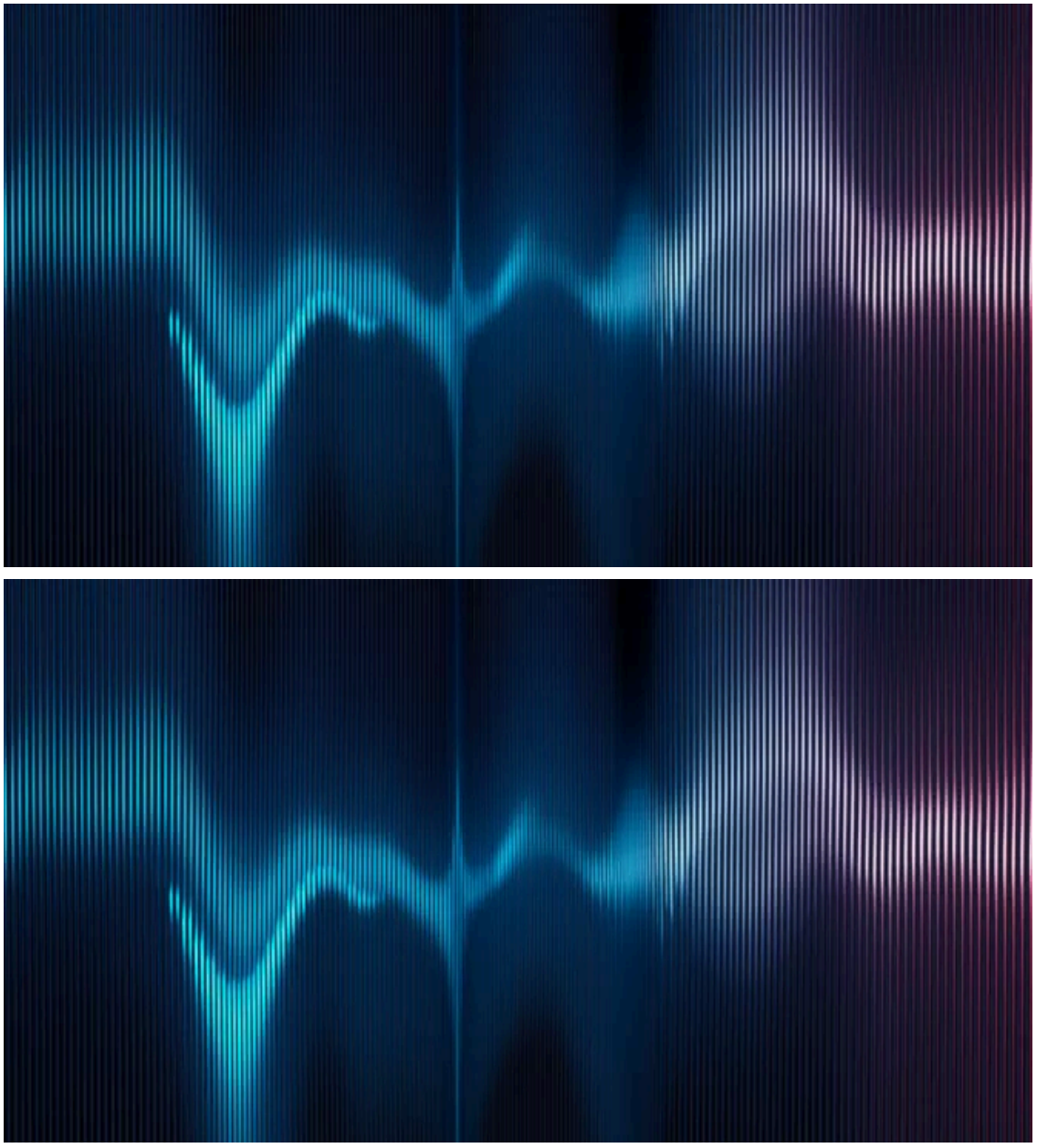
A packaging error in Anthropic’s Claude Code npm release briefly exposed internal source code. This entry examines how threat actors rapidly weaponized the resulting attention, pivoting an existing AI-themed campaign to spread Vidar and GhostSocks.



Privacy & Risks

TrendAI Insight: New U.S. National Cyber Strategy

TrendAI reviews the White House National Cyber Strategy, outlining six pillars to strengthen U.S. cybersecurity—from deterrence and regulation to federal modernization, critical infrastructure protection, AI leadership, and workforce development.



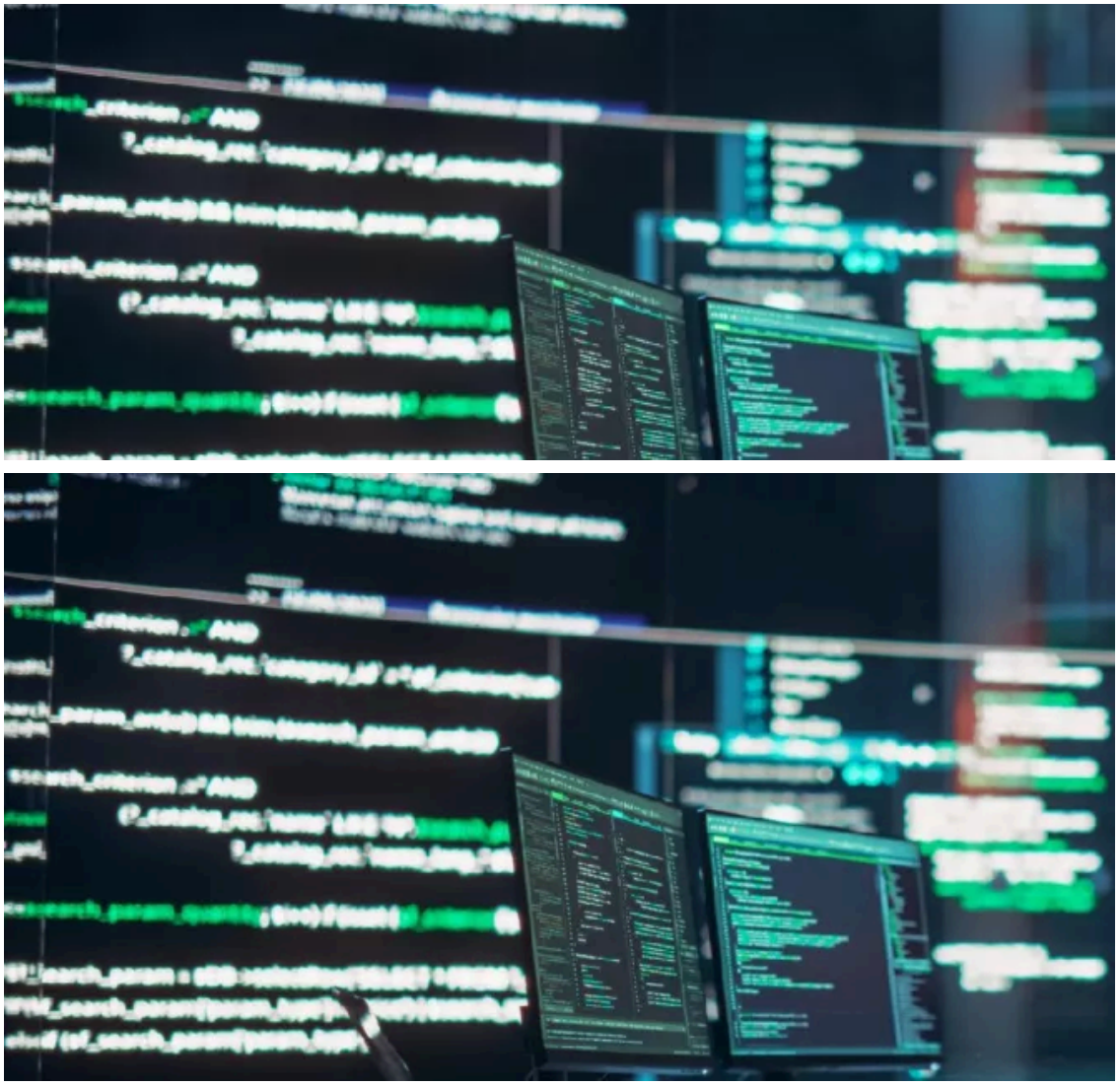
Artificial Intelligence (AI)

The Real Risk of Vibecoding

This blog looks at how AI-driven vibecoding speeds up software development while increasing security risk by outpacing traditional review and ownership. It explains why security needs to move earlier and be built into modern development workflows.

Expert Perspective Mar 31, 2026

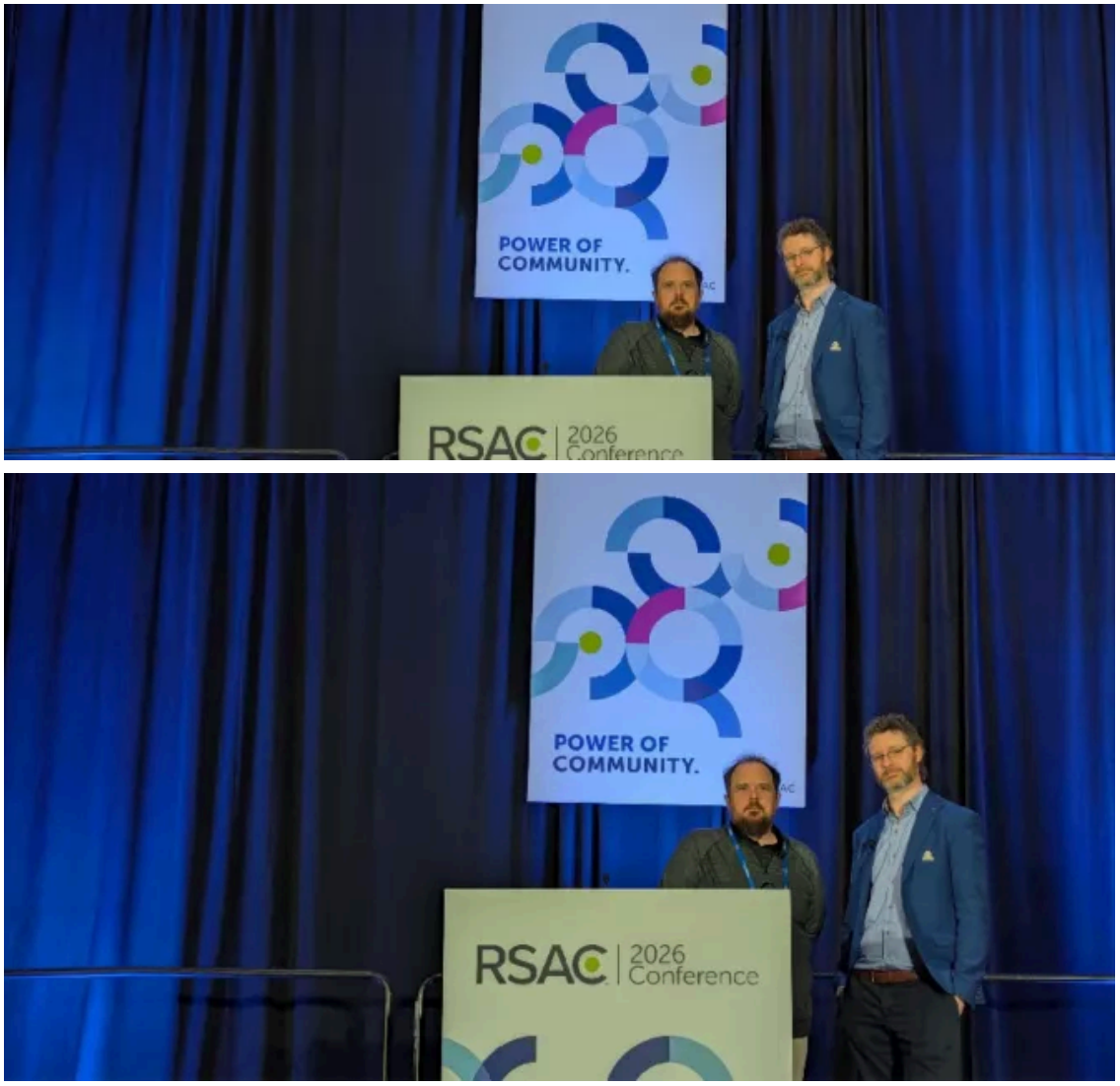
Expert Perspective Mar 31, 2026



Cyber Threats

Axios NPM Package Compromised: Supply Chain Attack Hits JavaScript HTTP Client with 100M+ Weekly Downloads

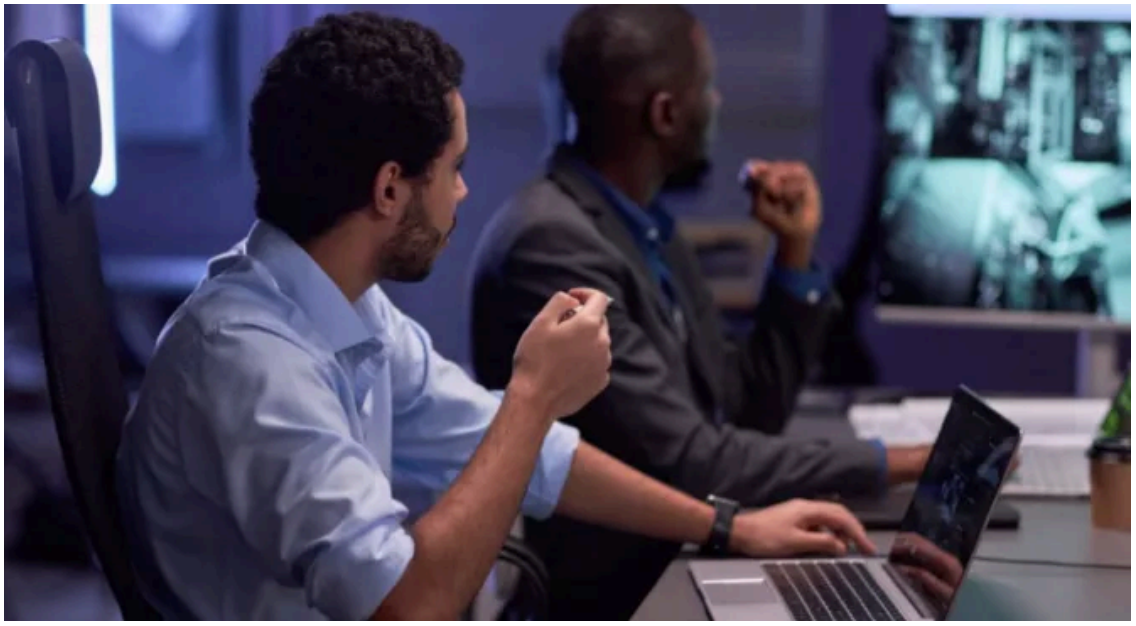
A supply chain attack hit Axios when attackers used stolen npm credentials to publish malicious versions containing a phantom dependency. This triggered a cross-platform RAT during installation and replaced its files with clean decoys, making detection challenging.



Artificial Intelligence (AI)

TrendAI™ Research at RSAC 2026: Advancing Defense Across AI-Driven and Cyber-Physical Threats

TrendAI™ Research explored agentic AI cybercrime and EV infrastructure security through two research sessions at RSAC 2026.



Malware

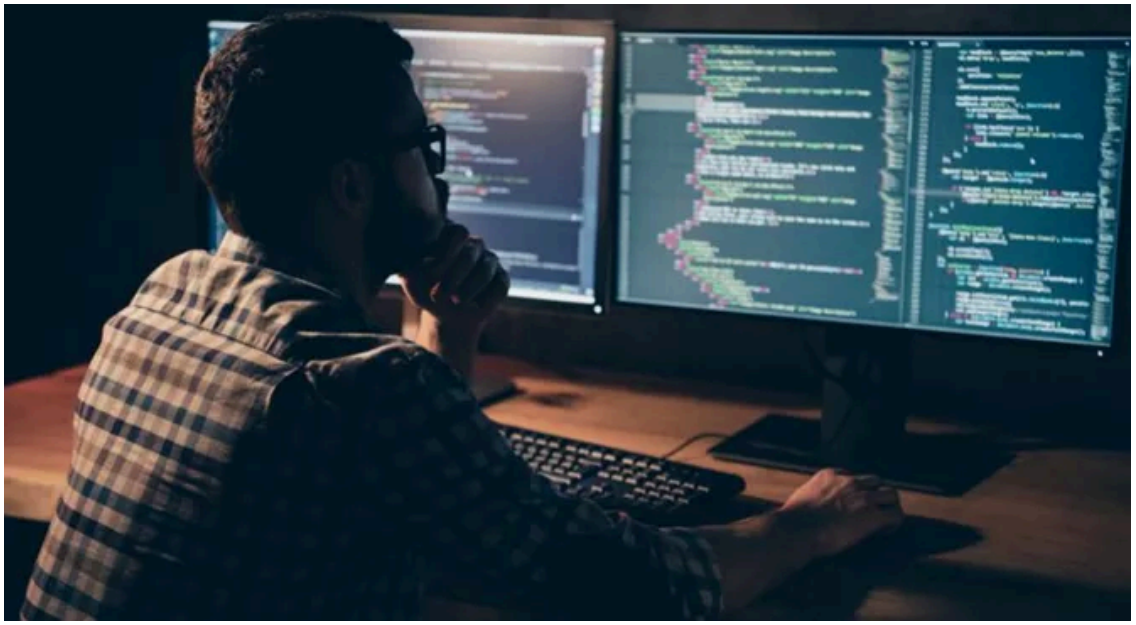
TeamPCP’s Telnyx Attack Marks a Shift in Tactics Beyond LiteLLM

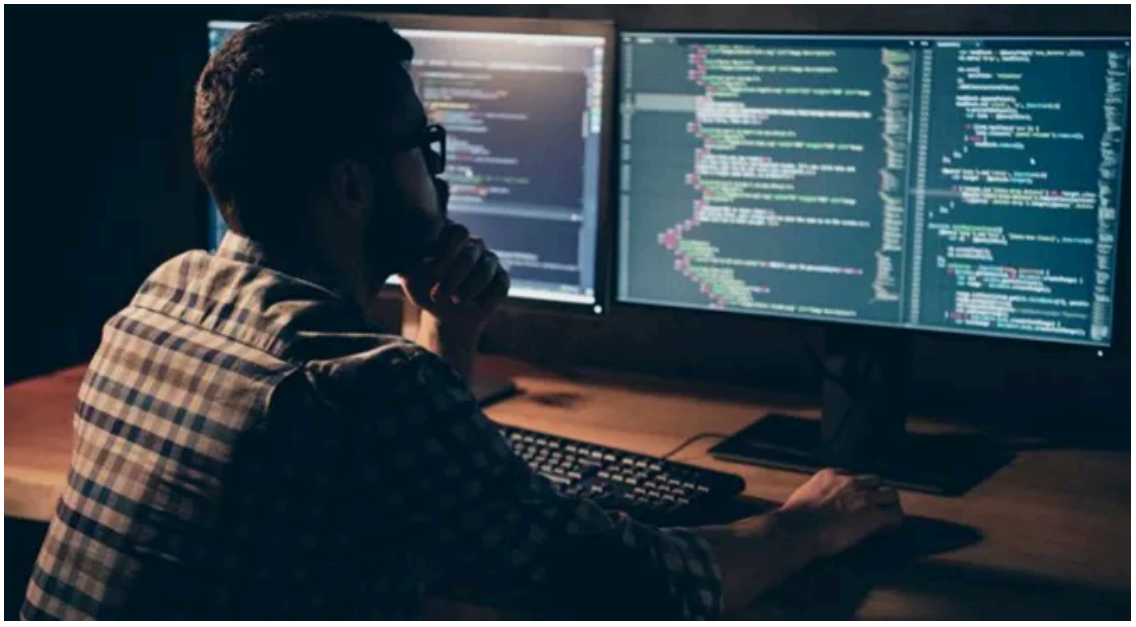
Moving beyond their LiteLLM campaign, TeamPCP weaponizes the Telnyx Python SDK with stealthy WAV-based payloads to steal credentials across Linux, macOS, and Windows.

Artificial Intelligence (AI)

Your AI Gateway Was a Backdoor: Inside the LiteLLM Supply Chain Compromise

TeamPCP orchestrated one of the most sophisticated multi-ecosystem supply chain campaigns publicly documented to date. It cascaded through developer tooling and compromised LiteLLM and exposed how AI proxy services that concentrate API keys and cloud credentials become high-value collateral when supply chain attacks compromise upstream dependencies.





APT & Targeted Attacks

Pawn Storm Campaign Deploys PRISMEX, Targets Government and Critical Infrastructure Entities

This blog discusses the steganography, cloud abuse, and email-based backdoors used against the Ukrainian defense supply chain in the latest Pawn Storm campaign that TrendAI™ Research observed and analyzed.

Artificial Intelligence (AI)

Your AI Stack Just Handed Over Your Root Keys: Inside the litellm PyPI Breach

Litellm PyPI breach explained: malicious versions steal cloud credentials, SSH keys, and Kubernetes secrets. Learn impact and urgent mitigation steps.

Expert Perspective Mar 25, 2026

Expert Perspective Mar 25, 2026

Malware

Copyright Lures Mask a Multi-Stage PureLog Stealer Attack on Key Industries

We look into a stealthy multi-stage attack campaign that delivers PureLog Stealer entirely in memory using encrypted, fileless techniques.

No matches found

Source: https://blog.trendmicro.com/trendlabs-security-intelligence/control-panel-files-used-as-malicious-attachments/