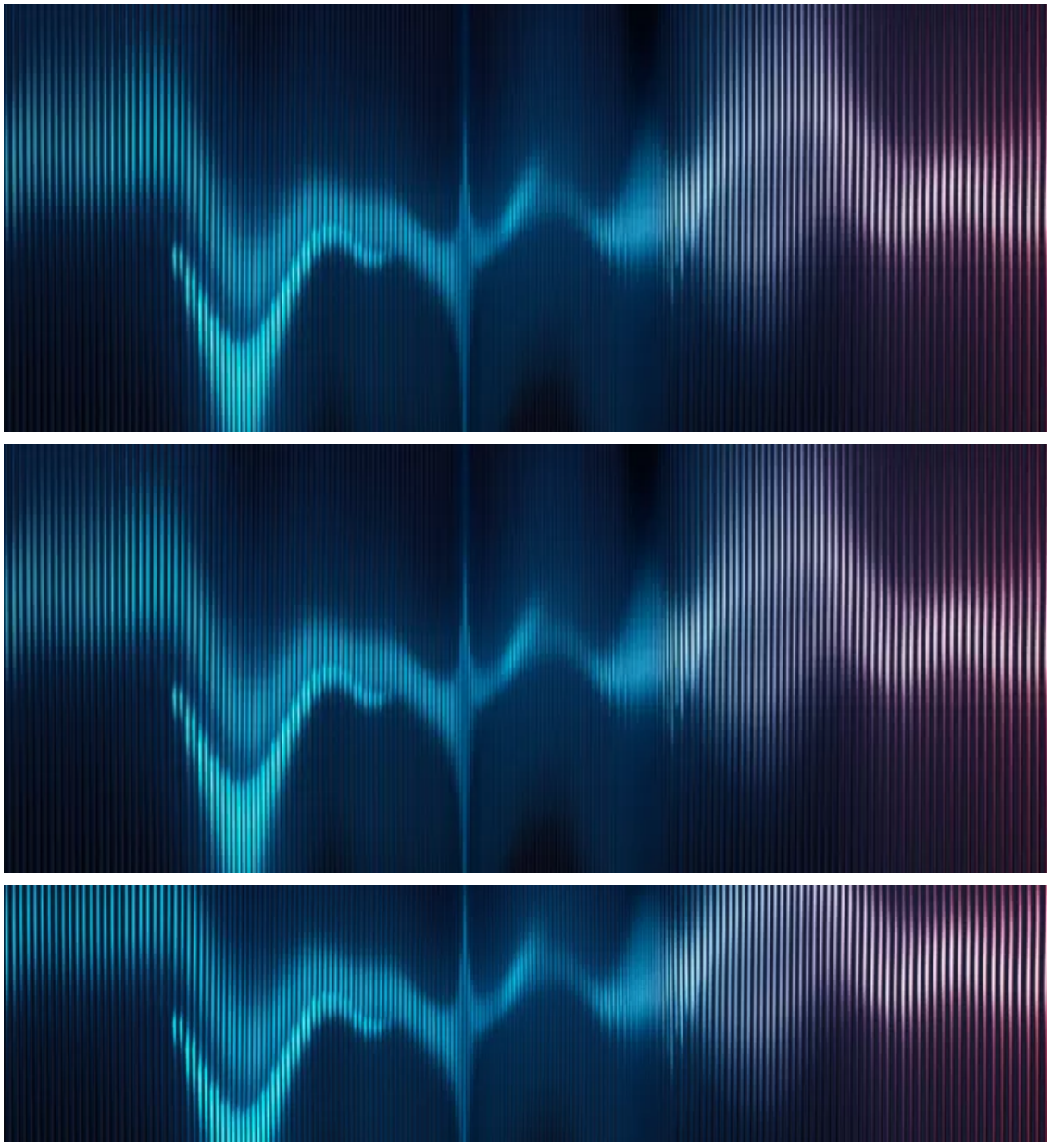
Research, News, and Perspectives

Archived: 2026-04-02 12:32:37 UTC



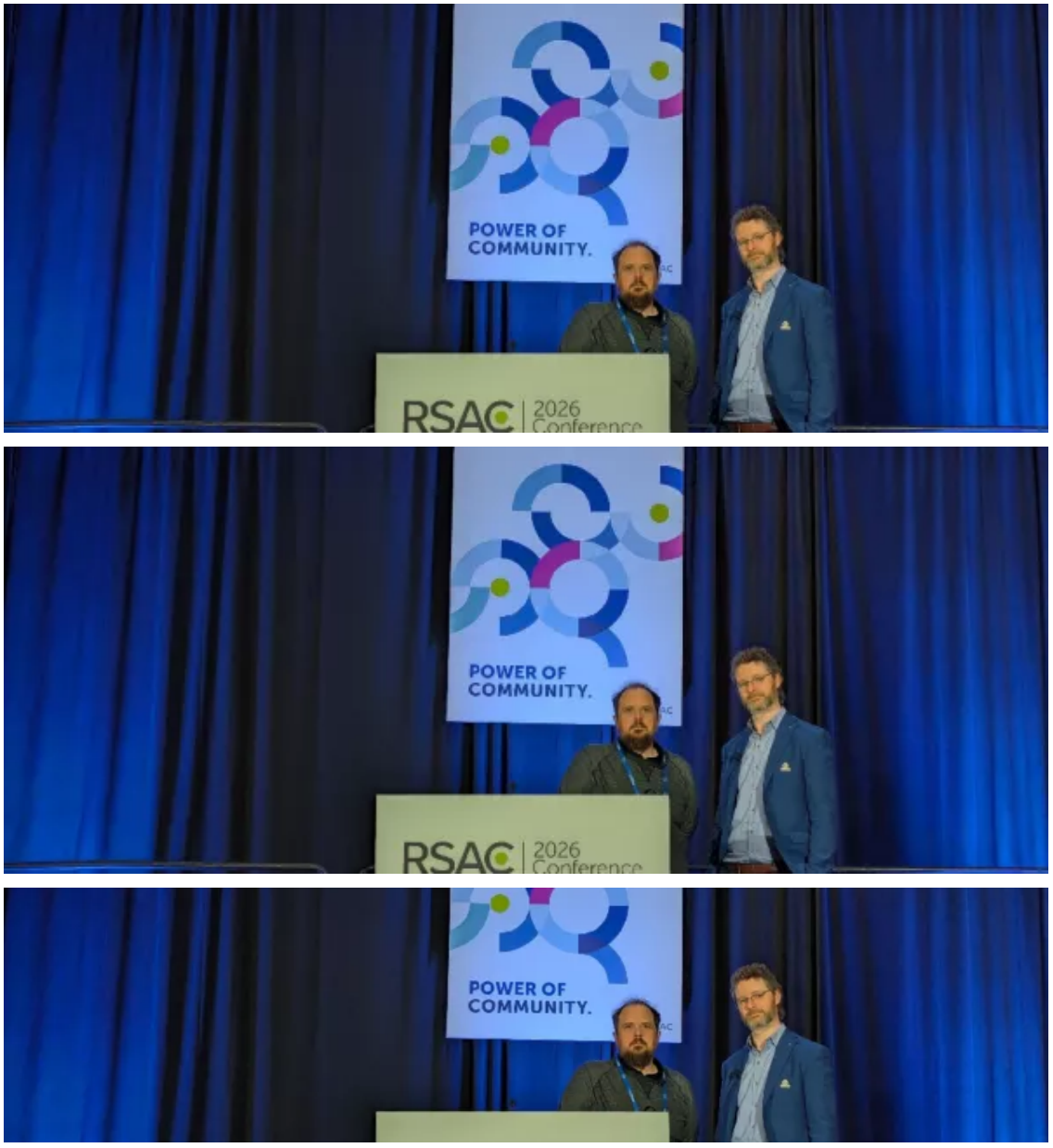
Artificial Intelligence (AI)

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

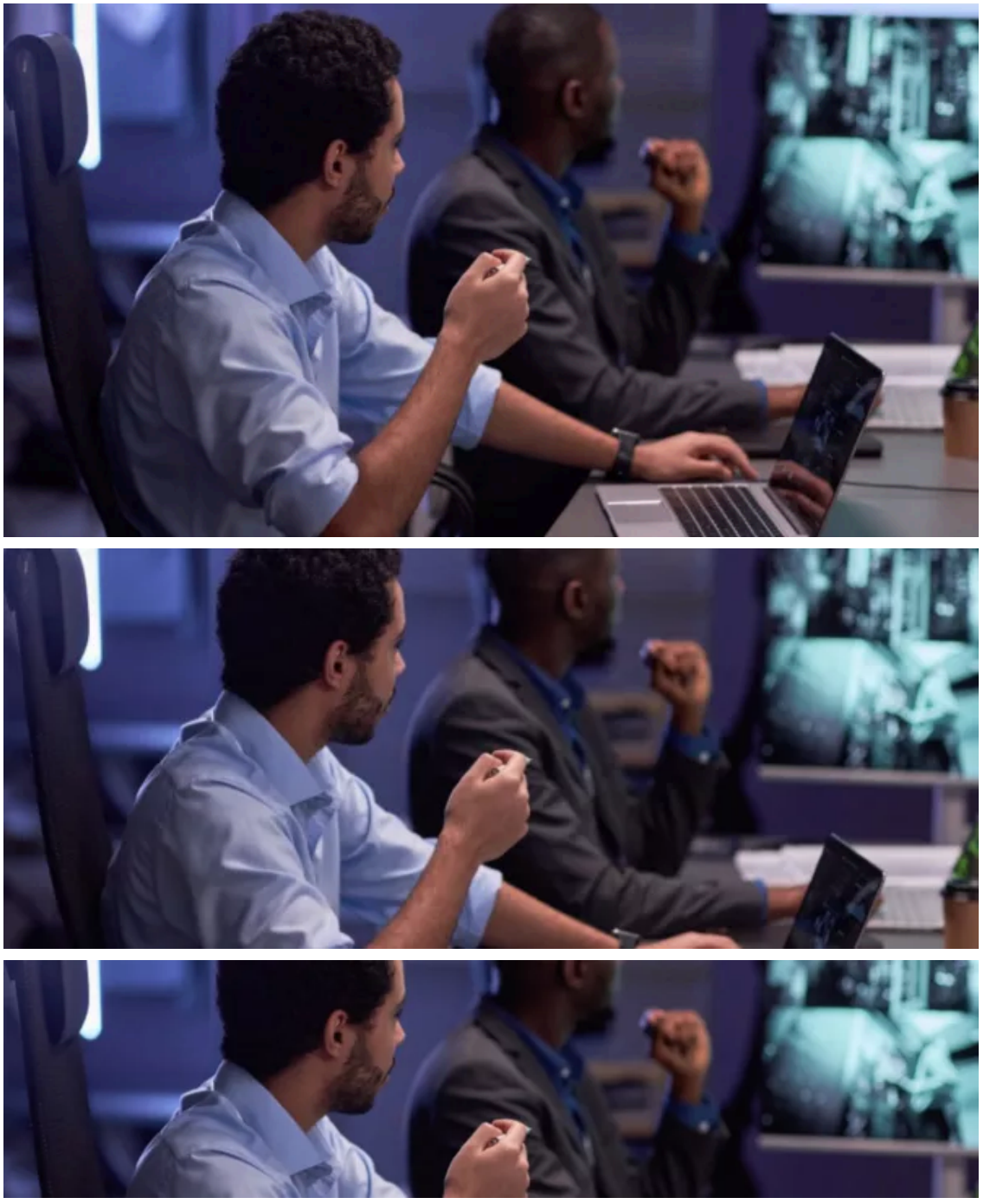
Expert Perspective Mar 31, 2026



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

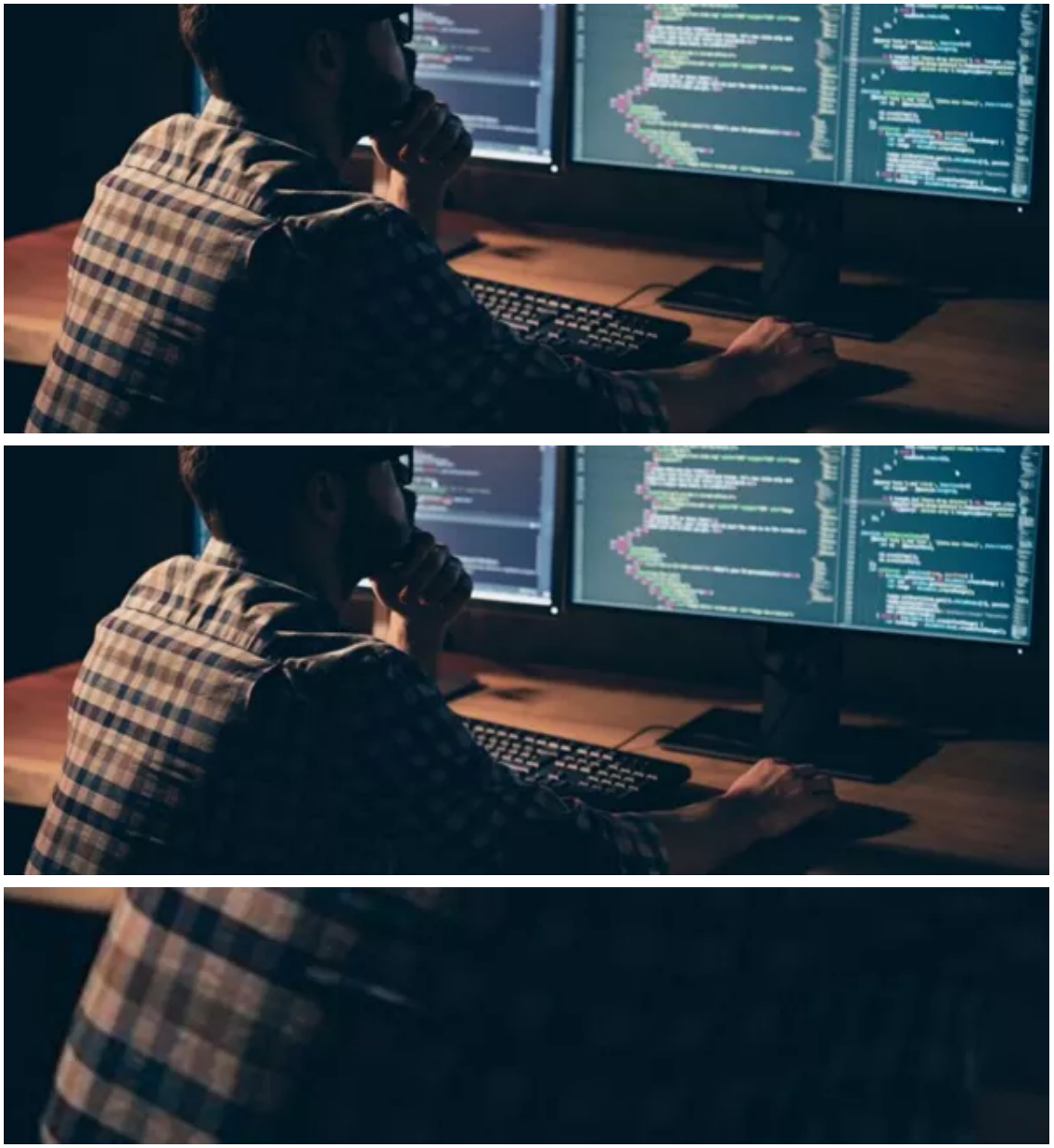
TeamPCP's Telnyx Attack Marks a Shift in Tactics Beyond LiteLLM

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.

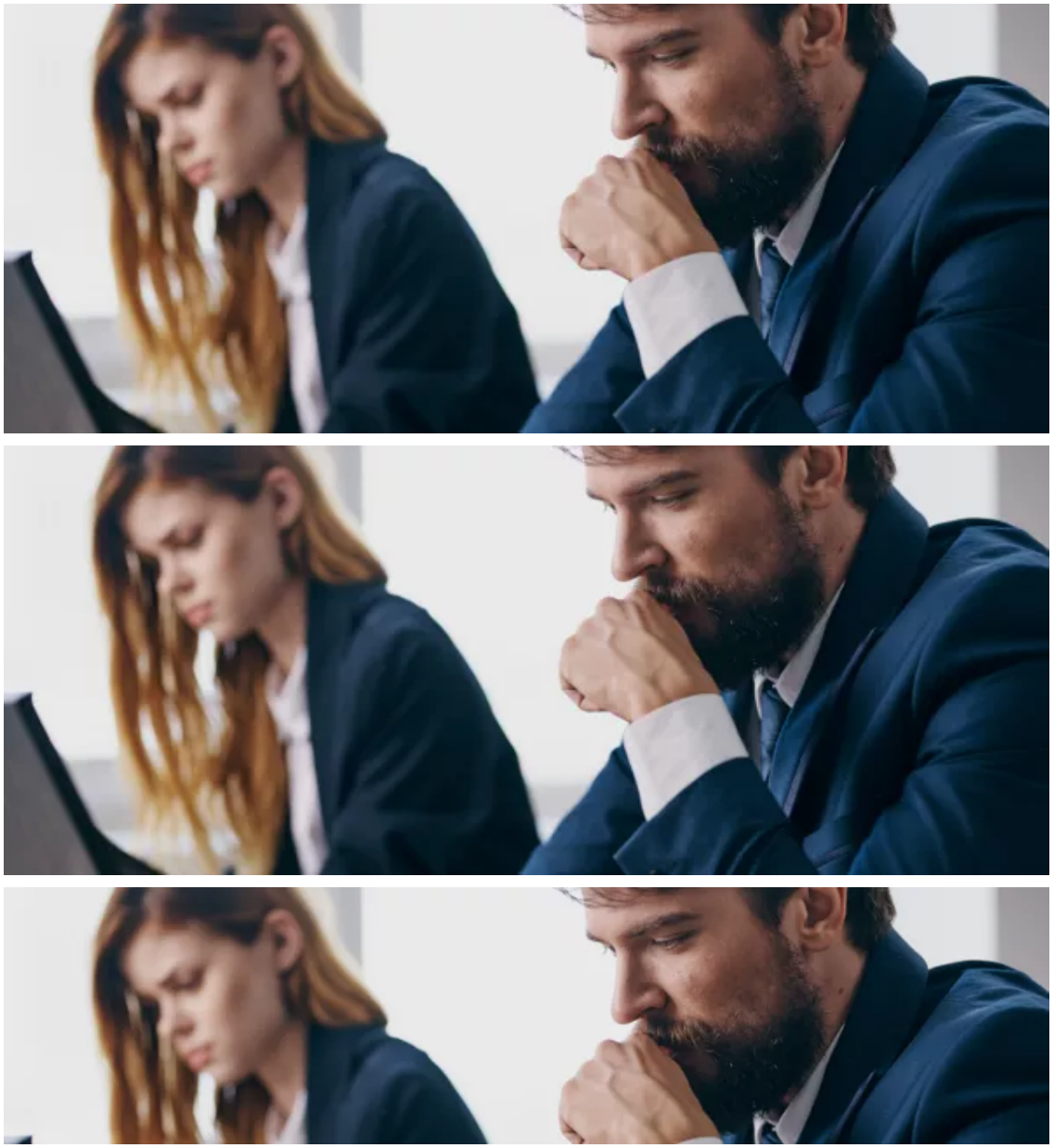
Artificial Intelligence (AI)

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.

Compliance & Risks

Why East-West Visibility Matters for Grid Security

Learn how east-west traffic visibility helps detect and stop lateral movement attacks inside electric grid infrastructure and critical OT networks.

Consumer Focus Mar 18, 2026

Consumer Focus Mar 18, 2026

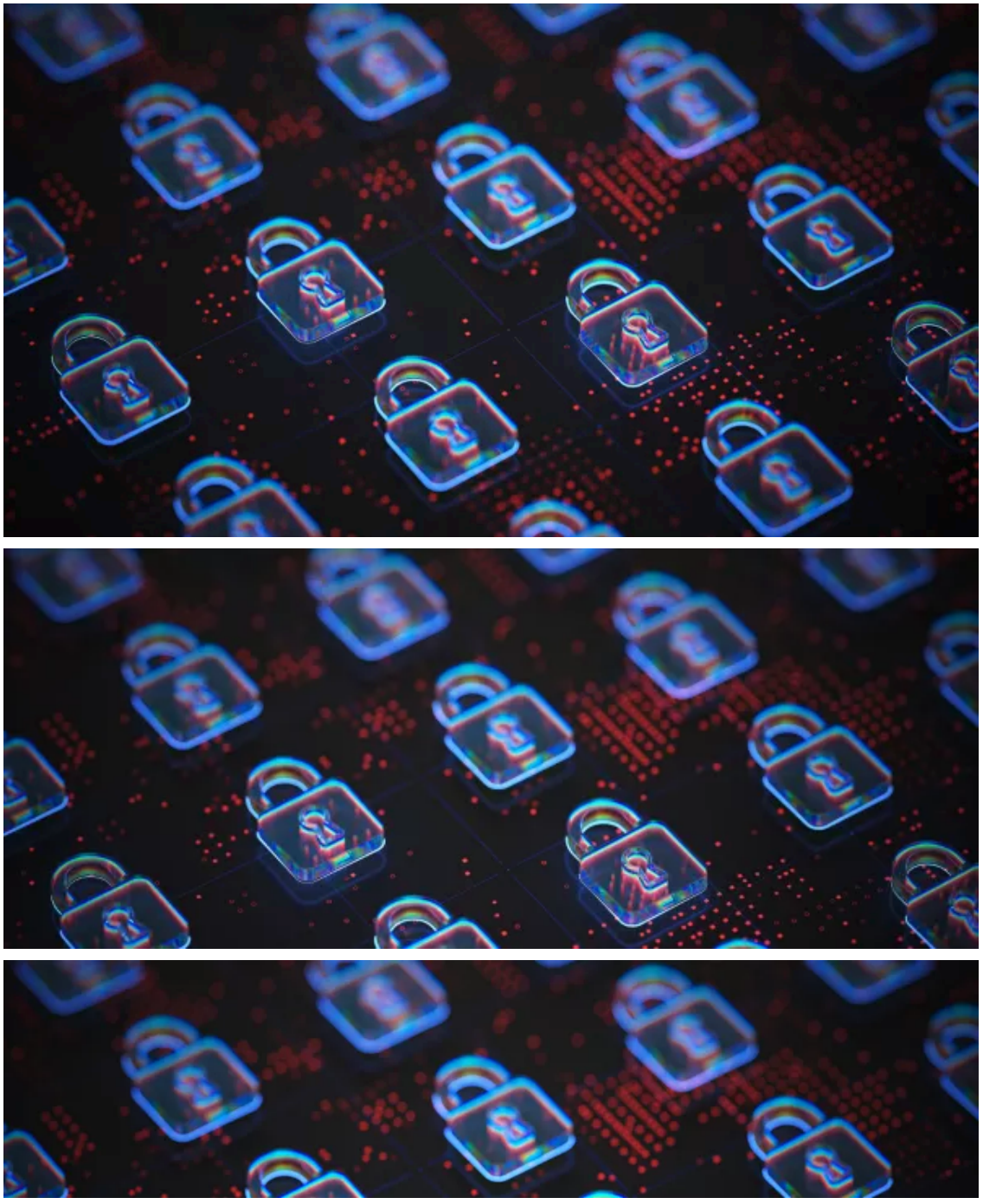
Cyber Threats

From Misconfigured Spring Boot Actuator to SharePoint Exfiltration: How Stolen Credentials Bypass MFA

Not every cloud breach starts with malware or a zero-day. In this incident, attackers discovered an exposed Spring Boot Actuator endpoint, harvested credentials from leaked configuration data, then used the OAuth2 Resource Owner Password Credentials (ROPC) flow to authenticate without MFA.

Investigations Mar 18, 2026

Investigations Mar 18, 2026



Cyber Crime

TrendAI™ Supports Global Law Enforcement Efforts

Learn how TrendAI™ and our researchers contributed threat intelligence and analysis to support INTERPOL against cybercrime.

No matches found
