Haftalık Siber Güvenlik Haber Özeti

Kapsam: Son 7 gün • Oluşturulma: 2026-01-07 20:06 UTC

Toplam haber: 42 • Kaynak sayısı: 5

The Hacker News: 25, BleepingComputer: 14, Cisco Talos Intelligence: 1, Krebs on Security: 1, PortSwigger Research: 1

BLEEPINGCOMPUTER

2026-01-07 15:05 UTC

1. Logitech Options+, G HUB macOS apps break after certificate expires

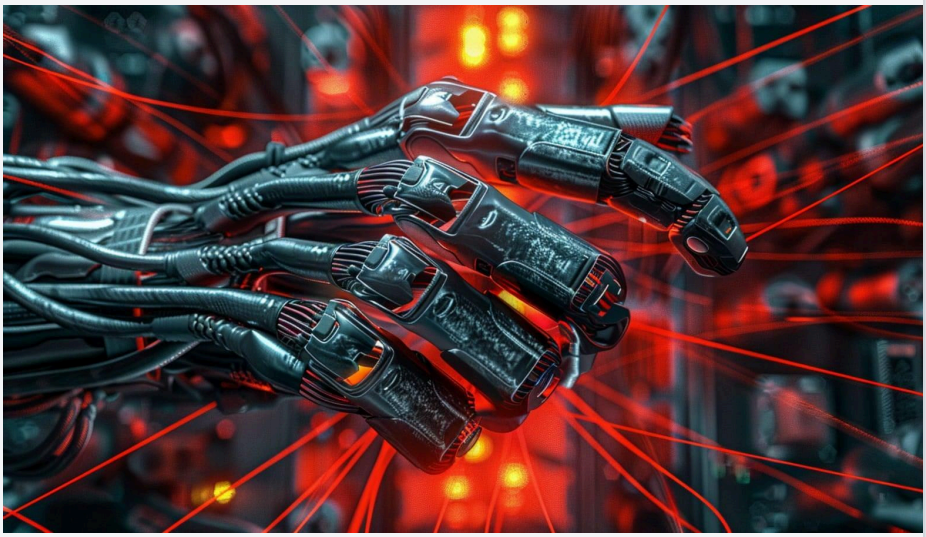
Logitech's Options+ and G Hub apps on macOS stopped working after their code-signing certificate expired, leaving users unable to launch them on Apple systems. [...]

Haberi aç

BLEEPINGCOMPUTER

2026-01-07 14:41 UTC

2. Max severity Ni8mare flaw lets hackers hijack n8n servers



A maximum severity vulnerability dubbed "Ni8mare" allows remote, unauthenticated attackers to take control over locally deployed instances of the N8N workflow automation platform. [...]

Haberi aç

THE HACKER NEWS

2026-01-07 14:19 UTC

3. Webinar: Learn How AI-Powered Zero Trust Detects Attacks with No Files or Indicators

Security teams are still catching malware. The problem is what they're not catching. More attacks today don't arrive as files. They don't drop binaries. They don't trigger classic alerts. Instead, they run quietly through tools that already exist inside the environment — scripts, remote access, browsers, and developer workflows. That shift is creating a blind spot. Join us for a deep-dive

Haberi aç

THE HACKER NEWS

2026-01-07 14:09 UTC

4. Black Cat Behind SEO Poisoning Malware Campaign Targeting Popular Software Searches

A cybercrime gang known as Black Cat has been attributed to a search engine optimization (SEO) poisoning campaign that employs fraudulent sites advertising popular software to trick users into downloading a backdoor capable of stealing sensitive data. According to a report published by the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) and

Haberi aç

BLEEPINGCOMPUTER

2026-01-07 13:30 UTC

5. Microsoft: Classic Outlook bug prevents opening encrypted emails

Microsoft has confirmed a known issue that prevents recipients from opening encrypted emails in classic Outlook. [...]

Haberi aç

BLEEPINGCOMPUTER

2026-01-07 12:00 UTC

6. In 2026, Hackers Want AI: Threat Intel on Vibe Hacking & HackGPT

Cybercriminals are increasingly using AI to lower the barrier to entry for fraud and hacking, shifting from skill-based to AI-assisted attacks known as "vibe hacking." Flare examines how underground forums promote AI tools, jailbreak techniques, and so-called "Hacking-GPT" services that promise ease rather than technical mastery. [...]

Haberi aç

BLEEPINGCOMPUTER

2026-01-07 11:34 UTC

7. ownCloud urges users to enable MFA after credential theft reports

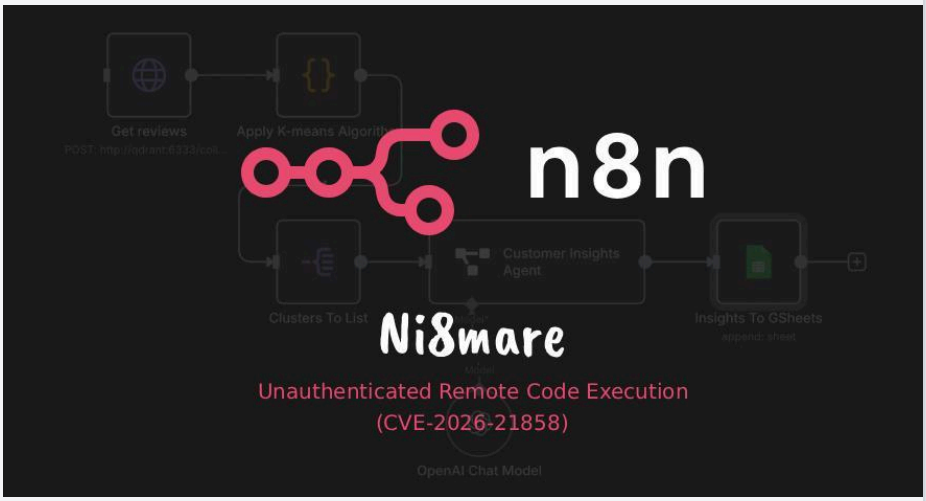
File-sharing platform ownCloud warned users today to enable multi-factor authentication (MFA) to block attackers using compromised credentials from stealing their data. [...]

Haberi aç

THE HACKER NEWS

2026-01-07 10:48 UTC

8. Critical n8n Vulnerability (CVSS 10.0) Allows Unauthenticated Attackers to Take Full Control



Cybersecurity researchers have disclosed details of yet another maximum-severity security flaw in n8n, a popular workflow automation platform, that allows an unauthenticated remote attacker to gain complete control over susceptible instances. The vulnerability, tracked as CVE-2026-21858 (CVSS score: 10.0), has been codenamed Ni8mare by Cyera Research Labs. Security researcher Dor Attias has been

Haberi aç

BLEEPINGCOMPUTER

2026-01-07 10:06 UTC

9. New Veeam vulnerabilities expose backup servers to RCE attacks

Veeam released security updates to patch multiple security flaws in its Backup & Replication software, including a critical remote code execution (RCE) vulnerability. [...]

Haberi aç

BLEEPINGCOMPUTER

2026-01-07 09:50 UTC

10. Google Search AI hallucinations push Google to hire "AI Answers Quality" engineers

AI, including AI Overviews on Google Search, can hallucinate and often make up stuff or offer contradicting answers when asked in two different ways. [...]

Haberi aç

BLEEPINGCOMPUTER

2026-01-07 09:15 UTC

11. UK announces plan to strengthen public sector cyber defenses

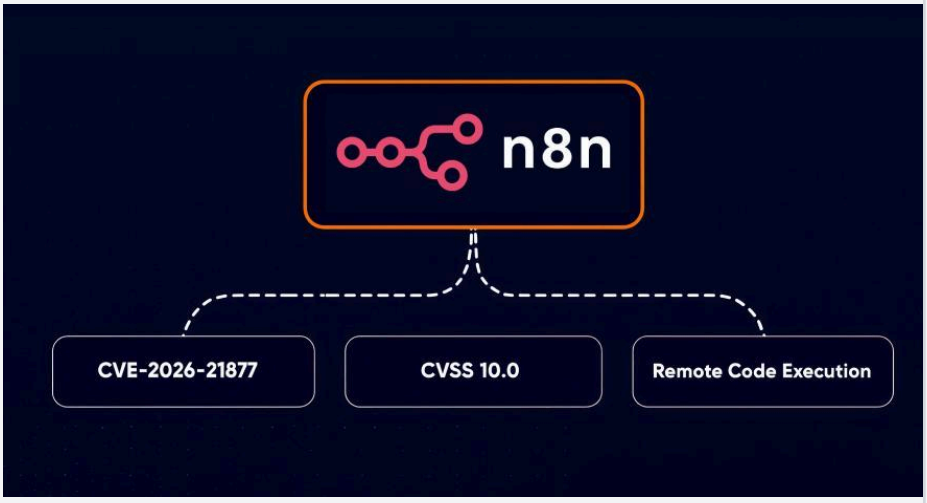
The United Kingdom has announced a new cybersecurity strategy, backed by more than £210 million ($283 million), to boost cyber defenses across government departments and the wider public sector. [...]

Haberi aç

THE HACKER NEWS

2026-01-07 08:26 UTC

12. n8n Warns of CVSS 10.0 RCE Vulnerability Affecting Self-Hosted and Cloud Versions



Open-source workflow automation platform n8n has warned of a maximum-severity security flaw that, if successfully exploited, could result in authenticated remote code execution (RCE). The vulnerability, which has been assigned the CVE identifier CVE-2026-21877, is rated 10.0 on the CVSS scoring system. "Under certain conditions, an authenticated user may be able to cause untrusted code to be

Haberi aç

CISCO TALOS INTELLIGENCE

2026-01-07 08:00 UTC

13. How Cisco Talos powers the solutions protecting your organization

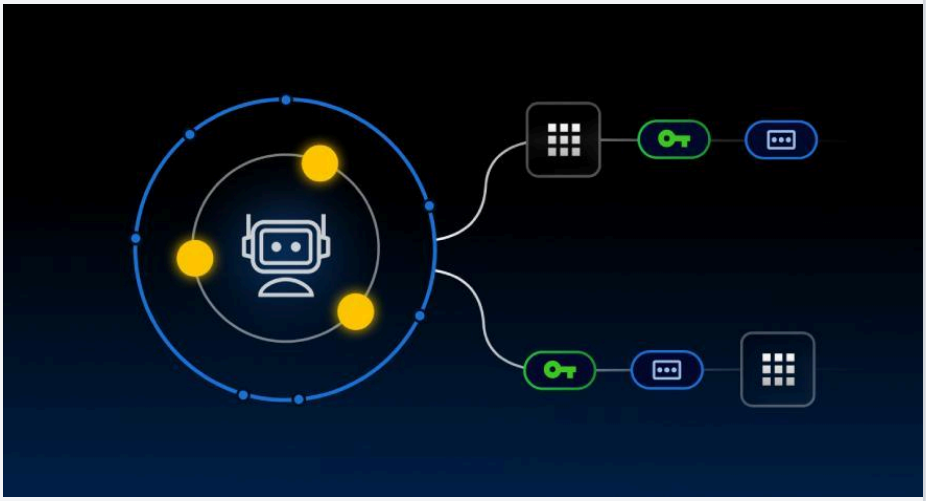
What happens under the hood of Cisco's security portfolio? Our reputation and detection services apply Talos' real-time intelligence to detect and block threats. Here's how.

Haberi aç

THE HACKER NEWS

2026-01-07 08:00 UTC

14. The Future of Cybersecurity Includes Non-Human Employees



Non-human employees are becoming the future of cybersecurity, and enterprises need to prepare accordingly. As organizations scale Artificial Intelligence (AI) and cloud automation, there is exponential growth in Non-Human Identities (NHIs), including bots, AI agents, service accounts and

automation scripts. In fact, 51% of respondents in ConductorOne’s 2025 Future of Identity Security Report

Haberi aç

THE HACKER NEWS

2026-01-07 07:41 UTC

15. Veeam Patches Critical RCE Vulnerability with CVSS 9.0 in Backup & Replication

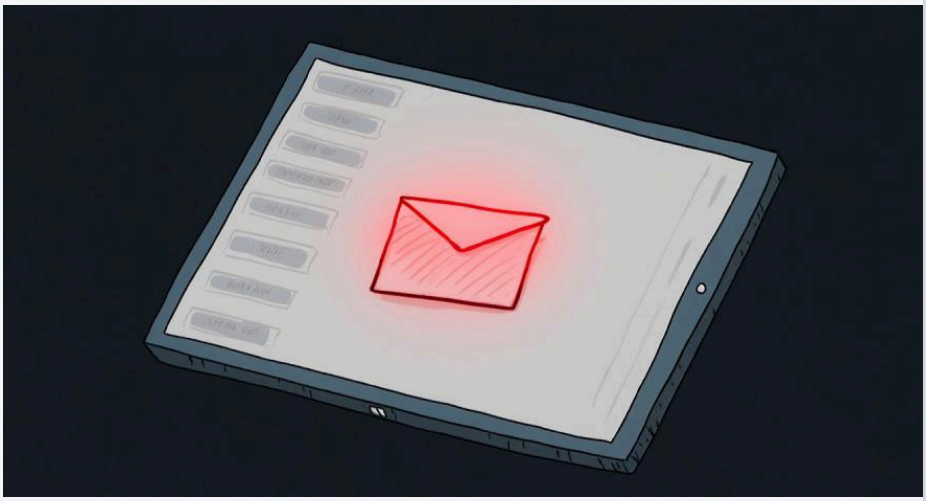
Veeam has released security updates to address multiple flaws in its Backup & Replication software, including a "critical" issue that could result in remote code execution (RCE). The vulnerability, tracked as CVE-2025-59470, carries a CVSS score of 9.0. "This vulnerability allows a Backup or Tape Operator to perform remote code execution (RCE) as the postgres user by sending a malicious

Haberi aç

THE HACKER NEWS

2026-01-07 06:42 UTC

16. Microsoft Warns Misconfigured Email Routing Can Enable Internal Domain Phishing



Threat actors engaging in phishing attacks are exploiting routing scenarios and misconfigured spoof protections to impersonate organizations' domains and distribute emails that appear as if they have been sent internally. "Threat actors have leveraged this vector to deliver a wide variety of phishing messages related to various phishing-as-a-service (PhaaS) platforms such as Tycoon 2FA," the

Haberi aç

THE HACKER NEWS

2026-01-07 01:31 UTC

17. Ongoing Attacks Exploiting Critical RCE Vulnerability in Legacy D-Link DSL Routers

A newly discovered critical security flaw in legacy D-Link DSL gateway routers has come under active exploitation in the wild. The vulnerability, tracked as CVE-2026-0625 (CVSS score: 9.3), concerns a case of command injection in the "dnscfg.cgi" endpoint that arises as a result of improper sanitization of user-supplied DNS configuration parameters. "An unauthenticated remote attacker can inject

Haberi aç

BLEEPINGCOMPUTER

2026-01-06 22:30 UTC

18. OpenAI is reportedly getting ready to test ads in ChatGPT

Multiple reports suggest that OpenAI is going ahead with its plans to add ads to ChatGPT, but the experiment will be initially limited to its employees. [...]

Haberi aç

BLEEPINGCOMPUTER

2026-01-06 21:30 UTC

19. OpenAI is rolling out GPT-5.2 “Codex-Max” for some users

OpenAI is testing a new model for Codex called "GPT-5.2-Codex-Max," and it's already rolling out to users with a subscription. [...]

Haberi aç

BLEEPINGCOMPUTER

2026-01-06 19:27 UTC

20. Taiwan says China's attacks on its energy sector increased tenfold

The National Security Bureau in Taiwan says that China's attacks on the country's energy sector increased tenfold in 2025 compared to the previous year. [...]

Haberi aç

BLEEPINGCOMPUTER

2026-01-06 17:49 UTC

21. Microsoft cancels plans to rate limit Exchange Online bulk emails

Microsoft announced today that it has canceled plans to impose a daily limit of 2,000 external recipients on Exchange Online bulk email senders. [...]

Haberi aç

BLEEPINGCOMPUTER

2026-01-06 16:52 UTC

22. New D-Link flaw in legacy DSL routers actively exploited in attacks

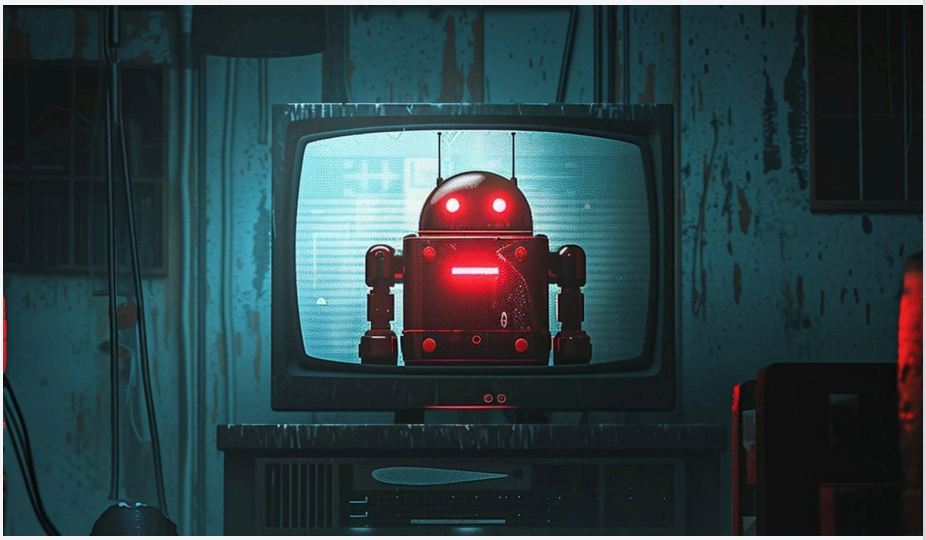
Threat actors are exploiting a recently discovered command injection vulnerability that affects multiple D-Link DSL gateway routers that went out of support years ago. [...]

Haberi aç

BLEEPINGCOMPUTER

2026-01-06 16:15 UTC

23. Kimwolf Android botnet abuses residential proxies to infect internal devices



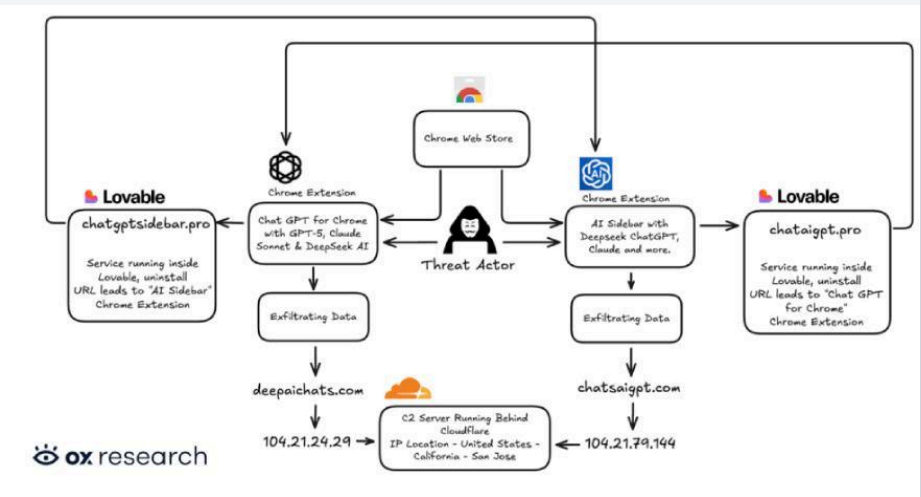
The Kimwolf botnet, an Android variant of the Aisuru malware, has grown to more than two million hosts, most of them infected by exploiting vulnerabilities in residential proxy networks to target devices on internal networks. [...]

Haberi aç

THE HACKER NEWS

2026-01-06 14:21 UTC

24. Two Chrome Extensions Caught Stealing ChatGPT and DeepSeek Chats from 900,000 Users



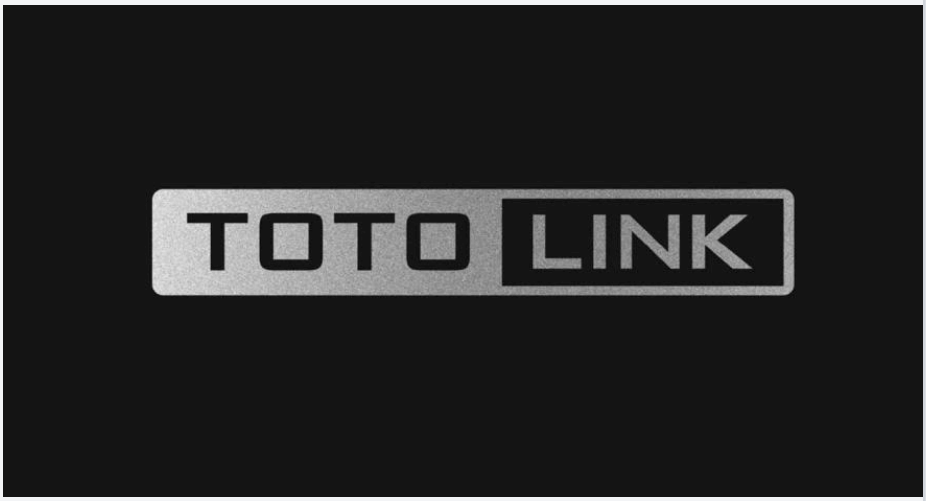
Cybersecurity researchers have discovered two new malicious extensions on the Chrome Web Store that are designed to exfiltrate OpenAI ChatGPT and DeepSeek conversations alongside browsing data to servers under the attackers' control. The names of the extensions, which collectively have over 900,000 users, are below - Chat GPT for Chrome with GPT-5, Claude Sonnet & DeepSeek AI (ID:

Haberi aç

THE HACKER NEWS

2026-01-06 12:47 UTC

25. Unpatched Firmware Flaw Exposes TOTOLINK EX200 to Full Remote Device Takeover



The CERT Coordination Center (CERT/CC) has disclosed details of an unpatched security flaw impacting TOTOLINK EX200 wireless range extender that could allow a remote authenticated attacker to gain full control of the device. The flaw, CVE-2025-65606 (CVSS score: N/A), has been characterized as a flaw in the firmware-upload error-handling logic, which could cause the device to inadvertently start

Haberi aç

PORTSWIGGER RESEARCH

2026-01-06 12:31 UTC

26. Top 10 web hacking techniques of 2025: call for nominations

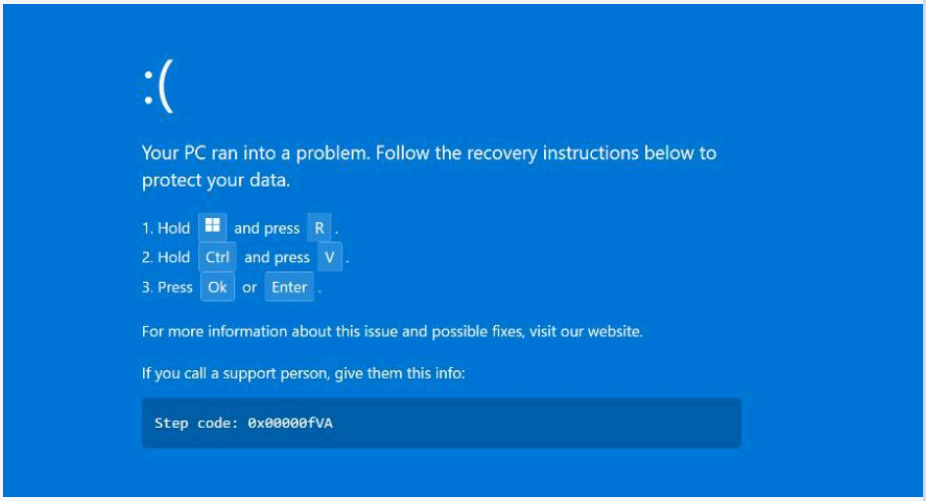
Over the last year, security researchers have shared a huge amount of work with the community through blog posts, presentations, and whitepapers. This is great, but it also means genuinely reusable te

Haberi aç

THE HACKER NEWS

2026-01-06 09:13 UTC

27. Fake Booking Emails Redirect Hotel Staff to Fake BSoD Pages Delivering DCRat



Source: Securonix Cybersecurity researchers have disclosed details of a new campaign dubbed PHALT#BLYX that has leveraged ClickFix-style lures to display fixes for fake blue screen of death (BSoD) errors in attacks targeting the European hospitality sector. The end goal of the multi-stage campaign is to deliver a remote access trojan known as DCRat, according to cybersecurity company Securonix.

Haberi aç

THE HACKER NEWS

2026-01-06 08:30 UTC

28. What is Identity Dark Matter?

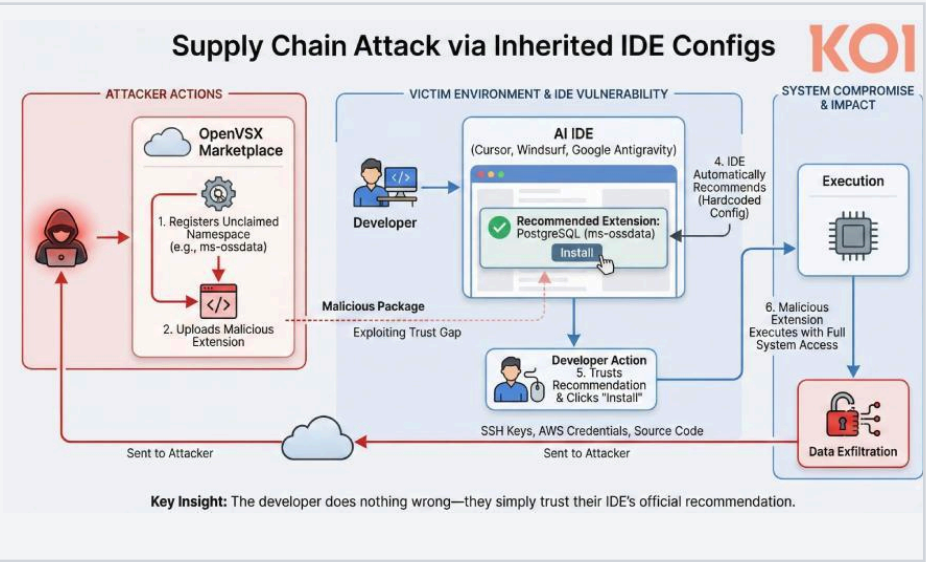
The Invisible Half of the Identity Universe Identity used to live in one place - an LDAP directory, an HR system, a single IAM portal. Not anymore. Today, identity is fragmented across SaaS, on-prem, IaaS, PaaS, home-grown, and shadow applications. Each of these environments carries its own accounts, permissions, and authentication flows. Traditional IAM and IGA tools govern only the nearly

Haberi aç

THE HACKER NEWS

2026-01-06 08:25 UTC

29. VS Code Forks Recommend Missing Extensions, Creating Supply Chain Risk in Open VSX



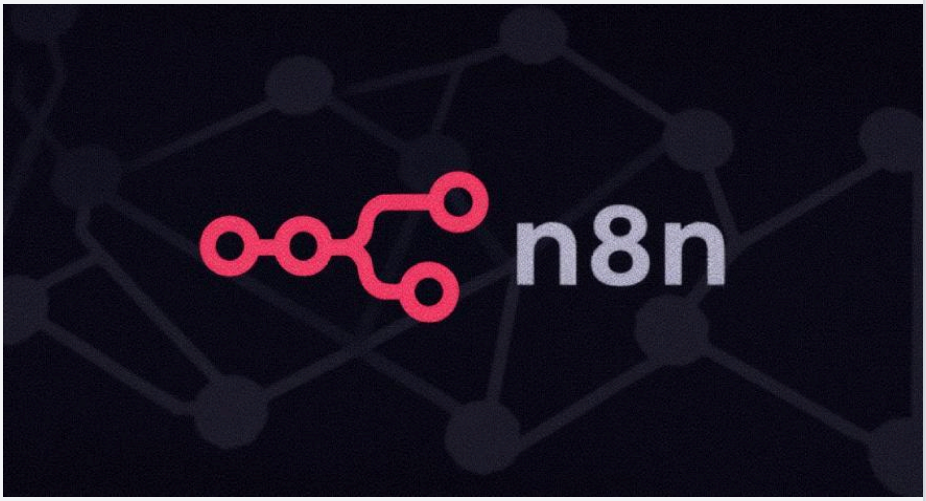
Popular artificial intelligence (AI)-powered Microsoft Visual Studio Code (VS Code) forks such as Cursor, Windsurf, Google Antigravity, and Trae have been found to recommend extensions that are non-existent in the Open VSX registry, potentially opening the door to supply chain risks when bad actors publish malicious packages under those names. The problem, according to Koi, is that these

Haberi aç

THE HACKER NEWS

2026-01-06 02:08 UTC

30. New n8n Vulnerability (9.9 CVSS) Lets Authenticated Users Execute System Commands



A new critical security vulnerability has been disclosed in n8n, an open-source workflow automation platform, that could enable an authenticated attacker to execute arbitrary system commands on the underlying host. The vulnerability, tracked as CVE-2025-68668, is rated 9.9 on the CVSS scoring system. It has been described as a case of a protection mechanism failure. Cyera Research Labs' Vladimir

Haberi aç

THE HACKER NEWS

2026-01-06 00:30 UTC

31. Critical AdonisJS Bodyparser Flaw (CVSS 9.2) Enables Arbitrary File Write on Servers

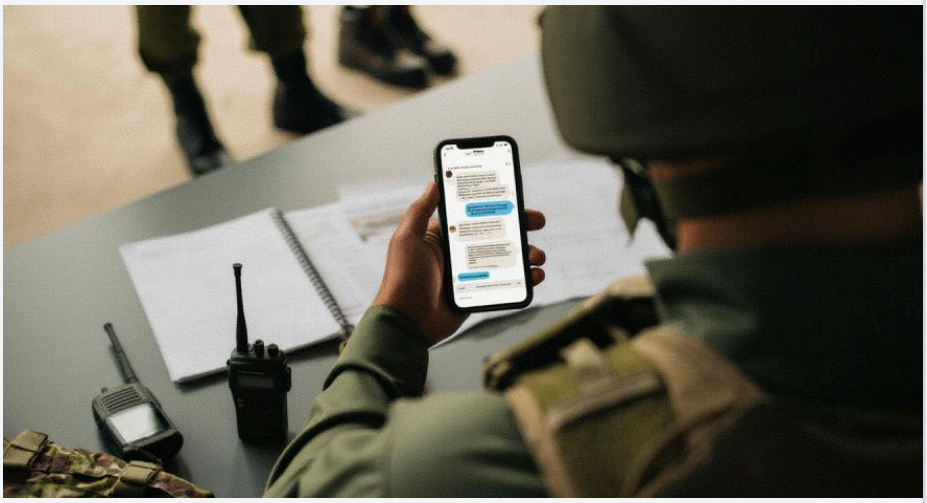
Users of the "@adonisjs/bodyparser" npm package are being advised to update to the latest version following the disclosure of a critical security vulnerability that, if successfully exploited, could allow a remote attacker to write arbitrary files on the server. Tracked as CVE-2026-21440 (CVSS score: 9.2), the flaw has been described as a path traversal issue affecting the AdonisJS multipart

Haberi aç

THE HACKER NEWS

2026-01-05 14:56 UTC

32. Russia-Aligned Hackers Abuse Viber to Target Ukrainian Military and Government



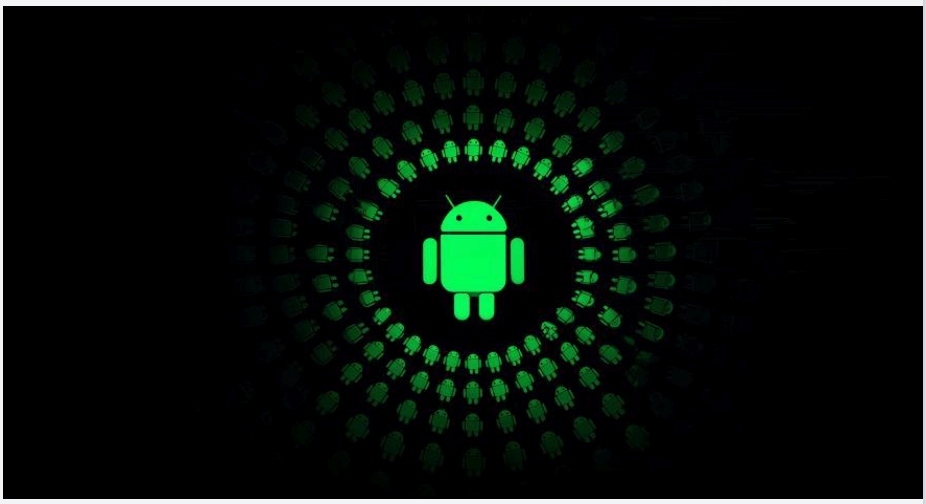
The Russia-aligned threat actor known as UAC-0184 has been observed targeting Ukrainian military and government entities by leveraging the Viber messaging platform to deliver malicious ZIP archives. "This organization has continued to conduct high-intensity intelligence gathering activities against Ukrainian military and government departments in 2025," the 360 Threat Intelligence Center said in

Haberi aç

THE HACKER NEWS

2026-01-05 13:41 UTC

33. Kimwolf Android Botnet Infects Over 2 Million Devices via Exposed ADB and Proxy Networks



The botnet known as Kimwolf has infected more than 2 million Android devices by tunneling through residential proxy networks, according to findings from Synthient. "Key actors involved in the Kimwolf botnet are observed monetizing the botnet through app installs, selling residential proxy bandwidth, and selling its DDoS functionality," the company said in an analysis published last week. Kimwolf

Haberi aç

THE HACKER NEWS

2026-01-05 09:53 UTC

34. ⚡ Weekly Recap: IoT Exploits, Wallet Breaches, Rogue Extensions, AI Abuse & More

The year opened without a reset. The same pressure carried over, and in some places it tightened. Systems people assume are boring or stable are showing up in the wrong places. Attacks moved quietly, reused familiar paths, and kept working longer than anyone wants to admit. This week's stories share one pattern. Nothing flashy. No single moment. Just steady abuse of trust — updates, extensions,

Haberi aç

THE HACKER NEWS

2026-01-05 08:55 UTC

35. The State of Cybersecurity in 2025: Key Segments, Insights, and Innovations

Featuring: Cybersecurity is being reshaped by forces that extend beyond individual threats or tools. As organizations operate across cloud infrastructure, distributed endpoints, and complex supply chains, security has shifted from a collection of point solutions to a question of architecture, trust, and execution speed. This report examines how core areas of cybersecurity are evolving in

Haberi aç

THE HACKER NEWS

2026-01-05 06:42 UTC

36. Bitfinex Hack Convict Ilya Lichtenstein Released Early Under U.S. First Step Act

Ilya Lichtenstein, who was sentenced to prison last year for money laundering charges in connection with his role in the massive hack of cryptocurrency exchange Bitfinex in 2016, said he has been released early. In a post shared on X last week, the 38-year-old announced his release, crediting U.S. President Donald Trump's First Step Act. According to the Federal Bureau of Prisons' inmate locator

Haberi aç

THE HACKER NEWS

2026-01-05 04:48 UTC

37. New VVS Stealer Malware Targets Discord Accounts via Obfuscated Python Code

Cybersecurity researchers have disclosed details of a new Python-based information stealer called VVS Stealer (also styled as VVS $tealer) that's capable of harvesting Discord credentials and tokens. The stealer is said to have been on sale on Telegram as far back as April 2025, according to a report from Palo Alto Networks Unit 42. "VVS stealer's code is obfuscated by Pyarmor," researchers

Haberi aç

KREBS ON SECURITY

2026-01-02 11:20 UTC

38. The Kimwolf Botnet is Stalking Your Local Network

The story you are reading is a series of scoops nestled inside a far more urgent Internet-wide security advisory. The vulnerability at issue has been exploited for months already, and it's time for a broader awareness of the threat. The short version is that everything you thought you knew about the security of the internal network behind your Internet router probably is now dangerously out of date.

Haberi aç

THE HACKER NEWS

2026-01-02 10:52 UTC

39. Transparent Tribe Launches New RAT Attacks Against Indian Government and Academia

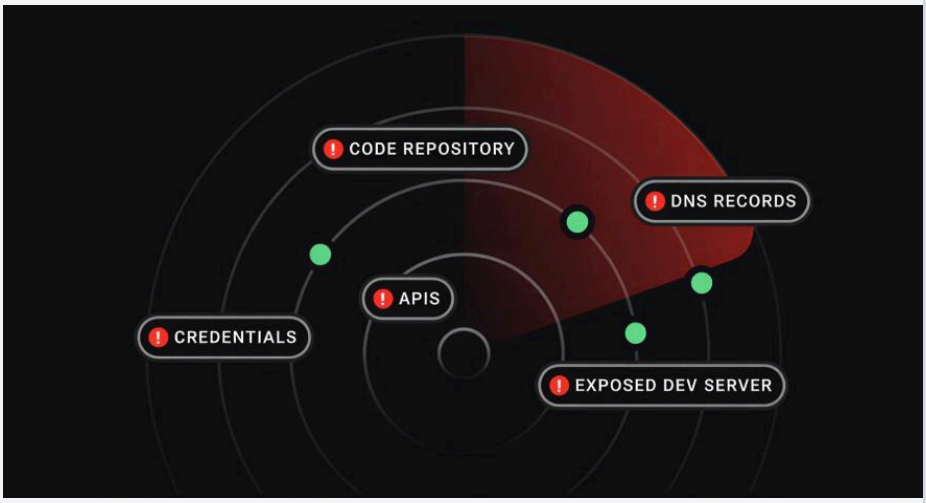
The threat actor known as Transparent Tribe has been attributed to a fresh set of attacks targeting Indian governmental, academic, and strategic entities with a remote access trojan (RAT) that grants them persistent control over compromised hosts. "The campaign employs deceptive delivery techniques, including a weaponized Windows shortcut (LNK) file masquerading as a legitimate PDF document

Haberi aç

THE HACKER NEWS

2026-01-02 08:30 UTC

40. The ROI Problem in Attack Surface Management



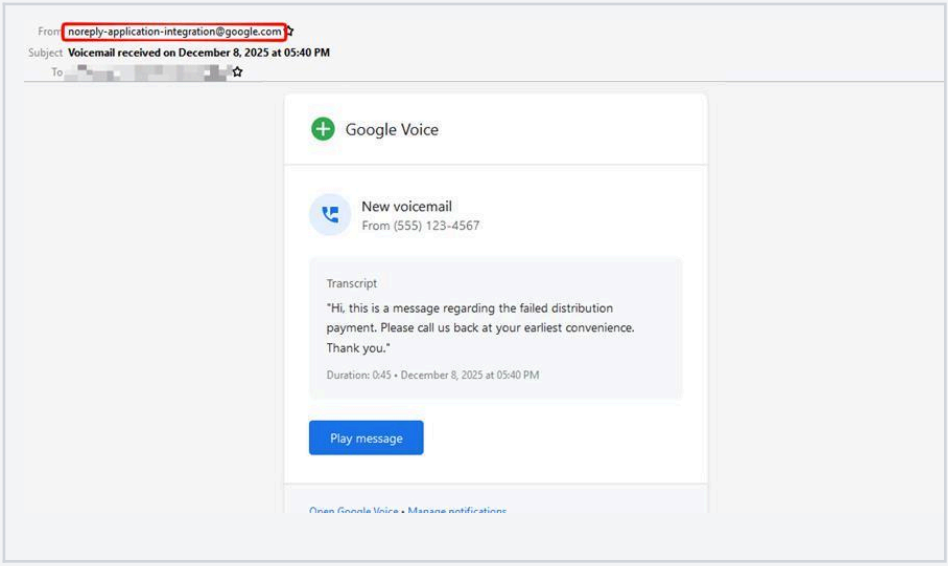
Attack Surface Management (ASM) tools promise reduced risk. What they usually deliver is more information. Security teams deploy ASM, asset inventories grow, alerts start flowing, and dashboards fill up. There is visible activity and measurable output. But when leadership asks a simple question, “Is this reducing incidents?” the answer is often unclear. This gap between effort and

Haberi aç

THE HACKER NEWS

2026-01-02 06:14 UTC

41. Cybercriminals Abuse Google Cloud Email Feature in Multi-Stage Phishing Campaign



Cybersecurity researchers have disclosed details of a phishing campaign that involves the attackers impersonating legitimate Google-generated messages by abusing Google Cloud's Application Integration service to distribute emails. The activity, Check Point said, takes advantage of the trust associated with Google Cloud infrastructure to send the messages from a legitimate email address ("

Haberi aç

THE HACKER NEWS

2026-01-01 12:52 UTC

42. ThreatsDay Bulletin: GhostAd Drain, macOS Attacks, Proxy Botnets, Cloud Exploits, and 12+ Stories

The first ThreatsDay Bulletin of 2026 lands on a day that already feels symbolic — new year, new breaches, new tricks. If the past twelve months taught defenders anything, it’s that threat actors don’t pause for holidays or resolutions. They just evolve faster. This week’s round-up shows how subtle shifts in behavior, from code tweaks to job scams, are rewriting what “cybercrime” looks like in

Haberi aç