Pagina 10 - Weekly Recap: iPhone Spyware, Microsoft 0-Day, TokenBreak Hack, AI Data Leaks and More

Classificações de Malware:

- spyware (Spyware)
- cve (Exploit)
- ads (Adware)
- backdoor (Backdoor)
- rat (Backdoor)
- virus (Virus)
- infection (Virus)
- trojan (Trojan)
- dropper (Trojan)
- exploit (Exploit)
- adware (Adware)

Some of the biggest security problems start quietly. No alerts. No warnings. Just small actions that seem normal but aren't. Attackers now know how to stay hidden by blending in, and that makes it hard to tell when something's wrong.This week's stories aren't just about what was attackedbut how easily it happened. If we're only looking for the obvious signs, what are we missing right in front of us?Here's a look at the tactics and mistakes that show how much can go unnoticed.Apple Zero-Click Flaw in Messages Exploited to Deliver Paragon Spyware Apple disclosed that a security flaw in its Messages app was actively exploited in the wild to target civil society members in sophisticated cyber attacks. The vulnerability, CVE-2025-43200, was addressed by the company in February as part of iOS 18.3.1, iPadOS 18.3.1, iPadOS 17.7.5, macOS Sequoia 15.3.1, macOS Sonoma 14.7.4, macOS Ventura 13.7.4, watchOS 11.3.1, and visionOS 2.3.1. The Citizen Lab said it uncovered forensic evidence that the flaw was weaponized to target Italian journalist Ciro Pellegrino and an unnamed prominent European journalist and infect them with Paragon's Graphite mercenary spyware.Sensitive data moves fast in the cloud. If y ou can't see it, you can't protect it. This guide shows how top teams use DSPM to reduce risk, improve compliance, and boost efficiencybacked by real metrics that drive measurable impact.Attackers love software vulnerabilities they're easy doors into your systems. Every week brings fresh flaws, and waiting too long to patch can turn a minor oversight into a major breach. Below are this week's critical vulnerabilities you need to know about. Take a look, update your software promptly, and keep attackers locked out.This week's list includes CVE-2025-43200(Apple),CVE-2025-32711(Microsoft 365 Copilot),CVE-2025-33053(Microsoft Windows),CVE-2025-47110(Adobe Commerce and Magento Open Source),CVE-2025-43697, CVE-2025-43698, CVE-2025-43699, CVE-2025-43700, CVE-2025-43701(Salesforce),CVE-2025-24016(Wazuh),CVE-2025-5484, CVE-2025-5485(SinoTrack),CVE-2025-31022(PayU CommercePro plugin),CVE-2025-3835(ManageEngine Exchange Reporter Plus),CVE-2025-42989(SAP NetWeaver),CVE-2025-5353,CVE-2025-22463,CVE-2025-22455(Ivanti Workspace Control),CVE-2025-5958(Google Chrome),CVE-2025-3052(DT Research DTBios and BiosFlashShell),CVE-2025-2884(TCG TPM2.0 reference implementation),CVE-2025-26521(Apache CloudStack),CVE-2025-47950(CoreDNS),CVE-2025-4230,CVE-2025-4232(Palo Alto Networks PAN-OS),CVE-2025-4278, CVE-2025-2254, CVE-2025-5121, CVE-2025-0673(GitLab),CVE-2025-47934(OpenPGP.js),CVE-2025-49219,CVE-2025-49220(Trend Micro Apex Central),CVE-2025-49212,CVE-2025-49213,CVE-2025-49216,CVE-2025-49217(Trend Micro Endpoint Encryption PolicyServer), CVE-2025-4922(HashiCorp Nomad),CVE-2025-36631,CVE-2025-36632,CVE-2025-36633(Tenable Nessus Agent),CVE-2025-33108(IBM Backup, Recovery, and Media Services),CVE-2025-6029(KIA-branded Aftermarket Generic Smart Keyless Entry System), and apatch bypass for CVE-2024-41713(Mitel MiCollab).Disclaimer: These newly released tools are for educational use only and haven't been fully audited. Use at your own riskreview the code, test safely, and app ly proper safeguards.4 Hidden Ways You're Tracked (and How to Fight Back) Most people know about cookies and ads, but companies now use sneaky technical tricks to track youeven if you're using a VPN, private mode, or a hardened browser. One method gaining attention islocalhost tracking: apps like Facebook and Instagram silently run a web server inside your phone. When you visit a website with a hidden code, it can ping this server to see if the app is installedleaking your activity back to the app, without your permission.Another trick isport probing. Some websites scan your device to check if developer tools or apps are running on certain ports (like 3000 or 9222). This reveals what software you use or whether you're running a specific company's toolleaking clues about your job, device, or activity. Sites may even detect browser extensions this way.On mobile, some websites silently test if apps like Twitter, PayPal, or your banking app are installed by triggeringinvisible deep links. If the app opens or responds, they learn what apps you use. That's often used for profiling or targeted phishing. Also, browser cache abuse (using things like ETags or service workers) can fingerprint your browsereven across private tabskeeping you identifiable even when you think you're clean.How to protect yourself:These aren't tinfoil hat ideasthey're real-world methods used by major tech firms and trackers today. Staying private means going beyond ad blockers and learning how the web really works behind the scenes.What goes undetected often isn't invisibleit's just misclassified, minimized, or misunderstood. Human error isn't always a technical failure. Sometimes it's a story we tell ourselves about what shouldn't happen.Review your recent alerts. Which ones were ignored because they didn't "feel right" for the threat profile? The cost of dismissal is risingespecially when adversaries bank on it.Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.We'll unpack how leading teams are using AI, pri vacy-first design, and seamless logins to earn user trust and stay ahead in 2025.Get the latest news, expert insights, exclusive resources, and strategies from industry leaders all for free.

Link: https://thehackernews.com/2025/02/microsoft-uncovers-new-xcsset-macos.html