Data: 2025-08-31 10:43:34

Autor: Inteligência Against Invaders

Security Affairs newsletter Round 539 by Pierluigi Paganini – INTERNATIONAL EDITION

A new round of the weekly Security Affairs newsletter has arrived! Every week, the best security articles from Security Affairs are free in your email box.

Enjoy a new round of the weekly SecurityAffairs newsletter, including the international press.

International Press – Newsletter

Cybercrime

U.S. Government Seizes Online Marketplaces Selling Fraudulent Identity Documents Used in Cybercrime Schemes

Auchan announces that it has been the victim of “an act of cybercrime”, with “hundreds of thousands” of its customers’ data hacked

Widespread Data Theft Targets Salesforce Instances via Salesloft Drift

Storm-0501’s evolving techniques lead to cloud-based ransomware

Hacker used a voice phishing attack to steal Cisco customers’ personal information

DSLRoot, Proxies, and the Threat of ‘Legal Botnets’

Cyberattack against several municipal and regional systems

Infostealers: The Silent Smash-and-Grab Driving Modern Cybercrime

Colt Technology Services gets ransomware’d via SharePoint initial access— some learning points

Germany charges man over cyberattack on Rosneft subsidiary

Ransomware gang takedowns causing explosion of new, smaller groups

Citrix forgot to tell you CVE-2025–6543 has been used as a zero day since May 2025

Malware

The Resurgence of IoT Malware: Inside the Mirai-Based “Gayfemboy” Botnet Campaign

Your Connection, Their Cash: Threat Actors Misuse SDKs to Sell Your Bandwidth

Android backdoor spies on employees of Russian business

Tamperedchef – The Bad PDF Editor

AppSuite PDF Editor Backdoor: A Detailed Technical Analysis

Malware devs abuse Anthropic’s Claude AI to build ransomware

Hacking

Breaking Docker’s Isolation Using… Docker? (CVE-2025-9074)

Vtenext 25.02: A three-way path to RCE

Citrix Patches Three NetScaler Flaws, Confirms Active Exploitation of CVE-2025-7775

Widespread Data Theft Targets Salesforce Instances via Salesloft Drift

Cache Me If You Can (Sitecore Experience Platform Cache Poisoning to RCE)

Inside the Lab-Dookhtegan Hack: How Iranian Ships Lost Their Voice at Sea

WhatsApp Issues Emergency Update for Zero-Click Exploit Targeting iOS and macOS Devices

Intelligence and Information Warfare

APT36: Targets Indian BOSS Linux Systems with Weaponized AutoStart Files

Deception in Depth: PRC-Nexus Espionage Campaign Hijacks Web Traffic to Target Diplomats

ZipLine Campaign: A Sophisticated Phishing Attack Targeting US Companies

Citizen Lab director warns cyber industry about US authoritarian descent

Dutch providers targeted by Salt Typhoon

TAOTH Campaign Exploits End-of-Support Software to Target Traditional Chinese Users and Dissidents

Biased AI chatbots can sway people’s political views in minutes

Amazon disrupts watering hole campaign by Russia’s APT29

Cybersecurity

2025 State of the Internet: Digging into Residential Proxy Infrastructure

Electronics manufacturer Data I/O reports ransomware attack to SEC

FTC Calls on Tech Firms to Resist Foreign Anti-Encryption Demands

ENISA to operate the EU Cyber Reserve

Over 28,000 Citrix devices vulnerable to new exploited RCE flaw

Microsoft Releases Guidance on High-Severity Vulnerability (CVE-2025-53786) in Hybrid Exchange Deployments

TransUnion says hackers stole 4.4 million customers’ personal information

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,newsletter)