Data: 2025-08-17 00:35:32

Autor: Inteligência Against Invaders

Security Affairs newsletter Round 537 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

Google says hackers stole its customers' data by breaching its Salesforce database

ShinyHunters sent Google an extortion demand; Shiny comments on current activities

Two Defendants Plead Guilty To Fraud Scheme Involving Data Stolen From Hospital Patients

Unmasking Interlock Group's Evolving Malware Arsenal

Rapid7 Access Brokers Report: New Research Reveals Depth of Compromise in Access Broker Deals, with 71% Offering Privileged Access

When Hackers Call: Social Engineering, Abusing Brave Support, and EncryptHub's Expanding Arsenal

Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals

Malware

'Blue Locker' Analysis: Ransomware Targeting Oil & Gas Sector in Pakistan

Persistent Risk: XZ Utils Backdoor Still Lurking in Docker Images

SCENE 1: SoupDealer – Technical Analysis of a Stealth Java Loader Used in Phishing Campaigns Targeting Türkiye

Crypto24 Ransomware Group Blends Legitimate Tools with Custom Malware for Stealth Attacks

Threat Bulletin: Fire in the Woods – A New Variant of FireWood

Hacking

BadCam: Now Weaponizing Linux Webcams

Postman, engineer, cleaner: Are hackers sneaking into your office?

You Snooze You Lose: RPC-Racer Winning RPC Endpoints Against Services

Chrome Sandbox Escape Earns Researcher $250,000

Case: Citrix vulnerability (Update 11-08-2025)

Fortinet Warns About FortiSIEM Vulnerability (CVE-2025-25256) With In-the-Wild Exploit Code

Uncovering memory corruption in NVIDIA Triton (as a new hire)

Don’t Phish-let Me Down: FIDO Authentication Downgrade

Attacking GenAI applications and LLMs – Sometimes all it takes is to ask nicely!

The Root(ing) Of All Evil: Security Holes That Could Compromise Your Mobile Device

Intelligence and Information Warfare

ScarCruft’s New Language: Whispering in PubNub, Crafting Backdoor in Rust, Striking with Ransomware

From Drone Strike to File Recovery: Outsmarting a Nation State

New Ransomware Charon Uses Earth Baxia APT Techniques to Target Enterprises

Curly COMrades: A New Threat Actor Targeting Geopolitical Hotbeds

Norway spy chief blames Russian hackers for dam sabotage in April

House of Commons hit by cyberattack from ‘threat actor’: internal email

Vulnerabilities exposed: Israeli company reveals how users can hack ChatGPT accounts remotely

UAT-7237 targets Taiwanese web hosting infrastructure

Cybersecurity

The August 2025 Security Update Review

SAP Security Notes: August 2025 Patch Day

AI agents are being drafted into the cyber defense forces of corporations

Manpower Says Data Breach Stemming From Ransomware Attack Impacts 140,000

How we’re using AI in new ways to fight invalid traffic

Cisco Warns of CVSS 10.0 FMC RADIUS Flaw Allowing Remote Code Execution

The First Federal Cybersecurity Disaster of Trump 2.0 Has Arrived

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,newsletter)