Security Affairs newsletter Round 543 by Pierluigi Paganini – INTERNATIO

Data: 2025-09-29 00:03:21

Autor: Inteligência Against Invaders

Security Affairs newsletter Round 543 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

Threat Actors Spoofing the FBI IC3 Website for Possible Malicious Activity

Hacking Activities of Pro-Russian Cyber Crime Group Targeting Korean Companies

Canada dismantles TradeOgre exchange, seizes $40 million in crypto

Scattered Spider Suspect Arrested in US

ShadowV2: An emerging DDoS for hire botnet

Feds Tie ‘Scattered Spider’ Duo to $115M in Ransoms

Volvo Group Employee Data Stolen in Ransomware Attack

USD 439 million recovered in global financial crime operation

Eurojust coordinates action to halt cryptocurrency fraud of over 100 million euros across Europe

European Airport Cyberattack Linked to Obscure Ransomware, Suspect Arrested

260 suspected scammers arrested in pan-African cybercrime operation

Ransomware attack on Ohio county impacts over 45,000 residents, employees

Malware

Brewing Trouble — Dissecting a macOS Malware Campaign

Large-Scale Attack Targeting Macs via GitHub Pages Impersonating Companies to Attempt to Deliver Stealer Malware

Malware Analysis Report RayInitiator & LINE VIPER

XCSSET evolves again: Analyzing the latest updates to XCSSET's inventory

Bearlyfy: The Evolution of a New Ransomware Group and Its Connection to PhantomCore

Updated BO Team Grouping Tools

Hacking

ComicForm, start: F6 analysts have studied the phishing campaigns of a new attacker

Project Rain:L1TF

Heap-based buffer overflow in Kernel Streaming WOW Thunk Service Driver – CVE-2025-53149

Cloudflare mitigates new record-breaking 22.2 Tbps DDoS attack

CISA Shares Lessons Learned from an Incident Response Engagement

Cisco warns of IOS zero-day vulnerability exploited in attacks

IMDS Abused: Hunting Rare Behaviors to Uncover Exploits

Cisco Event Response: Continued Attacks Against Cisco Firewalls

Technical Analysis – CVE-2025-10035

It Is Bad (Exploitation of Fortra GoAnywhere MFT CVE-2025-10035) – Part 2

ForcedLeak: AI Agent risks exposed in Salesforce AgentForce

SVG Phishing hits Ukraine with Amatera Stealer, PureMiner

Intelligence and Information Warfare

Mapping the Infrastructure and Malware Ecosystem of MuddyWater

Inside Palantir: The Secretive Tech Company Helping the US Government Build a Massive Web of Surveillance

U.S. Secret Service dismantles imminent telecommunications threat in New York tristate area

Cache of Devices Capable of Crashing Cell Network Is Found Near U.N.

ICE unit signs new $3M contract for phone-hacking tech

Operation Rewrite: Chinese-Speaking Threat Actors Deploy BadIIS in a Wide Scale SEO Poisoning Campaign

Libraesva Email Security Gateway Vulnerability Exploited by Nation-State Hackers

Another BRICKSTORM: Stealthy Backdoor Enabling Espionage into Tech and Legal Sectors

NCSC warns of persistent malware campaign targeting Cisco devices

How RainyDay, Turian and a new PlugX variant abuse DLL search order hijacking

DeceptiveDevelopment: From primitive crypto theft to sophisticated AI-based deception

RedNovember Targets Government, Defense, and Technology Organizations

Microsoft Reduces Israel's Access to Cloud and AI Products Over Reports of Mass Surveillance in Gaza

Cybersecurity

European airports disruption due to ransomware — EU agency

Auto giant Stellantis investigating data breach following 'unauthorized access'

Statement on AI and Cybersecurity

European airports still dealing with disruptions days after ransomware attack

SolarWinds Releases Hotfix for Critical CVE-2025-26399 Remote Code Execution Flaw

CISA: ED 25-03: Identify and Mitigate Potential Compromise of Cisco Devices

Cyberattack on Jaguar Land Rover threatens to hit British economic growth

Statement from the Canadian Centre for Cyber Security on malware targeting global organizations through Cisco Systems

Brits warned as illegal robo-callers with offshored call centers fined half a million

Gcore Radar Attack Trends Q1?Q2 2025

Viral call-recording app Neon goes dark after exposing users' phone numbers, call recordings, and transcripts

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,newsletter)