Boletim informativo de Assuntos de Segurança Rodada 544 por Pierluigi P

Data: 2025-10-05 22:08:43

Autor: Inteligência Against Invaders

Boletim informativo de Assuntos de Segurança Rodada 544 por Pierluigi Paganini – EDIÇÃO INTERNACIONAL

Uma nova rodada do boletim semanal de Assuntos de Segurança chegou! Toda semana, os melhores artigos de segurança da Security Affairs são gratuitos em sua caixa de e-mail.

Desfrute de uma nova rodada do boletim semanal SecurityAffairs, incluindo a imprensa internacional.

GreyNoise detecta aumento de 500% nas varreduras direcionadas aos portais da Palo Alto Networks
A CISA dos EUA adiciona falhas Smartbedded Meteobridge, Samsung, Juniper ScreenOS, Jenkins e GNU Bash ao seu catálogo de vulnerabilidades exploradas conhecidas
ShinyHunters lança site de vazamento de dados: Trinity of Chaos anuncia novas vítimas de ransomware
Malware ProSpy e ToSpy se passam por Signal e ToTok para roubar dados nos Emirados Árabes Unidos
Google alerta para campanha de extorsão Cl0p contra usuários do Oracle E-Business
CERT-UA avisa que UAC-0245 tem como alvo a Ucrânia com backdoor CABINETRAT
Violação de dados da Allianz Life afetou 1,5 milhão de pessoas
Grupo de crimes cibernéticos afirma ter violado repositórios privados do GitHub da Red Hat
APT Phantom Taurus, vinculado à China, usa malware Net-Star em campanhas de espionagem contra setores-chave
OpenSSL corrige 3 vulnerabilidades, pedindo atualizações imediatas
Apple pede aos usuários que atualizem o iPhone e o Mac para corrigir o bug da fonte
WestJet confirma que IDs e passaportes expostos a ataques cibernéticos em incidente de junho
Broadcom corrige VMware Zero-Day explorado ativamente pela UNC5174
Reino Unido condena cidadão chinês por fraude cripto de £ 5,5 bilhões, marca a maior apreensão de Bitcoin do mundo
A CISA dos EUA adiciona falhas Adminer, Cisco IOS, Fortra GoAnywhere MFT, Libraesva ESG e Sudo ao seu catálogo de vulnerabilidades exploradas conhecidas
Asahi interrompe pedidos, remessas e atendimento ao cliente após ataque cibernético
Aranha Dispersa, Reestruturação de ShinyHunters – Novos Ataques em Andamento
Reino Unido concede empréstimo de £ 1,5 bilhão à Jaguar Land Rover após ataque cibernético
Harrods alerta clientes sobre nova violação de dados vinculada a provedor terceirizado
Akira Ransomware ignora MFA em VPNs da SonicWall
Apesar da influência russa, a Moldávia vota a favor da UE, destacando os riscos futuros das eleições
Adolescentes holandeses presos por espionagem em nome de hackers pró-Rússia
Ataque cibernético à cooperativa deixa prateleiras vazias, dados roubados e US$ 275 milhões em receita perdida

Imprensa Internacional – Newsletter

Cibercrime

Smash and Grab: Campanha agressiva de Akira tem como alvo VPNs da SonicWall e implanta ransomware em uma hora ou menos

Mulher condenada após a maior apreensão de criptomoedas do mundo

As crianças não estão bem

Trinity of Chaos: The LAPSUS$, ShinyHunters e Scattered Spider Alliance embarcam em uma onda global de crimes cibernéticos

‘Você nunca mais precisará trabalhar’: criminosos oferecem dinheiro a repórter para hackear a BBC

Red Hat confirma incidente de segurança após hackers alegarem violação do GitHub

Pesquisadores dizem que sinalizaram falhas cibernéticas na Jaguar antes de violação incapacitante

Aplicativos Oracle Explorados por Hackers em Nova Campanha de Extorsão

Smishing silencioso: o abuso oculto de APIs de roteador celular

Malware

Primeiro MCP malicioso na natureza: o backdoor do carimbo postal que está roubando seus e-mails

Klopatra: expondo uma nova operação de trojan bancário Android com raízes na Turquia

Verifique suas meias – um mergulho profundo no pacote PyPI soopsocks

Novas campanhas de spyware têm como alvo usuários do Android preocupados com a privacidade nos Emirados Árabes Unidos

Rhadamanthys 0.9.x – percorra as atualizações

Hacking

AppSuite, OneStart e ManualFinder: o nexo do engano

A Apple corrige um bug crítico de processamento de fontes. Atualizar agora!

Por que os hackers estão mirando o transporte marítimo mundial

Relatório da HackerOne encontra aumento de 210% nos relatórios de vulnerabilidade de IA em meio ao aumento da autonomia da IA

Palo Alto Scanning sobe ~ 500% em 48 horas, marcando alta de 90 dias

WireTap: Quebrando o SGX do servidor via interposição de barramento DRAM

Ataques de intermediários de baixo custo contra RAM em computação confidencial

OneLogin, muitos segredos: Clutch descobre vulnerabilidade crítica de API expondo credenciais de cliente

Inteligência e guerra de informação

Dois adolescentes holandeses presos em raro caso de espionagem russa

Partido pró-UE na Moldávia deve vencer votação atolado em alegações de interferência russa

Você escolhe, a VMware eleva (CVE-2025-41244)

Touro Fantasma: Um Novo Nexus Chinês APT e a Descobertaf o NET-STAR Malware Suite

SVG Phishing atinge a Ucrânia com Amatera Stealer, PureMiner

Backdoor CABINETRAT usado pelo UAC-0245 para ataques cibernéticos direcionados contra SOU (CERT-UA#17479)

Lobisomem de Cavalaria invade o setor público da Rússia com ataques de relacionamento confiável

Confúcio Espionagem: De Ladrão a Backdoor

Cibersegurança

Harrods avisa clientes que seus dados podem ter sido roubados em violação de TI

Governo apoia Jaguar Land Rover com garantia de empréstimo de £ 1,5 bilhão

WestJet confirma que passaportes de clientes expostos a violações recentes

Os agentes de IA estão corroendo as bases da segurança cibernética

Os federais cortaram o financiamento para o programa que compartilhava informações sobre ameaças cibernéticas com os governos locais

Califórnia promulga lei de segurança de IA visando gigantes da tecnologia

Mantenedores de pacotes pedem melhorias no novo plano de segurança npm do GitHub

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–Hackingboletim informativo)