Boletim informativo de Assuntos de Segurança Rodada 542 por Pierluigi P

Data: 2025-09-22 00:46:08

Autor: Inteligência Against Invaders

Boletim informativo de Assuntos de Segurança Rodada 542 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.

Imprensa Internacional – Newsletter

Cibercrime

Dados privados de Gucci, Balenciaga e Alexander McQueen resgatados por hackers

Os hackers reivindicam acesso a portais de aplicação da lei, mas eles realmente têm acesso?

Fundador de um dos maiores fóruns de hackers do mundo é condenado a três anos de prisão

RaccoonO365: uma campanha ativa e novos recursos

FileFix na natureza! Nova campanha do FileFix vai além do POC e aproveita a esteganografia

Microsoft apreende 338 sites para interromper o serviço de phishing ‘RaccoonO365’ em rápido crescimento

Cidadão do Reino Unido acusado de vários ataques cibernéticos, inclusive em infraestrutura crítica

Dois acusados por ataque cibernético TfL

Campanhas Inside the Lighthouse e Lucid PhaaS direcionadas a 316 marcas globais

SystemBC – Trazendo o Ruído

Evolução do crime cibernético – principais tendências, ameaças à segurança cibernética e estratégias de mitigação a partir de dados históricos

Malware

SmokeLoader ressurge das cinzas

Pacote popular Tinycolor npm comprometido em ataque à cadeia de suprimentos que afeta 40+ pacotes

Alerta de inteligência de ameaças Satori: SlopAds cobre fraudes com camadas de ofuscação

Prompts como código e chaves incorporadas | A Caça ao Malware Habilitado para LLM

Ataque em larga escala direcionado a Macs por meio de páginas do GitHub que se passam por empresas para tentar entregar malware ladrão

Hacking

Uma abordagem de aprendizado sobre como explorar o CVE-2020-9273

Ataque Rowhammer demonstrado contra DDR5

6 ataques baseados em navegador para os quais as equipes de segurança precisam se preparar agora

Google corrige o CVE-2025-10585 de dia zero do Chrome enquanto o exploit V8 ativo ameaça milhões

SonicWall solicita redefinições de senha após hackers obterem configurações de firewall

ShadowLeak: um ataque sem clique, do lado do serviço, exfiltrando dados confidenciais usando o agente de pesquisa profunda do ChatGPT

CISA divulga relatório de análise de malware sobre ouvintes maliciosos direcionados aos sistemas móveis do Ivanti Endpoint Manager

Inteligência e guerra de informação

APT Down – Os Arquivos da Coreia do Norte

Hive0154, também conhecido como Mustang Panda, descarta backdoor Toneshell atualizado e novo worm USB SnakeDisk

Israel anuncia apreensão de US$ 1,5 milhão de carteiras de criptomoedas vinculadas ao Irã

Ucrânia alega ataques cibernéticos aos sistemas eleitorais russos; Moscou confirma interrupções

TRÊS ATORES CIBERNÉTICOS IRANIANOS

SEC tem como alvo empresas americanas ligadas a suspeitas de golpes chineses de ‘pump and dump’

Cuidando da lacuna dos drones: a guerra de drones e a UE

Colaboração Gamaredon X Turla

Modus Operandi do Caracol Sutil

Cibersegurança

Os agentes de IA estão corroendo as bases da segurança cibernética

Crianças no Reino Unido estão hackeando suas próprias escolas em busca de desafios e notoriedade

Cloudflare participa de operação global para revolucionar o RaccoonO365

JLR pode enfrentar interrupções até novembro após hack

Fortra lança luz sobre o exploit de dia zero do GoAnywhere MFT usado em ataques de ransomware

Unidade 42 da Palo Alto Networks reconhecida pelo NCSC do Reino Unido como um provedor de serviços garantido de resposta a incidentes cibernéticos de nível aprimorado

Alemanha aprova novas regras para proteger infraestrutura crítica

Passageiros retidos em Heathrow e outros aeroportos europeus após ataque cibernético

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,boletim informativo)