Radar de Ciberataques

Incidentes no Brasil, o resumo do mundo e as falhas que estão sendo exploradas

Sábado, 14 de novembro de 2026 Janela: 13/11 (manhã) a 14/11, 18h · inclui casos divulgados na noite de 12/11 Edição nº 1

5	5	2
CASOS NO BRASIL	CONFIRMADOS	FALHAS EXPLORADAS

BRASIL · SETOR PÚBLICO

Tesouro Nacional e Caixa Vida e Previdência comunicam incidentes com dados de cadastro

O Tesouro informou acesso indevido a 30 mil cadastros e a 4 mil chaves Pix; a seguradora da Caixa Seguridade, a uma base com 7,6 milhões de clientes. A Petrobras relatou tentativa de ataque aos seus sites.

Como ler: CONFIRMADO a vítima ou uma autoridade confirmou · EM ANDAMENTO caso ainda aberto · "Nota oficial" marca a fonte publicada pelo próprio afetado ou por autoridade.

ÓRGÃO FEDERAL · DF

Tesouro Nacional comunica acesso indevido a 30 mil cadastros e 4 mil chaves Pix

CONFIRMADO Tesouro Nacional · acesso não autorizado

Detectado em 4/11 e comunicado só na noite de 12/11, o acesso indevido expôs cerca de 30 mil cadastros do portal e-Serviços (nome, CPF e e-mail) e cerca de 4 mil chaves Pix de beneficiários de pagamentos federais.

O Tesouro diz que não houve impacto financeiro nem nos sistemas estruturais e que notificou a ANPD e o CTIR Gov.

Para outros órgãos: reduzir o volume de dados cadastrais guardados, exigir verificação em duas etapas nos portais e encurtar o prazo entre a detecção e a comunicação aos afetados.

Fonte: Convergência Digital, 13/11

PORTOS · SP / SANTOS

Autoridade Portuária de Santos segue restabelecendo sistemas após incidente

CONFIRMADO EM ANDAMENTO Autoridade Portuária de Santos (APS) · ataque hacker; tipo e grupo não divulgados

Os sistemas de TI da APS ficaram indisponíveis na sexta, 6/11, depois de uma reinicialização que se seguiu a uma queda de energia. Em 12/11, cerca de 70% dos backups dos arquivos afetados tinham sido recuperados; no dia 13, os sistemas on-line ainda oscilavam.

A operação não parou: navios e acesso terrestre seguem com procedimentos alternativos. A APS ainda apura o alcance do incidente e se houve acesso a dados, e a Polícia Federal abriu inquérito em 10/11.

Para outros órgãos: manter backups isolados e testados e procedimentos alternativos de operação ajuda a reduzir o tempo de recuperação.

Fontes: Convergência Digital, 12/11 · Fast Company Brasil, 13/11 · Rondoniaovivo, 13/11

GRUPO CAIXA · NACIONAL

Caixa Vida e Previdência comunica acesso indevido a base de 7,6 milhões de clientes

CONFIRMADO Caixa Vida e Previdência (Caixa Seguridade) · invasão com cópia de dados

Identificado em 6/11 e divulgado seis dias depois, o ataque à seguradora da Caixa Seguridade copiou nome e CPF de clientes atuais e antigos; parte dos registros tem endereço, telefone, e-mail e nascimento.

A empresa diz não ver acesso a dados financeiros ou senhas. A ANPD analisa as medidas.

Fonte: Baguete, 13/11

ESTATAL DE ENERGIA · RJ

Petrobras informa tentativa de ataque aos sites corporativos

CONFIRMADO Petrobras · tipo não detalhado

Na tarde de 11/11, o site corporativo e a Agência Petrobras, em servidores externos, ficaram lentos e intermitentes; sistemas internos e produção não foram atingidos, diz a empresa. A autoria não está confirmada.

Para outros órgãos e empresas: separar os sites institucionais dos sistemas internos e protegê-los contra negação de serviço.

Fonte: Rondoniaovivo, 13/11

PLATAFORMA DIGITAL · MG / BELO HORIZONTE

Hotmart comunica usuários sobre acesso indevido a dados

CONFIRMADO Hotmart · acesso não autorizado a dados

Em 13/11, a plataforma de cursos avisou por e-mail de um incidente que conhecia desde 12/10: nome, e-mail, volume de transações e dados do dispositivo. Diz que não houve movimentação indevida de valores e que comunicou a ANPD.

Fonte: O Reporter, 13/11

NÃO FOI ATAQUE

Apagão do Microsoft 365 parou o Judiciário

A falha de 12 e 13/11 levou o CNJ a suspender os prazos processuais no país. A Microsoft descartou ataque hacker. Os prazos voltam a correr em 16/11.

Fonte: Convergência Digital, 13/11

Mundo

OS CASOS MAIS RELEVANTES DO PERÍODO

BELARUS · NUVEM

Ransomware tira do ar provedor de nuvem e seus clientes

A ActiveCloud teve parte da infraestrutura criptografada, e empresas do país ficaram dias sem site, e-mail e servidores virtuais. Os serviços principais voltaram na sexta; a empresa diz não ver roubo de dados de clientes.

Fonte: The Record, 13/11

EUROPA E EUA · OPERAÇÃO POLICIAL

Operação Endgame derruba Gootloader, CastleRAT e StealC

Polícias da Alemanha, Holanda, Dinamarca e EUA, com apoio da Europol, apreenderam 235 servidores, 257 domínios e cerca de 6,4 milhões de logins roubados de mais de 40 mil vítimas. Segundo o DOJ, o Gootloader abriu caminho para ao menos 44 ataques de ransomware nos EUA.

Fonte: The Hacker News, 13/11

EUA · COREIA DO NORTE

FBI desmonta golpe de videochamada que roubou US$ 400 mi

A campanha FaceStealer sequestrava contas de mensageiros para marcar reuniões falsas, exibia gravações de conhecidos da vítima e simulava um erro técnico para induzir a instalação de malware. A infraestrutura em nuvem foi apreendida.

Fonte: BleepingComputer, 14/11

JAPÃO · PREFEITURA

Fornecedor de e-mail vaza contatos de 1 milhão em Osaka

A invasão do serviço de disparo de e-mails usado pela plataforma de serviços on-line da prefeitura expôs mais de 1 milhão de endereços. O fornecedor diz que o ataque atingiu 77 milhões de endereços de cerca de 400 clientes e foi usado para enviar golpes.

Fonte: The Record, 13/11

EUA · CADEIA DE FORNECIMENTO

Credencial de fornecedor de IA leva extensão falsa ao Cursor

Com uma chave roubada da Fireworks AI, invasores publicaram versões maliciosas da extensão Claude Code no marketplace do Cursor, com tentativa de instalar backdoor SSH; até 5 mil usuários podem ter baixado. A Uber também confirmou acesso indevido por credenciais de um fornecedor.

Fontes: BleepingComputer, 14/11 · Olhar Digital, 13/11

⚠ Alerta: falhas exploradas agora

PRIORIDADE PARA BORDA E FERRAMENTAS DE GESTÃO

Check Point Security Gateway / Gaia OS

CVE-2026-123039 · encadeada com PHP2Shell (CVE-2026-109618 e CVE-2026-109619)

A exploração começou em 30/10. O invasor entra pelo portal Mobile Access usando as falhas do PHP, vira root no gateway, instala backdoor e salta para hosts VMware ESXi, onde roda um wiper que apaga dados. A Check Point viu exploração em cerca de duas dezenas de clientes.

No Brasil, a Anatel já tinha tirado o SEI do ar de forma preventiva por causa do PHP2Shell em 21/10.

O QUE FAZER

1. Aplicar o Jumbo Hotfix de novembro (SK1000362), começando pelos portais Mobile Access expostos.
2. Sem patch: parar o processo dynamic_server (paliativo).
3. Procurar IOCs e acessos SSH do gateway para o ESXi.

Fontes: BleepingComputer, 13/11 · InvestNews, 23/10

N-able N-central (RMM)

CVE-2026-90436 · Apache Axis · CVSS 9.8 · cadeia "4EverAble2Shell"

Uma cadeia sem autenticação dá root no servidor que gerencia os endpoints dos clientes. Foram 21 servidores invadidos com minerador de cripto, 19 deles já com o Hotfix 2.

O QUE FAZER

1. Atualizar Agents e Probes para 2026.4 HF1 ou superior.
2. Desligar a Legacy API em servidores locais.
3. Tratar qualquer indício como comprometimento total.

Fonte: The Hacker News, 13/11

Método: notícias públicas, rastreadores e as notas dos próprios afetados (fabricantes, órgãos, empresas, CVM, ANPD, CTIR Gov), com o link de cada fonte junto do texto; nenhum site de vazamento ou fórum criminoso foi acessado. Os textos são paráfrases. Conteúdo informativo, produzido com apoio de inteligência artificial a partir de fontes públicas. Alegações de grupos criminosos não foram confirmadas pelas vítimas. Correções e atualizações são publicadas nas edições seguintes.