Fique um passo à frente: receba o Radar todo dia útil, de graça. Inscreva-se → hubterritory.com/radar/inscricao

UMA PUBLICAÇÃO HUB TERRITORY · INTELIGÊNCIA DE AMEAÇAS EDIÇÃO Nº 7

Radar de Ciberataques

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

Sexta-feira, 20 de novembro de 2026 Janela: qui 19/11, 07h04 a sex 20/11, 06h57 Edição nº 7

1	1	1
CASOS NO BRASIL	CONFIRMADOS	FALHAS EXPLORADAS

BRASIL · PLATAFORMA DIGITAL

iFood confirma acesso indevido a dados de entregadores, clientes e restaurantes

Segundo a empresa, o acesso de 14/11 foi identificado e contido, e senhas, cartões e saldos não foram atingidos. No mundo, a Broadcom corrigiu uma falha do VMware vCenter que já vinha sendo explorada desde setembro.

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.

DELIVERY · BRASIL

iFood confirma acesso indevido a dados de clientes, entregadores e restaurantes

CONFIRMADO EM ANDAMENTO iFood · Acesso não autorizado (autoria não identificada)

O iFood confirmou um acesso indevido a dados pessoais ocorrido em 14/11. Segundo a empresa, o acesso foi identificado e contido, sem interrupção do serviço.

Os dados variam por perfil: clientes e usuários do iFood Benefícios tiveram exposto só o telefone; representantes de restaurantes, o telefone e, em alguns casos, o CPF; entregadores, dados cadastrais como nome, e-mail, telefone, endereço e CPF, e alguns também a conta de repasse. Senhas, cartões, saldos e biometria não foram acessados, diz a empresa.

O iFood notificou a ANPD e está avisando os afetados por e-mail; não divulgou quantas pessoas foram atingidas. Quem recebeu o aviso deve desconfiar de contatos que peçam códigos ou dados bancários em nome da empresa.

Fontes: Olhar Digital, 19/11 · Gazeta Mercantil, 19/11 · Canaltech, 19/11 · Convergência Digital, 19/11

CORREÇÃO CRÍTICA · SEM ATAQUES RELATADOS

Drupal corrige falha no instalador que permite tomar o site

O aviso SA-CORE-2026-017, de 18/11, corrige uma falha no instalador do Drupal (CVE-2026-132165) que pode permitir a um atacante sem login assumir o site. Há prova de conceito, mas não há ataques relatados. Relevante para portais públicos e institucionais feitos em Drupal: atualizar para 11.4.13, 11.3.22 ou 10.6.22 e bloquear o acesso a /core/install.php.

Fontes: The Hacker News, 19/11 · Nota oficial: Drupal Security Team — SA-CORE-2026-017, 18/11

Atualizações CASOS DE EDIÇÕES ANTERIORES QUE MUDARAM

Porto de Santos (APS) Em 18/11, SAP e SDD tinham voltado em parte, para uso interno, e mais de 30 sistemas seguiam em modo alternativo; a movimentação de navios, cargas, caminhões e trens segue normal. Segundo a APS, a queda de energia desligou os datacenters e a invasão apagou dados, mas não houve vazamento de dados sigilosos. Para outros órgãos: backup isolado e testado, e plano de continuidade que preveja falha de energia.

Fontes: ABC do ABC, 11/11 · CyberDelegate, 17/11 · ABC do ABC, 18/11

Visa e JPMorgan Segundo a AP, o JPMorgan confirmou em 19/11 que dados de marketing de milhares de clientes (nomes, e-mails e alguns telefones) vazaram após ataque a fornecedores; Visa e Mastercard também confirmaram exposição, sem dados de pagamento. A ligação com a reivindicação do grupo n0n não foi confirmada.

Fonte: Diário do Grande ABC (Associated Press/Broadcast), 19/11

Java4Shell (CVE-2026-114938) GreyNoise, watchTowr, Cloudflare e Previdian registraram as primeiras tentativas de exploração em 18 e 19/11, ainda sem invasão confirmada. A Cisco listou mais de uma dúzia de produtos afetados sem correção; o Keycloak publicou a imagem corrigida 26.8.2-3.

Fonte: SecurityWeek, 19/11

PHP Saíram em 19/11 as versões 8.5.13, 8.4.28, 8.3.37 e 8.2.36, que corrigem 7 falhas críticas (CVSS 9,2), sem exploração relatada. Sem atualizar já, desligue session.upload_progress e reinicie o PHP-FPM.

Fontes: Nota oficial: PHP.net (anúncio das versões 8.5.13/8.4.28/8.3.37/8.2.36), 19/11 · The Hacker News, 19/11

Mundo

OS CASOS MAIS RELEVANTES DO PERÍODO

UE · GOVERNO

Comissão Europeia confirma ataque com uso de IA que tirou sistemas internos do ar

A Comissão Europeia confirmou em 19/11 uma campanha de ataques detectada em 22/10, que levou à retirada temporária de aplicativos e sistemas internos. Segundo o Politico, citado pelo Olhar Digital, foram afetados sistemas de RH e de reembolso de despesas médicas, com cerca de dez dias de interrupção; a maioria já voltou.

O ataque teria usado de forma indevida uma ferramenta de IA para testes de invasão. A Comissão diz não ter evidência de vazamento que afete o conjunto dos funcionários; não há autoria conhecida. Para outros órgãos, a lição é controlar quais ferramentas de teste e de IA rodam na rede e ter contingência para sistemas de RH e pagamento.

Fonte: Olhar Digital, 19/11

EUA · GATEWAY DE E-MAIL NA NUVEM

Invasão a servidor da N-able derruba gestão do Mail Assure e SpamExperts

A N-able confirmou que invasores ainda não identificados acessaram um servidor da nuvem do Mail Assure e do SpamExperts. Para conter o incidente, desligou o portal de gestão, as APIs, a quarentena e os logs nas regiões Américas, APAC e Europa; o fluxo e a filtragem de e-mail seguem funcionando.

A instabilidade começou em 16/11 e só depois foi tratada como incidente de segurança. A empresa diz não ter indício de acesso a dados de clientes nem às caixas postais e afirma que o caso não tem relação com as falhas do N-central.

Fontes: The Hacker News, 19/11 · Nota oficial: N-able — página de status do incidente (citada pela imprensa; não abriu), 19/11

NORUEGA · ENERGIA

Equinor confirma ataque em andamento a sistemas de TI

A norueguesa Equinor, maior fornecedora de gás da Europa, informou em 17/11 que detectou um ataque cibernético em andamento contra parte de seus sistemas de TI e mobilizou equipes para conter a ameaça.

Em atualizações de 18 e 19/11 na sua sala de imprensa, a empresa disse que o ataque não é um vírus (sem risco de propagação), não parece mirar a Equinor especificamente e ainda está em curso; não há prazo para normalizar.

A produção segue normal e não há indício de roubo ou alteração de dados. A empresa está em contato com as autoridades de segurança nacional e registrou queixa na polícia. Autoria e sistemas atingidos não foram divulgados.

Fontes: Nota oficial: Equinor — Update regarding cyber-attack (nota oficial), 19/11 · Gulf News (com Reuters), 17/11 · Times Brasil (CNBC), 17/11

IRLANDA · FORNECEDOR DE TI

Invasão em fornecedor de TI expõe dados de mais de 40 cooperativas de crédito na Irlanda

Hackers exploraram uma falha no software da Wellington IT, de Belfast, que fornece a plataforma bancária a mais de um terço das cooperativas de crédito da Irlanda, e extraíram registros de membros e detalhes de pagamentos. Mais de 40 cooperativas foram avisadas no início da semana de 17/11.

A liga das cooperativas (ILCU) confirmou o incidente, disse que a falha foi corrigida e que saldos não foram afetados. A autoridade de proteção de dados recebeu várias notificações; o impacto pode chegar a 1,8 milhão de pessoas (estimativa de teto, não confirmada). A lição vale para órgãos e provedores: avaliar a segurança dos fornecedores que guardam dados de terceiros.

Fonte: The Irish Times, 17/11

EUA · JUSTIÇA

Britânico ligado ao Scattered Spider pega seis anos de prisão nos EUA

A Justiça federal dos EUA condenou a seis anos de prisão um britânico de 24 anos apontado como ligado ao Scattered Spider, por uma campanha de phishing que roubou mais de US$ 11,6 milhões em criptomoedas de pessoas nos EUA.

O grupo é acusado de invasões a empresas como Twilio, Mailchimp e LastPass e de participar do ataque à MGM Resorts.

Fonte: The Record, 18/11

⚠ Alerta: falhas exploradas agora

PRIORIDADE PARA BORDA E FERRAMENTAS DE GESTÃO

VMware vCenter 8.0, 9.0 e 9.1 (inclui VCF, vSphere Foundation e Telco Cloud)

CVE-2026-123890 (CVSS 9,8) + CVE-2026-123891 a 123894 (6,7–8,1) — explorada como zero-day segundo Google/Mandiant; fora do KEV até o catálogo de 18/11

A Broadcom corrigiu em 19/11 uma falha de bypass de autenticação no VMware Directory Service do vCenter (CVE-2026-123890, CVSS 9,8), que dá sessão de administrador a quem alcança o servidor pela rede. Atinge vCenter 8.0, 9.0 e 9.1, inclusive nas versões embutidas no Cloud Foundation e no Telco Cloud.

Segundo o Google Threat Intelligence Group e a Mandiant, citados pelo The Hacker News em 20/11, a falha já era explorada como zero-day desde o início de setembro pelo grupo de espionagem com suspeita de vínculo chinês Armory Castle (antes UNC5221), com uma ferramenta chamada BONESAW, que roubou dados de ESXi. A mesma campanha usa uma falha do BeyondTrust Remote Support (CVE-2026-102764).

Vítimas e setores não foram divulgados. Não há workaround: é preciso atualizar.

O QUE FAZER

1. Aplicar a atualização do VMSA-2026-0009 em todos os vCenter: 8.0 U3m; VCF/vSphere Foundation 9.0.x → 9.0.2.0200; 9.1.x → 9.1.1.0200; VCF 5.2.5; Telco Cloud → vCenter 8.0 U3m. Não há workaround oficial.
2. Atenção: 8.0 U3m ou 9.0.2.0200 bloqueiam upgrade posterior para VCF 9.1.1 — a FAQ sugere ir direto ao 9.1.1 ou aguardar o VCF 9.1.2.
3. Restringir o acesso de rede ao vCenter à rede de gestão até atualizar.
4. Procurar sinais de invasão: contas de administrador desconhecidas no vsphere.local (ex.: prefixo "sps-"), SSH habilitado no vCenter via VAMI, chaves SSH não autorizadas no root do ESXi, tráfego nas portas 2012, 5480 e 9080.
5. Se usar BeyondTrust Remote Support, conferir a correção da CVE-2026-102764 e sinais de comprometimento.
6. Atualizar também SDDC Manager e VMware Tools para Windows (13.1.5.0 ou 12.5.5).
7. vSphere 6.5/6.7/7.0: considerar afetado; 7.0 só com suporte estendido.

Fontes: The Hacker News, 19/11 · Nota oficial: VMware/Broadcom — FAQ oficial do VMSA-2026-0009 (GitHub), 19/11 · The Hacker News (exploração por grupo ligado à China, segundo Google/Mandiant), 20/11

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.

Receba o Radar todo dia útil

Inovação e Ciberataques por e-mail ou no canal do WhatsApp. É grátis, e você cancela quando quiser.
Inscreva-se: hubterritory.com/radar/inscricao