NEWSLETTER · EDIÇÃO Nº 003

O apurado OSINT da semana

Brasil, mundo e ciber em poucos minutos de leitura, com técnica, ferramenta e oportunidades para Hunters. Toda segunda e toda sexta.

SEGUNDA-FEIRA, 02/11/2026
APURADO DE SEXTA A DOMINGO · 30/10 A 01/11/2026

NESTA EDIÇÃO · 12 ITENS

01 Abertura — EDITORIAL
02 Brasil — 4 ITENS
03 No mundo — 4 ITENS
04 Ciber e Radar da comunidade — CIBER
05 Filtrar o catálogo KEV da CISA por data, com curl e jq — TÉCNICA
06 EPSS (FIRST) — FERRAMENTA
07 Indicação da comunidade — COMUNIDADE
08 Mercado de trabalho OSINT — CARREIRA
09 Agenda — EVENTOS
10 Leituras e novidades do portal — LEITURAS

01 · ABERTURA

Atribuir, medir e priorizar: o método por trás das manchetes

O maior roubo de cripto já registrado ganhou autoria oficial em poucos dias: FBI e Serviço Secreto apontaram o grupo norte-coreano TraderTraitor e pediram ao setor que bloqueie as carteiras divulgadas. No Brasil, o Aos Fatos mediu que boatos sobre cortes de benefícios renderam quase o dobro das interações de alegações de fraude eleitoral na semana após o segundo turno.

O fio comum é o método. Atribuir exige dizer quem afirmou o quê, comparar narrativas exige critério de medição e corrigir falhas exige fonte de priorização. Esta edição traz uma técnica para filtrar o catálogo KEV, uma ferramenta gratuita de probabilidade de exploração e, como destaque da comunidade, as skills OSINT-BR indicadas pelo Prof. Emerson Wendt.

Equipe OsintHunters Brasil
osinthunters.com.br

02 Brasil

01 DESINFORMAÇÃO · 30/10/2026

Boatos sobre benefícios têm quase o dobro de interações de alegações de fraude

Levantamento do Aos Fatos somou 3,1 milhões de interações em 12 alegações falsas sobre cortes de programas e direitos, contra 1,6 milhão em seis checagens sobre fraude, entre 26 e 30 de outubro. A medida se limita às publicações mapeadas pela agência.

Fonte: Aos Fatos · 30/10/2026
https://www.aosfatos.org/noticias/apos-derrota-bolsonarismo-desinformacao-lula-fraude/

02 VERIFICAÇÃO · 30/10/2026

Mais eleitores que habitantes em cidades da Bahia não indica fraude

Segundo a Lupa, dados de reportagem de julho sobre 23 municípios foram tirados de contexto; a diferença pode decorrer de migração sem transferência do título e de defasagem nas estimativas populacionais.

Fonte: Agência Lupa · 30/10/2026
https://www.agencialupa.org/jornalismo/2026/10/30/numero-de-eleitores-maior-que-o-de-habitantes-em-cidades-da-bahia-nao-indica-fraude/

03 DADOS ABERTOS · 29/10/2026

ANPD abre consulta para definir quais bases de dados devem ser abertas

A tomada de subsídios integra o primeiro Plano de Dados Abertos da agência, para 2026 a 2028, e permite sugerir até dez bases. É uma oportunidade para Hunters indicarem dados úteis à pesquisa.

Fonte: ANPD · 29/10/2026
https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-para-elaboracao-do-plano-de-dados-abertos-2026-2028

04 DADOS PESSOAIS · 29/10/2026

Operação Luctus apura suposta venda de registros de óbitos em São Paulo

Segundo a Corregedoria da Polícia Civil e a Controladoria do município, houve ordens de busca contra 21 investigados, suspeitos de obter registros de forma irregular e repassá-los a empresas funerárias.

Fonte: Metrópoles · 29/10/2026
https://www.metropoles.com/sao-paulo/operacao-mira-grupo-suspeito-de-vender-dados-de-mortos-para-funerarias

03 No mundo

05 ATRIBUIÇÃO · 02/11/2026

FBI atribui à Coreia do Norte o roubo de US$ 6,3 bilhões da Binance

FBI e Serviço Secreto apontaram o grupo TraderTraitor, divulgaram endereços e pediram bloqueio de transações. Especialistas citados pelo The Record estimam cerca de US$ 3 bilhões congelados.

Fonte: The Record · 02/11/2026
https://therecord.media/fbi-blames-tradertraitor-for-binance-hack

06 PRIVACIDADE · 30/10/2026

Departamento de Justiça dos EUA questiona possível venda de chats da Character.AI

Em processo de falência, o órgão pediu um ombudsman de privacidade para orientar o tribunal sobre a venda de dados de usuários, que podem incluir conversas sensíveis e de menores.

Fonte: The Record · 30/10/2026
https://therecord.media/doj-raises-privacy-concerns-over-character-ai-sale

07 VAZAMENTO · 31/10/2026

Chancelaria do Japão diz que 3.600 registros pessoais podem ter vazado

Segundo o ministério, o acesso não autorizado a uma de suas redes teria exposto nomes e e-mails. O caso se soma a outros incidentes recentes no país.

Fonte: The Japan Times · 31/10/2026
https://japantimes.co.jp/news/2026/10/31/japan/foreign-ministry-data-leak

08 GEOINT · 29/10/2026

Bellingcat aponta atraso de 24 horas em imagens Sentinel sobre Gaza

A análise indica liberação atrasada de imagens gratuitas do Copernicus sobre Gaza, partes de Israel e da Cisjordânia. Vale conferir a data real da cena antes de concluir que não há imagem recente.

Fonte: Bellingcat · 29/10/2026
https://www.bellingcat.com/news/2026/10/29/eu-satellite-imagery-delayed-over-gaza-and-parts-of-west-bank-by-24-hours/

04 Ciber no fim de semana

Números do Radar Ciber no período, com ressalva: quase todo o prejuízo informado vem de um único caso, o de falsos investimentos em cripto citado abaixo.

5 CASOS COM AÇÃO POLICIAL	**4** UFS
6 PRESOS (INFORMADO)	**R$ 45,2 mi** PREJUÍZO INFORMADO

09 FRAUDE · 31/10/2026

PM de SP prende foragido apontado como responsável por falsos investimentos em cripto

Segundo o Metrópoles, ele foi identificado por câmeras do programa Muralha Paulista; o esquema teria lesado ao menos 300 pessoas e ultrapassado R$ 45 milhões.

Fonte: Metrópoles · 31/10/2026
https://www.metropoles.com/sao-paulo/rei-das-criptomoedas-de-manaus-e-preso-pela-policia-militar-em-perdizes

10 VULNERABILIDADE · 01/11/2026

Alpine Linux refaz GitLab após tentativas de explorar falha crítica

A equipe diz não ver sinais de adulteração de pacotes, mas não pode descartar execução de código por falta de registros. A CISA confirmou a exploração ativa da CVE-2026-97229.

Fonte: BleepingComputer · 01/11/2026
https://www.bleepingcomputer.com/news/security/alpine-linux-rebuilds-gitlab-after-attempted-rce-attack/

11 IA OFENSIVA · 31/10/2026

Chainalysis relata invasão com técnicas agênticas ofensivas

A empresa de análise de blockchain informou acesso a nomes, e-mails e identificadores de clientes, e afirma não haver evidência de exposição de dados de investigação ou credenciais.

Fonte: BleepingComputer · 31/10/2026
https://www.bleepingcomputer.com/news/security/chainalysis-discloses-data-breach-from-offensive-agentic-techniques/

12 NUVEM · 31/10/2026

Northflank orienta clientes a trocar segredos após uso indevido de chaves de IA

A plataforma pediu a rotação imediata de variáveis de ambiente e chaves de API depois de uma violação de segurança.

Fonte: BleepingComputer · 31/10/2026
https://www.bleepingcomputer.com/news/security/northflank-security-breach-leads-to-abuse-of-customers-ai-api-keys/

Radar Ciber Brasil — casos registrados no período: **5**

Radar Drogas Brasil — notícias mapeadas no período: **10**

05 · TÉCNICA DA SEMANA

Filtrar o catálogo KEV da CISA por data, com curl e jq

O catálogo de vulnerabilidades exploradas da CISA é público em JSON. Com poucas linhas no terminal, você vê o que entrou na lista e confere se algo afeta o seu ambiente.

TERMINAL

```
# Baixa o catálogo e guarda a cópia com a data da coleta
curl -s
https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json -o kev-$(date +%F).json

# Lista o que entrou a partir de uma data
jq -r '.vulnerabilities[] | select(.dateAdded ≥ "2026-10-26") | [.dateAdded, .cveID, .vendorProject, .product, .dueDate] | @tsv' kev-*.json

# Procura um fabricante do seu inventário
jq -r '.vulnerabilities[] | select(.vendorProject == "Cisco") | .cveID' kev-*.json
```

Quando usar

Na triagem semanal de correções, na preparação de um boletim interno e ao avaliar se um alerta público afeta o seu inventário.

Atenção

O prazo dueDate vale para órgãos federais dos EUA. Estar fora do catálogo não significa que a falha não é explorada. Rode a consulta só para defesa e inventário próprios.

Para ir além: CISA: arquivo JSON do catálogo KEV
https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

06 · FERRAMENTA NO RADAR

EPSS (FIRST)

GRATUITA · API

O Exploit Prediction Scoring System estima a probabilidade de uma CVE ser explorada nos 30 dias seguintes, com atualização diária. Ajuda a ordenar o que corrigir quando a lista é maior do que o tempo disponível.

Dica de Hunter. Consulte a nota junto com o KEV. Falha já listada no catálogo vai à frente mesmo com nota baixa, porque a exploração está confirmada.

```
curl -s "https://api.first.org/data/v1/epss?cve=CVE-2026-97229"
```

Abrir a ferramenta →

https://www.first.org/epss/

07 Indicação da comunidade

Material sugerido por Hunters do grupo OsintHunters Brasil.

INDICAÇÃO DO PROF. EMERSON WENDT

OSINT-BR: skills de investigação em fontes abertas para o Claude

Repositório público do Prof. Dr. Emerson Wendt, sob licença MIT, com três skills adaptadas às fontes, à legislação e à prática brasileiras: método e cadeia de custódia, infraestrutura digital, e mídia e ativos. É uma iniciativa acadêmica pessoal, sem posição oficial de órgãos ou instituições, e vale pelo roteiro de método que oferece em português.

Por onde começar. Leia o ETICA.md e o AVISO-LEGAL.md antes de instalar e comece pela skill osint-fontes-abertas, em um caso fictício ou de interesse público.

Atenção

As skills são método e não autorizam identificar pessoas por trás de contas ou transações, tarefa que depende de requisição ou ordem judicial. Aplique minimização pela LGPD e faça com que pessoa qualificada confira as respostas da IA.

Abrir a indicação →

https://github.com/emersonwendt/osint-br-skills

08 Mercado de trabalho OSINT

Quatro anúncios do LinkedIn em segurança e detecção de ameaças, conferidos em 02/11/2026. Confirme requisitos e condições na página de cada vaga.

VAGA · SP

Lead Security Engineer - Vulnerability Management, Nubank

Liderança técnica em gestão de vulnerabilidades, em São Paulo, no modelo híbrido (2 a 3 vezes por semana), em tempo integral e nível pleno-sênior.

Fonte: LinkedIn (Nubank) · 01/11/2026
https://www.linkedin.com/jobs/view/4473786826/

VAGA · BRASIL

Especialista em Cyber Security, Finaya

Principal referência interna de segurança em uma empresa de infraestrutura financeira (contas digitais, Pix, Open Finance), com foco em corrigir e automatizar, detecção com MITRE ATT&CK e SOAR, e normas como ISO 27001, SOC 2 e PCI DSS.

Fonte: LinkedIn (Finaya) · 01/11/2026
https://www.linkedin.com/jobs/view/4484549878/

VAGA · REMOTO

Especialista em Engenharia de Detecção de Ameaças de Identidade, Solutis Tecnologias

Função remota, no Brasil, voltada à engenharia de detecção de ameaças de identidade.

Fonte: LinkedIn (Solutis Tecnologias) · 01/11/2026
https://www.linkedin.com/jobs/view/4485236532/

VAGA · SP

Identity Threat Detection Engineering Specialist, Serasa Experian

Criação de detecções para ameaças de identidade, autenticação e autorização, como account takeover, credential stuffing e abuso de sessão, além de apoio a investigações de incidentes, em São Paulo e tempo integral.

Fonte: LinkedIn (Serasa Experian) · 01/11/2026
https://www.linkedin.com/jobs/view/4480546776/

09 Agenda

09 NOV — WEBINAR
Bellingcat: Verification, Disordered Discourse, and the Repair of Democratic Reality
On-line · 11h às 13h (Brasília) · pago
https://www.bellingcat.com/workshops/verification-disordered-discourse-and-the-repair-of-democratic-reality-webinar/

16 NOV — WORKSHOP
Bellingcat Deep-Dive into Open Source Investigations (cinco dias)
Toronto, Canadá · 16 a 20/11
https://www.bellingcat.com/workshops/november-16-20-2026-bellingcat-deep-dive-into-open-source-investigations-five-day-workshop-toronto-canada/

23 NOV — CURSO
Bellingcat: Introduction to Geolocation, Satellite Imagery Techniques & Chronolocation
On-line · 23 a 25/11 · 11h às 15h (Brasília) · pago
https://www.bellingcat.com/workshops/introduction-to-geolocation-satellite-imagery-techniques-chronolocation-2/

10 Para ler com calma

2026 SANS Cyber Threat Intelligence (CTI) Survey Insights
SANS Institute · 15/05/2026
https://www.sans.org/white-papers/2026-sans-cyber-threat-intelligence-survey-insights

Relatório de Cenário de Ameaças do Brasil 2026
SOCRadar · 26/10/2026
https://socradar.io/resources/country-reports/relatorio-de-cenario-de-ameacas-do-brasil-2026/

Cenário de ameaças digitais no Brasil: o que mudou no primeiro semestre de 2026
ESET · 18/09/2026
https://www.welivesecurity.com/pt/ameacas-digitais/cenario-no-brasil-o-que-mudou-no-primeiro-semestre-de-2026/

NO PORTAL
Print de WhatsApp como prova: o que o STJ exige e como preservar
https://osinthunters.com.br/artigos/print-de-whatsapp-como-prova-stj-cadeia-de-custodia

NO PORTAL
Lei de Benford na investigação: como testar dados e quando não usar
https://osinthunters.com.br/artigos/lei-de-benford-como-testar-dados-python-quando-nao-usar

NO PORTAL
Protocolo de Berkeley: o padrão da ONU para investigação OSINT
https://osinthunters.com.br/artigos/protocolo-de-berkeley-padrao-onu-investigacao-osint

Conhece outro Hunter que precisa ler isto?

Encaminhe esta edição. A comunidade cresce quando o método circula.

Encaminhar no WhatsApp

Entrar na comunidade

Equipe OsintHunters Brasil

Pesquisa em fontes abertas, sem caráter oficial. Casos citados descrevem o que foi publicado e não implicam juízo sobre a culpa de ninguém. Conteúdo educacional: pratique OSINT com ética, respeitando a LGPD, o Marco Civil da Internet e os termos de uso de cada plataforma.