OsintHunters Brasil

VER NO NAVEGADOR · PDF

NEWSLETTER · EDIÇÃO N° 001

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, 26/10/2026

APURADO DE SEXTA A DOMINGO · 23 A 25/10/2026

NESTA EDIÇÃO · 11 ITENS

01 Abertura EDITORIAL
02 Brasil 5 ITENS
03 No mundo 3 ITENS
04 Ciber e Radar da comunidade CIBER
05 Conferir a exposição do PHP nos sites que você administra TÉCNICA
06 BrasilAPI (consulta de CNPJ) FERRAMENTA
07 Mercado de trabalho OSINT CARREIRA
08 Agenda EVENTOS
09 Leituras e novidades do portal LEITURAS

01 · ABERTURA

Mídia sintética no voto e servidores na mira

O fim de semana do segundo turno concentrou o que mais importa para quem verifica conteúdo: áudios e vídeos gerados por IA circulando em escala, detectores que não concordam entre si e agências de checagem mostrando que a conclusão depende de contexto, não de um único número. O balanço do Aos Fatos e a checagem da Lupa são leitura obrigatória para entender os formatos que mais circularam.

No ciber, a semana foi dominada pelo PHP2Shell, um conjunto de falhas críticas no PHP que levou órgãos de vários países a recomendar atualização imediata, e por novos detalhes sobre um grupo baseado no Brasil que mirou Pix e nuvem de uma instituição financeira. Nesta primeira edição da newsletter, a Equipe OsintHunters Brasil reúne os fatos, uma técnica, uma ferramenta, vagas abertas e leituras para a semana.

Equipe OsintHunters Brasil
osinthunters.com.br

02 Brasil

01 DESINFORMAÇÃO · 25/10/2026

Aos Fatos mapeia IA ultrarrealista e canais de WhatsApp na campanha

Segundo o levantamento, uma rede de 255 perfis somou 58 milhões de visualizações em um mês, e vídeos que simulavam telejornais e eleitores fictícios passaram de 21 milhões de visualizações no TikTok.

Fonte: Aos Fatos · 25/10/2026
https://www.aosfatos.org/noticias/ia-ultrarrealista-whatsapp-desinformacao-moldou-eleicoes/

02

VERIFICAÇÃO · 24/10/2026

Lupa classifica como falso áudio atribuído ao presidente

Três detectores deram 73%, 97,1% e 65% de probabilidade de geração por IA; a conclusão se apoiou também na ausência de qualquer registro do episódio em veículos confiáveis.

Fonte: Agência Lupa · 24/10/2026
https://www.agencialupa.org/verificacao/2026/10/24/e-falso-o-audio-em-que-lula-supostamente-xinga-roberta-luchsinger-apos-entrevista-a-cnn/

03

ELEIÇÕES · 25/10/2026

TSE registra 138 ocorrências e 0,18% de urnas substituídas no 2º turno

No balanço parcial, o tribunal informou ter intensificado o monitoramento de plataformas digitais entre os turnos e ampliado o diálogo com empresas de tecnologia contra conteúdo falso.

Fonte: Tribunal Superior Eleitoral · 25/10/2026
https://www.tse.jus.br/comunicacao/noticias/2026/Outubro/presidente-do-tse-destaca-estabilidade-no-pais-neste-2o-turno-das-eleicoes-2026

04

VERIFICAÇÃO · 24/10/2026

Guia reúne sinais para identificar vídeos e áudios gerados por IA

Sincronia labial, expressões e iluminação ajudam, mas nenhum sinal é decisivo; a recomendação é checar canais oficiais, contexto e agências de checagem.

Fonte: O Tempo · 24/10/2026
https://www.otempo.com.br/eleicoes/2026/2026/10/24/eleicoes-2026-como-identificar-videos-e-audios-gerados-ou-alterados-por-inteligencia-artificial

---

05

REGULAÇÃO · 09/09/2026

Consulta da ANPD sobre fiscalização da LGPD termina em 26/10

A revisão do regulamento de fiscalização e do processo sancionador recebe contribuições até esta segunda pela plataforma Brasil Participativo.

Fonte: ANPD · 09/09/2026
https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-audiencia-consulta-atualizacao-regulamento-fiscalizacao

---

03

No mundo

06

VULNERABILIDADE · 23/10/2026

Centro canadense atualiza alerta sobre falhas críticas no PHP

O alerta lista as versões corrigidas e acrescenta a CVE-2026-115560, que não é resolvida pelo pacote de 21/10 e tem mitigação temporária por configuração.

Fonte: Canadian Centre for Cyber Security · 23/10/2026
https://cyber.gc.ca/en/alerts-advisories/al26-026-critical-vulnerabilities-impacting-php-cve-2026-109618-cve-2026-109619

07

SPYWARE · 19/10/2026

Citizen Lab confirma Pegasus no celular de reitor em Belgrado

A confirmação veio dias antes da eleição antecipada na Sérvia; um segundo aparelho, de um promotor notificado pela Apple, segue em análise.

Fonte: The Record · 19/10/2026
https://therecord.media/serbia-spyware-pegasus-elections

08

ADTECH · 16/10/2026

AdFection: anúncios segmentados entregaram spyware sem clique

Segundo o Citizen Lab, ao menos 45 dispositivos ligados à rede Al Jazeera teriam sido alvo entre 2024 e 2025; plataformas de anúncios removeram contas após os relatórios.

Fonte: BleepingComputer · 16/10/2026
https://bleepingcomputer.com/news/security/zero-click-attacks-used-targeted-ads-to-deliver-candiru-spyware

04 Ciber no fim de semana

Casos com ação de autoridade registrados pelo Radar Ciber Brasil entre 23 e 25 de outubro, além dos alertas que mais pesaram.

4 CASOS COM AÇÃO POLICIAL	**4** UFS
2 PRESOS OU APREENDIDOS (INFORMADO)	

09

GOLPE · 23/10/2026

PCGO cumpre mandado contra suspeitos do golpe do boleto falso no WhatsApp

Segundo a polícia, os suspeitos se passariam por funcionários de uma imobiliária e o pagamento caiu em empresa aberta dias antes, com inscrição depois suspensa.

Fonte: Portal Notícias Goiás · 23/10/2026
https://portalnoticiasgoias.com.br/pcgo-mandado-busca-golpe-boleto-senador-canedo/

10

THREAT INTEL · 25/10/2026

Relatório da CrowdStrike detalha grupo do Brasil que mirou Pix e nuvem

O SLIM SPIDER teria usado credenciais temporárias de nuvem e painéis para automatizar transferências; a análise não comprovou uso bem-sucedido do painel de Pix.

Fonte: NC News · 25/10/2026
https://ncnews.com.br/2026/10/25/crime-com-pix-grupo-hacker-cria-ferramenta-para-automatizar-fraudes-em-bancos-brasileiros/

11

ALERTA · 21/10/2026

PHP2Shell: atualizar WordPress não basta, é preciso atualizar o PHP

As versões corrigidas são 8.5.12, 8.4.27, 8.3.36 e 8.2.35; donos de sites devem confirmar com a hospedagem que a correção já foi aplicada.

Fonte: Malwarebytes · 21/10/2026
https://www.malwarebytes.com/pt-br/blog/bugs/2026/10/php2shell-why-websites-are-going-offline-for-emergency-security-updates

Radar Ciber Brasil	casos registrados no período	4
Radar Drogas Brasil	notícias mapeadas no período	5

05 · TÉCNICA DA SEMANA

Conferir a exposição do PHP nos sites que você administra

Antes de pedir a correção do PHP2Shell, descubra que versão está rodando e se o recurso usado como mitigação está ativo. Use apenas em sistemas sob sua responsabilidade.

TERMINAL

```
# Versão anunciada no cabeçalho HTTP (pode estar oculta)
curl -sI https://seusite.com.br | grep -i x-powered-by

# No servidor: versão instalada do PHP
php -v

# Mitigação temporária indicada para a CVE-2026-115560
php -i | grep session.upload_progress.enabled
```

Quando usar

Ao revisar o inventário de sites próprios, ambientes de teste e painéis esquecidos, ou para confirmar com a hospedagem que a atualização foi aplicada.

Atenção

Cabeçalho ausente não significa sistema corrigido; confirme a versão no servidor. Não faça varreduras em sistemas de terceiros sem autorização.

Para ir além: Canadian Centre for Cyber Security: AL26-026 https://cyber.gc.ca/en/alerts-advisories/al26-026-critical-vulnerabilities-impacting-php-cve-2026-109618-cve-2026-109619

06 · FERRAMENTA NO RADAR

BrasilAPI (consulta de CNPJ)

GRATUITA API DADOS ABERTOS

API pública e gratuita que devolve em JSON dados cadastrais de CNPJ, como razão social, data de início de atividade e situação cadastral. Útil para checar rapidamente o beneficiário de um boleto ou Pix suspeito.

Dica de Hunter. Empresa aberta há poucos dias ou com situação diferente de ATIVA recebendo pagamento de cobrança é sinal forte de conta de passagem. Compare sempre com o CNPJ da empresa credora.

```
curl -s https://brasilapi.com.br/api/cnpj/v1/33000167000101 | jq '{razao_social, data_inicio_atividade, descricao_situacao_cadastral}'
```

Abrir a ferramenta →

https://brasilapi.com.br/docs

07 Mercado de trabalho OSINT

Vagas com OSINT na descrição, com anúncio ativo na consulta de 26/10. Muitas não trazem a sigla no título.

→ VAGA · SP

Assistente de Inteligência Junior

Pesquisa em fontes abertas, background check, due diligence e redação de relatórios; presencial em São Paulo.

Fonte: Glassdoor · 26/10/2026
https://www.glassdoor.com.br/job-listing/assistente-de-inteligência-junior-grupo-invicta-JV_IC2479061_KO0,33_KE34,47.htm?jl=1010249922532

→ VAGA · SP

Analista de Inteligência Cibernética

Digital Risk Protection e Cyber Threat Intelligence, com conhecimento sólido em OSINT e plataformas como MISP; Barueri.

Fonte: Glassdoor · 26/10/2026
https://www.glassdoor.com.br/job-listing/analista-de-inteligência-cibernética-accenture-JV_IC2464198_KO0,36_KE37,46.htm?jl=1010265263653

→ VAGA · SP

Executive Protection Analyst (12x36, diurno)

Elo entre centro de operações e proteção executiva, com uso de OSINT para monitorar notícias e ameaças; inglês fluente e espanhol avançado.

Fonte: Glassdoor · 26/10/2026
https://www.glassdoor.com.br/job-listing/executive-protection-analyst-day-shift-12x36-control-risks-JV_IC2479061_KO0,44_KE45,58.htm?jl=1010274649183

08 Agenda

31
OUT

WEBINAR

OSINT Collective Oct'26: um dia de palestras de praticantes

On-line · gratuito · a partir das 7h (Brasília)
https://osintverse.com/collective/oct26

09 Para ler com calma

↗

IOCTA 2026: How encryption, proxies and AI are expanding cybercrime

Europol

https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf

PDF: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf

---

↗

CrowdStrike 2026 Threat Hunting Report

CrowdStrike

https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike-2026-Threat-Hunting-Report.pdf

PDF: https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike-2026-Threat-Hunting-Report.pdf

---

↗

Trace Labs Weekly OSINT Challenges

Trace Labs

https://docs.tracelabs.org/osint-challenges/osint-challenges-intro

---

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.

Todas as edições: osinthunters.com.br/newsletter · Radares: Ciber · Drogas