**OsintHunters Brasil** VER NO NAVEGADOR · PDF

NEWSLETTER · EDIÇÃO Nº 004

# 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.

SEXTA-FEIRA, 06/11/2026

APURADO DE SEGUNDA A QUINTA · 02 A 05/11/2026

NESTA EDIÇÃO · 14 ITENS

01 Abertura EDITORIAL
02 Brasil 5 ITENS
03 No mundo 5 ITENS
04 Ciber e Radar da comunidade CIBER
05 Do IP à rede responsável, com a API pública do RIPEstat TÉCNICA
06 Whois do Registro.br FERRAMENTA
07 Mercado de trabalho OSINT CARREIRA
08 Agenda EVENTOS
09 Leituras e novidades do portal LEITURAS

01 · ABERTURA

## Entre o primeiro alerta e a versão oficial, fica o trabalho de apurar

A semana foi marcada por incidentes em que a primeira versão precisou de complemento. O Mercado Bitcoin suspendeu saques enquanto empresas de blockchain estimavam a saída de mais de US$ 46 milhões, número não confirmado pela corretora. O Serpro passou da fala sobre um ataque sem precedentes à nota que relata recorde de DDoS e nega impacto no Gov.br. O FGC comunicou um acesso indevido identificado dias antes.

O fio comum é o método: registrar quem afirmou o quê, quando, com qual base. Esta edição traz uma técnica para mapear redes com dados públicos, a consulta de titulares de endereços brasileiros e, no portal, um guia sobre prazos de guarda de logs no Marco Civil da Internet, publicado hoje.

**Equipe OsintHunters Brasil**
osinthunters.com.br

## 02 Brasil

01 PROTEÇÃO DE DADOS · 05/11/2026

### ANPD publica balanço de seis anos de atividade

Das 19 iniciativas regulatórias apresentadas no relatório de 85 páginas, 16 seguem em andamento, segundo o Mobile Time.

**Fonte:** Mobile Time · 05/11/2026
https://www.mobiletime.com.br/noticias/06/11/2026/os-seis-anos-da-anpd/

02 VERIFICAÇÃO · 05/11/2026

### Lupa desmente que 8 milhões de votos

### sem biometria comprovem fraude

Segundo a checagem, a habilitação sem biometria não torna o voto irregular, e as etapas de identificação impedem o registro em nome de pessoa falecida.

**Fonte:** Agência Lupa · 05/11/2026
https://www.agencialupa.org/eleicoes/2026/11/05/e-falso-que-8-milhoes-de-votos-sem-biometria-comprovam-fraude-nas-eleicoes/

---

03 DEEPFAKE · 04/11/2026

### MPSP investiga deepfakes de famosos em anúncios de suplementos

Segundo a apuração, o grupo investigado usaria imagem e voz manipuladas de pessoas conhecidas, em produtos que não teriam aprovação da Anvisa.

**Fonte:** Diário do Estado de SP · 04/11/2026
https://diarioesp.com.br/sao-paulo/2026/11/04/operacao-merovingian-mpsp-investiga-uso-de-voz-e-imagem-de-famosos-em-anuncios-falsos-de-suplementos.html

---

04 DADOS PESSOAIS · 04/11/2026

### Operação Sem Nexo apura suposta venda de dados de segurados do INSS

A Polícia Federal informa que, até agora, não há indícios de participação de servidores nem de concessão irregular de benefícios.

**Fonte:** Polícia Federal · 04/11/2026
https://www.gov.br/pf/pt-br/assuntos/noticias/2026/11/pf-e-mps-combatem-fraudes-contra-a-previdencia-social

---

05 CÂMERAS · 03/11/2026

### Prefeitura de SP abre nova apuração sobre senhas de câmeras do Smart Sampa

A gestão municipal diz não haver sinais de ataque ao sistema. A reportagem citada aponta 17 mil câmeras, algumas em locais privados.

**Fonte:** Convergência Digital · 03/11/2026
https://convergenciadigital.com.br/seguranca/smart-sampa-tem-novo-vazamento-de-dados-em-17-mil-cameras/

---

## 03 No mundo

06 BOTNET · 02/11/2026

### Google desmonta botnet XCPE, com 1,3 milhão de TV boxes

O grupo de inteligência da empresa atribui o backdoor, com alta confiança, a uma fabricante que teria vendido o acesso a afiliados.

**Fonte:** Google Threat Intelligence · 02/11/2026
https://cloud.google.com/blog/topics/threat-intelligence/shutting-the-door-on-the-xcpe-botnet

---

07 GOLPES · 03/11/2026

### Europol apoia ação contra suposto fornecedor de plataformas de investimento falsas

Sete pessoas foram presas e mais de 100 servidores apreendidos, em caso com potenciais vítimas em mais de 50 países.

**Fonte:** Europol · 03/11/2026
https://www.europol.europa.eu/media-press/newsroom/news/investment-scams-potential-victims-in-least-50-countries-over-100-servers-seized

---

08 AMEAÇAS · 03/11/2026

### Chefe do NCSC britânico prevê alta de incidentes por falhas antigas

O risco viria menos de técnicas novas de IA e mais da exploração em escala de vulnerabilidades toleradas há muito tempo, segundo o The Record.

**Fonte:** The Record · 03/11/2026
https://therecord.media/uk-ncsc-predicts-rise-cyberattacks-coming-months

---

09 FRAUDE · 04/11/2026

### Banco francês Arkéa confirma ataque via fornecedor

Rastreio público estimou mais de US$ 133 milhões. O banco não confirmou o valor exato e afirma que contas de clientes não foram acessadas.

**Fonte:** The Record · 04/11/2026

https://therecord.media/french-bank-confirms-cyber-heist

---

10 **GEOINT · 05/11/2026**

### Bellingcat mostra o que mapas online revelam sobre bases dos EUA

O grupo cruzou rótulos, avaliações, fotos oficiais e satélite, em exemplo de método e de discussão sobre exposição involuntária de dados.

**Fonte:** Bellingcat · 05/11/2026
https://www.bellingcat.com/news/2026/11/05/how-online-maps-lay-bare-the-us-military-bases-targeted-by-iran/

04

## Ciber na semana

Números do Radar Ciber de 2 a 5 de novembro, com base no que autoridades e veículos informaram.

| | |
|---|---|
| **37**<br>CASOS COM AÇÃO POLICIAL | **19**<br>UFS |
| **75**<br>PRESOS (INFORMADO) | **R$ 6,8 mi**<br>PREJUÍZO INFORMADO |

11 **VAZAMENTO · 05/11/2026**

### FGC comunica acesso não autorizado a dados pessoais

O fundo diz não ter evidência, até agora, de divulgação, uso indevido ou perda financeira, e informa que comunicou a ANPD.

**Fonte:** Convergência Digital · 05/11/2026
https://convergenciadigital.com.br/mercado/fundo-garantidor-de-creditos-sofre-invasao-hacker-dados-foram-vazados/

---

12 **DDOS · 05/11/2026**

### Serpro relata recorde de DDoS e nega impacto no Gov.br

A nota veio no mesmo dia em que um diretor da estatal falou em ataque sem precedentes, sem dar detalhes.

**Fonte:** Convergência Digital · 05/11/2026
https://convergenciadigital.com.br/governo/serpro-ultimo-semestre-marcou-o-maior-volume-de-ataques-ddos-da-historia-mas-sem-impacto-no-gov-br/

---

13 **CRIPTO · 02/11/2026**

### Mercado Bitcoin suspende saques após incidente de segurança

Empresas de blockchain estimam a saída de mais de US$ 46 milhões, número não confirmado pela corretora, que afirma não haver prejuízo a clientes.

**Fonte:** The Record · 02/11/2026
https://therecord.media/mercado-bitcoin-brazil-cryptocurrency-heist

---

14 **FRAUDE · 05/11/2026**

### Operação Fortuna Reversa prende 34 em dez estados e no DF

A apuração começou com fraude de mais de R$ 1,2 milhão contra uma lotérica no RS e teve apoio do Ciberlab, segundo a Agência Brasil.

**Fonte:** Agência Brasil, via Tribuna do Sertão · 05/11/2026
https://tribunadosertao.com.br/geral/2026/11/05/1014647-operacao-contra-fraudes-resulta-em-34-prisoes-em-dez-estados-e-no-df

| | |
|---|---|
| Radar Ciber Brasil<br>casos registrados no período | 37 |
| Radar Drogas Brasil<br>notícias mapeadas no período | 33 |

05 · TÉCNICA DA SEMANA

## Do IP à rede responsável, com a API pública do RIPEstat

A história dos proxies na rede da Casa Branca partiu de um dado aberto: o número do sistema autônomo. Com a API do RIPEstat, dá para ver quem anuncia um IP e quais blocos uma rede publica, sem tocar no alvo.

TERMINAL

```
# Mostra o bloco e a rede que anunciam um IP (exemplo: NIC.br)
curl -s "https://stat.ripe.net/data/prefix-overview/data.json?resource=200.160.2.3" | jq -r '.data.resource, .data.asns[].holder'

# Consulta o titular de um sistema autônomo
curl -s "https://stat.ripe.net/data/as-overview/data.json?resource=AS2650" | jq -r '.data.holder'

# Lista os blocos anunciados por essa rede
curl -s "https://stat.ripe.net/data/announced-prefixes/data.json?resource=AS2650" | jq -r '.data.prefixes[].prefix'
```

**Quando usar**

Para situar um IP visto em logs, cabeçalhos de e-mail ou alertas, e indicar a provável rede responsável em um relatório.

**Atenção**

O resultado mostra a rede, e não o usuário. Em CGNAT ou proxy residencial, um IP pode estar ligado a muitas pessoas. Identificar o assinante depende de ordem judicial. Guarde a saída com data e hora.

**Para ir além:** RIPEstat
https://stat.ripe.net/

06 · FERRAMENTA NO RADAR

## Whois do Registro.br

GRATUITA NAVEGADOR

Consulta pública mantida pelo Registro.br para domínios .br e recursos de numeração brasileiros. Ajuda a confirmar quem é o titular de um domínio ou de um bloco de endereços.

**Dica de Hunter.** Registre a data da consulta junto com o resultado: dados de registro mudam, e a ficha vale como retrato daquele momento. Dados de contato devem ficar fora do relatório quando não forem necessários.

Abrir a ferramenta →

https://registro.br/tecnologia/ferramentas/whois/

## 07 Mercado de trabalho OSINT

Quatro anúncios do LinkedIn conferidos em 06/11/2026 e um processo seletivo com prazo curto. Confirme requisitos e condições na página de cada oportunidade.

→ VAGA · SP

### Líder de Prevenção à Fraude e Investigação OSINT, Solva

Vaga afirmativa para mulheres, em tempo integral, nível pleno-sênior, na empresa de serviços compartilhados ligada à DiDi, que atua com prevenção de fraudes para a 99Pay.

**Fonte:** LinkedIn (Solva) · 06/11/2026
https://www.linkedin.com/jobs/view/4484078701/

→ VAGA · SP

### Analista Sênior de Threat Intelligence, BTG Pactual

Monitoramento e análise de ameaças externas, com foco em proteção de marca, takedown de domínios e perfis falsos e inteligência de ameaças.

**Fonte:** LinkedIn (BTG Pactual) · 06/11/2026 https://www.linkedin.com/jobs/view/4460133985/

---

VAGA · SP

### Analista Sênior de Cyber Intelligence, Itaú Unibanco

Monitoramento, identificação e análise de ameaças cibernéticas externas e internas que possam afetar ambiente, clientes e operações do banco.

**Fonte:** LinkedIn (Itaú Unibanco) · 06/11/2026
https://www.linkedin.com/jobs/view/4485252703/

---

VAGA · MG

### Cyber Threat Intelligence Specialist, Stellantis

Função em Belo Horizonte e região, com monitoramento, detecção e análise de ameaças para transformar dados em inteligência acionável.

**Fonte:** LinkedIn (Stellantis South America) · 06/11/2026
https://www.linkedin.com/jobs/view/4478608742/

---

CONCURSO · FEDERAL

### ABDI: Analista de Produtividade e Inovação, perfil Analista de Dados

Processo seletivo com banca FGV. Inscrições até 10/11, provas em 20/12. São 2 vagas e 16 em cadastro reserva nesse perfil, segundo o Estratégia Concursos; confira o edital.

**Fonte:** Estratégia Concursos · 20/10/2026
https://concursos.estrategia.com/portal/concurso-abdi/

---

## 08 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/

**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/

**03**
DEZ

CURSO

### Bellingcat: Online Masterclass in Visual Intelligence

On-line · 03 e 04/12 · pago, confira horários na página
https://www.bellingcat.com/workshops/online-masterclass-in-visual-intelligence-the-art-of-advanced-geolocation-2/

**14**
DEZ

WEBINAR

### Bellingcat: Tracking Organised Crime Through Open Sources

On-line · 14 e 15/12 · pago, confira horários na página
https://www.bellingcat.com/workshops/tracking-organised-crime-through-open-sources-webinar-2/

---

## 09 Para ler com calma

### The Rise of LLMJacking: How Threat Actors Monetize Compromised Cloud and Model Resources

Google Threat Intelligence Group e Mandiant · 02/11/2026

https://cloud.google.com/blog/topics/threat-intelligence/llmjacking-monetizing-compromised-cloud-models

### Poisoned Source: APT29 Watering Holes Targets Mobile Devices

Sekoia · 04/11/2026

https://www.sekoia.com/blog/poisoned-source-apt29-watering-holes-targets-mobile-devices-with-n-day-exploits

### Appraisal by AI: Model-driven victim prioritization in the VOLTA infostealer

Cisco Talos · 31/10/2026

https://blog.talosintelligence.com/appraisal-by-ai-model-driven-victim-prioritization-in-the-volta-infostealer/

---

◆ **NO PORTAL**

### Analista de threat intelligence: o que faz e como entrar na carreira

https://osinthunters.com.br/artigos/analista-de-threat-intelligence-o-que-faz-como-entrar-na-carreira

---

◆ **NO PORTAL**

### Google dorks para OSINT: operadores, exemplos e limites legais

https://osinthunters.com.br/artigos/google-dorks-osint-operadores-exemplos-limites-legais

---

◆ **NO PORTAL**

### Deepfake: como identificar vídeo e áudio gerados por IA

https://osinthunters.com.br/artigos/deepfake-como-identificar-video-audio-gerados-por-ia

---

◆ **NO PORTAL**

### Golpe do falso leilão: como verificar leiloeiro, site e pagamento

https://osinthunters.com.br/artigos/golpe-do-falso-leilao-como-verificar-leiloeiro-site-pagamento

---

## 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