Relatório de Threat Intelligence – Domínio **blackconviteexclusivo.com**

> **Fonte dos dados**: WHOIS.com, URLScan.io, VirusTotal, AlienVault OTX.
> **Última coleta VirusTotal**: 2025-10-04 (horário UTC da API).

1. Resumo Executivo

O domínio **blackconviteexclusivo.com** foi registrado em 26/09/2025 via GoDaddy, com privacidade de registro (Domains By Proxy). O único endereço IPv4 resolvido é **191.252.227.30**, pertencente ao ASN **AS27715 – Locaweb Serviços de Internet SA (Brasil)**. A página hospeda um site em português que exibe um blog de café, mas está marcada como **"suspect"** no URLScan.io e aparece em um *pulse* da AlienVault OTX que descreve uma campanha de **phishing bancário (Bradesco / American Express)** ativa desde outubro 2025.

Apesar de o domínio estar **"undetected"** em 95+ engines do VirusTotal, ele está associado a indicadores de phishing, uso de servidores de nuvem (Google Cloud Run, Linode/Akamai) e técnicas de **mascaramento** para ocultar tráfego de sistemas Linux. O certificado TLS (Let's Encrypt) tem validade de 89 dias, indicando renovação recente e uso típico em sites de curto-prazo.

Principais pontos de risco:

- Domínio incluído em campanha de phishing direcionada a instituições financeiras brasileiras.
- Endereço IP hospedado em infraestrutura brasileira (Locaweb) que pode ser usada como *C2* ou *landing page* para captura de credenciais.
- Histórico de comportamento suspeito (tag "suspect" no URLScan, presença em OTX).
- Possível uso de técnicas de **cloaking** e **dynamic resolution** (TTPs MITRE ATT&CK: T1036, T1056, T1071, T1566, T1568).

2. Análise de Comportamento

Evidência	Interpretação
URLScan.io – Tag "suspect"	Indica que o site apresenta características típicas de conteúdos mal-intencionados (ex.: redirecionamentos, carga de scripts suspeitos).
Título da página – "Giovani e Adenir Oliveira: da terra ao seu paladar — Blog Veroo Cafés"	Conteúdo aparentemente legítimo (blog), possivelmente usado como *camada de disfarce* para atrair vítimas.
Servidor – Apache/2.4.52 (Ubuntu)	Servidor padrão, comum em ambientes comprometidos ou em hosting barato.
TLS – Let's Encrypt, validade 89 dias	Certificado recente, prática comum em campanhas de phishing que criam domínios de curta vida.

Evidência	Interpretação
ASN – AS27715 (Locaweb)	Infra-estrutura de provedores de hospedagem no Brasil; pode ser compartilhada por múltiplos clientes, dificultando atribuição direta.
AlienVault OTX Pulse – "Phishing Bradesco / American Express – Campaign (Oct 2025)"	O domínio está listado como parte de uma campanha de coleta de credenciais bancárias (CPF, senha de 4 dígitos, etc.). O pulse descreve uso de: • **Google Cloud Run**, **RouterHosting LLC**, **Linode/Akamai** • **Mascaramento** para bloquear Linux OS • **Técnicas MITRE**: Masquerading, Input Capture, Application Layer Protocol, Phishing, Dynamic Resolution.
VirusTotal – 0 deteções, 34 "undetected"	Falta de assinaturas conhecidas, mas a ausência de deteções não exclui uso malicioso (campanhas frescas).
Whois – Registro privado, status "client delete/renew/transfer/update prohibited"	Impede alterações de registro, estratégia comum para dificultar a tomada de domínio.

Conclusão comportamental:
O domínio demonstra padrões típicos de **phishing** (uso de página aparentemente legítima, certificado renovado, registro privado) e está efetivamente citado em um *pulse* que associa o domínio a uma campanha de coleta de credenciais bancárias brasileiras. Não há evidências de botnet ou C2 ativo, mas o endereço IP pode servir como ponto de entrega (landing page) para a coleta de dados.

---

3. Informações de Rede e Geográficas

Campo	Valor
ASN	**AS27715 – Locaweb Serviços de Internet SA**
ISP / Provedor	**Locaweb** (provedor de hospedagem/infraestrutura)
IP resolvido	**191.252.227.30**
Cidade / Região	**Brasil** (dados de WHOIS não especificam cidade; IP geralmente geolocado em São Paulo – validar em base de geolocalização)
País	**Brasil (BR)**
Nome dos servidores DNS	`ns69.domaincontrol.com`, `ns70.domaincontrol.com` (GoDaddy)
Data de registro	26/09/2025
Data de expiração	26/09/2026
Status do domínio	client delete/renew/transfer/update prohibited

4. Domínios e IPs Relacionados

Tipo	Valor	Observação
IP principal	191.252.227.30	ASN AS27715 – Locaweb (BR)
Nameservers	ns69.domaincontrol.com / ns70.domaincontrol.com	Gerenciados por GoDaddy
Domínios citados em OTX	- (não explicitados, porém a campanha pode usar sub-domínios ou domínios associados a Google Cloud Run, Linode, Akamai)	
Domínios de infraestrutura	`googleusercontent.com`, `linode.com`, `akamai.net` (potenciais hosts de recursos CDN) – observar nos registros de solicitações HTTP.	
Domínios de referência	`domainsbyproxy.com` (provedor de privacidade), `godaddy.com` (registrar)	Não necessariamente maliciosos, mas parte do ecossistema de registro.
Outros IPs (uniqIPs no URLScan.io)	Não listados explicitamente – recomenda-se analisar os logs de URLScan para extrair.	

5. Recomendações de Follow-up (investigação)

1. **Correlacionar logs de rede** – Verificar se há conexões HTTP/HTTPS provenientes do IP **191.252.227.30** ou para ele em seus firewalls/IDS nos últimos 30 dias.
2. **Consultar feeds de ameaças** – Realizar buscas por `191.252.227.30`, `blackconviteexclusivo.com` e `AS27715` em fontes como AbuseIPDB, Spamhaus, Emerging Threats, Cisco Talos, etc.
3. **Passive DNS / DNS History** – Utilizar serviços (PassiveTotal, SecurityTrails) para identificar histórico de resoluções, sub-domínios e mudanças de IP.
4. **Análise de conteúdo da página** – Capturar o HTML/JS da landing page (via sandbox) e procurar por scripts de coleta de credenciais, chamadas a APIs externas (ex.: `api.php`).
5. **Verificar reputação de certificados** – Conferir a cadeia de confiança do certificado Let's Encrypt (emissão recente) e se há outras constelações de certificados semelhantes associadas a campanhas de phishing.
6. **Monitoramento contínuo** – Adicionar o domínio e o IP a watchlists internos (SIEM, EDR) e criar alertas de *DNS resolution* e *HTTP request* para detectar novas atividades.
7. **Compartilhar indicadores** – Enviar IOCs (domínio, IP, URI, hash de recursos) para plataformas de inteligência (MISP, ThreatConnect) e para a equipe de resposta a incidentes.
8. **Verificar outras campanhas OTX** – Avaliar se há mais *pulses* que referenciam o mesmo domínio ou IP, para entender se a campanha está em expansão.
9. **Análise de tráfego TLS** – Se houver captura de TLS, inspecionar o SNI e a negociação de certificados para confirmar uso de hostnames adicionais.

6. Conclusão

O domínio **blackconviteexclusivo.com** apresenta claras indicações de uso em uma campanha de **phishing bancário** focada no público brasileiro, associada a coleta de credenciais sensíveis (CPF, senhas, dados de cartões). Embora ainda não esteja listado como malicioso em várias engines antivírus, a presença no OTX e a classificação “suspect” no URLScan.io sugerem que ele deve ser tratado como **indicador de ameaça ativo**. Recomenda-se a monitorização constante, correlação com logs internos e a disseminação dos IOCs a equipes de defesa para prevenir possíveis comprometimentos.