



INVESTIGAÇÃO DE CAMPO · CASHCLOAK LATAM · CTI-LATAM-2026-001

Anúncios verificados, destinos que não coincidem

Como os falsos investimentos e os formulários de cartão chegam a usuários argentinos. Em dois dias de uso normal de um celular vi anúncios pagos, marcados como «Patrocinado» e com a identidade do anunciante verificada pelo Google, que levavam a falsas matérias jornalísticas, chatbots de investimento, formulários de cartão com a marca de uma corretora argentina e captação de telefones para um call center. As peças compartilham público, marcas e técnicas de persuasão, mas não um dono comprovado.

ID DO RELATÓRIO

CTI-LATAM-2026-001 · v2

AUTOREzequiel Jorge La Terra
[ORCID 0009-0008-1677-4218](https://orcid.org/0009-0008-1677-4218)**OBSERVAÇÃO**30/9 e 1/10/2026 (horário
da Argentina)**PUBLICAÇÃO**

outubro de 2026

**CLASSIFICAÇÃO ·
LICENÇA**

TLP: CLEAR · CC BY 4.0

ÍNDICE

01 Resumo executivo

02 Principais achados

03 O que é e o que não é

04 O que um anúncio verificado prova

05 O percurso

06 As verticais

07 O que compartilham

08 Demonstrado e não demonstrado

09 Impacto

10 Indicadores (IOCs)

11 MITRE ATT&CK

12 Recomendações

13 Método e limitações

14 Conclusão

15 Divulgação coordenada

16 Como citar e licença

▲ Não é uma quadrilha: é um mercado de tráfico

Entre 30 de setembro e 1º de outubro de 2026 (horário da Argentina) observei, como usuário comum, anúncios pagos dirigidos a usuários argentinos, muitos com a identidade do anunciante verificada pelo Google, que levavam a falsas matérias jornalísticas com chat de investimento, chatbots que simulam um «gestor pessoal» do Mercado Libre e um percurso de «CFD do Mercado Pago» que termina em captação para um call center. Nos mesmos dias documentei também um formulário de cartão com código de segurança que usa a marca Balanz sem ser a Balanz.

Os anunciantes declarados estão em pelo menos seis países (Reino Unido, Chipre, Países Baixos, Ucrânia, Austrália e Brasil) e não pude estabelecer um operador comum. A evidência descreve um **circuito de aquisição de tráfico**: compradores de tráfico e modelos que trabalham sobre o mesmo público, não uma pessoa nem um grupo. Para os defensores, isso significa que bloquear domínios ajuda, mas chega tarde: o ponto de intervenção mais cedo é o anúncio, e o mais concreto para um banco é a primeira operação do cliente em direção a uma «corretora» que ninguém conhece.

CASHCLOAK LATAM é o nome de acompanhamento que uso na Cyber Threat Intelligence LATAM para esta investigação. É um rótulo de trabalho, não o nome de um grupo nem de um ator.

▲ Sete achados

01 A porta de entrada é publicidade paga e verificada.

Anúncios do Google no navegador e no Gmail Promoções com a legenda «Identidade do anunciante verificada pelo Google». Essa verificação atesta quem paga o anúncio, não que a oferta seja legítima.

02 Os anunciantes declarados são muitos e estão dispersos.

Anunciantes declarados em pelo menos seis países (Reino Unido, Chipre, Países Baixos, Ucrânia, Austrália e Brasil), com anúncios dirigidos a usuários argentinos. Isso é coerente com um mercado de compradores de tráfico, não com um operador único.

03 O domínio do anúncio e o do destino podem não coincidir.

Um anúncio que mostrava um site de moda feminina levou a uma falsa matéria de investimento em outro domínio. Isso é compatível com um redirecionamento ou com cloaking; do lado do usuário não é possível determinar qual dos dois ocorreu.

04 O Mercado Libre é a marca mais usada como isca,
em pelo menos três formatos: falsa matéria com chat, chatbot de «gestor pessoal» e «CFD do Mercado Pago». Compartilhar a marca não demonstra que compartilhem operador.

05 Um site com a marca Balanz pede o cartão completo com código de segurança.
Não é a Balanz. Pedir o CVC em um formulário próprio para «depositar» é um sinal de risco grave, embora não tenha sido possível confirmar que cartões foram roubados.

06 Nem tudo o que aparece neste circuito é fraude.
Uma landing de «Guia de Créditos ANSES» mostrava conteúdo temático sem pedir dados sensíveis. Ela é incluída como contexto, não como phishing.

07 Um anúncio verificado apontava para um subdomínio genérico
que não remete a nenhuma marca conhecida. É publicado como indicador de busca, sem afirmar que conteúdo servia.

▲ 03 • ESCOPO

▲ O que esta publicação é e o que não é

Tudo o que descrevo eu vi como qualquer usuário veria: os anúncios exibidos em um celular, as informações que o Google oferece na «Minha Central de Anúncios» ao tocar nos três pontos de cada anúncio e as páginas que se abriam ao tocar no anúncio. Guardo as capturas de tela com seu hash criptográfico para que cada afirmação possa ser auditada.

Esta edição **não** atribui nada a pessoas, **não** afirma que os anunciantes declarados operem os sites de destino e **não** sustenta que todos os destinos pertençam a uma mesma operação. Também não afirma que Google, Mercado Libre, Balanz, YPF, La Nación, ANSES ou os bancos cujos logotipos aparecem tenham participado: são plataformas ou marcas usadas como isca.

OS PAPÉIS ANTES DOS NOMES

PAPEL	O QUE FAZ	O QUE NÃO IMPLICA
Anunciante declarado	Aparece como pagador do anúncio na «Minha Central de Anúncios», com país e identidade verificada	Não implica que desenhe a fraude, que controle o destino nem que saiba que conteúdo é servido
Domínio exibido	O site que aparece no anúncio	Pode ser um site de fachada, diferente do destino real
Destino ou landing	A página que efetivamente se abre	Pode mudar, alterar o conteúdo ou pertencer a um terceiro
Etapa de conversão	Chat, formulário de telefone, formulário de cartão	O tipo de etapa define o dano: um lead não é o mesmo que um CVC
Marca falsificada	Mercado Libre, Balanz, La Nación, YPF, bancos, ANSES	É vítima, não parte
Plataforma de publicidade	Serve o anúncio e publica o disclosure	Sua verificação é da identidade do pagador, não da oferta

Não nomeio nem identifico de nenhuma forma os anunciantes que aparecem como pagadores, nem indico de que tipo são; seus dados vão apenas para a plataforma, pelo canal de denúncia correspondente. Falo somente do país declarado, porque o que importa é o padrão e não quem aparece como titular.

▲ 04 • O SINAL DE CONFIANÇA

▲ O que um anúncio «verificado» prova e o que não prova

A «Minha Central de Anúncios» é uma das ferramentas de transparência mais úteis que um usuário tem: ao tocar em um anúncio do Google é possível ver quem o pagou, sua localização declarada e se sua identidade foi verificada. Em todos os anúncios relevantes que observei aparecia a legenda «Identidade do anunciante verificada pelo Google».

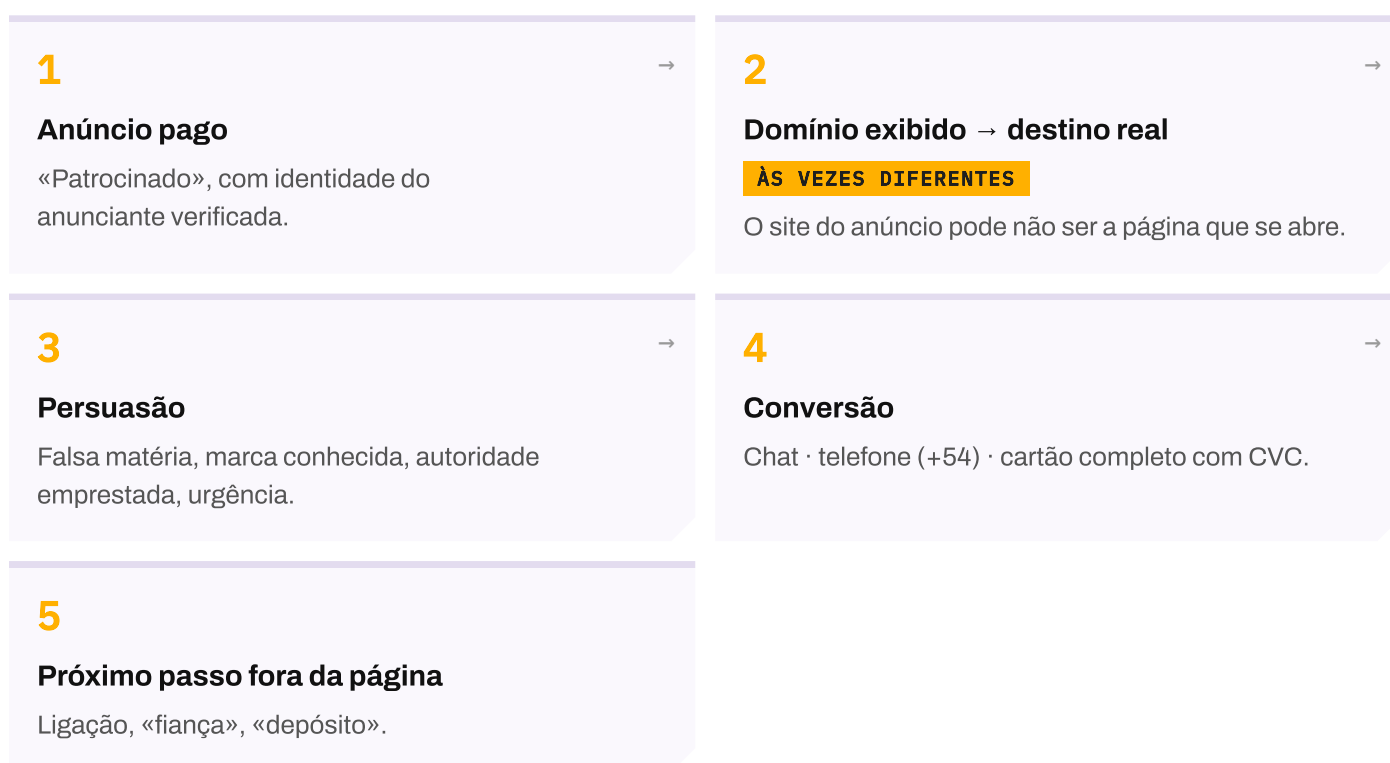
Essa informação prova que existe uma conta de publicidade cujo titular declarado passou pela verificação de identidade e pagou esse anúncio. **Não prova** que esse titular tenha desenhado o conteúdo de destino, que receba o dinheiro ou que opere o golpe: pode ser um afiliado que recebe por clique ou por lead, um intermediário ou alguém cuja identidade comercial foi usada por outro. Por isso trato o disclosure como um ponto de partida para a plataforma, não como uma atribuição.

O problema de fundo: o sinal de verificação descreve o pagador, mas o usuário o lê como se descrevesse a oferta. Um anúncio «verificado» que leva a uma matéria com o design de um jornal nacional é percebido como duplamente confiável.

▲ 05 • O PERCURSO

▲ Da atenção ao dado

As verticais observadas não percorrem todas as mesmas etapas, mas se encaixam em um esquema comum:



As setas descrevem o percurso de um usuário, não uma relação entre operadores. Que dois destinos compartilhem uma etapa não significa que sejam operados pela mesma pessoa.

▲ 06 • PERCURSO DOS ANÚNCIOS

▲ Seis verticais e um destino genérico

Vistas uma a uma, parecem golpes isolados. O que se observa é que quase todas chegaram pelo mesmo caminho: publicidade paga, exibida como «Patrocinado» no navegador, na aba Promoções do Gmail ou em redes de anúncios nativos. Alguns destinos pedem dados de cartão; outros, um telefone; outros só mostram conteúdo. Nem todos são fraude, e isso é esclarecido em cada caso.

A falsa matéria jornalística com chat de investimento

Um anúncio do Google mostrava um site de moda feminina; seu disclosure identificava como pagador um anunciante declarado na Ucrânia. Ao tocá-lo abriu-se `lunarbutton[.]site`, com uma matéria que imitava o design do La Nación: uma plataforma de investimento «vinculada ao Mercado Libre» e «endossada por figuras públicas» prometia 450% sobre um mínimo de 200.000 pesos. Em seguida vinha um chat com estética de WhatsApp, logotipos de bancos que operam na Argentina e a palavra-chave da fraude de adiantamento: uma «fiança» a pagar antes de receber.

Outro anúncio, com pagador declarado na Austrália, levava a uma falsa matéria com o mesmo design, que usava o nome de figuras públicas. A mudança de domínio é compatível com um redirecionamento ou com cloaking; não afirmo nenhum dos dois.

Por que importa. Uma revisão publicitária que olha o domínio exibido (um site de roupas) e não o destino final perde exatamente a etapa em que está a fraude.

O «gestor pessoal» do Mercado Libre

`epicharvest[.]info` chegou por um anúncio do Google com pagador declarado nos Países Baixos e identidade verificada. Era um chatbot que simulava um «gestor pessoal» do Mercado Libre, com planos de 5, 10 e 20 milhões de pesos, «verificado pela YPF», que prometia transformar 150.000 pesos em 5.000.000 por mês. Terminava em um formulário com prefixo +54 e uma página de «Obrigado!».

Avalio com **confiança moderada** que compartilha o modelo de chat com a vertical 1. Isso não basta para dizer que sejam operados pela mesma pessoa: esses modelos são vendidos e copiados.

Por que importa. O produto não é um pagamento imediato, e sim um contato: um telefone argentino disposto a ouvir uma oferta de investimento.

Formulários de captação com «alavancagem»

No Gmail Promoções, um banner do Mercado Libre oferecia operar com «alavancagem de 200:1» (anunciante declarado no Reino Unido). Outro anúncio (anunciante declarado em Chipre) levava a um formulário idêntico: mesmo design, depósito mínimo de 100 dólares e as mesmas carteiras eletrônicas. Avalio com **confiança moderada** que se trata de um mesmo modelo usado por dois pagadores, padrão típico das redes de afiliação de investimento de alto risco.

Não afirmo que essas páginas sejam fraudulentas; por isso seus domínios não são publicados como indicadores e ficam para a denúncia à plataforma.

Um cartão pedido para «depositar»

`app.balanztrading[.]com` usa a marca da Balanz, uma entidade financeira argentina real, com um formulário de «depósito» que pede número do cartão, titular, validade e código de segurança, acompanhado de selos de «Compatível com PCI-DSS» e 3-D Secure. **Não é a Balanz:** a marca falsificada é vítima. As capturas não registram qual anúncio levou a essa página, por isso ela não é associada a nenhum anunciante.

Pedir o CVC em um formulário próprio, fora de um processador de pagamentos reconhecível, é um sinal de risco grave. Não foi possível confirmar que cartões tenham sido roubados nem que tenham ocorrido cobranças.

Por que importa. Para um banco, um cartão cadastrado em um site assim é um cartão potencialmente comprometido antes da primeira cobrança suspeita.

«CFD do Mercado Pago» e o call center

Em redes de anúncios nativos (os blocos de «conteúdo recomendado» no rodapé de sites de notícias), três anunciantes diferentes ofereciam «CFD do Mercado Pago/Mercado Libre». O percurso: uma landing que imitava um «app de pagamentos» e pedia um telefone +54; depois `falcon-press[.]com`, com o aviso de que «um executivo de investimentos ligará para você»; por fim `lpa.voltfalcon-press[.]com`, com um identificador de subafiliado que não é publicado.

Avalio com **confiança moderada** que se trata de captação de interessados para um call center de investimento: a pressão e o pedido de dinheiro acontecem depois, por telefone.

Por que importa. Quando a conversão é um telefone, bloquear o domínio chega tarde. A defesa útil está antes (no anúncio) e depois (no alerta do banco diante da primeira transferência para uma «corretora»).

ANSES como gancho comercial, sem phishing observado

Publicidade com temática da ANSES no Gmail Promoções levava a uma landing «Guia de Créditos ANSES» em um subdomínio argentino de um site brasileiro (anunciante declarado no Brasil). O domínio não é publicado como indicador. Não se observou formulário de dados sensíveis nem pedido de pagamento. **Não é classificado como phishing.** É incluído como contexto porque usar um órgão da previdência social como gancho confunde um público especialmente exposto.

Um subdomínio sem marca, pago e verificado

Um anúncio «Patrocinado», de um anunciante declarado no Brasil com identidade verificada, levava a `descubre.upmegaconnectnotification[.]click`. Não há captura do conteúdo, por isso ele não é descrito nem recebe vertical. É publicado para **busca, não para bloqueio**, por três características: destino pago e verificado, nome genérico sem marca e extensão de baixo custo frequente em infraestrutura descartável.

▲ 07 • PADRÃO

▲ O que compartilham: um repertório, não um servidor

- **Autoridade emprestada.** Um jornal nacional, uma petroleira estatal, bancos, uma corretora, um órgão público, o maior marketplace da região.
- **Verificação como escudo.** O anúncio «verificado» transfere sua credibilidade ao destino, embora cubra apenas o pagador.

- **Promessas desproporcionais.** 450%, 150.000 pesos transformados em 5.000.000 por mês, alavancagem de 200:1.
- **Uma cobrança antecipada.** «Fiança», «depósito mínimo», «depositar com cartão».
- **Uma conversão que sai da página.** Chat, ligação, formulário: o dano se completa em um canal que a página não mostra.

Esse repertório é compatível com um mercado de modelos, afiliados e compradores de tráfego. Não foi possível estabelecer um operador comum, e a diversidade de pagadores e países sugere o contrário: muitos atores que competem pelas mesmas vítimas com as mesmas ferramentas.

▲ 08 • NÍVEL DE CERTEZA

▲ O que está demonstrado e o que não está

AFIRMAÇÃO	SITUAÇÃO
Houve anúncios pagos dirigidos a usuários argentinos com identidade do anunciante verificada pelo Google	OBSERVADO
Esses anúncios levavam a falsas matérias, chatbots de investimento, captação de telefones e um formulário de cartão com CVC	OBSERVADO
Pelo menos um anúncio mostrava um domínio e levava a outro	OBSERVADO
Esse salto se deve a cloaking	NÃO DETERMINADO Compatível com redirecionamento ou cloaking
Dois chatbots usam o mesmo modelo	AVALIAÇÃO • MODERADA
Dois formulários de captação usam o mesmo modelo	AVALIAÇÃO • MODERADA
O percurso de «CFD do Mercado Pago» alimenta um call center	AVALIAÇÃO • MODERADA
Os anunciantes declarados operam os destinos	NÃO ESTABELECIDO
Todas as verticais pertencem a uma mesma operação ou ator	NÃO ESTABELECIDO
Cartões foram roubados ou houve cobranças	NÃO CONFIRMADO
A landing da ANSES é phishing	NÃO Não se observou captura de dados sensíveis
Google, as marcas ou os bancos participam	NÃO São plataforma ou marcas falsificadas

▲ Quem é atingido e onde

Usuários. A fraude chega com todos os sinais de legitimidade que eles aprenderam a procurar: um buscador conhecido, o selo de verificação, o design de um jornal nacional, o logotipo do seu banco. «Desconfie de sites estranhos» não basta quando o site estranho chega envolto em sinais oficiais.

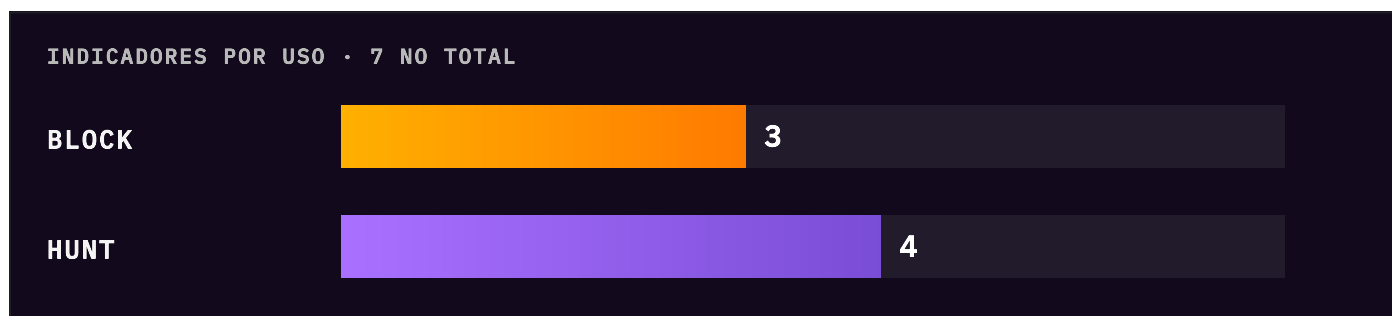
Marcas falsificadas. Dano de reputação e de atendimento: os usuários lesados reclamam com o Mercado Libre, com a Balanz ou com o seu banco, não com o anunciante.

Bancos e fintechs. O risco se materializa no cartão cadastrado em um formulário de «depósito» e nas transferências que se seguem à ligação de um «executivo de investimentos». Nos dois casos o primeiro indício chega ao banco antes de chegar a qualquer lista de bloqueio.

Plataformas de publicidade. O caso mostra o limite de verificar apenas a identidade do pagador quando o destino pode mudar ou não coincidir com o domínio exibido.

▲ Indicadores de comprometimento (IOCs)

Sete domínios, todos **desativados** com `[.]` (defang): **não os visite**. Para importá-los, substitua `[.]` por `. . first_seen` é a data da minha primeira observação (horário da Argentina), não a de criação do domínio.



INDICADOR	USO	VISTO	NOTA
<code>lunarbutton[.]site</code>	BLOCK	2026-10-01	Falsa matéria com o design do La Nación e chat de investimento com a marca Mercado Libre (mínimo de ARS 200.000, 450%, «fiança»). Acessado a partir de um anúncio do Google que mostrava outro domínio.
<code>epicharvest[.]info</code>	BLOCK	2026-09-30	Chatbot falso de «gestor pessoal» do Mercado Libre («verificado pela YPF»), formulário +54. Bloquear apenas o FQDN. Vínculo com os demais indicadores: não estabelecido.
<code>app.balanztrading[.]com</code>	BLOCK	2026-09-30	Formulário de «depósito» com a marca Balanz que pede cartão completo, titular, validade e CVC. Não é a Balanz. Bloquear apenas o FQDN; o domínio pai não é publicado como indicador.
<code>descubre.upmegaconnectnotification[.]click</code>	HUNT	2026-09-30	Destino de um anúncio do Google com identidade do anunciante verificada. Conteúdo não documentado. Apenas busca em registros.
<code>upmegaconnectnotification[.]click</code>	HUNT	2026-09-30	Domínio pai do anterior. Apenas busca; não bloquear (baixa especificidade pública).
<code>falcon-press[.]com</code>	HUNT	2026-10-01	Etapas de um percurso de «CFD do Mercado Pago» a partir de anúncios nativos («um executivo de investimentos ligará para você»). Avaliado como captação para call center. Apenas busca. Não se afirma quem é o titular do domínio.
<code>lpa.voltfalcon-press[.]com</code>	HUNT	2026-10-01	Etapas finais do mesmo percurso, com identificador de subafiliado (não publicado). Apenas busca. Não se afirma quem é o titular do domínio.

- **BLOCK** destinos com conteúdo fraudulento observado. Podem ser bloqueados por FQDN.

- **HUNT** buscar em registros de DNS e proxy; não bloquear sem análise própria.

▲ 11 • TÉCNICAS

▲ Mapeamento para o MITRE ATT&CK

O ATT&CK é usado apenas onde representa bem o que foi observado.

TÉCNICA	O QUE SE OBSERVOU
T1583.008 · Acquire Infrastructure: Malvertising	Anúncios pagos que levam a destinos de falso investimento
T1656 · Impersonation	Uso das marcas Mercado Libre, Balanz, La Nación, YPF e de bancos
T1056.003 · Input Capture: Web Portal Capture	Formulário de cartão com CVC (captura de dados não confirmada)

Como complemento, o [MITRE Fight Fraud Framework \(F3\)](#) é mais adequado que o ATT&CK Enterprise para descrever fraude financeira contra consumidores.

▲ 12 • RECOMENDAÇÕES

▲ O que fazer, segundo o papel

USUÁRIOS

- Antes de informar dados, convém olhar o endereço real da página, não o do anúncio.
- Convém desconfiar de qualquer rendimento garantido e de qualquer «fiança» para liberar ganhos.
- Nenhuma corretora legítima pede o código de segurança do cartão em um formulário próprio para «depositar».
- «Identidade verificada» fala de quem paga o anúncio, não da oferta.
- Se um anúncio parecer enganoso, denuncie-o a partir do próprio anúncio.

BANCOS, FINTECHS E MARCAS

Bancos e fintechs

Tratar como sinal de risco as primeiras transferências ou pagamentos com cartão para «corretoras» de CFD ou plataformas de investimento desconhecidas, sobretudo de clientes sem histórico de investimento. Avisar na comunicação com os clientes que ninguém legítimo pede o CVC para «depositar» nem uma «fiança».

Prevenção de fraude

Buscar os indicadores em registros de proxy e DNS e cruzar esses acessos com operações posteriores. Vigiar as palavras do roteiro nas reclamações: «fiança», «gestor pessoal», «verificado pela YPF», «um executivo ligará para você».

Marcas falsificadas

Monitorar o uso do seu nome em anúncios pagos com as ferramentas públicas de transparência publicitária e publicar canais oficiais claros sobre o que nunca pedem.

PLATAFORMAS E COMUNIDADE

Plataformas de publicidade

Revisar o destino final e não apenas o domínio exibido, e tratar a discrepância entre ambos como sinal. Comunicar ao usuário que a verificação cobre o pagador, não a oferta.

SOC e CTI

Bloquear os BLOCK, buscar sem bloquear os HUNT. Analisar os destinos com um perfil parecido com o da vítima (celular, conexão local, chegada a partir de um anúncio): de outro contexto pode ser exibida uma página diferente.

CERT e CSIRT

Receber os indicadores e, quando for o caso, coordenar com as marcas e com os registradores dos domínios marcados para bloqueio.

▲ 13 • MÉTODO E LIMITAÇÕES

▲ Como foi feito e até onde chega

MÉTODO

- **Observação passiva, como usuário.** Anúncios exibidos em um celular durante dois dias de uso normal (30/9 e 1/10/2026, horário da Argentina), no navegador, no Gmail Promoções e em redes de anúncios nativos.

- **Fonte do pagador.** As informações públicas da «Minha Central de Anúncios» do Google para cada anúncio: pagador declarado, localização e status de verificação.
- **Destinos.** Apenas as páginas que se abriram ao tocar no anúncio, documentadas com capturas guardadas com seu hash criptográfico.
- **Linguagem de certeza.** Cada afirmação é marcada como observada, avaliada (com nível de confiança) ou não estabelecida.

LIMITAÇÕES

- É uma amostra pequena: um celular, dois dias. **Não mede prevalência** nem alcance.
- Do lado do usuário não é possível distinguir um redirecionamento de um cloaking, nem saber o que outro visitante ou o revisor da plataforma vê.
- Não há captura do conteúdo do destino genérico, e não ficou registrado qual anúncio levou ao formulário com a marca Balanz.
- Não foram estabelecidas relações técnicas entre destinos; as coincidências de modelo são avaliações de confiança moderada.
- Não se sabe quem opera os destinos, se algum compartilha dono com outro nem quantas pessoas deixaram seus dados.
- Os destinos podem mudar ou alterar o conteúdo depois da observação.

▲ 14 • CONCLUSÃO

▲ A porta de entrada, não a infraestrutura

Esses golpes não se parecem pela infraestrutura, mas pela porta de entrada. Cada vertical isoladamente é conhecida: a falsa matéria, o chatbot de investimento, a corretora que pede o cartão. O que muda a leitura é vê-las juntas, nos mesmos dias, chegando por anúncios pagos e verificados, com pagadores em pelo menos seis países (Reino Unido, Chipre, Países Baixos, Ucrânia, Austrália e Brasil) e a mesma lista de marcas argentinas como isca.

A ameaça não é uma quadrilha, e sim um mercado: anunciantes que compram tráfego, modelos que são reutilizados e destinos que convertem a atenção em um telefone, um depósito ou um cartão. Bloquear domínios ajuda, mas chega depois. **Não uni o que a evidência não une.**

▲ 15 • DIVULGAÇÃO COORDENADA

▲ Divulgação coordenada

Antes da publicação, os achados foram notificados a equipes de resposta a incidentes da região e às marcas falsificadas.

▲ Como citar

La Terra, Ezequiel Jorge (2026). *CASHCLOAK LATAM: anúncios verificados e destinos de fraude de investimento e de cartão dirigidos a usuários argentinos* (CTI-LATAM-2026-001, edição pública v2). Cyber Threat Intelligence LATAM.
<https://cyberthreatintelligence.lat/pt/relatorio/cashcloak-latam/>

```
@techreport{laterra2026cashcloak,  
  author      = {La Terra, Ezequiel Jorge},  
  title       = {{CASHCLOAK LATAM}: anúncios verificados e destinos de fraude  
                de investimento e de cartão dirigidos a usuários argentinos},  
  institution = {Cyber Threat Intelligence LATAM},  
  number      = {CTI-LATAM-2026-001},  
  year        = {2026},  
  note        = {Edição pública v2, TLP:CLEAR},  
  url         = {https://cyberthreatintelligence.lat/pt/relatorio/cashcloak-latam/},  
}
```

LICENÇA

Textos e dados sob [Creative Commons Atribuição 4.0 Internacional \(CC BY 4.0\)](#). Podem ser reutilizados e adaptados, inclusive para fins comerciais, citando a autoria.

AVISO

Esta publicação descreve observações feitas como usuário e avaliações analíticas sinalizadas como tais. Não atribui responsabilidade a pessoas nem a empresas. Os anunciantes declarados são mencionados apenas pelo país e não se presumem responsáveis pelos destinos. As marcas e plataformas citadas são vítimas de falsificação ou prestadoras de um serviço, não partes. As correções são publicadas no [registro de correções](#), com a respectiva data.