

O que se sabe do malware bancário na América Latina, e em quem se apoia

Estes números descrevem o arquivo público do Atlas LATAM —não a prevalência de ataques—: de quantas fontes independentes cada família depende e onde se concentra o que foi publicado. Corte: 17.09.2026.

56 famílias

84 fontes primárias

26 sites

Dados em 17.09.2026

Ezequiel Jorge La Terra · cyberthreatintelligence.lat
contacto@cyberthreatintelligence.lat

Quatro achados

Metade das famílias apoia-se em um único relatório.

31 de 56 famílias têm um único relatório primário no índice. 22 têm dois e 3 têm três. Sem uma segunda fonte, não há contraste: se esse relatório falha ou desaparece, a ficha fica sem âncora.

Quatro vendedores concentram 54% das fontes.

Kaspersky (Securelist), ESET (WeLiveSecurity), ThreatFabric e Cleafy somam 45 de 84 fontes primárias. As outras 39 vêm de 22 sites. Uma mudança editorial em qualquer uma dessas quatro vozes reescreve o que o arquivo pode afirmar.

O Brasil concentra o mapa publicado — não o mapa de vítimas.

29 de 56 famílias mencionam o Brasil (52%). Apenas 7 de 27 territórios têm famílias documentadas; 20 estão vazios. «País mencionado» é o que a fonte nomeou, não a geografia da fraude.

O rótulo de nível de evidência não prioriza.

55 de 56 famílias figuram no nível A; só Hydra no B. Quando quase todas compartilham o mesmo rótulo, contar relatórios independentes distingue mais do que o nível máximo.

Como ler isto. Estes números descrevem o arquivo, não o mundo. Montei o arquivo com o que pude encontrar e documentar: quanto do viés vem do que se publica e quanto da minha busca não se pode separar com estes dados. Por isso o relatório mostra a dependência em vez de escondê-la.

O que foi contado e como

UNIDADE

Uma família de malware financeiro, ou uma plataforma de phishing como serviço, com menção de um país da região ou de «LATAM»: 56 linhas do índice mestre.

RELATÓRIOS POR FAMÍLIA

Quantos relatórios primários distintos figuram no índice para essa família, de 1 a 3.

O QUE ESTE RELATÓRIO NÃO DIZ

- Não mede prevalência nem infecções.
- Não ordena países nem fornecedores por risco ou por qualidade.
- Não inclui telemetria própria: tudo vem de fontes públicas.

FONTE PRIMÁRIA

O relatório técnico ou o alerta de um organismo que o índice registra como base da ficha. Cada família leva até três endereços canônicos; o índice não guarda mais.

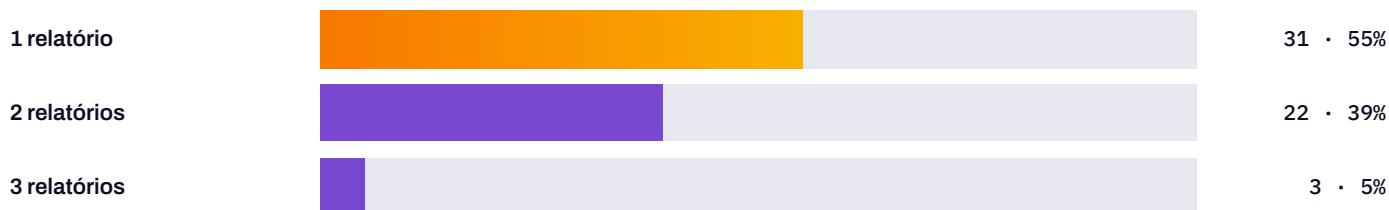
PAÍS

Os países que as fontes mencionam para a família. Não é a geografia das vítimas. Uma família pode figurar em vários países e com o rótulo regional «LATAM».

Metade das famílias apoia-se em um único relatório

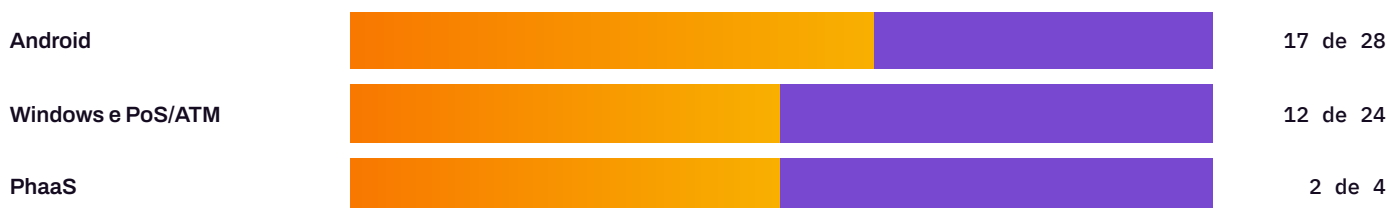
Uma família com um único relatório depende de que esse relatório esteja correto, continue disponível e não a descreva de forma diferente de outras fontes. Com dois ou mais, é possível contrastar.

FAMÍLIAS SEGUNDO QUANTOS RELATÓRIOS PRIMÁRIOS AS SUSTENTAM



POR PLATAFORMA – PROPORÇÃO COM UM ÚNICO RELATÓRIO

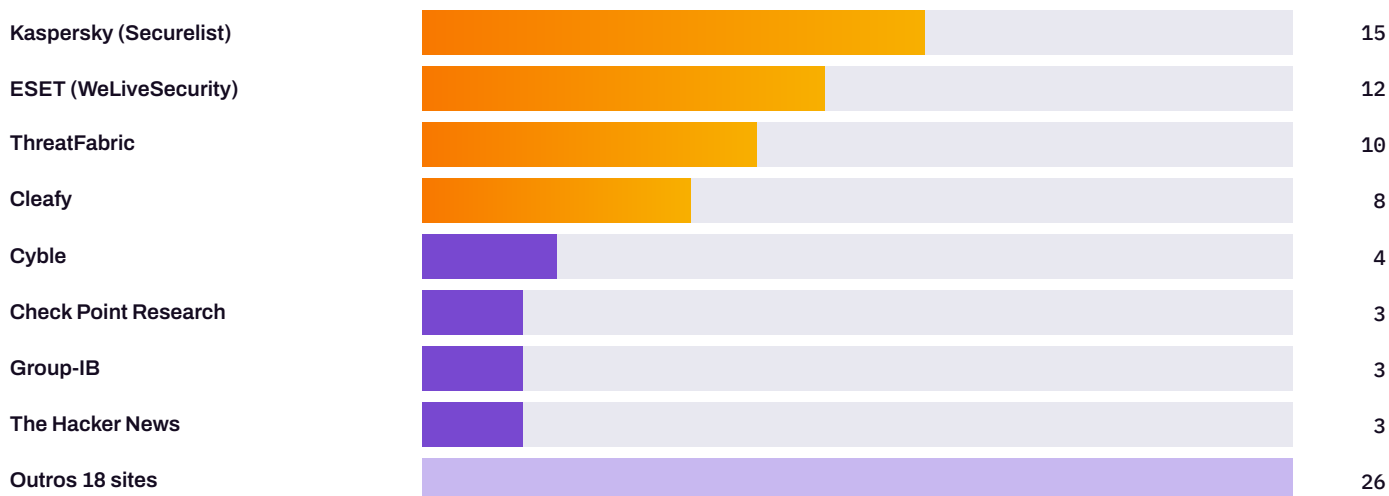
com um único relatório com 2 ou 3 relatórios



O Android concentra a dependência de fonte única (17 de 28). Windows/PoS/ATM e PhaaS ficam na metade (12 de 24 e 2 de 4). Isso não significa que essas famílias sejam menos reais: significa que a evidência pública reunida sobre elas é menos contrastável.

Quatro vendedores concentram 54% das fontes

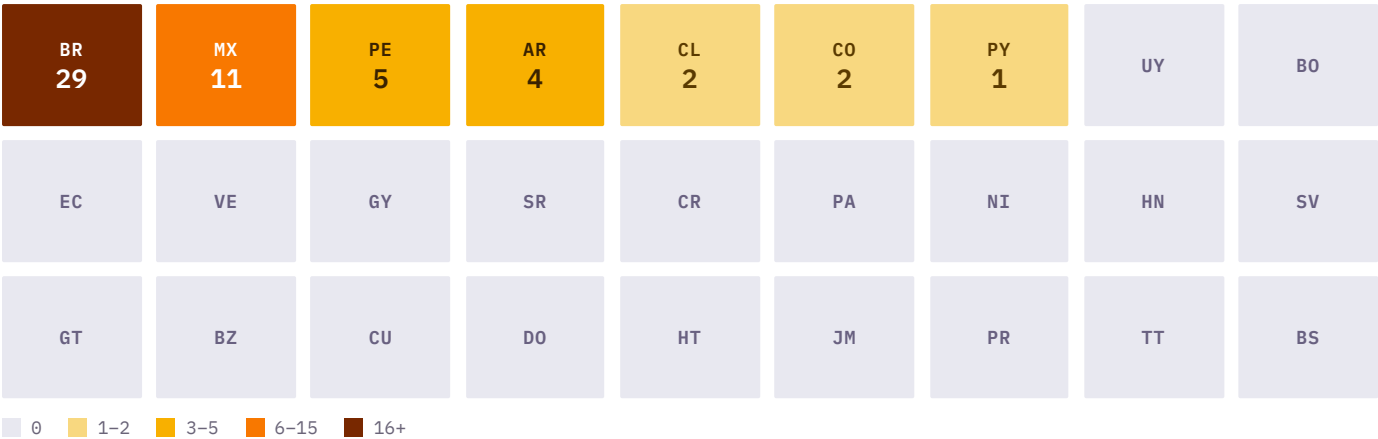
FONTES PRIMÁRIAS POR SITE



Os quatro primeiros somam 45 de 84 fontes (54%). O arquivo não pode dizer se pesam tanto porque publicam mais sobre a região ou porque eu as encontrei mais. Mostra sim que uma mudança no que qualquer uma delas publica mudaria o que o arquivo pode afirmar. The Hacker News aparece com 3 fontes: é um meio que resume pesquisas de outros, não um laboratório.

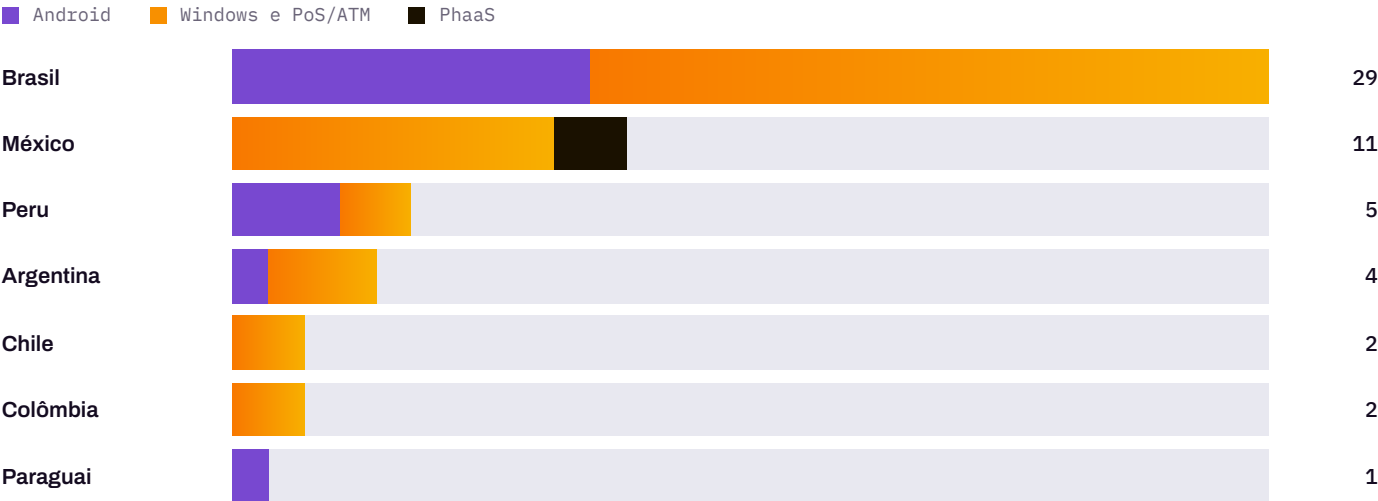
O Brasil concentra o mapa publicado

FAMÍLIAS MENCIONADAS POR TERRITÓRIO



Cada quadro é um território; o número são famílias mencionadas pelas fontes —não vítimas confirmadas. O Brasil aparece em 29 famílias (52%): 19 de Windows, incluindo PoS/ATM, e 10 de Android. O México soma 11 e o Peru 5.

FAMÍLIAS POR PAÍS E PLATAFORMA



15 famílias carregam o rótulo regional «LATAM» sem que a fonte diga em que país atuam. Que 20 territórios estejam vazios descreve o que foi publicado e o que encontrei, não onde há menos ataques.

O rótulo de nível de evidência não prioriza

O índice atribui a cada família um nível máximo de evidência. 55 de 56 estão no nível A e uma (Hydra) no B. Quando quase todas compartilham o mesmo rótulo, o rótulo não serve para priorizar. Contar relatórios independentes distingue mais.

► O que eu faria com isto

- **Equipe de fraude:** priorizar a triagem de famílias com um único relatório que toquem seus canais (Android, Windows/PoS ou PhaaS) e pedir ao fornecedor uma segunda fonte independente antes de elevá-las a playbook ou a lista de bloqueio permanente.
- **CISO:** em RFP ou renovação de threat intel, pedir desdobramento de fontes próprias vs. agregadas/terceiros. Este arquivo mostra que a cadeia pública é curta: quatro vendedores sustentam 54% das fontes.
- **Analista:** ao citar uma família, anotar o n de relatórios primários (1 / 2 / 3) junto ao nome. Não usar só o rótulo A/B: quase todas estão em A e esse rótulo não prioriza.

► Limites

- Isto descreve o arquivo. O arquivo fui eu quem montei; não posso separar o viés do que se publica do viés da minha busca.
- Uma das 24 entradas de Windows é um grupo de ameaças (Blind Eagle), não uma família. Mantém-se por continuidade do índice.
- Cada família guarda até três fontes primárias; a contagem de relatórios por família chega no máximo a 3.
- «País mencionado» não é a geografia das vítimas.
- Não há telemetria própria nem dados de perdas.

► Como citar

La Terra, E. J. (2026). O que se sabe do malware bancário na América Latina, e em quem se apoia. Cyber Threat Intelligence LATAM. Dados em 17 de setembro de 2026. <https://cyberthreatintelligence.lat/informe/>

Consultas e correções: contacto@cyberthreatintelligence.lat