Lo que se sabe del malware bancario en LATAM, y en quién se apoya

Estos números describen el archivo público de Atlas LATAM —no la prevalencia de ataques—: de cuántas fuentes independientes depende cada familia y dónde se concentra lo publicado. Corte: 17.09.2026.

56 familias | 84 fuentes primarias | 26 sitios | Datos al 17.09.2026

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

Cuatro hallazgos

La mitad de las familias descansa en un solo informe.
31 de 56 familias tienen un único informe primario en el índice. 22 tienen dos y 3 tienen tres. Sin segunda fuente, no hay contraste: si ese informe falla o desaparece, la ficha queda sin ancla.

Cuatro vendors concentran el 54% de las fuentes.
Kaspersky (Securelist), ESET (WeLiveSecurity), ThreatFabric y Cleafy suman 45 de 84 fuentes primarias. Las otras 39 salen de 22 sitios. Un cambio editorial en cualquiera de esas cuatro voces reescribe lo que el archivo puede afirmar.

Brasil concentra el mapa publicado — no el mapa de víctimas.
29 de 56 familias mencionan a Brasil (52%). Solo 7 de 27 territorios tienen familias documentadas; 20 están vacíos. «País mencionado» es lo que la fuente nombró, no la geografía del fraude.

La etiqueta de nivel de evidencia no prioriza.
55 de 56 familias figuran en nivel A; solo Hydra en B. Cuando casi todas comparten la misma etiqueta, contar informes independientes distingue más que el nivel máximo.

Cómo leer esto. Estos números describen el archivo, no el mundo. El archivo lo armé con lo que pude encontrar y documentar: cuánto del sesgo viene de lo que se publica y cuánto de mi búsqueda no se puede separar con estos datos. Por eso el informe muestra la dependencia en lugar de esconderla.

Qué se contó y cómo

UNIDAD

Una familia de malware financiero, o una plataforma de phishing como servicio, con mención de un país de la región o de «LATAM»: 56 filas del índice maestro.

INFORMES POR FAMILIA

Cuántos informes primarios distintos figuran en el índice para esa familia, de 1 a 3.

FUENTE PRIMARIA

El informe técnico o la alerta de un organismo que el índice registra como base de la ficha. Cada familia lleva hasta tres direcciones canónicas; el índice no guarda más.

PAÍS

Los países que las fuentes mencionan para la familia. No es la geografía de las víctimas. Una familia puede figurar en varios países y con la etiqueta regional «LATAM».

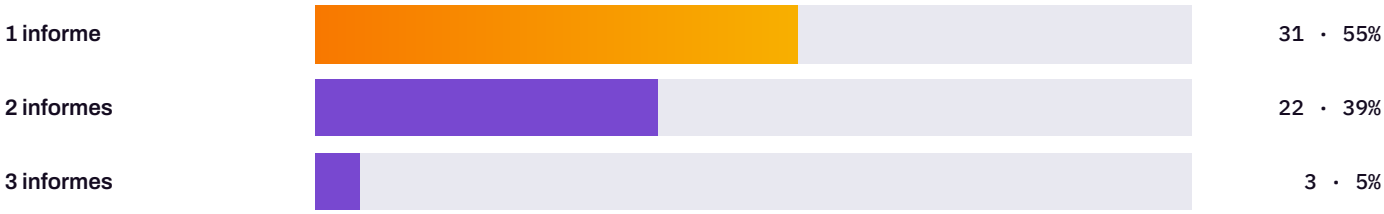
QUÉ NO DICE ESTE INFORME

- No mide prevalencia ni infecciones.
- No ordena países ni proveedores por riesgo o por calidad.
- No incluye telemetría propia: todo viene de fuentes públicas.

La mitad de las familias descansa en un solo informe

Una familia con un solo informe depende de que ese informe sea correcto, siga disponible y no la describa distinto de otras fuentes. Con dos o más, se puede contrastar.

FAMILIAS SEGÚN CUÁNTOS INFORMES PRIMARIOS LAS SOSTIENEN

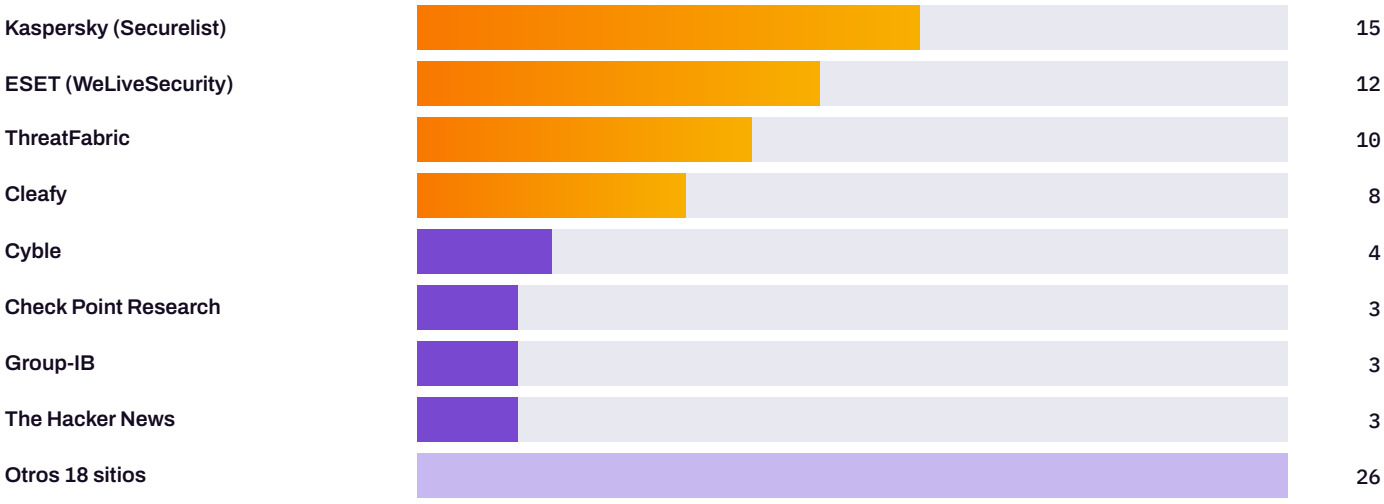


POR PLATAFORMA — PROPORCIÓN CON UN SOLO INFORME

Android concentra la dependencia de fuente única (17 de 28). Windows/PoS/ATM y PhaaS quedan en la mitad (12 de 24 y 2 de 4). No significa que esas familias sean menos reales: significa que la evidencia pública reunida sobre ellas es menos contrastable.

Cuatro vendors concentran el 54% de las fuentes

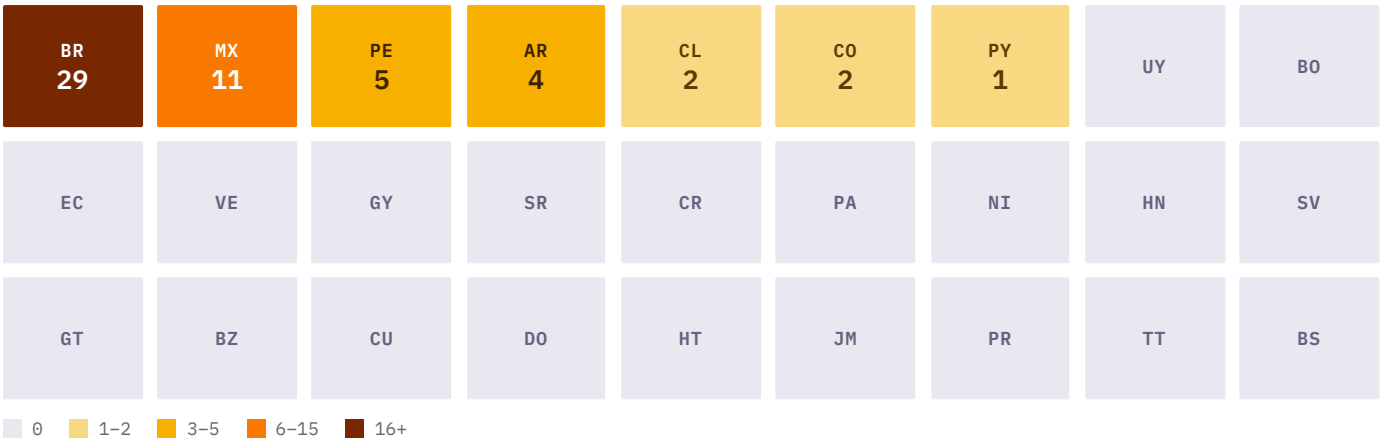
FUENTES PRIMARIAS POR SITIO



Los cuatro primeros suman 45 de 84 fuentes (54%). El archivo no puede decir si pesan tanto porque publican más sobre la región o porque yo las encontré más. Sí muestra que un cambio en lo que publica cualquiera de ellas cambiaría lo que el archivo puede afirmar. The Hacker News aparece con 3 fuentes: es un medio que resume investigaciones de otros, no un laboratorio.

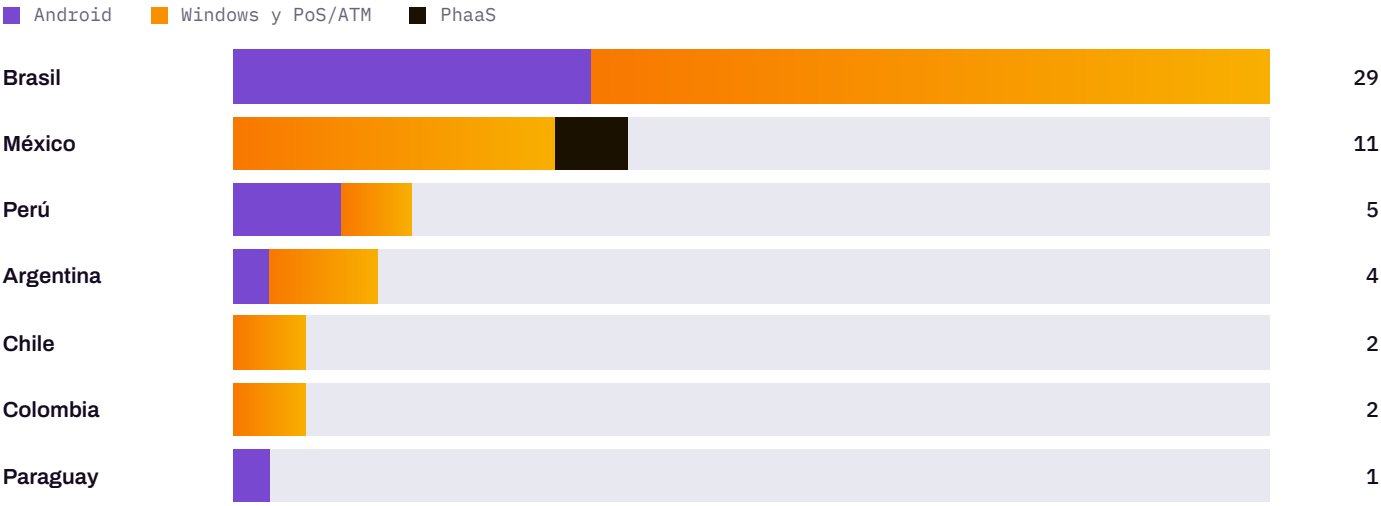
Brasil concentra el mapa publicado

FAMILIAS MENCIONADAS POR TERRITORIO



Cada cuadro es un territorio; el número son familias mencionadas por las fuentes —no víctimas confirmadas. Brasil aparece en 29 familias (52%): 19 de Windows, incluido PoS/ATM, y 10 de Android. México suma 11 y Perú 5.

FAMILIAS POR PAÍS Y PLATAFORMA



15 familias llevan la etiqueta regional «LATAM» sin que la fuente diga en qué país actúan. Que 20 territorios estén vacíos describe qué se publicó y qué encontré, no dónde hay menos ataques.

La etiqueta de nivel de evidencia no prioriza

El índice asigna a cada familia un nivel máximo de evidencia. 55 de 56 están en el nivel A y una (Hydra) en el B. Cuando casi todas comparten la misma etiqueta, la etiqueta no sirve para priorizar. Contar informes independientes distingue más.

Qué haría con esto

- **Equipo de fraude:** priorizar el triaje de familias con un solo informe que toquen tus canales (Android, Windows/PoS o PhaaS) y pedir al proveedor una segunda fuente independiente antes de elevarlas a playbook o a lista de bloqueo permanente.
- **CISO:** en RFP o renovación de threat intel, pedir desglose de fuentes propias vs. agregadas/terceros. Este archivo muestra que la cadena pública es corta: cuatro vendors sostienen el 54% de las fuentes.
- **Analista:** al citar una familia, anotar el n de informes primarios (1 / 2 / 3) junto al nombre. No usar solo la etiqueta A/B: casi todas están en A y esa etiqueta no prioriza.

Límites

- Esto describe el archivo. El archivo lo armé yo; no puedo separar el sesgo de lo publicado del sesgo de mi búsqueda.
- Una de las 24 entradas de Windows es un grupo de amenazas (Blind Eagle), no una familia. Se mantiene por continuidad del índice.
- Cada familia guarda hasta tres fuentes primarias; el conteo de informes por familia llega como máximo a 3.
- «País mencionado» no es la geografía de las víctimas.
- No hay telemetría propia ni datos de pérdidas.

Cómo citar

```
La Terra, E. J. (2026). Lo que se sabe del malware bancario en LATAM, y en quién se apoya. Cyber Threat Intelligence LATAM. Datos al 17 de septiembre de 2026. https://cyberthreatintelligence.lat/informe/
```

Consultas y correcciones: contacto@cyberthreatintelligence.lat