

What is known about banking malware in LATAM, and who it rests on

These numbers describe the public Atlas LATAM archive—not attack prevalence—: how many independent sources each family depends on, and where published coverage concentrates. Cutoff: 17.09.2026.

56 families

84 primary sources

26 sites

Data as of 17.09.2026

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

Four findings

Half of the families rest on a single report.

31 of 56 families have a single primary report in the index. 22 have two and 3 have three. Without a second source, there is no contrast: if that report fails or disappears, the entry is left without an anchor.

Four vendors account for 54% of the sources.

Kaspersky (Securelist), ESET (WeLiveSecurity), ThreatFabric and Cleafy add up to 45 of 84 primary sources. The other 39 come from 22 sites. An editorial shift at any of those four voices rewrites what the archive can assert.

Brazil concentrates the published map — not the victim map.

29 of 56 families mention Brazil (52%). Only 7 of 27 territories have documented families; 20 are empty. “Country mentioned” is what the source named, not the geography of fraud.

The evidence-level label does not prioritize.

55 of 56 families are at level A; only Hydra is at B. When almost all share the same label, counting independent reports distinguishes more than the maximum level.

How to read this. These numbers describe the archive, not the world. I built the archive from what I could find and document: how much of the bias comes from what gets published versus from my search cannot be separated with these data. That is why the report shows the dependency instead of hiding it.

What was counted and how

UNIT

A financial-malware family, or a phishing-as-a-service platform, with a mention of a country in the region or of “LATAM”: 56 rows in the master index.

REPORTS PER FAMILY

How many distinct primary reports appear in the index for that family, from 1 to 3.

WHAT THIS REPORT DOES NOT SAY

- It does not measure prevalence or infections.
- It does not rank countries or vendors by risk or by quality.
- It does not include proprietary telemetry: everything comes from public sources.

PRIMARY SOURCE

The technical report or agency alert that the index records as the basis of the entry. Each family carries up to three canonical URLs; the index does not keep more.

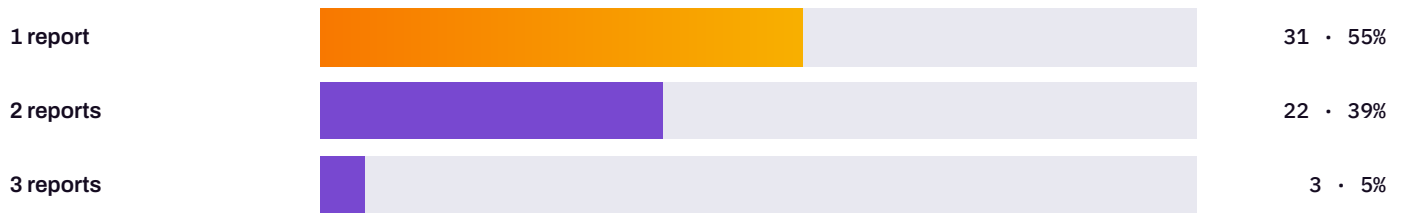
COUNTRY

The countries the sources mention for the family. It is not the geography of victims. A family may appear in several countries and under the regional label “LATAM”.

Half of the families rest on a single report

A family with a single report depends on that report being correct, remaining available, and not describing it differently from other sources. With two or more, contrast is possible.

FAMILIES BY HOW MANY PRIMARY REPORTS SUPPORT THEM



BY PLATFORM — SHARE WITH A SINGLE REPORT

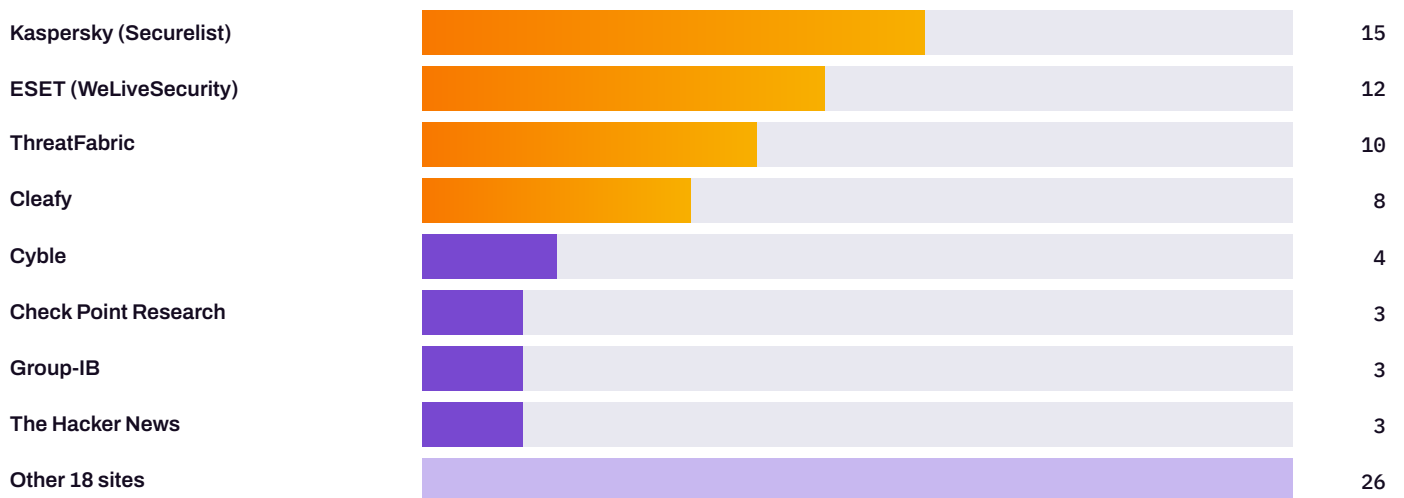
with a single report with 2 or 3 reports



Android concentrates single-source dependency (17 of 28). Windows/PoS/ATM and PhaaS sit at half (12 of 24 and 2 of 4). That does not mean those families are less real: it means the public evidence gathered on them is less contrastable.

Four vendors account for 54% of the sources

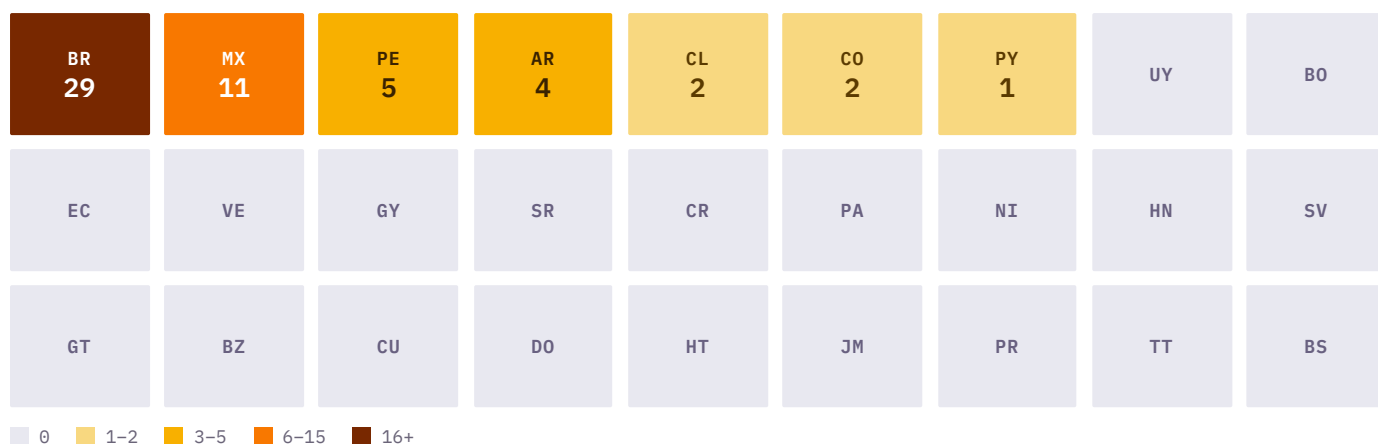
PRIMARY SOURCES BY SITE



The top four add up to 45 of 84 sources (54%). The archive cannot say whether they weigh so much because they publish more on the region or because I found them more often. It does show that a change in what any of them publishes would change what the archive can assert. The Hacker News appears with 3 sources: it is a medium that summarizes others' research, not a lab.

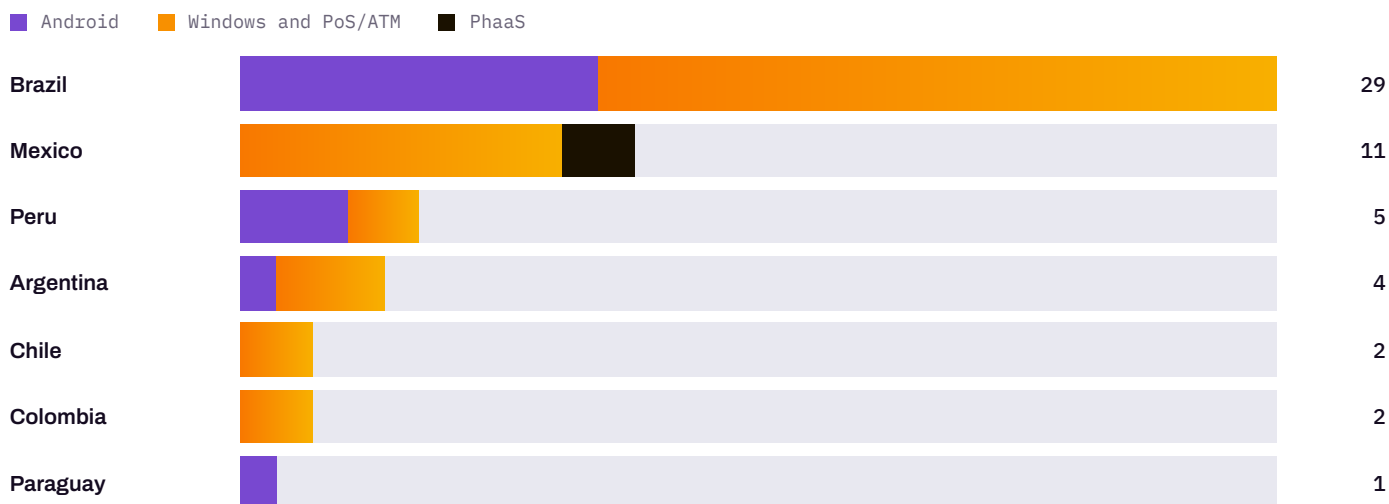
Brazil concentrates the published map

FAMILIES MENTIONED BY TERRITORY



Each tile is a territory; the number is families mentioned by the sources—not confirmed victims. Brazil appears in 29 families (52%): 19 Windows, including PoS/ATM, and 10 Android. Mexico totals 11 and Peru 5.

FAMILIES BY COUNTRY AND PLATFORM



15 families carry the regional label “LATAM” without the source saying in which country they operate. That 20 territories are empty describes what was published and what I found, not where there are fewer attacks.

The evidence-level label does not prioritize

The index assigns each family a maximum evidence level. 55 of 56 are at level A and one (Hydra) at B. When almost all share the same label, the label does not help prioritize. Counting independent reports distinguishes more.

▶ What I would do with this

- **Fraud team:** prioritize triage of single-report families that touch your channels (Android, Windows/PoS or PhaaS) and ask the vendor for a second independent source before elevating them to a playbook or a permanent block list.
- **CISO:** in an RFP or threat-intel renewal, ask for a breakdown of proprietary vs. aggregated/third-party sources. This archive shows that the public chain is short: four vendors hold 54% of the sources.
- **Analyst:** when citing a family, note the n of primary reports (1 / 2 / 3) next to the name. Do not rely on the A/B label alone: almost all are at A and that label does not prioritize.

▶ Limits

- This describes the archive. I built the archive; I cannot separate the bias of what gets published from the bias of my search.
- One of the 24 Windows entries is a threat group (Blind Eagle), not a family. It is kept for index continuity.
- Each family stores up to three primary sources; the per-family report count is capped at 3.
- “Country mentioned” is not the geography of victims.
- There is no proprietary telemetry and no loss data.

▶ How to cite

La Terra, E. J. (2026). What is known about banking malware in LATAM, and who it rests on. Cyber Threat Intelligence LATAM. Data as of 17 September 2026. <https://cyberthreatintelligence.lat/informe/>

Inquiries and corrections: contacto@cyberthreatintelligence.lat