

AiTM: the banking session theft that has not yet reached LATAM

Mechanism, 2022–2026 timeline and regulatory landscape of the region

3 cases worldwide

0 in LATAM

1,200+ domains (Tycoon 2FA)

Data as of Sep 24, 2026

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

▲ Four findings

The mechanism steals the already authenticated session, not the password.

Adversary-in-the-Middle (AiTM, MITRE ATT&CK T1557) lets the full login and second factor go through, and captures the session cookie at the moment the bank issues it.

An international takedown did not close the market: it reshaped it.

Microsoft and Europol dismantled 330 Tycoon 2FA domains in March 2026. The operators rebuilt within weeks; a newer competitor (Sneaky 2FA) gained ground.

Three 2026 platforms with a financial focus; none names LATAM.

Phoenix System (Group-IB), ZeroTokens (Abnormal AI) and UNC6671 (Google TIG/Mandiant) document AiTM against the financial sector. None mentions a country in the region.

The bank's app token does not solve this.

The proxy does not attack the origin of the code (SMS or app): it attacks the moment it is typed into a fake site. Only FIDO2/passkeys or push with detail verification resist.

How to read this. n=3 cases worldwide is not a sample that supports talking about a statistical trend: it is a documented absence in the corpus reviewed, not a law. The data point on the CNBV regulatory change on SMS rests on a single source (SILIKN) and needs a second independent confirmation before being treated as a firm fact.

▲ What was counted and how

UNIT

A phishing platform or kit with a documented AiTM mechanism (reverse proxy + post-MFA session cookie capture), worldwide, 2022–2026.

DOCUMENTED CASES

3 platforms with an explicit financial focus in 2026 (Phoenix System, ZeroTokens, UNC6671), plus the general reference kits (EvilProxy, Tycoon 2FA, Sneaky 2FA).

WHAT THIS REPORT DOES NOT SAY

- It does not predict that AiTM “will reach” LATAM within a given time frame.
- It does not measure what percentage of regional fraud already uses this mechanism without being identified as such.
- It does not include its own telemetry: everything comes from verified public sources.

PRIMARY SOURCE

The technical report from the vendor or security firm that documented the case, re-read directly, not a search summary.

TARGET COUNTRY

The country the source explicitly names. Absence of mention is not equivalent to absence of activity, only to absence of public documentation found.

▲ How the mechanism works

Unlike classic phishing, which steals a static password, AiTM lets the full authentication go through—including the second factor—because the victim is using the real bank through an invisible proxy.

THE SIX STEPS OF SESSION THEFT



Step 6 is the central difference from classic phishing: the attacker does not need the password or the code again. They operate with the session already validated by the bank itself.

▲ From a kit to an industry that survives the police

TIMELINE 2022–2026

EvilProxy
May 2022

Sneaky 2FA
Dec 2024

MS+Europol takedown
Mar 2026



Tycoon 2FA accumulated more than 1,200 domains since 2023. The March 2026 takedown (330 domains seized) did not end the model: within weeks the operators rebuilt infrastructure and added device-code OAuth abuse. Sneaky 2FA, newer and cheaper (~USD 200/month via a Telegram bot), gained ground in parallel.

▲ Three documented cases, zero in LATAM

AITM PLATFORMS WITH A FINANCIAL FOCUS, 2026

Phoenix System Group-IB · 2026-04-29		Financial vertical top 3 · no country
ZeroTokens Abnormal AI · 2026-08-25		53 brands · only country: Australia
UNC6671 / BlackFile Google TIG/Mandiant · 2026-08-06		Vishing + AiTM · financial sector

The three sources are organizations independent of each other (Group-IB, Abnormal AI, Google TIG/Mandiant). None documents a Latin American bank, fintech or country as a target.

▲ The regulatory landscape: advances and setbacks at the same time

MEASURES BY COUNTRY, 2026

	Biometrics	SMS enabled	Cloud / Pix	CERT AiTM alert
Mexico	 YES	 YES*	 —	 —
Brazil	 —	 —	 YES	 —
Rest of LATAM	 —	 —	 —	 —

 verified advance
  advance with risk (SMS does not resist AiTM)
  no measure found

* The CNBV change on SMS is confirmed by a single source (SILIKN, 2026-09-04); a second independent confirmation is missing. According to what was reviewed, no country in the region has a CERT alert specific to AiTM.

▲ What I would do with this

- **Fraud team:** check whether any actor already active in the region (operator-driven RAT, vishing) could add a rented AiTM kit as an upgrade — it is the path of least friction.
- **CISO:** assess migration to FIDO2/passkeys or push with transaction-detail verification, at least for higher-value operations. The current app token does not resist this vector.
- **Analyst:** add the AiTM scenario to threat modeling even though there is no confirmed case yet; documented absence is not equivalent to absence of installed capability.

▲ Limits

- n=3 cases worldwide with a financial focus does not support talking about a statistical trend or a probability of arrival in the region.
- The CNBV regulatory change on SMS rests on a single source; it could not be independently confirmed at the time of this report.
- The absence of a CERT alert was not verified by reviewing each agency's full archive, only through a dedicated search with no result.
- It was not determined whether any PhaaS kit already documented in LATAM has latent AiTM capability not yet exploited against banks in the region.

▲ How to cite

La Terra, E. J. (2026). AiTM: the banking session theft that has not yet reached LATAM. Cyber Threat Intelligence LATAM. Data as of September 24, 2026. <https://cyberthreatintelligence.lat/en/blog/>

Questions and corrections: contacto@cyberthreatintelligence.lat