CYBER THREAT INTELLIGENCE LATAM · INFORME TÉCNICO 2026

AiTM: el robo de sesión bancaria que todavía no llegó a LATAM

Mecanismo, cronología 2022–2026 y panorama regulatorio de la región

3 casos mundiales | 0 en LATAM | 1.200+ dominios (Tycoon 2FA) | Datos al 24.09.2026

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

Cuatro hallazgos

El mecanismo roba la sesión ya autenticada, no la contraseña.
Adversary-in-the-Middle (AiTM, MITRE ATT&CK T1557) deja pasar el login y el doble factor completos, y captura la cookie de sesión en el instante en que el banco la emite.

Un takedown internacional no cerró el mercado: lo reordenó.
Microsoft y Europol desmantelaron 330 dominios de Tycoon 2FA en marzo de 2026. Los operadores reconstruyeron en semanas; un competidor más nuevo (Sneaky 2FA) ganó terreno.

Tres plataformas de 2026 con foco financiero, ninguna nombra a LATAM.
Phoenix System (Group-IB), ZeroTokens (Abnormal AI) y UNC6671 (Google TIG/Mandiant) documentan AiTM contra el sector financiero. Cero mencionan un país de la región.

El token de la app del banco no resuelve esto.
El proxy no ataca el origen del código (SMS o app): ataca el instante en que se escribe en un sitio falso. Solo FIDO2/passkeys o push con verificación de detalle resisten.

Cómo leer esto. n=3 casos mundiales no es una muestra que permita hablar de tendencia estadística: es una ausencia documentada en el corpus revisado, no una ley. El dato del cambio regulatorio de la CNBV sobre SMS está sostenido en una sola fuente (SILIKN) y falta una segunda confirmación independiente antes de tratarlo como hecho firme.

Qué se contó y cómo

UNIDAD

Una plataforma o kit de phishing con mecanismo AiTM documentado (proxy inverso + captura de cookie de sesión post-MFA), mundial, 2022–2026.

CASOS DOCUMENTADOS

3 plataformas con foco financiero explícito en 2026 (Phoenix System, ZeroTokens, UNC6671), más los kits de referencia general (EvilProxy, Tycoon 2FA, Sneaky 2FA).

FUENTE PRIMARIA

El informe técnico del vendor o de la firma de seguridad que documentó el caso, releído directamente, no un resumen de búsqueda.

PAÍS OBJETIVO

El país que la fuente nombra explícitamente. Ausencia de mención no equivale a ausencia de actividad, solo a ausencia de documentación pública encontrada.

QUÉ NO DICE ESTE INFORME

- No predice que AiTM «va a llegar» a LATAM en un plazo determinado.
- No mide qué porcentaje del fraude regional ya usa este mecanismo sin ser identificado como tal.
- No incluye telemetría propia: todo viene de fuentes públicas verificadas.

▲ Cómo funciona el mecanismo

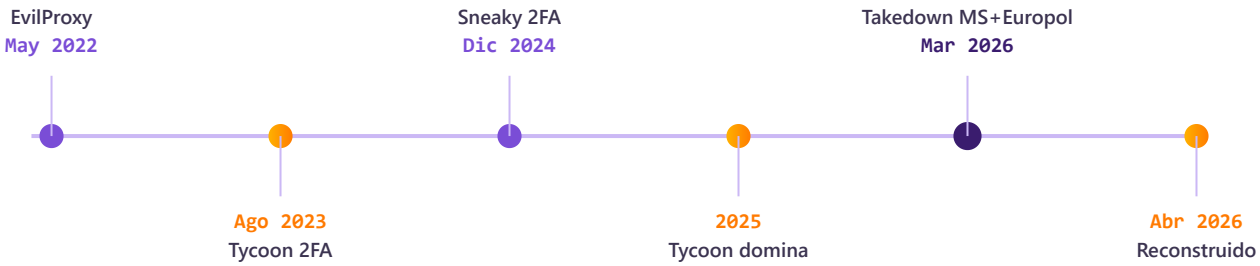
A diferencia del phishing clásico, que roba una contraseña estática, AiTM deja pasar la autenticación completa — incluido el doble factor— porque la víctima está usando el banco real a través de un proxy invisible.

LOS SEIS PASOS DEL ROBO DE SESIÓN

El paso 6 es la diferencia central con el phishing clásico: el atacante no necesita la contraseña ni el código otra vez. Opera con la sesión ya validada por el propio banco.

▲ De un kit a una industria que sobrevive a la policía

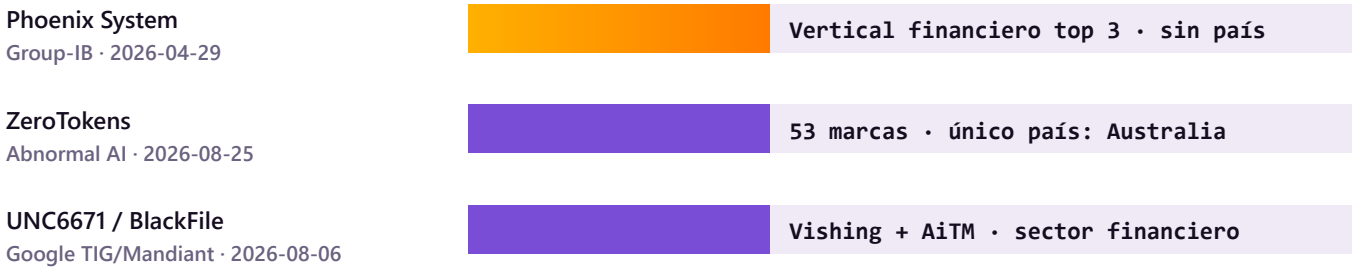
CRONOLOGÍA 2022–2026



Tycoon 2FA acumuló más de 1.200 dominios desde 2023. El takedown de marzo de 2026 (330 dominios incautados) no terminó con el modelo: en semanas los operadores reconstruyeron infraestructura y sumaron abuso de OAuth por código de dispositivo. Sneaky 2FA, más nuevo y más barato (~USD 200/mes vía bot de Telegram), ganó terreno en paralelo.

▲ Tres casos documentados, cero en LATAM

PLATAFORMAS AITM CON FOCO FINANCIERO, 2026



Las tres fuentes son organizaciones independientes entre sí (Group-IB, Abnormal AI, Google TIG/Mandiant). Ninguna documenta un banco, fintech o país de Latinoamérica como objetivo.

▲ El panorama regulatorio: avances y retrocesos en simultáneo

MEDIDAS POR PAÍS, 2026

* El cambio de la CNBV sobre SMS está confirmado en una sola fuente (SILIKN, 2026-09-04); falta segunda confirmación independiente. Ningún país de la región tiene, según lo revisado, una alerta de CERT específica sobre AiTM.

▲ Qué haría con esto

- **Equipo de fraude:** mirar si algún actor ya activo en la región (RAT con operador, vishing) podría incorporar un kit AiTM alquilado como upgrade — es el camino de menor fricción.
- **CISO:** evaluar migración hacia FIDO2/passkeys o push con verificación de detalle transaccional, al menos en operaciones de mayor valor. El token de app actual no resiste este vector.
- **Analista:** incorporar el escenario AiTM al threat modeling aunque no haya caso confirmado todavía; la ausencia documentada no equivale a ausencia de capacidad instalada.

▲ Límites

- n=3 casos mundiales con foco financiero no permite hablar de tendencia estadística ni de probabilidad de llegada a la región.
- El cambio regulatorio de la CNBV sobre SMS se sostiene en una sola fuente; no se pudo confirmar de forma independiente al momento de este informe.
- La ausencia de alerta de CERT no fue verificada revisando el archivo completo de cada organismo, solo mediante búsqueda dedicada sin resultado.
- No se determinó si algún kit PhaaS ya documentado en LATAM tiene capacidad AiTM latente no explotada todavía contra bancos de la región.

▲ Cómo citar

> La Terra, E. J. (2026). AiTM: el robo de sesión bancaria que todavía no llegó a LATAM. Cyber Threat Intelligence LATAM. Datos al 24 de septiembre de 2026. https://cyberthreatintelligence.lat/blog/

Consultas y correcciones: contacto@cyberthreatintelligence.lat