

AiTM: o roubo de sessão bancária que ainda não chegou à América Latina

Mecanismo, cronologia 2022–2026 e panorama regulatório da região

3 casos no mundo

0 na América Latina

1.200+ domínios (Tycoon 2FA)

Dados até 24/09/2026

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

▲ Quatro descobertas

O mecanismo rouba a sessão já autenticada, não a senha.

Adversary-in-the-Middle (AiTM, MITRE ATT&CK T1557) deixa passar o login e o segundo fator completos e captura o cookie de sessão no instante em que o banco o emite.

Um takedown internacional não fechou o mercado: reorganizou-o.

A Microsoft e a Europol desmantelaram 330 domínios do Tycoon 2FA em março de 2026. Os operadores reconstruíram em semanas; um concorrente mais novo (Sneaky 2FA) ganhou terreno.

Três plataformas de 2026 com foco financeiro; nenhuma cita a América Latina.

Phoenix System (Group-IB), ZeroTokens (Abnormal AI) e UNC6671 (Google TIG/Mandiant) documentam AiTM contra o setor financeiro. Nenhuma menciona um país da região.

O token do aplicativo do banco não resolve isso.

O proxy não ataca a origem do código (SMS ou aplicativo): ataca o instante em que ele é digitado em um site falso. Só FIDO2/passkeys ou push com verificação de detalhes resistem.

Como ler isto. n=3 casos no mundo não é uma amostra que permita falar de tendência estatística: é uma ausência documentada no corpus revisado, não uma lei. O dado da mudança regulatória da CNBV sobre SMS se apoia em uma única fonte (SILIKN) e falta uma segunda confirmação independente antes de tratá-lo como fato firme.

▲ O que foi contado e como

UNIDADE

Uma plataforma ou kit de phishing com mecanismo AiTM documentado (proxy reverso + captura de cookie de sessão pós-MFA), mundial, 2022–2026.

CASOS DOCUMENTADOS

3 plataformas com foco financeiro explícito em 2026 (Phoenix System, ZeroTokens, UNC6671), mais os kits de referência geral (EvilProxy, Tycoon 2FA, Sneaky 2FA).

O QUE ESTE RELATÓRIO NÃO DIZ

- Não prevê que o AiTM «vai chegar» à América Latina em um prazo determinado.
- Não mede que porcentagem da fraude regional já usa esse mecanismo sem ser identificada como tal.
- Não inclui telemetria própria: tudo vem de fontes públicas verificadas.

FONTE PRIMÁRIA

O relatório técnico do fornecedor ou da empresa de segurança que documentou o caso, relido diretamente, não um resumo de busca.

PAÍS-ALVO

O país que a fonte cita explicitamente. Ausência de menção não equivale a ausência de atividade, apenas a ausência de documentação pública encontrada.

▲ Como o mecanismo funciona

Diferentemente do phishing clássico, que rouba uma senha estática, o AiTM deixa passar a autenticação completa —incluindo o segundo fator— porque a vítima está usando o banco real por meio de um proxy invisível.

OS SEIS PASSOS DO ROUBO DE SESSÃO



O passo 6 é a diferença central em relação ao phishing clássico: o atacante não precisa da senha nem do código outra vez. Opera com a sessão já validada pelo próprio banco.

▲ De um kit a uma indústria que sobrevive à polícia

CRONOLOGIA 2022–2026

EvilProxy
Mai 2022

Sneaky 2FA
Dez 2024

Takedown MS+Europol
Mar 2026



O Tycoon 2FA acumulou mais de 1.200 domínios desde 2023. O takedown de março de 2026 (330 domínios apreendidos) não acabou com o modelo: em semanas os operadores reconstruíram a infraestrutura e somaram abuso de OAuth por código de dispositivo. O Sneaky 2FA, mais novo e mais barato (~USD 200/mês via bot do Telegram), ganhou terreno em paralelo.

▲ Três casos documentados, zero na América Latina

PLATAFORMAS AITM COM FOCO FINANCEIRO, 2026

Phoenix System Group-IB · 2026-04-29		Vertical financeiro top 3 · sem país
ZeroTokens Abnormal AI · 2026-08-25		53 marcas · único país: Austrália
UNC6671 / BlackFile Google TIG/Mandiant · 2026-08-06		Vishing + AiTM · setor financeiro

As três fontes são organizações independentes entre si (Group-IB, Abnormal AI, Google TIG/Mandiant). Nenhuma documenta um banco, fintech ou país da América Latina como alvo.

▲ O panorama regulatório: avanços e retrocessos ao mesmo tempo

MEDIDAS POR PAÍS, 2026

	Biometria	SMS habilitado	Nuvem / Pix	Alerta CERT AiTM
México	SIM	SIM*	—	—
Brasil	—	—	SIM	—
Resto da AL	—	—	—	—

■ avanço verificado ■ avanço com risco (SMS não resiste ao AiTM) ■ nenhuma medida encontrada

* A mudança da CNBV sobre SMS está confirmada por uma única fonte (SILIKN, 2026-09-04); falta uma segunda confirmação independente. Nenhum país da região tem, segundo o revisado, um alerta de CERT específico sobre AiTM.

▲ O que eu faria com isto

- **Equipe de fraude:** verificar se algum ator já ativo na região (RAT com operador, vishing) poderia incorporar um kit AiTM alugado como upgrade — é o caminho de menor atrito.
- **CISO:** avaliar a migração para FIDO2/passkeys ou push com verificação de detalhes da transação, ao menos nas operações de maior valor. O token de aplicativo atual não resiste a esse vetor.
- **Analista:** incorporar o cenário AiTM ao threat modeling mesmo que ainda não haja caso confirmado; a ausência documentada não equivale a ausência de capacidade instalada.

▲ Limites

- n=3 casos no mundo com foco financeiro não permite falar de tendência estatística nem de probabilidade de chegada à região.
- A mudança regulatória da CNBV sobre SMS se apoia em uma única fonte; não foi possível confirmá-la de forma independente no momento deste relatório.
- A ausência de alerta de CERT não foi verificada revisando o arquivo completo de cada órgão, apenas por meio de busca dedicada sem resultado.
- Não se determinou se algum kit PhaaS já documentado na América Latina tem capacidade AiTM latente ainda não explorada contra bancos da região.

▲ Como citar

La Terra, E. J. (2026). AiTM: o roubo de sessão bancária que ainda não chegou à América Latina. Cyber Threat Intelligence LATAM. Dados até 24 de setembro de 2026. <https://cyberthreatintelligence.lat/pt/blog/>

Consultas e correções: contacto@cyberthreatintelligence.lat