Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:58:23 UTC

Tool: TrickMo

Names	TrickMo
Category	Malware
Type	Banking trojan, Loader
Description	(IBM) IBM X-Force researchers analyzed an Android malware app that's likely being pushed to infected users by the TrickBot Trojan. This app, dubbed "TrickMo" by our team, is designed to bypass second factor and strong authentication pushed to bank customers when they need to authorize a transaction. While it's not the first of its kind, this Android malware app is more sophisticated than similar apps and possesses interesting features that enable its operators to steal transaction authorization codes from victims who download the app.
Information	<https://securityintelligence.com/posts/trickbot-pushing-a-2fa-bypass-app-to-bank-customers-in-germany/> <https://www.cleafy.com/cleafy-labs/a-new-trickmo-saga-from-banking-trojan-to-victims-data-leak> <https://www.zimperium.com/blog/expanding-the-investigation-deep-dive-into-latest-trickmo-samples/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0427/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.trickmo>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:TrickMo>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool TrickMo

Changed	Name	Country	Observed

APT groups

	Wizard Spider, Gold Blackburn		2014-May 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6bedcca0-561d-48a0-942f-bf68911e53d8