Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:53:46 UTC

Tool: GoldPickaxe

Names	GoldPickaxe
Category	Malware
Type	Banking trojan
Description	(Group-IB) The GoldPickaxe family, which includes versions for iOS and Android, is based on the GoldDigger Android Trojan and features regular updates designed to enhance their capabilities and evade detection. GoldPickaxe.iOS, Group-IB researchers found, is capable of collecting facial recognition data, identity documents, and intercepting SMS. Its Android sibling has the same functionality but also exhibits other functionalities typical of Android Trojans. To exploit the stolen biometric data, the threat actor utilizes AI-driven face-swapping services to create deepfakes. This data combined with ID documents and the ability to intercept SMS, enables cybercriminals to gain unauthorized access to the victim's banking account – a new technique of monetary theft, previously unseen by Group-IB researchers in other fraud schemes.
Information	<https://www.group-ib.com/blog/goldfactory-ios-trojan/>

Last change to this tool card: 07 March 2024

Download this tool card in JSON format

All groups using tool GoldPickaxe

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8ec4514b-485c-4391-ba81-02d06c44d33b