

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:31:29 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool SharkBot

Tool: SharkBot

Names	SharkBot
Category	Malware
Type	Banking trojan , Info stealer , Credential stealer
Description	<p>(Cleafy) At the end of October 2021, a new Android banking trojan appeared on Cleafy's telemetries. Since the lack of information and the absence of a proper nomenclature of this malware family, we decided to dub it SharkBot to better track this family inside our internal Threat Intelligence taxonomy.</p> <p>SharkBot belongs to a “new” generation of mobile malware, as it is able to perform ATS attacks inside the infected device. This technique has been already seen recently from other banking trojans, such as Gustuff. ATS (Automatic Transfer System) is an advanced attack technique (fairly new on Android) which enables attackers to auto-fill fields in legitimate mobile banking apps and initiate money transfers from the compromised devices. Contrary to TeaBot and Oscorp/UBEL where a live operator is required to insert and authorize a money transfer, with ATS technique Threat Actors can scale up their operations with minimum user intervention. We assume that SharkBot is trying to bypass behavioural detection countermeasures (e.g.,biometrics) put in place by multiple banks and financial services with the abuse of Android Accessibility Services, also bypassing the need of a “new device enrollment”.</p>
Information	<p><https://www.cleafy.com/cleafy-labs/sharkbot-a-new-generation-of-android-trojan-is-targeting-banks-in-europe></p> <p><https://research.nccgroup.com/2022/03/03/sharkbot-a-new-generation-android-banking-trojan-being-distributed-on-google-play-store/></p> <p><https://blog.checkpoint.com/2022/04/07/android-banking-stealer-dubbed-sharkbot-found-disguised-as-legitimate-anti-virus-apps-on-the-google-play-store/></p> <p><https://www.bitdefender.com/blog/labs/android-sharkbot-droppers-on-google-play-underlines-platforms-security-needs/></p>
MITRE ATT&CK	< https://attack.mitre.org/software/S1055 >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/apk.sharkbot >

Last change to this tool card: 22 June 2023

Download this tool card in [JSON](#) format

All groups using tool SharkBot

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=fba647ac-53a5-4801-828c-6f6cc549bc09>