Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:50:16 UTC

Tool: Anubis

Names	Anubis BankBot Go_P00t android.bankbot android.bankspy
Category	Malware
Type	Banking trojan, Backdoor, Keylogger, Info stealer, Credential stealer
Description	(Trend Micro) The Anubis malware masquerades as a benign app, prompts the user to grant it accessibility rights, and also tries to steal account information. Banking trojans usually launch a fake overlay screen when the user accesses a target app and tries to steal information when the user inputs account credentials into the overlay. However, Anubis' process is a little different. It has a built-in keylogger that can simply steal a users' account credentials by logging the keystrokes. The malware can also take a screenshot of the infected users' screen, which is another way to get the victims credentials.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/> <https://blogs.quickheal.com/android-malware-combines-banking-trojan-keylogger-ransomware-one-package/> <https://securityintelligence.com/after-big-takedown-efforts-20-more-bankbot-mobile-malware-apps-make-it-into-google-play/> <https://securityintelligence.com/anubis-strikes-again-mobile-malware-continues-to-plague-users-in-official-app-stores/> <http://b0n1.blogspot.de/2017/05/tracking-android-bankbot.html> <http://blog.koodous.com/2017/04/decrypting-bankbot-communications.html> <https://www.welivesecurity.com/2017/11/21/new-campaigns-spread-banking-malware-google-play/> <http://blog.koodous.com/2017/05/bankbot-on-google-play.html> <https://www.fortinet.com/blog/threat-research/bankbot-the-prequel.html> <https://eybisi.run/Mobile-Malware-Analysis-Tricks-used-in-Anubis/>

	<https://pentest.blog/n-ways-to-unpack-mobile-malware/> <https://info.phishlabs.com/blog/new-variant-bankbot-banking-trojan-aubis> <https://www.fortinet.com/blog/threat-research/a-look-into-the-new-strain-of-bankbot.html> <https://sysopfb.github.io/malware,/reverse-engineering/2018/08/30/Unpacking-Anubis-APK.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0422/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.anubis>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Anubis>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Anubis

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=0a30f599-8c6c-4721-a736-4b21c8def62b