Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:16:51 UTC

Tool: TeaBot

Names	TeaBot Anatsa Toddler ReBot
Category	Malware
Type	Banking trojan, Backdoor, Info stealer, Keylogger, Credential stealer
Description	(Cleafy) TeaBot appears to have all the main features of nowadays Android bankers achieved by abusing Accessibility Services such as: • Ability to perform Overlay Attacks against multiple banks applications to steal login credentials and credit card information • Ability to send / intercept / hide SMS messages • Enabling key logging functionalities • Ability to steal Google Authentication codes • Ability to obtain full remote control of an Android device (via Accessibility Services and real-time screen-sharing)
Information	<https://www.cleafy.com/documents/teabot> <https://labs.k7computing.com/?p=22407> <https://www.threatfabric.com/blogs/smishing-campaign-in-nl-spreading-cabassous-and-anatsa.html> <https://labs.bitdefender.com/2021/06/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/> <https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368> <https://blog.nviso.eu/2021/05/11/android-overlay-attacks-on-belgian-financial-applications/> <https://www.buguroo.com/hubfs/website/pdf/reports/buguroo-malware-report-Toddler_EN.pdf> <https://www.bitdefender.com/blog/labs/new-flubot-and-teabot-global-malware-campaigns-discovered> <https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe> <https://www.threatfabric.com/blogs/anatsa-hits-uk-and-dach-with-new-campaign>

	<https://www.zscaler.com/blogs/security-research/technical-analysis-anatsa-campaigns-android-banking-malware-active-google>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.anatsa>

Last change to this tool card: 19 June 2024

Download this tool card in JSON format

All groups using tool TeaBot

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

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