Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:05:36 UTC

Tool: ERMAC

Names	ERMAC
Category	Malware
Type	Banking trojan, Backdoor, Info stealer, Credential stealer, Botnet
Description	(Threatfabric) On July 23 a forum post appeared regarding a new Android banking trojan. The attached screenshots show that it is named ERMAC. Our investigation shows that ERMAC is almost fully based on the well-known banking trojan Cerberus, and is being operated by BlackRock actor(s).
Information	<https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html> <https://blog.cyble.com/2022/05/25/ermac-back-in-action/> <https://blog.cyble.com/2022/10/18/ermac-android-malware-increasingly-active/> <https://www.threatfabric.com/blogs/hook-a-new-ermac-fork-with-rat-capabilities.html> <https://research.nccgroup.com/2023/09/11/from-ermac-to-hook-investigating-the-technical-differences-between-two-android-malware-variants/> <https://securityintelligence.com/posts/ermac-malware-the-other-side-of-the-code/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.ermac>

Last change to this tool card: 06 March 2024

Download this tool card in JSON format

All groups using tool ERMAC

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

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

↑