ERMAC - another Cerberus reborn

Published: 2024-10-01 · Archived: 2026-04-05 19:53:44 UTC

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).

On August 17, a forum member named “ermac” invited anyone interested in this topic to send a PM to make a deal. The user registered just the day before and posted a similar advertisement in his profile. Interestingly enough, the topic starter said that he found the contact 4 days earlier. On the same day, another forum member, “DukeEugene”, posted a message in his account:

“Android botnet ERMAC. I will rent a new android botnet with wide functionality to a narrow circle of people (10 people). 3k$ per month. Details in PM.”

DukeEugene is known as an actor behind the BlackRock banking trojan that we discovered in 2020. DukeEugene claimed to be the one of the actors shortly after we published our discovery.
