Hacker Group "Caracal Kitten" Targets KDP Activists With Malware
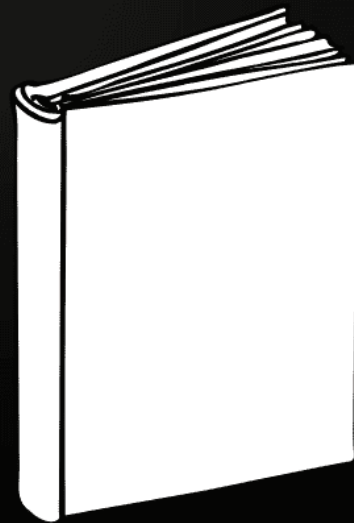
October 11, 2023

Security experts from Qi An Xin company recently uncovered cyberattacks on activists associated with the Kurdistan Democratic Party by a previously unknown hacker group named "Caracal Kitten."

The Caracal Kitten group disguised malware as official Kurdistan Democratic Party (KDP) mobile apps. Users, mistaking these apps for genuine ones, unwittingly installed them, granting hackers access to their contacts, SMS, and messenger data.

Qi An Xin analysts investigating this malicious campaign found that cybercriminals utilized two types of malware simultaneously: MOrder RAT and Ahmyth RAT.

MOrder RAT allowed them to receive and execute remote commands from their server, permitting actions such as uploading contacts, SMS, and other data. Ahmyth RAT, on the other hand, enabled covert photo and video recording, audio recording, and access to the victim's location.

As the report says, the attacks on KDP were carried out in two stages—during the summer of 2021 and from May 2023 onward. The malware code contained time zone settings corresponding to the Middle East, and some IP addresses used by the hackers were linked to major telecom operators in the region.

Due to the group's tactics, researchers coined the name "Caracal Kitten" for the group, which refers to a cat breed found in certain Middle Eastern countries.