RedAlert2 (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:09:34 UTC

RedAlert2

URLhaus

RedAlert 2 is an new Android malware used by an attacker to gain access to login credentials of various e-banking apps. The malware works by overlaying a login screen with a fake display that sends the credentials to a C2 server.
The malware also has the ability to block incoming calls from banks, to prevent the victim of being notified.
As a distribution vector RedAlert 2 uses third-party app stores and imitates real Android apps like Viber, Whatsapp or fake Adobe Flash Player updates.

References

There is no Yara-Signature yet.
