PINEFLOWER (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:04:45 UTC

PINEFLOWER

According to Mandiant, PINEFLOWER is an Android malware family capable of a wide range of backdoor functionality, including stealing system inform information, logging and recording phone calls, initiating audio recordings, reading SMS inboxes and sending SMS messages. The malware also has features to facilitate device location tracking, deleting, downloading, and uploading files, reading connectivity state, speed, and activity, and toggling Bluetooth, Wi-Fi, and mobile data settings.

References

There is no Yara-Signature yet.
