Retefe (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:56:54 UTC

apk.retefe (Back to overview)

Retefe

The Android app using for Retefe is a SMS stealer, used to forward mTAN codes to the threat actor. Further is a bank logo added to the specific Android app to trick users into thinking this is a legitimate app. Moreover, if the victim is not a real victim, the link to download the APK is not the malicious APK, but the real 'Signal Private Messenger' tool, hence the victim's phone doesn't get infected.

References

2017-08-03 · GovCERT.ch · GovCERT.ch
The Retefe Saga
Retefe Dok Retefe

2017-02-24 · Some stuff about security.. Blog · Angel Alonso
Hunting Retefe with Splunk - some interesting points
Retefe

2015-11-03 · Angel Alonso-Parrizas
Reversing the SMS C&C protocol of Emmental (1st part - understanding the code)
Retefe

2015-10-28 · Angel Alonso-Parrizas
Reversing the C2C HTTP Emmental communication
Retefe

2014-09-23 · maldr0id blog · Łukasz Siewierski
Android malware based on SMS encryption and with KitKat support
Retefe

2014-07-07 · Victor Dorneanu
Disect Android APKs like a Pro - Static code analysis
Retefe

There is no Yara-Signature yet.
