# Retefe (Android) - Threat Group Cards: A Threat Actor Encyclopedia





## Tool: Retefe (Android)

| | |
|---|---|
| Names | Retefe (Android) |
| Category | Malware |
| Type | Banking trojan, Backdoor, Info stealer, Credential stealer, Botnet |
| Description | (GovCERT.ch) Recently, some anti-virus companies and newspapers reported that Retefe is distributing the Signal App (a secure messenger). Rumours say that the threat actor may use the Signal App as a communication channel with the victim. This is not the case. As a matter of fact, the Signal App is just decoy that the Retefe Gang serves to IP addresses who are not geo located in Switzerland and whose user agent does not correspond to an Android device. If the accessing IP address uses an Android user agent and is geographically located in Switzerland, the APK server will serve an Android trojan that the Retefe gang use to commit e-banking fraud.<br><br>The trojan is an SMS stealer which allows the threat actor to steal text messages sent by the bank to the customer for two factor authentication (2FA) and transaction signing (so called mobile TAN or mTAN). To have the victim install the android trojan, the Retefe gang uses social engineering to convince the victim to either enter his mobile phone number where he then receives an SMS from the threat actor with a link to the Android APK, or to scan a QR code displayed by the threat actor in the fake e-banking portal, which also leads to the Android APK. But the Android trojan is more than just an SMS stealer. It is also able to send text messages to other victim’s and uses a sophisticated anti VM detection technique. Unlike Retefe itself, which doesn’t have any botnet C&C channel, the SMS stealer has such one. It uses two hard coded botnet C&Cs which are usually hosted on compromised websites. |

| | |
|---|---|
| Information | <https://www.govcert.ch/blog/the-retefe-saga/><br><http://blog.angelalonso.es/2015/10/reversing-c2c-http-emmental.html><br><http://blog.angelalonso.es/2017/02/hunting-retefe-with-splunk-some24.html><br><http://maldr0id.blogspot.ch/2014/09/android-malware-based-on-sms-encryption.html><br><http://blog.angelalonso.es/2015/11/reversing-sms-c-protocol-of-emmental.html><br><http://blog.dornea.nu/2014/07/07/disect-android-apks-like-a-pro-static-code-analysis/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/apk.retefe> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:Retefe> |

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

### All groups using tool Retefe (Android)

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **Other groups** | | | | |
| | Retefe Gang, Operation Emmental |  | 2013 | |

*1 group listed (0 APT, 1 other, 0 unknown)*

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=07d8d046-a4f0-434c-b7a4-d971f660b0d4