Cerberus behavior:

|  |
| --- |
| Overlaying: Dynamic (Local injects obtained from C2) |
| Keylogging |
| SMS harvesting: SMS listing |
| SMS harvesting: SMS forwarding |
| Device info collection |
| Contact list collection |
| Application listing |
| Location collection |
| Overlaying: Targets list update |
| SMS: Sending |
| Calls: USSD request making |
| Calls: Call forwarding |
| Remote actions: App installing |
| Remote actions: App starting |
| Remote actions: App removal |
| Remote actions: Showing arbitrary web pages |
| Remote actions: Screen-locking |
| Notifications: Push notifications |
| Self-protection: Hiding the App icon |
| Self-protection: Preventing removal |
| Self-protection: Emulation-detection |

Target list:

|  |  |
| --- | --- |
| Package name | Application name |
| com.android.vending | Play Market |
| com.boursorama.android.clients | Boursorama Banque |
| com.caisseepargne.android.mobilebanking | Banque |
| com.chase.sig.android | Chase Mobile |
| com.clairmail.fth | Fifth Third Mobile Banking |
| com.connectivityapps.hotmail | Connect for Hotmail |
| com.google.android.gm | Gmail |
| com.imo.android.imoim | imo free video calls and chat |
| com.infonow.bofa | Bank of America Mobile Banking |
| com.IngDirectAndroid | ING |
| com.instagram.android | Instagram |
| com.konylabs.capitalone | Capital One® Mobile |
| com.mail.mobile.android.mail | mail.com mail |
| com.microsoft.office.outlook | Microsoft Outlook |
| com.snapchat.android | Snapchat |
| com.tencent.mm | WeChat |
| com.twitter.android | Twitter |
| com.ubercab | Uber |
| com.usaa.mobile.android.usaa | USAA Mobile |
| com.usbank.mobilebanking | U.S. Bank - Inspired by customers |
| com.viber.voip | Viber |
| com.wf.wellsfargomobile | Wells Fargo Mobile |
| com.whatsapp | WhatsApp |
| com.yahoo.mobile.client.android.mail | Yahoo Mail – Organized Email |
| fr.banquepopulaire.cyberplus | Banque Populaire |
| fr.creditagricole.androidapp | Ma Banque |
| jp.co.rakuten\_bank.rakutenbank | 楽天銀行 -個人のお客様向けアプリ |
| mobi.societegenerale.mobile.lappli | L'Appli Société Générale |
| net.bnpparibas.mescomptes | Mes Comptes BNP Paribas |
| org.telegram.messenger | Telegram |