Cerberus

Cerberus, il trojan bancario per Android che aggira l'autenticazione a due fattori: come proteggersi

Un'applicazione Android dannosa è stata scoperta sul Google Play Store e sta distribuendo una variante del trojan bancario Cerberus in grado di bypassare anche l'autenticazione a due fattori. Ecco tutti i dettagli e i consigli per difendersi

L'app disponibile per gli utenti Android in Spagna dal mese di marzo ha già totalizzato migliaia di download e potrebbe presto diffondersi anche in altri Paesi.

Secondo il tradizionale modus operandi dei trojan bancari, dicono i ricercatori, quest'app di conversione di valuta ha funzionato in modo normale per un certo lasso di tempo, al fine di guadagnare la fiducia degli utenti che l'hanno scaricata e evitare anche il rilevamento iniziale da parte sia dei ricercatori di malware che dello stesso team Play Protect di Google, e solo in un secondo momento si è attivata per cercare di rubare credenziali di conti bancari, aggirando ogni eventuale misure di sicurezza, inclusa anche l'autenticazione a due fattori (2FA).

Ciò che ha destato particolare interesse e che ha caratterizzato la campagna in esame è stato il modo in cui il trojan bancario è riuscito a intrufolarsi subdolamente sul Google Play Store.

I ricercatori hanno rilevato, durante il monitoring dei campioni esaminati, che le versioni più recenti dell'app, rilasciate nel mese di giugno, includevano un codice dropper dormiente che solo in una seconda fase (dai primi giorni di luglio) è stato attivato da un server di controllo remoto trasformando l'app in un effettivo dropper per il download furtivo di Cerberus sui dispositivi delle ignare vittime come pacchetto aggiuntivo Android (APK).

Cerberus, così come dichiarato da Ondrej David di Avast, una volta installato, sfruttando la funzione di accessibilità di Android può sovrapporsi con tecniche di attacco overlay ad un'app bancaria preesistente sullo smartphone, restando in attesa che gli utenti accedano ai propri conti bancari, per poi presentare una falsa schermata di login e rubare loro credenziali bancarie e carpendo anche messaggi di testo o eventuali codici di autenticazione multi fattore inviati tramite SMS.

Come proteggersi dai trojan del mobile banking

Anche se gli analisti hanno affermato che:

- il server C2 e il payload associati alla campagna non risultano più attivi;
- il convertitore di valuta "Calculadora de Moneda" su Google Play store non contiene più il trojan Cerberus;
- Avast ha responsabilmente notificato a Google l'accaduto nei tempi e nei modi canonici;

- lo stesso team di ricerca suggerisce che per proteggersi dal fenomeno sempre più dilagante del mobile banking trojan è bene seguire le seguenti misure preventive:
- verificare sempre l'attendibilità delle app bancarie utilizzate, confrontandosi con i relativi servizi clienti;
- utilizzare e attivare se possibile l'opzione di autenticazione multi fattore;
- affidarsi solo ad app store affidabili, Google Play o App Store di Apple restano sempre e comunque le fonti ufficiali;
- controllare le valutazioni degli utenti prima di scaricare una nuova app;
- prestare attenzione alle autorizzazioni (amministrative, di controllo ecc.) richieste durante l'installazione di un'app, concedendole solo se sicuri che siano necessarie per il suo corretto funzionamento;
- istallare come vale per i PC degli strumenti antivirus affidabili