SMARTPHONE ANDROID TROPPO VULNERABILI: A RISCHIO IL 99% DEI DISPOSITIVI

È una ricerca dell'università tedesca di Ulm ad aver riconosciuto il bug in questione che interesserebbe il sistema operativo mobile di Google legato al protocollo di autenticazione denominato ClientLogin, una volta che ciascun device venga collegato a reti Wi-Fi aperte. Un "baco" non trascurabile per Montain View, dato che offrirebbe il fianco a chiunque intenda impossessarsi delle informazioni che gli utenti utilizzano per avere accesso ai servizi sul web, come password di autenticazione per la posta elettronica o per i social network. Lo studio che ha rivelato tale fragilità nei sistemi di sicurezza per la quasi totalità dei supporti mobili della versione 2.3.3. come di quelle precedenti, suggerisce però anche una soluzione e cioè quella di aggiornare il sistema operativo del proprio telefonino alla versione 2.3.4. di Android. L'unico inconveniente è che il suddetto update risulti compatibile con pochissimi modelli, a quanto pare, solo con gli ultimi lanciati sul mercato e di fascia alta come il Nexus S, scaturito dalla partnership tra Google e la Samsung, oltre che il Desire della HTC.
Ma vediamo di capire qual sia la principale minaccia per la privacy degli utenti. La ricerca tedesca specifica che i dati di identificazione archiviati in cache per 14 giorni, potrebbero essere catturati dall'esterno da un qualsiasi cracker in grado di far propria l'identità della sua vittima, un rischio che risulta direttamente proporzionale alle opportunità di monetizzazione delle informazioni prelevate. Anche il più timido degli hacker intuirebbe che non sono poche. Il servizio di ClientLogin incriminato verrebbe utilizzato oltre che per i comuni servizi Google Calendar e Contact apps, anche per diverse applicazioni di terze parti (la Gallery app sviluppata da Cooliris consapevole della falla nel sistema), risultando quindi responsabile dell'invio di tutti i dati relativi alla autenticazione in chiaro, senza l'impiego della connessione protetta in https.
Ad oggi solo l'1% dei device Android presenti sul mercato è stato aggiornato. Ma come procedere alla messa in sicurezza del restante 99% dei dispositivi ancora sotto palese minaccia? Per limitare i danni, sarebbe opportuno disabilitare la sincronizzazione automatica ed evitare di connettersi a una rete Wi-Fi pubblica. Per ora Google si limita a ribadire l'urgenza di collaborare in maniera continuativa con i carrier, provvedendo alla diffusione di un software in grado di risolvere a monte questo tipo di difetti, anche se la comunicazione aziendale non sembra essere generosa di particolari, specie quando nella gestione dei dati sensibili, la superficialità tende ad essere giustificata con l'innovazione, mentre l'utente è sempre l'ultimo a venirne informato.
Manuela Avino

approfondimenti

articoli correlati

Il link al sito dell'Università di Ulm