Esiste veramente una backdoor nelle conversazioni di WhatsApp?

Data: Invalid Date | Autore: Paolo Fernandes

BERKELEY, 13 GENNAIO - Un ricercatore dell’università di Berkeley, Tobias Boelter, avrebbe trovato una falla nel sistema di WhatsApp che permetterebbe di accedere alle conversazioni degli utenti, finora ritenute inviolabili.[MORE]

Dai primi mesi dello scorso anno, l'applicazione di messaggistica istantanea dichiara apertamente di proteggere le conversazioni dei propri utilizzatori con un sistema di crittografia end-to-end, che consente la lettura dei messaggi solo al mittente ed al destinatario.

La presunta falla consisterebbe in una “backdoor” (porta sul retro), attraverso la quale WhatsApp, e quindi potenzialmente anche altri interessati, potrebbero accedere al contenuto dei messaggi inviati ma non ancora consegnati, grazie ad una modifica delle chiavi di lettura del mittente.

Il ricercatore ha dichiarato di aver già informato Facebook, proprietario del servizio dal 2014, della propria scoperta, e di aver ricevuto conferme circa la conoscenza da parte dei gestori del social network di questa anomalia.

Quanto però sembrerebbe una sgradevole sorpresa, è in realtà una conseguenza necessaria del meccanismo di funzionamento dell’app: al fine di evitare che ogni messaggio non recapitato vada nuovamente inoltrato, WhatsApp provvede a rispedirlo al momento della riconnessione alla rete, utilizzando chiavi rigenerate.

Gli utenti più prudenti, peraltro, possono attivare l’impostazione che consente di ricevere notifiche ogni qual volta cambi la chiave di sicurezza del destinatario.

WhatsApp è il più diffuso servizio di messaggistica istantanea al mondo, e conta oltre un miliardo di utilizzatori.

Paolo Fernandes