Signal vs Telegram, la crittografia al centro della querelle

Administrator | 29/12/2021 | Di tutto di più

Il fondatore dell'app di chat sicura Signal, Moxie Marlinspike, si è scagliato contro Telegram.

Archivierebbe tutti i dati inviati e ricevuti - foto, video, messaggi, file audio - nei suoi server senza applicare alcun tipo di crittografia sicura. Trasformandoli in un "*parco giochi*" per hacker e governi.

WhatsApp e persino **Messenger di Facebook**, prosegue Marlinspike, offrono una protezione di gran lunga maggiore a Telegram. Non a caso, Messenger e WhatsApp integrano in parte o in tutto il protocollo crittografico di Signal.

Non si è fatta attendere la risposta di Pavel Durov, il fondatore di Telegram.

> Un recente rapporto ha dimostrato che Telegram mantiene la sua promessa di mantenere privati i dati degli utenti. Mentre app come WhatsApp danno i dati degli utenti in tempo reale a terzi, e nonostante le loro numerose affermazioni sulla "crittografia E2E", possono anche rivelare il contenuto dei messaggi.
>
> ### Il rapporto ha confermato che Telegram è una delle poche app di messaggistica che non viola la fiducia dei propri utenti.
>
> Non sono sorpreso.
>
> La maggior parte delle altre app non potrebbero garantire la privacy ai loro utenti anche se volessero.
>
> Poiché i loro ingegneri risiedono negli Stati Uniti, devono implementare segretamente delle backdoor nelle loro app quando il governo americano glielo ordina.
>
> Se un ingegnere ne parla pubblicamente, può andare in prigione per aver violato un ordine di riservatezza.
>
> Nella maggior parte dei casi le agenzie non hanno nemmeno bisogno di un ordine del tribunale per estrarre informazioni private dalle app di messaggistica come WhatsApp. E in altri casi, i documenti del tribunale sono avvolti nella segretezza. Alcune app apparentemente sicure sono state finanziate da agenzie governative fin dal loro inizio (ad esempio Anom, Signal).
>
> **Per molti anni la National Security Agency (NSA) si è assicurata che gli standard internazionali di crittografia siano in linea con ciò che la NSA può decifrare. E tutti gli altri approcci alla crittografia sono etichettati come "non-standard" o "home-brew".**

Attraverso i loro proxy nell'industria della crittografia (come questo), la NSA ha imposto standard difettosi sulla crittografia utilizzata dal resto del mondo. Ha messo in guardia tutti gli altri dal "lanciare la propria crittografia".

Non c'è da stupirsi che le applicazioni basate negli Stati Uniti come WhatsApp siano afflitte da backdoor - scappatoie di sicurezza intenzionalmente piantate che i governi (e chiunque altro) possono usare per violare gli smartphone ed estrarre dati privati dalle persone.

Ho sentito che i nostri concorrenti con sede negli Stati Uniti sono frustrati perché non possono eguagliare la crescita di Telegram, nonostante i forti investimenti in marketing (qualcosa in cui Telegram non ha mai dovuto investire).

Ma per eguagliare la nostra crescita, devono prima assicurarsi che le loro azioni corrispondano alle loro affermazioni di marketing.

Fino ad allora, le violazioni dei dati e i problemi di sicurezza nelle loro app rimarranno, purtroppo, inevitabili.