Bug in Instagram permetteva di rubare gli account

Lug 16, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Una falla di sicurezza nel sistema di recupero password consentiva di eseguire un attacco di brute forcing per violare il codice di conferma.

L'utilizzo dei codici inviati via SMS non è uno strumento particolarmente sicuro quando viene usato come sistema di autenticazione a due fattori. Se viene usato come unico strumento per l'autenticazione, però, rischia di trasformarsi in una vera voragine di sicurezza.

Per spiegarlo agli sviluppatori di **Instagram**, però, c'è voluto l'intervento di **Laxman Muthiyah**, un ricercatore di sicurezza che ha scovato una clamorosa falla nel sistema di autenticazione del social network.

Come spiega in un articolo pubblicato su Internet, nella sua attività di "cacciatore di bug" Muthiyah si è concentrato per qualche tempo sul sistema di recupero della password di Instagram. Il social network, infatti, prevede diverse modalità per chiedere il reste della password.

Quello per la versione Web utilizza un classico link che ha tutte le carte in regola per resistere a qualsiasi attacco. Quello per mobile, invece, sfrutta un codice a sei cifre che viene inviato tramite SMS al telefono del legittimo proprietario dell'account.

Ciò è che si è chiesto Muthiyah è: cosa succede se qualcuno prova a violare il codice provando tutte le possibili combinazioni?

Teoricamente, operazioni come queste (con un codice a sei cifre stiamo parlando di **un milione di possibili combinazioni**) dovrebbero essere bloccate automaticamente. Prima di escludere a priori l'ipotesi, però, il ricercatore ha deciso di provarci.

Il primo tentativo, spiega nel suo articolo, gli ha permesso di capire che il sistema di protezione scelto da Instagram contro gli attacchi di brute forcing è quello di limitare il numero di tentativi di accesso. Non solo: la validità del codice è di 10 minuti.

Nello specifico, Muthiyah ha scoperto di essere in grado di inviare fino a un massimo di 200 codici in 10 minuti da un singolo computer.

Quello che ha scoperto, però, è che il sistema di protezione considera soltanto il singolo dispositivo, individuandolo attraverso l'indirizzo IP. Un attacco contemporaneo da parte di più computer (o da differenti indirizzi IP) però, può far saltare la protezione.

[embedded content]

Nel video qui sopra, Muthiyah mostra come sia riuscito a eseguire 200.000 tentativi di accesso utilizzando 1.000

indirizzi IP.

Per garantire un successo al 100%, di conseguenza, basterebbe utilizzare **5.000 IP differenti** e una potenza di calcolo sufficiente per inviare un milione di richieste in 10 minuti. Impossibile? Non proprio. **Secondo il ricercatore, le risorse su cloud per un'operazione del genere richiedono un investimento di soli 150 dollari**.

Molti se si pensa di hackerare account a caso, ma decisamente pochi se si vuole colpire uno specifico bersaglio di "alto profilo", come un politico o una celebrità.

Prima di correre ad affittare server su Amazon, sappiate che dopo la segnalazione di Muthiyah Instagram ha tempestivamente corretto la falla di sicurezza, ricompensando il ricercatore con 30.000 dollari.

La cifra (piuttosto modesta) riconosciuta come "taglia" per il bug è giustificata, tutto sommato, dalla relativa pericolosità del bug. **Per poter portare l'attacco, infatti, è necessario conoscere il numero di telefono della vittima**. Un dettaglio che, nel caso di bersagli di alto profilo, non dovrebbe essere facile da ottenere.

Condividi l'articolo

Nuovi attacchi ai router. La minaccia arriva dal Brasile

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/16/bug-in-instagram-permetteva-di-rubare-gli-account/