Zero-day in Whatsapp: lo spyware si installa con una chiamata

Mag 14, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

La clamorosa falla di sicurezza sarebbe stata sfruttata per portare attacchi mirati con il famigerato spyware Pegasus della società israeliana NSO Group.

La notizia, diffusa in anteprima dal **Financial Times**, è una vera bomba. Prima di tutto perché riguarda **Whastapp**, cioè un'app utilizzata da 1,5 miliardi di persone. In secondo luogo perché la vulnerabilità scoperta dai ricercatori è di un'efficacia devastante: **basterebbe infatti una chiamata vocale per installare un malware sul telefono del destinatario**.

Da un punto di vista tecnico, in realtà, l'exploit (CVE-2019-3568) sfrutta un "semplice" **buffer overflow**, che per essere innescato richiede una manipolazione dei dati inviati nel corso della chiamata. **Il vero problema è che, stando a quanto riportano i tecnici, l'attacco funziona anche se la vittima non risponde**.

Insomma: si tratterebbe dell'attacco perfetto. Per due motivi: prima di tutto perché il bug funziona su **tutte le piattaforme mobili** (Android, iOS e Windows Phone). In secondo luogo perché prende di mira un'applicazione che, normalmente, ha accesso a tutte le funzionalità del telefono che possono interessare a un cyber-criminale.

Un pirata informatico, sfruttando questa tecnica, potrebbe non

solo accedere a tutti i messaggi e le chiamate Whatsapp aggirando la crittografia, ma anche utilizzare microfono e fotocamera per spiare la sua vittima.



E lo spionaggio sembra essere lo scopo principale di chi ha utilizzato questo attacco. Nel dettaglio, tutti gli indizi porterebbero a **NSO Group**, la società israeliana specializzata nello sviluppo di software di spionaggio destinati all'uso da parte di forze di polizia e servizi segreti.

L'azienda, valutata 1 miliardo di dollari, deve il suo successo a **Pegasus**, uno spyware particolarmente apprezzato dai governi di tutto il mondo che lo usano per operazioni di polizia e di spionaggio.

Proprio alcune analogie tra Pegasus e il software spia veicolato attraverso l'attacco via Whatsapp avrebbe portato i ricercatori a puntare il dito verso NSO Group, che a questo punto avrebbe trovato un formidabile vettore di attacco per il suo spyware.

Non solo: secondo quanto riporta **Citizen Lab**, associazione no-

profit che da tempo denuncia il fatto che NSO Group venda i suoi prodotti anche a regimi autoritari che li usano per spiare giornalisti e dissidenti, **un attacco tramite Whatsapp sarebbe stato tentato ai danni di un avvocato specializzato nella difesa di diritti umani, promotore di una serie di cause che hanno preso di mira proprio NSO Group**.



L'attacco sarebbe stato bloccato dagli amministratori di Whatsapp attraverso delle modifiche del back-end che avevano introdotto per mitigare il rischio di attacchi in attesa della patch, pubblicata nella giornata di ieri su tutte le piattaforme.

Se la disponibilità di un aggiornamento che risolve il problema è una buona notizia, resta da vedere quello che succederà in seguito. **Ora che la vulnerabilità è pubblica, non**

ci vorrà molto perché tutti i cyber-criminali del pianeta comincino a lavorare per mettere a punto un exploit simile a quello individuato.

Per fortuna, stando a quanto si è letto nei report finora, non si tratterebbe di un exploit facilmente riproducibile, Considerato poi che il codice per l'attacco non è incorporato in un file (e quindi non si può ottenere facilmente) è difficile che ci siano conseguenze immediate.

Considerato però che molti utenti hanno il pessimo vizio di non aggiornare mai le loro applicazioni, e visto che si sta parlando di un bacino di potenziali vittime di 1,5 miliardi di persone, i possibili sviluppi della vicenda potrebbero essere devastanti.

Please follow and like us:



Battaglia tra due gruppi hacker: è strage di server sul cloud

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/14/zero-day-in-whatsapp-lo-spyware-si-installa-con-una-chiamata/