

Arrestati gli hacker che hanno violato l'account Telegram di Bolsonaro

Lug 29, 2019 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Leaks, News, RSS 0

Il presidente del Brasile e numerosi esponenti del governo vittime di un attacco piuttosto artigianale. La tecnica si conosce dal 2016.

C'è anche il presidente **Jair Bolsonaro** nell'elenco di esponenti del governo brasiliano i cui account Telegram sono stati violati da un gruppo di hacker che le forze di polizia hanno arrestato la scorsa settimana. **Oltre a lui, nel mirino sono finiti il ministro della giustizia Sergio Moro e il ministro dell'economia Paulo Guedes.**

La vicenda è emersa dopo una serie di leak riguardanti messaggi scambiati tra i ministri pubblicati dal sito di news **The Intercept**, fondato dal giornalista **Glenn Greenwald**.

Il reporter statunitense, diventato celebre per aver "coperto" la vicenda di **Edward Snowden**, è considerato uno dei migliori nel settore del giornalismo investigativo e non stupisce che gli hacker abbiano scelto il suo giornale online per diffondere il materiale che hanno "acquisito".

I messaggi, in particolare quelli del ministro della giustizia Moro, hanno creato un clamoroso terremoto politico in Brasile. Dalle chat sarebbe infatti emerso un vero e proprio piano per influenzare il processo nei confronti dell'ex-presidente **Luiz Inácio Lula da Silva**, deposto in seguito a un'inchiesta che a questo punto appare essere stata pilotata ad arte da Moro (che

ai tempi era giudice) con lo scopo di screditarlo.

Gli arrestati sono il 33enne **Danilo Cristiano Marquez**, **Walter Delgatti Neto** (30), **Judy Gustavo Henrique Elias Santos** (28) e sua moglie **Suelen Priscilla de Oliveira** (25).

La parte davvero sorprendente di tutta la vicenda riguarda però il modo in cui avrebbero ottenuto l'accesso ai messaggi. **Per violare gli account dei politici brasiliani, gli hacker hanno usato un trucchetto che è emerso 3 anni fa e di cui abbiamo parlato ampiamente in questo articolo.**

Come funziona l'attacco? In pratica, fa leva sul sistema utilizzato da Telegram per attivare il servizio di messaggistica su desktop. La procedura prevede infatti l'inserimento del numero di telefono con cui è registrato l'account e una conferma attraverso **un codice di sicurezza** che viene inviato con un SMS al telefono stesso.

Telegram, però, prevede anche la possibilità di ottenere il codice attraverso **una chiamata vocale automatica**. Ed ecco qui la falla di sicurezza. Se il telefono non è raggiungibile (ad esempio perché è impegnato in un'altra chiamata) il messaggio con il codice viene registrato sulla segreteria telefonica.

Tutto quello che i pirati hanno dovuto fare, quindi, è stato chiamare il telefono in questione e, nel frattempo, tentare l'accesso via desktop chiedendo l'invio del codice tramite chiamata vocale.

A questo punto, non rimane che collegarsi alla segreteria telefonica della vittima per appropriarsi del codice di autenticazione. Farlo è più facile di quanto si possa credere.

Basta utilizzare un servizio VoIP (o un'app) che consenta di impostare il numero di telefono in uscita con lo stesso della vittima o "indovinare" il PIN di accesso al servizio che consente di ascoltare i messaggi da un altro telefono.

Visto che quasi nessuno modifica il PIN di accesso alla

segreteria telefonica, infatti, ci sono buone probabilità che sia quello predefinito, di solito “0000” o “1234”.

Insomma: nessuna tecnica sofisticata o strumenti fantascientifici, ma qualcosa che potrebbe utilizzare anche un ragazzino sufficientemente sveglio. Di più: per proteggersi da questo tipo di attacco basterebbe un piccolo accorgimento: **disattivare la segreteria telefonica**.

La ricostruzione fatta dagli investigatori, che per il momento non hanno ancora formalizzato le accuse, è però ancora tutta da verificare.

In seguito agli arresti e alle indagini che stanno seguendo, Greenwald ha infatti negato che i quattro arrestati fossero la fonte del leak riportato da The Intercept. Tanto più che, secondo Greenwald, i primi contatti con la sua fonte sarebbero avvenuti un mese prima del presunto hacking degli account come denunciati dal ministro Moro, che avrebbe indicato il 5 giugno come data in cui gli hacker avrebbero violato il sistema.

La vicenda, insomma, rimane ancora piuttosto intricata. L'unico dato certo è che Jair Bolsonaro e i suoi accoliti, già al centro delle polemiche per le loro politiche illiberali e per la malcelata nostalgia per i tempi della dittatura, non ne escono particolarmente bene. Per lo meno dal punto di vista dell'astuzia.

Condividi l'articolo

Kaspersky supera l'audit indipendente SOC 2 Gli strani effetti collaterali degli attacchi ransomware

Articoli correlati

Altro in questa categoria

<https://www.securityinfo.it/2019/07/29/arrestati-gli-hacker-che-hanno-violato-laccount-telegram-di-bolsonaro/>