

Iran: malware per Android che aggira l'autenticazione a due fattori

Set 21, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il gruppo Rampant Kitten usa una tecnica che gli permette di rubare dagli smartphone i codici di autenticazione inviati tramite SMS.

Una strategia su doppio binario, che coinvolge i sistemi Windows e quelli Android. Ad adottarla è un gruppo di cyber-spioni legati al **governo di Teheran** che è finito anche sotto la lente d'ingrandimento dell'**FBI**.

I pirati informatici iraniani di **Rampant Kitten** hanno avviato negli scorsi mesi una serie di campagne che prendevano di mira varie associazioni politiche in **Azerbaijan** e **Belucistan** (un'area geografica compresa tra Iran, Pakistan e Afghanistan – ndr) utilizzando un trojan per **Windows**.

La backdoor utilizzata per infettare i PC Windows, che viene distribuita utilizzando un documento Word contenente codice malevolo, prende di mira **Telegram** e **KeePass**, un'applicazione per la gestione delle password.

Insomma: si tratterebbe di un “grimardello” pensato per garantire ai pirati informatici l’accesso a tutti i servizi utilizzati dalle vittime.

Come spiegano i ricercatori di **Check Point** in un report pubblicato sul sito della società di sicurezza, l’elemento più rilevante in questa ondata di attacchi è l’utilizzo di un malware per Android che è in grado di rubare i codici usati per l’autenticazione a due fattori di numerosi servizi.

Il malware per Android, in pratica, integra una funzionalità che gli permette di inoltrare a un numero controllato dai pirati informatici tutti gli SMS che contengono il testo “G-“, usato normalmente dal sistema di autenticazione a due fattori di **Google**.

Non solo: il trojan sarebbe in grado di inoltrare anche tutti i messaggi ricevuti su **Telegram** e altre applicazioni social. Un elemento questo, che concorda con la versione Windows del malware utilizzato da Rampant Kitten per spiare le sue vittime.

Per distribuirlo, i pirati hanno usato un’app che si propone come uno strumento per aiutare le persone che parlano persiano a ottenere la patente in Svezia.

Uno stratagemma che lascia pochi dubbi sugli obiettivi degli hacker: la Svezia (e i paesi nordici in generale) ospitano infatti una nutrita comunità di dissidenti iraniani, che hanno abbandonato il loro paese e chiesto asilo politico in Europa.

Condividi l'articolo

In Germania la prima morte provocata da un attacco informatico?

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/09/21/iran-malware-per-android-che-aggiunge-lautenticazione-a-due-fattori/?utm_source=rss&utm_medium=rss&utm_campaign=iran-malware-per-android-che-aggiunge-lautenticazione-a-due-fattori