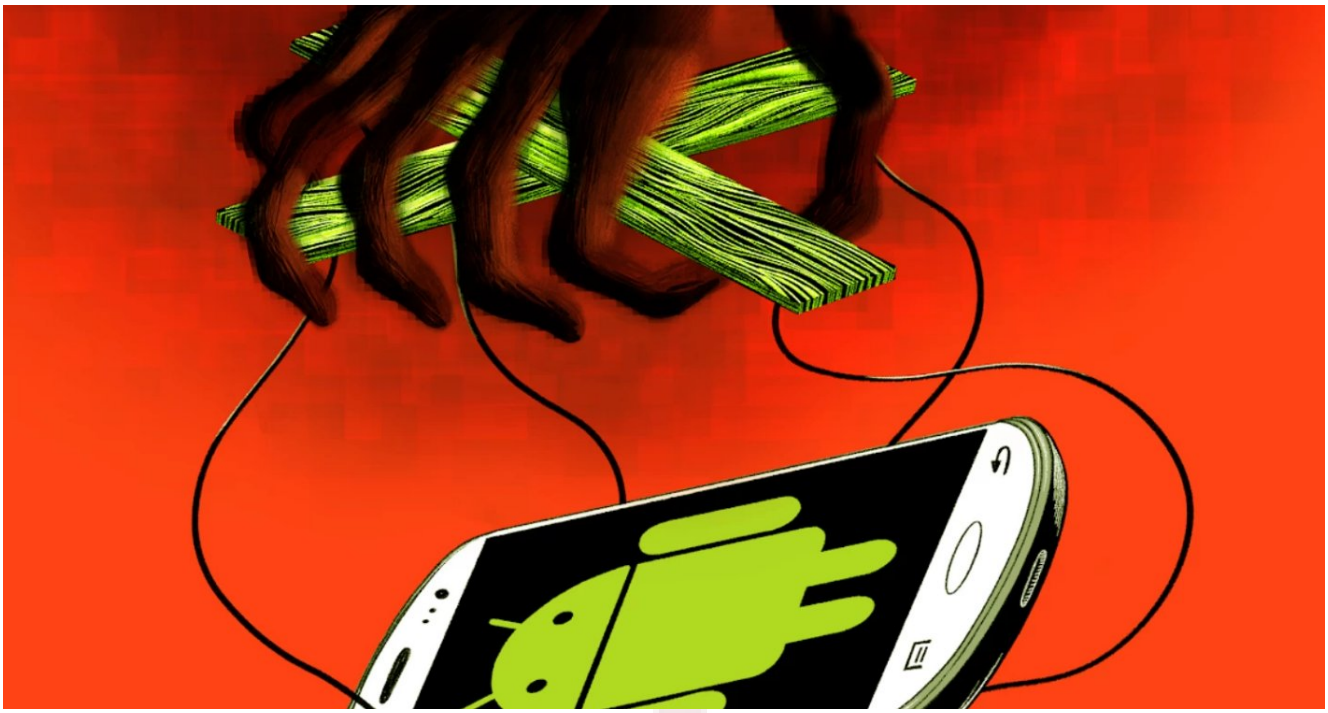
Centinaia di italiani sono stati infettati da un mal-ware nascosto da anni sul Play Store

Data: Invalid Date | Autore: Nicola Cundò



ROMA 28 MARZO- Si tratterebbe di un malware governativo che ha collegamenti con un'azienda italiana finora sconosciuta. Secondo diversi esperti, siamo davanti a un caso di intercettazioni legali finite molto male.
Alcuni hacker che lavorano per un'azienda di sorveglianza hanno infettato per mesi centinaia di persone grazie a diverse app malevole per Android che erano state caricate sul Play Store ufficiale di Google, stando a quanto Motherboard ha appreso.

Non è la prima volta che hacker governativi o hacker legati a organizzazioni criminali riescono a caricare malware sul Play Store. Questo nuovo caso sottolinea per l'ennesima volta i limiti deifiltridi Google che dovrebbero evitare che i malware finiscano sul Play Store. In questo caso, più di 20 app malevole sono passate inosservate sotto il naso di Google, per un periodo di circa due anni.

Motherboard ha anche appreso dell'esistenza di un nuovo tipo di malware per Android presente sul Play Store di Google, che il governo italiano ha acquistato da un'azienda che generalmente vende sistemi di videosorveglianza ma che, fino a ora, non era conosciuta per lo sviluppo di malware.

Alcuni esperti hanno riferito a Motherboard che l'operazione potrebbe aver colpito vittime innocenti, dal momento che lo spyware sembrerebbe essere difettoso e mal direzionato. Esperti legali e delle forze dell'ordine hanno riferito a Motherboard che lo spyware potrebbe essere illegale.

Le diverse app di questo spyware sono state scoperte e studiate in un'indagine congiunta tra i

ricercatori di Security Without Borders, una non-profit che spesso compie investigazioni su minacce contro i dissidenti e attivisti per i diritti umani, e Motherboard. I ricercatori hanno pubblicato un dettagliato report tecnico dei propri risultati nella giornata di venerdì.

“Abbiamo identificato copie di uno spyware precedentemente sconosciuto che sono state caricate con successo sul Google Play Store più volte nel corso di oltre due anni. Queste applicazioni sono normalmente rimaste disponibili su Play Store per mesi,” hanno scritto i ricercatori.

Lukas Stefanko, un ricercatore dell’azienda di sicurezza ESET, specializzato in malware per Android ma che non è coinvolto nella ricerca di Security Without Borders, ha detto a Motherboard che è allarmante, ma non sorprendente, che dei malware continuino a scavalcare i filtri del Play Store di Google.

“Nel 2018 e persino nel 2019 alcuni malware sono riusciti a penetrare fra i meccanismi di sicurezza di Google Play. Sono necessari dei miglioramenti,” Stefanko ha detto in una chat online. “Google non è un’azienda di sicurezza, forse dovrebbero focalizzarsi di più su questo.”

PIACERE, EXODUS

Nel tentativo apparente di indurre i bersagli a installarle con l’inganno, le app dello spyware erano progettate per assomigliare a innocue app per ricevere promozioni e offerte di marketing da operatori telefonici italiani, o da app per migliorare le performance del dispositivo.

All’inizio di quest’anno i ricercatori hanno allertato Google dell’esistenza di queste app, che poi sono state rimosse. Google ha detto sia ai ricercatori che a Motherboard di aver trovato 25 versioni differenti dello spyware negli ultimi due anni, risalenti fino al 2016. Google ha rifiutato di condividere il numero esatto di vittime, ma ha detto che è inferiore alle 1000 e che sono tutte italiane. L’azienda non ha fornito ulteriori informazioni riguardo le persone colpite.

I ricercatori chiamano il malware Exodus, a partire dal nome del server di comando e controllo (C&C) a cui le app si connettevano. Una persona informata sullo sviluppo del malware ha confermato a Motherboard che quello è il nome del malware usato internamente.

Exodus era programmato per agire in due stadi. Nel primo stadio, lo spyware si installa e controlla solamente il numero di telefono e l’IMEI del cellulare — ovvero, il codice identificativo del dispositivo — presumibilmente per controllare se lo smartphone è effettivamente quello da attaccare. Apparentemente, per questa attività, il malware ha una funzione chiamata “CheckValidTarget.”
Notizia segnalata da (Motherboard.vice)