Potrebbe essere dannoso!

Installazione di spyware tramite attacchi di ingegneria sociale in Italia

Potrebbe essere dannoso! Installazione di spyware tramite attacchi di ingegneria sociale in Italia

Original text in Italian

2025

brughiere.noblogs.org/post/2025/11/12/potrebbe-essere-dannoso

Layout

No Trace Project

notrace.how/resources/it/#potrebbe-dannoso

Nota del No Trace Project:

Questo testo descrive come alcunx compagnx italianx siano statx indottx con l'inganno a installare spyware sui propri telefoni tramite attacchi di ingegneria sociale che hanno coinvolto falsi tecnici che affermavano di lavorare per operatori telefonici. Sulla base della nostra esperienza e di quella di altrx compagnx, riteniamo che gli attacchi descritti in questo testo:

- Siano stati probabilmente condotti da attori statali, forse forze di polizia locali o procure.
- Abbiano molto probabilmente richiesto la collaborazione di operatori telefonici, che avrebbero disconnesso e poi ricollegato la linea da remoto per far sembrare che il telefono avesse problemi di connessione, consentendo al falso tecnico di intervenire in modo credibile.

Questo testo ricorda che le capacità di sorveglianza delle autorità repressive sono limitate dalle loro risorse, finanziarie e di altro tipo. Mentre le agenzie di intelligence possono avere accesso a spyware più sofisticati che possono essere installati in modo più affidabile e furtivo, le forze di polizia locali e i procure potrebbero dover fare affidamento su tecniche meno sofisticate.

Ciò dimostra l'importanza di diffondere la consapevolezza degli attacchi di ingegneria sociale all'interno dei nostri movimenti, in modo che altrx compagnx non cadano in questi trucchi.

Nell'ultimo periodo abbiamo visto un aumento nell'utilizzo di spyware contro politici, aziende, avvocati e attivisti. Abbiamo motivo di credere che simili dispositivi si stiano diffondendo anche nel corso di indagini condotte contro individui associati a determinate aree di movimento. Probabilmente sta diventando sempre più facile per le procure affidarsi a start-up esterne per dotarsi di software, non necessariamente sofisticati e costosi come i noti Pegasus, Predator, Graphite o Triangulation (che utilizzano exploit di tipo zero-day con modalità zero-click), ma che svolgono ugualmente la loro infame funzione di raccogliere informazioni riguardanti l'attività del malcapitato senza il suo consenso.

Di recente alcuni compagni hanno subito un'intrusione sui propri dispositivi mobili. Innanzitutto hanno improvvisamente e inspiegabilmente riscontrato l'assenza di connettività internet e telefonica. Contestualmente tutte le telefonate in uscita venivano deviate al centralino dell'operatore telefonico (o questo veniva contattato volontariamente per avere spiegazioni). In ogni caso, dopo la telefonata con l'assistente che, ignaro o ignavo, segnalava probabili problemi di campo, venivano subito ricontattati dallo stesso numero ma da una persona diversa e sedicente tecnico dell'operatore telefonico.

Questo segnalava, invece, il mancato aggiornamento del telefono e dettava, con gentilezza e precisione, tutte le operazioni da eseguire per ristabilire le funzionalità, facendo installare un app con il nome e il logo dell'operatore associato alla scheda telefonica.

Riportiamo i passaggi dell'installazione, da cui si può desumere il grado di intrusività dell'app installata:

- Per prima cosa viene fatta disattivare l'analisi delle app di Play Protect su Playstore, che serve a proteggere il dispositivo da app potenzialmente dannose e a garantire che le app installate siano sicure e affidabili.
- Arriva un SMS con il link ad una pagina simile al sito dell'operatore telefonico. Qui si viene indotti a cliccare su

un bottone graficamente simile a quello di Google Play per scaricare l'«aggiornamento».

- Il file viene in realtà scaricato bypassando il Playstore, e aperto dai downloads nonostante gli avvisi da parte del telefono, che vengono tutti fatti skippare. Per completare l'installazione vengono fatte modificare le impostazioni del telefono per consentire l'installazione di app da questa sorgente.
- Dalle impostazioni del telefono viene dato l'accesso alla rete mobile che consente di usare la connessione dati dell'operatore telefonico per inviare e ricevere informazioni.
- Viene dato il consenso all'esecuzione dell'app in background in modo che possa continuare a funzionare anche quando non è attiva sullo schermo, all'attività sullo sfondo, in modo che possa svolgere delle attività mentre è in background e all'avvio automatico, in modo che possa avviarsi all'accensione del telefono senza aprirla manualmente.
- Vengono dati tutti i permessi all'app, plausibilmente Fotocamera, Microfono, Contatti, Telefono, SMS, Calendario, Posizione, Archivio, etc.
- Sempre dalle impostazioni viene disattivata l'ottimizzazione della batteria per l'app in modo da non limitare l'attività per risparmiare energia.
- Il telefono è stato fatto riavviare e alla riaccensione è subito comparso il simbolino verde del microfono in alto a sinistra, poi diventato un punto verde e, infine, scomparso.
- Per chiudere in bellezza, è arrivato un SMS che chiedeva «Sei soddisfatto della mia gestione?»

Plausibilmente, attraverso queste operazioni, tutti i dati contenuti nel telefono (file, media, contatti, messaggi, etc.) sarebbero stati inoltrati ad un server remoto attraverso l'app (spyware) precedentemente installata con l'inganno e reso il telefono una vera e propria microspia

mobile con possibilità di attivare il microfono, la fotocamera, la geolocalizzazione, fare screenshot dello schermo, etc.

Non è difficile immaginare l'origine di questa invasione, considerata l'identità delle persone colpite e le possibilità di chi ha attaccato. Invitiamo perciò a prestare attenzione a episodi di questo genere, nonostante non tutti i malware abbiano bisogno di essere attivamente installati dal proprietario del telefono come accaduto in questo caso.

Questo testo descrive come alcunx compagnx italianx siano statx indottx con l'inganno a installare spyware sui propri telefoni tramite attacchi di ingegneria sociale che hanno coinvolto falsi tecnici che affermavano di lavorare per operatori telefonici.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention. Be careful about what zines you print and where you store them.