Simjacker mette a rischio privacy e sicurezza di 1 miliardo di telefoni

Set 17, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, Phishing, Privacy, RSS, Vulnerabilità 0

La tecnica di attacco permette di colpire qualsiasi modello di telefono sfruttando una vulnerabilità nel codice delle SIM. E viene usato da due anni…

Potremmo definirla una vulnerabilità "democratica", che colpisce sia gli smartphone **Android**, sia quelli con sistema **iOS**.

Stiamo parlando di **Simjacker**, la tecnica di attacco scoperta dai ricercatori di **AdaptiveMobile Security** e che interessa almeno **un miliardo di dispositivi** in tutto il mondo.

La chiave di tutto è **S@T Browser**, una funzionalità integrata nelle SIM dei telefoni e che viene normalmente utilizzata per visualizzarne il contenuto. Il problema è che S@T Browser può anche ricevere istruzioni attraverso semplici messaggi SMS che contengono istruzioni **SIM Toolkit (STK)**.

Come spiegano i ricercatori nella pagina Web dedicata a Simjacker, l'invio di questi comandi avviene in maniera del tutto "trasparente" per il proprietario del dispositivo. **In altre parole: la ricezione del messaggio non viene segnalata in alcun modo e consente, di conseguenza, di portare un attacco silenzioso e invisibile**.

Ma quali sono le azioni che si possono compiere attraverso l'invio di comandi con Simjacker? L'attacco individuato dai

ricercatori è, in buona sostanza, un sistema per tenere sotto controllo la posizione della vittima.

Attraverso un semplice SMS, infatti, è possibile istruire la SIM per inviare una risposta con **la posizione rilevata dal GPS** (o l'identificativo della cella a cui il telefono è collegato se non è dotato di GPS) a un numero predefinito.

Secondo gli analisti di AdaptiveMobile Security, questo attacco è stato utilizzato per almeno due anni da quella che i ricercatori definiscono "una società specializzata nel cyber-spionaggio".

Non ne fanno il nome, ma molti esperti di sicurezza hanno fatto notare che la descrizione corrisponde ad almeno un paio di aziende di spionaggio (per esempio **NSO Group**) specializzate nella fornitura di strumenti di controllo a governi (non sempre di specchiata democraticità) e forze di polizia.

L’uso dei comandi STK, però, apre potenzialmente la strada anche ad altri tipi di attacchi che possono avere conseguenze decisamente più gravi.

Attraverso l’invio di SMS confezionati ad hoc sarebbe possibile, infatti, forzare la SIM a effettuare telefonate o ad aprire automaticamente pagine Web. Un pirata informatico, di conseguenza, potrebbe avviare a distanza una chiamata a un numero a pagamento per frodare la vittima.

La possibilità di “forzare” l’apertura di una pagina Web rappresenta invece un vettore di attacco formidabile per portare attacchi di phishing o colpire uno smartphone con un malware, sfruttando per esempio un exploit inserito nel codice della pagina stessa.

Insomma: gli scenari che si aprono sono devastanti e, almeno per il momento, non si vede quale possa essere la soluzione per correggere la vulnerabilità. **A peggiorare la situazione, poi, c’è il fatto che le SIM vulnerabili vengono stimate in circa 1 miliardo**.

Nel report dedicato a Simjacker, i ricercatori si rivolgono infatti direttamente agli operatori telefonici (gli stessi che hanno lasciato un software obsoleto e pericoloso sulle loro SIM) suggerendo di mettere in atto policy che siano in grado

di filtrare i messaggi per bloccare quelli potenzialmente dannosi.

Condividi l’articolo

Esperti di sicurezza arrestati per effrazione. “Stavamo lavorando”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/17/simjacker-mette-a-rischio-privacy-e-sicurezza-di-1-miliardo-di-telefoni/