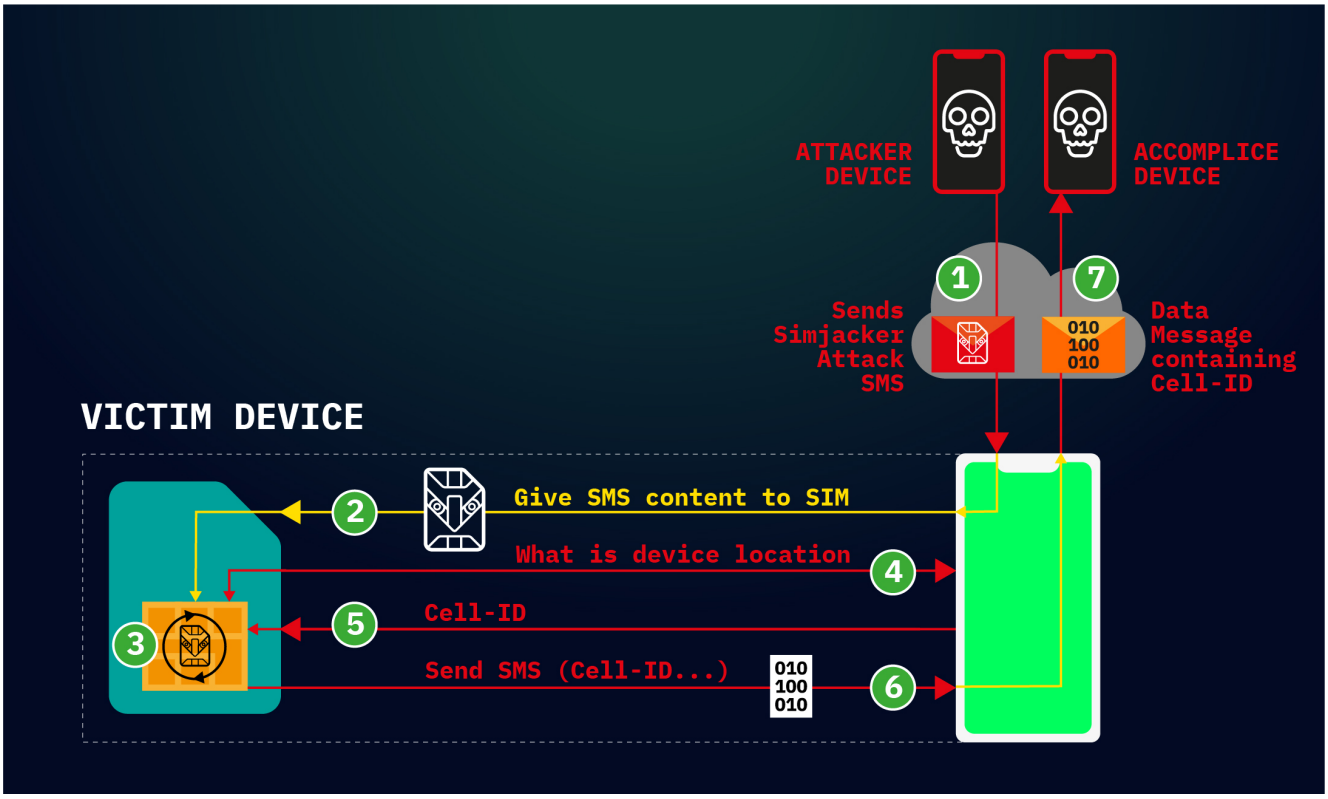
Sim sotto attacco hacker: il virus trasforma lo smartphone in una microspia

Attraverso l'uso della funzione S@t Browser, lo spyware Simjacker prende il possesso della sim card e la istruisce per rivelare informazioni sensibili. A rischio 1 miliardo di utenti

La soluzione più semplice, si suol dire, è sempre la migliore. E la regola vale anche quando la soluzione ha scopi tutt'altro che benevoli. È il caso di un **attacco informatico che sfrutta gli sms**. Già, i messaggini di cui ormai ci siamo dimenticati, soppiantati dalle chat, sono il cavallo di Troia di un **codice tipo spyware**, che **istruisce la sim card** perché prenda il controllo del dispositivo ed effettui operazioni sensibili, **spiando le informazioni** e spedendole all'attaccante.
La falla è stata scoperta da **Adaptive Mobile Security**, azienda

di sicurezza informatica di Dublino specializzata in telecomunicazioni. **Simjacker**, questo il nome con cui è stato ribattezzato l'attacco, rappresenta una minaccia per almeno un **miliardo di proprietari di telefoni, in 30 paesi** in tutti i continenti. E, come se non bastasse, c'è già chi l'ha sfruttata. *"Crediamo che questa vulnerabilità sia stata **utilizzata da almeno due anni** da un gruppo di attacco altamente sofisticato"*, mettono nero su bianco i ricercatori. Nello specifico, *"una **compagnia privata che lavora con i governi** per monitorare individui"*.
Una vera e propria **operazione di spionaggio**, che mette milioni di persone a repentaglio, perché si basa su una funzione non più aggiornata dal 2009 e perché può colpire indiscriminatamente tutti i modelli e le marche di smartphone sono esposti. I ricercatori di Adaptive Mobile hanno osservato che Simjacker può prendere in ostaggio **cellulari Apple, Zte, Motorola, Samsung, Google e Huawei** e persino dispositivi internet of things che montano sim card, ma anche e-sim. Una situazione che rende ancora più complesso mettere una toppa.

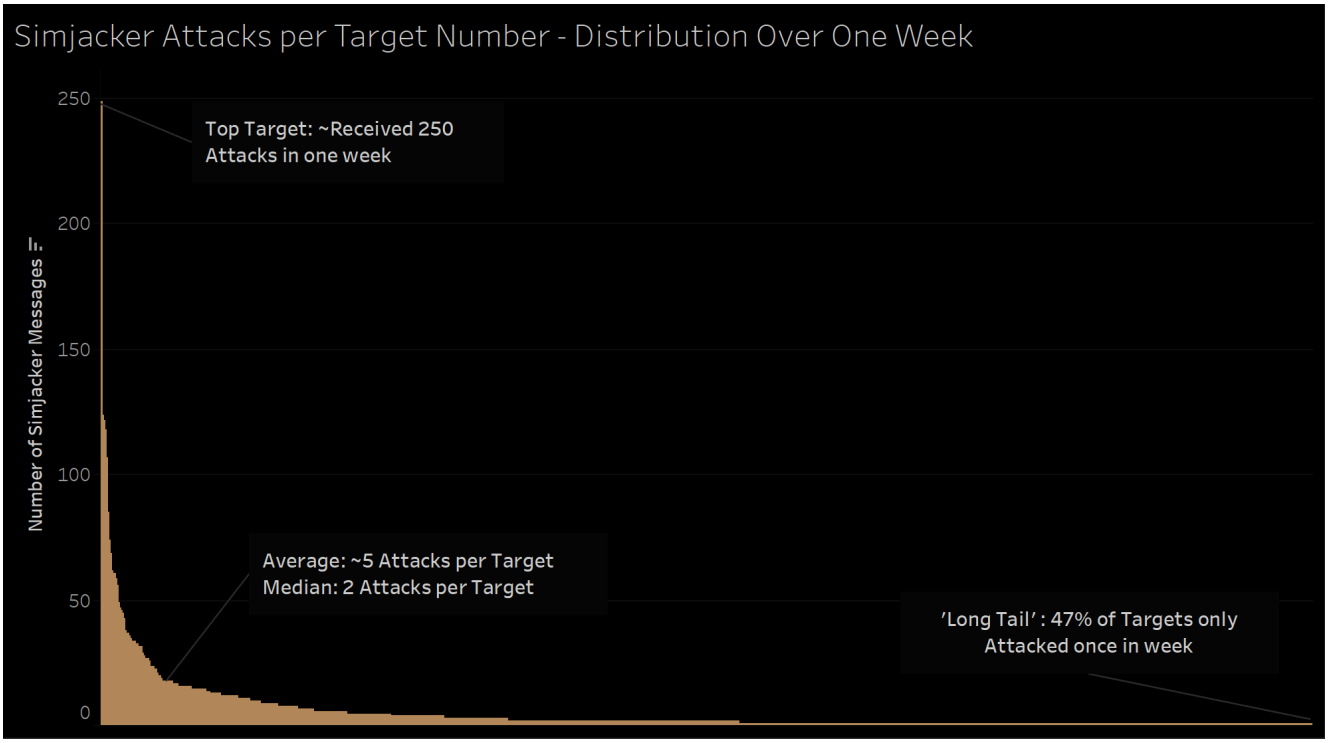


Il funzionamento dell'attacco Simjacker alle sim (Adaptive Mobile Security)

Come funziona l'attacco

Il cavallo di Troia è un **sms**, che contiene le **istruzioni per la sim card**, di cui sfrutta una funzione, il S@t Browser. Il codice maligno raccoglie informazioni sulla localizzazione del dispositivo e sul numero Imei (International mobile equipment identity), che lo identifica, e le spedisce all'attaccante. Il tutto avviene all'**insaputa del proprietario** del cellulare, perché nelle caselle degli sms ricevuti o inviati non c'è traccia di queste comunicazioni.

Per la prima volta, sottolineano i ricercatori, è stato **scoperto un attacco malware via sms**. In precedenza con i messaggini arrivava il link a una pagina web da cui scaricare il virus. In questo caso, invece, il pacchetto è completo.
"*Il S@t Browser permette generalmente alle sim card di implementare* ***servizi a valore aggiunto***", spiega a *Wired* Pierluigi Paganini, responsabile tecnologico della società di sicurezza informatica Cybaze e membro di Enisa, l'agenzia europea della cybersecurity. Per esempio, è adoperato dalle compagnie telefoniche per inviare via sim card il credito telefonico della propria utenza. "*È un protocollo adoperato dagli operatori di telecomunicazioni*", ricorda Alessio Pennasilico, componente del comitato tecnico di Clusit, l'associazione nazionale della cibersicurezza.
Tuttavia, come osservano da Adaptive Mobile, è poco conosciuto, abbastanza vecchio e **non è stato aggiornato dal 2009** ma sopravvive nelle pieghe delle tecnologie mobili. Tanto che gli analisti hanno stimato che è adoperato dalle compagnie telefoniche di almeno 30 Paesi di Europa, Asia, Africa e Americhe e si stima che almeno un miliardo di persone siano a rischio attacchi.



Numeri di attacchi alle sim con Simjacker (Adaptive Mobile Security)

Le conseguenze dell'attacco

Conoscere **posizione e numero identificativo dello smartphone** è già una cattiva notizia. "*Io posso mandare il messaggio infetto a un utente, creare gruppi omogenei e, attraverso questo malware, conoscere gli spostamenti, le intersezioni e le interconnessioni tra queste persone*", aggiunge Pennasilico.
Ma c'è di più. Debitatamente istruito, Simjacker può ordinare alla sim card operazioni più complesse. Come "*recuperare le email; accedere a un browser e scaricare malware; far sì che il telefono chiami un numero quando si inizia una conversazione e usarlo come microspia, oppure che componga numeri a pagamento per attività fraudolente*", elenca Paganini.
Il tutto senza che la vittima se ne accorga e, di conseguenza, possa prendere delle contromisure. È un attacco che si presta a **campagne di spionaggio industriale, sabotaggio, disinformazione e sorveglianza** di massa.
Tanto che gli analisti hanno già visto il malware all'opera. Un'azienda privata di sorveglianza, al soldo dei governi, lo usa da due anni per spiare target specifici. In un paese, si

legge nel rapporto di Adaptive mobile, circa **100-150 persone ogni giorno erano vittime di ripetuti attacchi Simjacker**. In alcuni il controllo durava settimane, in altre era un raid fulmineo. Nel complesso, gli analisti non la descrivono come "*un'operazione di controllo di massa, ma come una progettata per monitorare un ampio numero di individui per vari motivi*". E quando l'attacco non andava a buon fine, la società tirava fuori dal cilindro altri malware simili, meno sofisticati.
Per Paganini "*è tra i peggiori attacchi rivelati di recente*". "*La **falla di Whatsapp** di qualche mese fa era un attacco spaventoso, ma richiedeva attrezzature specifiche e quindi è presumibile che fosse indirizzato a target puntuali. Questo attacco invece colpisce tutti*", osserva Pennasilico.

Le contromisure

E difendersi è complicato. L'ampia varietà di modelli e di dispositivi rende complesso individuare una soluzione. E disabilitare la funzione incriminata potrebbe rivelarsi controproducente. Gli analisti hanno allertato l'associazione Gsm, che riunisce gli operatori, e la Sim alliance, che associa i produttori di card, perché drizzino le antenne sul traffico di sms sospetti con comandi S@t browser e perché **aggiornino le protezioni.**
Nel frattempo il 3 ottobre, alla presentazione ufficiale della ricerca alla Virus bulletin conference di Londra (incontro di cibersicurezza), Adaptive Mobile fornirà più dettagli sull'attacco. "*Trattandosi di **sim card, ci vorrà tempo***", riconosce Paganini. E quindi il rischio che la falla sia adoperata da altri malintenzionati o spioni cresce.
In generale nel 2019 malware e ransomware sono aumentati. E secondo il rapporto Trend Micro, l'Italia è il quarto paese al mondo per numero di malware intercettati nella prima metà del 2019. In parallelo nel Belpaese sta **calando l'uso degli sms**. L'Autorità per le telecomunicazioni ha calcolato che nel 2018 l'invio è sceso del 27% rispetto al 2017. Ridotto a 12 miliardi di unità, circa la metà del 2012. Di contro, sono

sempre più utilizzati dalle aziende per le lo comunicazioni. A cominciare dalle banche.