

## Un bug Gsm può mettere in ginocchio gli operatori: la scoperta arriva da Genova

di **Redazione**

01 Luglio 2014 - 12:43



**Genova.** Se siete stati colpiti dal recente #winddown, sapete cosa può significare ritrovarsi di colpo “senza rete”: in un mondo fatto di connettività esasperata, per qualche ora si è spezzata la sottile linea che ci collega a tutti gli altri, come innumerevoli puntini. Il rischio che un evento simile si ripeta, ma su scala assai più ampia, esiste: e sarebbe tutta colpa di un bug delle infrastrutture Gsm e Umts (gli standard utilizzati oggi per telefonare e navigare da cellulare).

La scoperta arriva da Genova, precisamente da Alessio Merlo, docente presso l'Università di Genova ed E-Campus, e già noto alle cronache per aver scovato qualche anno fa un importante falla di Android a cui si interessò anche la stessa Google. Ed anche questa volta il suo nome si lega ai cellulari, insieme a quello dei colleghi Mauro Migliardi e Nicola Gobbo (Università degli Studi di Padova), Francesco Palmieri (Seconda Università di Napoli) e Aniello Castiglione (Università di Salerno).

In pratica il team ha scovato una vulnerabilità nei protocolli attualmente utilizzati dai nostri telefonini che consente a un malintenzionato di generare traffico malevolo fino a congestionare le linee, a livello di intere aree geografiche. Uno scenario preoccupante, in cui un singolo potrebbe attaccare e quindi ricattare intere regioni isolandone le comunicazioni a prescindere dal gestore.

“L'attacco sfrutta la fase di attachment, ovvero la fase in cui un utente viene autenticato per accedere alla rete cellulare attraverso le informazioni contenute nella scheda SIM”, spiegano i 5: in sostanza la fase in cui il cellulare si accende e “aggancia” la rete. Ogni accensione comporta un lavoro aggiuntivo per il network: Merlo e i suoi colleghi hanno dimostrato come sia possibile, forzando continui e ripetuti “accessi” in pochi secondi, generare un carico di lavoro tale da portare al blocco del sistema

“Forzando l'esecuzione ripetuta di un grande numero di operazioni attachment, seppur destinate a non andare a buon fine, è possibile generare carico aggiuntivo che può portare

ad un degrado funzionale delle attività dell'Home Location Register (HLR) - spiegano - ovvero la componente della rete cellulare in cui sono salvati i dati degli utenti connessi in una specifica macro-area e le regole a cui le chiamate che interessano gli utenti suddetti sono soggette. Un attacco del genere, rende impossibile l'accesso alla rete cellulare agli utenti le cui SIM/USIM siano registrate o tentino di registrarsi presso l'HLR colpito".

Il sistema era finora ritenuto impraticabile nella realtà: richiederebbe decine di migliaia di cellulari, tutti controllati da un'unico aggressore. Il team ha però scoperto a livello teorico un metodo molto più semplice, attraverso l'utilizzo di un dispositivo apposito senza sim. E' sufficiente che abbia un modulo telefonico programmabile e la capacità di effettuare chiamate d'emergenza: con uno di questi dispositivi si simulerebbe l'accesso di decine di cellulari, con poche centinaia il sistema andrebbe in tilt.

Per ovvie ragioni i cinque ricercatori non hanno potuto verificare la loro intuizione nella pratica, attaccando la rete di un gestore italiano. Tuttavia i loro risultati sono stati validati sulla base di misurazioni mai smentite dai provider stessi e quindi ritenute affidabili. Il problema infatti è teorico solo sulla carta: un'organizzazione che disponga delle risorse necessarie potrebbe trasformare questo bug in una vera e propria arma tecnologia per attaccare nemici o dissidenti.

In attesa dell'istituzione di un tavolo tecnico che affronti le possibili soluzioni al problema, il lavoro del gruppo è stato pubblicato anche su prestigiose riviste internazionali, portando anche un po' di Genova nel mondo della tecnologia: per una volta i cervelli non sono "in fuga".