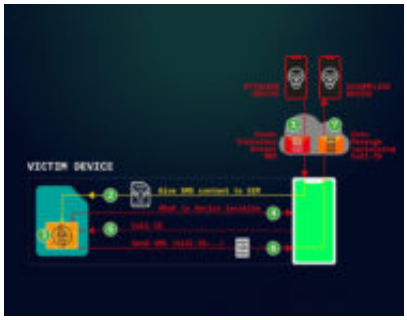
Vulnerabilità S@tBrowser e SimJacker

Author : Daniele Rigitano

Date : 20 Settembre 2019



CyberCrime Conference 2018. Al microfono **Andrea Ghirardini**[1], esperto di Computer Forensics.

Nel corso della sua presentazione, incentrata sugli *exploit* sfruttabili in ambito forense, diede un primo accenno a quello che oggi è noto ai media come **attacco SimJacker**.

Nel dettaglio, in una collaborazione con una società di spionaggio, sono stati forniti al nostro esperto un dispositivo Apple (nuovo e sigillato) e una SIM card (sigillata). È stato inoltre chiesto di provvedere all'aggiornamento OTA del dispositivo alle ultime patch disponibili, all'inserimento della SIM e di controllare che fosse tutto nella norma.

In seguito, i tecnici della società hanno provveduto a una dimostrazione di violazione del cellulare tramite l'invio di un semplice SMS.

A seguito di tale testimonianza, in assenza di prove oggettive, molti dei presenti non hanno dato pienamente credito a quanto asserito da Ghirardini.

Ad oggi, c'è da dire che tutti **ci sbagliavamo di grosso**.

Le vulnerabilità preesistenti

Durante la *CyberCrime Conference* dell'anno successivo, io stesso ho ampiamente dibattuto riguardo la grande varietà di vulnerabilità che ci circondano.

Partendo dalle fragilità dei dispositivi IoT, passando per i bug HW/SW e per i dispositivi mobili, ho approfondito le vulnerabilità, tuttora presenti, nelle **reti mobili**.

Attacchi quali *aLTEr*, *ToRPEDO*, *PIERCER* sono tuttora applicabili alle reti 4G e alle imminenti 5G. Lo scopo di questi attacchi è esfiltrare dati dal dispositivo vittima e, ove possibile, tentare di ottenere il codice *IMSI* del dispositivo[2].

L’ottenimento del codice IMSI decifrato permette a un attaccante di utilizzare il dispositivo della vittima in vari modi: dalla semplice microspia, fino alla clonazione agli occhi dell’ISP, garantendo uno scambio di persona in potenziali crimini informatici[3].

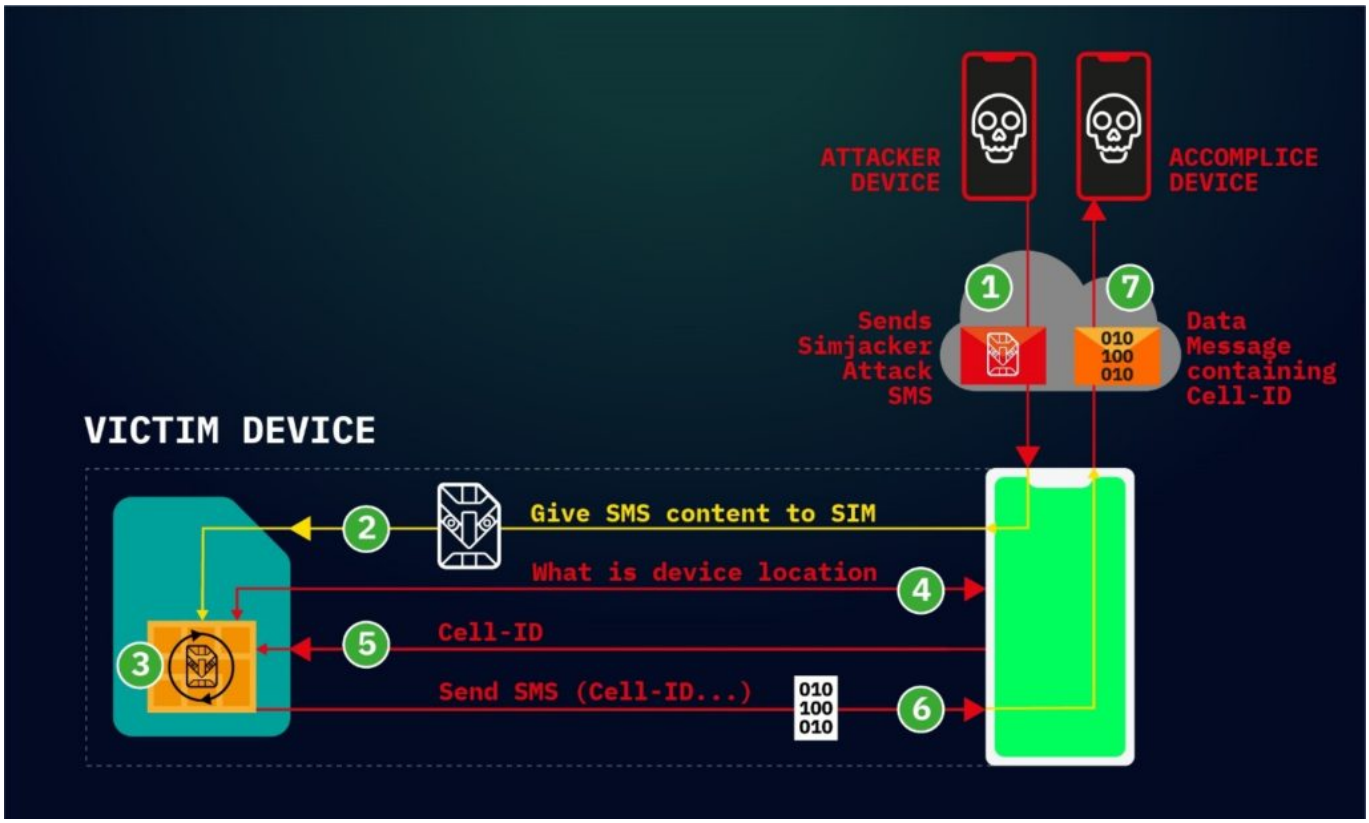
SIMJACKER – come funziona

A inizio settembre u.s. il gruppo *AdaptiveMobile Security*, leader nel campo della sicurezza informatica in ambito telecomunicazioni[4], annuncia di aver scoperto una vulnerabilità intrinseca nel firmware di gestione delle SIM card, che permetterebbe di trasformare ogni dispositivo, banalmente, in una **microspia**.

Il principale attacco Simjacker richiede di disporre di un modem GSM: inviando un SMS contenente un tipo specifico di codice *spyware-like*, con all’interno una serie di istruzioni SIM Toolkit (STK) appositamente predisposte, è possibile per recuperare dati sensibili da una SIM Card ed eseguire particolari tipologie di comandi.

Affinché queste istruzioni funzionino, l’attacco sfrutta la presenza di un **particolare software** all’interno della SIM, chiamato *S@T Browser*.

Una volta ricevuto il messaggio, la SIM utilizza la libreria S@T Browser come ambiente di esecuzione, dove può attivare logiche di esecuzione codice direttamente sul telefono.



Il codice Simjacker in esecuzione è quindi in grado di richiede la posizione e le informazioni specifiche sul dispositivo (IMEI) dal dispositivo.

Una volta recuperate queste informazioni, il codice invia le informazioni a un destinatario tramite un altro SMS (che chiamiamo "messaggio dati"), attivando nuovamente la logica di esecuzione sul telefono. Questo “messaggio dati” è tipicamente recapitato a un telefono controllato dall’aggressore.

Durante tutte le fasi dell’attacco, l’utente non è consapevole né di aver ricevuto l'SMS di tipo Simjacker, né di aver inviato informazioni all’attaccante.

Dettagli della vulnerabilità

L’attacco quindi si basa sullo sfruttamento dell’*utility* S@T Browser - SIMalliance Toolbox Browser -, un’applicazione specificata da SIMalliance[5] e installata tipicamente su tutte le SIM card (e varianti eSIM, USIM).

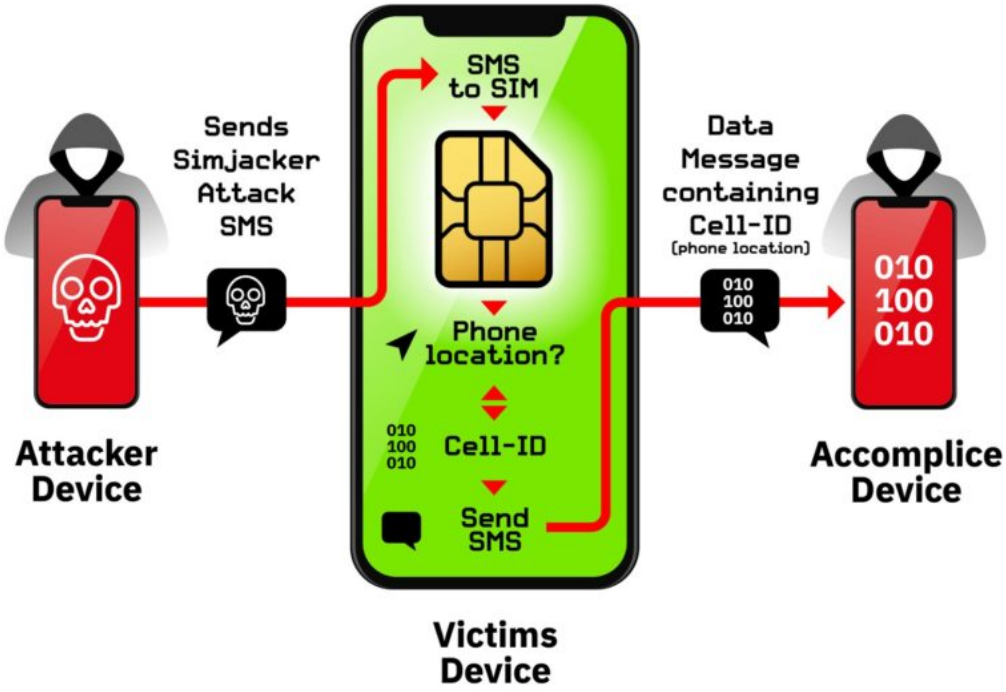
Tale software, non opportunamente documentato, è anche piuttosto **obsoleto**: il suo scopo iniziale era quello di abilitare servizi, come il saldo residuo attraverso comandi SIM.

Nel tempo, le sue funzioni sono state interamente sostituite da nuove tecnologie, mentre le sue specifiche non sono state più aggiornate dal 2009[6]; tuttavia, come molti *software legacy*, è stata dimenticata pur rimanendo attiva in background[7].

Attacchi avanzati

Il vettore di attacco potrebbe essere utilizzato anche per scopi più laboriosi. Simjacker potrebbe facilmente portare al caricamento completo del *payload* di un *malware*.

Questo perché l'elenco di istruzioni richiamate fanno parte di quelle che la carta SIM "deve" eseguire, quindi prive di alcun tipo di controllo sulla genuinità del richiedente (tipicamente un ISP).



Una lista di tali comandi (STK) è la seguente:

- PLAY TONE
- SEND SHORT MESSAGE
- SET UP CALL
- SEND USSD
- SEND SS
- PROVIDE LOCAL INFORMATION
    - Location Information, IMEI, Battery, Network, Language, etc
- POWER OFF CARD
- RUN AT COMMAND
- SEND DTMF COMMAND
- LAUNCH BROWSER
- OPEN CHANNEL
    - CS BEARER, DATA SERVICE BEARER, LOCAL BEARER, UICC SERVER MODE, etc

- SEND DATA
- GET SERVICE INFORMATION
- SUBMIT MULTIMEDIA MESSAGE
- GEOGRAPHICAL LOCATION REQUEST.

Usando combinazioni di comandi, i ricercatori sono stati in grado di aprire il browser web sul dispositivo vittima, far squillare altri telefoni, inviare messaggi di testo e così via. Questi attacchi potrebbero essere utilizzati per soddisfare **molteplici scopi**, quali:

- invio di informazioni errate (SMS/MMS con contenuto controllato dagli aggressori);
- tentativi di frode (componendo numeri a tariffa premium);
- spionaggio (rilevamento della posizione della cella e microspia);
- diffusione di *malware* (forzando l'apertura, tramite browser, di una pagina Web contenente un link a un *malware*);
- *denial of service* (disabilitando la scheda SIM);
- recupero delle informazioni aggiuntive (lingua, tipo di radio, livello della batteria ecc.).

Dal punto di vista dell'utente malevolo, molti degli attacchi sembrano funzionare indipendentemente dal dispositivo in oggetto, perché la vulnerabilità è insita nel firmware di gestione della SIM.

È stato osservato che i dispositivi di quasi tutti i produttori sono vulnerabili: Apple, ZTE, Motorola, Samsung, Google, Huawei; senza contare i dispositivi IoT con schede SIM.

Cosa si può fare

Si ipotizza che questo *exploit* sia stato sviluppato da una specifica **società privata** che lavora con i governi con lo scopo di monitorare determinati individui di spicco.

Per far fronte a questa vulnerabilità, il settore della telefonia mobile dovrebbe lavorare sui seguenti **punti**:

- costringere gli ISP a bloccare questo tipo di attacchi;
- elaborare una patch del firmware in modo da poter autenticare l'ISP che utilizza i comandi STK;
- revisionare o eliminare l'obsoleta tecnologia S@T Browser.

Conclusioni

In base a quanto detto a inizio analisi, la rete cellulare è "buggata" *de facto*.

Molti tipi di attacco sono laboriosi: riuscire a ottenere il codice IMSI di un dispositivo-vittima comporta una mole di lavoro non banale. Inoltre, la condizione principale è che la vittima sia "a portata di tiro" per un attaccante.

Tramite Simjacker, il livello di laboriosità scende notevolmente, poiché è possibile ottenere il codice IMSI codificato (anche in *plaintext*?) della vittima, semplicemente confezionando un SMS *ad hoc* con i giusti comandi STK e senza avere "a portata di tiro" la vittima designata.

Questo potrebbe permettere al dispositivo di un attaccante di assumere tranquillamente le sembianze di un dispositivo mobile vittima in una potenziale attività criminale.

Detto ciò, il **consiglio principale** è che la comunità mobile forzi quanto prima gli operatori mobili ad analizzare e bloccare eventuali messaggi sospetti, soprattutto se contengono comandi

rivolti al S@T Browser.

Dal canto loro, gli operatori mobili potrebbero tentare a modificare le impostazioni di sicurezza del firmware di gestione delle SIM da remoto, o addirittura disinstallare e smettere di usare completamente tale tecnologia obsoleta. Sebbene questo possa essere considerato solo un primo passo, permetterebbe di arginare nel breve tempo una vulnerabilità fortemente impattante.

Note

[1] https://www.ictsecuritymagazine.com/eventi/eventi/cyber_crime_conference_2018/speakers/ghirardini.

[2] https://it.wikipedia.org/wiki/IMSI.

[3] https://www.ictsecuritymagazine.com/atti-convegno-cyber-crime-conference-2019/.

[4] https://www.adaptivemobile.com/about-us.

[5] https://simalliance.org/about-us/mission-objectives/.

[6] https://simalliance.org/key-technical-releases/st-specifications/st-specifications-2009/.

[7] AdaptiveMobile Security ha osservato che il protocollo S@T è utilizzato almeno 30 Paesi la cui popolazione cumulativa ammonta a oltre un miliardo di persone. Quindi un numero considerevole di persone è potenzialmente interessato.

Articolo a cura di **Daniele Rigitano**