PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4370 di Mercoledì 12 dicembre 2018

È possibile intercettare il mio telefono cellulare?

Le tecniche grazie alle quali è possibile intercettare la comunicazione di un telefono cellulare.

Alla fine di ottobre, il prestigioso quotidiano New York Times ha pubblicato una notizia afferente al fatto che i servizi di intelligence russi e cinesi potevano intercettare le telefonate del cellulare personale del presidente Trump. Ovviamente, la possibilità di acquisire queste informazioni poteva essere utilizzata per meglio inquadrare, con ampio anticipo, le possibili future politiche degli Stati Uniti.

La notizia, per quanto recente, non dà certo una informazione del tutto nuova, in quanto in precedenza situazioni simili si erano registrate in relazione all'utilizzo del cellulare del presidente Obama, il quale fu obbligato dai servizi segreti utilizzare specifici apparati protetti.

Per questa ragione ritengo che i lettori possono essere interessati a conoscere le tecniche, grazie alle quali è possibile intercettare la comunicazione di un telefono cellulare.

In estrema sintesi, vi sono due aree nelle quali è possibile intercettare, o meglio ascoltare una comunicazione cellulare. Queste due aree sono presenti in qualsiasi sistema di comunicazione; l'intercettazione può avvenire agli estremi della comunicazione oppure durante la trasmissione. Un attaccante può manipolare uno dei due cellulari o può intercettare la comunicazione in corso sulla rete cellulare. Vi è poi un terzo approccio, che è stato ampiamente pubblicizzato sui quotidiani di tutto il mondo, che viene utilizzato dalla National security Adminstration- NSA. Questa agenzia americana preferisce intercettare in blocco tutte le telefonate che avvengono tramite telefoni cellulari, alla ricerca della presenza di parole chiave, che possono essere utilizzate per approfondire le indagini sulla specifica comunicazione intercettata. La foto che accompagna questo articolo mette in evidenza la stazione di intercettazione, che si trova sul tetto della ambasciata americana a Ginevra.

Quando l'intercettatore, che può essere un servizio di intelligence o un gruppo di criminali specializzati, decide di mettere sotto controllo un cellulare, deve riuscire ad inserire in questo apparato un virus, che permette di smistare le comunicazioni ad un soggetto terzo. Una popolare trasmissione televisiva americana, chiamata *60 minuti*, dette una dimostrazione pratica, in diretta, di questa capacità di intercettazione, nel 2016. Delle fughe di informazioni hanno anche permesso, nel lontano 2005, di conoscere un elenco di apparati cellulari di politici greci che erano sotto intercettazione da parte di un gruppo ignoto. Infine, è possibile inserire questi virus addirittura nei sistemi di trasmissione delle reti cellulari, come è stato fatto dalla NSA per le reti cellulari, che sono state installate dalla compagnia telefonica siriana.

Un'azienda che è specializzata nell'inserire dei virus nei cellulari ha base in Israele e sembra che abbia venduto i propri applicativi a numerosi paesi, come l'Algeria, il Bangladesh, la Grecia, l'India, il Kazakistan e così via, per un totale di 45 paesi.

La possibilità di inserire questo malware negli smartphone varia molto in funzione del tipo di apparato preso a bersaglio. Come regola generale, è più difficile introdurre questi applicativi nei telefoni di Apple, in quanto la distribuzione di questi telefoni è direttamente controllata dalla società produttrice, che provvede anche a periodici aggiornamenti del sistema operativo.

Meno sicuri sono gli apparati di tipo Android, in quanto essi vengono fabbricati da un gran numero di società ed il controllo sull'aggiornamento software è meno incisivo. A conferma di questa situazione, un'azienda specializzata chiedeva 1 milione e mezzo di dollari per un applicativo in grado di violare il sistema IOS, e solo 200.000 $ per uno stesso intervento su sistemi Android. Un altro approccio per inserire questo malware è quello di creare una back door durante lo sviluppo dell'applicativo. È questo un problema che i servizi di sicurezza degli Stati Uniti ritengono sia presente nei telefoni prodotti dalla società cinese Huawei. Per questa ragione, si sconsiglia di acquistare questi apparati a soggetti potenzialmente a rischio e ne è stata bloccata la vendita nei centri commerciali, destinati alle forze armate americane.

A questo punto ci si dovrebbe chiedere quali potrebbero essere i soggetti vittima di queste intercettazioni. Oltre evidentemente a personaggi di rilievo nel mondo politico, non dobbiamo dimenticare personaggi di rilievo nel mondo dell'industria, della finanza e del commercio. Un attaccante, che abbia tempestiva conoscenza di una possibile aumento di capitale di un'azienda, potrebbe mettere a buon frutto queste informazioni.

Per quanto riguarda il comportamento dei gestori telefonici, occorre dividerli in due categorie, a seconda che siano gestori della rete vera e propria, come ad esempio Tim in Italia, oppure soltanto gestori che acquistano traffico e lo rivendono con proprio marchio, come ad esempio Coopvoce e simili. È evidente che questi rivenditori di servizi non hanno alcuna influenza sulle modalità con cui il gestore della rete vera e propria protegge la rete stessa da possibili vulnerabilità.

Infine, è bene ricordare che i servizi di intelligence e le forze dell'ordine non sono molto favorevoli all'utilizzo allargato di tecniche troppo efficaci ed efficienti di protezione delle comunicazioni, perché un attento monitoraggio delle comunicazioni di persone sospette potrebbe dare preziose indicazioni alle forze dell'ordine stesse. Ancora una volta, il diritto alla protezione dei propri dati, da parte di un cittadino, va messo a confronto con il diritto della società civile di essere protetta dall'azione di soggetti malavitosi.

Quale sia il corretto punto di equilibrio, lasciamolo decidere ai lettori!

Adalberto Biasiotti

www.puntosicuro.it