PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4983 di Venerdì 23 luglio 2021

Da Cellebrite a Pegasus

Un cenno sugli strumenti, usati per violare i dati archiviati su smartphone, nonché alcune funzioni operative.

Le cronache dei tempi dettero notizia che una azienda israeliana aveva messo a punto un applicativo, in grado di violare i dati, archiviati in forma criptografica, sugli smartphone in questione.

Negli ultimi tempi sono stati effettuati degli approfondimenti su questo applicativo, mettendo in evidenza alcuni problemi non trascurabili.

Se è vero che questo applicativo è in grado di violare i dati criptografati, è anche vero che questo applicativo presenta alcune debolezze, che potrebbero essere utilizzate in maniera inappropriata.

Una di queste debolezze ha subito attirato l'attenzione degli studi legali, coinvolti in questi problemi, per la ragione che ora vado illustrare.

Quando l'applicativo Cellebrite va ad esplorare uno smartphone, è possibile che una app, installata in precedenza sullo stesso smartphone, possa alterare l'applicativo stesso, in modo da impedire che esso possa estrarre dallo smartphone sotto controllo tutti i dati presenti.

Ad esempio, questa app potrebbe impedire di accedere a determinati dati, o addirittura inserirne deliberatamente altri. Questi dati possono fare riferimento a testo, messaggi di posta elettronica, contatti ed altri dati.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

Questa app surrettizia non lascia tracce, perché non altera i contrassegni temporali presenti. Poiché questa app può anche operare in modo casuale, può essere messa in dubbio la integrità e accuratezza dei dati che vengono prelevati dall'applicativo Cellebrite.

Una tale situazione mette evidentemente in grave difficoltà le forze dell'ordine, che fino ad oggi avevano ritenuto che i dati estratti con questo applicativo rispecchiassero esattamente ciò che era presente all'interno dello smartphone. Se l'avvocato difensore di un soggetto, il cui cellulare è stato così analizzato, può mettere in dubbio il fatto che i dati estratti siano corrispondenti alla situazione effettiva, il valore probatorio dei dati estratti dallo smartphone viene compromesso.

Ancora più preoccupante è il fatto che questa app può essere inserita all'interno dello smartphone ad insaputa del soggetto coinvolto, il quale quindi potrebbe affermare che egli non è in alcun modo direttamente responsabile di un'eventuale alterazione dei dati estratti dal suo smartphone.

Gli studi legali stanno studiando se questa situazione può essere contemplata dal Computer Fraud and Abuse Act, che negli Stati Uniti governa la gestione di questi dati.

Mentre ancora si discuteva su questa situazione, le cronache in questi giorni hanno dato notizia di un nuovo e clamoroso utilizzo su larga scala di un altro applicativo, che esso sviluppato da un'azienda israeliana, chiamato Pegaso. Questa azienda israeliana, composta da 250 dipendenti e con un significativo fatturato, mette a punto questi strumenti di intercettazione e li vende a chiunque sia disposto a pagare la fattura. Eventuali vincoli all'utilizzo devono pertanto essere posti dalle entità governative dei paesi coinvolti, e non dalla azienda. Gli specialisti hanno fatto presente che ci troviamo davanti a una situazione non dissimile da quella dei fabbricanti di armi. Un fabbricante di pistole, negli Stati Uniti, può produrre liberamente queste armi e mettere a disposizione dei commercianti. Sono poi le autorità federali le autorità statali che stabiliscono delle regole, in base alle quali tali armi possono essere o meno acquistate dai privati cittadini. La così rapida diffusione di questi applicativi, indipendentemente dall'uso legittimo di legittimo, mette in evidenza alcuni aspetti, che meritano di essere posti all'attenzione dei lettori.

Tanto per cominciare, gli applicativi dei moderni smartphone sono talmente complessi, che non è praticamente possibile garantire che non esistano dei buchi, che possono essere utilizzati da applicativi fraudolenti. Le tecniche di aggiornamento, messi appunto dai produttori dei due principali sistemi operativi, si basano sostanzialmente sulla tecnica di mettere una toppa, dopo che un buco è stato individuato.

Un problema che devono risolvere gli sviluppatori di questi applicativi di spionaggio e la scelta della modalità con cui questo applicativo può essere caricato sullo smartphone, oggetto dell'attacco. Vi sono tecniche ormai ben note, come ad esempio messaggi fraudolenti di posta elettronica, apparentemente inviati dalla banca del soggetto oppure da un corriere, che avverte che un pacco in attesa di essere consegnato. Negli ultimi tempi sono stati individuati anche messaggi pubblicitari, che promuovono apparati di potenziale interesse per il soggetto preso di mira, che offre uno prezzi oltremodo favorevoli prodotti assai attraenti. Basta cliccare su questo messaggio pubblicitario per consentire al software fraudolento di scaricarsi sull'apparato bersagliato.

L'esperienza ha dimostrato che le tecniche di difesa sono sempre in forte ritardo, rispetto all'evoluzione delle tecniche di attacco e quindi l'unico vero efficace metodo di difesa è quello di non utilizzare l'apparato ed anzi tenerlo anche spento, perché molti applicativi possono attivare la funzionalità di tracciamento, che può costituire comunque un'informazione preziosa per chi ha presa a bersaglio un apparato.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it