PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5298 di Lunedì 19 dicembre 2022

Quanti lettori conoscono EncroChat?

Dopo le centinaia di arresti di circa un anno fa, nuovi interventi radicali delle forze dell'ordine hanno smantellato questa rete in tutta Europa.

EncroChat è il nome di una rete di comunicazione per telefoni cellulari, messa a punto da una organizzazione criminale per garantire agli utenti uno scambio crittografato e protetto di comunicazioni, perlopiù afferenti al traffico di droga.

I telefonini criptati venivano venduti a circa 1000 $ l'uno, ma questa era solo la spesa iniziale, perché poi l'utente doveva pagare un abbonamento annuale del valore di diverse migliaia di dollari. L'utilizzo di questa rete permetteva di accedere a comunicazioni protette di altissimo livello, o almeno così garantivano i gestori della rete.

Il sistema operativo dei telefonini era basato su Android, ma venivano tolti tutti i servizi non indispensabili, come ad esempio il microfono ambientale, le fotocamere e il tracciamento con GPS. Inoltre, gli smartphone venduti alla rete criminale potevano essere puliti, privandoli di qualsiasi dato in essi memorizzato, inserendo un codice di autodistruzione. Tutte le comunicazioni passavano esclusivamente attraverso i server di EncroChat ed i progettisti della rete garantivano la pratica inviolabilità degli algoritmi di cifratura dei messaggi e delle conversazioni.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[ALDIG02] ?#>

L'unione delle competenze degli esperti di informatica delle forze di polizia tedeschi, francesi ed olandesi, unite al prezioso supporto di Europol, ha permesso di violare l'algoritmo di cifratura, mettendo a disposizione delle magistrature inquirenti di vari paesi tutte le informazioni necessarie per arrestare centinaia di malviventi e sequestrare gigantesche partite di droga.

I gestori di questa rete ad un certo punto si erano accorti che erano comparse alcune anomalie, riconducibili ad un malware, iniettato su alcuni dispositivi. L'allarme subito inviato a tutti i possessori telefonini è però giunto in ritardo, tanto è vero che nel frattempo le forze dell'ordine erano già entrate in azione.

Una fonte investigativa italiana ha confermato che anche in Italia questi telefonini erano largamente utilizzati, ma non sono state fornite informazioni su eventuali interventi delle forze dell'ordine.

È interessante esaminare la struttura di questi apparati telefonici, che potevano funzionare con due modalità:

- premendo il solo pulsante di accensione dell'apparato, il telefono caricava un sistema Android normale;
- premendo il pulsante di accensione, assieme a quello del volume, il telefono caricava un applicativo protetto, sviluppato dai gestori della rete.

È bene notare, al proposito, che in linea di principio nulla impedisce ad un cittadino di avvalersi di sistemi di comunicazione non standard, in grado di assicurargli un'elevata protezione delle proprie comunicazioni.

Il problema nasce quando la finalità della protezione della comunicazione è legata allo svolgimento di traffici illeciti.

È anche interessante rilevare come servizi di comunicazioni protette sono presenti sul mercato già da parecchio tempo.

Gli specialisti olandesi, che erano in prima fila nelle operazioni di violazione della rete, non hanno evidentemente mai svelato le tecniche utilizzate, ma secondo alcuni esperti del settore gli investigatori avrebbero penetrato il network di EncroChat effettuando un'operazione di hacking, che permetteva di inserire un malware della rete stessa.

Secondo altri esperti, la penetrazione sarebbe avvenuta inviando degli applicativi di aggiornamento, sviluppati dagli investigatori.

Tra le ultime notizie fornite dalle forze dell'ordine vi è quella relativa all'estradizione di alcuni sospetti, coinvolti in questa rete, dalla Spagna alla Francia.

Al proposito, è interessante rilevare che la legge sulla estradizione, in vigore in Spagna, consente l'estradizione di un soggetto solo se in entrambi i paesi coinvolti è presente lo specifico reato.

Questo limite è stato fortunatamente superato da un'importante decisione del consiglio d'Europa, che ha superato questo limite per 32 tipi di attività criminali, tra cui traffico di droga, riciclaggio di denaro sporco e appartenenza ad un'organizzazione criminale.

Ricordo ai lettori, che comunque desiderano utilizzare un telefono cellulare con più elevate caratteristiche di protezione da intercettazioni, che è sufficiente andare su Internet e trovare numerose offerte, con prezzi che variano da 200 a 1000 ?, più un significativo canone annuale!

Adalberto Biasiotti

Licenza Creative Commons

www.puntosicuro.it