L’invasione dei Trojan, i file “malevoli” amati dalle procure. Giulia Merlo

L’ultima “vittima” è stata l’ex governatrice umbra. Si installa in tutti i dispositivi mobili trasformandoli in **microspie portatili** registrano **audio**, **messaggi** e **fotografie dell’indagato** che non ha più nessun segreto

L’ultima in ordine di tempo a incappare nel loro utilizzo a fine giudiziari è stata l’ormai ex presidente della Regione Umbria, Catiuscia Marini. L’inchiesta sulla sanità in regione e sui presunti scambi di favori per le nomine di persone amiche si regge principalmente su intercettazioni: telefoniche, ambientali e attraverso il cosiddetti Trojan horse. Questo strumento di indagine, che in gergo tecnico si definisce malware – un file “malevolo” che si installa in

tutti i dispositivi mobili e che li trasforma in microspie portatili addosso all'indagato, di cui registrano audio, messaggi e fotografie.

Si tratta di un file apparentemente innocuo, che finisce nella memoria del dispositivo mobile attraverso allegati mail o app gratuite, ma che funzione esattamente come l'oggetto di cui porta il nome: il cavallo di Troia. Una volta installato sul cellulare o sul pc, gli inquirenti hanno pieno accesso a tutti i dati contenuti e a tutto ciò che avviene, dalle chiamate ai messaggi, fino all'utilizzo della fotocamera. Nel caso della Marini, il Trojan era installato nel telefono del dirigente regionale Emilio Duca (oggi ai domiciliari) e ha prodotto diverse intercettazioni, diventando l'orecchio segreto della Procura di Perugia e della Guardia di Finanza nelle stanze della Asl e della Regione.

Proprio per l'estrema invasività nella sfera della privacy dell'indagato, l'utilizzo del Trojan come strumento di indagine è stato più volte modificato da parte del legislatore, riducendone – o allargandone – la fattispecie di utilizzo. La riforma Orlando del 2017 permetteva l'utilizzo del malware limitatamente ai reati di mafia, terrorismo e criminalità organizzata. Questa previsione aveva reso inutilizzabili le intercettazioni attraverso Trojan di Alfredo Romeo, al centro del caso Consip: la Cassazione le aveva infatti ritenute disposte "senza una reale notizia di reato perchè Romeo non era interessato dalle indagini di criminalità organizzata che si stavano compiendo". Inoltre, la riforma Orlando aveva introdotto anche proceduralmente una serie di paletti.

Innanzitutto, il decreto autorizzativo del giudice deve indicare le ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini; l'attivazione del microfono deve avvenire solo in conseguenza di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei

limiti stabiliti nel decreto autorizzativo del giudice; l'attivazione del dispositivo è disposta nel domicilio soltanto in caso di svolgimento in corso di attività criminosa, (questo punto in particolare aveva provocato le reazioni della magistratura, che lamentava la complessità di tale requisito) e altri dettagli previsti dalla delega.

Con l'approvazione della legge Spazzacorrotti da parte dell'attuale governo Conte, invece, l'impiego del Trojan è stato esteso anche alle indagini per reati contro la pubblica amministrazione, puniti con la pena della reclusione non inferiore al massimo a 5 anni. Proprio per questa ragione, la guardia di finanza ha potuto per la prima volta piazzare questa "cimice" ipertecnologica nel cellulare di un funzionario regionale. Inoltre, la Spazzacorrotti ha abrogato anche alcuni dei paletti fissati all'utilizzo: in particolare, ha abrogato la norma che impediva l'uso dei Trojan "quando non vi è motivo di ritenere che ivi sia stia svolgendo l'attività criminosa". Dunque – almeno potenzialmente – ne ha allargato l'utilizzo anche a tutte le fasi temporalmente precedenti, non fissando più un requisito almeno indiziario per "l'accensione" del Trojan.

Non solo, anche dal punto di vista della motivazione all'utilizzo, la norma voluta dal Guardasigilli Alfonso Bonafede non rende più necessaria, nel decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico, l'indicazione da parte del Pm delle ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini.

Lo strumento si presta non solo ad usi di giustizia, ma anche ad abusi. Il caso recente più noto di installazione all'insaputa di privati cittadini di un Trojan sui loro dispositivi mobili è stato lo scandalo "Exodus", risalente allo scorso marzo: secondo le rivelazioni fatte da Security Wthout Borders – organizzazione no- profit attiva sui diritti digitali – in Italia è stato diffuso su ampia scala un trojan che si installava sui cellulari attraverso gli Store di applicazioni. Il virus, creato da una casa di sviluppo calabrese e in dotazione alle forze dell'ordine, avrebbe raccolto per oltre due anni i dati personali di circa un migliaio di persone.

Difficile valutare se si sia trattato di un errore da parte della casa di produzione che detiene i server oppure di un tentativo di "valutare" il grado di sicurezza delle piattaforme come Google Play, da cui l'app Exodus è stata scaricata da cittadini ignari di cosa stava finendo nella memoria del loro cellulare. Attualmente le piattaforme web hanno eliminato la app dalla possibilità di venire scaricata e di "infettare" i terminali e la procura di Napoli ha aperto un'inchiesta a carico dell'azienda E- Surv. Tuttavia, il

fenomeno e la diffusione di questo tipo di prassi solleva in tutta la sua complessità la questione del diritto alla privacy e della sicurezza informatica.

di Giulia Merlo

Fonte: https://ildubbio.news

***