Spy-wars: le guerre di spionaggio giocate con i nostri cellulari e computer. Siamo tutti controllati

Autore : Angelo Greco

Data: 14/12/2011

> ***Telefonini controllati da software-spia, in grado di registrare conversazioni, sms, di rilevare la posizione geografica del proprietario e, persino, di modificare il testo dei messaggini inviati. Esistono trojan che si annidano dentro i computer per intercettare le pagine internet consultate, le email, le password, i testi scritti, le conversazioni via Skype.***

In tutto il mondo, enti governativi e società private incaricano periodicamente software house perché mettano **sotto controllo** il traffico della rete cui si agganciano i cellulari di ultima generazione.

Per ogni minuto che segna l'orologio, navigano sul web **168 milioni di email**, 370 mila telefonate via Skype, 600 video nuovi su YouTube, 98 mila tweet, 694.445 ricerche su Google, 1.500 posti sui blog. Evitare che tutte queste informazioni vengano controllate è impresa inutile.

Un mercato da cinque miliardi di dollari l'anno che vede la "**pirateria dei dati**" in rapida crescita. La tecnologia si muove senza i lacci della legge, vive nell'ombra e, proprio per questo, si muove più agilmente dei sistemi a tutela della legalità.

L’Italia.

Un’inchiesta condotta sulle pagine dell’Espresso di questa settimana addita l’Italia come uno dei Paesi più all’avanguardia nel mercato dello spionaggio. **WikiLeaks** ci denuncia al centro di un vera e propria bufera, dove il mercato dei dati personali e dei tabulati telefonici è tra i più selvaggi e incontrollati del globo.

Un’azienda milanese ha creato “**Remote Control System**” (RCS), una vera e propria arma cibernetica. RCS può entrare nei computer, nei tablet e negli smartphone, intercettando mail, conversazioni, post, sms, persino la posizione geografica del suo titolare. Può addirittura **attivare** segretamente la **telecamera**, la macchina fotografica del telefonino o lo stesso microfono, filmando, facendo scatti o registrazioni ambientali all’insaputa del proprietario.

RCS è stato già venduto a 30 clienti in 20 Paesi diversi. Spionaggi politici e commerciali sono le principali motivazioni per l’acquisto di questo 007 telematico.

Poi c’è “**Cogito**”, un software ideato da un’azienda di Varese, in grado di setacciare una quantità enorme di dati e informazioni, analizzandone il significato e le relazioni tra le parole, ricavandone una serie infinite di connessioni e informazioni.

Spesso questi dati vengono raccolti legittimamente per conto della **magistratura**, ma poi rimangono in mani private per essere rivenduti.

Intrighi internazionali.

Molte di queste aziende creatrici di software spia (con tanto di brochure illustrative) sono al servizio dei **regimi dittatoriali**, interessati a reprimere nel sangue le rivolte dei dissidenti. Lo scopo è la sorveglianza di massa, l’interesse di alcuni governi

(principalmente quelli arabi e orientali) a localizzare un individuo, le persone a lui associate e membri di interi gruppi.

Wikileaks ha rivelato che un'azienda fracese spiava ovunque gli oppositori di **Gheddafi**.

Il caso più eclatante è scoppiato poche settimane fa in **Germania**. Lì, il più noto gruppo di hackers (il Chaos Computer Club) ha scoperto un trojan che, installato nei computer, non solo ruba informazioni, ma può anche inserire "file esterni", immettendo nell'hard disk prove false di un nemico politico.

Eric King, dell'organizzazione umanitaria londinese **Privacy International**, lascia un laconico commento a un giornalista dell'Espresso: "*Le leggi europee impediscono l'esportazione di strumenti per torturare, ma non fanno nulla per vietare la vendita di tecnologia che in Paesi come la Siria, Iran, Bahrain aiuta i torturatori. È inaccettabile che le aziende continuino a fornire legalmente sistemi che individuano la posizione degli oppositori e sorveglino i loro siti*".

Consentiamo la persecuzione dei **dissidenti**, poi offriamo loro asilo politico. Un vero controsenso della nostra società, che prima scopre e tutela il concetto di privacy, poi invece la calpesta in nome del progresso.

Spesso le informazioni servono per pescare i sospettati o i criminali prima di passare alle intercettazioni legali; ma, nel frattempo, nelle maglie del database planetario ci finiamo tutti. Peraltro, il concetto di **criminale** varia a seconda del tipo di regime al potere. Così, vengono perseguiti, in determinati Paesi, soggetti che in altri sarebbero considerati **eroi** nazionali.

A questi programmi sono interessate anche le società commerciali, rivolte allo **spionaggio industriale** (primo tra tutti quello della Formula 1) o alla pubblicità. Esse sono disposte a pagare cifre astronomiche pur di entrare in possesso dei nostri gusti e abitudini.

I computer.

Nessun dato contenuto nei nostri computer è realmente sicuro se si viaggia in rete.

Meno del 10% di tutti i siti web rispetta le **linee direttrici dell'OCSE in materia di privacy** (secondo cui le persone hanno il diritto di attendersi che i dati personali forniti attraverso Internet non siano utilizzati senza il loro consenso, hanno il diritto di rettificare eventuali errori e di presumere che i dati saranno tutelati da eventuali utilizzi impropri).

Del resto, l'architettura del ciberspazio dipende dalle **leggi** degli Stati e dagli interessi del **commercio**. Ed entrambi traggono vantaggi dal sapere il più possibile cosa fa la gente e dove lo fa.

“*Per cui non è certo casuale che l'architettura di Internet si vada configurando in modi che facilitano l'identificazione delle persone e la raccolta di dati personali, visto che identificare le persone piace particolarmente agli Stati, e raccogliere dati personali piace particolarmente alle imprese commerciali*”. (Thomas L. Friedman, "New York Times", 26 settembre 2000)

I cellulari.

I cellulari, migliori amici dell’uomo del XXI secolo, sono diventati i suoi principali **rivali**.

Ci sono una marea di società in Internet che vendono **cellulari spia** e pagano **Google** affinché (con il sistema Google adwords) faccia loro pubblicità, indicizzandoli sui motori di ricerca.

Si tratta di software in grado di configurare un normale telefonino in modo da poter

essere **controllato a distanza**, senza che il possessore se ne accorga, oppure in modo che possa funzionare come telecamere e microfono. Il tutto a **prezzi accessibili** per chiunque.

Altri siti **spiegano**, passo dopo passo, come modificare il proprio smartphone affinché controlli il **partner** o l'**avversario** di lavoro. Il tutto alla mercé di chiunque.

La vostra privacy è sotto pericolo continuo. Ciò nonostante, se credete ancora che il problema non vi riguardi, che le intercettazioni siano solo per scopi militari o per interessi economici al di sopra di voi, provate a pensare a **quante email** avete ricevuto sino ad oggi in cui erano probabilmente presenti, in **copia nascosta** (il campo "ccn"), altre persone, capaci di leggere la vostra risposta…

La legge.

Il fatto che questi comportamenti siano astrattamente possibili, pubblicizzati e, addirittura, commercializzati alla luce del sole, non vuol dire che essi siano anche leciti. V'è un'ampia tutela che qui sotto evidenzieremo, cui si può far ricorso sia nei confronti dello **spionaggio** commerciale, sia nei confronti del **marito geloso**.

Al primo gradino della scala dei divieti c'è la Costituzione che, all'art. 15, proclama l'**inviolabilità**, la **libertà** e la **segretezza della corrispondenza** e di ogni altra forma di comunicazione, ivi comprese quindi anche le email, gli short message, le conversazioni telefoniche. Le eventuali **limitazioni** possono avvenire solo con un atto motivato del Giudice e con il rispetto delle garanzie previste dalla legge.

Ogni violazione di tale diritto, dunque, trova nella più somma delle leggi una rigorosa censura.

Al successivo gradino delle tutele, c'è la legge sulla privacy **[1]** che vieta ogni interferenza, sia pure se eseguita con strumenti di per sé leciti (per es., il telemarketing), all'interno della sfera di riservatezza del privato, quando non è stata da questi preventivamente autorizzata.

Si tratta di una normativa di carattere **civilistico**, la cui violazione comporta solo la possibilità di chiedere la **rimozione** del comportamento illecito e il conseguente **risarcimento del danno**.

In ultimo c'è la tutela **penale**. Un complesso corpo di norme sanziona ogni condotta volta a ledere, con l'ausilio dei più svariati sistemi, la sfera di riservatezza della persona, creando una illecita intrusione nella vita privata e professionale del singolo.

Il legislatore, in particolare, consapevole della precarietà di un assetto codicistico risalente al 1930, ha introdotto una serie di nuovi delitti **[2]**. Si è così cercato di attribuire disvalore a qualunque condotta che, tramite qualsiasi apporto o accorgimento tecnico, possa illecitamente captare, impedire comunicazioni di tipo telefoniche, informatiche o telematiche.

La foto del presente articolo è un'opera artistica di Dantemanuele De Santis, DS Photostudio. Ogni riproduzione riservata.

Note:

[1] Legge 196/2003.

[2] Dapprima con la legge 8/04/1974 n. 98 (introduttiva dell'art. 615 bis del codice penale, che punisce le illecite interferenze nell'altrui vita privata), successivamente con legge 23/12/1993, n. 547 (a seguito di raccomandazione del Consiglio dell'Unione Europea del 13/09/1989 N° 99), che ha a sua volta introdotto gli articoli 615*ter* c.p., 615*quater* c.p., 615*quinquies* c.p., 615*sexties.*