• Anno 26 - n. 143 - € 3,00* - ChF. 4,50 - Sped. in a.p. art. 1, c. 1, legge 46/04 - DCB Milano - Lunedì 19 Giugno 2017 •
* Offerta indivisibile con Affari Legali (ItaliaOggi Sette € 2,50 + Affari Legali € 0,50)

• VERSO UNICO 2017: TUTTE LE NOVITÀ PER I CONTRIBUENTI • a pag. 11

ItaliaOggi Sette
IL PRIMO GIORNALE PER PROFESSIONISTI E IMPRESE

Dio ti vede. E anche il giudice

Con i trojan di Stato può ordinare l'accesso a computer, smartphone, radio, tv, trasformarli in micidiali strumenti d'intercettazione e acquisire tutti i dati

DI MARINO LONGONI
mlongoni@class.it

Nella riforma del processo penale, varata in via definitiva dalla Camera il 14 giugno, c'è un aspetto, passato sottotraccia, che rischia invece di avere effetti dirompenti. Si tratta del comma 84, lettera e), con la quale si legalizzano i captatori informatici, più noti come trojan di Stato. Si tratta di malware che possono essere inseriti in smartphone, computer, apparecchi tv, perfino automobili e in tutti gli altri strumenti connessi a internet e che consentono di assumere il totale controllo da remoto dell'apparecchio infettato con conseguente possibilità di accedere a tutto il suo contenuto (contatti, email, dati di navigazione, comunicazioni telefoniche, chat, file, foto ecc.) e di attivare, sempre da remoto, il microfono o la telecamera, trasformando il cellulare o la playstation in uno strumento di intercettazione. In pratica questi virus una volta iniettati possono intercettare tutte le conversazioni, email o qualsiasi altro tipo di dato, possono anche prendere documenti, foto e video e sparire senza lasciare traccia. Infine possono modificare i contenuti dei file e dei dati presenti negli strumenti informatici. Le intercettazioni telefoniche via cavo sono ormai preistoria. Queste tipologie di indagine potranno essere attivate non solo per la ricerca di prove relative ai reati più gravi (mafia, terrorismo, concorrenza sleale), ma anche per attività criminali minori, collegate a sostanze stupefacenti, reati di ingiuria o minaccia, frode commerciale e vendita di prodotti alimentari non genuini. Praticamente sempre.

Di fatto con questa norma si finisce per dare una copertura giuridica molto ampia a una prassi già da tempo adottata dai tribunali e legittimata finora, ma in modo parziale e incompleto, da poche sentenze della Corte di cassazione. La più importante è la Sezioni unite n. 26889/16, con cui la Corte ha sancito la legittimità, limitatamente ai procedimenti di criminalità organizzata, dell'uso dei captatori informatici al fine di effettuare intercettazioni di conversazioni tra presenti in luoghi di privata dimora.

Naturalmente ad occuparsi di queste attività saranno società private delegate dal tribunale. Società commerciali che, una volta sperimentato il potere enorme che le conoscenze informatiche mettono a loro disposizione, potrebbero essere anche tentate (loro o qualcuno dei loro dipendenti) di prestare i loro servigi non solo ai tribunali. I clienti non mancano di sicuro. Quello che una volta gli investigatori privati facevano con grande impegno e dispendio di tempo, e con risultati spesso modesti, ora si può fare a costi contenuti e con la garanzia di ottenere una quantità di informazioni sterminata. E certamente già lo si fa su larga scala in tutto il mondo. Basti questo caso, ovviamente non di pubblico dominio: una grande azienda italiana del fashion si accorge che i suoi modelli, dopo due o tre giorni dalle sfilate sono già in vendita su internet, identici, ovviamente taroccati. Chiede la consulenza di un esperto in cybercrime e si accorge che, grazie a un trojan, tutto quella che passava sui suoi computer veniva immediatamente girato a un server cinese, dove aziende specializzate riuscivano a produrre e commercializzare in tutto il mondo i suoi modelli subito dopo la presentazione ufficiale.

Secondo Europol, la bassa probabilità di identificare e perseguire i crimini informatici li colloca tra le attività più redditizie e a basso rischio da un punto di vista criminale. Nel 2016 il tasso di crescita di queste attività ha superato il 70%. Nel Regno Unito la criminalità informatica rappresenta il 53% di tutti i crimini commessi. Il costo del cybercrimine nell'economia globale si aggira tra i 375 e i 575 miliardi di dollari. E non fa che crescere.

Oggi ancora poche persone sono consapevoli dei rischi connessi all'uso degli strumenti elettronici (ma i manager delle più importanti società americane hanno già l'accortezza di lasciare i propri smartphone in un'altra stanza, quando devono partecipare a riunioni importanti). Non c'è dubbio che di qui a pochi anni la consapevolezza di questi rischi sarà generale. A quel punto la libertà di comunicazione, che ha costruito la più forte spinta all'espansione della rete, si potrebbe ribaltare nel suo contrario.

Come le strade romane nel medioevo, sempre più infestate di briganti, finirono per non essere più utilizzate, sarà questo, a breve, anche il destino delle autostrade informatiche?