DOPO IL CASO HACKING TEAM

# Smartphone e pc tesori degli 007

Per le intercettazioni telematiche +65% in dieci anni - I rischi dell'esternalizzazione

di **Roberto Galullo**
e **Angelo Mincuzzi**

I cecchini informatici si adeguano ai bersagli da colpire: se prima la violazione dei dati sensibili o segreti correva solo sul filo del telefono ora segue il flusso dei pc e, sempre più, degli smartphone.

Il caso Hacking Team – la società italiana sottoposta il 6 luglio a un attacco che ha violato 400 gigabyte di dati riservati pubblicati online su Wikileaks– svela, suo malgrado, uno scenario con il quale fare i conti. Le imprese italiane che operano nel settore delle intercettazioni – nel 2014 erano 148, con 1.910 dipendenti, 198mila interventi operati e un fatturato di 285 milioni ai quali si aggiungono gli 85 milioni della filiera – sono all'avanguardia nel mondo (i competitor sono soprattutto israeliani, inglesi, tedeschi e statunitensi). Oltre alle società che vendono software-spia (come Hacking Team) ci sono quelle che vendono, noleggiano agli organismi statali le apparecchiature e i server nei quali immagazzinare il flusso di informazioni.

## I dati ministeriali

Che l'hackeraggio sia indirizzato verso pc, tablet e telefoni intelligenti è confermato dai dati del ministero della Giustizia. In dieci anni le intercettazioni telematiche sono aumentate del 65%, passando dai 1.854 bersagli del 2004 ai 3.058 del 2013 (ultimo anno rilevato e reso noto il 23 gennaio 2015 con l'apertura dell'anno giudiziario). Anche a voler prendere in considerazione l'ultimo biennio rilevato la tendenza è confermata: rispetto al 2012, le intercettazioni telefoniche restano pressoché costanti mentre aumentano sia le ambientali (+4%) che le telematiche (+35%).

È la crescita più sostenuta nel raffronto con le intercettazioni telefoniche e quella ambientali che, numericamente, continuano a rappresentare le tipologie più utilizzate. Le prime sono cresciute del 53,2%, passando da 81.307 utenze sotto controllo nel 2004 alle 124.610 del 2013. L'aumento meno significativo riguarda le intercettazioni ambientali, passate dalle 10.270 del 2004 alle 14.106 del 2013 (+37,5%).

Anche se le spese per le intercettazioni telematiche non sono ancora paragonabili alle altre, sono comunque in aumento. Nel 2012 hanno toccato 3,48 milioni mentre l'anno successivo hanno raggiunto i 4,73 milioni di euro (+35,6%), in controtendenza rispetto al capitolo di spesa complessivo delle intercettazioni sceso dai 218 milioni del 2012 ai 215 del 2013.

## Da Milano a Reggio Calabria

Da Nord a Sud investigatori e inquirenti si infiltrano sempre più nei pc e negli smartphone dei bersagli, soprattutto quando questi ultimi sono terroristi o mafiosi. Lo dimostrano due casi esemplificativi, l'uno a Milano e l'altro a Reggio Calabria.

Nel capoluogo lombardo l'inchiesta sui foreign fighters dello Stato islamico che il 1° luglio ha portato all'arresto dei familiari di Maria Giulia Sergio, la ragazza di Inzago (Milano) partita per la Siria insieme al marito albanese per combattere a fianco dell'Isis, è stata possibile grazie a un software che ha infettato il computer della sorella. In questo modo Ros dei Carabinieri e Digos della Polizia, coordinati dal procuratore aggiunto di Milano Maurizio Romanelli, hanno potuto ascoltare in diretta le telefonate via Skype, prima che fossero criptate. Grazie a questo "007 telematico" gli organi investigativi hanno individuato i coordinatori dei foreign fighters dell'Isis in Turchia e Libia.

Da un capo all'altro d'Italia, l'11 febbraio 2014, lo Sco della Polizia di Stato (il Servizio centrale operativo della direzione centrale anticrimine) e la Squadra Mobile di Reggio Calabria, coordinati dal procuratore aggiunto Nicola Gratteri, hanno svelato una presunta organizzazione criminosa dedita al narcotraffico. I collegamenti tra la famiglia Gambino di Cosa Nostra americana e la 'ndrangheta, sono stati svelati non solo dalla collaborazione con l'Fbi ma soprattutto grazie alle intercettazioni telematiche.

## Non solo Hacking Team

Finora la società milanese Hacking Team è stata leader nella vendita diretta del software ad agenzie di sicurezza e forze dell'ordine nazionali e internazionali, oltre che alla cessione delle licenze alle società di noleggio che hanno il compito di infettare i bersagli per conto degli organismi statali. Questa società, fondata nel 2003 e che nel 2007 ha ricevuto un'iniezione di 1,5 milioni dal fondo Next gestito da Finlombarda gestioni Sgr (controllata dalla regione Lombardia) e dal fondo Innogest capital (ciascuno fondo detiene il 26% del capitale di Hacking team), ha chiuso il bilancio 2014 con un fatturato di 7,4 milioni di euro e un utile di 473mila euro (nel 2013 era stato di 1,8 milioni e nel 2012 di 2,4 milioni).

L'hackeraggio che ha colpito la società milanese è stato preceduto negli anni da casi analoghi – sebbene di minore entità – che hanno coinvolto alcuni tra i principali concorrenti, tra i quali la tedesca FinFisher. Quest'ultima società, la cui sede è a Monaco di Baviera, è stata oggetto di intrusione nel 2014. Wikileaks ha svelato che la società, che avrebbe fatturato in quell'anno 47,5 milioni, aveva ceduto tra il 2013 e il 2014 sette licenze a due clienti, i cui nomi sono coperti, per un importo complessivo di quasi 2 milioni.

Qualche esempio può dare l'idea del prezzo al quale sono venduti alcuni servizi. Un pacchetto che comprende licenza base dei un software-spia e un centinaio di bersagli da colpire supera i 500mila euro. La vendita di un modulo base non scende mai sotto i 250mila euro, ad esempio per infettare un singolo sistema operativo come Microsoft.

## I rischi dell'esternalizzazione

Gli hackeraggi che si sono susseguiti negli ultimi mesi, il più clamoroso dei quali quello di Hacking Team, sollevano il dubbio se sia sicuro delegare a società esterne l'intera filiera delle intercettazioni, a partire dalla raccolta e dalla gestione delle informazioni intercettate. Dubbi che si fanno sempre più forti nelle società del settore. Tommaso Palombo, presidente di Iliia, l'associazione di riferimento delle società che offrono servizi e materiali per le attività di intelligence e intercettazioni è chiaro sul punto. «Secondo noi quello che è avvenuto alla Hacking Team può avvenire anche nelle società dei grandi serveristi – spiega Palombo al Sole 24 Ore – ai quali molte procure demandano le intercettazioni. Una cosa è produrre sistemi, tecnologie e gestire in outsourcing la loro messa in cantiere sui bersagli, altra cosa è la raccolta, la criptazione la conservazione dei dati intercettati».

Lo scenario – inquinato da continui hackeraggi e complicato dall'irrompere del terrorismo islamico – è difficile da prevedere anche se forse la lezione di Hacking Team può aver insegnato qualcosa. Atteso che il vuoto di mercato andrà coperto, è probabile che le società che occuperanno gli spazi vacanti, lo faranno in modo più discreto e meno commerciale. Agiranno sotto traccia per rendersi meno vulnerabili agli attacchi esterni.



## In Italia

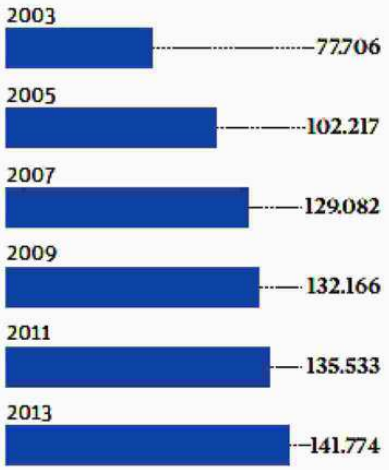
### LE INTERCETTAZIONI

Le intercettazioni dal 2009 e il costo delle operazioni di ascolto in milioni di euro

| | 2009 | 2011 | 2013 |
|---|---|---|---|
| Telefoniche | 119.307 | 121.072 | 124.610 |
| Ambientali | 11.143 | 11.888 | 14.106 |
| Telematiche | 1.716 | 2.573 | 3.058 |
| Costi operazioni di ascolto | 306,07 | 271,18 | 215,0 |

### I BERSAGLI

Trend dei bersagli, aumentati in 10 anni dell'82%, a un tasso medio annuo del 6,2%




Fonte: ministero della Giustizia