

Confisca e utilizzo "sociale" per i pc degli hackers

2010-05-21 12:25:26



Pubblichiamo un articolo apparso su liberainformazione.org scritto da **Lorenzo Frigerio**:

I magistrati di Milano propongono una modifica di legge per dare strumenti alle forze dell'ordine

Far utilizzare alle forze dell'ordine i beni informatici e telematici sottratti agli hacker, promuovendo una modifica legislativa che completi le previsioni in materia di confisca e utilizzo sociale. La proposta, alquanto singolare ma non per questo meno valida, è stata formulata nel corso dei lavori del convegno "Cybersecurity, computer forensics & digital investigation" che si è tenuto la scorsa settimana a Milano organizzato dal capitolo italiano della associazione **I.I.S.F.A. – International Information Systems Forensics Association** (www.iisfa.it).

In due giornate di lavoro, davvero partecipate e animate nella discussione, si sono confrontati magistrati, avvocati, esponenti delle forze dell'ordine, esperti informatici sulle problematiche connesse all'accertamento e al perseguimento dei reati informatici, nell'ultimo decennio in sempre più rapida evoluzione.

È questo un campo nel quale sempre più la criminalità organizzata dimostra di investire grandi somme, non soltanto per aumentare le potenzialità connesse al riciclaggio dell'enorme liquidità che deriva dai diversi business illeciti, ma anche e soprattutto per aumentare l'entità di questi proventi, grazie alla commissione di nuovi reati, un tempo impensabili ma oggi invece possibili perché connessi allo sviluppo delle potenzialità dell'informatica. Alle organizzazioni criminali di stampo mafioso, poi si aggiunge una folta pletora di singoli hackers e di soggetti che giocano in proprio, ma che non sono meno pericolosi, visto che si avvalgono di dispositivi di ultima generazione in grado di sostituire l'azione di più persone contemporaneamente.

Quali sono gli strumenti di contrasto e quali le norme che possono facilitare la repressione di questi reati? A questa domanda ha cercato di rispondere il convegno e il quadro tratteggiato non è molto confortante. Le forze dell'ordine e la magistratura che sono chiamate a confrontarsi con questi fenomeni delinquenziali si trovano a che fare innanzitutto con un campo di battaglia, quanto mai vasto e difficile da monitorare e tutelare, un "cyberspazio" che, proprio per la sua virtualità e indefinibilità, si presta alle numerose scorribande informatiche dei più malintenzionati. Gli strumenti sui quali il personale di polizia giudiziaria può contare invece sono quanto di più obsoleto possa esistere, a fronte dei potenti server e dei computer e quant'altro di ultima generazione che i criminali gestiscono e utilizzano a proprio piacimento.

L'ultimo capitolo di spesa degno di nota per l'acquisto di strutture informatiche per tutte le sezioni di P.G. del nostro Paese risale al 1992 (sic!), peraltro liquidato in una soluzione una tantum e addirittura un anno prima che fossero introdotte nel codice penale le prime fattispecie di contrasto ai reati informatici. Da allora pm e forze dell'ordine hanno dovuto arrangiarsi con quello che passava il convento, facendo di necessità virtù e spesso e volentieri sopperendo con la fantasia e i propri risparmi, acquistando pc e altro di tasca propria.

Anti-Phishing Italia: il portale contro le truffe on-line

Confisca e utilizzo “sociale” per i pc degli hackers

Nel frattempo, la legge 48 del 2008, recependo la convenzione di Budapest sul cyber crime, ha introdotto tutta una serie di nuovi reati nel codice penale e ha aumentato, di fatto, il carico di lavoro delle procure distrettuali, ma **non ha previsto contestualmente le necessità di un aggiornamento professionale per le forze dell'ordine e di una dotazione informatica all'altezza per il contrasto della criminalità informatica.**

Nasce proprio dall'esperienza del pool reati informatici della Procura della Repubblica presso il Tribunale di Milano, costituitosi sul finire del 2004, la proposta in oggetto che tiene conto del fatto che spesso e volentieri **nel contrasto dei reati informatici ci si trova di fronte a beni che possono essere confiscati**, ai sensi dell'art. 240 comma 1 del codice penale, poiché si tratta di **“cose pertinenti al reato”** ovvero “corpo del reato”: stiamo parlando di pc portatili e fissi, cellulari e smartphone, supporti vari per l'archiviazione e documenti.

Allo stato attuale della normativa, tutti questi beni restano inutilizzati per anni presso l'Ufficio corpi di reato anche dopo la loro confisca: il che significa che da un deperiscono rapidamente e dall'altro diventano obsoleti dal punto di vista tecnologico, solo in ragione del semplice trascorrere del tempo.

Ecco che i magistrati di Milano, **Francesco Cajani**, sostituto procuratore del pool reati informatici della procura milanese e **Alberto Nobili**, procuratore aggiunto coordinatore del pool, arrivando a prefigurare una “simbolica ottica deterrente”, propongono di **prevedere ex lege la destinazione di questi beni alle forze dell'ordine**, in ciò richiamandosi a quanto è già oggi previsto nel contrasto alla pedopornografia e agli altri reati per i quali è prevista una attività sotto copertura, come nelle operazioni antidroga e anticontrabbando, nella prevenzione e repressione dell'immigrazione clandestina e, da ultimo, secondo quanto previsto dall'ultimo “pacchetto sicurezza” ai sensi della normativa antimafia.

Se quindi le vetture confiscate ai narcotrafficienti possono essere utilizzate da carabinieri e polizia per pattugliare le città perché non consentire alla Polizia Giudiziaria di utilizzare i pc per inseguire gli hacker da una parte all'altra del cyberspazio?

Per cercare di dare una risposta a questa domanda, **i magistrati milanesi indicano la strada della confisca obbligatoria, limitata ai “beni informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati di cui agli artt. 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 635-quinquies, 640, 640-ter e 640-quinquies del codice penale”.**

Il lungo elenco copre una serie di reati, di cui i più ricorrenti sono oggi l'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.); l'installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-bis c.p.); la falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617-sexies c.p.); il danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.); il danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.); la frode informatica (640-ter c.p.) e le varie forme di truffa (art. 640 c.p.) commesse quotidianamente con l'ausilio di supporti informatici e/o telematici.

Un esempio per tutti è dato dal cosiddetto “phishing” a danno dei titolari di conti correnti online che vengono quotidianamente fatti oggetto di e-mail false che sembrano provenire dagli istituti di credito, ma in realtà hanno soltanto lo scopo di carpire fraudolentemente i dati personali e i codici d'accesso ai conti in questione.

Una volta che sia stabilito con certezza, tramite una apposita analisi di “computer forensics” (n.d.r. vale a dire il protocollo investigativo applicato al mondo digitale per trarre indicazioni utili in sede processuale), il

Anti-Phishing Italia: il portale contro le truffe on-line

Confisca e utilizzo “sociale” per i pc degli hackers

nesso di strumentalità tra i beni informatici e telematici confiscati e la commissione dei suddetti reati, ecco entrare in gioco l'ulteriore proposta dei magistrati milanesi: **la destinazione di questi beni alle sezioni di Polizia Giudiziaria che ne abbiano fatto esplicita richiesta, ai fini di un successivo loro impiego nel contrasto ai crimini informatici.**

Tutta questa procedura ha senso e valore nella misura in cui non vengano pregiudicate le indagini nell'ambito delle quali i beni vengono confiscati e questa valutazione è rimessa al vaglio del giudice chiamato a pronunciarsi sulla destinazione di quanto è stato regolarmente sottratto agli hacker.

Un'ultima norma servirebbe a sanare la situazione di questi beni che siano stati confiscati nel contrasto della pedopornografia, per i quali attualmente viene disposta la custodia giudiziale e successivamente la vendita. Anche in questo caso si suggerisce che vengano consegnati alla P.G. per le indagini in questa delicatissima e complessa materia, che vede coinvolti minori innocenti.

Il quadro completo della proposta ([vedi allegato](#)) è stato presentato a Milano e punta ad arrivare ad una soluzione che se ha già fatto discutere, ha un intento molto chiaro: "evitare dopo il danno la beffa", secondo le parole del pm Cajani che chiede soltanto gli strumenti necessari perché la magistratura, insieme ai suoi collaboratori, possa fare bene il proprio lavoro.

La parola, a questo punto, passa al Parlamento e a coloro che vorranno farsi carico di portare avanti queste indicazioni utili alla lotta contro i crimini del web.

Fonte: Anti-Phishing Italia – www.anti-phishing.it

Image credit: [.Michi.](#) da Flickr