

Attacco a Poste, nuovo caso di terrorismo informatico

2009-10-23 21:46:46



cyber_terrorismL'attacco a Postelitaliane è stato soltanto un attentato dimostrativo, si è trattato di un accesso abusivo al portale web finalizzato al "defacement" (sostituzione) di alcune pagine del sito. Certo, dimostrativo quanto vogliamo, sempre di attentato di tratta. Per questo l'attenzione non si è certo acquietata dopo il comunicato stampa di Poste con cui comunicava che i correntisti non avrebbero subito alcun danno economico a seguito dell'attentato. Secondo quanto riportano i commenti di alcuni esperti si tratterebbe di **un chiaro episodio di terrorismo informatico**. Ciò anche perché tale attacco è stato preceduto di pochi giorni da altri analoghi casi in danno di colossi informatici come Microsoft e Google.

In particolare **due esperti di antiriciclaggio Razzante e Barbetti, hanno messo in relazione questo attacco con altri attentati terroristici telematici avvenuti negli ultimi dieci anni**. E così gli hacker che hanno "bucato" Poste Italiane sarebbero parte di un complesso meccanismo criminale che ormai vede nella rete il più favorevole brodo di coltura per le loro iniziative.

Non sarebbe certo un caso, se i terroristi di Al Qaeda lanciano proclami e reclutano militanti sul web, e non tramite videotape da consegnare ai media. Come non sarebbe **un caso che l'attentato alle Torri Gemelle dell'11-9-2001 sia stato preceduto da un attacco "denial of service" ai siti della Casa Bianca (bloccato per ben 6 ore) e prima ancora della stessa CIA**.

Idem dicasi per Canberra 2004, quando la città australiana rimase isolata per 5 ore con l'interruzione della rete internet pur in assenza di alcun guasto elettrico, a causa dell'intervento estorsivo di cybercriminali.

Secondo quanto riportano i due esperti, **ogni giorno nel mondo vi sarebbero almeno 1400 attacchi telematici** di vario genere, con un incremento annuale registrato dal 2005 ad oggi del 35 %, mentre **in Italia sarebbero in corso attualmente 350 indagini penali a carico di 600 tra persone e aziende coinvolte**. E nella maggior parte dei casi si tratta di attacchi che riguardano il settore finanziario.

Nel 2005, Mark Rash, già a capo della divisione criminalità informatica del Dipartimento di Giustizia degli Stati Uniti, lanciava i suoi allarmi contro le reti di computer "infettate" da organizzazioni criminali, tra cui anche stessa Al Qaeda, che reclutavano cracker e virus writer capaci di generare attacchi volti a minare le vulnerabilità dei sistemi informatici dei principali governi.

In passato attacchi del genere hanno anche portato a sfiorare crisi diplomatiche o crolli in borsa, come accaduto nel 2005 tra Cina e Giappone nel 2005, quando ignoti crackers violarono le pagine cinesi della Sony, tempestandole di messaggi antigiapponesi.

O come accadde **nel 2000 quanto diverse importati società operanti su internet vennero prese di mira e bombardate con attacchi incrociati provenienti da città diverse tra loro** coordinati, con migliaia di messaggi privi di senso, provocando la paralisi del sistema.

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

Attacco a Poste, nuovo caso di terrorismo informatico

Vittime di tali inusitati –quanto mortiferi- attacchi furono **Yahoo**, rimasto inattivo per tutta la giornata; **Amazon**, che chiuse i battenti per circa un'ora; la **Cnn**, interrotta in piena prima serata; **eBay**, che pagò con l'interruzione delle proprie celebri aste; ed infine **Buy.com**, impegnato in quell'istante nel lancio delle proprie azioni in Borsa.

Wall Street registrò un'impennata nelle vendite delle azioni di queste società, provocando il crollo degli indici Dow Jones e Nasdaq. L'ordinamento italiano punisce gli abusi telematici reclusione fino a tre anni, ai sensi degli articoli 651 – ter e 635 bis del Codice Penale. Nel 2003 il Parlamento italiano ha approvato inoltre l'adozione della c.d. E-commerce Directive (2002/38/CE) sul commercio elettronico, che invita le associazioni commerciali, professionali e dei consumatori a contribuire all'elaborazione di un quadro affidabile e flessibile per il commercio elettronico definendone codici di condotta.

Ranieri Razzante, oltre ad essere docente di Legislazione Antiriciclaggio all'Università Mediterranea di Reggio Calabria, è presidente di AIRA, l'Associazione Italiana dei Responsabili Antiriciclaggio. Mirko Barbetti, laureando presso la facoltà di Giurisprudenza dell'Università Luiss Guido Carli di Roma, è assistente dal Professor Razzante e collabora attivamente con AIRA fin dalla sua fondazione.

Il loro interessante articolo è leggibile al seguente link

http://www.wallstreetitalia.com/articolo.asp?art_id=803614

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

Immagine tratta da www.dailymail.co.uk