INTERNER E CRIMINE. I TERRORISTI USANO IL WEB PER COMUNICARE CON TECNOLOGIE CRITTOGRAFATE. LE ORGANIZZAZIONI CRIMINALI USANO IL WEB PER CYBER-TRUFFE E AFFARI ILLECITI

(Corriere Economia, giugno 2008)

Internet è un mezzo efficiente per comunicare e trasmettere informazioni. Per tutti. Anche criminali e terroristi. «Per inviare ordini da una cellula all'altra, scambiare dati con altre organizzazioni malavitose. Non ultimo, eseguire transazioni finanziarie sotto copertura. Ecco il motivo per cui il crimine organizzato e terroristi del fondamentalismo islamico come Al Quaeda, non hanno interesse a mettere fuori uso il web». A spiegarlo è l'inglese ***Simon Moores***, esperto di sicurezza informatica e direttore dell'agenzia Zentelligent. Senza dimenticare che la rete, grazie a connessioni wireless e programmi di comunicazione Voip (voice over internet) rende difficile intercettare telefonate. Il perché secondo Moores è presto detto: «sistemi senza fili come il Wi-Fi consentono di delocalizzare le connessioni in mobilità, specie per gli hot spot dei centri urbani». Inoltre i programmi per comunicare attraverso il web si avvalgono di software con crittografia per l'invio dei dati.

Ed è proprio questa tecnologia che facilita l'uso di Internet da parte di criminali e terroristi. Meglio ancora se si tratta si steganografia, cioè dell'invio di fotografie digitali che al loro interno contengono messaggi criptati. Dopo gli attentati dell'11 settembre i servizi segreti americani hanno scoperto che i gruppi legati a Osama Bin Laden usavano inviare messaggi segreti nascosti nei file di fotografie digitali. «Di fatto chi ne osserva una, dal punto di vista grafico non nota nulla di particolare – spiega Moores - ma una volta analizzata con un programma di decodifica, rivela informazioni nascoste nel file». Non solo. Con tecniche analoghe si inseriscono messaggi segreti in un qualunque brano musicale Mp3. «Anche in questo caso chiunque lo può ascoltare senza notare differenze con la musica originale. Però chi possiede il software di decodifica metterà in chiaro il messaggio nascosto».

Alle organizzazioni criminali il web interessa perché riescono a mettere a segno truffe "mordi e fuggi" in rete. A livello planetario. Un esempio? «Lo scorso anno una donna a Vancouver in Canada, ha fatto spese in un supermercato con la carta di credito - spiega l'esperto inglese - notando solo una doppia strisciata sul lettore». Sembrava un pagamento normale, invece in pochi secondi ne è stato fatto il duplicato elettronico, venduto online a una gang cinese. Poi, sempre via Internet i cinesi hanno trasmesso i dati in un laboratorio illegale del Myanmar (ex Birmania) per realizzare una copia fisica. A ritirarla un emissario della mafia russa. Che in un giorno da Mosca, attraverso una donna corriere, l'ha fatta recapitare a Londra, per acquisti fraudolenti. Valore delle spese, qualche migliaio di sterline. Alla fine è stata distrutta prima che l'ignara massaia di Vancouver si accorgesse della clonazione. Il risultato? L'assicurazione ha risarcito il danno fraudolento della card. Senza però che le polizie canadese, birmana, russa e inglese potessero intervenire. «Problemi di tempi, procedure e competenze territoriali - conclude Moores – ma grazie alla tempistica online, lo scorso anno e solo in Nord America, i criminali hanno duplicato oltre 25 mila card». Rimanendo impuniti.