Poliziamoderna

Divieto di pesca (nella Rete)

Si definisce “phishing” l’insieme di quelle attività che sfruttano le tecniche dell’ingegneria sociale, nonché le vulnerabilità dei sistemi informatici, cioè lo studio del comportamento individuale delle persone, per carpirne informazioni riservate con finalità illegali. Nella grande maggioranza dei casi, si tratta di appropriazione illecita di identità, di denaro o di canali informativi privati. Il phishing è un fenomeno relativamente recente. È molto complesso, perché coinvolge realtà umane assai diverse tra loro ed un mondo tecnologico in costante evoluzione. Da non confondere con il pharming – che è una tecnica distinta e molto più difficile da realizzare – il phishing è un tipo di reato insidioso e subdolo: la priorità del phisher, ovvero di colui che attacca, è infatti sempre e rigorosamente quella di non mostrare in nessun modo le proprie abilità tecnologiche o informatiche, al fine di non farsi scoprire. È quindi molto facile cadere nelle sue trappole, sempre ben confezionate e a volte persino allettanti. Contemporaneamente, però, esistono molti sistemi di difesa preventiva che i singoli utenti possono applicare in totale autonomia. Per scoprire quali sono, abbiamo visto insieme al vice questore aggiunto Stefano Zireddu come si verificano generalmente gli attacchi dei phisher. La divisione in cui opera il vice questore è quella che si occupa dei crimini economici e finanziari commessi online, che vigila con un monitoraggio continuo sulle nuove frontiere del commercio e della circolazione di denaro, che studia attentamente le nuove risorse tecnologiche al fine di garantirne la sicurezza.

Come si va “a pesca” nella rete del world wide web? In linea generale, i processi connessi al phishing seguono sempre le stesse linee standard e si articolano per lo più in pochi e definiti passaggi. In primo luogo, il phisher invia a una lista di utenti un messaggio e-mail, studiato e realizzato ad hoc per simulare una comunicazione ufficiale di una qualsiasi istituzione o struttura che sia familiare ai destinatari. Può trattarsi ad esempio di una proposta di lavoro, di un avviso da parte di una banca, di una comunicazione relativa ad un provider web, oppure della pubblicità di un sito di aste online; normalmente, comunque, il messaggio avvisa l’utente di un problema apparentemente grave ed urgente, relativo al suo conto corrente bancario, al suo account di posta elettronica o alla scadenza imminente di un contratto o di un’offerta che lo riguarda. Il secondo e fondamentale passaggio del processo riguarda il link, che è sempre presente nelle mail “incriminate”: al fine di risolvere il problema segnalato, infatti, il messaggio invita con chiarezza l’utente a seguirlo, clicc

...

01/05/2010