Occhio agli «spam» e al conto in banca

PIRATI INFORMATICI POSSONO SCOPRIRE IL CODICE TRAMITE MESSAGGI INSOSPETTABILI IN INTERNET

Alberto Viotto

NEGLI ultimi mesi su Internet vi sono stati diversi casi di "spam" (messaggi di posta elettronica non richiesti, in cui di solito il mittente è falsificato) tesi a rubare i codici segreti per il prelievo di contanti dagli sportelli automatici. Fortunatamente ben pochi navigatori italiani sono clienti delle banche attaccate, quasi tutte statunitensi, ma in questo caso la creatività dei "pirati della rete" si è superata.

La veste grafica del messaggio è insospettabile e fa pensare ad una vera comunicazione della banca attaccata, che appare come mittente (questo campo è molto facile da falsificare). Il messaggio dice che, per motivi di sicurezza, è necessario che l'utente modifichi il proprio codice di prelievo dei contanti, rimandando ad un sito che sembra appartenere alla banca stessa, ma in realtà è ospitato da un server dei "pirati".

Se si clicca sul "link" proposto si apre una finestra in cui si devono inserire il vecchio ed il nuovo codice, come si fa abitualmente quando si cambia una password.

Inutile dire che il codice non viene affatto cambiato e quello vecchio, ancora valido, potrà essere usato dai pirati per prelievi illegali.

Attacchi di questo genere sono stati rivolti ad istituzioni del calibro di Barclays, Citibank (la più colpita), Bank of America, Visa. I messaggi di spam, veicolo della maggior parte delle truffe, possono provenire anche dai PC di ignari utilizzatori della rete, rendendone più difficile l'individuazione. Alcuni virus, infatti, chiamati "trojan horses" (cavalli di Troia), dopo aver ottenuto il controllo di un PC, restano silenti per un certo tempo per essere poi messi a disposizione degli "spammer" per inviare messaggi a partire da indirizzi insospettabili, senza che il proprietario del PC si possa accorgere di nulla (se non di una attività anomala sul sistema). In questo modo i software antispam che bloccano i messaggi provenienti da indirizzi "sospetti", già utilizzati per altri attacchi, vengono facilmente aggirati.

Secondo alcuni analisti sono in vendita intere reti di PC infettati, che possono essere usati come veicolo di truffe o, peggio ancora, per attacchi contro aziende o organizzazioni sgradite (con un invio di massa di messaggi ai loro indirizzi si possono bloccare facilmente i sistemi informatici). Per non diventare complici involontari dei pirati della rete, quindi, è indispensabile utilizzare un antivirus affidabile, in grado di riconoscere ogni tipo di virus e di aggiornarsi automaticamente per

Virus e posta indesiderata, due problemi gravi della Rete

fronteggiare anche le minacce più recenti. Oltre all'esame dell'indirizzo di provenienza, i filtri antispam controllano il contenuto dei messaggi, bloccando quelli che comprendono parole o combinazioni di parole legate agli argomenti tipici degli spammer (come l'offerta di Viagra) o già rilevate in altri messaggi di spam.

I pirati della rete, però, sono molto abili ad aggirare queste protezioni, sia cambiando continuamente i testi, sia aggiungendo ai messaggi dei caratteri a caso in posizioni poco significative, che non vengono notati dal destinatario ma rendono inefficace il filtro.

Quasi tutti i filtri permettono all'utente di selezionare il livello di protezione che vuole ottenere. E' meglio evitare un livello di protezione eccessivamente alto, perché filtri troppo "severi" rischiano di bloccare messaggi del tutto legittimi (il che è capitato più volte anche all'autore di questo articolo).

In questo caso le conseguenze possono essere ancora peggiori del fastidio arrecato dai messaggi non desiderati; si possono perdere delle occasioni o interrompere relazioni importanti.

Non ci si può quindi fidare più di tanto dei filtri, che possono lasciare passare i messaggi veicolo di truffe. L'unica soluzione è mantenere sempre alto il livello di attenzione quando si utilizza la posta elettronica ed essere coscienti che le truffe sono sempre in agguato.

alberto_viotto@hotmail.com