soldi › l'infiltrato

di Alessandro Calderoni
redazione@millionaire.it

LA TRUFFA CORRE ON LINE

INTERNET, E-MAIL, BANCOMAT E CONTI VIRTUALI. LA FRODE È IN AGGUATO. ECCO COME DIFENDERSI

Avete un conto corrente on line? Fate acquisti in Rete? Volete rispondere a una e-mail arrivata dalla Nigeria? Usate con disinvoltura bancomat e carte di credito? Seguiteci, questo articolo fa per voi e potrebbe mettervi in guardia. Le frodi telematiche, truffe perpetrate grazie alle nuove tecnologie, sono in aumento. Si parla di tremila e 500 denunce nei primi tre mesi del 2007 fatte al Gat, il Nucleo Speciale Frodi Telematiche della Guardia di Finanza. Senza contare quelle pervenute nello stesso periodo alla Polizia Postale e quelle non denunciate. Ma vediamo quali sono i tecnoraggiri più frequenti, grazie all'aiuto del colonnello delle Fiamme Gialle Umberto Rapetto, comandante del Gat, che all'argomento ha dedicato un libro (vedi riquadro a pag. 102).

I classici raggiri

Nella top ten dei sistemi utilizzati per fregare la gente figurano termini stranieri ormai noti ai più. I *dialer* sono quei programmini che, scaricati, sono in grado di interrompere la connessione alla rete e instaurarne una nuova molto più costosa, con tariffazione da chiamata internazionale. «Possono essere molto silenziosi ma non invisibili» suggerisce Rapetto, che invita a controllare le icone di connessione presenti sullo schermo. «Se non si può passare a una connessione a banda larga, che non richieda la composizione di un numero ogni volta, basta comunque innalzare il livello di sicurezza del proprio browser dalle opzioni del programma e chiedere al fornitore di linea telefonica di disabilitare le chiamate verso numeri ad alta tariffazione».

Un altro tormentone degli ultimi anni è il *phishing*, il sistema con cui i truffatori lanciano esche via e-mail, proponendosi in modo anche graficamente credibile come istituti di credito e chiedendo agli utenti le loro credenziali d'accesso ai conti on line, con la scusa di una procedura di aumento di sicurezza. Se l'utente clicca sul link contenuto nel messaggio di posta elettronica è rimandato a un falso sito, normalmente un clone di quello originale, ottenuto con un semplice software gratuito detto *spider* - e se vi inserisce *user id* e *password* cascando nella trappola, il suo conto corrente viene svuotato in men che non si dica. Fine della fase uno. Fase due: come ripulire i soldi e dove farli finire? Ecco una nuova truffa e una nuova e-mail: qualcuno ti contatta offrendoti un lavoro come rappresentante commerciale per una determinata zona e proponendoti di ricevere denaro sul tuo conto corrente e di trattenerne

Dal 2005, ogni giorno, sono circa 8 milioni i tentativi di carpire dati e informazioni personali attraverso una e-mail

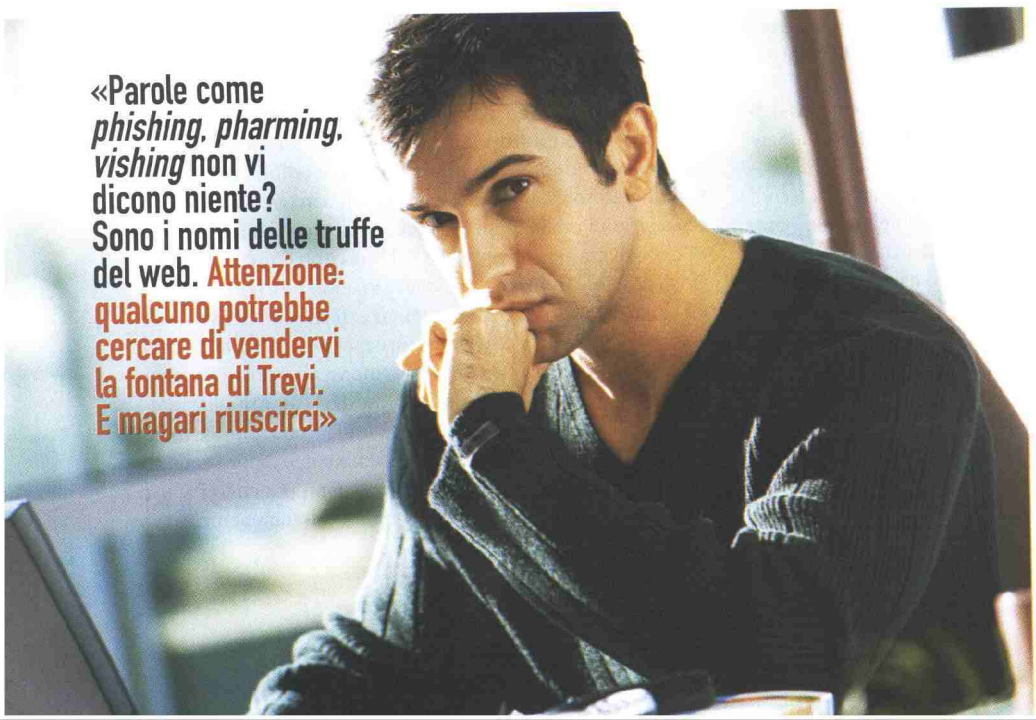
una percentuale spedendo il resto con un servizio di *money transfer* tipo Western Union. «I soldi arrivano davvero e già nel momento in cui finiscono sul conto del cittadino per ripulirsi, l'ingenuo padre di famiglia o il ragazzino in cerca di arrotondamenti diventa suo malgrado partecipe di una grande operazione di riciclaggio e rischia il carcere. In pratica, i soldi che lui riceve sono quelli rubati dal conto on line di un altro truffato».

Frodi nuove ma già note

L'evoluzione del phishing si chiama *pharming* e si avvale di un escamotage tecnico per superare il buon senso e la diffidenza degli utenti ormai furbi. Il trucco consiste nel far credere all'internauta di essere davvero sul sito della sua banca, mentre è altrove. In pratica il pirata informatico attacca il *Dns*, cioè il computer che funge da centralinista per la Rete e collega l'indirizzo che digitiamo nel nostro browser (www.eccetera) all'indirizzo numerico IP che contraddistingue la macchina su cui risiede il sito che vogliamo visitare. In caso di *pharming*, insomma, l'utente digita l'indirizzo corretto ma finisce ugualmente sul sito del truffatore.
«Nel 2004, un 19enne tedesco è riuscito a spostare migliaia di utenti dal sito EBay.de a un sito fasullo. Scoperto e arrestato, ha sostenuto che voleva soltanto divertirsi». Esistono comunque altri canali per il pharming, oltre all'attacco ai Dns. «Talora i truffatori inviano tramite e-mail un virus che cambia l'elenco dei siti cui l'utente si connette più spesso, per dirottarli a loro piacimento, o addirittura attaccano il server della banca per ricevere le connessioni regolari dei correntisti e rimpallarle su un altro sito. Più spesso sfruttano la velocità con cui leggiamo sul monitor per sostituire alcune lettere con altre simili e deviarci verso siti non voluti. Il processo si chiama *mistyping* e accadde per esempio al sito di pagamento on line Paypal, il cui link truffaldino fu inserito in alcune mail come Paypai: una sola lettera cambiata comportava il via alla truffa».
Ha meno di un anno di vita invece il cosiddetto *vishing*, un sistema col quale i truffatori inviano un messaggio di posta elettronica o un sms (sempre da parte di un pretestuoso istituto di credito o affine), invitando l'utente a chiamare un numero telefonico proprio per non incorrere in una truffa on line. «Rassicurato, il ricevente chiama e trova un risponditore telefonico che lo invita a digitare le cifre della sua carta di credito, la data di scadenza e il codice impresso sul retro. In pochi istanti, ha regalato a chissà chi il proprio denaro» aggiunge Repetto.

Ti rubo l'identità e pure la password

Negli Usa l'*identity theft*, il furto di identità, è molto diffuso. «Una delle cose prese di mira è il curriculum on line. Se metti in rete tutti i fatti tuoi sperando di trovare un lavoro, qualcuno può appropriarsi di ciò che dici di te, fingersi un tuo vecchissimo conoscente e ottenere favori o denaro. Quando non addirittura costruirsi un personaggio molto simile a te e agire in nome e per conto della tua persona. Basta che uno trovi on line nome, cognome, data di nascita, telefono, codice fiscale, residenza di una persona e può fargli di tutto». Per esempio, chiamare una compagnia te-



Umberto Rapetto

colonnello **hi tech**

Umberto Rapetto, classe 1959, due lauree (in Giurisprudenza e in Scienze della sicurezza economico-finanziaria), comandante del GAT, è uno dei quattro "esperti" nominati nel Comitato per la tutela della proprietà intellettuale presso la Presidenza del Consiglio dei Ministri. Repetto ha recentemente scritto un libro a quattro mani con la moglie Maria Teresa Lamberti, vicecaporedattore del Giornale Radio Rai, sulle frodi telematiche. Si intitola *Truffe.com* (Cairoeditore, 13 euro) e spiega come difendersi dalle frodi on line. Ha messo in piedi anche www.rapetto.it, il portale della sua famiglia. «Viviamo tutti in posti strani e lontani e questo è l'unico modo che abbiamo per tenerci in contatto. Così ho dedicato una pagina a mio fratello Vittorio, informatico vero, una a mia moglie, giornalista, una a mia figlia Barbara, ingegnere elettronico».

come ti clono il bancomat

Si chiama *skimmer*, il catturacarta inserito nella fessura del bancomat con una microcamera installata nei pressi dello sportello, per rilevare il codice segreto dal movimento delle vostre dita. Ricordate di digitarlo sempre coprendo una mano con l'altra o mettendo sulla tastiera tutte e dieci le dita per confondere la visuale» consiglia Rapetto. I dati della carta di credito e quelli del conto corrente però possono arrivare da altre due banalissime forme di intelligence. «Il *trashing*, cioè il recupero di documenti sensibili dalla spazzatura. E il *boxing*, vale a dire il prelevamento di corrispondenza creditizia dalla cassetta delle lettere».

lefonica e farsi bloccare un'utenza cellulare o peggio inoltrare una dichiarazione dei redditi compilata in modo falso inventando guadagni assurdi. Che, a loro volta, comporteranno un enorme dispendio di denaro per la vittima dello "scherzo": la normativa vigente in Italia prevede che per fare ricorso in materia fiscale si debba comunque prima versare un terzo del massimo importo che si ottiene dall'imposta evasa più la sanzione applicata (che è da due a quattro volte superiore). In pratica, con quei pochi dati posso affermare che uno ha guadagnato 800 mila euro di diritti d'autore compilandogli il quadro E del 740 e lui, fatti due conti, per poter ricorrere contro il fatto che di dichiarazioni ne esistono due (la sua, vera, e quella falsa) dovrà sborsare poco meno di mezzo milione di euro.

Il furto d'identità può avvenire anche in modo più indiretto. Pensate per esempio a quant'è comodo eliminare tutti i cavi di connessione dalla propria scrivania e poter navigare senza fili. Attenzione, però: **gli aggeggi che consentono le connessioni *wi-fi* sono privi di protezione e richiedono un minimo di buona volontà e applicazione per settare una password protettiva**. Basta regalare a qualcuno non molto esperto un kit wi-fi per avere una buona probabilità di accesso alla rete con le sue credenziali. Lungo le strade delle grandi città si consuma il cosiddetto *wardriving*: orde di hackers (e non solo loro) girano in auto con un portatile acceso, un'antennina collegata e un software di rilevazione reti e mappano i punti d'accesso non protetti per scroccare una navigatina gratuita o, peggio ancora, per attaccare un computer terzo attraverso la connessione di un (ancora una volta) ignaro ma ingenuo proprietario di pc domestico.

Un altro modo usato dai professionisti del furto d'identità indiretto è lo *spoofing*. «Mentre stai chiudendo la tua sessione di comunicazione l'hacker ti aggancia e continua la sessione con la tua identità telematica». Oppure il *proxying*. «Che consiste nel navigare su un sito-lavatrice che ti fa cedere il tuo numero IP, cioè la targa con cui ti muovi in rete, e te ne dà uno diverso in cambio. In questo caso è vero che tu ti muovi in sostanziale anonimato, ma non sai che fine fa il tuo IP originario e come può essere utilizzato nel caso in cui venga riattribuito a un altro internauta».

gli acchiappafurfanti

Investigatori sempre addosso ai furbi. Come fate? «Siamo trentacinque tecnici – spiega il colonello Rapetto - e ci basiamo sul concetto di *reverse engineering*: qualunque cosa che sia stata montata può anche essere smontata a ritroso. Oggi come oggi è possibile "tracciare" chiunque, correre dietro a tutti. Le difficoltà maggiori insorgono in termini temporali quando a un'alta complessità tecnica si aggiungono lungaggini burocratiche dovute alle leggi vigenti (o inesistenti), nelle zone in cui si trovano i server che ospitano i siti o il materiale che cerchiamo. Tecnicamente parlando, effettuiamo un monitoraggio puntuale di eventi e fenomeni che sembrano trascinare con sé strumenti o forme di raggiro informatico». Nel lavoro di Rapetto e compagni, spesso, ciò che non è strategia è software. «Sono strumenti che ci consentono di recuperare *file* cancellati e irrintracciabili, ricostruendo gli stati precedenti del computer». Nel Gat è ormai mitico il brigadiere Davide Mancini, l'uomo che ha recuperato i dati di Ricucci, inchiodato gli hacker che hanno violato il Pentagono e salvato la tesi cancellata della figlia di un giudice di Cassazione a due giorni dalla consegna. «Il suo record? Riesce a far tornare un disco fisso indietro nel tempo fino a cinque formattazioni prima». «