

Phishing all'attacco!

I cybercriminali si fanno sempre più furbi: adesso hanno scoperto come aggirare la chiusura dei siti usati per attacchi di phishing

Franco Forte

Come ormai quasi tutti sanno, il phishing è una frode on-line ideata per sottrarre con l'inganno numeri di carte di credito, password e informazioni su account personali. Essa si basa sull'invio da parte di un malintenzionato di e-mail che sembrano provenire da siti web autentici o noti (soprattutto di banche) i quali richiedono all'ignaro utente l'inserimento di informazioni personali.

A questo link, una demo flash (in inglese) realizzata dalla divisione Cyota Consumer Solutions di RSA Security che illustra come avviene un attacco di phishing: <http://cyota.com/media/ConferenceDemoSept2.swf>.

I "truffatori digitali" hanno sviluppato una nuova tecnica in risposta alle sempre più agguerrite contromisure messe in campo dalle aziende specializzate in sicurezza informatica per contrastare questo fenomeno, identificando e chiudendo i siti utilizzati per perpetrare attacchi di questo tipo.

La nuova tecnica di difesa sviluppata dai truffatori digitali è mirata a far sì che le potenziali vittime del phishing accedano sempre a un sito attivo. Essa è stata scoperta e resa nota oggi dai ricercatori dell'RSA Cyota Anti-Fraud Command Centre, il centro per il monitoraggio permanente delle minacce in rete creato da Cyota, società specializzata in soluzioni e servizi di sicurezza per le banche recentemente acquistata da RSA Security.

Attualmente sono due gli attacchi condotti secondo questo nuovo tipo di "reindirizzamento intelligente" di cui si ha notizia certa. Le vittime, in entrambi i casi, sono banche: una britannica e una canadese.

Come funziona? In pratica, il cybercriminale attiva un apposito indirizzo IP a cui linkano tutti gli URL contenuti nelle email inviate alle ignare vittime. Questo indirizzo IP, però, ospita il "reindirizzatore intelligente" approntato dai truffatori, ovvero un sistema che effettua la verifica di tutti i diversi siti a supporto dell'attacco di phishing precedentemente creati quali sono ancora attivi e vi reindirizza automaticamente il visitatore.

"A mano a mano che le aziende e le organizzazioni impegnate nella lotta al phishing diventano più rapide nell'individuare e chiudere i siti creati per perpetrare questi tipi di attacchi, anche i truffatori on-line diventano sempre più esperti nell'aggirare l'ostacolo e questa tecnica è l'ultima soluzione che hanno individuato. I destinatari delle e-mail contenenti l'inganno del phishing non hanno alcuno strumento per accorgersene se non, come sempre, il loro buon senso oltre che, naturalmente, le varie tecnologie di difesa e l'impegno profuso dalle società esperte nella lotta alle minacce dei truffatori online quali RSA Security", ha commentato Andrew Moloney, Senior Product Manager di RSA Cyota Consumer Solutions.