CLUSIS
Association suisse de la sécurité des systèmes d'information
Schweizerischer Verband der Sicherheit von Informationssystemen
Associazione svizzera della sicurezza dei sistemi d'informazione
Swiss Association for the Security of Information Services

Phishing e Pharming: analisi degli attacchi e possibili contromisure.

Silvano Marioni, CISSP

Lugano, 26 aprile 2005

CLUSIS

Che cosa è il phishing

- Il termine Phishing indica l'utilizzo di messaggi di posta elettronica e siti web che sembrano autentici per ottenere con l'imbroglio informazioni personali quali password, numeri di conto, numeri di carta di credito, ecc.
- Si basa su tecniche di Social Engineering

Social Engineering

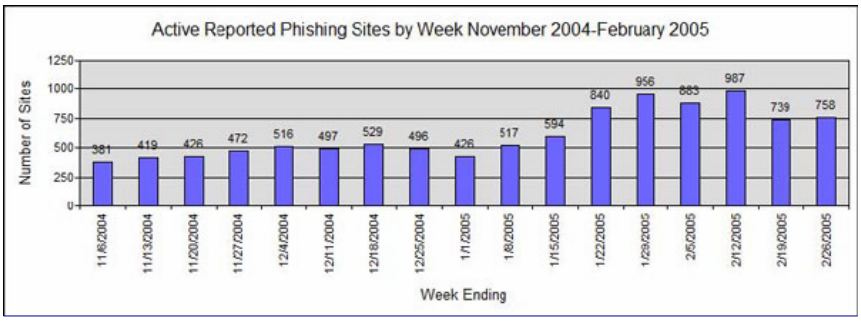
Microsoft Corporation Security Center [vbercsnhsceuenw-fyfyvf@bulletin.msdn.com]

this is the latest version of security update, the "October 2003, Cumulative Patch" update which resolves all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three newly discovered vulnerabilities. Install now to continue keeping your computer secure from these vulnerabilities, the most serious of which could allow an attacker to run code on your computer. This update includes the functionality of all previously released patches.

System requirements: Windows 95/98/Me/2000/NT/XP
This update applies to:
- MS Internet Explorer, version 4.01 and later
- MS Outlook, version 8.00 and later
- MS Outlook Express, version 4.01 and later

Recommendation: Customers should install the patch at the earliest opportunity.
How to install: Run attached file. Choose Yes on displayed dialog box.
How to use: You don't need to do anything after installing this item.

Evoluzione del phishing



Fonte: www.antiphishing.org

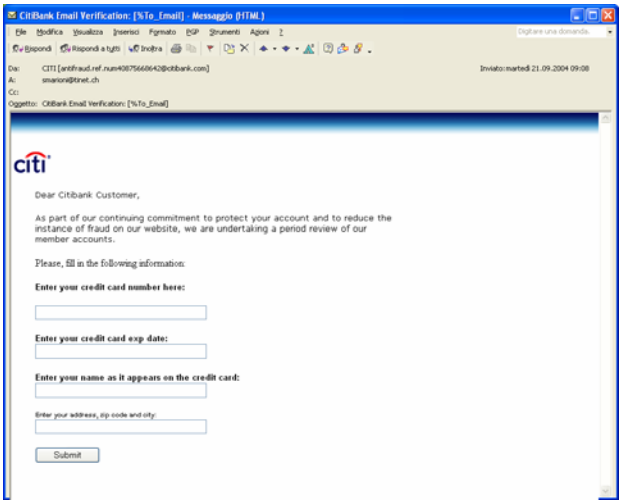
Modalità di utilizzo del phishing

- Invito a fornire le proprie informazioni facendo leva su paura, inesperienza o avidità.
  - Il conto è bloccato, c'è un problema di sicurezza, è necessario utilizzare un nuovo servizio, ecc.
- Come fornire le informazioni
  - Richiesta di compilazione di un form nel messaggio
  - Link a siti falsi
  - Link a siti con offerte estremamente interessanti
  - Istallazione di programmi malefici di ridirezione, keylogging, ecc.

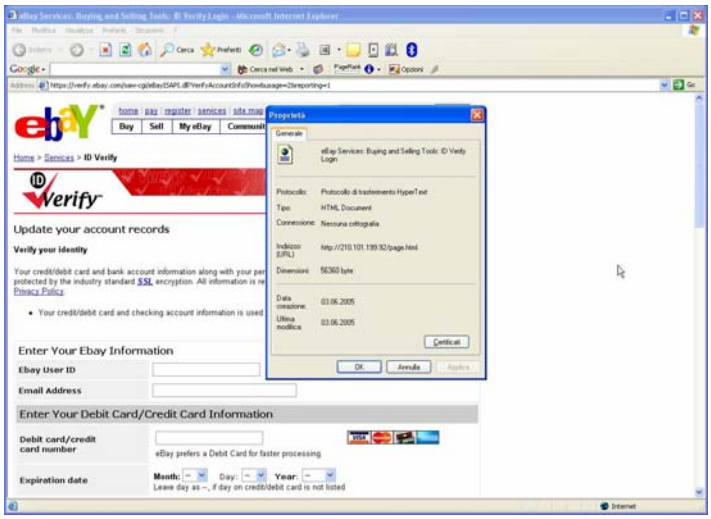
Tecniche di mascheramento

- URL offuscate
  - http://www.ro1ex.com
  - http://www.mybank.com → www.mybank.credit.com
  - http://www.cnn.com:@1040363912
- Frame nascosti
- Uso dell'istruzione DIV
- Mascheramento dell'indirizzo con un'immagine

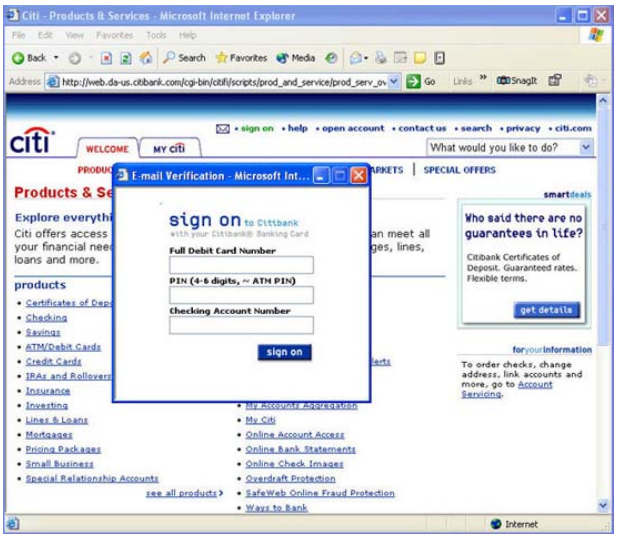
Richiesta di compilazione di un form nel messaggio



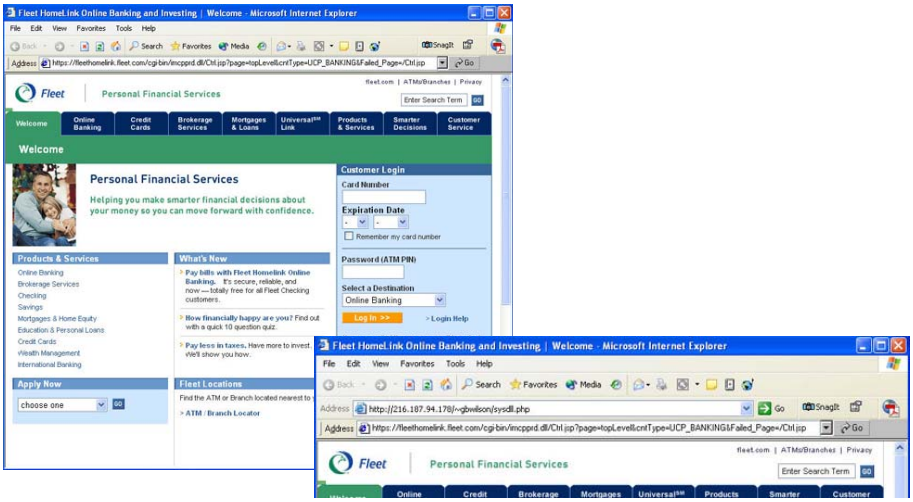
Link a un sito falso



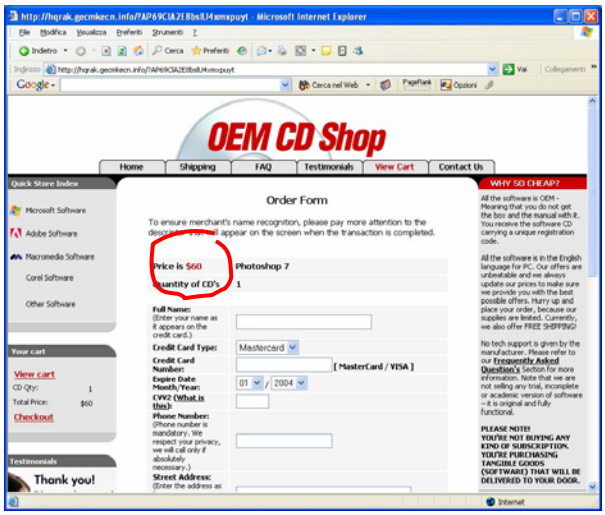
Link a un sito vero con pop-up falso



Mascheramento dell'indirizzo con un'immagine



Link a un sito con offerte estremamente interessanti

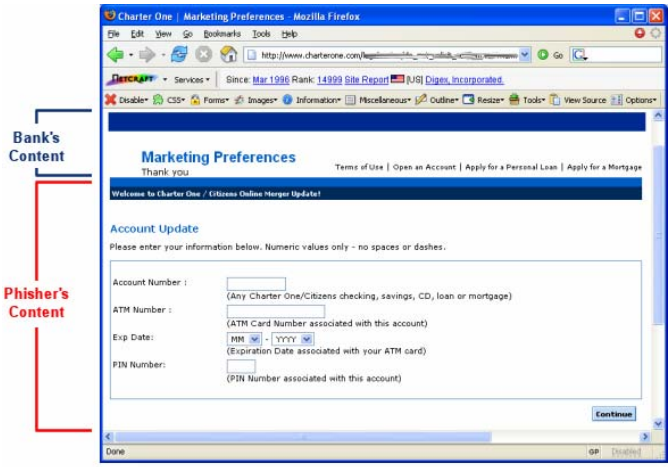


Dimostrazione pratica

- Esempi di messaggi di Phishing
- Come proteggersi tecnicamente

demo

Un esempio che neutralizza la barra anti-phishing

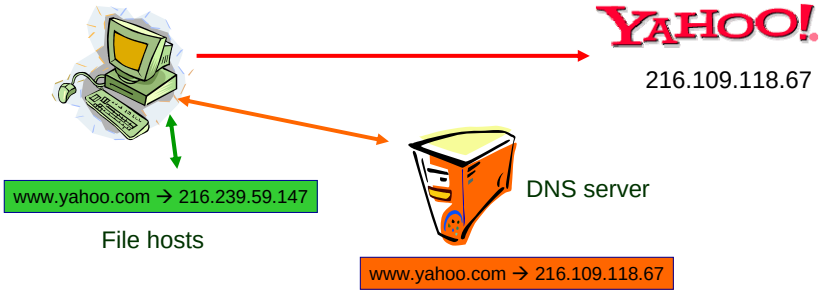


Che cosa è il pharming

- Il termine Pharming indica la tecnica di ridirezione dell'accesso verso siti web che sembrano autentici per ottenere informazioni personali quali password, numeri di conto, numeri di carta di credito, ecc.
- Si basa su tecniche di DNS hijacking or poisoning

Come funziona il pharming

- www.yahoo.com → 216.109.118.67
- www.google.com → 216.239.59.147



Dimostrazione pratica

- Esempio di attacco di Pharming
- Come proteggersi tecnicamente

demo

Suggerimenti comportamentali

- Essere sospettosi di ogni messaggio di posta elettronica con richieste urgenti relative alle informazioni personali
- Non usare i link su messaggio di posta elettronica sospette ma digitare direttamente gli indirizzi
- Non compilare formulari che richiedono informazioni personali

Suggerimenti tecnici

- Verificare l'autenticità delle pagine usando un toolbar anti-phishing
  - Netcraft Toolbar, EarthLink Toolbar
- Rendere read-only il file hosts
- Utilizzare prodotti che identificano i cambiamenti di configurazione (in particolare del file hosts)
  - Microsoft Antispyware

Grazie dell'attenzione