

Alla scoperta del phishing

(i tutorial di Alessandro de Simone)

Copyright Alessandro de Simone 2005 (www.alessandrodesimone.net) - È vietato trascrivere, copiare, stampare, tradurre, riprodurre o divulgare il presente documento, anche parzialmente, senza l'autorizzazione scritta dell'autore. I siti Internet, le case editrici e le pubblicazioni di settore che intendano utilizzare questo documento possono contattare l'autore (FastSum@alessandrodesimone.net) per gli accordi del caso.

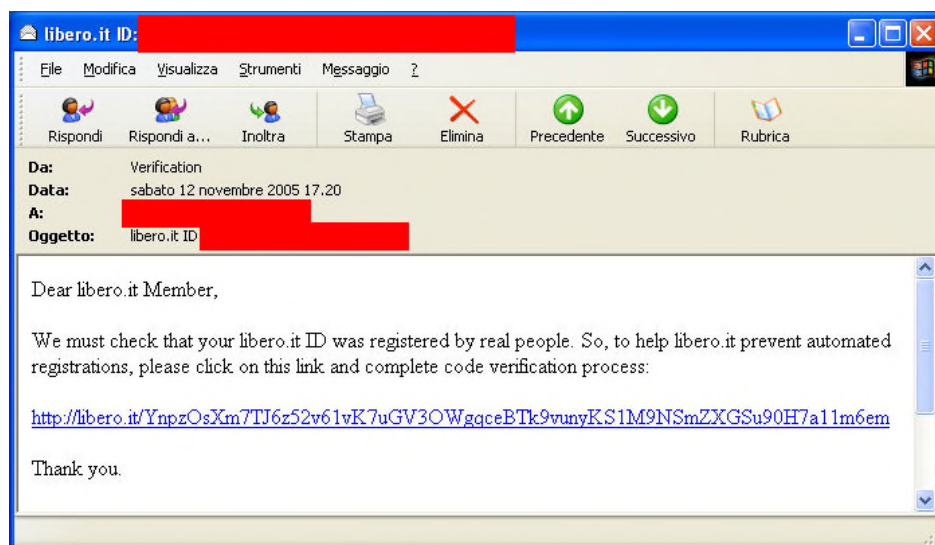
Copyright Alessandro de Simone 2005 (www.alessandrodesimone.net) - No transcribing, no copyng, no reproducing, no translating, no printing, no publishing this document - even if partially - without author's written authorization. Websites and publishing house who wish to employ this document must write the author (FastSum@alessandrodesimone.net).

Premessa

Prima di mettere in pratica ciò che segue è assolutamente indispensabile essere consapevoli che tali “esperimenti” – se mal condotti – possono generare disastri talvolta irrimediabili sia sul proprio PC sia sull'eventuale rete (alla quale il PC risulti eventualmente connesso) sia ai nostri abituali destinatari di posta elettronica, il cui indirizzo è

memorizzato nella rubrica del client e-mail.

Le considerazioni che seguono traggono spunto da una mail (ovviamente non richiesta) a me pervenuta (figura 1), ma presumibilmente distribuita in migliaia di esemplari a ignari utenti. L'aspetto della mail non è per nulla dissimile da quello classico di una



qualsiasi lettera di posta elettronica: la provenienza (campo “Da”) è relativamente professionale (*Verification*), il campo oggetto è intenzionalmente rassicurante (“*libero.it ID indirizzo@libero.it*”) l'apertura (“*Dear libero.it Member...*”) e la chiusura (“*Thank you*”) seguono i canoni del bon-ton. A dire il vero, se arrivate a visualizzare la mail così come la vedete in figura, in realtà avete già commesso un'imprudenza: è infatti noto che usando il client *Microsoft Outlook Express* – anche se in casi omai rari – la semplice visualizzazione (addirittura in anteprima!) di una mail può innescare un'infezione virale. Sembra tuttavia che il problema sia stato risolto da tempo grazie alle patch rilasciate periodicamente da Microsoft. Ovvio che non ne sono immuni gli utenti che **non** si collegano da troppo tempo a <http://windowsupdate.microsoft.com/> per scaricare i preziosi aggiornamenti. Ma torniamo alla mail incriminata, che è stata sottoposta a esame avendo ovviamente avuto l'accortezza di operare off-line, in modo da impedire involontari collegamenti al link oggetto

della presente relazione. Il complicato link (collegamento) di figura 1, comunque, può essere esplicitato posizionando (attenzione: semplicemente posizionando e non cliccando)

[http://www.google.nl/url?q=http://sTaND%09%61R%09T%09Za.%43%09%4fm
/%63g%09%69-%62i%6e|p%6f%63h|r%65%64%69%72.c%67i?s=libero.it](http://www.google.nl/url?q=http://sTaND%09%61R%09T%09Za.%43%09%4fm/%63g%09%69-%62i%6e|p%6f%63h|r%65%64%69%72.c%67i?s=libero.it)

il puntatore del mouse. Sulla barra di stato della mail compare, in tal modo, il collegamento "in chiaro". In realtà l'indirizzo non è affatto comprensibile, ma quanto meno ci si può accorgere che il link "punta" a un non meglio precisato *www.google.nl* che a sua volta sembra nascondere un secondo indirizzo (notare *?q=http//sTa* eccetera) che chissà dove conduce. Si noti, infine, la parte terminale del link ("*libero.it*") che probabilmente servirà all'autore del *virus / phishing* di archiviare ordinatamente le risposte degli utenti raggirati.

Questo spazio è disponibile per il tuo messaggio pubblicitario.

Per informazioni, [clicca qui](#) o invia un [messaggio](#)

This space is for your advertisement.

[Click here](#) for details or [Contacts](#)

Espace pour votre annonce.

[Clic ici](#) pour détail ou [Contact](#)

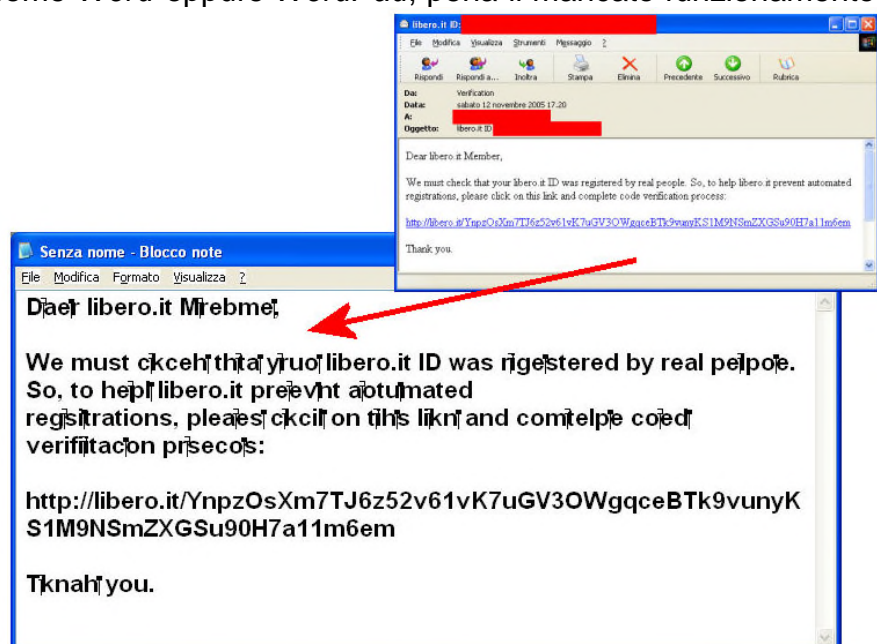
Come si può intuire, non è possibile stabilire a priori se si tratta di un semplice scherzo(?), di un phishing (per ottenere ID e password di account e-mail) oppure di diffusione di virus. L'unica cosa certa è che la metodologia usata serve per nascondere accuratamente un collegamento sospetto.

Il testo nascosto

Limitandoci semplicemente alle considerazioni precedenti, dovremmo responsabilmente concludere che, per prudenza, è meglio cancellare (o quanto meno ignorare) la mail, immediatamente. Tuttavia, se rimane ancora qualche dubbio sull'autenticità (e soprattutto sulla buona fede) del messaggio ricevuto, basterà compiere un'ultima analisi: partiremo però dal presupposto che il mittente, se realmente in buona fede, non ha alcun motivo per inserire parti nascoste nella lettera. Basterà quindi attenersi alla seguente procedura:

- 1) Selezionare l'intero testo della mail (menu *Modifica/Seleziona tutto*), quindi copiarlo (menu *Modifica/Copia*) nella clipboard di Windows.
- 2) Aprire un qualsiasi text editor come *Blocco Note* (attenzione: parliamo di un text editor, non di un word processor come *Word* oppure *WordPad*, pena il mancato funzionamento della procedura!).
- 3) Incollare il testo nella finestra di *Blocco Note* (menu *Modifica/Incolla*). Ciò che appare è un testo assolutamente incomprensibile (vedi figura 3). Che cosa è successo?

L'apparente "sporcizia" che si può notare è, in realtà, un insieme di caratteri speciali semigrafici, non stampabili o, quantomeno, non interpretabili. Si tratta di codici di programmazione, che l'utente non



è certo in grado di decifrare, ma che per un PC rappresentano una serie di istruzioni ben precise. Senza entrare nel dettaglio, sarà sufficiente rendersi conto che i “codici di controllo” non sono applicati solo sul link (applicazione che, in fin dei conti, potrebbe essere lecita, anche se in casi molto particolari), ma sull’intero testo, a partire addirittura dall’intestazione: si noti, infatti, la presenza di codici di controllo perfino in “*Dear libero.it Member*”, che appare infarcito di vari caratteri semigrafici, quanto meno insoliti. Questo è senza ombra di dubbio un sintomo di malafede perché non ci sono ragionevoli motivi per nascondere caratteri all’interno di frasi di prammatica.

A chi ha esperienza di programmazione, ci limiteremo a dire che i “codici di controllo” sono del tutto simili ai cosiddetti “*codici cursore*” del Commodore 64, che consentivano, appunto, di attivare speciali procedure all’insaputa dell’utente. È molto probabile, pertanto, che siano proprio quei codici a dirottare il collegamento verso il sito Internet, nel quale sono certamente presenti sofisticate procedure, capaci di elaborare le informazioni provenienti dall’utente che avesse imprudentemente cliccato sul collegamento incriminato.

Condotta pratica

Che cosa conviene fare, quindi, quando siamo in dubbio se cliccare su un collegamento ritenuto sospetto? Semplice:

- 1) Non aprire mai una mail se non conosciamo il mittente.
- 2) Non dimentichiamo che se, al contrario, il mittente ci è noto, questi potrebbe comunque essere stato vittima di un attacco virale e la mail a noi pervenuta potrebbe essere la conseguenza dell’azione del virus.
- 3) Se non abbiamo l’opportunità di contattare il mittente in altro modo (per esempio, telefonicamente) per scoprire la reale provenienza del messaggio – e se abbiamo aperto la mail (operazione comunque rischiosa) – seguite la procedura descritta ed esaminate il testo “trasportandolo” nella finestra di *Blocco Note*.
- 4) Se il testo appare *interamente* leggibile, le probabilità di essere in presenza di un fenomeno virus o phishing diminuiscono.
- 5) Se, al contrario, il testo appare illeggibile, non abbiate timore a cancellare immediatamente la mail. Subito dopo effettuate una scansione antivirus e antispy: occorrerà almeno un’ora, ma ne può valere la pena.

Questo spazio è disponibile per il tuo messaggio pubblicitario.
Per informazioni, [clicca qui](#) o invia un [messaggio](#)

This space is for your advertisement.
[Click here](#) for details or [Contacts](#)

Espace pour votre annonce.
[Clic ici](#) pour détail ou [Contact](#)

Il presente Tutorial è stato modificato il giorno 13 novembre 2005
Per ulteriori aggiornamenti consultare il sito <http://www.alessandrodesimone.net>