

Guida alla sicurezza su internet

Hackers

Si definiscono tali, gli esperti di informatica che hanno ottime conoscenze per ciò che riguarda Internet e l'integrazione dei sistemi operativi, con essi.

Un Hackers, a parte il fatto che non verrebbe mai ad attaccare, il vostro computer di casa, se anche lo facesse, non lo danneggerebbe in alcun modo, magari si limiterebbe a cancellare qualche file che possa servire ad identificarlo, e a prelevare il vostro indirizzo di posta, al quale poi magari manderà un'email contenente le spiegazioni per correggere il difetto che ha potuto sfruttare per avere accesso al vostro pc.

Quindi ribadisco il concetto: gli hackers, non sono responsabili degli atti CRIMINALI di cui parlano spesso i mass-media.

L'unico motivo per cui si infiltrano nei computer è o per scopo di aiuto a difendersi "dai cattivi" o per scopo di studio.

Crackers

Loro, sono i veri colpevoli degli atti criminosi che vengono commessi su internet a danno delle società.

Un cracker, definito tale, infatti si infila nel vostro sistema solo per il gusto della sfida, ma non si accontenta di ciò, vuole lasciare un segnale visibile del loro passaggio, o cancellando qualcosa o addirittura tutto.

Parte I - I Firewall

Per evitare che persone o programmi non autorizzati abbiano accesso al vostro computer, esistono da molto tempo dei software, in grado di controllare le comunicazioni tra voi e internet, tali software, si chiamano "Firewall", in italiano, risulterebbe come "Muro di fuoco", è un nome che rende abbastanza bene il loro lavoro.

Ogni computer, ha per comunicare con il modem e quindi con internet, a disposizione delle "porte" tali porte consentono lo scambio di dati. Ogni computer, ha 65535 porte dentro di se, queste porte, virtuali, proprio come quelle di casa, possono essere aperte o chiuse; aperte consentono lo scambio, dati, chiuse no.

Le porte aperte in un computer sono generalmente molto poche, in genere c'è la porta: 23 per Telnet, un programma di comunicazione, la 135, per i servizi Microsoft, la 80, per Internet, la 400, la 1025, la 1026, e varie.

Ogni porta aperta, poi cambia da computer a computer, dipende dai programmi che avete e dall'uso che ne fate.

I Firewall, in pratica, hanno una lista che voi dovete fornirgli, di programmi che hanno l'accesso verso internet, come magari la posta elettronica, ed un sistema di controllo che non fa altro che mettersi a controllare in continuazione le porte che avete aperte e vi segnala ogni cosa anomala che accade.

Esistono molti Firewall, alcuni distribuiti gratuitamente, come ZoneAlarm o Sygate Personal Firewall, solo che naturalmente la qualità e la sicurezza sono abbastanza per gli utenti normali, altrimenti esistono molte buone alcune versioni a pagamento come il pacchetto Norton Internet Security, che però ha un costo.

Le grandi ditte, invece si affidano oltre che ad un personale specializzato, ad una macchina firewall, che non è software, ma è un'altro apparecchio che viene messo prima della linea di entrata del segnale al vostro computer, ma questa apparecchiatura ha un notevole costo.

Parte II - I Dialer

A) Cosa sono?

Tasto molto dolente, in quanto questi piccoli programmi, sono molto comuni e si espandono sempre di più, nonostante come vedremo più avanti, non siano strumenti molto leciti. Sono dei piccoli programmi "di connessione gratuita" che si scaricano gratuitamente da internet.

Li troviamo principalmente sui siti di carattere sessuale (porno, in parole povere), ma non sono certo rari su siti dedicati a sfondi per computer e ai famosi Loghi&Suonerie oppure per lo scaricamento di programmi, ed infine come evidenziato da una retata della Polizia Postale addirittura da siti di previsioni meteorologiche.

B) Il funzionamento

Il funzionamento di questi piccoli programmi, è molto semplice, dialer in italiano significa qualcosa come "chiamatore, compositore"; infatti questi programmi, una volta attivati, hanno il solo scopo di staccare l'attuale connessione internet in uso (o di attivarla se non siete su internet) e dirottare verso le cosiddette "Numerazioni per servizi a sovrapprezzo" ovvero verso numerazioni 144, 166, 899, 163 e 164. Talvolta cercando una interpretazione al piano di numerazione questi programmi compongono numerazioni 701, 702, 709, che per definizione dell'ultimo "Piano numerazione nazionale" sono "Numerazioni per servizi Internet". Una volta fatto ciò, si disattivano da soli, per riattivarsi al vostro prossimo clic.

Il guaio è che talvolta questa procedura è abilmente mascherata (non esiste infatti un solo messaggio che vi informi delle operazioni in corso) oppure non viene chiaramente indicata la tariffa che andremo a pagare. Tutto ciò si ripercuote sulla bolletta telefonica dell'utente: le "Numerazioni per servizi a sovrapprezzo" infatti sono numeri assegnati da Telecom Italia a subconcessionari che rivendono queste numerazioni e che hanno un costo largamente superiore a quello della comune chiamata internet. Ad esempio chiamate su numerazioni 144, 166, 899, 163 e 164 possono arrivare a costare circa 2,50 euro al minuto più IVA, numerazioni verso 709 attualmente costano circa 0,06 euro al minuto.

Naturalmente c'è un massimo di tot minuti, solo che questo massimo è di solito fissato verso i 75 minuti, quindi alla fine dei conti viene fuori un conto purtroppo molto salato.

La fregatura (o "sola" in romanesco) è che le società che gestiscono questi programmi, pubblicano queste informazioni in caratteri piccolissimi, cosicché risulta difficile, sia notarle che leggerle; anche se questa pratica può risultare illegale, purtroppo per il consumatore, non lo è affatto, la legge infatti stabilisce che l'informazione deve essere riportata, ma non ne specifica le dimensioni minime del carattere.

C) Aspetti legali

Come dicevamo inizialmente questi programmi non sono legali o meglio, nel migliore dei casi chi propone questi programmi commette un illecito amministrativo. Nello specifico la legislazione sulla fornitura di servizi su numerazioni telefoniche apposite viene definito dal "Piano di numerazione nazionale" definito dalla "Autorità per le Garanzie nelle comunicazioni" e possiamo leggerlo a questo link http://www.agcom.it/comunicati/cs_040703.htm e per completezza anche a questo link http://www.agcom.it/provv/d_09_02_CIR.htm avremo un utile integrazione di quanto stabilito dal Piano di Numerazione Nazionale. Di interesse per quanto vedremo di seguito è il primo comma dell'articolo 4.

Il Piano di Numerazione Nazionale stabilisce chiaramente e senza problemi di interpretazioni che "Viene ribadito il divieto di offerta di servizi a sovrapprezzo per le numerazioni dedicate ai servizi di accesso a Internet (701, 702, 709)" ovvero su numerazioni 701-2-9 non puoi fornire servizi a sovrapprezzo. Le "numerazioni per servizi a sovrapprezzo" vengono definite sempre dall'Autorità e sono state suddivise in 3 categorie: "1) Sociale-informativo: si tratta di servizi riguardanti pubbliche amministrazioni ed enti locali, servizi di pubblica utilità e servizi di informazione abbonati, 2) Servizi di assistenza, consulenza tecnico-professionale e di intrattenimento, 3) Servizi di chiamate di massa, quali sondaggi di opinione, televoto, servizi di

raccolta fondi" escludendo così di fatto la fornitura di servizi internet e/o di connettività internet su queste numerazioni. In totale riferimento a questa legislazione recentemente la Polizia Postale ha indicato chiaramente che si può richiedere un rimborso in caso di fatturazione di servizi non autorizzati. La Polizia Postale indica i passi da eseguire per richiedere tale rimborso.

<http://www.poliziadistato.it/pds/primapagina/709/index.htm>

su questo sito è possibile anche scaricare il modulo per la denuncia da effettuare per ottenere il rimborso.

L'ADUC oltre a questo mette a disposizione un modulo per richiedere il rimborso e la disattivazione di tali numerazioni:

<http://www.aduc.it/dyn/sosonline/...>

Il Senato sta per approvare un disegno di legge che senza ogni dubbio chiude questi "sfruttamenti" poco leciti:

<http://www.senato.it/bgt/ShowDoc.asp...>

D) Come difendersi

Naturalmente un rimedio c'è e consiste nel fatto di stare attenti quando navigate su internet a dei messaggi con riportato, "Installare ed eseguire XXXXX ?", il messaggio si presenta quasi sempre con un'altra parte con scritto "Autenticità verificata da XXXX".

Spiegazione: la maggior parte delle volte, questi messaggi mascherano il download di questi cosiddetti Dialer.

Le uniche volte che possono essere "vere" queste richieste di installare e di eseguire un determinato programma, sono da parte del "Flash plugin X" di 'Macromedia, Inc.' e di "Windows Update versione X" da parte della 'Microsoft', programmi che servono, il primo per visualizzare animazioni, il secondo per aggiornare e rendere sicuro Windows. Controllate bene però che si tratti di prodotti delle rispettive società, altrimenti potrebbe essere anche un Dialer, chiamato così per scopi "poco nobili".

Questi programmi funzionano solo per gli utenti che hanno le connessioni con il numero telefonico da comporre, infatti gli utenti xDSL, non hanno bisogno di comporre niente, poiché sono sempre connessi alla rete. Se invece disponete delle meno veloci connessioni Dialup come con modem analogico o ISDN, dovete fare molta attenzione.

E' altrettanto vero che questi programmi funzionano solo su sistemi operativi MICROSOFT, e non su sistemi operativi su MAC o sistemi operativi Linux. Un buon consiglio è quello di installare un programma firewall per evitare l'installazione di quel tipo di dialer AUTOMATICI.

Un buon metodo per riconoscerli è guardare il nome sotto il quale si presentano, come "supersesso.exe", "scarica.exe", "345255.exe", "loghi.exe" che hanno tutti in comune il fatto di essere degli exe, ovvero il formato dei programmi che usa Windows, pensateci, se dovete scaricarvi un'immagine che di solito ha il formato "jpg, jpeg, gif, png", che diavolo ci fa quell'exe??

E) Riferimenti Legislativi e modulistica varia

http://www.agcom.it/provv/d_467_00_CONS.htm

Disposizioni in materia di autorizzazioni generali

http://www.agcom.it/L_naz/l_59_2002.htm

Disciplina relativa alla fornitura di servizi di accesso ad internet

http://www.agcom.it/provv/d_09_02_CIR.htm

Norme di attuazione dell'articolo 1, comma 1, della legge n. 59 dell'8 aprile 2002:
Criteri di applicazione agli Internet Service Provider delle condizioni economiche dell'offerta di riferimento.

Di rilievo: Articolo 4 comma 1

http://www.agcom.it/provv/d_6_00_CIR.htm

Piano di numerazione nel settore delle telecomunicazioni e disciplina attuativa

Di rilievo: Artivolo 21

http://www.agcom.it/comunicati/cs_040703.htm

Piano di numerazione nazionale attualmente in vigore

<http://www.poliziadistato.it/pds/....pds>

Modulo di querela precedente alla richiesta di rimborso.

<http://www.aduc.it/dyn/sosonline/....>

TELECOMITALIA: RIMBORSO TELEFONATE 70X E DISATTIVAZIONE DELLE STESSE DIRETTRICI NUMERICHE

Parte III - I Virus, cosa sono, come si suddividono, come difendersi.

A) Cosa sono?

Principalmente i virus sono "Malicious code", come certamente saprete infatti qualsiasi programma alla sua origine non è altro che un ammasso di codice, ove per codice si intende il linguaggio di programmazione.

Per malicious code, si intende un codice che riporta istruzioni sulle operazioni da far compiere al vostro computer, che è malicious in quanto le suddette operazioni posso andare dalla semplice cancellazione di qualche file fino alla perdita completa di tutti i dati presenti nel vostro computer.

B) Suddivisione

I virus si suddividono in varie categorie: analizziamole una per una.

B1) Worm

Si definiscono worm (vermi) tutti i virus più diffusi, che si presentano sotto forma di piccoli programmi.

Alcuni non sono dannosi come il W32.Blaster.B.Worm che sebbene riavvii il computer ogni 60 secondi, non cancella niente.

Il perchè di quel nome? Analizziamolo: W32, sta per Windows 32 ovvero tutti i Sistemi operativi Windows in modalità 32 bit (Win98, Win 2000, WinME, WinXP, Ecc.), il punto serve solo per dividere, poi Blaster, è il nome vero e proprio del virus, la B sta per la versione, infatti di ogni virus, possono esistere moltissime versioni; l'ultima parola sta ad indicare di che tipo di virus si tratta ovvero di un worm.

B2) Trojan

Sono programmi, che stanno nel computer, e di solito non cancellano niente, ma hanno la brutta abitudine di aprire una di quelle porte di cui vi parlavo prima, consentendo al suo

programmatore di prendere il controllo completo (anche del mouse e della tastiera) del vostro computer. In questo caso, i Firewall, sono importantissimi, in quanto chiedendovi se il programma, "netbus.exe" può andare su internet, voi che non avete mai installato un programma di nome "Netbus", insospettiti, dapprima gli negherete il permesso, successivamente farete un'indagine per stabilire se il programma sia un programma per la posta, per internet o se invece sia un pericoloso Trojan.

B3) MacroVirus

Si tratta di virus contenuti nei file come i documenti di Word o nelle cartelle di Excel. Questi virus, sfruttano uno strumento presente in tutti i programmi per videoscrittura, il gestore delle Macro.

Le Macro non sono altro che semplici istruzioni che inserite nei documenti, permettono cose come animare il titolo del vostro racconto, o far cambiare il colore del testo a seconda dell'ora, ecc.

Sfortunatamente i creatori di virus (virus writer) usano questa funzione per creare dei virus che danneggiano il vostro computer.

B4) Vari

Fanno parte di questa sezione tutti quei virus che magari, inibiscono il collegamento ad internet, oppure vanno ad infettare il sistema di avvio del computer e quindi non fanno caricare il sistema operativo, rendendo molto più difficile la loro rimozione.

C) Come difendersi

La precauzione prima di tutto. I virus possono purtroppo arrivare da qualsiasi parte, via internet, via posta elettronica e via programmi.

Uno strumento indispensabile è un ottimo "Antivirus", in commercio c'è ne sono molti, il migliore a detta dei 'critici' è il Norton Antivirus, ma che purtroppo ha la sfortunata caratteristica di voler molta memoria per essere eseguito, se non disponete di tanta memoria o vi serve per un'altra cosa, e meglio scegliere prodotti come McAfee, F-Secure o Panda Antivirus, che sebbene non così potenti, offrono un'ottima protezione con poca richiesta di memoria.

Uno strumento comune a tutti gli antivirus è l'auto-update, si tratta di uno strumento che ogni volta che voi andate su internet, si collega al sito del produttore e scarica le cosiddette "Impronte dei virus" aggiornando quelle precedenti, ogni virus, ha infatti delle impronte, proprio come quelle digitali, che permette di riconoscerlo ed eliminarlo dal sistema.

Quasi tutti i sistemi Antivirus offrono anche l'auto-protect, ovvero hanno un programma che controlla costantemente il computer alla ricerca di file infetti e che vi avvisa qualora siate in procinto di aprire un file che ritiene sospetto.

Come dicevo sopra la precauzione prima di tutto, perciò quando navigate su internet, se non siete molto esperti, navigate solo su siti ritenuti sicuri, per quanto riguarda le e-mail, diffidate sempre da quelle che hanno allegati, controllandoli con un antivirus prima di aprirle soprattutto se hanno formati come "vbs", "exe", "com", "bat", "doc".

Se poi vi arriva un e-mail da vostro padre, con in oggetto una qualsiasi frase in inglese, è meglio che la cancelliate subito, primo perchè vi può anche telefonare, e poi perchè dovrebbe essere con l'oggetto in inglese? E' un classico trucco adottato da molti virus.

Il sistema di trasmissione dei virus sono molteplici, possono essere trasmessi attraverso altri programmi comuni o via posta elettronica, molti virus, infatti quando vi infettano, aprono il programma di posta elettronica e si autospediscono ad ognuno degli indirizzi che trovano nella rubrica.

All'inizio ho anticipato questo argomento, naturalmente uno dei principali pericoli della rete è rappresentato anche da loro.

Una brutta notizia che devo darvi, è che se sono bravi, non c'è nessun sistema per negargli l'accesso al vostro computer.

Ma come sempre esistono delle soluzioni, potete difendervi da loro grazie a degli accorgimenti:

- non andate su siti che contengono materiale di dubbia provenienza (pirata tanto per intenderci)
- evitate i siti pornografici
- usate un buon Firewall, dovete metterci tanta pazienza a configurarlo, ma dopo i risultati saranno ottimi
- se usate una connessione DSL o a fibre ottiche, chiedete al fornitore se potete non avere l'indirizzo IP fisso.

L'indirizzo IP è infatti una sigla composta da quattro blocchi di numeri da 0 a 255 separati da un punto

(es. 123.245.185.254), chi infatti ha una connessione DSL, ha di solito l'IP fisso, cioè ogni volta che va su internet rimane quello, cosa che invece non succede per chi usa i tradizionali modem come la Dialup, l'ISDN e NetSystem.

Sarebbe come andare in giro con il volto coperto ma con sotto scritto: sono "tizio caio" ogni volta che si esce, a che servirebbe la maschera? Gli utenti invece con modem normale, invece ogni volta che escono, cambierebbero nome, difficile, andarlo a rintracciare no?