



Sicurezza Informatica 1.0

Guida pratica alla sopravvivenza in rete

In due parole

Ci credereste che basta visitare una pagina web creata ad-hoc per infettare il vostro computer?

E se vi dicessi che esistono programmi capaci di dirottare la vostra connessione verso numeri che costano anche 15 euro per il solo scatto alla risposta?

Pensereste mai che qualcuno stia spiando le vostre abitudini su internet?

Vi siete mai chiesti perché la vostra casella di posta è sempre piena di messaggi indesiderati o molesti?

Se avete risposto sì alle prime tre domande e conoscete la risposta della quarta, allora probabilmente non avete bisogno di questa guida. Se, invece, una o più di queste domande vi suonano nuove allora siete dei lettori qualificati per questa guida. Non preoccupatevi, cercherò di essere meno noioso possibile, e nella maggior parte dei casi scoprirete che è sufficiente modificare qualche piccola abitudine per mettersi al riparo da brutte sorprese.

Norme di distribuzione

Questa guida è offerta alla comunità di internet senza alcuna forma di protezione.

Può essere scaricata, utilizzata e ridistribuita liberamente purché:

- ✓ se ne conservi integralmente il contenuto, compresa l'indicazione dell'autore;
- ✓ non venga chiesto alcun corrispettivo in caso di distribuzione;

Indice

- Introduzione
- 1. Una rete di insidie
 - 1.1 Virus
 - 1.2 Worm
 - 1.3 Programmi spia (Spyware)
 - 1.4 La piaga dei Dialer
 - 1.5 Lo Spam
- 2. Fine della corsa

Introduzione

Cominciamo, col dire una grossa banalità: un computer non connesso alla rete (a nessuna rete) è inattaccabile!!! Se in passato i virus erano “costretti” a spostarsi su scomodi dischetti l’avvento di internet con milioni di macchine tra loro connesse ha aperto una vera e propria autostrada agli attacchi informatici. Di conseguenza se il vostro computer non è connesso buona parte delle raccomandazioni che seguiranno non vi riguardano. Potreste perfino rinunciare all’antivirus in quanto l’unica strada che lascereste aperta è quella di programmi o file che voi stessi deciderete di installare.

Capita spesso di ricevere messaggi di posta infettati da virus che apparentemente provengono da persone che conosciamo o che comunque appaiono credibili. In realtà modificare il mittente di una mail è un'operazione elementare ed è proprio ciò che fanno molti virus recuperando gli indirizzi mail nella rubrica di un pc infettato e poi spedendo una copia di se stessi a tutti gli indirizzi trovati falsificando il mittente con uno degli indirizzi carpiti. In questo senso qualsiasi messaggio di posta elettronica va considerato a rischio e vagliato dall'antivirus.

Viceversa un pc collegato ad una rete (internet o LAN) necessita di una serie di accortezze. Peraltro le forme di attacco sono in costante aumento, per cui se in passato era sufficiente proteggersi dai soli virus oggi tra Spywere, Dialer, Trojan, e quant’altro i rischi si sono centuplicati. Con essi cresce la complessità delle soluzioni da adottare come risposta. A questo punto, però, potrebbe esservi sorto un dubbio: perché ci sono così tanti “elementi ostili” a popolare la rete?

Diciamo subito che il virus dimostrativo che nasce per pura sfida intellettuale costituisce ormai una sorta di ricordo romantico degli albori della rete. I virus e più in generale i malware attuali hanno sempre finalità ostili. Molte infezioni puntano ad “aprire” il vostro computer rendendolo controllabile da remoto, più spesso hanno il fine di obbligarvi a visitare determinate pagine o di raccogliere informazioni sulle vostre abitudini al fine di sommergervi di pubblicità molesta. Di recente tecniche sempre più sofisticate puntano alla sottrazione di dati sensibili come le password del vostro conto corrente (phishing).

Altre volte l'obiettivo è più semplicemente quello di dirottare la vostra connessione su numerazioni a costi elevati di diversi euro a minuto (dialer). Insomma come avete capito per chi inventa queste trappole voi siete solo il “solito” pollo da spennare.

Nella maggior parte dei casi non ha un interesse specifico per voi, ma vi ha individuato nel mucchio perché siete i più vulnerabili. Non fatene quindi un questione personale, piuttosto rimboccatevi le maniche e cominciate a difendervi.

Una precisazione: non seguite la moda dei mass-media di indicare come hacker chi scrive un virus o viola una rete informatica arrecandovi danno: nell'accezione originale l' hacker era colui che sfruttava una tecnologia oltre quelle che erano le intenzioni del suo creatore (se utilizzate la camera d'aria di un pneumatico come salvagente siete hacker!). Il termine inglese che andrebbe usato è più correttamente cracker.

Quali misure adottare lo vedremo nelle pagine seguenti, permettetemi però un suggerimento: **siate diffidenti**. Internet, la posta, le chat non sono luoghi per facili guadagni o altrettanto facili conquiste. Così come avverrebbe nella vita reale anche questi posti sono assediati da persone poco raccomandabili, che sicuramente sono una esigua minoranza ma che al tempo stesso hanno avuto un ruolo preponderante nel creare una certa cattiva fama di cui, suo malgrado, gode internet. Ciò non vuol dire che dobbiate stare alla larga da questi sevizii, tutt’altro. La quantità di informazioni che questi canali offrono è impagabile così come eccezionali possono essere le persone conosciute con

la mediazione del vostro amato pc. Ricordatevi solo di dubitare quando vi viene prospettata una soluzione troppo semplice! Nemmeno il Web in questo senso fa miracoli. Facciamo un esempio classico: ricevete un e-mail, magari da un indirizzo credibile, il cui testo è del tipo:

*Ti invio un simpatico passatempo, io lo ho trovato molto divertente!!!
Il mio record è di 234 punti, poi fammi sapere il tuo, buon divertimento!!!!*

Se cedete alla curiosità ed aprite l'allegato non troverete un simpatico giochino ma un molto meno amichevole virus. Complimenti siete riusciti ad auto infettarvi. Questo è un classico esempio in cui la naturale prudenza sarebbe stata sufficiente a salvarvi. Perché mai uno sconosciuto dovrebbe inviarvi una cosa che non avete richiesto? E poi come fa ad avere il vostro indirizzo? E in ogni caso non vi ho già detto che l'indirizzo del mittente non deve farvi sentire sicuri e che ogni allegato va vagliato dall'antivirus?

1. Una rete di insidie

In questo capitolo troverete una rassegna delle maggiori insidie informatiche. Data la complessità dei contenuti trattati non entrerà nei dettagli tecnici ma mi soffermerò sulle contromisure pratiche da adottare. Chi volesse approfondire in internet non ha che l'imbarazzo della scelta.

1.1 Virus

I virus sono l'insidia storica dei calcolatori. Si tratta di un mondo molto eterogeneo che può diffondersi sotto forma di file eseguibile (.exe .bat), di Script e perfino nelle pagine Html di Internet. Un attacco virale avviene sempre con l'installazione di componenti del virus nel pc. Tali componenti possono essere veri e propri programmi, voci di registro, set di istruzioni etc.

Una differenza importante da tenere a mente è che esistono virus distruttivi e non distruttivi.

La prima categoria è quella i cui effetti sono più disastrosi, e si manifestano con cancellazione di file o applicazioni o ancora file di sistema, in breve il vostro pc sarà inservibile e spesso risulterà impossibile riavviare lo stesso Windows.

Un virus non distruttivo è una minaccia altrettanto grave ma più subdola che si manifesta con sintomi meno eclatanti ma porta alla fine allo stesso risultato. In questo caso può essere "interesse" del virus essere invisibile come accade quando questo è programmato per fare del pc infetto una testa di ponte per il diffondersi dell'infezione o per portare un attacco più massiccio alle reti informatiche.

I SINTOMI

- ✓ Impossibilità di collegarsi ai siti degli antivirus o di Microsoft update;
- ✓ Anomalie di funzionamento (programmi che non si avviano, altri che si lanciano automaticamente, comparsa di strani messaggi di errore etc);
- ✓ Riduzione immotivata dello spazio disponibile (che viene progressivamente saturato dal diffondersi dell'infezione);
- ✓ Spegnimenti immotivati;
- ✓ Impossibilità ad eseguire operazioni prima consentite;

Ricordate che un virus può presentare contemporaneamente uno o più dei sintomi citati, ma può anche non presentarne nessuno, per cui non lanciatemi anatemi se incappate in un virus che non ha letto le mie istruzioni!

LE SOLUZIONI

A costo di ripetermi vale la regola base della prudenza: non visitare siti poco affidabili o quantomeno fatelo imponendo le massime restrizioni al vostro browser, non aprite gli allegati di posta elettronica a meno che non siate certi del mittente e riteniate plausibile il contenuto della mail stessa, diffidate di programmi o file che provengono da siti di dubbia attendibilità o da circuiti di scambio file (nei quali trovate veramente di tutto incluso un vastissimo campionario di bestioline virali).

Una volta attivata la prima linea di difesa (meglio nota come cervello) la soluzione migliore per difendersi resta comunque quella di dotarsi di un buon antivirus. Facile a dirsi un pò meno a farsi: gli antivirus commerciali, come quelli pre-installati, prevedono un abbonamento da rinnovare annualmente con costo dai 20 ai 70 euro, non tantissimo quindi ma neanche poco se sul vostro pc conservate dati "non vitali".

Il costo unitamente alle procedure di rinnovo un pò macchinose sono motivi più che sufficienti a molti utenti per disfarsi dell'antivirus. Esistono diverse soluzioni, gratuite e a pagamento, entrambe molto valide. Tra queste vi segnalo:

- **Norton Antivirus** www.symantec.it (pagamento circa € 70,00)
- **Grisoft AVG antivirus** <http://free.grisoft.com> (free)
- **Avast antivirus** www.avast.com (free)
- **Antivir** www.free-av.com (free)
- **Stinger** <http://vil.nai.com/vil/stinger> (free)

Il primo programma lo considero il più completo e affidabile; i successivi tre sono antivirus in senso stretto, nel senso che offrono sia la protezione in tempo reale sia le funzioni di scansione dei file su richiesta dell'utente. **Avg** è un'antivirus piuttosto completo che prevede anche un modulo di scansione della posta elettronica, la funzione di quarantena, la creazione di dischetti di emergenza e la schedulazione delle scansioni (potete cioè programmare i giorni e le ore in cui effettuare la scansione in automatico, per esempio nelle ore notturne), inoltre l'operazione di aggiornamento è piuttosto semplice e rapida, a prova di modem analogico.

Discorso simile si può fare per **Avast** che in più supporta anche la lingua italiana per l'interfaccia.

Antivir è invece un antivirus tedesco leggero ed efficiente, non dispone di moduli per la posta tuttavia tra le tre soluzioni descritte è quella che ottiene la maggiore percentuale di riconoscimento dei virus (non prendete questi dati come oro colato, scegliete secondo le vostre esigenze, tutti e tre gli antivirus proposti offrono un livello di protezione più che adeguato). **Stinger** è, invece, uno strumento messo a disposizione dalla nota società McAfee che viene aggiornato periodicamente per riconoscere i virus più diffusi. Non offre quindi alcuna protezione in tempo reale e riconosce solo un numero limitato di virus tuttavia può tornarvi molto utile in caso di infezioni che impediscono il corretto funzionamento del vostro antivirus.

Ricordate poi che anche i siti degli antivirus commerciali offrono pagine molto approfondite ed aggiornate sui virus, su come rimuoverli a mano e spesso anche strumenti di rimozione gratuiti di un specifico virus (ma prima dovete individuarlo in base ai sintomi).

Dove è il trucco? Potreste chiedervi perché alcune società offrano gratuitamente il loro prodotti, in fondo questa sembra proprio una tecnica commerciale suicida. Anzitutto gli antivirus di cui vi ho parlato sono gratuiti solo per "uso personale e non professionale" se quindi li usate in azienda o per la vostra professione dovete acquistare la licenza commerciale che vi dà anche diritto ad ulteriori funzioni come l'aggiornamento da server riservati o l'assistenza tecnica. Considerate inoltre che non c'è modo migliore per farsi conoscere che quello di offrire gratis qualcosa che l'utente reputa utile.

AGGIORNARE

Avere un ottimo antivirus è inutile se poi non lo si aggiorna. Partireste per un volo transatlantico senza sapere quanto carburante avete nei serbatoi? L'aggiornamento è una abitudine fondamentale ed andrebbe eseguita almeno un paio di volte al mese (meglio se più spesso), ne va della vostra sicurezza.

Due è meglio di uno? Non pensate che essendo gratuiti vi convenga installare più di un antivirus, i moduli real-time di questi programmi interferiscono vicendevolmente quindi non solo non vi garantiscono più protezione ma possono anche rendere instabile il computer. Tanto per capirci è come se nel calcio giocaste con due numero 11: anziché segnare il doppio vi trovereste due giocatori in

perenne competizione che si ostacolano e calpestano a vicenda, e con il vostro presidente che ha già pronta la lettera di esonero!

UN PC IN AFFANNO

I pc di oggi offrono potenze di calcolo molto elevate e ciò a portato al rilascio di programmi sempre più pesanti e difficili da “far girare”. Se il vostro pc non è più recentissimo potreste avere qualche difficoltà a convivere con le versioni più recenti degli antivirus (specialmente con il Norton), orientate quindi la vostra scelta su programmi leggeri come il già citato Antivir o NOD32 e al limite ricordate che siti come quello Panda (www.pandasoftware.com) consentono una scansione on-line del sistema. A volte è possibile disporre anche di antivirus eseguibili da cd che risolvono parzialmente questo problema, qualcosa del genere viene offerto, ad esempio, dalla finlandese F-prot.

Negli ultimi anni si sono diffusi particolari virus chiamati i Trojan (cavalli di Troia) la cui funzione è quella di creare una breccia nella difesa di un computer facilitando l'attacco da parte di altri virus o consentendo al loro creatore di prendere il controllo di tutte le macchine infettate. Anche se la tipologia di attacco è, in questo caso, differente non cambiano le contromisure, analoghe a quelle descritte qui sopra.

1.2 Worms

Un worm (letteralmente “verme”) è una particolare categoria di malware in grado di autoreplicarsi. È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi. Il termine deriva da un romanzo di fantascienza degli anni ‘70 di John Brunner: i ricercatori che stavano scrivendo uno dei primi studi sul calcolo distribuito notarono le somiglianze tra il proprio programma e quello descritto nel libro e ne adottarono il nome.

Uno dei primi worm diffusi sulla rete fu Internet Worm, creato dal figlio di un alto dirigente della NASA il 2 novembre 1988, quando Internet era ancora agli albori. Tale virus riuscì a colpire oltre un terzo dei computer collegati a quel tempo in rete.

Tipicamente un worm modifica il computer che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo finché non si spegne il computer o non si arresta il processo corrispondente. Il worm tenta di replicarsi sfruttando Internet in diverse maniere: spesso i mezzi di diffusione sono più di uno per uno stesso worm.

Il mezzo più comune impiegato dai worm per diffondersi è la posta elettronica: il programma malizioso ricerca indirizzi e-mail memorizzati nel computer ospite ed invia una copia di sé stesso come file allegato (attachment) a tutti o parte degli indirizzi che è riuscito a raccogliere. I messaggi contenenti il worm utilizzano spesso tecniche di social engineering per indurre il destinatario ad aprire l'allegato, che spesso ha un nome che permette al worm di camuffarsi come file non eseguibile. Alcuni worm sfruttano dei bug di client di posta molto diffusi, come Microsoft Outlook Express, per eseguirsi automaticamente al momento della visualizzazione del messaggio e-mail. Tutti i worm più recenti effettuano la falsificazione dell'indirizzo mittente, creando un fastidioso effetto collaterale di proliferazione di messaggi: alcuni software antivirus, montati tipicamente sui server, respingono il messaggio infetto e notificano il fatto al mittente, ma dato che questo è falso tale notifica arriva ad un destinatario diverso da chi ha realmente inviato la mail e che nulla ha a che fare con l'invio del worm. Questi eseguibili maligni possono anche sfruttare i circuiti del file sharing (E-Mule, Win Mx etc.) per diffondersi. In questo caso si copiano tra i file condivisi dall'utente vittima, spacciandosi per programmi ambiti o per crack di programmi molto costosi o ricercati, in modo da indurre altri utenti a scaricarlo ed eseguirlo.

La tipologia forse più subdola di worm sfrutta dei bug di alcuni software o sistemi operativi, come Windows XP, in modo da diffondersi automaticamente a tutti i computer vulnerabili connessi in rete.

SINTOMI

Un worm semplice, composto solamente dalle istruzioni per replicarsi, di per sé non crea gravi danni diretti al di là dello spreco di risorse computazionali. Spesso però questi programmi per nascondersi interferiscono con il funzionamento di software volti a scovarli e a contrastarne la diffusione, come antivirus e firewall, impedendo così il funzionamento normale del computer ospite. La maggior parte dei worm, così come i virus, contiene una parte detta payload, che ha il solo scopo di causare dei danni al sistema infettato. Molto di frequente un worm funge da veicolo per l'installazione automatica sul maggior numero di macchine di altri malware, come per esempio backdoor o keylogger, che potranno poi essere sfruttati da un malintenzionato cracker o addirittura da un altro worm.

LE SOLUZIONI

Sono le stesse utilizzate per i virus!

1.3 Programmi Spia

I programmi spia (in inglese Spyware) sono una piaga relativamente recente ma al tempo stesso molto diffusa e variegata nelle sue incarnazioni.

I programmi spyware si installano clandestinamente sul vostro pc e raccolgono informazioni sulle vostre abitudini (cosa scrivete, quali siti visitate, quale configurazione ha la macchina che li ospita etc.). Sfruttando la connessione ad Internet queste informazioni vengono inviate a computer remoti in cui vengono raccolte e catalogate a scopi illeciti incluso l'invio di pubblicità indesiderata.

Il rischio implicito in questa pratica è che qualcuno possa venire a conoscenza di informazioni riservate. Sicuramente starete pensando ad aspetti economici come i codici di carte di credito o di conto corrente tuttavia il problema è più esteso, basta pensare quanto personali siano informazioni riguardanti la salute, i comportamenti o le idee che noi tutti spesso riversiamo in file o nei motori di ricerca.

Ma immaginate anche uno scenario più semplice, state consultando la posta alla presenza di un vostro parente, quando aprendo un messaggio ecco a tutto schermo una "esplicita immagine...." che qualcuno ha deciso sia di vostro interesse. Provate solo a pensare quanto chilometriche dovranno essere le vostre giustificazioni, paura eh?

I SINTOMI

Visto il ruolo che svolgono, i programmi spyware debbono essere il più possibile invisibili all'utente, e ciò ne rende più difficoltosa l'individuazione, insomma siete di fronte a veri esperti di camuffamento e mimetismo assai difficili da stanare. Il sintomo più evidente può essere il rallentamento della navigazione (più evidente nelle connessioni via modem). Altri sintomi potrebbero essere un comportamento anomalo di internet (che si ostina a mostrarvi pagine diverse da quelle che state cercando) o un rapido aumento dello spam nella vostra casella di posta.

La combinazione di tasti [Ctrl]+[Alt]+[Canc] – da premere in simultanea – può consentirvi di visualizzare quali programmi o processi sono in esecuzione in quel momento. Si tratta di sigle spesso incompressibili tra le quali si nascondono questo genere di programmi. Se avete dei dubbi annotate il nome del programma sospetto ed inseritelo in un motore di ricerca (www.google.it, www.yahoo.com, www.virgilio.it etc.) se si tratta di componenti malevoli i risultati dovrebbero essere eloquenti (troverete in cima alle ricerche siti dei produttori di Antivirus).

LE SOLUZIONI

A differenza di ciò che avviene per i virus e i worms, per i quali esiste una lunga esperienza ed strumenti di rimozione efficaci, per i programmi spia le soluzioni sono molto meno valide e molto meno rapide nell'aggiornarsi. Ad-Aware (www.lavasoft.com) e SpyBot S&D (www.spybot.info) sono le soluzioni gratuite più diffuse ma non fanno miracoli. Il consiglio è di installare entrambi i programmi e tenerli aggiornati, facendo periodicamente la scansione del sistema.

Non temete, in questo caso non vale la limitazione detta a proposito degli antivirus e i due programmi possono coesistere (fate attenzione però a non attivare in entrambi i moduli real-time che sono stati introdotti nelle ultime versioni).

No panic! La prima volta che lanciate Ad-aware o Spybot potreste trovare decine di file ritenuti pericolosi, non lasciatevi spaventare, nella maggior parte dei casi si tratta di minacce potenziali e non reali. Entrambi i programmi evidenziano il grado di pericolosità di ciò che hanno individuato e solo quando questo livello è alto ci si deve preoccupare seriamente. In ogni caso rimuovere tutto ciò che viene proposto in genere non ha controindicazioni.

Gli stessi produttori di antivirus si stanno attrezzando ma siamo ancora agli inizi delle battaglie. Se avete rintracciato un componente spia, per esempio con la ricerca che vi ho suggerito sopra, in attesa di un aggiornamento efficace del vostro antivirus o anti-spyware la soluzione migliore è renderlo inoffensivo: da Start scegliete Esegui e digitate "msconfig" (senza virgolette), nella finestra che si apre scegliete il tab Avvio e togliete il segno di spunta del processo incriminato (purtroppo questa soluzione funziona solo in Windows 98 e in Windows XP).

Questa procedura evita l'avvio automatico del programma ma spesso per la complessità dell'attacco può risultare inefficace (come nel caso di più processi che si riattivano a vicenda se vengono spenti). In rari casi l'unica soluzione efficace rimane la formattazione.

FONDAMENTALE

Se curare in questi casi può essere difficile assai più efficace è prevenire! Un firewall (letteralmente muro taglia fuoco) è un programma che controlla tutti i programmi che tentano di accedere alla rete o dalla rete al vostro computer. Windows XP comprende già di suo un firewall leggermente migliorato nella sp2 (un service pack è una raccolta di correzioni da apportare ad un programma, e rilasciata dal produttore). Se non utilizzate Windows XP o non siete soddisfatti del firewall integrato, potete far riferimento ai seguenti programmi:

- Zone Alarm (www.zonelabs.com)
- Outpost Firewall (www.agnitum.com)
- Kerio Personal Firewall (www.kerio.com)

Di questi Zone Alarm è il più semplice da usare. Senza istruzioni vi chiederà di autorizzare ogni singolo accesso alla rete rispondendo ad una finestra di messaggio. Il prodotto Kerio è invece il più professionale ma è di più difficile configurazione.

Tutti e tre i programmi sono disponibili in una versione commerciale ed in una versione semplificata gratuita (già sufficiente per i nostri scopi).

L'installazione di un firewall è un'operazione da non rimandare (forse più importante dell'antivirus) per cui non esitate!

Negli ultimi mesi molti firewall gratuiti sono scomparsi perché il produttore non sviluppa più la versione freeware (come nel caso di Outpost dove questa versione è ferma alla 1.0) o perché la società è stata acquisita da qualche multinazionale. Ciò ovviamente non vi impedisce di utilizzare le versioni precedenti di questi software. Per essere certi delle condizioni d'uso visitate sempre il sito del produttore. Al momento, tra i software segnalati, continua ad essere disponibile la versione gratuita ed aggiornata di Zone Alarm. Una buona alternativa è costituita da Jetico personal firewall disponibile presso www.jetico.com per tutte le versioni di Windows dalla 98 a quella attuale.

Non sentitevi in una botte di ferro, un firewall svolge come detto due funzioni fondamentali: tiene lontani gli aggressori che tentano di accedere al vostro pc e vi consente un controllo dettagliato dei programmi che tentano di accedere alla rete.

Non attribuite al firewall capacità che non può possedere, ancora una volta molto in termini di sicurezza dipende dal vostro modo di operare. Se avete il click facile non c'è software che possa salvarvi.

UN UNIVERSO IN ESPANSIONE

Mi rendo conto di avervi proposto fin qui un panorama piuttosto tetto, popolato da viscido creature e astute spie, purtroppo, però, per l'alba dovrete pazientare ancora un pò giusto il tempo di mostrarvi qualche altra insidia da cui tenersi a distanza di sicurezza.

È, per esempio, frequente l'installazione "di barre extra" in Internet Explorer, si tratta di componenti aggiuntivi del Browser che ne aumentano le funzioni. Di per se sono degli strumenti assolutamente leciti ed utili, tuttavia siti congeniati apposta possono indurvi a scaricare la loro barra che in realtà è un ricettacolo di spyware. Questo problema coinvolge, per ora, solo Internet Explorer, quindi se utilizzate un diverso browser non correte questo rischio. Internet Explorer è anche facile vittima di programmi dirottatori (hijacker) che ne alterano la Home Page, rinviandovi a siti di dubbia utilità e di certo pericolo. Per l'eliminazione di questi componenti valgono le considerazioni fin fatte sopra, mentre per renderli inefficaci si può procedere come segue :

- > Aprite Internet Explorer;
- > Nel menù Strumenti scegliete Opzioni internet;
- > Nella finestra che si apre scegliete il tab Avanzate;
- > Togliete il segno di spunta sulla voce "abilita estensioni di terze parti";

Questa funzione è disponibile solo nelle ultime versioni di IE.

I CATTIVI SIETE VOI

E se foste stati voi stessi, senza alcun raggirò, a installare uno spyware nel vostro pc?

Non fate quella faccia, capita anche questo. Molti programmi di uso comune (per esempio, molti programmi di scambio P2P) possono installare spyware o aware (questi ultimi sono programmi che durante l'uso fanno comparire banner pubblicitari). È questo il prezzo che vi viene chiesto per poter usare "gratis" quel programma. In genere di ciò si fa cenno nelle licenze d'uso ma, quante licenze avete letto prima di installare un software? In questo senso ricordate che se con Ad-Aware o con Spybot rimuovete le componenti ostili di un programma questo smette di funzionare, a voi la scelta.

1.4 La piaga dei Dialer

Nell'accezione originaria il termine dialer era riferito ai programmi che consentivano la configurazione di un pc per la navigazione in internet. Come questa innocua funzione sia potuta degenerare in un vera piaga è in parte un mistero. In realtà il dietro le quinte è sempre il medesimo: ci siamo noi sprovveduti

navigatori del Web, e una marmaglia di malintenzionati che ci vede come corpulenti polli da fare allo spiedo, più o meno come capita a Silvestro quando osserva il povero Titti.

Badate che la metafora è ironica ma non esagerata, esistono interi trattati di marketing e di ingegneria sociale in materia. Il meccanismo di funzionamento di un dialer è piuttosto semplice: collegandovi ad un certo sito per accedere ad alcuni contenuti vi viene chiesto di scaricare un piccolo programma che dovrete usare al posto della vostra normale connessione.

Con questo meccanismo possono essere interdetti alla normale navigazione solo alcuni contenuti o anche l'intero contenuto di un sito. Ma cosa offrono queste pagine di così particolare da richiedere un apposito programma di connessione? Quasi sempre la risposta è nulla! Si va da fantomatiche tesine per gli studenti alle "emoticon" (ben note a chi chatta) fino all'onnipresente pornografia. Insomma niente che non possiate trovare sul Web con una navigazione tradizionale.

Non facciamo di tutta tua l'erba un fascio. Una precisazione è doverosa, la tecnica del dialer è perfettamente lecita, ed è anzi un modo molto semplice per addebitare un servizio, molto più comodo della carta di credito. Potrebbe, per esempio, essere impiegata quando si vuole accedere agli archivi di una biblioteca o di un quotidiano o ancora come tariffa per scaricare legalmente da internet musica, film e libri, rispettando le leggi sul diritto d'autore. Il problema sta nel fatto che navigando per la rete difficilmente vi imatterete in questo tipo di servizi, mentre con grande probabilità troverete qualcuno pronto a scucirvi denaro in cambio del nulla.

Da quanto vi ho detto finora però "il bidone" non è ancora ben manifesto. Vi ricordate l'invito alla diffidenza? Bene allora chiedetevi a cosa possa servire il programma che vi viene chiesto di scaricare ed usare al posto del vostro caro accesso remoto.

Non dubito che, a questo punto della guida, abbiate capito in che direzione tira il vento... In realtà da qualche parte nella pagina che vi chiede di scaricare il dialer sono riportate le condizioni di fornitura del servizio (spesso in realtà non ci sono neppure quelle). Sono clausole scritte in piccolo spesso rilegate in una scomoda TextArea da scorrere con il mouse. Leggendole però si "scopre" il trucco: sfruttando il programma di connessione scaricato ci si collega a server con numerazioni particolari a costo aggiuntivo per cui un minuto di connessione può costarvi diversi euro contro il centesimo o poco più della normale connessione via modem.

Per altro questi programmi sono molto insistenti, una volta installati creano delle copie del programma di installazione e si reinstallano al successivo avvio se provate ad disinstallarli.

Per evitare ciò dovrete setacciare il vostro disco fisso alle ricerca di tracce del programma ed eliminarle. Convieni poi eliminare il contenuto della cartella temp [start > esegui > temp (invio)], in Windows 2000 ed Xp vi serviranno i privilegi di amministratore, ricordate inoltre che la cartella Temp potrebbe, in alcune configurazioni, non essere unica.

Potreste anche intervenire nella sezione Run del registro di configurazione [start > esegui > regedit (invio)] che contiene l'elenco dei programmi eseguiti all'avvio, tuttavia data la delicatezza dei file di registro in questa guida non entriamo mai nel dettaglio di queste procedure poiché un intervento maldestro potrebbe rendere inservibile Windows.

In Windows 98 ed Xp potreste eseguire la stessa procedura attraverso l'unità di configurazione [start > esegui > msconfig (invio)] accedendo alla sezione avvio e togliendo il segno di spunta sul nome del programma sospetto. Ovviamente anche un buon programma antivirus può darvi una mano nel debellare questo tipo di attacco. Molto efficace risulta essere allo scopo un antivirus italiano, Virit Explorer della Tgsoft (www.tgsoft.it) di cui potete scaricare una versione di prova.

La protezione migliore anche in questo caso è comunque la diffidenza: diffidare da tutti i siti che vi chiedono di scaricare programmi per accedere al contenuto è già garanzia piuttosto estesa di non

incappare in un dialer. Come contromisura preventiva potete installare programmi come Antidialer di Digisoft (www.digisoft.cc) che è gratuito, in italiano e consente di stabilire quali numeri è consentito usare nelle connessioni internet.

I soliti fortunati: se avete la fortuna di disporre di una connessione ADSL ho una seconda buona notizia per voi, siete immuni ai dialer. Questi infatti funzionano componendo un numero telefonico, operazione che non dovete più fare con i modem adsl.

Una raccomandazione infine: il bubbone dialer può apparire meno traumatico di altre forme di attacco prima descritte, però, sottovalutarlo può costare molto caro! Raggiungere in pochi giorni bollette di diverse migliaia di euro è più facile di quanto appare. A quel punto solo il “buon cuore” della vostra compagnia telefonica vi può salvare. Se non volete correre rischi sul problema dialer potete chiedere al vostro gestore di disabilitare l'accesso alle numerazioni “non geografiche” (come 144, 166, 899, 892,...). La disabilitazione permanente è gratuita per legge, mentre quelle mediante codice personale prevede un canone mensile. Valutate che con la disabilitazione permanente non potrete accedere a nessun servizio che usi una numerazione non geografica.

1.5 Lo Spam

Spam è il nome di una delle prime carni in scatola in gelatina, inventata da tal J.C. Hormel nel 1936 in una cittadina dello stato del Minnesota. L'idea di conservare la carne in barattoli da aprire all'occorrenza deve essere piaciuta molto visto il successo del prodotto e il grande numero di imitazioni. Tranquilli, non ho sbagliato un copia-incolla, era solo per dirvi che lo spam, quello originale, è piuttosto buono, soprattutto in primavera quando si risveglia la voglia di scampagnate. Nei primi anni novanta una coppia di avvocati dell'Arizona inonda il mondo dei newsgroups (“bacheche” virtuali in cui si scambiano opinioni su determinate tematiche, per es. su it.comp.aiuto si discute di problemi che riguardano il mondo dei computer) di messaggi pubblicitari in cui offrivano il loro servizi. Le poteste furono così numerose che qualcuno chiamò il fenomeno spam perché, come l'originale, destinato a capillare diffusione.

Oggi lo spam è essenzialmente questo, un ondata di mail non richieste, inutili e spesso offensive.

Si tratta di una vera tecnica di marketing che consiste nello spedire mail pubblicitarie ad indirizzi generati casualmente sfruttando le risposte dei server per capire se il destinatario esiste o meno.

Di per se non è una tecnica molto persuasiva (si stima che solo 4 persone ogni mille contattate mostrino qualche interesse) ma è molto diffusa in quanto praticamente gratuita!

Lo Spam non solo è un fastidio in quanto intasa le nostre caselle di posta ma è anche un costo aggiuntivo, basta pensare al tempo che ci fa perdere o ai maggiori costi di connessione che sosteniamo leggendo la posta.

Una soluzione radicale del problema è purtroppo lontana e, di conseguenza si possono dare solo consigli di massima:

1. Non rispondere mai ad una lettera spam (confermereste l'esistenza del vostro indirizzo);
2. Usate un indirizzo mail per registrarvi sui siti ed uno distinto per la corrispondenza privata;
3. Eventualmente installate un programma antispam;
4. Più in generale se frequentate forum, newsgroups, chat, o mailing-list, evitate di fornire in chiaro il vostro indirizzo mail;

Mi spiego meglio, uno spammer non raccoglie singolarmente gli indirizzi mail, ma sfrutta tecniche automatiche che generano gli indirizzi in modo casuale o che riconoscono la struttura dell'indirizzo

mail "pino@pt-art.it" all'interno dei messaggi pubblici e li raccolgono in un database. Se per qualche ragione dovete trasmettere il vostro indirizzo di posta elettronica cercate quantomeno di ingannare i programmi automatici. Di seguito vi mostro tre esempi, tuttavia non sperate che sia questa la soluzione al problema delle mail spazzatura:

1. [pino\(at\)pt-art.it](mailto:pino(at)pt-art.it)
2. pino @ pt-art.it (si...bastano due spazi)
3. pinoELIMINA@pt-art.it

Questi trucchetti ingannano i programmi di riconoscimento meno sofisticati, ma consentono ad una persona reale di capire qual'è il nostro vero indirizzo.

Eventualmente usare un programma anti spam... vi chiederete perché questa opzione, all'apparenza risolutrice, sia messa in coda e "gravata" da un eventuale. Il motivo è semplice, è sì vero che i filtri antispam sono piuttosto efficienti nel riconoscere le mail indesiderate, ma questa classificazione può avvenire solo dopo che il messaggio è già stato scaricato in locale, quando cioè avete già sostenuto i costi di connessione. Certo se ricevete moltissimo spam anche questo può considerarsi un risultato e contribuisce a rendere un po migliore la vostra giornata.

Un programma anti-spam riconosce le mail spam con metodi statistici (presenza di determinate parole) o mediante liste di indirizzi. In una lista nera (blak-list da aggiornare periodicamente) sono contenuti indirizzi di spammer noti, mentre in una lista bianca potrete inserire gli indirizzi dei vostri contatti. Programmi antispam gratuiti da affiancare al vostro programma di posta sono, tra gli altri:

- ✓ SpamBayes (www.spambayes.sourceforge.net)
- ✓ K9 Antispam (www.keir.net)
- ✓ Spamihilator (www.spamihilator.com)

Se vi piace la semplicità orientate pure la vostra scelta su Spamihilator, che per altro è anche piuttosto leggero ed efficace.

2. Fine della corsa

Bene, siete stati bravi. E' stata dura ma non avete mollato, qualche altra riga e poi potrete tornare alla vostra vita.

Dopo aver predicato la diffidenza e dopo aver descritto internet come luogo impestato dai mali più differenti, sento il bisogno di tranquillizzarvi. Se sarete prudenti, ed attuerete le contromisure minime necessarie, il Web non vi riserverà brutte sorprese. Anzi vi prospetterà sempre nuovi orizzonti e nuovi universi da esplorare.

Lo scopo di questa guida, spero si sia capito, non era quello di spaventare, quanto di informare.

Quando si ha conoscenza di un pericolo, si è anche in grado di superarlo.

Se volete avere chiarimenti, se avete suggerimenti, o semplicemente se vi va di scrivermi, potete farlo all'indirizzo di posta: pino@pt-art.it