Mario Pascucci

Windows XP in sicurezza

APOGEO

NOBUG
SOFTWARE & SERVICES

Windows XP in sicurezza

Autore:
Mario Pascucci

Socio Unico Giangiacomo Feltrinelli Editore srl
Via Natale Battaglia 12 – 20127 Milano (Italy)
Telefono: 02-289981 – Telefax: 02-26116334
Email apogeo@apogeonline.com
U.R.L. http://www.apogeonline.com/ebook

ISBN 978-88-503-1008-1

Impaginazione elettronica in LATEX a cura dell'Autore
Copertina di Enrico Marcandalli

Presentazione

Nonostante il largo impiego di firewall, antivirus, antispyware, scanner di sicurezza, aggiornamenti automatici, browser alternativi, e chi più ne ha più ne metta, i problemi di sicurezza che i normali utilizzatori di Windows XP sperimentano rimangono irrisolti. Nel tentativo di stabilire cosa renda vulnerabile Windows XP, e se sia possibile renderlo affidabile il minimo indispensabile per un uso casalingo, questo testo spiega passo passo le contromisure e le strategie alla portata di tutti per proteggere il proprio computer e se stessi dai pericoli che ogni giorno si possono incontrare in Rete.

Questo libro non avrebbe mai visto la luce senza il contributo di Lorenzo, titolare di Nobug Srl (http://www.nobug.it), a cui va la mia più sincera gratitudine.

Mario Pascucci

Diario delle Revisioni
Revisione 0.2.1 2007-03-29 Revisionato da: mp
Cambiato il titolo.
Revisione 0.2.0 2007-03-14 Revisionato da: mp
Aggiustamenti “cosmetici” per la pubblicazione.
Revisione 0.1.0 2006-11-25 Revisionato da: mp
Versione definitiva.

Sommario

1. Prima di iniziare 1

Introduzione 1
Perché 2
Cosa c'è e cosa non c'è 3
Cosa occorre 5
Legalese 5
Come leggerlo 5

2. Conosci il Nemico 7

I problemi di Windows XP 7
Come "i cattivi" entrano nel computer 8
Senza fare nulla 10
Antivirus? Firewall? Che fanno, dormono? 11
L'esercito delle infinite scimmie 13
C'è poco da scherzare 14

3. Falle, porte e fossati 16

Difendere un fortino 16
Il laboratorio 16
Quanto resiste il fortino? 17
L'epidemia della rete 18
Prevenire e difendere 20

4. Cominciamo dalle basi 22

La prima linea di difesa: sapere 22
La prima contromisura: il backup 22
La seconda linea di difesa: diritti e gerarchie 26
La seconda linea di difesa bis: password 31
Seconda linea di difesa ter: filesystem e permessi 34
La terza linea di difesa: cosa mi nascondi? 40
Incorreggibile 42

5. Vietato l'accesso 45

La quarta linea di difesa: porte murate 45
Porta 135/TCP e 135/UDP 47

Porte da 1024 a 5000, sia TCP che UDP 52
La sincronizzazione oraria 56
I servizi server: porte 137/UDP, 138/UDP e 139/TCP 57
I servizi server bis: porte 445/TCP e 445/UDP 59
Condivisioni amministrative 60
L'assedio 63

6. Porte tagliafuoco 65

Una sentinella incorruttibile 65
La quinta linea difensiva 66
Arrivano i rinforzi 70
Regole ed eccezioni 74
Indirizzi, reti, maschere 76
Eccezioni... eccezionali! 78
Sentinelle a pagamento 79
Sceglierne uno 81

7. Difetti di fabbricazione 84

Crepe nel muro 84
Non solo il sistema operativo 85
Cosa e quando 86
Cliccare informati 87
Come si aggiorna 88
Aggiornare senza Internet 91
Rattoppare o non rattoppare? 92

8. Clicca QUI! 94

Terre inesplorate 94
Spyware e demolitionware 95
La cura sbagliata 97
Vieni a vedere cosa ho trovato! 99
Esca, trappola e vittima 100
Servizi gratuiti... a pagamento 101
C'è un aggiornamento! Corri! 103
Un secchio d'acqua per una goccia di olio 110
Nessuna salvezza 116

Caramelle dagli sconosciuti? 118
Se sembra complicato, forse lo è 119
Dico io chi chiamare 126
Esplorare con il cervello 128
9. Antibiotico a largo spettro 130
Virus, firme e DNA 130
Il laboratorio di virologia 131
Il database del DNA 132
Sempre, o su chiamata? 133
Reazioni immunitarie 135
L'analizzatore portatile 135
Perché non ha funzionato? 136
Scanner antispyware 140
Voglio il migliore! 141
Un uso efficace 142
10. Il postino suona N-volte 144
Lettere e pacchi 144
Aprimi, non aver paura... 145
Banche, pesci ed esche 147
Spam spam spam spam 150
NO SPAM, please! 152
Filtri, chiavi e liste 153
Opportunità da mancare 156
Il nigeriano generoso 156
Uomo fortunato! 158
Un lavoro facile facile 159
Il copertone farcito 160
Campanelli d'allarme 161
E' vero! L'ha detto mio cugino 162
Catene scatenate 164
C'è il postino, apro? 165

11. Tenere la destra 167
Sii ordinato 167
Attento a non sporcarti 169
Prevenire è meglio che curare 170
Ho seguito tutto, ma è successo lo stesso... 170
Io? Non ho fatto niente! 172
Ad ognuno il suo 173
La *checklist* 173
Basta così 176
12. Il finale 178
Approfondire 178
Dediche 180
Ringraziamenti 180
Glossario 182

Lista delle Figure

2-1. Un esempio di messaggio istantaneo 9
3-1. Virus Sensor: le connessioni TCP in arrivo 18
3-2. Dopo un anno 20
4-1. Le proprietà di base 35
4-2. Attivare la gestione dei permessi 35
4-3. Chi può fare cosa 36
4-4. Utenti normali e directory di Windows 38
4-5. Un uso degli Alternate Data Streams 42
5-1. Il primo effetto del virus Blaster 49
5-2. Servizi componenti 49
5-3. Servizi DCOM: Proprietà predefinite 50
5-4. Servizi DCOM: Protocolli predefiniti 51
5-5. Proprietà di un servizio 54
5-6. Il pannello di configurazione del NetBIOS 58
5-7. Le condivisioni amministrative 60
5-8. La modifica al registro di sistema 62
5-9. Modifica del valore di una chiave del registro 63
6-1. Attivare il firewall 66
6-2. Collegamento senza firewall 67
6-3. Collegamento con firewall 68
6-4. Servizi conosciuti dal firewall 69
6-5. Apertura di un nuovo servizio 69
6-6. L'accesso al nuovo firewall 70
6-7. Le impostazioni principali 72
6-8. Le eccezioni 73
6-9. Aggiungere una eccezione come porta 74
6-10. L'ambito di applicazione della eccezione 76
7-1. Configurare gli aggiornamenti automatici 88
7-2. Pronti per l'installazione 89
7-3. Scelta degli aggiornamenti da scaricare 90
8-1. Un dialer: icona, collegamento e pannello di avviso 102
8-2. Sta per scattare la trappola... 103
8-3. Una stampante che non abbiamo, ed un aggiornamento a 15 euro 105

8-4. Il computer non è più nostro... 106
8-5. Programmi indesiderati (col pallino rosso) 106
8-6. Programmi avviati automaticamente 107
8-7. Siti attendibili... per chi? 109
8-8. Per installare un nuovo sfondo 111
8-9. ...ma lo sfondo dov'è? 112
8-10. Si abbassi le braghe, prego! 113
8-11. Un amministratore per cambiare lo sfondo? 114
8-12. Le impostazioni delle "zone" di protezione 119
8-13. Le impostazioni avanzate 120
8-14. La configurazione di una zona 124
8-15. I permessi sul file dei collegamenti Internet 126

Capitolo 1. Prima di iniziare

Introduzione

Serata a casa di amici (o parenti, fate voi, il risultato non cambia). La cena è ottima, le voci pacate e l'atmosfera rilassata e tranquilla. Gli argomenti sono neutri, e a bassissimo livello culturale. Non che sia un problema, anzi, qualche volta riposare il cervello parlando di argomenti frivoli fa bene.

Arriva il caffè e magari un grappino. Perso nei vapori profumati del malvasia, arriva la domanda che rovina tutto. Sanno che "lavori coi computer", un modo elegante per dire che in realtà il tuo lavoro non lo conoscono, è anche difficile da spiegare in effetti. Ma ormai tutti hanno un computer in casa, quando non due o tre. E la domanda non ha tantissime varianti: il succo è "c'è qualcosa che non va, cosa può essere?".

Inizia l'incubo. Il cervello è ottenebrato dai vapori della grappa, lo stomaco protesta che vuole più sangue per il suo onesto lavoro, e si sa che noi maschietti ne abbiamo appena a sufficienza per un solo organo fra i tre: cervello, stomaco e... vabbè, ci siamo capiti. Con il barlume di lucidità che rimane abbozzi un tentativo di resistenza: mah, non saprei, possono essere tante le cause, in questo momento non ho con me la borsa dei ferri... L'altro non demorde: eddài, *che vuoi che sia per uno come te!* (questa è la frase che odio più di ogni altra). Ho tutto quello che ti serve: segue un elenco più o meno completo di noti antivirus, firewall, antispyware, programmini di test del computer, tutti rigorosamente *"scaricati" da Internet*, e corredati del rispettivo *crack*.

Rassegnato ti avvicini al rottame. In realtà è una meraviglia di computer, mediamente due-tre volte più potente di quello che usi normalmente per lavorare. Il *case* è di quelli ultramoderni, cattivissimi, pieno di lucine blu (luminosissime e fastidiosissime), nero metallizzato. Masterizzatore DVD double layer quantistico, masterizza talmente veloce che il DVD è pronto *prima* di inserire il supporto vergine. Monitor LCD da 19" spettacolare, a 16:9, impianto audio 5.1 con subwoofer messo dietro il monitor.

Poi lo accende: giga e giga di RAM, centinaia di giga di disco, velocissimo passa per le schermate del BIOS, poi appare la fatidica schermata in modo te-

sto, quella che mostra Windows XP quando qualcosa non è andato per il verso giusto nell'ultimo avvio. Selezioni "Ultima configurazione funzionante", e l'incrociatore stellare si trasforma in un canotto: rumore di trituramento del disco, il logo Windows XP ha la barra sottostante che si inceppa per dieci secondi, poi si muove un pezzetto, si blocca di nuovo. Dopo un paio di minuti buoni appare finalmente il desktop, pieno di icone di programmi installati. Ce ne sono centinaia, lo schermo è a 19", alla risoluzione massima, ed è pieno.

Troppo tardi comprendi che non sarà per niente facile. Fai un giretto esplorativo, non troppo convinto: lo "Start menù" è pieno all'inverosimile, tre-quattro colonne; in Rete e connessioni Internet ci sono delle icone con nomi fantasiosi; non hai attivato il collegamento a Internet, apri il browser e nei preferiti ci sono link che farebbero vergognare un marinaio dopo un anno di mare a bordo di una baleniera. Ovviamente la pagina iniziale punta su un sito dal nome molto adatto, per un fumetto porno, non certo per un sito web. Apri l'utility **msconfig**, e nelle voci di avvio trovi veramente di tutto.

Per farla breve, il computer è totalmente compromesso. Solo per eliminare i guasti più evidenti ci vorrebbe una settimana. Ovviamente i *due* antivirus e il personal firewall sono disattivati, qualcosa li spegne immediatamente all'avvio. Per non parlare dello scanner antispyware, che non parte proprio.

Vi suona familiare? Da che parte siete di solito? Quella del proprietario o quella del povero *esperto di computer*?

Basta con gli scherzi. La cosa è seria per un motivo molto semplice: un computer in queste condizioni non fa più quello che vogliamo, ma è nelle mani di qualcun altro. E' uno *zombi* agli ordini di altri. Quelli che hanno creato i vari spyware, virus, worm: in una parola dei *malware* che si sono infiltrati nel computer, con lo scopo di sfruttarne la capacità di elaborazione e il collegamento a Internet.

Perché

Chi ha letto uno dei miei pochi scritti, sa che di solito mi concentro su argomenti connessi al sistema operativo GNU/Linux. Ma ha anche capito che non appartengo alla schiera dei fanatici manicheisti per cui Linux è luce e bene, tutto il resto è

tenebra e male. Uso quello che trovo più adatto al lavoro che devo fare, e non mi creo problemi a usare un sistema operativo piuttosto che un altro. Se posso, uso e sostengo il software libero, ma è il cliente che comanda, e al di là di fornire un consiglio professionale, se il cliente vuole Giovanna invece di Marianna per me va bene.

La difficoltà maggiore con cui mi trovo tutti i giorni a combattere è data dall'aura di magia e mistero che circonda in generale i computer, con gli innumerevoli miti di contorno, primo fra tutti: il computer può fare qualsiasi cosa, basta il programma giusto.

NO. Non è vero. Se chi lo afferma è competente in materia sa di dire una gigantesca bugia, se invece non è "del mestiere", non ha ben chiara la funzione dei computer. I computer fanno quello che gli si dice di fare, chi impartisce ordini è l'essere umano. Il programma è uno strumento e basta. Tutti abbiamo usato almeno una volta martello e scalpello. Michelangelo ci ha fatto il Mosé in San Pietro. Io a malapena riesco a fare una traccia nel muro (storta), pestandomi tre-quattro dita. Il martello è lo stesso, è la *competenza* che cambia.

Eccoci al perché di questo testo: Windows XP può essere reso relativamente sicuro e mantenuto tale, a patto di sapere dove mettere le mani, e di accettare alcune regole di comportamento, semplicissime al punto da risultare banali, ma che richiedono impegno costante.

Non ci aspetteremo la soluzione totale, puntuale e definitiva, ma piuttosto l'occasione di apprendere un metodo, per capire come le cose sono realmente, e come sviluppare da soli le proprie strategie e contromisure. Non troveremo il pesce, ma impareremo a pescarlo.

Ci prefiggiamo uno scopo ambizioso, ma senza sfide la vita è una noia.

Cosa c'è e cosa non c'è

Se siamo stufi di stare con l'ansia addosso per ogni e-mail con allegati, per ogni *popup* che si apre durante la navigazione e per ogni stranezza che ci troviamo davanti, se vogliamo essere sicuri che il computer sia solo ai nostri ordini, e i dati siano accessibili solo a noi, questo potrebbe essere un punto di partenza.

Se vogliamo *capire* come funzionano le cose "sotto il cofano", perché i virus entrano, da dove entrano e perché le contromisure più consigliate e applicate sembrano inefficaci, questo è il posto giusto.

In breve, sia che ci ritroviamo nel personaggio dell'esperto che in quello del normale utilizzatore dell'aneddoto di poco fa, questo documento potrebbe fare al caso nostro.

Quello che non dobbiamo aspettarci sono le ricette magiche: fai così e cosà e tutto va a posto senza fatica. Se è questo che cerchiamo, non è il testo che fa per noi. Lo stesso se siamo convinti che basti antivirus e firewall per stare tranquilli: molliamo qui.

Altra cosa che non troveremo è come rimettere in sesto un computer ridotto a un rottame come quello citato nell'introduzione. Il numero di differenti schifezze che potrebbe aver messo i piedi dentro i meccanismi più delicati del sistema operativo per fare i propri comodi è astronomico: serve tempo, qualcuno che sappia dove mettere le mani e soprattutto *competenza*. Questa non si acquisisce leggendo un paio di pagine web o un testo introduttivo come questo. Quindi se vogliamo rimettere in sesto il nostro computer devastato dai virus, non troveremo aiuto qui.

Come termine di paragone, quando un server o in generale un computer con installato un sistema operativo GNU/Linux o Unix viene colpito da un malware, la procedura standard è di considerare *compromesso* il computer: niente di quello che vi è contenuto come sistema operativo, driver o programmi è ritenuto attendibile, perché il malware potrebbe aver sostituito qualsiasi cosa con programmi propri, modificati per far sembrare il sistema integro (vedremo che molto spesso i malware per Windows impiegano strategie dello stesso tenore per renderne più difficile sia la rilevazione che la rimozione). Per questo motivo, nel momento in cui si ha la conferma che qualcosa è successo, si fa una copia immagine (una copia bit per bit del contenuto) del disco contenente il sistema operativo, un backup dei dati, e si cancella tutto, ripartendo da una installazione pulita. Poi viene la parte più difficile e delicata: l'analisi dell'immagine salvata del sistema operativo compromesso alla ricerca del punto di ingresso, non sempre facile da trovare, allo scopo di evitare che l'intrusione si ripeta. Il mio consiglio è di applicare la stessa procedura: è più sicura, e permette di partire da una situazione di totale certezza di pulizia.

Cosa occorre

Un computer con una installazione fresca di Windows XP Professional. Non devono essere aggiunti programmi di alcun tipo, solo i driver basilari per le periferiche principali: video, rete, modem. Non deve essere *mai* stato collegato a Internet. Non occorre il Service Pack 2. Non subito almeno.

Se e quando occorrerà installare qualcosa si tratterà di software libero, che non richiederà di spendere nulla, e sarà perfettamente legale. Niente *crack*, niente programmi in prova o da acquistare.

Si presume che il lettore conosca l'uso di Windows, in particolare sappia effettuare le normali operazioni di gestione e configurazione del computer.

Legalese

L'incorretto uso di alcune delle procedure spiegate nel testo può causare perdita di dati nel computer su cui vengono effettuate e nei computer collegati in rete da esso raggiungibili. Si fa presente quindi che eventuali danni causati dall'incauto o incosciente uso di quanto spiegato in questo testo sono completamente a carico di chi opera. Non sono e non posso essere responsabile di errori e danni commessi per incoscienza, inesperienza o imperizia.

Quanto scritto qui è frutto di studio, di test accurati e di esperienza diretta di chi scrive. Ma niente e nessuno può pensare di prenderlo come bibbia assoluta e immutabile. L'errore è in agguato, sempre, e l'evoluzione nella giungla virtuale di Internet è rapidissima: quello che in questo istante è sicuro e provato, fra due ore potrebbe non valere più.

Ultima cosa: niente e nessuno può garantire che con una qualsiasi operazione, quale che sia, possa rendere qualcosa perfettamente sicuro. Nessun programma, nessuna procedura, nessuna magia tecnologica può assicurare l'invulnerabilità. Né tantomeno lo posso fare con questo testo: ogni giorno escono nuovi modi per aggirare le protezioni e le contromisure, anche le più sofisticate, quindi l'unica salvezza è *diffidare, dubitare e controllare*. Tenere sempre presente il motto del protagonista di X-Files: *Trust no one*. Non fidarti di nessuno.

Come leggerlo

Il testo è diviso in argomenti chiusi, per ognuno dei provvedimenti da applicare. Ogni *malware* ha la sua porta di ingresso, e la relativa contromisura, che qualche volta è scomoda e richiede un cambio di abitudini.

Per avere le maggiori possibilità di riuscita, sarebbe opportuno applicare tutte le misure riportate, nell'ordine elencato. Saltarne anche una sola potrebbe rendere inutile tutto il lavoro, in breve il nostro computer sarebbe di nuovo una fogna.

Una nota importante: in presenza di termini particolari che, pur essendo sinonimi, sono usati in contesti e significati differenti, per non generare equivoci in una nota spiegheremo il senso e la differenza fra loro.

Capitolo 2. Conosci il Nemico

Prima di partire per la guerra, e vedremo che di guerra si tratta, faremo come molti noti strateghi: studieremo il problema da tutti i punti di vista, con particolare attenzione alle caratteristiche del campo di battaglia e soprattutto alle motivazioni del nemico. Niente di meglio che sapere cosa spinge qualcuno a fare una qualsiasi cosa, quali siano le sue aspettative, le sue mire, le sue tecniche, le sue convinzioni per poi capire come e dove colpirà, e con quali metodi.

I problemi di Windows XP

E' ormai opinione consolidata che Windows XP sia un prodotto nato con qualche problema di sicurezza, in gran parte determinato da bug molto critici in alcune parti del sistema operativo e in alcune delle librerie di base.

Questo è innegabile, ma questi problemi affliggono in misura variabile *tutti* i sistemi operativi, e più in generale tutti i software, di qualsiasi tipo essi siano. La realtà è che i problemi di sicurezza di Windows XP (nel seguito per brevità ci riferiremo a esso come XP e basta) derivano soprattutto da una scelta di impostazioni iniziali del sistema tesa a renderne semplice l'uso da parte di tutti, soprattutto da parte di utenti non propriamente "informatici".

L'intento è ammirevole e degno di considerazione, ma purtroppo si scontra con una realtà che di amichevole ha ben poco.

L'installazione base di XP prevede le seguenti impostazioni:

- Viene tollerata una installazione con un unico account, di tipo amministratore. La password viene richiesta, ma può essere nulla, vuota.
- Vi sono servizi attivi e accessibili dalla rete, utilizzabili con credenziali anonime o dell'account amministratore locale. Se l'account amministratore non è protetto da password questi servizi sono praticamente accessibili senza restrizioni. I servizi comprendono, fra gli altri: la modifica remota al registro di sistema, il servizio di messaggistica, il servizio di esecuzione programmi a orario.

- Il servizio di condivisione file e stampanti è attivo e ha una directory aperta e scrivibile da tutti, in modo anonimo, quella denominata `Documenti condivisi`. Non sarebbe un gran problema, in quanto non è una cartella critica o di sistema, ma tramite il servizio di esecuzione programmi a orario è possibile depositare un programma in questa directory e avviarlo dalla rete, senza accedere fisicamente al computer.
- Sono attive alcune condivisioni nascoste, dette *administrative shares*, usate per l'amministrazione remota del computer: le più pericolose corrispondono a tutte le directory principali dei dischi fissi e alla directory di sistema di XP. I nomi sono rappresentati dalla lettera del disco fisso con il simbolo del dollaro alla fine (C$, D$, E$, ecc.), e ADMIN$ per la cartella di sistema di XP, e sono accessibili con l'utente amministratore. Se questi ha password nulla diventano accessibili da chiunque.
- I servizi accessibili da rete sono raggiungibili da tutte le interfacce di comunicazione presenti sul computer, anche su quelle attivate successivamente all'accensione, per esempio tramite modem analogico o ADSL.
- Eseguendo il browser con l'unico utente presente sul computer, che, lo ricordiamo, ha diritti di amministratore, esiste la possibilità di far scaricare ed eseguire porzioni di codice binario, denominati *ActiveX*, con i diritti dell'amministratore, di conseguenza con totale e illimitato accesso a tutte le risorse del computer. In teoria questo è stato fatto deliberatamente per permettere il funzionamento di Windows Update, che altrimenti non potrebbe funzionare.

Queste sono alcune delle principali falle introdotte dalla configurazione di base al momento dell'installazione. A chi ha esperienza di configurazione di servizi di rete in Unix/Linux, non può non sfuggire l'enormità di alcune di esse.

Lo ripetiamo: l'intenzione è ottima e condivisibile, ma il risultato è disastroso, ed è sotto gli occhi di tutti.

Come "i cattivi" entrano nel computer

Nella situazione di una installazione fresca di XP, con un utente solo, senza pas-

sword assegnata, le porte aperte messe a disposizione dalle configurazioni viste poco sopra sono molteplici, tutte facilmente sfruttabili.

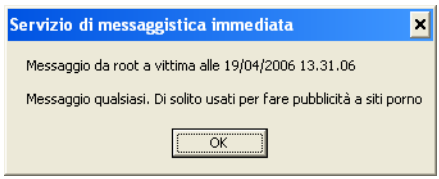
Utenti e account

Capita che questi due termini siano utilizzati come sinonimi, mentre ci sarebbe una distinzione, anche se la maggior parte delle volte sarebbe desumibile dal contesto. *Utente* è la persona che usa il computer, mentre *account* è lo spazio e l'accesso ad uso personale che si ha su un computer, normalmente identificato da un nome breve, detto anche *login name* o solo *login*. Per evitare confusione useremo i due termini in modo appropriato, quindi con utente indicheremo la persona, mentre con account lo spazio personale che ha sul computer. Per fare un parallelo, l'account è il conto in banca, la login è il numero di conto bancario, e sono entrambi ben altra cosa rispetto al proprietario del conto.

La login dell'account creato al momento dell'installazione è rilevabile dall'esterno tramite una semplice operazione di richiesta anonima via rete. Il sistema operativo fornisce diligentemente il nome del computer, del gruppo di lavoro e dell'utente connesso in quel momento. Una volta scoperto il nome, se l'account non ha password assegnata è immediatamente sfruttabile per connettersi a una condivisione amministrativa, scaricare un programma in una qualsiasi directory all'interno del computer e avviarlo con il servizio di esecuzione a orario. Il gioco è fatto.

Alcuni servizi sono accessibili e utilizzabili senza fornire alcuna credenziale. Il servizio detto *Messenger* (niente a che vedere col noto programma di chat e *Instant Messaging* di Microsoft) è attivo e in ascolto, e basta la semplice ricezione di un messaggio per provocare la comparsa di un *popup* dal titolo "Servizio di messaggistica immediata". Un esempio lo possiamo vedere in Figura 2-1.

Figura 2-1. Un esempio di messaggio istantaneo



Allo stesso modo si può accedere al disco da un altro computer via rete, dopo aver individuato il nome dell'utente connesso in quel momento, e senza fornire altri dati si possono depositare file a piacere, in qualsiasi punto del disco.

Per ora fermiamoci qui. Dovrebbe essere chiaro il livello di accesso possibile a un qualsiasi malintenzionato con una installazione base di XP. Inutile dire che questa situazione è inaccettabile, sotto tutti i punti di vista.

Senza fare nulla

Tutto quanto elencato rende possibile l'ingresso di ogni genere di porcherie nel computer *anche senza fare nulla di particolare*. Basta essere collegati a Internet, non occorre aprire il browser, leggere la posta elettronica, o fare qualsiasi altra cosa.

Qui sta la relativa novità e la estrema pericolosità di questa situazione: non occorre che l'ignaro utilizzatore del computer faccia qualcosa in particolare, non deve avviare programmi, scaricare la posta o aprire allegati. Attraverso le falle indicate sopra (e alcune altre), i malware entrano senza problemi, e prendono possesso del computer.

Una volta entrati e attivati, non c'è più protezione che tenga: gli antivirus vengono disattivati, o più sottilmente si disattiva la scansione automatica e l'aggiornamento, per cui l'antivirus non è in grado di riconoscere il virus, né di aggiornare il proprio database; il firewall viene modificato e configurato silenziosamente per accettare senza protestare le nuove connessioni stabilite dal

malware stesso; vengono scaricate e avviate nuove versioni del malware, o aggiunti componenti per attivare funzioni particolari. In pratica, il computer passa sotto le mani di qualcun altro, che installa ed esegue quello che vuole.

Il peggio deve ancora venire. Una volta insediato il malware, si avvia la fase di *zombificazione*: a seconda delle necessità, il nostro computer può diventare un server di posta anonimo per inviare valanghe di messaggi pubblicitari e copie del virus stesso; può diventare *untore* andando alla ricerca di altri computer da infettare, passandogli il programma malevolo; può essere usato come un registratore della nostra attività, memorizzando tutti i tasti che premiamo, i siti web che visitiamo, le parole che mettiamo nei motori di ricerca, gli indirizzi di posta elettronica a cui scriviamo, per poi comunicarli al proprietario. Non c'è limite: il malware ha completo accesso al computer e può fare quello che vuole.

Quel che è peggio, per la legge italiana la responsabilità è nostra, e sta a noi dimostrare che abbiamo fatto il possibile per evitarlo. Paradossale, ma è così.

Antivirus? Firewall? Che fanno, dormono?

Per quanto strano possa sembrare, questi due strumenti sono i più diffusi e contemporaneamente i più bistrattati dagli utilizzatori. Quello che dobbiamo capire è che sono solo strumenti automatici, e che fanno quello che sono progettati per fare. Chi ogni giorno studia nuovi modi per entrare furtivamente nei computer altrui ha una conoscenza estesa dei meccanismi interni di antivirus e firewall, e può aggirarne le protezioni in modi che neanche immaginiamo.

Questo non vuol dire che siano strumenti inutili, ma la trappola è pensare che si possano sostituire al buonsenso, alle regole di comportamento e al nostro cervello. Apriamo allegati, lanciamo *crack*, navighiamo per siti di malaffare, *tanto c'è l'antivirus*. E' il comportamento più ingenuo del mondo. L'antivirus arriva sempre tardi, quando il danno è fatto. *L'antivirus è l'ultima spiaggia*, l'ultimo fossato, la difesa estrema. Se un malware arriva all'antivirus vuol dire che ha sconfitto e aggirato tutto quello che c'era prima, è a un passo dalla meta. E quando arriva spesso l'antivirus non ha i dati per riconoscerlo, perché *può scoprire solo i virus vecchi*, quelli che già conosce. Il virus nuovo, per definizione, è sconosciuto, e se riesce ad arrivare a contatto dell'antivirus lo rende innocuo: ferma la scansione

in tempo reale e impedisce l'aggiornamento delle *firme* dei nuovi virus. Da quel momento l'antivirus è del tutto inutile.

Connessioni e collegamenti

Per evitare confusioni, useremo i due termini *collegamento* e *connessione* non come sinonimi, ma indicheremo con il primo quello che si usa per l'ingresso in Internet o in una rete locale, mentre con il secondo i canali logici che vengono stabiliti fra due computer in rete, locale o Internet, quando scambiano dati fra loro. Purtroppo in Windows i collegamenti a Internet o in rete locale sono chiamati "connessioni" nello spazio apposito del Pannello di Controllo, ma questa sarà l'unica eccezione nel seguito. Quindi diremo: il *collegamento* a Internet, le *connessioni* rifiutate dal firewall.

Il firewall è appena un passo prima dell'antivirus. I personal firewall di ultima generazione controllano non solo le connessioni in ingresso, ma anche quelle in uscita e da quali applicazioni vengono. Lo ripetiamo: chi crea malware conosce benissimo il funzionamento dei firewall, e ha già pronte tutte le contromisure necessarie. La prima e più banale è di disattivarlo, seguita dal registrare autonomamente come autorizzate le connessioni verso l'esterno avviate dal malware stesso. Altro trucco molto usato è di sfruttare programmi autorizzati e insospettabili, come il browser, per avviare connessioni che poi vengono pilotate dal malware. Il firewall non si accorge di nulla, l'applicazione che chiede la connessione è abilitata a farlo. Si è arrivati a dimostrare la possibilità di intercettare la finestrella di conferma che mostra il firewall per ogni nuova connessione da parte di una applicazione sconosciuta, e di simulare la pressione del pulsante OK. Tutto questo è ampiamente documentato nelle mailing list che si occupano di sicurezza e vulnerabilità delle applicazioni e dei sistemi operativi:

- Su Securityfocus, un articolo[1] sull'utilizzo di applicazioni "fidate" per connettersi aggirando il firewall.

1. http://www.securityfocus.com/archive/1/411908

- Sempre su Securityfocus, un altro articolo[2] sulla manipolazione degli avvisi del firewall.

Solo due esempi sui tanti possibili.

Se il malware arriva dentro il computer e si attiva, non c'è più niente da fare. Affidare la nostra difesa unicamente a firewall e antivirus (utilissimi, sia ben chiaro) è come lasciare aperte le porte e le finestre di casa, tanto abbiamo la pistola. Va benissimo fino a quando il ladro non sa che ci siamo noi dentro. Poi entrerà con un bastone, e ci sorprenderà alle spalle.

L'esercito delle infinite scimmie

Come in ogni esercito esistono i vari corpi con le rispettive specialità, anche con i malware esistono le categorie e le classificazioni, anche se non c'è uno standard. Ci sono stati tentativi di uniformare la denominazione, ma con i malware di ultima generazione si vede che è impossibile assegnarli ad una classe specifica, possedendo caratteristiche di più classi differenti fuse in una miscela micidiale.

Il ritmo di creazione di nuovi virus con nuove abilità è impressionante: per strumenti come gli antivirus è impossibile stare dietro a tutte le novità ed a tutte le varianti, lo vedremo meglio nel capitolo apposito. Ma abbiamo una strategia migliore: capire come il virus riesce a propagarsi, a insediarsi in un computer. Una volta scoperto il vettore di trasmissione e il punto debole colpito, proprio come si fa con i virus biologici, si può procedere all'applicazione delle contromisure. In un colpo solo possiamo chiudere la porta a migliaia di malware differenti, e bloccare un vettore di trasmissione una volta per tutte. Questa strategia è infinitamente più efficace di andare a cercare i virus uno per uno.

Malware e virus

I due termini indicano due cose diverse, ma li useremo come sinonimi: vista la complessità dell'argomento almeno su questo non faremo troppo i pignoli.

2. http://www.securityfocus.com/archive/1/385930

Ci sono virus in grado di propagarsi autonomamente via rete, e virus che necessitano di un nostro (certamente involontario) aiuto per diffondersi. Alcuni sono capaci di nascondersi e di impedire all'antivirus di scoprirli o di rimuoverli una volta scoperti. Malware che possono creare un avamposto nel computer colpito e metterlo agli ordini di chi ha creato il virus. Virus capaci di spiare la nostra attività al computer e mettere i nostri segreti nelle mani di qualcun altro. Non c'è limite a quello che può fare un malware, e ogni giorno nascono nuove abilità per fare danni. Ne vedremo molti strada facendo, ed al momento di nominarli spiegheremo le loro abilità particolari.

Ma il peggio è che un virus non si limita a fare una sola cosa, ma sempre più spesso è in grado di compiere molte attività differenti, gran parte delle quali destinate ad impedirne la rilevazione o la rimozione. Per questo non è sufficiente installare un paio di programmini magici consigliati dall'amico e via, come non potrà mai esistere il programma antivirus definitivo.

E' una lotta senza fine fra chi crea virus e chi crea programmi per combatterli, per molti versi simile alla eterna lotta fra chi crea serrature sempre più sofisticate e gli scassinatori sempre più abili.

Per fortuna, come dicevamo, c'è una differenza: si può intervenire a monte, chiudendo la via attraverso cui si propagano, ma rimane sempre una strada che non potrà mai chiudersi: l'inganno. Vedremo che quando non è possibile propagare un malware in altro modo, i creatori di virus contano sul nostro tanto prezioso quanto involontario aiuto.

C'è poco da scherzare

Possiamo sempre dire che in fondo nel nostro computer non abbiamo cose importanti. O che non ci crea problemi se un virus o due rompono un po' le scatole mentre navighiamo in Internet. Se però il nostro computer, controllato da un malware, va a infilarsi nel computer di qualcun altro per fare danni, di questo siamo legalmente responsabili. Se per nostra incuria il virus che abbiamo si propaga all'interno di una rete aziendale potremmo essere ritenuti responsabili di danneg-

giamento. E sta a noi dimostrare che non è intenzionale.

Quindi non è ammissibile sottrarci alle nostre responsabilità adducendo scuse più o meno plausibili. Certo, moralmente non è colpa nostra, perfettamente d'accordo. E' come addossarci la colpa del fatto che le automobili, legalmente vendute e regolarmente acquistate, siano in effetti inquinanti e nocive per la salute. Il discorso potrebbe andare all'infinito con mille altri esempi: acquistiamo un prodotto e poi dopo un anno ci avvertono che non solo è nocivo per noi, ma lo è anche per chi ci sta intorno, e dopo un po' diventa anche illegale continuare a possederlo.

Sono i paradossi della nostra cultura tecnologicamente frivola e sprecona, ma questa è un'altra storia. In questo caso possiamo fare qualcosa per riprendere possesso del nostro computer, e non costa nulla.

Capitolo 3. Falle, porte e fossati

Difendere un fortino

Iniziamo la nostra sfida assumendo un modello di pensiero: il nostro computer è un fortino, un castello da proteggere, inespugnabile e sorvegliato. Il problema è che questo castello è stato costruito lasciando aperte tante vie d'accesso, pensate per facilitarne la vita all'interno, offrendo però la possibilità ai malintenzionati di entrare senza essere ostacolati. Abbiamo lo scarico delle fogne, l'ingresso di servizio per le consegne, l'acquedotto, gli sportelli degli uffici aperti al pubblico esposti all'esterno, insomma tutto quello che serve per renderne efficienti i servizi e comoda la vita all'interno.

Pensiamo da malviventi: le fogne arrivano praticamente in tutti i locali interni; l'ingresso di servizio per le consegne è accessibile a chiunque si presenti con un pacco in mano; i tubi dell'acquedotto non sono interrati; gli sportelli degli uffici consentono l'accesso all'interno del castello senza controlli.

Se prendiamo contromisure estreme il castello diventa in breve invivibile: fogne chiuse, niente consegne, niente acqua, uffici chiusi. In breve diventa inutile.

Questa metafora rende l'idea del problema che si trova davanti chi si occupa di sicurezza: la sicurezza estrema rende la vita impossibile ed è indirettamente un incentivo per i normali utilizzatori a cercare scorciatoie per aggirare quello che percepiscono come un ostacolo, mentre la comodità estrema è purtroppo antitetica alla sicurezza. La sicurezza sostenibile è un compromesso fra usabilità e invulnerabilità.

Lo scopo è di rendere il castello un po' più inaccessibile ai malintenzionati, e di mantenere un livello accettabile di comodità per chi ci vive.

Il laboratorio

Le soluzioni che andremo ad applicare al nostro computer non sono semplicemente lette qua e là e riportate in bella copia, ma sono state sperimentate in un

ambiente controllato che replica il peggior concorso di circostanze sfavorevoli in cui un computer si può trovare.

La situazione in cui sono stati fatti i test è la seguente: il computer è in realtà virtuale, creato con Qemu[1], un emulatore Open Source di computer, nella versione 0.8.0, installato nel mio notebook sotto il sistema operativo Linux Fedora Core 4 (per i curiosi ci sono delle guide per installare Fedora sul mio sito[2]). La rete a cui fa capo il computer virtuale è dietro un router ADSL, configurato per fare il NAT uno a uno con l'indirizzo di rete del computer virtuale. In parole povere significa che il computer virtuale è praticamente collegato direttamente a Internet, e non beneficia di alcuna protezione dal router. Nel computer che ospita quello virtuale c'è in esecuzione il noto *sniffer* di rete Wireshark[3], che permette di tenere sotto controllo il traffico fra il computer virtuale e il resto di Internet.

Per chi avesse dubbi sul funzionamento di questa configurazione, sappia che è una modalità utilizzata in molti laboratori che studiano i metodi di infezione e propagazione dei malware.

In alcuni test, quelli sul browser specialmente, per verificare che i malware siano effettivamente introdotti solo dalle azioni compiute e non si propaghino senza controllo, le operazioni sono eseguite con una configurazione piuttosto differente, in cui il computer è posizionato dietro due firewall in cascata: quello principale, fornito dal router citato sopra, e quello implementato da un computer con due schede di rete e una distribuzione Linux, per impedire all'eventuale malware di accedere agli altri computer sulla rete casalinga.

Quanto resiste il fortino?

Per fugare ogni dubbio, anche a me stesso, sull'efficacia di questo sistema di prova, ho fatto l'unica cosa possibile: ho esposto il computer virtuale, con XP installato di fresco e senza aver applicato nessuna delle configurazioni citate nel seguito, connettendolo a Internet.

1. http://fabrice.bellard.free.fr/qemu/
2. http://www.ismprofessional.net/pascucci/
3. http://www.wireshark.org/

Prima del collegamento ho attivato Wireshark per catturare tutto il traffico di rete, e ho configurato il router come detto sopra. Il risultato è stato devastante: appena sei secondi dopo che il computer virtuale ha avviato l'interfaccia di rete è arrivato il primo tentativo di connessione, ottenendo il risultato voluto: è iniziato immediatamente il trasferimento di un file all'interno del computer virtuale, terminato dopo un minuto e mezzo. Dopo una quarantina di secondi il malware si è attivato, stabilendo una connessione con un server IRC, partendo poi con una scansione a tappeto della rete per infettare altri computer. Nel frattempo sono arrivati altri tre tentativi da tre indirizzi differenti, tutti conclusi con successo, e tutti accompagnati dall'inizio del trasferimento di un file verso il computer virtuale, diventato intanto lentissimo.

Fermato il tutto, ed esaminata l'immagine del disco del computer virtuale ho trovato una serie di file nuovi nella directory `C:\windows\system32`, uno dei quali dal nome `Issass.exe`, di quasi trecento kilobyte. Passato al sito Virustotal[4], che permette la scansione al volo di un file con un nutrito gruppo di antivirus, metà degli antivirus lo riconoscono come una variante del worm *Rbot*, l'altra metà non rileva nulla di sospetto.

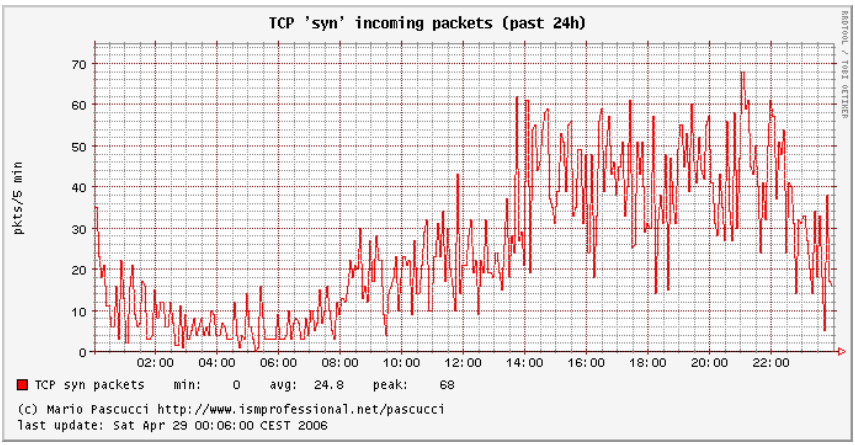
Riassumendo: meno di dieci secondi per essere raggiunti da un altro computer infetto; meno di due minuti per avere il computer con un virus attivo all'interno. E non era l'ora di punta.

L'epidemia della rete

Chi ha visitato il mio sito ha potuto vedere il *Virus Sensor*. La spiegazione di cosa faccia e di come funzioni sarebbe molto lunga, ma limitiamoci a guardare un singolo grafico, relativo al 28 aprile 2006 (Figura 3-1), e a spiegarne il senso.

4. http://www.virustotal.com/

Figura 3-1. Virus Sensor: le connessioni TCP in arrivo



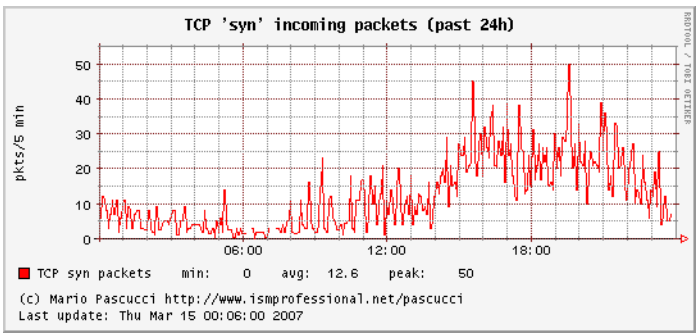
Il grafico mostra il numero di pacchetti di richiesta di inizio connessione provenienti da Internet, conteggiati ogni trecento secondi, cinque minuti. L'andamento generale è influenzato dal numero di computer accesi sul tratto di rete del provider a cui sono collegato. Di notte, dall'una alle sei del mattino, il traffico è ridotto e causato in parte da computer infetti perennemente accesi, certamente infetti a insaputa del proprietario, ed in parte da computer posizionati in altre nazioni, attivi data la differenza di orario. Il traffico aumenta leggermente durante la mattinata, arrivando al triplo del traffico notturno. Il massiccio aumento intorno alle prime ore del pomeriggio non è occasionale, ma si ripete tutti i giorni, e coincide con l'accensione di computer di ignari studenti e lavoratori che, terminata l'attività della giornata, arrivano a casa.

Il significato di questa situazione è che un computer collegato a Internet senza particolari precauzioni e senza protezioni, a parte l'antivirus, viene attaccato da un virus in media ogni dieci secondi dal momento in cui inizia il collegamento a Internet. La probabilità che l'antivirus non riconosca il virus è molto alta e, sommato alla frequenza delle infezioni, potrebbe far sì che in una giornata di

collegamento a Internet un computer collezioni (è proprio il caso di dirlo) una ventina di virus differenti.

Cosa è cambiato ad un anno di distanza? Quasi nulla. Possiamo rendercene conto guardando una immagine recente, relativa al 14 marzo 2007 (Figura 3-2), quindi dopo quasi un anno (ed innumerevoli aggiornamenti di sicurezza, nuove versioni di antivirus, antispyware, firewall, un nuovo rilascio di Windows). Ne è passata di acqua sotto i ponti, informaticamente parlando ma, come possiamo vedere, non è che la situazione sia migliorata di molto...

Figura 3-2. Dopo un anno...



Se mai ci fosse bisogno di ulteriori conferme, questa è in “presa diretta”.

Prevenire e difendere

Se abbiamo avuto la pazienza di leggere fin qui, dovremmo aver capito quale sia la posta in gioco e la facilità di cadere vittime di infezioni. La buona notizia è che si può fare molto, e rendere difficilissima la vita a chi voglia infilarsi nel nostro fortino. Fatto il giro di ispezione in cui troviamo tutte le falle nel nostro muro esterno, e i punti di accesso non sorvegliati, possiamo partire con le opere

di fortificazione. E' questo il punto fondamentale che dobbiamo comprendere: se non chiudiamo i punti di accesso, è perfettamente inutile riempire il cortile del castello di guardie armate: in breve sarà ridotto a un campo di battaglia, con cadaveri, rottami e devastazioni.

E' molto più efficiente e sicuro ridurre i punti d'accesso a uno solo e sorvegliarlo attentamente. I castelli avevano il ponte levatoio prima della unica porta di accesso, un fossato profondo, pieno di animaletti poco amichevoli, la porta di accesso era sorvegliata da guardie armate che infilzavano chiunque si avvicinava senza farsi riconoscere *prima* di arrivare alla porta. Come ulteriore misura c'erano gli scarichi fognari chiusi da pesanti grate e pozzi per prendere acqua potabile *all'interno* del castello.

A partire dal prossimo capitolo cominceremo a fortificare il nostro castello, modificando comportamenti nostri e configurazioni del computer. Questa operazione è quello che in gergo tecnico viene chiamato *hardening*, fortificare, indurire, rendere più solido.

Capitolo 4. Cominciamo dalle basi

Partiamo da alcune misure basilari, semplici da applicare e molto efficaci. Due sono i tipi di intervento: difese e contromisure. La differenza è che le difese servono a evitare di cadere vittime di malware e disastri, mentre le contromisure servono per ridurre il danno a disastro avvenuto. Quindi: le difese per impedire il disastro, le contromisure per evitare che sia irreparabile.

La prima linea di difesa: sapere

La prima cosa che ci protegge dal pericolo è il sapere che esiste. Se poi ne conosciamo i dettagli, possiamo cominciare a prendere provvedimenti, studiare strategie, decidere contromosse. Nella beata ignoranza camperemo certamente più tranquilli, fino al duro risveglio, che può essere una semplice bolletta del telefono a quattro cifre intere, o la propria carta di credito totalmente svuotata, e pure in rosso. O trovarsi invischiato in una indagine della magistratura per aver ospitato sul proprio computer immagini delle quali non sappiamo nulla.

Per cui occorre essere informati, conoscere i pericoli, quelli veri, e da fonti affidabili, non dall'amico praticone, o dalle catene di santantonio. Esistono vari siti web conosciuti e apprezzati per il servizio che offrono, tutto sta a perdere qualche minuto ogni settimana per aggiornarsi, avremo solo che da guadagnarci.

Sapere che il nostro computer ha una potenziale falla, o che i messaggi di posta elettronica annuncianti premi di milioni di dollari sono in realtà elaborate truffe è tanto importante quanto sapere che esistono i borseggiatori e i ladri d'appartamento.

Lo scopo dei malviventi è sempre lo stesso: rubare soldi e farla franca, cambia solo la modalità, e dobbiamo essere pronti a conoscerla in anticipo.

La prima contromisura: il backup

Leggendo un qualsiasi testo sulla sicurezza, o gran parte delle risposte date nei forum, per strano che possa sembrare, questa operazione non appare quasi mai, non viene neanche presa in considerazione. Il fatto banale che nessuno sembra

tenere presente è che i componenti di cui è composto il computer, quelli fisici, sono soggetti a usura e guasti. I dischi rigidi hanno bronzine e cuscinetti che si usurano, gli alimentatori e la scheda madre hanno varie decine di componenti che invecchiano con l'uso. Anche i componenti più affidabili, quali i circuiti integrati, sono soggetti a rotture interne per via dei cosiddetti *cicli termici*: il passaggio dal freddo, a computer spento, al caldo, a computer acceso, provoca una serie di stress meccanici tali che un numero abbastanza prevedibile di cicli acceso/spento porta al guasto. Inoltre situazioni come la cattiva aerazione e il ristagno di polvere provocano l'accelerazione dell'invecchiamento a causa della mancanza di dissipazione del calore. Non basta una ventola più grande, se poi il computer è chiuso all'interno di un mobile senza aperture.

Un guasto elettronico o peggio meccanico del disco interno implica nella quasi totalità dei casi la perdita irrecuperabile del contenuto. Non c'è programma di recupero che tenga, se il disco ha un guasto meccanico, confermato da rumori insoliti durante l'accensione o il funzionamento, l'unico modo di recuperare qualcosa è rivolgersi alle società specializzate, che chiedono un tanto a kilobyte. Sempre che non sia successa una catastrofe, come mi è capitato di vedere, tipo una testina magnetica che si stacca e incide il disco raschiandone la superficie.

Per quanto strano possa sembrare, non sono racconti dell'orrore, sono cose che succedono tutti i giorni. Un mio amico aveva aggiunto memoria al computer, rivelatasi poi difettosa. Ma nel frattempo, nell'aprire la contabilità che teneva con un programma apposito, la memoria guasta aveva rovinato i dati e nello scriverli su disco li aveva resi inservibili. Risultato: reinserimento di tre anni di fatture e di contabilità, di cui per fortuna aveva conservato l'archivio cartaceo. Una collega mi ha chiamato disperata perché il computer dell'ufficio non partiva più, ed aveva nel disco il lavoro dell'ultimo anno. Arrivato là, la società pagata appositamente per la manutenzione aveva già decretato la perdita definitiva dei dati. La collega insisteva così disperatamente che non potevo tirarmi indietro, ma all'accensione del computer ho capito subito che non c'era più nulla da fare: il disco emetteva un cigolìo continuo senza mai arrivare al numero di giri necessario per il funzionamento. Ovviamente il lavoro era solo su quel disco.

Arriviamo al punto. Per capire se abbiamo bisogno di un backup basta rispondere a queste domande:

- I dati sono conservati in più posti fisici differenti? (due dischi nello stesso computer non vale)
- I dati si possono ricreare, per esempio reinserendoli?
- Per ricrearli è sufficiente solo qualche ora di lavoro?

Se abbiamo risposto con un *no* anche a una sola di queste domande abbiamo assoluta necessità di un backup. Se poi si verifica la condizione che i dati cambiano spesso, una volta al giorno per esempio, abbiamo necessità di una politica di backup adeguata.

Cerchiamo di capire meglio cosa fare, prendendo esempi pratici. Se con il computer lavoriamo i filmini delle vacanze, possiamo accontentarci di conservare le videocassette in originale, e di tenerle almeno fino alla realizzazione del supporto finale, per esempio un DVD video. Una volta masterizzato il DVD, meglio se in doppia copia su supporti di produttori differenti, possiamo pensare di cancellare i file sul computer e di riutilizzare le cassette video. Se perdessimo i file nel computer in un momento qualsiasi della lavorazione, avremmo sempre gli originali su videocassetta, anche se occorre rifare il lavoro di riversamento daccapo.

Chi sviluppa software ha un problema molto più grande, dovuto non solo alla estrema mutevolezza dei dati, visto che i sorgenti vengono modificati in continuazione, ma al fatto che spesso deve tenere versioni differenti dello stesso sorgente. Qui viene molto utile un sistema di versionamento e conservazione centralizzata, tipo CVS[1] o Subversion[2], disponibili anche per Windows. Lo spazio dove questi programmi conservano i sorgenti può essere sottoposto a backup senza problemi, dato che usano normali file senza strani trucchi.

Un discorso a parte merita la posta elettronica, subordinato al tipo di programma che si usa. Alcuni di essi non offrono possibilità di fare backup, e il formato in cui è conservata la posta è assolutamente proprietario e chiuso, quindi se uno dei file di archivio si rovina il contenuto è perso. Punto.

Altri programmi mettono a disposizione sia strumenti per esportare l'archivio della posta in formati semplici da maneggiare, come file di testo o XML, oppure

1. http://www.nongnu.org/cvs/
2. http://subversion.tigris.org/

conservano i messaggi in un file la cui struttura è trasparente. Ad esempio Thunderbird e Mozilla usano un formato semplicissimo, con un file di testo per ogni cartella di posta, leggibile anche col solo Notepad. Outlook, al contrario, usa un formato chiuso con un solo file per tutto, che spesso quando raggiunge dimensioni oltre il gigabyte (credetemi, succede...) inizia a diventare ingestibile. Outlook Express usa un file per ogni cartella di posta, e soffre degli stessi problemi di Outlook. Il mio consiglio è di pensare sempre al peggio: se un giorno non avremo più la possibilità di installare una versione di programma compatibile con i file in cui abbiamo salvato la posta non potremo più leggerne il contenuto se è in un formato chiuso e proprietario. Meglio il testo semplice, e tenere pulito l'archivio della posta. Conosco qualcuno che conserva lo spam...

In definitiva, facciamo il backup, facciamolo spesso, e su un supporto che non sia dentro il computer che usiamo normalmente. Avere due dischi e copiare da un disco all'altro non è molto più sicuro che averli su un disco solo in due directory differenti. Un malware, un guasto, un problema di alimentazione elettrica, e i dati sono persi. Possiamo usare un disco esterno USB, un CD-RW, un altro computer (usando il notebook si possono salvare periodicamente i dati sul computer dell'ufficio o di casa). Posso assicurare che non è tempo perso.

Per la modalità, basta copiare i file dal disco del computer all'altro supporto, senza strane procedure o alchimie. Se il programma che utilizziamo non permette l'uso di semplici file che possono essere copiati e recuperati, allora è meglio cambiare programma. Se il nostro programma di posta non riconosce i suoi stessi file, rimessi al suo posto, è da buttare. Se chi produce il programma non ci fornisce un metodo per il backup, quale che sia, *non ha nessuna cura dei suoi clienti*, quindi non merita il nostro denaro, o il nostro sostegno.

Per quanto riguarda la periodicità dei backup, è molto semplice: se i dati non cambiano mai, basta una copia di riserva (in totale due copie, originale e riserva), ed è sufficiente controllarne lo stato di conservazione due volte l'anno (non sto esagerando: il filmino del mio matrimonio stava per andare perduto dopo appena un anno per la cattiva qualità dei supporti usati da chi aveva masterizzato il DVD: per fortuna ne avevo una copia fatta qualche mese dopo). Se i dati cambiano raramente, possiamo fare una copia a ogni modifica, e solo di quelli modificati. Se invece i dati cambiano spesso, possiamo scegliere di fare la copia con cadenza

settimanale, indipendentemente dalle effettive modifiche ai dati. O per esempio giornaliera se i cambiamenti non sono facilmente riproducibili. Per esempio chi sviluppa software sa bene che scovare un problema in un programma è una operazione difficile e impegnativa, e una volta trovato l'errore è bene mettere al sicuro le modifiche correttive, dato che replicare tutta la sequenza che ha portato alla scoperta dell'errore potrebbe essere impossibile.

Terminiamo qui, anche se ci sarebbe molto altro da dire. Dalla estensione con cui abbiamo trattato l'argomento dovrebbe essere evidente che questa particolare contromisura è forse la più importante e l'unica che ci mette veramente al riparo da qualsiasi disastro possa colpire il nostro computer: sottovalutarla è solo incoscienza.

La seconda linea di difesa: diritti e gerarchie

Il concetto di diritti dell'utente (inteso come account del computer, administrator o root per intenderci) è ben noto a chi usa sistemi operativi Unix/Linux.

In un sistema operativo che si rispetti, deve esistere una gerarchia di utenti in cui è ben delineato il compito di ognuno. Per cui esistono gli amministratori, in grado di fare qualsiasi cosa e di disporre di ogni singola funzione del computer e del sistema operativo; gli utenti normali, quelli che il computer lo usano e basta; gli ospiti, a cui vengono concesse risorse limitatissime. Senza questa distinzione e questa classificazione nel sistema operativo vige l'anarchia: tutti possono fare tutto e, a peggiorare le cose, tutti possono disporre a piacimento del contenuto del computer e delle funzioni del sistema operativo.

Ma il motivo principale per questa distinzione fra tipi di account utente è la sicurezza. Solo gli amministratori possono toccare le parti vitali del sistema operativo, perché si suppone che sappiano dove mettere le mani e cosa stiano facendo. Tutti gli altri utenti non devono poter pasticciare nel computer rischiando di metterlo in condizione di non funzionare più.

Se diamo uno sguardo al Pannello di Controllo, sotto la voce Account Utente, c'è un argomento della guida chiamato Tipi di account utente, che mostra i due tipi principali disponibili in XP: amministratore e limitato. L'account limitato

può fare molto poco, sembrerebbe. Ecco il principale equivoco, e la fonte della maggioranza dei fantomatici problemi di XP.

In GNU/Linux, gli account utente sono tutti di questo tipo, limitato, ed esiste un solo account amministratore, quello chiamato root. Posso assicurarvi che l'utente normale può lavorare tranquillamente, senza alcuna limitazione. Quello che l'utente non può fare è di cambiare qualsiasi cosa nel computer che possa anche solo lontanamente comprometterne il funzionamento regolare. Per esempio non può cambiare l'ora o la data, non può andare a vedere i file degli altri utenti, non può cancellare o installare un programma di uso comune, non può cambiare le impostazioni delle interfacce di rete e non può crearne di nuove. Per far questo c'è il *superuser*, root appunto.

La differenza è che la denominazione è riduttiva e psicologicamente fuorviante in XP: l'utente normale è amministratore, mentre l'altro è un poveretto che ha delle limitazioni. In Linux l'utente normale è appunto normale, *è l'altro che ha diritti in più*. Ma questo non ha nulla a che fare con le capacità e l'attività al computer degli utenti normali. L'amministratore è da paragonare ad un amministratore di condominio, che ha il compito di mantenere ordinato l'edificio, assicurarsi che tutti abbiano gli impianti comuni funzionanti (riscaldamento, ascensore, cancelli automatici, ecc.), ma non può in alcun modo mettere il naso negli appartamenti dei condòmini, né può decidere nulla dello spazio privato di ognuno. Allo stesso modo un utente con account aministrativo ha il compito di rendere il computer sicuro, funzionale ed efficiente per tutti gli altri utenti.

Questo non ha nulla a che vedere con le capacità dei singoli: in alcuni dei server che amministro per lavoro, operano colleghi che sviluppano in linguaggio C++ e Java, dei quali so poco o nulla. Nei miei computer uso abitualmente account normali, e impiego l'account amministrativo solo lo stretto necessario. E' soltanto una strategia collaudata per tenere in ordine il computer ed impedire agli utilizzatori di creare disagi a se stessi e agli altri. Tutto qui.

Cominciamo col rivalutare questo povero account limitato in XP. I compiti cosiddetti amministrativi in un qualsiasi sistema operativo dovrebbero essere molto ridotti. Una volta preparato il sistema, e installate le applicazioni richieste per l'uso che del computer se ne farà, l'account amministrativo si usa solo per poche operazioni: aggiornamenti del sistema operativo, aggiungere o togliere le appli-

cazioni, sistemare qualche parametro di funzionamento, aggiungere o cambiare collegamenti di rete. L'uso normale del computer, che si traduce in navigare, leggere la posta, lavorare sui propri filmati e sulle foto, scrivere documenti, giocare, ascoltare musica, ecc. è costituito di attività pienamente accessibili dall'account *limitato* di XP. Quindi la temuta limitazione non esiste. Inoltre, in molte applicazioni rilasciate negli ultimi tempi, al momento dell'installazione viene rilevata la natura dell'account, ed eseguita automaticamente una procedura specifica senza usare diritti amministrativi. Ovviamente l'applicazione così installata sarà utilizzabile solo da quell'account, cioè dall'utente che ha operato l'installazione.

Rimangono alcune applicazioni che non solo devono essere installate con un account amministrativo, cosa abbastanza normale se si vuole rendere accessibile il programma da tutti gli utenti del computer, ma anche per il funzionamento richiedono i diritti di amministratore. Questo dipende fortemente dal tipo di applicazione, e in ogni caso dal lavoro che ci si attende. Chi sviluppa software spesso usa applicazioni che necessitano dei diritti di amministratore. Stessa cosa per le utility diagnostiche o di recupero e riparazione, come pure le applicazioni dedicate per periferiche particolari. Se invece abbiamo una applicazione abbastanza banale che richiede i diritti amministrativi anche solo per tenere il registro delle fatture, o per modificare una foto, è il caso di valutare il passaggio a una differente, che tenga conto della struttura dei moderni sistemi operativi e permetta l'uso dei sistemi di sicurezza presenti.

Quali sono i vantaggi nell'uso di un account non amministratore? Pressoché infiniti. Per andare al sodo, tutti i programmi avviati con quell'account possono fare le stesse cose, e hanno le stesse limitazioni: un normale virus per funzionare ha bisogno di modificare file e configurazioni accessibili solo agli utenti amministratori: attivato con un utente normale non avrebbe accesso a questi file, né potrebbe modificare gran parte delle configurazioni, proprio come l'account da cui parte, del quale possiede gli stessi diritti. Rimane il problema dei *dialer* (un tipo di malware che aggiunge o cambia il collegamento via modem in Internet per usare un numero telefonico a tariffazione salatissima, spesso a totale insaputa di chi usa il computer, o comunque senza specificarlo chiaramente al momento dell'attivazione), alcuni dei quali purtroppo continuano a funzionare, ed a fare danni, anche usando un account normale, non amministrativo. Comunque, buona parte di essi non possono più funzionare, proprio perché non hanno più accesso

libero a qualsiasi parte del computer, e con qualche altra contromisura specifica, che vedremo più avanti, potremo rendere la vita difficile anche a quelli più furbi.

La protezione supplementare che viene da un account con assegnati i diritti strettamente necessari al lavoro che deve compiere può venir meno solo in presenza di falle gravissime nel software: esiste un meccanismo chiamato *privilege escalation*, che permette ad un programma avviato con un account utente normale di guadagnare in modo permanente i diritti di amministratore, e diventare quindi equivalente al *superuser*. Rimane il fatto che è un trucco difficilissimo da sfruttare e richiede una serie di circostanze favorevoli, la prima delle quali un software con errori gravi e di tipo assolutamente specifico.

Al netto di questa particolarissima situazione, l'uso di un account normale riduce sensibilmente il rischio anche in presenza di una eventuale infezione da parte di un virus, imponendogli lavorare solo con i diritti dell'account compromesso. Per esempio sia nel caso della vulnerabilità causata da un errore nella decodifica dei file di tipo WMF (Windows MetaFile), segnalazione del Bollettino Microsoft MS06-001[3], che nel caso di un errore analogo nella decodifica dei file Jpeg, segnalazione del Bollettino Microsoft MS04-028[4], immediatamente sfruttati da un ampio ventaglio di malware come porta di ingresso, uno dei fattori di riduzione del danno e del rischio in entrambi i casi era proprio l'uso di un account normale, non privilegiato.

Nel caso peggiore, in cui un malware comprometta irrimediabilmente l'accesso di un utente di questo tipo, la soluzione è abbastanza semplice: dall'account di amministrazione si salvano i dati importanti di quell'utente, si cancella completamente sia l'accesso che la directory dell'utente, e si ricrea pulito. Oppure, se il danno non è gravissimo, si può tentare di ripulire l'area di lavoro di quell'utente con uno scanner antivirus, eliminando il malware. Questo è possibile solo e soltanto se l'account di amministrazione è pulito, integro e non compromesso, altrimenti è una fatica inutile.

C'è anche un altro aspetto, assolutamente da non trascurare: servizi come antivirus e firewall, se correttamente progettati e utilizzati, lavorano usando i privilegi di amministrazione (in realtà su XP usano un livello di privilegio denominato

3. http://www.microsoft.com/technet/security/bulletin/ms06-001.mspx
4. http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx

SYSTEM, che accetta ordini solo da un amministratore, ma per quanto ci serve possiamo parlare di privilegi di amministratore senza troppi giri di parole). Questo implica che un malware che riesca a introdursi usando un account utente normale non avrà i permessi per terminare l'antivirus o il firewall, né per modificarne il comportamento. In questa situazione questi due programmi saranno invulnerabili al malware, che sarà molto più facilmente individuato e reso inoffensivo.

Chiarito che questo tipo di account non solo non è limitato, ma ci assicura una notevolissima dose di sicurezza per il nostro computer, ora passiamo ai fatti. Abbiamo molte possibili strategie, ma in fondo abbiamo due casi: un computer con un solo account, di tipo amministrativo, con cui abbiamo già lavorato e ci siamo già sistemati secondo i nostri gusti, oppure un computer vergine, appena installato. In questo ultimo caso le cose sono più semplici: si crea un secondo account di tipo limitato, il primo lo abbiamo già creato al momento dell'installazione di XP, ed è un amministratore. Da questo momento in poi useremo solo l'account normale (limitato per XP), e cambieremo solo quando dovremo fare un lavoro da amministratore.

Per questo ci viene in aiuto in XP la possibilità di saltare da un account all'altro, usando la sequenza Start, Disconnetti, Cambia utente (o più rapidamente con la combinazione di tasti **WindowsLogo+L**). Senza chiudere niente del nostro lavoro potremo tranquillamente installare una applicazione appena scaricata, o aggiornare il sistema operativo, o cambiare l'ora senza problemi e senza perdere troppo tempo. Appena terminato torneremo all'account normale per continuare il lavoro.

Nel caso in cui abbiamo il sistema operativo installato e già usato e vogliamo passare ad un account normale possiamo, a scelta, crearne uno normale e usarlo al posto dell'account che abbiamo già (che rimane amministrativo), oppure creare un altro account amministrativo e "declassare" il proprio a normale.

La prima soluzione va bene se abbiamo troppi dati e personalizzazioni da trasferire da un account all'altro e dobbiamo per forza di cose lavorare con applicazioni che richiedano diritti amministrativi: l'account appena creato lo useremo soltanto per navigare in Internet o per i compiti più esposti al rischio, come leggere la posta o usare un programma di file sharing *peer to peer*; la seconda soluzione va bene se vogliamo mantenere dati e impostazioni senza soffrire troppo. Ovviamente la

soluzione migliore sarebbe partire da subito con la configurazione a due account (amministrativo e normale), ma non sempre è possibile.

Il mio consiglio è di partire con una situazione pulita, una installazione fresca di XP su cui abbiamo configurato le applicazioni che usiamo regolarmente, con i due account. Saremo anche più sicuri che le impostazioni elencate nel seguito siano fatte correttamente, e soprattutto saremo sicuri di non avere già un ospite sgradito annidato da qualche parte.

Tutte queste operazioni si fanno dal Pannello di Controllo, alla voce Account utente. Per declassare il proprio account si seleziona la voce Cambia tipo di account e si sceglie Limitato. Le impostazioni valgono solo dopo il termine della sessione, o dopo un riavvio: l'utente mantiene i privilegi finché è collegato, e li perde alla prima uscita.

Per sicurezza, XP non fa declassare l'utente amministratore se è l'unico esistente con quei diritti. Per poterlo declassare occorre creare un altro account amministratore, e solo allora possiamo far diventare *normale* il nostro account utente.

La seconda linea di difesa bis: password

Non potevamo non affrontare questo argomento. Il motivo è molto semplice: anche in computer blindati sotto tutti i punti di vista e con tutte le sicurezze possibili, il punto debole può essere una password di accesso banale, o peggio non averla prorio.

Se il nostro account amministrativo non è adeguatamente protetto, e parimenti non lo sono tutti gli altri account del computer, tutte le precauzioni prese sono inutili. Basti tenere presente un dettaglio non da poco: alcuni tipi di malware, quando non riescono a fare altro perché il computer è correttamente chiuso ad accessi indesiderati, tentano un semplice *attacco a dizionario* sulle password. Cosa sia un attacco a dizionario è presto detto: tentare tutte le password prese da un elenco, il dizionario appunto, fino a trovare quella giusta. Un esempio del contenuto di un dizionario di questo tipo, si può trovare nell'analisi di alcuni malware reali, come Gaobot.AA, di cui possiamo vedere l'analisi dettagliata sul sito Symantec[5],

5. http://www.symantec.com/avcenter/venc/data/w32.hllw.gaobot.aa.html

e Gaobot.gen, la cui analisi completa è disponibile sempre sul sito Symantec[6].

Occorre chiudere anche questa porta, e tenerla chiusa. Le regole di base sono molto semplici: niente che sia prevedibile a priori, e niente che possa indovinare chi ci conosce. Di conseguenza: niente nomi di persone care né di personaggi noti o preferiti; niente parole di senso compiuto, anche se in altre lingue; niente numeri di telefono o di altro tipo. La lunghezza deve essere adeguata, almeno sei-sette caratteri misti (lettere, numeri e simboli).

Possono andare bene parole con errori intenzionali di ortografia, frasi senza senso, combinazioni di sillabe facili da ricordare ma prive di senso. Ad esempio "tore-tazi", con il trattino di separazione, è una buona password: lunga nove caratteri, contiene simboli, non ha senso compiuto ed è abbastanza facile da ricordare. Altra possibilità, se ad esempio ne abbiamo molte da tenere a mente, è di stabilire un metodo di generazione, da tenere segreto: "password@nomecomputer" è un buon esempio. La regola in questo caso è piuttosto semplice: la prima parte è uguale per tutti i computer in cui viene usata, e la seconda è data dal nome del computer, separato con il simbolo della chiocciola (mi raccomando, adesso non usate tutti questo esempio come oro colato...).

Eviteremo quelle che sembrano ottime idee, perché, poco ma sicuro, qualcun altro ci avrà pensato prima: password uguale all'account utente (non potete immaginare quanti account "pippo" con password "pippo" ho visto...), oppure con la sostituzione da "hacker da strapazzo" (la lettera "i" o la "l" sostituita con il numero "1", la lettera "e" sostituita con il numero "3", il numero "4" che sostituisce la lettera "a", in questo modo: "m4r10" invece di "mario"). Questo perché chi tenta di forzare una password, dopo l'attacco a dizionario andato a vuoto, passa quasi subito a tentare con questo tipo di sostituzione. Allo stesso modo occorre evitare altri tipi di sostituzioni banali, derivate sempre da una parola di senso compiuto. Se proprio vogliamo usare una sostituzione, facciamolo a partire da una parola senza senso. Invece di "tore-tazi" possiamo usare "t0r3-taz1", che in definitiva è ancora più robusta della precedente, non per via della sola sostituzione, ma *perché viene da una parola senza senso*, e la sostituzione non è stata sistematica, cioè non ho cambiato *tutte* le lettere che è possibile cambiare in numeri.

6. http://www.symantec.com/avcenter/venc/data/w32.gaobot.gen!poly.html

Il perché l'attacco a dizionario è così efficace si dimosta molto semplicemente con pochi calcoli: prendiamo una password di soli sei caratteri: "dev4-z". Anche supponendo di sapere in anticipo che è lunga solo sei caratteri, per trovarla siamo costretti ad un attacco di tipo *brute force*: tentare con tutte le combinazioni possibili di lettere, numeri e simboli lunghe sei caratteri. Considerando le sole lettere minuscole dell'alfabeto inglese (quindi niente accentate, né altri segni linguistici particolari), i dieci numeri ed i simboli principali, che limiteremo ad una decina per comodità di calcolo, sono in totale 26+10+10, 46 simboli differenti. Combinati in gruppi di sei con la possibilità di ripeterli generano in totale 46 elevato sei combinazioni, 9.474.296.896 password differenti, poco meno di nove miliardi e mezzo.

Il dizionario di una lingua complessa come l'italiano contiene molto meno di un milione di termini, anche includendo tutte le coniugazioni dei verbi, le forme plurali, riflessive, i termini tecnici, i nomi propri di persona, storici, geografici e mitologici. Curiosando sui siti di note case editrici specializzate in dizionari, per le edizioni aggiornate del 2006 si trovano questi numeri: 250.000 termini per la lingua italiana (comprendenti 7.500 coniugazioni di verbi irregolari), 107.000 termini tecnico-scientifici in inglese ed in italiano, 52.500 toponimi (nomi geografici), 5.000 nomi storici. In totale, abbiamo 414.500 termini differenti. Arrotondiamo a mezzo milione aggiungendo i nomi propri di persona e un campione di cognomi italiani, e non teniamo conto che buona parte dei 107.000 termini tecnici sono già compresi nei 250.000 termini della lingua italiana. Stiamo esagerando, ma teniamo un milione come cifra tonda. E' importante notare che il vocabolario di una persona di cultura medio-elevata è di meno di 15.000 parole differenti, compresi i termini tecnici che usa nel lavoro, ma non ne terremo conto.

Arriviamo al nostro attacco per forzare la password: supponendo di avere un programma in grado di fare mille tentativi al secondo, se usiamo una fra i nove miliardi di combinazioni di sei caratteri ci vogliono in media quasi cinque milioni di secondi (oltre cinquantaquattro giorni di attacco continuo). Se invece prendiamo una qualsiasi del milione di parole di senso compiuto, senza tenere conto della lunghezza, il tempo di attacco diventa in media di *otto minuti*, che diventano sedici se abbiamo applicato la trovata della sostituzione "hacker da strapazzo", lettere con numeri.

Chi non è ancora convinto, pensi alla lista di password trovata dentro il codice del virus Gaobot, citata poco sopra. Non stiamo parlando di fantascienza, o di complotti oscuri: qui le prove ci sono, documentate e chiarissime.

Seconda linea di difesa ter: filesystem e permessi

Il filesystem, detto in parole povere, è il modo in cui i dati vengono organizzati e memorizzati sul disco. Quello usato da XP è chiamato *NTFS*, e, fra le altre caratteristiche, consente una gestione corretta di quelli che vengono chiamati *permessi*: ogni file e directory sul disco ha dei dati aggiuntivi che indicano a chi appartiene, cosa può fare il proprietario, cosa possono fare gli altri utenti. Ad esempio, se sul computer abbiamo tre account utente, uno amministratore e due normali, i due utenti normali potranno accedere liberamente al proprio spazio sul disco (la *home directory*), posizionato in `C:\Documents and Settings\nomeutente`, in cui possono creare file, directory, cancellare a piacere, spostare, rinominare, ecc., ma non possono neanche entrare nello spazio dell'altro utente, o in quello dell'amministratore. Allo stesso modo possono entrate nella directory di XP, leggere file ed eseguire programmi, ma non possono modificare nulla, tantomeno creare altri file.

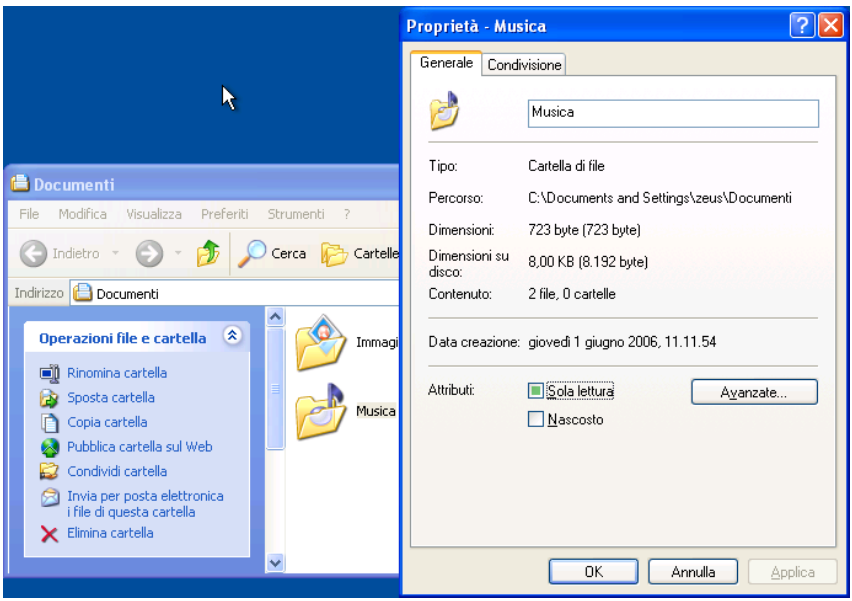
Questa altro non è che una forma di protezione, efficacissima se applicata correttamente, che permette ad ogni utente di fare quello che deve, senza far danni e senza disturbare gli altri.

E' questo il motivo per cui se un utente normale rimane vittima di un malware, che viene eseguito con i diritti di quell'utente, non può danneggiare parti vitali del sistema operativo, né lo spazio degli altri: il malware non ha i *permessi* per entrare o modificare quei file e quelle directory, quindi non può installarsi nei punti vitali, come la directory di Windows o la directory `system32` in cui sono tutti i pezzi più importanti del sistema operativo.

Tutto questo vale solo se il disco in cui risiede XP è con filesystem NTFS. Anche qui, pensando all'utente medio, la gestione dei permessi è semplificata ed è usata con una modalità chiamata *condivisione semplice*, che nasconde le impostazioni che XP applica ai file e alle directory. Se apriamo la cartella Musica dentro la directory `Documenti`, e ne chiediamo le proprietà, il pannello avrà in tutto due

pagine, Generale e Condivisione (Figura 4-1), e la prima mostra i permessi più comuni, come ad esempio quello di *Sola lettura*.

Figura 4-1. Le proprietà di base



Da un account amministratore, andiamo nel Pannello di Controllo, selezioniamo Aspetto e temi, ed apriamo Opzioni cartella. Nel pannello che appare prendiamo la pagina Visualizzazione (Figura 4-2), fra le voci ce n'è una denominata Utilizza condivisione file semplice (scelta consigliata). Ebbene, ignoriamo il consiglio e disabilitiamo questa opzione. Se chiediamo di nuovo le proprietà della directory Musica, appare una nuova pagina (Figura 4-3), Protezione.

Figura 4-2. Attivare la gestione dei permessi

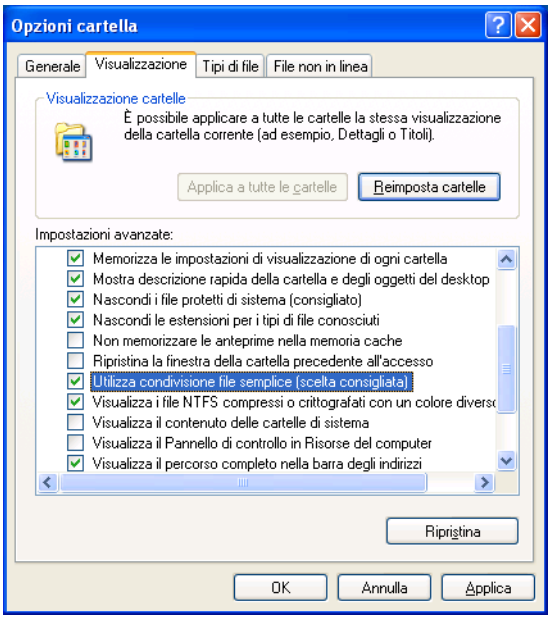
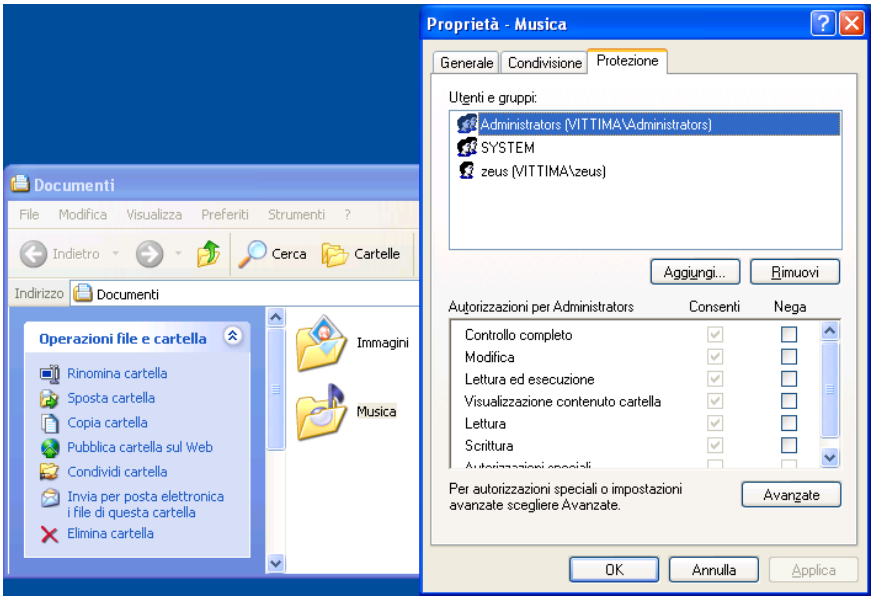


Figura 4-3. Chi può fare cosa



Questa pagina mostra, per ogni utente o gruppo di utenti, quali operazioni sono consentite. Gli utenti sono indicati con l'icona rappresentante un solo personaggio, i gruppi di utenti sono indicati con l'icona a due personaggi affiancati. Un gruppo di utenti è un modo rapido di assegnare diritti senza specificare ogni volta tutti i dettagli: ad esempio tutti gli utenti normali sono automaticamente assegnati al gruppo Users, mentre gli utenti amministratori sono assegnati al gruppo Administrators. Se al momento della creazione di un account utente viene assegnato un gruppo, automaticamente tutti i diritti definiti per quel gruppo sono assegnati all'utente creato. Vedremo fra poco le differenze fra questi due gruppi.

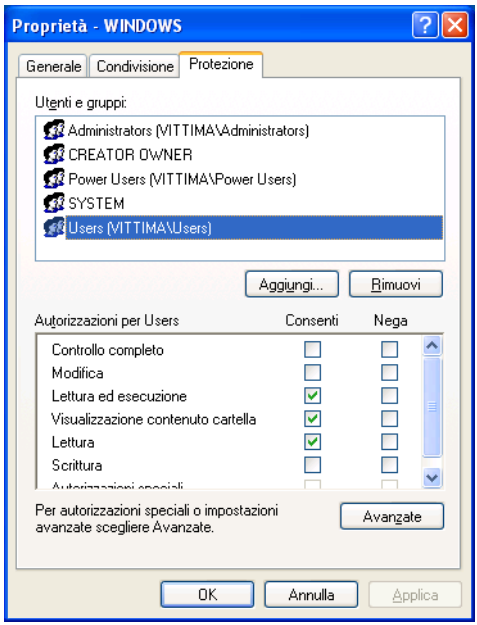
Permessi e mal di testa

La gestione dei permessi su file e directory in Windows è una vera giungla. Il significato dei permessi cambia in funzione dell'oggetto a cui sono applicati, e non sempre il risultato ottenuto è a prova di logica. Inoltre i permessi sono propagati a file e directory con un meccanismo di "ereditarietà": se una directory ha permessi di esecuzione e modifica per un determinato utente, allora tutti i file e le directory in essa, se non diversamente specificato, avranno gli stessi permessi.

Per questo motivo, a chi è interessato ad approfondire l'argomento consigliamo di rivolgersi alle innumerevoli guide in circolazione che spiegano nel dettaglio ed estensivamente il significato e l'applicazione di ognuno. Per quanto ci interessa qui ci limiteremo al minimo indispensabile.

Per la directory che abbiamo scelto, quella dei brani musicali dell'utente zeus, che è un amministratore, sono assegnati permessi pieni all'utente stesso, al gruppo degli amministratori, ed al gruppo speciale SYSTEM. Questo significa che tutti gli altri utenti non possono fare nulla, neanche vederne il contenuto. Se andiamo nella cartella di Windows, e andiamo a vederne le proprietà (Figura 4-4), scopriamo qualcosa in più: i gruppi Power Users e Users. Anche qui il gruppo di utenti amministratori ha tutti i permessi, mentre il gruppo dei Power Users non ha il Controllo completo, che consente operazioni particolari come assegnare particolari permessi o cambiare il proprietario del file o della directory, operazione riservata solo agli amministratori. Il gruppo Users, che è quello a cui vengono assegnati gli utenti normali creati dal Pannello di Controllo, ha solo i permessi di lettura (possono aprire e leggere il contenuto di un file, quindi anche copiarne il contenuto in una directory in cui possono scrivere), esecuzione (avviare un programma che risiede in questa directory) e visualizzazione (vedere la lista dei file e delle directory).

Figura 4-4. Utenti normali e directory di Windows



Ecco dove la corretta gestione dei diritti e dei permessi degli utenti diventa un potente strumento di difesa: un malware che colpisca un utente con account normale non potrà toccare nessuno dei file o delle cartelle dove sono posizionate le parti più delicate del sistema operativo. Il malware potrà addirittura svuotare completamente lo spazio di quell'utente, ma non potrà né toccare lo spazio degli altri utenti, né andare a modificare qualsiasi cosa nel sistema operativo.

Dal lato opposto, se invece è un utente amministratore ad essere colpito, nel momento stesso in cui il malware si attiva può modificare a piacimento qualsiasi cosa, anche nei punti più vitali del sistema operativo, perché avrà permessi pieni su tutto: in questo caso non c'è più alcuna difesa.

Anche la directory `Programmi` è protetta allo stesso modo, impedendo agli uten-

ti normali qualsiasi modifica alle applicazioni installate per tutti gli utenti, impedendo così ad un malware di utilizzare un programma comune per trasmettersi da un account all'altro.

Vedremo come questa gestione sofisticata dei permessi ci tornerà utile più avanti per impedire ad alcune categorie di malware di fare danni.

La terza linea di difesa: cosa mi nascondi?

Sempre avendo in mente l'utente medio, XP ha una serie di comportamenti dettati dalla necessità di non confondere e di semplificarne l'uso. E come sempre questi comportamenti sono qualche volta fonte di pericolo. Vediamone due in particolare: non sono mostrati i file considerati necessari per il buon funzionamento del sistema operativo; viene nascosta l'estensione dei nomi di file (i caratteri nel nome dopo il punto che identificano in un certo senso il contenuto del file stesso) quando è utilizzata da un programma installato nel computer. Ad esempio un file di testo, il cui nome sia `documento.txt` viene visualizzato con l'icona rappresentante un foglietto scritto, con nome `documento` senza il `.txt` finale. La ragione è che se andiamo a modificarne l'estensione, da `.txt` a `.xyz`, il file non si aprirà più, anche se il contenuto non è cambiato. Per questo motivo viene nascosta l'estensione nei file quando è installato il relativo programma di lettura, modifica e creazione.

Per i malware invece è una opportunità da cogliere: nel caso di applicazioni, i file con estensione `.exe`, l'icona mostrata da XP è presa dall'interno del file del programma stesso, memorizzata in un apposito spazio. Se ad esempio mettiamo in una applicazione la stessa icona di un documento di testo, quando viene visualizzata sul desktop o all'interno di una directory avrà lo stesso aspetto di un qualsiasi altro documento di testo. Nel momento in cui andiamo ad aprire l'applicazione con l'icona del documento, invece di aprirsi il **Notepad** con dentro il testo, *attiviamo l'applicazione camuffata*. E' un trucco molto usato in malware che si propagano come allegati di posta elettronica e da altri che vengono offerti come documenti da scaricare e da leggere, all'apparenza innocui, ma che celano una applicazione deleteria. Non vedendo l'estensione `.exe` del file, ed ingannati dall'icona del documento di testo, andiamo a cliccare per aprire e succede il

finimondo.

Se invece possiamo vedere il nome completo del file sotto l'icona c'è una buona probabilità che ci accorgiamo di qualcosa di sospetto, evitando così l'attivazione di un malware.

Altri malware riescono a nascondersi assegnandosi lo status di *file di sistema*, cioè file importanti per il funzionamento, che come abbiamo già detto sono nascosti. Anche qui non è detto che sia una buona scelta nascondere cose agli utenti, pur se fatto con le migliori intenzioni.

Riportiamo le cose al giusto posto, obbligando XP a non nasconderci nulla: dal Pannello di Controllo prendiamo la voce Aspetto e temi ed apriamo Opzioni cartella. Nel pannello che appare, visto poco fa, prendiamo la pagina Visualizzazione (Figura 4-2) e facciamo queste modifiche:

- Selezionare Visualizza cartelle e file nascosti - Per impedire ai malware di nascondersi in modo banale. Le directory ed i file che hanno impostato questa modalità saranno mostrate leggermente sbiadite rispetto alle altre.
- Togliere Nascondi i file protetti di sistema (consigliato) - Pur obbligando la visualizzazione dei file nascosti, i file definiti di sistema sono comunque nascosti. Per impedire ai malware di celarsi dietro questo trucco, togliamo questa opzione. XP ci avverte con un messaggio che è rischioso e che si può danneggiare il sistema, chiedendo conferma. Dato che useremo utenti non privilegiati per l'uso normale, e che le parti vitali del sistema operativo sono già protette dai permessi visti prima, è praticamente inutile nascondere i file e le directory. Anche qui le rispettive icone saranno rappresentate come sbiadite.
- Togliere Nascondi le estensioni per i tipi di file conosciuti - Lo abbiamo visto prima, è meglio sapere cosa si sta cliccando controllando il nome, e non fidarsi della sola icona. Ora i file saranno visualizzati col loro nome intero.
- Togliere Utilizza condivisione file semplice (scelta consigliata) - Per accedere alla gestione piena dei permessi, vista poco prima.
- Selezionare Visualizza il contenuto delle cartelle di sistema - Mostra immediatamente il contenuto delle directory `windows`, `Programmi` ed altre, senza mostrare la pagina di avviso col link per vederne ugualmente il conte-

nuto. E' anche questa una impostazione inutile, dato che invece di nascondere preferiamo assegnare diritti corretti agli utenti. Mentre invece è fondamentale accorgersi di cose strane se un malware ha messo i piedi nel nostro computer.

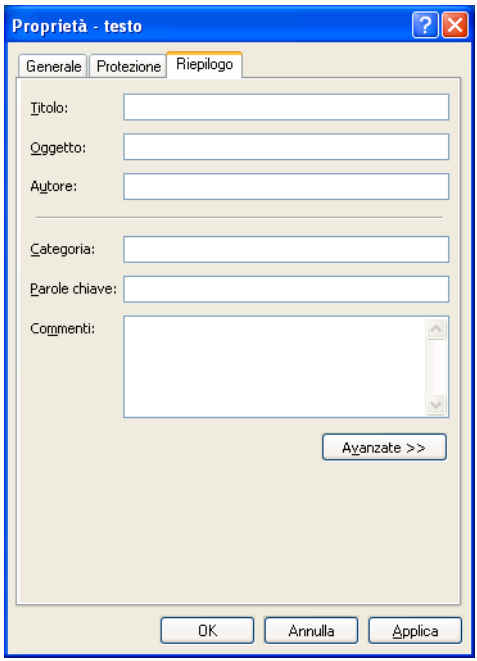
- Selezionare Visualizza il percorso completo sulla barra del titolo - Di solito XP mostra solo il nome della directory in cui siamo in quel momento nel titolo della finestra. Non è una impostazione critica, ma per capire dove siamo ed evitare di essere ingannati, è meglio sapere esattamente in quale punto di troviamo, dato che possono esistere directory con lo stesso nome in punti diversi del disco, o in dischi differenti.

Accettiamo le modifiche ed andiamo a vedere ad esempio il contenuto della directory `Documents and Settings`, ora mostrerà tre altre directory con l'icona sbiadita: `Default User`, `LocalService` e `Networkservice`. Molti altri file e directory compariranno se andiamo nella directory di Windows ed in altre che apparivano vuote. Niente paura, è proprio quello che volevamo: ora ci sono molti posti in meno per nascondersi, e molte meno opportunità di ingannarci.

Incorreggibile...

Rimane un problema, purtroppo al momento insormontabile. Usando un filesystem di tipo NTFS, è possibile assegnare delle proprietà aggiuntive ad un file, richiamandone le proprietà "normali" ed usando il pannello Riepilogo (Figura 4-5). Le informazioni che scriviamo in queste caselle vengono certamente salvate, ma non se ne trova traccia nel computer: niente file nascosti, niente chiavi di registro, niente di niente, eppure i dati sono lì. Ebbene, NTFS permette di creare i cosiddetti ADS, *Alternate Data Streams*, i quali altro non sono che file associati ad altri file, senza "dignità" di file indipendenti. In questi file vengono memorizzati anche altri dati, come ad esempio l'avviso associato ad ogni file scaricato da Internet e "bloccato" da XP, il quale deriva da un ADS generato dal sistema operativo il cui contenuto indica l'origine del file stesso.

Figura 4-5. Un uso degli Alternate Data Streams



Queste funzioni sono estensivamente utilizzate da XP e non sono disabilitabili in alcun modo, a meno di utilizzare un altro tipo di filesystem, perdendo però i vantaggi della gestione dei permessi vista poco fa (Sezione *Seconda linea di difesa ter: filesystem e permessi*), ma la cosa più fastidiosa è che non vi è un programma che permetta di vedere quali file hanno un ADS associato, né vederne il contenuto, a parte quello visibile dal pannello appena mostrato, limitato a questo specfico tipo di ADS.

Quanto detto non sembra un gran problema, ma c'è un dettaglio da non trascurare: il contenuto degli ADS può essere qualsiasi cosa e anche le directory possono averne uno associato. Ne discende che si possono "nascondere" programmi in

un ADS di una directory di XP, ad esempio `system32`, e che non potremo mai sapere che sono nascosti in quel punto. E' il nascondiglio perfetto per i malware: ci si può mettere qualsiasi cosa, non è visibile con niente del sistema operativo e non possiamo eliminarlo senza eliminare il file a cui è associato (non senza usare programmi appositi che *non sono compresi fra quelli forniti con XP*).

Non è difficile immaginare come i creatori di malware ci si siano tuffati, ottenendo un vantaggio consistente su molti programmi che servono a scovarli: molti antivirus e antispyware non controllano il contenuto degli ADS. Se lo fanno, spesso non riescono ad operare e segnalano la presenza di virus in file che non sembrano esistere, o peggio in file che non possono toccare senza compromettere il funzionamento di XP.

Unica salvezza è che la creazione di un ADS associato ad un file è sottoposta alle stesse restrizioni di sicurezza che ha il file principale, come per ogni altro file: un malware che tenti di inserirsi come ADS in un file su cui l'utente non ha i permessi di scrittura fallirà nell'intento. Perciò l'uso di utenti con diritti "giusti" mette al riparo da trucchi di questo tipo, salvaguardando almeno l'integrità dei file di sistema. Ovviamente se il malware si "accontenta" dei diritti di un account utente normale e non di un amministratore (e vedremo che ve ne sono parecchi), potrà comunque trarre vantaggio dal nascondersi in un ADS di un file dell'utente colpito, ma in questo caso non potrà sottrarsi all'antivirus o allo scanner antispyware eseguiti come amministratore, sempre che siano in grado di esaminare e manipolare gli ADS.

Non esiste altra protezione, non con gli strumenti messi a disposizione di XP. Ma dobbiamo tener presente che se un malware riesce a nascondersi in un ADS, vuol dire che è potuto entrare indisturbato, quindi il problema è a monte: impedire al malware di entrare e attivarsi, che è lo scopo che ci siamo prefissi.

Capitolo 5. Vietato l'accesso

Come abbiamo visto in precedenza (Capitolo 2), XP nella sua configurazione predefinita ha un certo numero di servizi attivi, gran parte dei quali all'utente casalingo o al piccolo ufficio risultano del tutto inutili. Per i malware sono invece una manna, rappresentando una opportunità per introdursi nei computer anche senza alcun intervento da parte nostra.

La quarta linea di difesa: porte murate

Pensando al tipico disegno architettonico di un castello medievale, quello che appare evidente è che il punto di accesso è uno solo, ed è sorvegliato da guardie armate. Tutti gli altri possibili accessi sono chiusi, murati, o al più protetti da una robusta grata di ferro, come ad esempio gli scarichi delle fogne. Meno punti di accesso ci sono, più è facile tenerli sotto controllo e impedire visite indesiderate.

Andiamo a fare un esperimento: con XP appena avviato, senza aprire alcuna applicazione, andiamo in Start, Esegui... e nella casella digitiamo **cmd**, per poi premere Ok. Compare il Prompt dei comandi, che ci tornerà utile anche nel seguito. Digitiamo il comando:

```
C:\Documents and Settings\utente> netstat -an

Connessioni attive

  Proto  Indirizzo locale       Indirizzo esterno       Stato
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    192.168.42.152:139     0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    192.168.42.152:123     *:*
  UDP    192.168.42.152:137     *:*
  UDP    192.168.42.152:138     *:*
  UDP    192.168.42.152:1900    *:*
```

Sono molte informazioni, vediamo come si leggono e cosa significano. Detto in modo molto semplice, il comando serve a mostrare quali servizi di rete sono attivi e accessibili. Ve ne sono di due tipi principali, un gruppo su protocollo TCP ed un gruppo su protocollo UDP, ed ognuno ha assegnato un punto di accesso, detto *porta*, indicato dal numero dopo i due punti. E' un semplice sistema per indirizzare ad ogni servizio i dati che arrivano dalla rete in modo rapido. La prima colonna indica appunto il protocollo scelto. La seconda indica su quale interfaccia di rete è raggiungibile, ed a quale porta: l'indirizzo 0.0.0.0 è un modo per dire *tutte le interfacce*, mentre l'indirizzo 127.0.0.1 appartiene ad una interfaccia virtuale, chiamata *loopback*, che non è raggiungibile dall'esterno, ed è in un certo senso isolata dal mondo: è raggiungibile solo dallo stesso computer, e possiamo immaginarla come una porta i cui lati sono entrambi all'interno del castello. L'indirizzo 192.168.42.152 è quello assegnato alla scheda di rete ethernet installata sul computer.

La terza colonna contiene indicazioni significative solo per i servizi che usano il protocollo TCP, che funziona stabilendo delle connessioni: se ad esempio apriamo il browser ed andiamo su un sito qualsiasi, in questa colonna apparirà l'indirizzo del sito remoto con la relativa porta, di solito la 80, che è standard per i siti web. Allo stesso modo se qualche computer è connesso al nostro tramite uno dei servizi attivi lo troveremo elencato in questa colonna. L'ultima colonna è riportata solo per i servizi che usano il protocollo TCP e rappresenta lo stato della connessione: la parola *LISTENING* indica che il servizio è attivo e in attesa di connessioni. Potremmo trovare anche altre indicazioni, la più interessante delle quali è *ESTABLISHED*, che indica la presenza di una connessione fra il nostro computer ed un altro, ma niente qui ci aiuta a capire se siamo noi ad essere connessi con un altro computer o è qualcun altro ad essere connesso al nostro. Nel protocollo TCP esiste una netta distinzione fra chi chiede la connessione e chi la riceve, ma il comando **netstat** non ci fornisce direttamente questa particolare indicazione. Esiste una regola empirica per dedurre la direzione della connessione, cioè chi chiede e chi riceve: se abbiamo un servizio in *LISTENING* ed esiste una connessione *ESTABLISHED* che ha dal lato del nostro computer la porta TCP del servizio e dal lato dell'altro computer una porta con numero superiore a 1024 vuol dire che un computer è connesso al nostro, che ha ricevuto ed accettato la richiesta di connessione. E' questo il primo passo con cui i malware che si propagano via rete, e

quindi via Internet, riescono ad infilarsi nel nostro computer.

Se apriamo Internet Explorer e andiamo su un sito web, siamo noi a chiedere e il server su cui è ospitato il sito riceve la nostra richiesta. Invece nel caso di un tentativo di accesso da parte di un malware, il nostro computer riceve ed accetta la richiesta di connessione su uno dei servizi mostrati in *LISTENING*. Con tutte le applicazioni chiuse e senza alcuna attività da parte nostra non dovrebbero mai comparire righe con l'indicazione *ESTABLISHED*. Ovviamente, ci sono delle situazioni in cui è perfettamente normale avere connessioni attive, ad esempio quando Windows Update controlla sui siti Microsoft la presenza di aggiornamenti del sistema operativo, o se abbiamo altri computer con cui condividiamo disco e stampante. Quindi, niente panico se vediamo delle righe con *ESTABLISHED*, ma teniamo presente queste indicazioni, ci possono tornare utili per capire se qualcosa si nasconde nel nostro computer.

Arriviamo a quello che ci interessa: la procedura di sicurezza standard è di analizzare lo stato dei servizi, fermare e disabilitare quelli che non servono, o nel caso in cui siano utilizzati per funzioni importanti all'interno del sistema operativo o non si possano disattivare, togliere le funzioni di accesso via rete o, se non è possibile, spostare il servizio sull'interfaccia virtuale (ricordiamo, quella con indirizzo 127.0.0.1). Qui ci imbattiamo nel primo vero ostacolo: alcuni servizi non possono essere fermati, perché ampiamente utilizzati per il funzionamento interno del sistema operativo, e la configurazione standard prevede che siano in ascolto anche su tutte le interfacce di rete presenti nel computer, quindi esposte al mondo. Inoltre cambiare la configurazione è spesso cervellotico, mancando una certa uniformità nella gestione delle caratteristiche generali dei servizi interni. Un esempio lo vedremo nel prossimo paragrafo.

Siamo giunti al momento dell'analisi di sicurezza: i servizi attivi sull'indirizzo 127.0.0.1 li possiamo ignorare, non sono raggiungibili dall'esterno e quindi non sono punti di accesso utilizzabili. Però *tutti gli altri* rappresentano una porta incustodita. Andiamo a vedere a cosa servono e se siano necessari.

Porta 135/TCP e 135/UDP

Il servizio in ascolto su questa porta è usato principalmente per la gestione remota

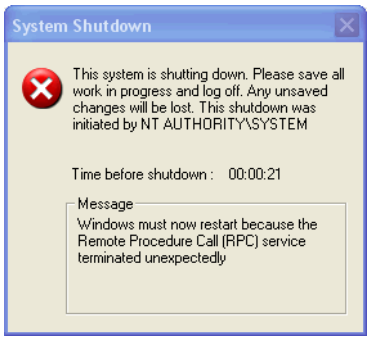
del computer, pensando ad una rete aziendale dove il responsabile informatico interviene dal proprio computer usando i programmi appositi forniti per questo scopo.

Occorre un minimo di spiegazione tecnica, che limiteremo al massimo per mantenere la comprensibilità. In Windows è attivo, fra gli altri, un servizio di esecuzione ad orario di programmi, fornito dal sistema operativo. Per accedere a questo servizio da un programma abbiamo varie possibilità: se il programma è in funzione nello stesso computer, possiamo chiedere al sistema operativo di attivare per noi il servizio usandone il nome (a titolo di informazione si chiama atsvc), senza sapere quale programma chiamare. Questo metodo è detto RPC (per *Remote Procedure Call*, chiamata a distanza di procedura), ed è usato per esempio per far funzionare anche il *drag&drop*, o la barra delle applicazioni (*taskbar*). Il metodo è utilizzabile anche da un programma in esecuzione su un diverso computer, mediante la comunicazione via rete: il programma si connette all'altro computer, chiede di accedere al servizio usando il nome, e riceve tutte le informazioni che servono. Di questo si occupa appunto il servizio sulla porta 135/TCP, che attiva se necessario il servizio e comunica dove sia raggiungibile. Altro metodo per attivare servizi particolari è denominato COM (per *Component-Object Model*, tradotto grossolanamente modello ad oggetti componenti), che permette di usare parti di sistema operativo senza conoscere i dettagli completi del funzionamento, di cui esiste la versione accessibile via rete, denominata DCOM (per *Distributed COM*, COM distribuito), accessibile sempre tramite la porta 135/TCP.

In una grande azienda dove i computer sono tanti, questo sistema permette di far gestire tutte le operazioni di configurazione e manutenzione, via rete, da una persona unica, che lavora senza muoversi dalla sua stanza. Ma per un computer usato a scopo privato e personale non ha alcuna utilità. Anzi, per via di un noto errore all'interno dei servizi RPC/DCOM, segnalato nel Bollettino Microsoft MS03-026[1] è divenuta la porta di ingresso del famigerato worm MSBlast o Blaster, la cui analisi dettagliata disponibile sul sito Symantec[2] e che ha fatto notevoli danni in giro per la Rete. Il sintomo principale >dell'infezione è la comparsa di un messaggio da parte proprio del servizio RPC che avverte del prossimo riavvio del computer per un grave errore (Figura 5-1).

1. http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx
2. http://www.symantec.com/avcenter/venc/data/w32.blaster.worm.html

Figura 5-1. Il primo effetto del virus Blaster

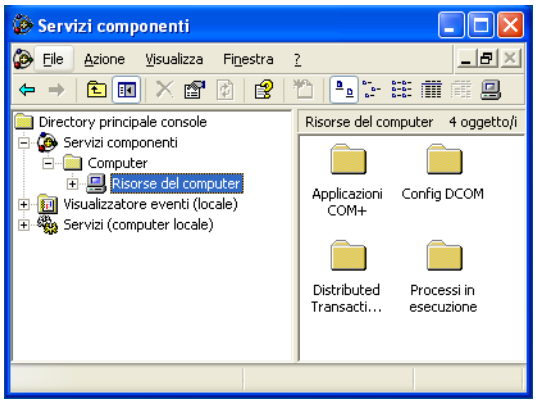


La situazione si è aggravata quando si sono scoperti altri errori altrettanto critici in servizi accessibili sempre dalla stessa porta 135. Per fortuna l'uscita del *Service Pack 2*, un aggiornamento massiccio di gran parte del sistema operativo, ha corretto tutte le falle conosciute relative ai servizi accessibili da questa porta TCP. Ma niente e nessuno può assicurare che non ci siano altre falle in agguato: per essere ragionevolmente tranquilli occorre chiudere ogni accesso a questa porta. Possiamo usare un firewall, anche quello interno di XP va bene.

Se però il computer è per uso personale e non fa parte della rete di una azienda che usa la gestione centralizzata, è infinitamente più sicuro rendere inaccessibili dalla rete i servizi che funzionano mediante RPC.

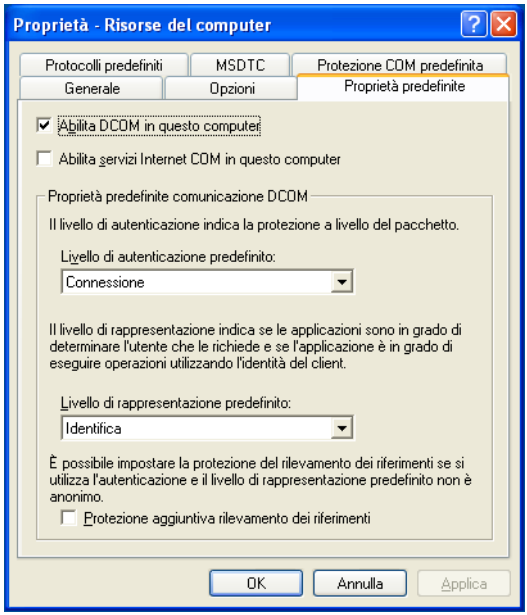
Il problema è che la porta 135/TCP è un punto di accesso centralizzato per moltissimi servizi e fino a che non sono tutti disabilitati questa porta rimane aperta. La scorciatoia di arrestare il servizio RPC non funziona perché, pur chiudendo in teoria la porta, rende del tutto inutilizzabile il sistema operativo: niente taskbar, niente menù Start, niente *drag&drop*, tanto per citare alcuni dei componenti che non funzioneranno più. L'unica possibilità è quindi andare ad esaminare servizio per servizio e chiudere quelli inutili o non usati.

Figura 5-2. Servizi componenti



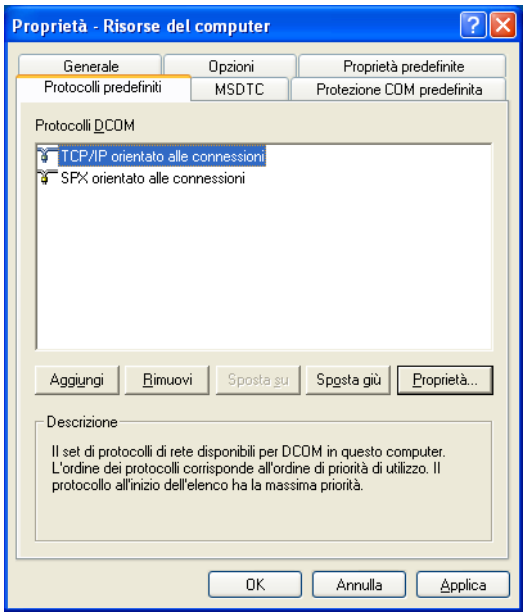
Per cominciare, intanto disabilitiamo tutto quello che riguarda l'accesso a DCOM. Dal prompt dei comandi lanciamo il programma **dcomcnfg**, che ci mostra un pannello chiamato Servizi componenti. Nel pannello (Figura 5-2) c'è una lista sulla sinistra: apriamo la voce Servizi Componenti; all'interno c'è Computer, che una volta aperta mostra Risorse del computer. Su questa voce facciamo clic col tasto destro del mouse e scegliamo Proprietà. Nel pannello che compare prendiamo Proprietà predefinite (Figura 5-3), togliamo la spunta alla voce Abilita DCOM in questo computer e premiamo il pulsante Applica per disabilitare il servizio.

Figura 5-3. Servizi DCOM: Proprietà predefinite



La seconda operazione la facciamo nello stesso pannello, selezionando però Protocolli predefiniti (Figura 5-4). Puntiamo i protocolli elencati e li cancelliamo tutti, uno per uno, con il pulsante Rimuovi.

Figura 5-4. Servizi DCOM: Protocolli predefiniti



Ora la situazione è che, pur continuando a funzionare regolarmente i servizi RPC e COM (ampiamente utilizzati sia per il funzionamento dell'interfaccia utente che per i meccanismi interni del sistema operativo), la corrispondente versione di rete, DCOM appunto, non è più accessibile dall'esterno. Questa porta è chiusa.

Porte da 1024 a 5000, sia TCP che UDP

Il servizio RPC citato in precedenza lavora in coppia con un altro servizio detto *RPC Locator*, che si occupa di rintracciare ed eventualmente rendere disponibile la particolare funzione del sistema operativo richiesta via RPC. Se la richiesta arriva via rete, *RPC Locator* rende raggiungibile il servizio richiesto aprendo una

porta TCP in ascolto. Dato che questi servizi non hanno una porta assegnata a priori per l'accesso via rete, la porta viene scelta fra quelle che vanno dalla 1024 alla 4999, disponibili proprio a questo scopo. Visto che possono differire da computer all'altro, il computer remoto chiede al Locator dove può trovare il servizio che gli interessa.

Le conseguenze sono che le porte aperte cambiano da computer a computer e non c'è una corrispondenza fissa fra porta e servizio. Inoltre, alcuni servizi sono attivati solo quando servono, e solo in quel momento aprono una porta in *LISTENING* sull'interfaccia di rete, e la lasciano aperta per tutto il tempo che rimangono attivi, spesso fino allo spegnimento del computer, rimanendo accessibili anche da qualsiasi altro computer, non solo quello che ha chiesto il servizio per primo.

Se abbiamo seguito attentamente il discorso fino ad ora, ci appare evidente che questa situazione è un vero disastro per la sicurezza: non sappiamo quali porte saranno aperte e da quali servizi. Soprattutto non sappiamo quali siano attivi, e fra questi quelli realmente pericolosi. Il risultato è che quando un malintenzionato vuole sfruttare uno di questi servizi non fa niente altro che tentare la connessione al gruppo di porte che più spesso sono utilizzate (di solito dalla 1025 alla 1050 TCP e UDP), a caso, cercando di imbroccare un servizio aperto incustodito.

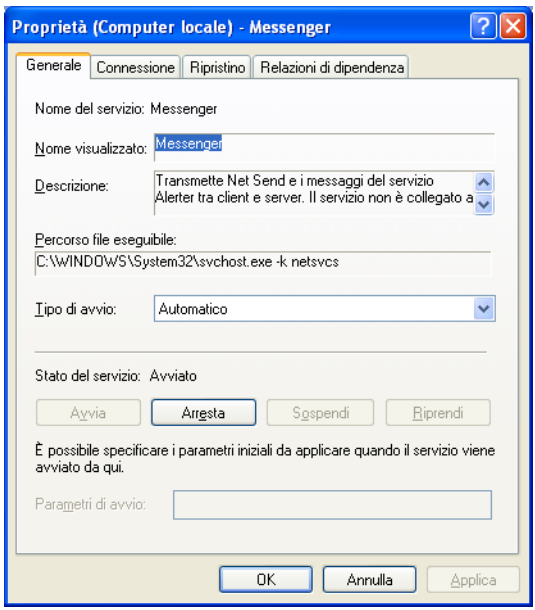
Partiamo da uno dei più innocui denominato Messenger (visto precedentemente, Figura 2-1). Il servizio è pensato in origine per avvisare chi sta usando il computer di situazioni particolari: l'avvio della procedura di backup da parte del server centrale in una grande azienda; il passaggio dell'alimentazione alla modalità di emergenza da parte di un UPS (*Uninterruptible Power Supply*) centralizzato, per via di un blackout. Se siamo a casa, non abbiamo un UPS, non abbiamo un server centrale che esegue il backup pianificato di tutti i computer collegati in rete, questo tipo di servizio è del tutto inutile. Viene sfruttato per far apparire messaggi trappola durante il collegamento a Internet, con l'intento di far visitare un sito web specifico, tipicamente segnalando che il computer è appestato da qualche innominabile morbo informatico, o che una fanciulla disinibita è ansiosa di conoscerci. Il sito web è invece una trappola che conterrà qualche tipo di malware, truccato da programma di disinfezione o da richiesta di autorizzazione per l'accesso alle immagini "pepate" della fanciulla.

Vale il principio del *trust no one*, citato precedentemente. Non ci dobbiamo fidare

di quello che dice il nostro computer, anche perché è qualcun altro, attraverso un servizio incustodito, che lo fa dire a XP.

Per disabilitare questo servizio, chiudendo la relativa porta, basta accedere al Pannello di Controllo, selezionare Prestazioni e manutenzione, Strumenti di amministrazione e fare doppio clic sull'icona Servizi. Compare un elenco con tutti i servizi disponibili, alcuni dei quali attivi. Si seleziona il servizio denominato Messenger, cliccando col tasto destro del mouse si richiama il menù di contesto e si sceglie Proprietà. Appare un pannello di configurazione (Figura 5-5), che sarà uguale per tutti i servizi che vedremo.

Figura 5-5. Proprietà di un servizio



Nel pannello Generale, alla voce Tipo di avvio, selezioneremo Disabilitato,

premendo poi il pulsante Applica. Poi premeremo anche il pulsante Arresta per fermare immediatamente il servizio. Chiudiamo questo pannello con il pulsante Ok. Possiamo notare che ora il servizio non ha più l'indicazione Avviato. Interrogando lo stato dei servizi in rete con il comando **netstat** visto prima, le porte risultano ancora aperte, ma verranno chiuse dopo il riavvio di Windows.

Chiudiamo anche qualche altra porta, visto che ci siamo. Andiamo al servizio denominato Registro di sistema remoto, usato per modificare il Registro di Windows da un altro computer via rete. Anche questo servizio è pensato per la gestione centralizzata, ma, come detto prima, sul computer di casa o su quello della piccola azienda, senza gestione centralizzata, non serve a nulla ed è una porta spalancata a chi vuole fare danni. Faremo la stessa modifica, disabilitando e fermando il servizio.

Poi è il turno del servizio chiamato Servizio di rilevamento SSDP, pensato per rilevare automaticamente dispositivi *Plug&Play* presenti sulla stessa rete a cui è collegato il computer. Questo servizio non si appoggia alla porta 135/TCP, ma ne apre ben due: 1900/UDP e 5000/TCP. Praticamente inutile, e nelle versioni di XP pre-SP2 è afflitto da qualche falla abbastanza critica.

Di seguito tocca a Utilità di pianificazione, Browser di computer, Servizi IPSEC e Webclient. Possiamo chiudere tutte le finestre e procedere ad un riavvio. Al ripresentarsi del desktop, apriamo di nuovo il Prompt dei comandi e vediamo cosa dice **netstat**:

```
C:\Documents and Settings\utente> netstat -an

Connessioni attive

  Proto  Indirizzo locale       Indirizzo esterno       Stato
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    192.168.42.152:139     0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    127.0.0.1:123          *:*
  UDP    192.168.42.152:123     *:*
  UDP    192.168.42.152:137     *:*
  UDP    192.168.42.152:138     *:*
```

Beh, abbiamo dato una bella sfoltita. Di punti di accesso ora ce ne sono molti meno, e quello che più conta è che la porta 135 sia chiusa.

Si possono avere effetti collaterali, perché questi servizi potrebbero essere usati da qualche applicazione specifica. Ad esempio Utilità di pianificazione potrebbe essere impiegata da applicazioni che eseguono compiti ad orario, mentre Browser di computer mantiene l'elenco di computer raggiungibili via rete che viene mostrato quando si *sfoglia la rete*. Quindi alcune operazioni potrebbero non essere più disponibili o funzionare in modo differente.

Un avvertimento: se qualcuna delle nostre applicazioni ha problemi a funzionare, non è detto che sia colpa di queste modifiche. Controlleremo bene sulle specifiche dell'applicazione e sui requisiti di funzionamento se qualcuno dei servizi disabilitati è richiesto per la normale attività dell'applicazione, prima di andare a modificare a caso i servizi attivi o spenti.

La sincronizzazione oraria

In una rete aziendale è piuttosto importante che gli orologi interni di tutti i computer siano impostati alla stessa data e ora, per motivi sia di sicurezza che di coerenza interna. Per questo motivo si usa un protocollo di rete standard (detto NTP, *Network Time Protocol*), che attraverso dei server locali o messi a disposizione gratuitamente in Internet permette ai computer di sincronizzarsi tra loro e con i server, raggiungendo spesso precisioni del millesimo di secondo.

In un computer singolo, o in una piccola rete dove non c'è un server NTP, è veramente poco utile e potrebbe essere usato per cambiare a piacere l'orario senza intervento da parte del proprietario del computer. Per questo motivo andiamo a disabilitarlo: con la stessa procedura vista sopra richiamiamo la gestione dei servizi, oppure dal prompt dei comandi digitiamo **services.msc**, che lancia direttamente il programma senza fare il giro dal Pannello di controllo. Puntiamo la voce Ora di Windows e tramite le proprietà fermiamo e disabilitiamo il servizio. La situazione ora sarà:

```
C:\Documents and Settings\utente> netstat -an

Connessioni attive

  Proto  Indirizzo locale       Indirizzo esterno       Stato
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    192.168.42.152:139     0.0.0.0:0              LISTENING
```

```
UDP    0.0.0.0:445            *:*
UDP    192.168.42.152:137     *:*
UDP    192.168.42.152:138     *:*
```

Siamo a buon punto.

I servizi server: porte 137/UDP, 138/UDP e 139/TCP

La possibilità di trasferire file tra due computer nello stesso ufficio o in casa, di condividere una stampante, di *sfogliare* la rete (per usare il modo di dire di Windows), è legata ad una serie di servizi che costituiscono la seconda fonte di propagazione dei malware in ordine di importanza. Se non abbiamo necessità di questo tipo di funzioni, o abbiamo un solo computer, possiamo disattivare questi servizi. Al di là di quella che può essere la comodità, il tempo di trasferimento di un file via rete è spesso molto più lungo di quanto ci voglia a copiarlo su un disco removibile USB e spostare il disco.

In ogni caso ci sono vari livelli di sicurezza che possono essere attuati. Per esempio se i nostri computer hanno soltanto sistemi operativi come Windows 2000, Windows XP, Linux, MacOS, e non abbiamo computer con Windows 95, 98 o ME, possiamo intanto disabilitare il servizio NetBIOS su IP, che chiude un altro gruppo di porte. Al solito andiamo su Pannello di Controllo, selezioniamo Prestazioni e manutenzione, Strumenti di amministrazione e avviamo il programma Servizi. Dalla lista selezioniamo il servizio Helper NetBIOS di TCP/IP e lo disabilitiamo nel solito modo.

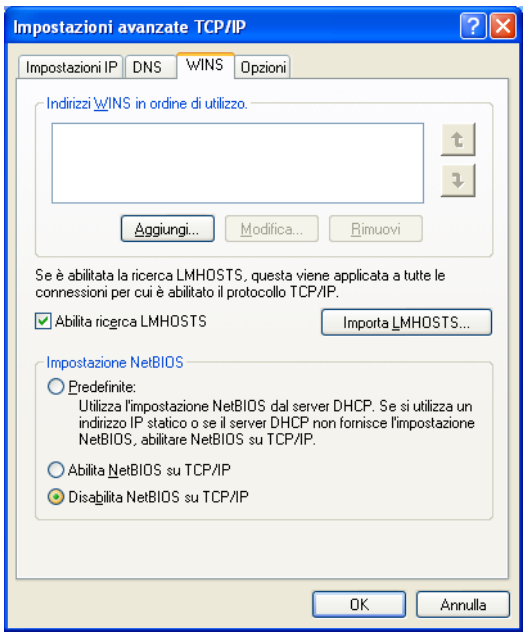
Questa operazione da sola non è sufficiente: l'impostazione di questo tipo di servizio è specifica per ogni interfaccia di rete, ed occorre disabilitarlo su tutte, una per una. Andiamo al Pannello di controllo, selezioniamo Rete e connessioni Internet, poi Connessioni di rete. Compare un elenco di tutte le interfacce presenti. Prendiamo la prima, richiamiamo il menù di contesto con il tasto destro del mouse e scegliamo Proprietà. Nel riquadro dal titolo La connessione utilizza gli elementi seguenti, selezionata la voce Protocollo Internet (TCP/IP) premiamo il pulsante Proprietà. Nel pannello che compare premiamo il pulsante Avanzate..., e selezioniamo il pannello WINS (Figura 5-6). Nel riquadro Impostazione NetBIOS selezioneremo la voce Disabilita NetBIOS su TCP/IP.

Questa operazione la ripeteremo per tutte le interfacce di rete e per i collegamenti via modem, analogico o ADSL.

Questa impostazione è specifica per ogni interfaccia di rete

Attenzione che questa operazione andrà ripetuta ogni volta che aggiungiamo o riconfiguriamo una interfaccia o un collegamento a Internet.

Figura 5-6. Il pannello di configurazione del NetBIOS



Ora la lista delle porte, dopo il riavvio, è questa:

```
C:\Documents and Settings\utente> netstat -an

Connessioni attive

  Proto  Indirizzo locale       Indirizzo esterno       Stato
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
```

Possiamo dire che va molto meglio.

L'effetto collaterale di questa serie di modifiche è che non possiamo più *sfogliare* la rete e vedere i computer presenti, né possiamo più accedere ad un altro computer usando il nome di rete, perché non è più attiva la risoluzione dei nomi NetBIOS, che faceva proprio questo. Il servizio di condivisione file e stampanti è ancora attivo, basta usare l'indirizzo IP del computer che si vuole raggiungere, invece del nome: se per accedere al computer di casa dal notebook prima usavamo ad esempio il percorso di rete `\\pccasa\condivisione`, ora dobbiamo cambiare in `\\192.168.42.140\condivisione`, supponendo che l'indirizzo IP 192.168.42.140 appartenga al computer di casa, oppure usare il metodo di risoluzione dei nomi tramite il file `LMHOSTS`, citato nel pannello appena visto. Questo file normalmente non c'è e dovrebbe trovarsi nella directory:

`C:\windows\drivers\etc`

dove si trova un file dal nome `lmhosts.sam`, che è un file di esempio su quale dovrebbe essere il contenuto del file `lmhosts`. In breve in ogni riga va messo l'indirizzo IP del computer che vogliamo raggiungere seguito dal nome che gli vogliamo dare. Seguendo l'esempio appena detto, il contenuto del file sarà qualcosa del genere:

```
192.168.42.140    pccasa
```

Con questa modifica ogni volta che cerchiamo il computer dal nome pccasa, automaticamente XP guarderà dentro questo file per vedere a quale indirizzo IP corrisponde. Se preferiamo andare con l'indirizzo al posto del nome questa modifica non è necessaria. La citiamo solo per completezza.

I servizi server bis: porte 445/TCP e 445/UDP

Se invece vogliamo proprio eliminare il servizio di condivisione file e stampanti, chiudendo anche le rispettive porte, visto che abbiamo un solo computer, o che per scambiare i dati usiamo un disco USB esterno, possiamo procedere in questo modo: torniamo al Pannello di controllo, e riprendiamo la gestione dei servizi con il solito percorso (Prestazioni e manutenzione, Strumenti di amministrazione). Andiamo al servizio Server, lo fermiamo e lo disabilitiamo. Occorre un riavvio per rendere effettive le modifiche. Il comando **netstat** riporta ancora le porte 445 TCP e UDP aperte, ma queste non accettano connessioni e a tutti gli effetti risultano chiuse.

Fra l'altro queste due porte sono punti di accesso alternativo ai servizi visti prima, per cui non basta chiudere la porta 135: servizi come Messenger sono raggiungibili anche dalla porta 445, quindi occorre comunque disabilitare il servizio Messenger per impedirne l'accesso dall'esterno.

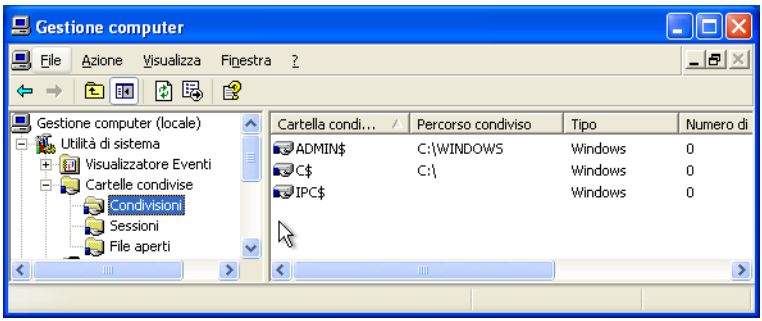
Al termine di questo gruppo di modifiche, siamo ancora in grado di usare normalmente il computer, di scambiare file con altri computer della nostra rete, di usare stampanti condivise. Se abbiamo lasciato attivo il servizio Server possiamo condividere file e stampanti del nostro computer, ancora completamente funzionale e molto più sicuro di prima, avendo chiuso molte porte di ingresso che neanche sapevamo esistessero.

Condivisioni amministrative

Se abbiamo lasciato attivo il servizio Server, abbiamo un problema non da poco: le condivisioni amministrative. Come sempre non è una porta aperta per motivi subdoli, ma semplicemente uno strumento di gestione pensato per l'amministrazione centralizzata, che però diventa un punto di ingresso perfetto per un malware. Se, al solito, il nostro computer lo usiamo in casa o in un piccolo ufficio, sono totalmente inutili, oltre che pericolose.

Per vedere le condivisioni amministrative possiamo usare il Pannello di controllo, alla voce Prestazioni e manutenzione, Strumenti di amministrazione, avviando il programma Gestione computer.

Figura 5-7. Le condivisioni amministrative



Sotto la voce Utilità di sistema c'è Condivisioni, che mostra un elenco di tutte le cartelle condivise (Figura 5-7). Se abbiamo abbiamo un solo disco interno, troveremo questa situazione: una condivisione specifica per il disco fisso (denominata C$), una per la directory di sistema di Windows (denominata ADMIN$), una per l'accesso ai servizi server (denominata IPC$) ed infine ne potrebbe esistere una (denominata print$) se abbiamo una stampante condivisa. L'accesso alle due condivisioni C$ e ADMIN$ permette di modificare a piacere tutti i file, praticamente tutto il contenuto del disco, mentre l'accesso alla condivisione IPC$ permette di avere informazioni dettagliate sul computer e sugli utenti anche senza fornire password o altro.

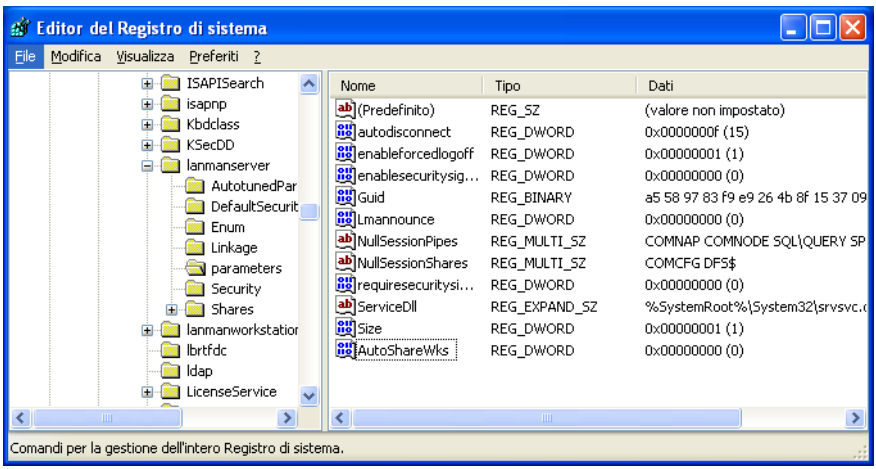
Per fortuna abbiamo varie possibilità di difesa: la prima è la password che abbiamo già assegnato a tutti gli utenti, e maggiormente a quelli amministratori; la seconda è di disabilitare le condivisioni; l'ultima è di usare il firewall per impedire l'accesso dalla rete.

Non possiamo pensare di usare una sola difesa, ma dobbiamo applicarle tutte. Partiamo dalla più delicata, ma più efficace: chiudiamo l'accesso al disco interno ed alla directory di Windows.

Pasticciare nel Registro di Sistema è pericoloso!

Quella spiegata di seguito è una operazione molto delicata che coinvolge il Registro di Sistema, ed un minimo errore può rendere il computer non più avviabile, quindi massima attenzione per scongiurare ogni possibile errore di digitazione.

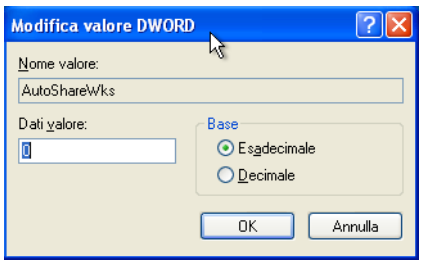
Figura 5-8. La modifica al registro di sistema



Per prima cosa avviamo l'editor del registro: dal menù Start, selezioniamo Esegui... e nella casella digitiamo **regedit**. Appare una interfaccia molto simile a Esplora Risorse. Sul lato sinistro apriamo HKEY_LOCAL_MACHINE, poi SYSTEM, CurrentControlSet, Services, LanManServer ed alla fine selezioniamo Parameters, sempre sul lato sinistro. A destra compare un elenco di voci (Figura 5-8), dobbiamo cercarne una dal nome AutoShareWks. Non dovrebbe esserci: andiamo a crearla facendo clic col tasto destro del mouse su un punto

vuoto del pannello di destra, e selezionando Nuovo, Valore DWORD. Lo chiameremo appunto AutoShareWks, e dovrà avere valore zero. Se dovesse essere già presente con un valore diverso, ci faremo clic col tasto destro del mouse sopra, selezioneremo Modifica, e nel pannello che compare assegneremo il valore corretto (Figura 5-9).

Figura 5-9. Modifica del valore di una chiave del registro



Occorre un riavvio per rendere effettive le modifiche, e se torniamo alla visualizzazione delle condivisioni stavolta avremo soltanto IPC$ ed eventualmente print$ se abbiamo una stampante condivisa.

Ulteriore protezione verrà poi dal firewall, quando ne parleremo. Per ora anche questa porta è chiusa.

L'assedio

Per capire fino a che punto queste modifiche sono efficaci, non rimane che fare delle prove. Ho simulato il collegamento a Internet senza protezioni: avviato il computer virtuale, ho deviato tutto il traffico in arrivo da Internet sulla sua interfaccia di rete, esattamente come fatto in precedenza (Sezione *Quanto resiste il fortino?* nel Capitolo 3). Ho avuto due differenti situazioni: una con il servizio Server attivo ed una con il servizio disabilitato.

Con il servizio attivo, si profila il problema degli errori presenti in XP: in pochi secondi un virus su un altro computer riesce ad agganciarsi alla porta 445/TCP, e compare un servizio in ascolto sulla porta 44445/TCP. Dopo qualche altro secondo parte una connessione verso un altro computer, con FTP (*File Transfer Protocol*), che cerca di scaricare nella directory `C:\windows\system32` un programma dal nome `taskmanger.exe` via FTP, ma il virus all'interno del computer virtuale sbaglia a comunicare l'indirizzo al computer remoto e il trasferimento fallisce.

Il servizio con la falla è chiamato LSA, ed è fornito dal programma `LSASS.EXE`. Questa falla, dettagliata nel bollettino di sicurezza Microsoft MS04-011[3] sotto la voce *LSASS vulnerability*, è stata sfruttata per la prima volta dal virus Sasser, analisi disponibile sul sito Sophos[4], ed è correntemente utilizzata da molti dei worm in giro per la Rete.

Ci sono vari metodi per impedire lo sfruttamento di questa falla, ma il migliore è correggere gli errori nei programmi, come vedremo nei capitoli a seguire.

Nel caso invece di servizio Server disabilitato, il problema non si pone. Il computer resiste senza problemi a tutti gli assalti, rifiutando correttamente le richieste di connessione in arrivo da Internet. Dopo un paio di ore di bombardamento tutto fila liscio e nessun file estraneo viene creato all'interno. E' certamente un successo pieno.

Questo però non significa *assolutamente* che possiamo andare tranquilli. Al contrario, questa è solo una delle modalità di intrusione dei malware, e neanche la più efficace. Vedremo fra qualche capitolo come anche con un computer blindato sia possibile essere colpiti da un ampio campionario di schifezze.

3. http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx
4. http://www.sophos.com/virusinfo/analyses/w32sassera.html

Capitolo 6. Porte tagliafuoco

La parola *firewall* in inglese indica una separazione a prova di incendio, come le porte speciali resistenti al calore poste ad esempio all'uscita delle sale cinematografiche o nei centri commerciali. Sono pensate per facilitare la fuga delle persone, e in caso di incendio possono contenere il calore e le fiamme per un certo tempo, impedendo al fuoco di propagarsi ad altri ambienti con troppa rapidità. Un *firewall* in senso informatico ha lo stesso significato: tenere fuori il pericolo, resistendo agli attacchi.

Una sentinella incorruttibile

Nel capitolo precedente abbiamo visto la situazione in cui, per validi motivi, siamo costretti a tenere attivo il servizio Server, ed aperta la relativa porta, che come abbiamo potuto constatare è vulnerabile a vari tipi di attacco da parte di malware.

La metafora del castello ci viene di nuovo in soccorso: dovendo lasciare aperta una porta d'accesso, lo faremo in modo ragionato: sentinelle, sorveglianza e chi vuole entrare deve farsi riconoscere o diventa cibo per i coccodrilli del fossato.

Ma come funziona in parole povere un firewall?

Quando si naviga in Internet, o si usa una stampante condivisa, il nostro computer stabilisce delle connessioni con altri computer attraverso il collegamento di rete: queste sono considerate in uscita, come una persona che esce dal castello. In questo caso la sentinella non ha necessità di riconoscere la persona che esce, né di chiedere dove va.

Differente è il caso di un computer che tenta di connettersi al nostro: se non abbiamo nessun servizio da offrire non c'è alcun motivo per entrare; mentre se offriamo un servizio, ad esempio una cartella condivisa, dovremmo essere certi che il computer che chiede quel servizio sia abilitato a farlo. Il firewall si occupa proprio di questo: come una sentinella al ponte levatoio, controllerà se chi chiede di entrare ha le carte in regola e dove sia diretto, e negherà l'accesso a tutti quelli che non sono autorizzati o non si facciano riconoscere.

Come questo sia possibile, è determinato dal funzionamento dei protocolli di rete, come abbiamo già visto nel capitolo precedente: ogni connessione ha una proce-

dura di avvio, con uno scambio di segnali ben precisi fra i due computer e la netta distinzione fra chi chiede la connessione e chi la accetta, permettendo al firewall di discriminare con certezza chi esce da chi chiede di entrare.

Tecnicamente parlando, per iniziare una connessione il computer che la chiede invia un segnale specifico, un pacchetto in protocollo TCP di tipo SYN. Chi riceve questo pacchetto ed accetta la connessione risponde con un altro pacchetto TCP di tipo SYN-ACK. Il firewall semplicemente non permette il transito in ingresso ai pacchetti TCP di tipo SYN: il servizio o il programma all'interno del computer non li riceve, quindi non può rispondere. Questo detto in modo molto semplice, nella realtà le cose sono infinitamente più complesse, ma questo ci serve e ci basta per la comprensione di quanto verrà in seguito.

Ricapitolando: per impedire ad altri computer di connettersi al nostro, il firewall impedisce le connessioni in ingresso, ma permette quelle in uscita.

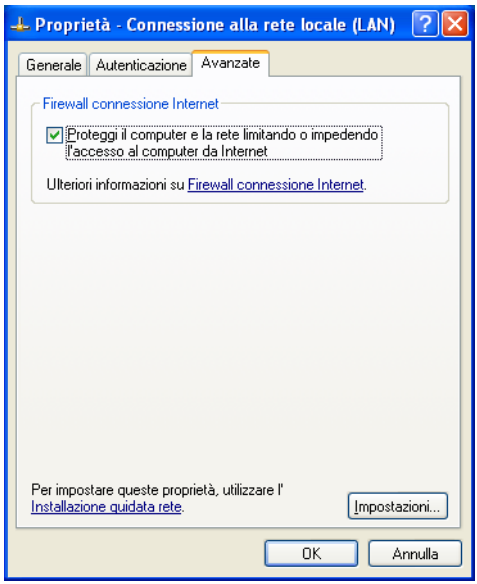
Una possibile evoluzione è di permettere connessioni in ingresso solo da alcuni computer: dato che ogni computer su una rete ha un suo indirizzo, si può istruire il firewall per accettare connessioni in ingresso solo da determinati indirizzi, e di rifiutare tutte le altre.

Tutte queste "norme di comportamento" sono impartite con le cosiddette *regole*, semplici istruzioni che vengono esaminate in sequenza dal firewall per decidere se accettare o rifiutare una connessione. Vedremo poi come si definiscono e come si modificano.

La quinta linea difensiva

XP mette a disposizione un firewall semplice ma efficace, che con il *Service Pack 2* viene migliorato, ma la sua funzionalità di base non cambia.

Figura 6-1. Attivare il firewall



Per attivare il firewall si entra nel Pannello di controllo, sotto la voce Rete e connessioni Internet, che mostra tutte le interfacce di rete presenti. Con un clic su una di esse del tasto destro del mouse si attiva il pannello delle proprietà, e si seleziona Avanzate (Figura 6-1). E' sufficiente mettere il segno di spunta nella casella Proteggi il computer e la rete limitando o impedendo..., ed il firewall viene attivato su quella particolare interfaccia.

Quando il firewall è attivo per un determinato collegamento, l'icona che lo rappresenta in Rete e connessioni Internet cambia, guadagnando un piccolo lucchetto in alto a destra (Figura 6-2 e Figura 6-3).

Figura 6-2. Collegamento senza firewall

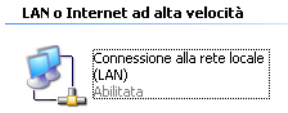


Figura 6-3. Collegamento con firewall

Ogni interfaccia ha il suo firewall

Se aggiungiamo un collegamento a Internet via modem, dobbiamo controllare le impostazioni anche di questo: ogni collegamento è differente, e occorre attivare e impostare il firewall separatamente per ognuno.

Con il *Service Pack 2* non è più necessario, il firewall una volta attivo vale per tutte le interfacce presenti. Quello che cambia sono le eventuali regole specifiche, che possono valere per la singola interfaccia o per tutte, in funzione del tipo di regola.

In questa modalità il firewall non guarda in faccia a nessuno: non si entra e basta. Il computer è irraggiungibile per chiunque, quale che sia il suo indirizzo di rete o il servizio che cerca. Questo va benissimo quando navighiamo in Internet, ma

quando il nostro computer deve condividere una stampante, diventa un problema: non sarà più accessibile da nessuno a parte noi.

Esiste la possibilità di aprire una porta per permettere l'accesso a determinati servizi: dal pannello di configurazione del firewall visto prima (Figura 6-1) si preme il pulsante Impostazioni... e si ottiene un pannello con elencati alcuni particolari servizi (Figura 6-4). Se il servizio è elencato basta spuntare la relativa casella. Quando invece non appare, come nel caso della condivisione file e stampanti, occorre creare la relativa regola: cliccando sul pulsante Aggiungi... si accede ad un pannello (Figura 6-5) che permette di specificare le caratteristiche del servizio che vogliamo aprire agli altri computer.

Figura 6-4. Servizi conosciuti dal firewall

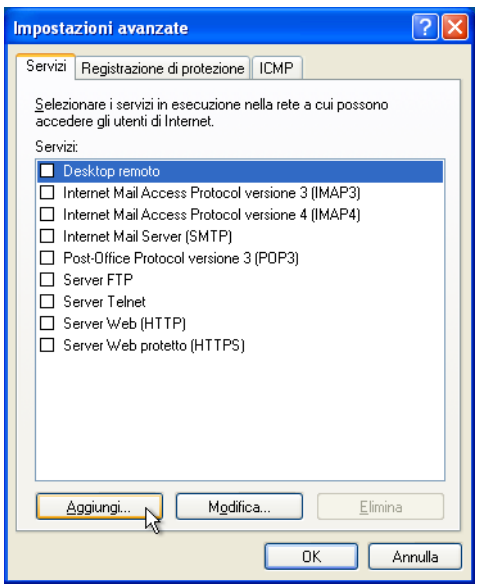
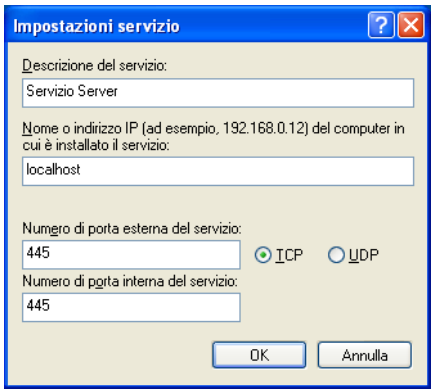


Figura 6-5. Apertura di un nuovo servizio

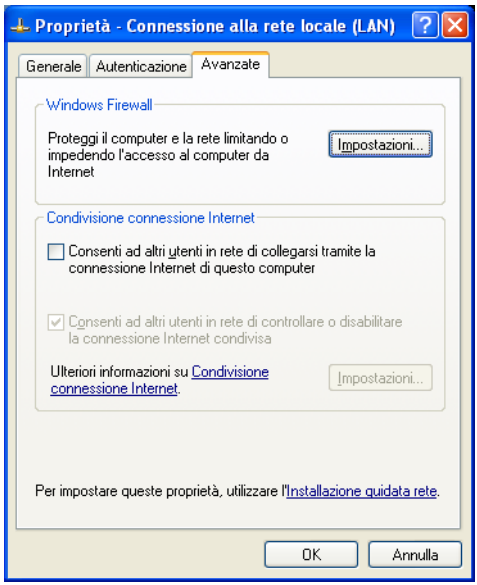


Nella casella Descrizione del servizio: scriveremo qualcosa di sensato, che ci ricorderà perché abbiamo aperto questa porta nel firewall: nell'esempio abbiamo scritto *Servizio Server* pensando alla condivisione di una stampante e di una cartella di file, che ricordiamo è legata al servizio Server di XP, disponibile sulla porta 445/TCP (Sezione *I servizi server bis: porte 445/TCP e 445/UDP* nel Capitolo 5). Nella casella Nome o indirizzo IP... scriviamo *localhost*, parola convenzionale che sta a significare *questo computer*. Controlleremo che sia selezionato il protocollo TCP e nelle due caselle Numero di porta... scriveremo 445, lo stesso numero in entrambe. Alla pressione del pulsante Ok le modifiche avranno effetto immediato.

Arrivano i rinforzi

Il problema con il firewall di XP in questa prima versione, che non sarà sfuggito ai più attenti, è che se permettiamo l'accesso a una determinata porta, non abbiamo la possibilità di discriminare fra amici o nemici: è aperta a tutti.

Figura 6-6. L'accesso al nuovo firewall



Nella versione disponibile con l'aggiornamento al *Service Pack 2* la situazione migliora notevolmente:

- Il firewall è unico per tutte le interfacce: una volta attivato difende tutte le interfacce di rete, sia di tipo LAN (ethernet o wireless) che di tipo WAN (Modem analogici, ISDN, ADSL). Non c'è più bisogno di andare interfaccia per interfaccia ad attivarlo.
- Le definizione delle regole permette di specificare le porte TCP o UDP da aprire o, in alternativa, a quale programma deve essere permesso l'accesso dall'esterno, risolvendo il problema dei servizi attivati su richiesta, a cui, ricordiamo, viene assegnata una porta a caso fra le prime disponibili (Sezione *Porte da 1024 a 5000, sia TCP che UDP* nel Capitolo 5).

- C'è la possibilità di far mostrare un avviso quando un programma in esecuzione riceve una richiesta di connessione dall'esterno che viene bloccata.
- Si può permettere o negare l'accesso a un servizio in base all'indirizzo di rete del computer che chiede la connessione.

Vediamo in dettaglio le funzioni principali. Il pannello di selezione del firewall è leggermente cambiato, riportando anche la funzione di condivisione del collegamento Internet (prima Figura 6-1, dopo Figura 6-6). Ora c'è solo il pulsante Impostazioni..., che porta ad un pannello con tutto quello che riguarda la gestione del firewall (Figura 6-7). Nella parte Generale ora le impostazioni sono in tutto tre: attivato con eccezioni, attivato senza eccezioni e disattivato. Le eccezioni, visibili dal pannello apposito (Figura 6-8), riguardano i servizi che a firewall attivo possono essere raggiunti da altri computer della rete o di Internet. Come vedremo fra poco, è stato risolto il problema di cui parlavamo: se si apre l'accesso ad una porta, prima era aperto a tutti, ora invece possiamo decidere chi può entrare e chi no.

Figura 6-7. Le impostazioni principali

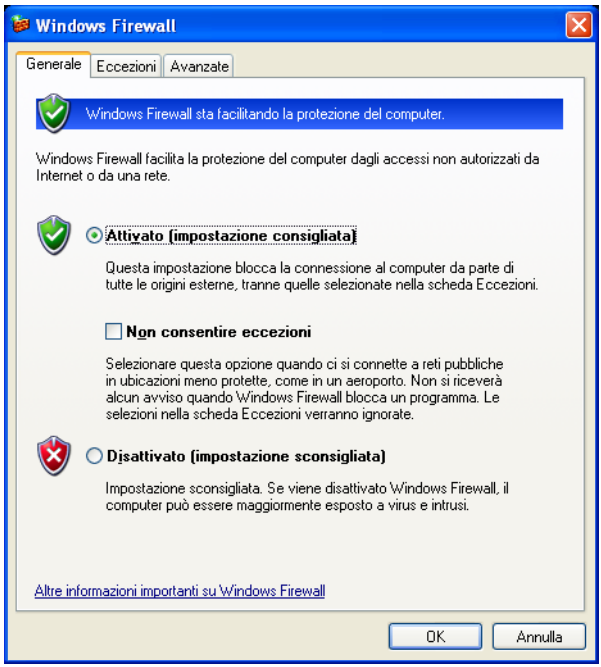
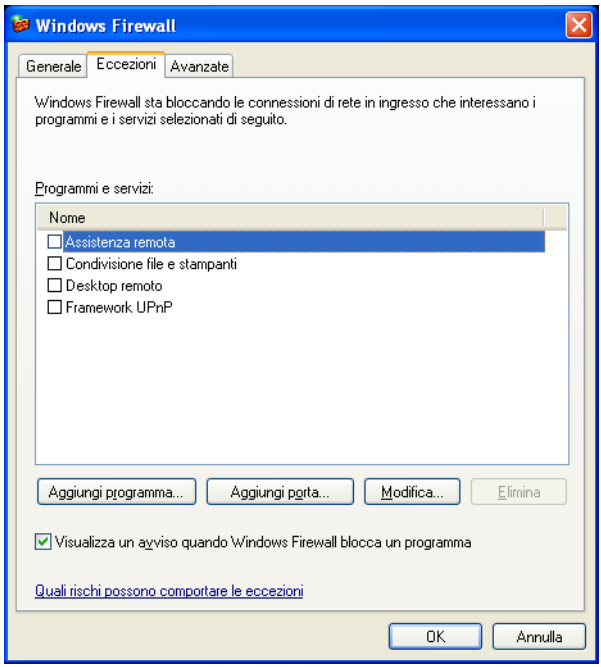


Figura 6-8. Le eccezioni



Regole ed eccezioni

Per capire meglio il funzionamento di questa nuova versione del firewall di XP, partiamo col definirne la regola di base: scartare tutte le richieste di connessione in arrivo, tranne quelle elencate e selezionate nelle eccezioni. Per vedere come viene definita una eccezione, possiamo premere il pulsante Aggiungi porta... nel pannello relativo (Figura 6-8). Ora l'interfaccia utente è più semplice (Figura 6-9), ma ha un pulsante in più, Cambia Ambito..., che nasconde la novità maggiore.

Figura 6-9. Aggiungere una eccezione come porta

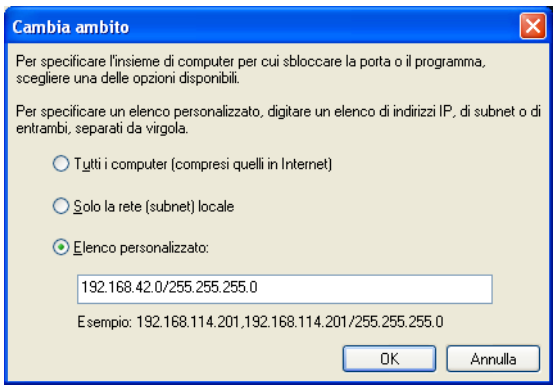
Usando lo stesso servizio di esempio citato prima, il servizio di condivisione file e stampanti, digiteremo nella casella Nome qualcosa di sensato, come sempre per ricordarci a distanza di tempo perché abbiamo creato questa eccezione. Scriveremo ad esempio *Condivisione per ufficio*, intendendo che solo i computer appartenenti alla rete dell'ufficio potranno accedere (fra poco vedremo come si indica). Nella casella Numero porta scriveremo il numero 445, come fatto precedentemente, e controlleremo che sia selezionato il protocollo TCP. Ora occorre definire *chi* può accedere, per cui premiamo il pulsante Cambia Ambito.... Nel pannello che appare (Figura 6-10) abbiamo tre possibilità:

- Tutti i computer: nessuna limitazione, la porta è accessibile da chiunque.
- Solo la rete (subnet) locale: tutti i computer che appartengono alla rete come definita dalla configurazione stabilita dal fornitore del collegamento. Per ora accettiamola così, fra un momento vedremo cosa significa.
- Elenco personalizzato: permette di specificare un elenco di computer o di gruppi di computer tramite l'indirizzo IP.

La prima possibilità opera esattamente come nel vecchio modello del firewall:

una volta aperta una porta, è accessibile a tutti, senza distinzioni. La seconda possibilità è predefinita proprio per il servizio di condivisione file e stampanti, già presente nella lista delle eccezioni. Questa è una trappola piuttosto pericolosa, fra poco vedremo perché.

Figura 6-10. L'ambito di applicazione della eccezione



Indirizzi, reti, maschere

Per capire meglio quanto diremo, occorre spiegare un momento cosa si intenda per *subnet*, o *ambito locale*, come lo definisce XP. Quando siamo collegati ad una rete di computer che faccia uso del protocollo IP, indipendentemente dal tipo di collegamento, ogni computer ha un proprio indirizzo, un numero particolare che permette di distinguerlo dagli altri senza fare confusione. Questo indirizzo, l'indirizzo IP appunto, è un numero a 32 bit che per comodità viene suddiviso in quattro numeri da 8 bit. La rappresentazione classica di un indirizzo IP è di scrivere i quattro numeri in base decimale separati dal punto, in questo modo: 192.168.42.152, dove i numeri decimali possono andare da 0 a 255. Per motivi che sono lunghi da spiegare, tutta la rete di Internet è suddivisa in una gerarchia

di reti più piccole, ognuna delle quali viene identificata tramite l'indirizzo IP dei computer che ne fanno parte.

Per semplificare la vita a tutti, si adotta la convenzione per cui i quattro numeri hanno peso decrescente da sinistra verso destra, proprio come nel normale sistema decimale: nel'indirizzo di esempio visto poco prima, il numero 192 è il più importante, mentre il numero 152 è quello di peso minore. Per facilitare la gestione e semplificare i problemi tecnici, l'indirizzo IP di un computer è convenzionalmente diviso in due parti: l'indirizzo della rete a cui appartiene, e l'indirizzo che ha in quella rete. Questa divisione non è fissa, ma è determinata da molti fattori, non sempre di tipo tecnologico, fra gli altri anche la necessità di semplificare la divisione delle responsabilità, per cui una società che gestisce una fetta di Internet è responsabile solo della parte di rete che le è assegnata. Questa suddivisione è fatta usando appunto il concetto di *subnet*, sottorete. I computer di una sottorete avranno la prima parte dell'indirizzo IP identica, e ogni computer avrà un suo indirizzo all'interno di quelli disponibili.

Per decidere quale sia la parte di indirizzo che identifica la sottorete, si usa un numero aggiuntivo, scritto allo stesso modo di un indirizzo IP, che però indica quale parte dell'indirizzo IP è l'indirizzo della subnet. Il computer usato in questi esempi ha indirizzo IP 192.168.42.152. La subnet a cui appartiene è definita in questo modo: 192.168.42.0/255.255.255.0. Senza introdurre concetti troppo pesanti o cervellotici, per quanto ci interessa, possiamo dire che questa indicazione si legge così: tutti i computer il cui indirizzo IP inizia con 192.168.42. Il numero 255.255.255.0 è detto *netmask* o *subnet mask*, tradotto qualche volta in *maschera di sottorete*. Grossolanamente potremmo dire che dove la netmask vale zero il corrispondente numero dell'indirizzo IP può avere un qualsiasi valore fra quelli ammessi per un indirizzo IP, un modo abbreviato per dire: *tutti i computer il cui indirizzo IP è compreso fra 192.168.42.0 e 192.168.42.255*.

Dato che gli indirizzi IP validi usano numeri vanno dal numero 0 al numero 255, e che proprio 0 e 255 hanno significati speciali e non possono apparire per ultimi, la *subnet* usata negli esempi può avere un computer per ogni indirizzo IP che va da 192.168.42.1 a 192.168.42.254. Questa subnet è per così dire "piatta", cioè ogni computer che vi è collegato può raggiungere tutti gli altri direttamente, senza intermediari.

La decisione di come sia definita una subnet è subordinata a standard ed accordi internazionali che stabiliscono la suddivisione a livello dell'intera Internet. Negli stessi standard è definito un certo numero di indirizzi IP che possono essere utilizzati per uso privato e che non appariranno mai su Internet. Sono i cosiddetti *indirizzi IP privati*, e ne esistono tre gruppi: da 10.0.0.0 a 10.255.255.255, da 172.16.0.0 a 172.31.255.255 ed infine da 192.168.0.0 a 192.168.255.255. Per usare questi indirizzi non dobbiamo dire niente a nessuno, li usiamo a piacere e definiamo noi quale sia la subnet, e quanto sia grande.

In casa o in un piccolo ufficio, si usa tipicamente una subnet con maschera di tipo 255.255.255.0, che, come abbiamo visto, permette di avere 254 differenti computer collegati. Difficilmente in casa o in ufficio potremmo aver bisogno di più computer.

Questo è il significato dei valori immessi nel pannello dell'ambito (Figura 6-10), e corrisponde esattamente al caso in cui scegliamo la voce Solo la rete (subnet) locale. Applicandolo alla eccezione, diremo che il servizio che fa capo alla porta 445/TCP è raggiungibile da tutti i computer che appartengono alla subnet 192.168.42.0/255.255.255.0, in totale 253 altri computer, quelli del nostro ufficio o di casa.

Se però andiamo in Internet, non possiamo presentarci con uno di questi indirizzi, ma dobbiamo usare l'indirizzo assegnatoci da chi fornisce il collegamento, il *provider*. Questi deve sottostare alle regole di Internet, e deve chiedere l'assegnazione di subnet dedicate, i cui indirizzi verranno "prestati" ai clienti nel momento in cui si connettono a Internet tramite il servizio offerto. In un normale collegamento ADSL viene fornito un indirizzo IP appartenente al provider, con la netmask decisa del provider stesso, non siamo noi a decidere indirizzo e netmask. Siamo pronti per affrontare il problema.

Eccezioni... eccezionali!

Questa situazione delle subnet e delle netmask è da tenere presente nel momento in cui usiamo le impostazioni predefinite previste per l'eccezione del firewall di XP sul servizio di condivisione file e stampanti.

La configurazione predefinita prevede l'uso della voce Solo la rete (subnet) locale. Ma sulle interfacce che sono collegate a Internet direttamente non siamo noi a decidere l'ampiezza della netmask, e quindi l'estensione della subnet: la decide il provider.

Supponiamo appunto che il nostro computer sia configurato con l'eccezione attiva, per permettere agli altri dell'ufficio di accedere alla nostra stampante ed a una cartella condivisa. Se andiamo ad avviare un collegamento tramite modem ADSL attaccato fisicamente al nostro computer, al momento della effettiva entrata in Internet il provider ci assegna un altro indirizzo IP e la rispettiva netmask. Nella totalità dei casi l'indirizzo assegnato avrà netmask 255.255.0.0. Supponendo che l'indirizzo sia 172.18.2.40, quella netmask dice che sulla stessa nostra rete possono essere presenti i computer con indirizzi IP da 172.18.0.0 a 172.18.255.255, per un totale di *oltre 60.000 computer*. Tutti questi computer potranno accedere al servizio offerto, involontariamente, dal nostro computer.

Ecco perché si prendono virus anche con il *Service Pack 2* e con il firewall attivo: l'eccezione per la condivisione, applicata a tutte le interfacce, permette l'accesso al servizio sulla porta 445, che come abbiamo visto (Sezione *I servizi server bis: porte 445/TCP e 445/UDP* nel Capitolo 5) è vulnerabile ad una serie di attacchi da parte di virus, e che anche su un computer perfettamente in ordine offre il fianco ad un attacco a dizionario sulle password (Sezione *La seconda linea di difesa bis: password* nel Capitolo 4). La mancanza o la debolezza delle password sugli account amministrativi diventa il punto di ingresso preferenziale in computer altrimenti blindati.

In questo caso la contromisura è proprio quella di cancellare l'eccezione predefinita, o di modificarne il contenuto in modo da specificare gli indirizzi IP usati dai nostri computer, cosicché tutti i tentativi di accesso da parte di altri computer andranno a vuoto.

Concludendo, appare evidente che il solo impostare il firewall per renderlo attivo con le configurazioni predefinite non è sufficiente: occorre dare sempre uno sguardo "sotto il cofano" per vedere se tutto è come dovrebbe.

Sentinelle a pagamento

Per via della latitanza di un firewall con funzioni più evolute di quello disponibile nella prima versione di XP, si è creato un mercato per i firewall software da installare su singoli computer, in sostituzione del firewall di XP. Le versioni disponibili sono moltissime, e molte sono le piccole differenze nel funzionamento, ma in particolare la funzione che è fornita da questi *personal firewall* e che non è disponibile sul firewall di XP, neanche in quello evoluto fornito col *Service Pack 2*, è il controllo sulle connessioni in uscita: viene controllata l'origine di ogni richiesta di connessione che dal computer è diretta ad un qualsiasi altro computer, sia esso della rete locale che su Internet, e da quale applicazione parte la richiesta di connessione.

Quando utilizziamo una nuova applicazione, nel momento in cui per la prima volta essa inizia una connessione verso un altro computer, il personal firewall la pone in attesa e mostra un avviso in cui chiede a noi cosa debba fare: se autorizzare, e se l'autorizzazione sia permanente. Questa, pur essendo a prima vista una potenziale carta in più da giocare contro malware ed altri tipi di attacchi, diventa in realtà fonte di confusione e di inutile allarmismo, che alla lunga si trasforma nel più classico esempio di "al lupo al lupo".

Leggendo l'avviso mostrato dal firewall, onestamente, pochi di noi hanno la preparazione necessaria per capire se l'applicazione che chiede di avviare la connessione verso l'esterno sia legittimata a farlo. Questo aumenta la confusione e porta in definitiva ad un comportamento che rende pressoché inutile questo tipo di controllo: si abilita tutto quello che ci passa per le mani, e spesso senza neanche leggere attentamente i messaggi. Inoltre, soprattutto nei primi minuti di uso del personal firewall, il pannello di richiesta di autorizzazione può essere proposto molto facilmente per un centinaio di volte. Il risultato è, nuovamente, che dopo un po' si clicca su Memorizza impostazione e Consenti senza neanche più leggere.

Se vogliamo andare a fondo, non è detto che questa funzione sia poi in grado di bloccare un eventuale malware che sia riuscito ad infilarsi nel computer, proprio perché chi crea i malware conosce il funzionamento dei personal firewall e può aggirare questa specifica protezione in vari modi (Sezione *Antivirus? Firewall? Che fanno, dormono?* nel Capitolo 2).

Come abbiamo già ribadito precedentemente, dobbiamo impedire al malware di entrare, piuttosto che prendere provvedimenti nella speranza di renderlo inoffensivo dopo. Una volta dentro, anche se non riesce a fare danni, o connettersi all'esterno, può comunque accedere a tutto il contenuto del computer, quindi avere un personal firewall che ne blocca le connessioni non è una grande sicurezza: se un ladro entra in casa, tenerlo chiuso dentro impedendogli di usare il telefono non è proprio una grande idea... Oltretutto, come ne è entrato uno ne possono entrare infiniti altri, per la stessa via da cui si è introdotto il primo.

Inoltre, anche l'installazione e la configurazione di questi tipi di firewall non è banale, ed anzi la maggiore disponibiltà di funzioni ne rende ancora più complicata la gestione. Molti includono funzioni per la configurazione automatizzata, che attraverso delle domande tentano di capire cosa ci serve e di conseguenza configurano regole ed eccezioni. Ma dovrebbe essere evidente ormai che una risposta sbagliata ad una domanda critica può aprire un falla gigantesca nel nostro muro di cinta. Occorre sempre sapere cosa c'è dietro le domande per capire come una nostra risposta possa lasciarci scoperti.

Sceglierne uno

Visto che il panorama commerciale è piuttosto vasto ed agguerrito, è normale avere qualche perplessità nello scegliere. Per orientarci un minimo, possiamo dare qualche consiglio di massima, senza scendere troppo in dettagli.

Per prima cosa il personal firewall deve essere installato solo da un utente con diritti amministrativi, altrimenti non potrebbe fare il suo lavoro. Seconda caratteristica da tenere presente è che il firewall vero e proprio deve lavorare come servizio di XP, e non come semplice applicazione. Ad esempio quello mostrato prima, di una nota casa, installa un servizio particolare che ha le funzioni di firewall, mentre la parte applicativa è soltanto il visualizzatore di allarmi e messaggi di attività, e l'interfaccia utente necessaria per chiedere l'autorizzazione a far connettere un programma con un server esterno.

Se il personal firewall che abbiamo scelto non si installa come servizio di XP, e non ha l'avvio automatico alla partenza del computer, ha una potenziale falla, neanche piccola: c'è un intervallo fra quando accendiamo il computer e quando

entriamo con il nostro utente in cui il personal firewall non è ancora attivo, lasciando aperte tutte le porte di accesso. Se stiamo utilizzando una rete senza fili, siamo in una rete aziendale, o siamo a casa di un nostro amico che ospita inconsapevolmente nel suo computer un qualsiasi malware, siamo fritti: il firewall non è ancora attivo e le porte di accesso ai nostri servizi sono aperte.

In ogni caso, tutti i personal firewall di note marche funzionano secondo lo schema del servizio di XP, attivato all'avvio del computer. Mi sono capitati solo due casi in cui accadeva che il firewall fosse attivato dopo l'accesso dell'utente, ma erano programmi molto rudimentali e non sono più in circolazione da parecchio tempo.

Il mio personale consiglio è di evitare programmi troppo complessi, con troppe funzioni, che ci subissino di *popup*, avvisi, messaggi, allarmi, ecc. Confondono le idee, distraggono, scocciano, insomma rendono l'attività al computer una fonte di ansia continua, ed un frenetico cliccare sui pulsanti di conferma. Fra l'altro, un firewall che fa il suo lavoro di solito lo fa silenziosamente. Avere in media tre-quattro messaggi al minuto in cui il firewall sbandiera ai quattro venti che sta facendo soltanto il suo dovere non è molto più utile che non averlo proprio. Certo, la presenza di questi messaggi deve quanto meno incuriosire, ma spesso si finisce col selezionare la casella Non mostrare più questa finestra..., e buonanotte.

C'è anche una alternativa, che per la mia modesta esperienza consiglio vivamente a chi ha un collegamento tramite ADSL: un *modem-router* con firewall interno. Questo tipo di apparecchi permettono di collegarsi ad Internet condividendo l'accesso con tutti i computer di casa o dell'ufficio, e contemporaneamente hanno all'interno un firewall efficiente e funzionale. I vantaggi sono molteplici: niente da installare sui computer, possibilità di collegarsi a Internet da più postazioni indipendenti, firewall sempre attivo, a fronte di un costo contenuto, e certamente abbordabile dai più. Inoltre questo tipo di collegamento permette di allontanare, dal punto di vista logico, il nostro computer da Internet, un po' come costruire un avamposto con fossato pieno di coccodrilli e muro di cinta cento metri prima del castello: un attaccante deve vedersela con le difese esterne prima di poter pensare di minacciare la sicurezza del castello.

Non c'è bisogno di ricordarlo: chi installa e configura un modem-router con firewall o un qualsiasi software di personal firewall deve sapere cosa sta facendo

e dove mettere le mani. La protezione offerta da questi due strumenti può essere elevatissima, ma solo se correttamente configurati. Come sempre, non è lo strumento che fa la differenza, ma la *competenza*.

Capitolo 7. Difetti di fabbricazione

Arrivati qui, con il computer relativamente blindato, potremmo connetterci a Internet e navigare, leggere posta, iniziare finalmente ad usarlo.

Ma ci sono ancora numerosi scogli da superare. Il nostro computer, pur infinitamente più sicuro di prima, non ha ancora tutte le carte in regola per poter affrontare il nemico. Portiamo pazienza, c'è ancora parecchia strada da fare.

Crepe nel muro

Visto che si presta molto bene alla nostra situazione, useremo ancora la metafora del castello. Può succedere che durante la costruzione delle mura esterne si usi una partita di mattoni difettosi, o che una delle travi che sorreggono il ponte levatoio sia meno resistente di quanto serve (chi è mai entrato in una casa appena costruita sa di cosa parlo).

Come abbiamo visto precedentemente (Sezione *Porta 135/TCP e 135/UDP* nel Capitolo 5 e Sezione *L'assedio* nel Capitolo 5), questi difetti sono ampiamente sfruttati da chi crea malware, perché permettono l'accesso a computer altrimenti inviolabili.

In questo caso l'unica difesa è di riparare il danno, sostituendo le parti difettose, e nel malaugurato caso in cui non sia possibile, prendere delle precauzioni specifiche per aggirare il problema. Ad esempio per il difetto nel servizio LSA, la procedura è di creare un file in una particolare directory e renderlo non modificabile per bloccare questa falla. La procedura completa è riportata in dettaglio nel bollettino di sicurezza Microsoft MS04-011[1], già citato in precedenza.

Può succedere anche che, oltre a non essere disponibile una sostituzione, non sia disponibile neanche un metodo per aggirare il problema. Questo è un vero disastro, perché avremo sempre una falla non riparabile, che manterrà il nostro computer vulnerabile. Questa situazione si verifica quando esiste un errore, conosciuto, ed il produttore del sistema operativo o della specifica applicazione non si affretta a rilasciare una correzione.

1. http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

In gergo tecnico queste correzioni si chiamano *patch* (pezza, rattoppo, cerotto), proprio per dare l'idea di "mettere una pezza".

Il rovescio della medaglia è che queste correzioni sono a loro volta programmi, e possono contenere errori esse stesse, introdurre problemi che nella versione precedente non si presentavano, risultare incompatibili con altri programmi.

Per far capire quanto sia delicato l'argomento, la politica di gestione delle patch quando si ha a che fare con un computer utilizzato come server o per applicazioni critiche, è che le correzioni non si applicano alla cieca, ma si devono provare prima su un computer gemello, che ha la stessa configurazione hardware, lo stesso sistema operativo e le stesse applicazioni. Se dopo test approfonditi non si rilevano problemi, si passa ad applicare la patch anche al computer principale.

Non solo il sistema operativo

Il problema degli errori nei programmi interessa anche le normali applicazioni, non solo il sistema operativo. Visto che sono fatte di software anche loro, è perfettamente normale che possiedano la loro dose di difetti.

Non tutti i difetti sono ugualmente pericolosi, tanto che esistono delle classificazioni. Dal punto di vista del difetto in sé, ne abbiamo di tre tipi principali:

- la "svista": un refuso nel nome di un menù, una icona con l'immagine rovinata e simili. Non provocano altri problemi che la semplice indicazione errata o confusa. Sono tipicamente errori di battitura, o confusione fra versioni differenti (l'icona rovinata viene inclusa al posto di quella corretta).
- l'errore: una voce di menù che non funziona al primo colpo o una operazione che porta un risultato sbagliato. In generale coinvolgono una sola funzione del programma utilizzato, o ne limitano in parte l'uso (ad esempio un formato di immagine che non viene letto correttamente da un programma di grafica), ma non rovinano dati o il funzionamento dell'applicazione o del sistema operativo nel complesso.
- l'errore grave: il salvataggio del lavoro non funziona, l'apertura di un tipo di file blocca completamente il computer. Sono problemi insormontabili, e di solito

portano a perdita di dati, quando non del sistema operativo. Ad esempio una versione del pacchetto Office aveva un errore di questo tipo: in un documento piuttosto esteso, se si premeva il pulsante Salva, e prima che l'operazione di scrittura del documento sul disco fosse completata si premeva il pulsante di chiusura della finestra, il salvataggio si bloccava a metà, lasciando il file rovinato e inutilizzabile, e senza fornire indicazioni su quanto era successo.

Il secondo e terzo tipo di errori sono buoni candidati per diventare porte di ingresso sfruttabili dai malware. Se il nostro browser ha un errore del secondo tipo, il semplice visitare un sito web che sfrutti questo errore potrebbe costringere il browser stesso a scaricare ed installare un programma senza avvertirci di nulla. Un errore del terzo tipo potrebbe far bloccare il computer alla semplice ricezione di una connessione dalla rete, o all'apertura di un messaggio di posta elettronica.

Fortunatamente anche per le applicazioni sta crescendo l'attenzione verso i difetti che possono essere classificati come problemi di sicurezza, e anche Microsoft ha avviato un programma di aggiornamenti per tutti i suoi prodotti.

Se abbiamo letto attentamente la parte sulla gestione degli utenti e dei privilegi (Sezione *La seconda linea di difesa: diritti e gerarchie* nel Capitolo 4), possiamo intuire che una eventuale applicazione errata sfruttata da un malware può accedere e modificare solo i file e le impostazioni dell'utente che l'ha avviata. Quindi usando per il lavoro normale un account utente normale, non privilegiato, impediremo ad un errore in un programma di essere sfruttato per modificare cose nel computer che solo un amministratore può modificare.

Cosa e quando

XP ha il suo sistema di aggiornamento, chiamato *Windows Update*, che si occupa degli aggiornamenti del sistema operativo e dei servizi connessi. La tendenza generale è di applicare gli aggiornamenti appena escono, e di applicarli tutti, lasciando fare al programma in automatico. Personalmente preferisco essere io a decidere quando aggiornare, per non avere fastidiose interferenze durante il lavoro. Ma in ogni caso gli aggiornamenti vanno fatti quando sono classificati come *critici*, cioè quando gli errori che vanno a correggere possono essere utilizzati come porta di ingresso dai malware.

Può succedere (e non solo con XP), che un aggiornamento interferisca con il normale funzionamento del computer. E' capitato alla fine di aprile 2006 che un aggiornamento critico provocasse malfunzionamenti con una intera famiglia di server di un noto produttore, in particolari circostanze. Certamente pochissimi di noi hanno un server in casa, ma può succedere che un aggiornamento sia incompatibile con qualcuna delle applicazioni che utilizziamo. Per evitare questi problemi si può operare in vari modi, ma forse il migliore è di attendere qualche giorno prima di applicare gli aggiornamenti, cioè non appena usciti. Questo ovviamente vale solo quando non vi siano emergenze del tipo di quella creata dal virus Blaster nell'agosto del 2003, nel qual caso l'aggiornamento conviene farlo immediatamente.

Per ogni aggiornamento è disponibile la disinstallazione, andando in Pannello di Controllo, Installazione applicazioni. Il problema è che gli aggiornamenti sono elencati con il loro codice, ma nei dettagli è possibile determinare la data di rilascio e di installazione, quindi non dovrebbe essere troppo difficile rintracciare quello incriminato.

Sia ben chiaro: stiamo parlando di eventualità abbastanza remote, ma è meglio sapere in anticipo dove mettere le mani in caso di problemi.

Cliccare informati

Il titolo di questo paragrafo fa il verso alle note trasmissioni di informazione per la viabilità stradale e marittima, e non a caso. Dove possiamo reperire informazioni attendibili e di prima mano sul nostro sistema operativo? Per quanto possa sembrare ovvio, pochi sanno del servizio dei bollettini di sicurezza messo a disposizione da Microsoft.

Molti di noi prestano fede ai messaggi che arrivano per posta elettronica, promettendo catastrofi e sventure inenarrabili se non facciamo qualcosa (di solito inviare lo stesso messaggio a tutti quelli che conosciamo: lo scopo di questi messaggi è solo questo, diffondersi attraverso la credulità, lo vedremo nel capitolo dedicato alla posta elettronica, più avanti), ma pochi si preoccupano di reperire le informazioni da fonti attendibili e di prima mano. Chi meglio del creatore di XP?

Per tenere sotto controllo i bollettini di sicurezza Microsoft, iscriviamoci quindi alla Newsletter dal titolo "Aggiornamenti sulla sicurezza" che troviamo sul sito Microsoft[2].

Occorre avere un profilo Passport valido per iscriversi, ma non è un problema visto che è gratuito sia ottenere il profilo che iscriversi alla Newsletter. Non avremo più bisogno di chiedere all'amico "smanettone", o di prestare fede a messaggi allarmistici e inverosimili: periodicamente ci verrà spedito un messaggio con tutte le informazioni necessarie. Questa operazione rientra nella prima linea di difesa citata qualche capitolo fa: *sapere*.

La Newsletter può essere inviata come messaggio di testo semplice, senza allegati e immagini, o con abbellimenti vari. Per maggior sicurezza sceglieremo la versione solo testo: i link e le immagini nei bollettini possono essere contraffatti, come è successo qualche tempo fa, per propagare virus e altre porcherie mediante falsi messaggi, con cui Microsoft ovviamente nulla ha a che fare.

Con questi bollettini avremo sempre il polso della situazione, e direttamente dal produttore di XP. In base a quanto leggeremo, sapremo poi se e cosa aggiornare, e quanto sia importante l'aggiornamento in arrivo.

Non è obbligatorio e non è fondamentale, ma è comunque un'arma in più in nostra difesa. E non costa quasi nulla, tranne che un po' del nostro tempo, ma i vantaggi sono evidenti.

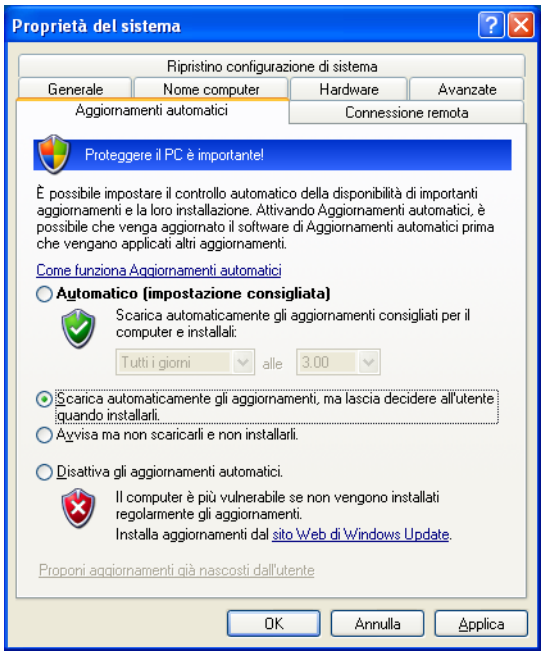
Come si aggiorna

Per aggiornare occorre che utilizziamo un account con diritti da amministratore, e che siamo collegati a Internet.

Si può fare in due modi: a mano o automaticamente. Nel Pannello di controllo e nel menù Start esiste la voce *Windows Update*, e dopo l'applicazione del *Service Pack 2*, anche nel Centro di sicurezza del PC. Attivando manualmente *Windows Update* si apre Internet Explorer e si visita una pagina web che controlla il nostro computer e elenca gli aggiornamenti disponibili, con il livello di criticità.

2. http://www.microsoft.com/italy/security/security_bulletins/decision.mspx

Figura 7-1. Configurare gli aggiornamenti automatici



Se scegliamo l'automatismo di *Windows Update*, possiamo configurarlo cliccando col tasto destro del mouse sull'icona Risorse del computer, e dal menù scegliere Proprietà.... Nel pannello che appare si sceglie Aggiornamenti automatici (Figura 7-1). La mia impostazione preferita è quella mostrata, che scarica gli aggiornamenti ed avverte quando sono pronti per l'installazione, ma non li installa finché non attivo esplicitamente l'operazione. Nel mio caso ho un collegamento fisso ad Internet, via ADSL, e posso permettermi di lasciare sempre attivo l'aggiornamento. In ogni caso le impostazioni sono in funzione del tipo di collegamento a Internet e delle preferenze personali.

Figura 7-2. Pronti per l'installazione

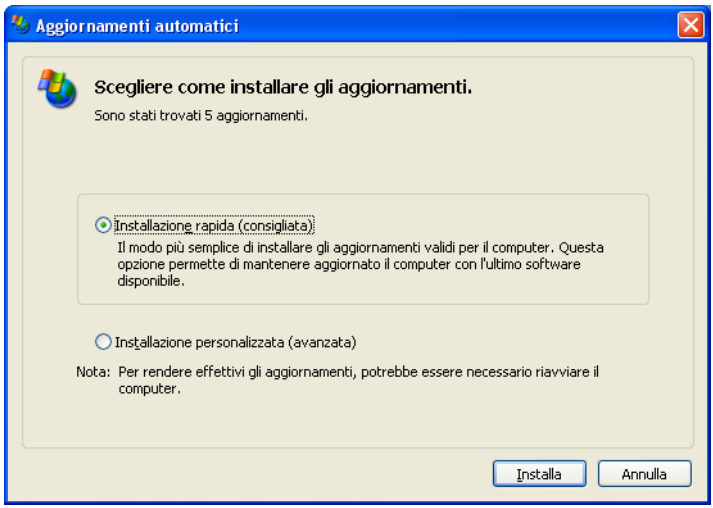
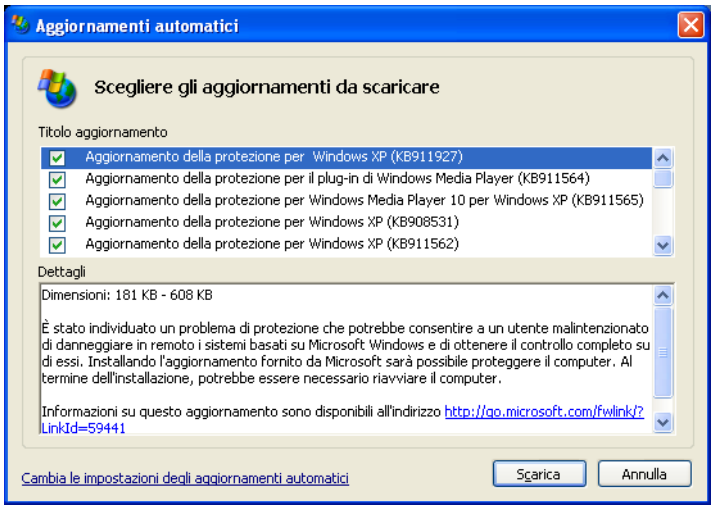


Figura 7-3. Scelta degli aggiornamenti da scaricare



Verremo avvertiti della disponibilità di aggiornamenti tramite un messaggio e una icona vicino l'orologio nella *taskbar*. Cliccando sull'icona comparirà un pannello che può cambiare in funzione del comportamento scelto nella configurazione degli aggiornamenti automatici. Ad esempio, con la mia impostazione preferita il pannello mostra solo due scelte (Figura 7-2), mentre nel caso del solo avviso ne appare uno (Figura 7-3) che ci propone gli aggiornamenti disponibili: occorre poi scegliere, scaricare e installare quelli che ci interessano.

Aggiornare senza Internet

Se non si ha un collegamento Internet, gli aggiornamenti diventano impossibili o quasi. Ma in un certo senso decade anche gran parte del problema dei malware e della necessità di aggiornamenti per chiudere falle.

Il problema si pone quando il collegamento ad Internet è con un normale modem a 56k, che rende lunghissime le operazioni di aggiornamento per via del tempo necessario a scaricare le patch. Per dare una indicazione, un aggiornamento ammonta in media a qualche megabyte, e con un modem siamo intorno a tre minuti di collegamento per ogni megabyte. Ci sono aggiornamenti da una decina di megabyte, e ci sono aggiornamenti da pochi kilobyte, ma ce ne sono anche da 75-100 megabyte, come nel caso del *Service Pack 2*. E' certamente improponibile pensare di scaricare una quantità simile di dati con un normale modem.

In questo frangente, ma anche in molte altre situazioni, l'aggiornamento è oggettivamente impossibile o impraticabile, per cui occorre valutare delle alternative: ad esempio, le operazioni citate nei capitoli precedenti mettono ragionevolmente al riparo da problemi di attacchi da parte di malware, anche se non rappresentano la soluzione definitiva; oppure si possono scaricare le patch tramite un amico che ha un collegamento veloce. Nel caso del *Service Pack 2* era disponibile presso Microsoft un servizio di spedizione che forniva gratuitamente un CD-ROM con l'aggiornamento. In tutti questi casi gli aggiornamenti vanno installati a mano, nello stesso modo in cui si installano normali applicazioni. Se abbiamo l'iscrizione al bollettino di sicurezza Microsoft, vi troveremo anche le istruzioni per reperire ed installare il singolo aggiornamento.

Insomma, non siamo completamente tagliati fuori, di possibilità ne abbiamo. L'importante è aver capito quanto sia fondamentale e delicato questo aspetto per la sicurezza del nostro computer e dei nostri dati.

Rattoppare o non rattoppare?

Per concludere, quando conviene aggiornare e quando è una fatica inutile? Se abbiamo letto fin qua, la risposta dovremmo averla già, ma riassumiamo un po'.

Se non abbiamo un collegamento ad Internet ed il nostro computer è usato principalmente in casa, il gioco non vale la candela, nel senso che gran parte dei malware in circolazione oggi si propagano e sfruttano unicamente il collegamento in rete: se non esiste, non esiste neanche il vettore di ingresso dei malware.

Se abbiamo un modem a 56k, ed il nostro uso di Internet è molto limitato, con

molta probabilità sono sufficienti le misure proposte nei capitoli precedenti. Ci si può limitare agli aggiornamenti più critici, e connessi con le applicazioni che usiamo.

Se invece abbiamo un collegamento Internet veloce, siamo spesso in rete o abbiamo una piccola rete domestica o in ufficio, con la possibilità di avere computer esterni che vengono collegati con gli altri, allora occorre applicare tutto lo spettro di strategie e contromisure. Non possiamo sapere se un amico arriva a casa nostra con il notebook appestato, o andiamo a casa sua con il nostro e ci riempiamo di malware, quindi conviene giocare d'anticipo.

Capitolo 8. Clicca QUI!

Siamo al principale motivo per cui di solito connettiamo il computer ad Internet: la navigazione. Il *browser*, il programma che ci permette di trasformare bit in immagini, testi, suoni, animazioni, è il protagonista assoluto dei nostri viaggi per l'oceano della rete. In un certo senso è il nostro ambasciatore, e purtroppo è la prima e più frequente vittima durante le nostre visite in territori poco amichevoli.

Internet Explorer è il browser di serie su tutte le versioni di Windows, e in XP raggiunge una forte integrazione con il sistema operativo stesso. Parte dei programmi e delle funzioni più importanti si appoggiano direttamente o indirettamente su di lui. Il fatto che sia chiamato "esploratore di Internet", curiosamente, ci permette di fare un parallelo con gli esploratori di fine ottocento: era facile per loro imbattersi in popolazioni ostili, lande inospitali, animali e piante mortali. Il tributo di vite è oramai storia. La sorte del nostro povero esploratore è molto simile: finisce prima o poi per cacciarsi in qualche guaio, o si contagia con qualche morbo che porta ad epidemie e disastri.

Vediamo di fare tesoro delle sventure di quanti, metaforicamente, non sono più tornati a casa.

Terre inesplorate

Il nostro esploratore nasce con un armamentario notevole: in un certo senso è già preparato ad affrontare di tutto. Come sempre, attivarne tutte le protezioni renderebbe la navigazione su Internet noiosa e difficoltosa, mentre senza alcuna protezione cadrebbe vittima della prima zanzara di passaggio.

Inoltre, la situazione è aggravata dalla possibilità di aggiungere pezzi: i *plugin*, per accedere a contenuti particolari, quali animazioni, giochi, suoni, video; le estensioni, o *browser helper object*, che arricchiscono di funzioni il browser.

Ebbene, ognuno di questi pezzi aggiunti, ed ognuna delle funzioni messe a disposizione dal browser Internet Explorer, se non correttamente e coscientemente utilizzata, può essere sfruttata per portarci in casa il nemico. Un nemico che non ha remore a fare del nostro computer e dei nostri dati l'uso che più gli aggra-

da. Cannibali, tagliatori di teste, schiavisti, predoni, pirati, briganti, tutti questi simpatici individui sono là fuori in attesa dei poveri esploratori.

Abbiamo un problema in più, rispetto a chi finanziava esplorazioni e spedizioni alla ricerca di tesori in terre inospitali: non possiamo mandare qualcuno di sacrificabile, nel senso che se l'esploratore cade vittima di un predone siamo noi a subire danni, non sempre virtuali, attraverso il nostro computer. Quindi dobbiamo fare attenzione a dove mandiamo il povero esploratore, e per quanto possibile fornirlo delle protezioni necessarie ad affrontare i pericoli che si pareranno sul suo cammino.

In questo capitolo vedremo se è possibile avere Internet Explorer configurato in modo che, pur permettendo una navigazione soddisfacente, non diventi porta di ingresso per malware, e non cada facilmente vittima di qualche predone. Purtroppo non sono molte le cose che si possono fare, ma controlleremo le difese a disposizione, ed eventualmente modificheremo quello che serve per indurirlo un po'. Non ci aspettiamo di avere un Indiana Jones™, ma almeno guarderà dove mette i piedi...

Spyware e demolitionware

Il termine *spyware* è usato per la categoria di malware che si limitano, se di limite si può parlare, a spiare la nostra attività al computer, nel senso più ampio del termine. Lo scopo di questi malware è molteplice, ma i principali obbiettivi sono la nostra identità, le nostre informazioni personali e soprattutto i nostri soldi. Una volta insediati nel computer possono collezionare i dati più disparati, ma soprattutto spiare la nostra attività, non solo durante la navigazione in Internet.

Ad esempio esistono dei programmi, chiamati in gergo *keylogger*, i quali, senza nessuna interferenza avvertibile, registrano tutti i caratteri che digitiamo sulla tastiera del computer, anche quando non siamo collegati a Internet, e li inviano al loro "creatore" non appena è disponibile un collegamento. In breve possono sapere tutte le nostre password, i dati personali, il contenuto delle nostre e-mail, i codici delle nostre carte di credito, e così via. Proprio come se fossero dietro le nostre spalle, spiando tutto quello che digitiamo.

Oppure programmi che registrano tutti i siti web che visitiamo e mandano l'elenco ad un server, dove viene analizzato il contenuto delle pagine. Successivamente viene ordinato al programma infiltrato nel nostro computer di mostrarci pubblicità "mirata", in funzione del tipo di siti che visitiamo di solito. Questo tipo di spionaggio viene chiamato *profiling*, prendendo in prestito un termine usato in criminologia: si costruisce il profilo di uno sconosciuto basato soltanto su alcune caratteristiche note del comportamento, in questo caso i siti visitati più frequentemente. Dato che il profilo viene creato per fare pubblicità, non c'è necessità di conoscere il nostro nome o l'indirizzo dove lavoriamo.

Alcuni malware modificano in modo più o meno esplicito il collegamento a Internet, cambiando il numero telefonico che utilizziamo di solito, o aggiungendo un nuovo collegamento a Internet in Rete e connessioni Internet, e marcandolo come predefinito. In questo modo chiameremo un numero telefonico che ha una tariffazione molto maggiore di quella del nostro provider abituale. Oppure installano un dialer, che oltrepassa completamente le impostazioni del nostro collegamento a Internet.

O, ancora, programmi che modificano le impostazioni del browser per mostrare all'avvio di Internet Explorer un determinato sito web, o modificano le pagine che visitiamo per includere pubblicità che non è presente sui siti originali. Sono chiamati *hijacker*, dirottatori, proprio perché costringono il browser ad andare dove vogliono loro, e non dove diciamo noi.

Per far tutte queste cose, questi programmi devono accedere liberamente alle parti vitali del sistema operativo, ed alle impostazioni del browser. Alcuni sono, per così dire, "gentili", passando per le normali funzioni di installazione del software e permettendo quindi un controllo della loro presenza e della loro attività. La maggior parte, purtroppo, è invece congegnata per invadere, modificare, deviare, nascondere, senza tanti complimenti e senza scrupolo alcuno.

Il risultato è un computer devastato, dal punto di vista del sistema operativo: impostazioni che non si modificano, programmi che si avviano senza il nostro consenso, finestre che si aprono su siti web non proprio eleganti. Questo tipo di spyware è fra i più fastidiosi, ma in fondo il meno insidioso per la nostra sicurezza, nel senso che *sappiamo subito che c'è*, vediamo immediatamente i suoi effetti. Nel caso dei keylogger il pericolo è infinitamente maggiore, proprio perché il princi-

pale scopo è di acquisire informazioni senza mettere in allarme la vittima, quindi lo sforzo per non essere scoperti è maggiore. Nei programmi che cambiano invece le impostazioni del browser o che modificano il collegamento a Internet lo sforzo maggiore è nel rendere inefficaci le contromisure: non si riesce a disinstallare il programma; ripristinare le impostazioni del browser o del collegamento a Internet è inefficace; eliminare manualmente i file è del tutto inutile, vengono ricreati immediatamente. Alcuni arrivano addirittura a disabilitare l'uso dei programmi di gestione del computer: il Task Manager e l'Editor del Registro vengono molto spesso disabilitati, quando non addirittura cancellati.

Questa breve panoramica ci mette di fronte al fatto che abbiamo a che fare con veri e propri criminali, che impiegano molte risorse nell'attività fraudolenta. Limitarci all'uso di un programmino "magico" può magari darci un senso di sicurezza, che però è più pericoloso: siamo tranquilli, *tanto c'è la magia tecnologica che ci salva*.

NO. Il criminale che voglia fare i suoi comodi con il nostro computer conosce perfettamente tutti questi programmini "magici", e sa come evitarli o come renderli inefficaci. Per capire quanto questo sia vero, basta frequentare newsgroup e forum dedicati all'argomento sicurezza del computer, per rendersi conto che i fallimenti dei programmini magici spesso sono molti più dei successi.

Nei paragrafi che seguono cercheremo di fare un breve profilo dei pericoli più comuni, e dei metodi usati dai criminali per demolire il nostro sistema operativo, in barba a tutte le contromisure. Chiederemo aiuto al nostro povero computer virtuale, usato come esca e cavia, il cui sacrificio ci permetterà di capire come i malware si fanno strada dentro i meccanismi più delicati di XP, e di come possano effettivamente ridurre a un rottame un computer altrimenti in perfette condizioni.

La cura sbagliata

Con questa categoria di predoni, malware che prendono di mira solo ed esclusivamente il browser, il firewall è totalmente inutile, o quasi. Siamo *noi* che navigando avviamo delle connessioni in protocollo TCP verso i server web in Internet ed a portare in casa una bomba ad orologeria. Il firewall, quale che sia, non può far nulla: il browser è per definizione autorizzato ad andare su Internet, e tutte le ope-

razioni sono eseguite per il suo tramite, quindi anche in presenza di un firewall che controlli le connessioni in uscita i danni vengono fatti lo stesso.

L'altra contromisura che ancora non abbiamo trattato, l'antivirus, è parimenti poco efficace. Per vari motivi che vedremo meglio nel capitolo specifico, contare sulla protezione dell'antivirus è una pia illusione. Nei prossimi esempi reali di attacchi automatizzati al nostro computer virtuale vedremo come gli antivirus sono in gran parte inefficaci e incapaci di riconoscere il pericolo, indipendentemente dal produttore, o da quanto sia ritenuto efficace dagli esperti del settore. Per far questo mi sono servito della scansione messa a disposizione gratuitamente dal sito Virustotal[1], che esamina un file fornito da noi con una nutrita schiera di differenti antivirus, praticamente tutti quelli conosciuti al momento. Le sorprese non mancheranno.

Una ulteriore contromisura, lo *scanner antispyware*, molto in voga e molto utilizzato in questi ultimi tempi, ha la stessa efficacia dello scanner antivirus, e funziona in modo assai simile: per individuare un malware annidato all'interno del computer cerca i segni della sua presenza. Quindi *può trovare solo quelli che conosce*.

Questo perché non esiste un chiaro segno di presenza di uno di questi ospiti sgraditi, facilmente individuabile e univoco. La porta di ingresso è, per così dire, regolare. Usano metodi e tecnologie normalmente impiegate per scopi non deleteri: ad esempio lo stesso Acrobat Reader™ installa e usa una estensione del browser per poter mostrare i documenti in formato PDF direttamente dentro Internet Explorer; la Google Toolbar™ è anch'essa una estensione del browser. Quindi non si può fare di ogni erba un fascio: sarebbe come dire che, visto che i virus sono programmi eseguibili, allora tutti i file con estensione `exe` sono virus.

Esistono dei dispositivi e dei software che in modo trasparente controllano tutto quello che prendiamo su Internet, ma hanno gli stessi limiti dei vari antivirus e antispyware, che vedremo meglio fra breve: possono bloccare solo i predoni che già conoscono.

Di tutte le strategie e le operazioni fatte fino ad ora, l'unica che possa fare qualcosa di veramente utile è l'uso corretto dei privilegi degli account, avvalersi cioè di utenti non amministratori durante la navigazione (Sezione *La seconda linea di*

1. http://www.virustotal.com/

difesa: diritti e gerarchie nel Capitolo 4). Nei paragrafi che seguono, vedremo come molti di questi predoni automatizzati rimangano scornati di fronte ad un browser che stia girando con diritti normali, e come invece possano fare i propri comodi sfruttando i diritti degli utenti amministratori.

Vieni a vedere cosa ho trovato!

Come per XP, anche per Internet Explorer si è fatta strada la convinzione che sia pieno di falle, al punto che la strategia più usata è di sostituirlo con un altro browser meno problematico. Questo ha un fondamento di verità, ma la maggioranza dei problemi di Internet Explorer ha la stessa origine dei problemi di XP: il pensarlo come parte del sistema operativo, e quindi integrarlo profondamente con esso, ha obbligato una serie di scelte che si sono rivelate infelici.

Prima fra tutti, e forse l'unica pericolosa sotto tutti gli aspetti, è la presenza della tecnologia Active-X, finalizzata a far eseguire programmi al browser come parte di una pagina web, chiamati in gergo *controlli Active-X*. A differenza di altre tecnologie, questi programmi possono accedere e modificare file e configurazioni all'interno del computer in cui viene eseguito Internet Explorer. Windows Update non potrebbe funzionare senza Active-X. Le applet Java, una tecnologia simile, non hanno per definizione accesso a nessuna parte del computer: non possono modificare nulla e non possono neanche leggere file dal computer. Un controllo Active-X eseguito dal browser, lanciato da un amministratore può accedere alle stesse cose a cui può accedere l'utente. Ci dovrebbe ricordare qualcosa (Sezione *La seconda linea di difesa: diritti e gerarchie* nel Capitolo 4).

Lo stesso problema si presenta con i cosiddetti *linguaggi di scripting*: veri e propri linguaggi di programmazione con tantissime funzioni, pensati per creare programmi da eseguire all'accesso ad una pagina web, all'interno del browser ed entro limiti piuttosto ristretti. Né Active-X, né i linguaggi di scripting hanno falle in sé, sono normali componenti del sistema operativo, regolarmente funzionanti: il vero problema discende dal fatto che Active-X è fortemente ed intimamente integrato con XP, mentre i linguaggi di scripting consentono l'uso di risorse di elaborazione su cui i limiti sono molto blandi. Per cui Active-X consente l'accesso in profondità ai meccanismi più delicati e più vulnerabili di XP, mentre i linguaggi

di scripting possono consumare risorse ed eseguire alcune operazioni scavalcando il nostro controllo.

Il problema si aggrava nel momento in cui sia gli script che i controlli Active-X sono scaricati da Internet, inglobati all'interno di pagine web o richiamati da esse. Per i controlli Active-X si può aggiungere un meccanismo di certificazione con firma crittografica digitale, che dovrebbe in qualche modo aumentarne la sicurezza, ma il problema è che la firma ne attesta solo la provenienza, cioè l'effettiva identità di chi afferma di aver creato quel particolare controllo.

Sicura è la firma, non il controllo

L'equivoco nasce dal confondere la sicurezza della firma, ossia la effettiva appartenenza a chi dichiara di essere il proprietario, e la sicurezza del contenuto. Quando una pagina web fa riferimento a un controllo Active-X firmato da scaricare, appare un pannello di conferma (Figura 8-2) che riporta la dicitura: *Attenzione: (nome del produttore) dichiara che il contenuto è sicuro. Installare o visualizzare il contenuto solo se (nome del produttore) è considerato attendibile* che purtroppo è una involontaria trappola, nel senso che letta la prima frase ci sentiamo più tranquilli, mentre invece la chiave di comprensione è nella seconda parte, dove si dice che quanto richiesto va accettato solo se il produttore è *per noi* attendibile.

Questo equivoco è una fonte potenziale di inganno, perché la lettura della prima parte prevale sulla seconda, che invece è la più importante: possiamo dare il permesso solo se consideriamo il fornitore attendibile. Per quanto possiamo sapere, l'unico attendibile al momento è soltanto il produttore del sistema operativo.

Là fuori conoscono a perfezione questi problemi, solo che dal punto di vista dei predoni sono *opportunità* da sfruttare.

Esca, trappola e vittima

Guardiamo da vicino qualcuno dei metodi di invasione e devastazione impiegati dai predoni, studiando il comportamento di alcune loro creature con l'aiuto della nostra cavia virtuale. Una considerazione prima di cominciare: solo uno dei siti malevoli usati per le prove sfrutta le famigerate falle di Internet Explorer, nell'iniettare schifezze nel computer tramite il browser. I metodi usati più frequentemente sono basati sull'uso di controlli Active-X, navigazione con diritti amministrativi e soprattutto l'inganno.

Non visitare i siti mostrati!

Eccesso di zelo, se a qualcuno fosse poco chiaro: i siti mostrati potrebbero essere attivi ed ancora pieni di trappole, senza dubbio aggiornate e ancora più micidiali di quelle trovate durante questa navigazione dimostrativa. Quindi, se ancora non fosse evidente, andare su uno di questi siti *è pericoloso!*

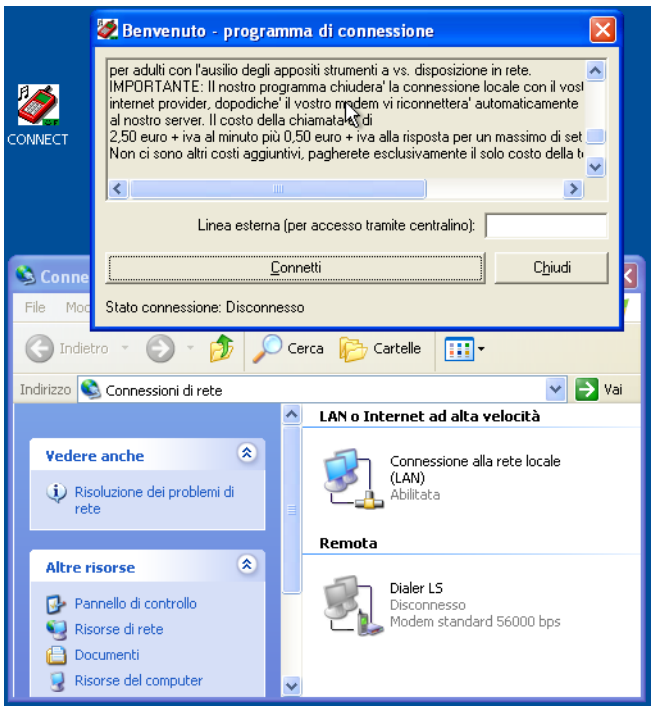
Servizi gratuiti... a pagamento

Un sito promette l'invio di SMS gratuiti. Seguendo il link, si arriva ad una pagina in cui si avvisa che il servizio è sospeso a tempo indeterminato, ma niente paura: ci viene offerto un sistema alternativo con un collegamento dedicato, e ci sono anche logo e suonerie per il telefono cellulare *gratis*! Basta solo scaricare il programmino... Che altro non è che un dialer, che crea un collegamento via modem (Figura 8-1) ad un numero a tariffazione speciale (i famigerati 899 o 709, quando non addirittura numeri internazionali). Dal pannello informativo si legge 2,50 euro al minuto, per un massimo di settantacinque minuti.

Al momento dell'attivazione volontaria del programma (non si avvia autonomamente, dobbiamo lanciarlo noi), viene creato un nuovo collegamento a Internet dal nome *Dialer LS*, che vediamo nel Pannello di controllo alla voce Connessioni di rete. Il pericolo è grande, visto che XP permette la creazione di collegamenti via modem anche ad utenti non privilegiati, cioè utenti normali, purché ci sia un

modem configurato. L'esca è un servizio definito *senza costi aggiuntivi tranne la connessione*, che gratuito alla fine non è proprio: calcolando un collegamento di mezzora, siamo a 75 euro, esclusa IVA.

Figura 8-1. Un dialer: icona, collegamento e pannello di avviso



In questo caso essere amministratori o utenti normali non salva dal disastro. Il dialer è ben congegnato e sfrutta a fondo le opportunità. Ma in fondo è un brigante *gentile*: richiede il nostro intervento per essere scaricato ed installato, e il nostro esplicito consenso per l'avvio del collegamento, avvertendo del costo.

Passando il file eseguibile al sito VirusTotal, citato sopra, il risultato è che solo nove antivirus lo identificano con certezza come un dialer, uno lo marca come sospetto, ma ben *quattordici* non trovano nulla di strano. E fra i quattordici ci sono nomi di tutto rispetto.

I due antispyware provati non rilevano nulla. Niente di niente.

Da una banale ricerca nei newsgroup, risulta che il sito in questione sta distribuendo dialer almeno da settembre 2003, quindi non è proprio una minaccia nuovissima visto che il test è stato fatto nel maggio del 2006.

C'è un aggiornamento! Corri!

Un altro sito promette lo scambio di link interessanti e divertenti per la navigazione in internet. Appena arrivati, se in quel momento si sta navigando con un utente amministratore, appare immediatamente un avviso (Figura 8-2) che riporta la dicitura "Aggiornamento Automatico di Window - Cliccare SI immediatamente." (non è un refuso, c'è scritto proprio *Window*).

Figura 8-2. Sta per scattare la trappola...

La trappola è pronta: basta un semplice click sul tasto Sì ed il gioco è fatto. Se si preme il pulsante No, durante la navigazione sul sito viene più volte riproposto il falso aggiornamento.

Alla pressione del tasto Sì succede il finimondo: in brevissimo tempo, senza che vengano fatte altre domande e senza che si abbia il tempo di reagire, si aprono in successione quattro nuove finestre del browser, il disco lavora a più non posso, vengono scaricati dati in continuazione da Internet. Poco dopo appare sul desktop una icona raffigurante una stampante, dal nome "Epson-Stylus", che in realtà è una applicazione dal nome `Epson-Stylus.exe`. Inutile dire che è una ulteriore trappola, con cui Epson™ non ha proprio nulla a che fare. Dopo qualche secondo, senza toccare nulla, appare un pannello che afferma di essere un aggiornamento del browser (Figura 8-3). Leggendo meglio nel microscopico testo di spiegazione, che appare solo dopo aver premuto il pulsante Dettagli>>>, si nota la frase: "Il costo della connessione ottonovenove flat a scatto unico alla risposta, sarà pari a quindici euro iva compresa con durata massima di quindici minuti.", che è un capolavoro di eufemismo.

Figura 8-3. Una stampante che non abbiamo, ed un aggiornamento a 15 euro.

Siamo di nuovo di fronte ad un dialer, dei più pericolosi: basta la sola risposta alla telefonata, anche in assenza di effettivo collegamento, e ci troveremo addebitati in bolletta 15 euro. Ora, anche ammettendo che siano "onesti" e ci facciano godere appieno dei quindici minuti di navigazione promessi, per mezzora siamo a 30 euro.

Non finisce qui. Notare che il pannello di Aggiornamento browser non ha pulsanti per rifiutare, e non ha neanche i pulsanti di chiusura della finestra: per eliminarla occorre chiamare il Task Manager e terminare l'applicazione da lì.

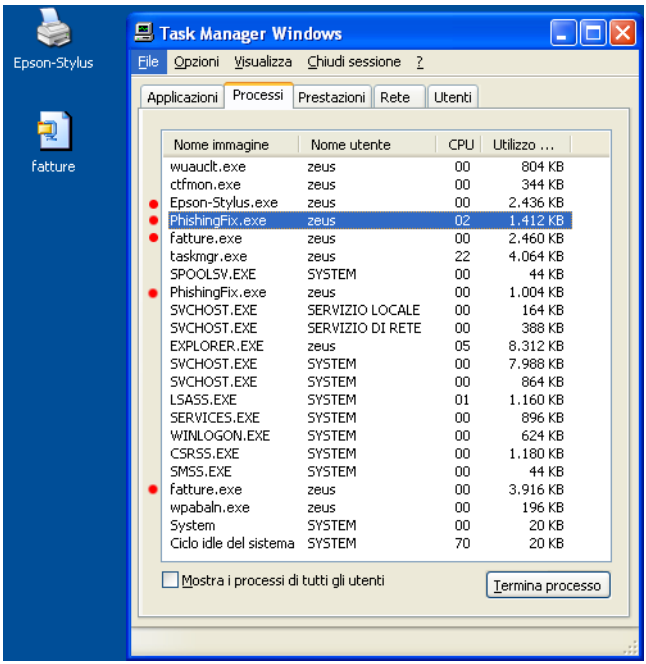
Anche senza accettare l'aggiornamento, nell'aprire Internet Explorer succede un altro terremoto (Figura 8-4): il numero di finestre che si aprono da sole arriva a quattro, tutte su siti differenti. C'è un messaggio che conferma di aver impostato con successo siti attendibili. Premendo il tasto OK, la finestra che si vede subito dietro prende tutto il desktop, nascondendo anche la taskbar: non ha pulsanti di chiusura, menù, insomma niente che possa levarla da davanti. Solo con la combinazione **Alt**-**F4** si riesce a chiuderla, ma l'effetto è di breve durata: immediatamente dopo se ne aprono altre due, una con la pubblicità ad un sito a luci rosse, l'altra con un fantomatico sito "Ricercadoppia". Appare un'altra icona sul desktop dal nome "fatture", con l'immagine di un file compresso. E' anche questo un dialer, dal nome `fatture.exe`.

Da questo momento in poi la situazione precipita: ad ogni click sulla falsa pagina di start, che molto ironicamente riporta la scritta “Dove vuoi andare oggi”, si apre un altro sito apparentemente gratuito, che contiene altre trappole ed altre applicazioni truccate. C’è persino un programma che viene presentato come la soluzione per navigare sicuri chiamato “PhishingFixer”. Fra breve faremo anche la sua conoscenza.

Figura 8-4. Il computer non è più nostro...

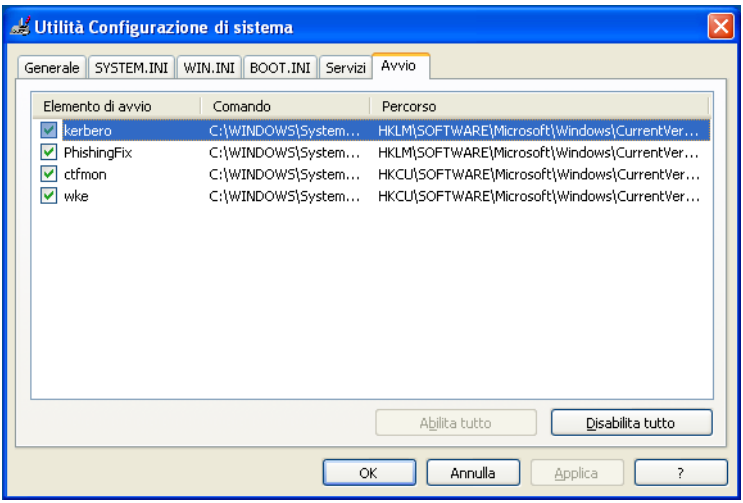
E’ un calvario: navigazione impossibile, avvisi di collegamento interrotto, finestre che si aprono su siti certamente non adatti ai bambini, computer lentissimo.

Figura 8-5. Programmi indesiderati (col pallino rosso)



Inutile continuare, il danno è evidente. Per completezza, vediamo fino a che punto è arrivato a fare i propri comodi nel nostro computer. Partiamo dal Task Manager: ci sono un certo numero di processi attivi che prima non c'erano (Figura 8-5), i cui nomi sono piuttosto strani, oltre ai due programmi di prima.

Figura 8-6. Programmi avviati automaticamente

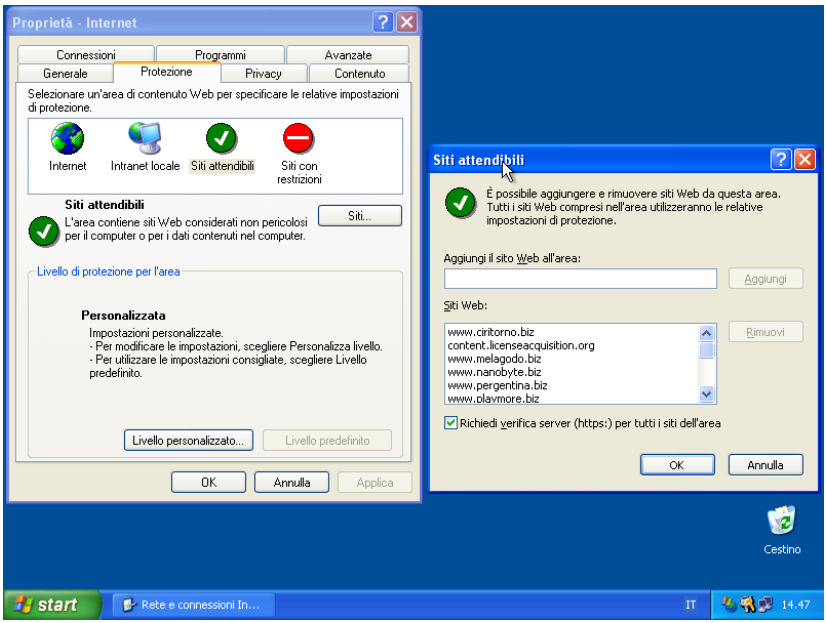


Chiamando il programma **msconfig** dallo Start menù, Esegui, al pannello Avvio abbiamo tre voci in più che prima non esistevano: kerbero, PhishingFix e wke (Figura 8-6). I primi due sono programmi posizionati nella directory `C:\windows\system32`, il terzo, che dovrebbe essere posizionato nella stessa directory con nome `wke.exe` non è presente. Il programma **msconfig** serve a mostrare le impostazioni ed il contenuto di tutti i file coinvolti nella configurazione di avvio iniziale di XP, soprattutto quello che non appare in "Esecuzione Automatica".

C'è ancora una modifica, che è molto più subdola: se andiamo in Pannello di controllo, Rete e connessioni Internet, Opzioni Internet, arriviamo a vedere le impostazioni di funzionamento di Internet Explorer: per il momento ci interessa il pannello Protezione. Se selezioniamo l'icona verde con il segno di spunta, dal nome Siti attendibili, e premiamo il pulsante Siti..., appare una lista di siti che possono fare una serie di operazioni senza alcuna restrizione (Figura 8-7). Per intenderci, questa lista di solito è vuota, e la presenza di siti che non abbiamo

inserito di persona è sicuro indice di intrusione da parte di un malware.

Figura 8-7. Siti attendibili... per chi?



Ultima cosa, che rispetto al resto è roba da poco: la pagina iniziale di Internet Explorer, quella caricata all'avvio del browser, punta ad un sito a luci rosse.

Inutile dire che un riavvio non risolve niente, e che addirittura anche se entriamo con un altro utente troviamo già in esecuzione il programma `PhishingFix.exe`.

Supponendo di avere un antivirus attivo e ben configurato, il livello di protezione sarebbe stato insufficiente. Passando i quattro file incriminati al sito VirusTotal, i risultati sono stati molto poco incoraggianti:

- Per il file `Epson-stylus.exe`: 12 antivirus lo identificano come malware, anche se non sono d'accordo fra loro sul tipo. Uno lo definisce sospetto, ma per 11 non c'è nulla di anomalo.
- Per il file `fatture.exe` va leggermente meglio: 15 lo identificano con sicurezza, anche qui senza essere d'accordo sul tipo di minaccia. Uno lo definisce sospetto, e per 8 va tutto bene.
- Per il file `kerbero.exe`: solo 2 lo identificano come una minaccia e anche qui non sono per nulla d'accordo sul tipo. Uno lo segnala come possibile sospetto, ma i 21 rimanenti non fanno una piega.
- Per il file `PhishingFix.exe`: è una sconfitta totale, nessuno lo identifica come minaccia, solo uno lo segnala come possibile sospetto. Gli altri 23 non trovano nulla di anomalo.

Inutile dire che i nomi noti falliscono tanto quanto i meno noti. C'è da dire che alcune di queste minacce sono relativamente nuove e poco note, per cui gli antivirus non hanno nel loro database le firme per riconoscerle.

Se invece usiamo un utente non privilegiato per navigare, all'entrata nel sito non succede nulla. Niente avvisi, messaggi, avvertimenti, richieste. Anche cliccando volontariamente sul link che dovrebbe portare all'installazione del controllo Active-X non succede nulla.

Le prime notizie di questo gruppo di siti malevoli appare in rete intorno al gennaio 2006, ed i test sono stati condotti nel maggio dello stesso anno.

Un secchio d'acqua per una goccia di olio

Mia nonna citava spesso questo proverbio, in cui si immaginava qualcuno che per bere una goccia di olio era costretto a trangugiare un secchio d'acqua, indicando una situazione dove per ottenere un guadagno irrisorio si deve subire un disagio enorme e non necessario. Su Internet le situazioni simili non mancano.

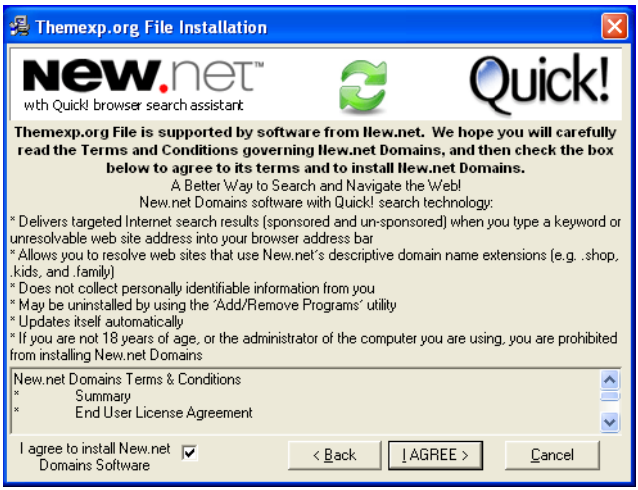
Un sito offre personalizzazioni per il desktop, quali sfondi, icone, temi e simili. Andiamo nella pagina degli sfondi, ne scegliamo uno molto carino, dimensione dichiarata 245kbyte. Un click sul pulsantino "Download", e la prima cosa strana è

che il file è un programma di 705kbyte. Uno sfondo è una immagine, niente di più, quindi un programma non è proprio necessario, ma la cosa che deve insospettire è che le dimensioni non corrispondono.

Simuliamo la persona fiduciosa, e facciamo un doppio clic sull'icona del file appena scaricato. Parte l'installazione che chiede immediatamente di accettare una licenza d'uso. Il testo è molto lungo, in inglese e pieno di "legalese". Il succo è: *se vuoi installare questo bellissimo sfondo, devi accettare che sul computer venga installato del software che ti mostrerà pubblicità, promozioni, offerte, e comunque il computer ti si rallenterà (incredibile, ma c'è proprio scritto), e il proprietario del software e tutti i suoi dipendenti, avvocati, soci, affiliati, parenti ed affini non saranno responsabili di nulla*.

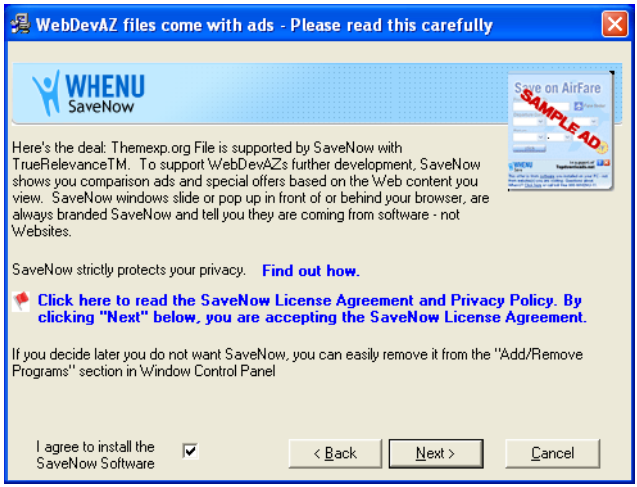
Già questo sarebbe un motivo molto più che sufficiente per non installare neanche un bit che venga da questo sito web, ma difficilmente leggiamo quanto viene scritto nelle licenze. Quindi andiamo avanti accettando le condizioni, tutte a nostro sfavore: ci viene chiesto di accettare l'installazione del primo software (Figura 8-8). L'applicazione è quello che viene chiamato un *search assistant*, che devia il browser ogni volta che tentiamo di andare su un sito che non esiste, o digitiamo parole chiave invece di un indirizzo web valido. Ci viene assicurato che grazie a questo sistema potremo accedere a contenuti per bambini e famiglie, e che il software può essere disinstallato. Però immediatamente sotto ci avvertono che se siamo minorenni o non siamo amministratori del computer, non possiamo proseguire. Siamo proprio sicuri che i siti siano per bambini?

Figura 8-8. Per installare un nuovo sfondo...



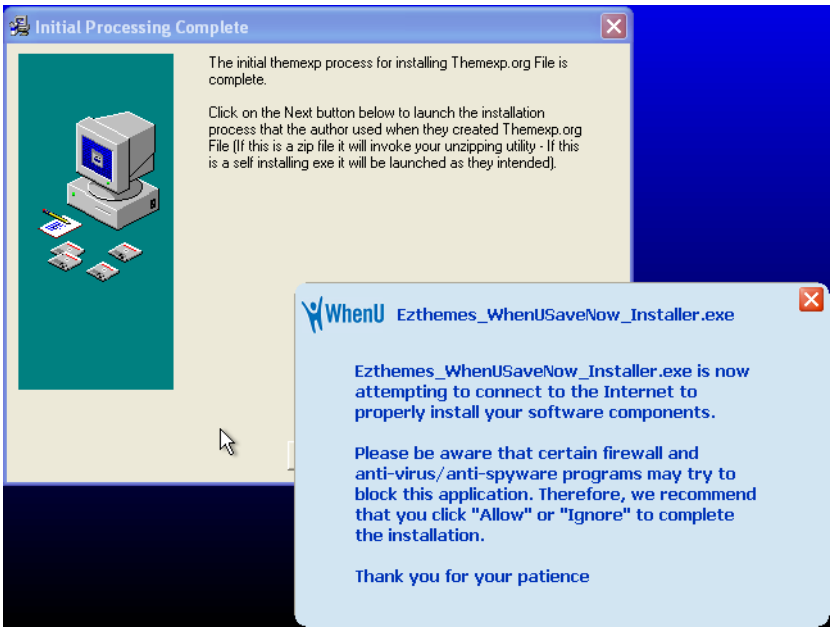
Accettiamo ed andiamo avanti, il pannello successivo invece ci presenta un software che durante la navigazione in Internet ci offre pubblicità di prodotti a prezzi vantaggiosi con la promessa di risparmiare sugli acquisti (Figura 8-9). Ci viene detto che è necessario, per sostenere nuovi sviluppi del software, accettare la comparsa di finestrelle davanti a quella del browser con pubblicità di prodotti e comparazione di prezzi. Anche qui la licenza è chilometrica, e contiene le stesse clausole che in sostanza ci chiedono di accettare che possano fare il loro comodo nel nostro computer senza essere ritenuti responsabili di nulla.

Figura 8-9. ...ma lo sfondo dov'è?



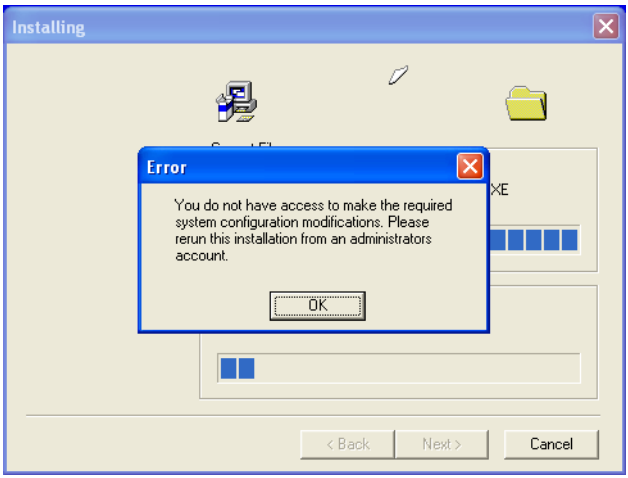
Accettiamo ancora, ed arriviamo al paradosso: ci avvisano (Figura 8-10) che il programma deve connettersi ad Internet, e che alcuni firewall, antivirus e antispyware lo bloccano pensando (giustamente, lo aggiungiamo noi) di aver a che fare con un malware, e ci avvisano di permettere al programma di uscire su Internet, altrimenti non potrà fare i propri comodi.

Figura 8-10. Si abbassi le braghe, prego!



Grazie al'uso di un account utente non privilegiato, il passo successivo, che dovrebbe portare all'installazione, si blocca con un errore (Figura 8-11), chiedendo diritti di amministratore. I diritti di amministratore *solo per installare uno sfondo!* Se non è sospetto questo...

Figura 8-11. Un amministratore per cambiare lo sfondo?



Se invece andiamo con un utente privilegiato, siamo nei guai. In breve tempo vengono aggiunti due programmi nascosti all'avvio del computer, due estensioni del browser, vengono inseriti siti web fra quelli attendibili. A parte queste operazioni, tutte silenziose e senza apparenti conseguenze per il funzionamento del computer, si nota un leggero calo di prestazioni. La comunicazione fra i programmi annidati nel computer e l'esterno è continua, e pur non andando a vedere che dati siano ricevuti e inviati, è evidente che tutto questo è fatto a nostra insaputa, in teoria, ma poco sopra abbiamo dato volontariamente il consenso all'installazione. Il problema è tutto qui: dare il consenso senza leggere cosa ci viene rifilato.

Gli antivirus non fanno una bellissima figura, di fronte a questo tipo di malware: solo sei identificano il programma come minaccia, uno pensa che sia un file rovinato, gli altri diciassette non notano nulla di strano.

I due antispyware non si accorgono di nulla. Nessun allarme, niente segnalazioni, neanche con la scansione approfondita.

Il gran finale: lo sfondo carino per il quale abbiamo subito tutto ciò, *alla fine non c'era*, il desktop era del solito colore blu di XP. Niente, neanche in giro per le cartelle immagini, né in quella di Windows o in quelle dei documenti.

Unica consolazione: tutto l'armamentario si può rimuovere dal Pannello di controllo, Installazione applicazioni. I due programmi installati si rimuovono senza obiezioni, e portano via tutte le loro cose. Anche questo in fondo è un predone gentile. Ma non tutti sono così.

Nessuna salvezza

Il sito in questione offre notizie su tutte le persone famose del momento, in particolare attori, rockstar, sportivi. Il sito in sé è pulito, il problema sono le pubblicità, di cui il sito è pieno. Basta entrare ed immediatamente parte l'attacco: sfruttando una falla nel linguaggio di script in Internet Explorer viene scaricato sul desktop ed eseguito un piccolo programma, di appena 5kbyte, dal nome `com.com`. In pochi secondi due programmi vengono scaricati, posizionati nella directory `C:\windows` ed attivati. Anche qui come nei casi precedenti gli stessi due programmi vengono inclusi fra quelli da far partire all'accensione del computer. I nomi cambiano (`mediacon.exe`, `sndman.exe` e `volumec.exe` per uno, `msncomm.exe` e `timed.exe` per l'altro) ma il risultato è sempre lo stesso, e li troviamo in esecuzione ad ogni avvio del computer.

La situazione è grave per vari motivi: colpisce sia utenti amministratori che utenti semplici; la presenza del *Service Pack 2* non cambia nulla, il malware colpisce lo stesso senza problemi; non occorre fare nulla per essere colpiti, basta visualizzare il sito web, non c'è bisogno di accettare download o installazione di controlli Active-X; l'unica impostazione che ne impedisce l'azione è la disabilitazione degli script in Internet Explorer, mentre l'uso di un utente non privilegiato limita il danno, compromettendo solo lo spazio di quell'utente; gli altri non vengono toccati, sempre a patto che XP sia installato usando il filesystem NTFS, altrimenti il malware aggira le protezioni e si installa nella directory di Windows.

Anche qui per gli antivirus è una vittoria di Pirro:

- Il file `com.com` è riconosciuto da 11 antivirus, 2 lo ritengono sospetto, gli altri 11 non trovano nulla.
- Il file `timed.exe` da circa 20 kbyte viene individuato da 14 antivirus in modo certo, uno lo indica come sospetto, gli altri nove non trovano nulla.
- Il file `sndman.exe` da 11 kbyte viene individuato solo da cinque antivurs, due lo segnalano come sospetto, gli altri 17 non trovano nulla.

Gli antispyware non fanno una bellissima figura: rilevano soltanto alcuni *cookies* impostati dal sito, uno dei quali serve ad evitare la duplicazione dell'infezione: se lo si toglie alla successiva visita del sito con Internet Explorer vengono scaricati e installati di nuovo i programmi, anche con nomi diversi, aggravando il danno invece di correggerlo.

L'unica soluzione che funziona veramente è l'aggiornamento di XP tramite Windows Update. Eseguendo l'aggiornamento da un utente amministratore, la falla in Internet Explorer viene chiusa, ed il sito web diventa innocuo.

In mancanza dell'aggiornamento di Windows Update, se abbiamo applicato fedelmente tutte le strategie elencate fino ad ora, il danno si limita ad un utente normale colpito. Nella situazione che va per la maggiore, invece, la situazione è molto più grave: l'utente amministratore è compromesso; il passaggio di antivirus ed antispyware non sortisce effetto, o peggio aggrava il problema; non avendo un backup aggiornato non è possibile cancellare tutto e ripartire da una situazione pulita, ma anche accettando la perdita di dati, dopo la reinstallazione di tutto alla prima visita del sito in questione si è daccapo.

Nella nostra situazione, il castello correttamente protetto e fortificato, il malware esaurisce la sua potenza distruttiva contro la seconda linea di difesa: utente con diritti limitati e permessi su directory e file; la terza linea di difesa ci permette di scoprire immediatamente i file annidati nella home directory dell'utente colpito, visibili nonostante si siano assegnati la caratteristica di file di sistema, ed eliminarli usando l'utente amministratore; se non fossimo in grado di trovare dove si è annidato il malware, la prima contromisura, il backup, ci dà la facoltà di usare le maniere forti: bonifica dell'area contaminata, la home directory dell'utente colpito, bruciando tutto per poi recuperare i dati di solo quell'utente dall'ultimo backup, che sarà del giorno precedente. Poi passiamo a chiudere le

falle con l'aggiornamento del sistema operativo. Da questo momento in poi questo metodo di attacco non ha più alcun effetto: abbiamo tagliato le gambe a tutta la famiglia di malware basati su questa specifica falla.

Tutte queste operazioni, si badi bene, sono eseguite con quello che viene messo a disposizione da XP, senza programmi da scaricare o strane alchimie con scanner antivirus o antispyware. E sono tutte operazioni che può fare un utente con un livello medio di conoscenza di XP. Non serve uno specialista per riparare il danno, ma solo perché *ci abbiamo pensato prima*.

Caramelle dagli sconosciuti?

Se siamo arrivati fin qui ed abbiamo ancora voglia di navigare su Internet, non rimane che fare il punto della situazione e provare a stabilire qualche possibile strategia di difesa.

Dovrebbe essere evidente che le contromisure più diffusamente applicate non sono assolutamente sufficienti a garantire l'integrità e la sicurezza del sistema operativo e dei dati: firewall, antispyware ed antivirus sono poco efficaci per i motivi mostrati nel corso del capitolo. L'unica strategia efficace nella quasi totalità dei casi è l'uso di un utente non privilegiato, cioè con i diritti "giusti" per il lavoro che deve fare. Un utente amministratore è una vera manna dal cielo per un predone.

Altra cosa che dovrebbe essere evidente è che la quasi totalità di questi predoni sono in qualche modo costretti a chiedere il nostro aiuto per fare danni: o perché dobbiamo scaricare e lanciare una applicazione, o perché dobbiamo cliccare su un pulsante Sì o Ok, devono chiedere aiuto a noi. Quindi, come tutti i truffatori, cercheranno sempre di prenderci alla sprovvista, offrendoci qualcosa che ci fa gola, o ingannandoci con qualche messaggio ben confezionato. Le offerte sono sempre basate sugli istinti più primordiali (sesso, denaro, paura, adulazione, empatia), non perché siamo tutti incivili, ma proprio perché più l'istinto è "basso", meno difese abbiamo. Tieni questo, *è gratis*. C'è una ragazza che vuole parlare *proprio con te*! Il tuo computer *è infetto*! Clicca QUI per vincere *il tuo premio*! Abbiamo bisogno *del tuo aiuto!*!

Studi autorevoli dimostrano che il meccanismo più efficace per commettere reati è l'inganno, attuato con tecniche ben precise che prendono di mira proprio quegli istinti primordiali che fanno parte del nostro bagaglio di esseri umani. Perché dover faticare per creare un sito web che sfrutti una determinata falla di Internet Explorer per iniettare un malware, quando si possono convincere le persone a scaricare ed installare *da soli* il programma?

C'è anche un altro vantaggio, sempre di ordine psicologico: la vittima ha difficoltà ad ammettere di aver aiutato il truffatore, seppur involontariamente ed in perfetta buona fede, proprio perché gli ha creduto: in molti casi la reazione della vittima, davanti alle prove della truffa, è di difendere l'operato del truffatore, almeno in un primo tempo. Eppure la credulità non è un male, ma anzi è un meccanismo di difesa perfezionato nel corso di tutta l'evoluzione. Possiamo immaginare una tribù di ominidi, dove uno dei componenti arrivi di corsa urlando a squarciagola per avvertire della presenza di un predatore: se il comportamento primario è diffidare (ma sei sicuro? Io non vedo nulla... Ma dove?) finiranno in breve tempo per essere pranzo di qualche carnivoro di grossa taglia.

Quello che dobbiamo imparare è che su Internet non dobbiamo fidarci di nessuno, esattamente come dicevano i nostri genitori quando uscivamo per andare al parco o dagli amici: non accettare caramelle da nessuno!

Se sembra complicato, forse lo è

Le cose che possiamo fare per rendere un po' meno vulnerabile il nostro esploratore sono abbastanza limitate, e sono tutte accessibili dal Pannello di controllo, Rete e connessioni Internet, Opzioni Internet. Le voci che ci interessano sono: Protezione (Figura 8-12) e Avanzate (Figura 8-13).

Figura 8-12. Le impostazioni delle "zone" di protezione

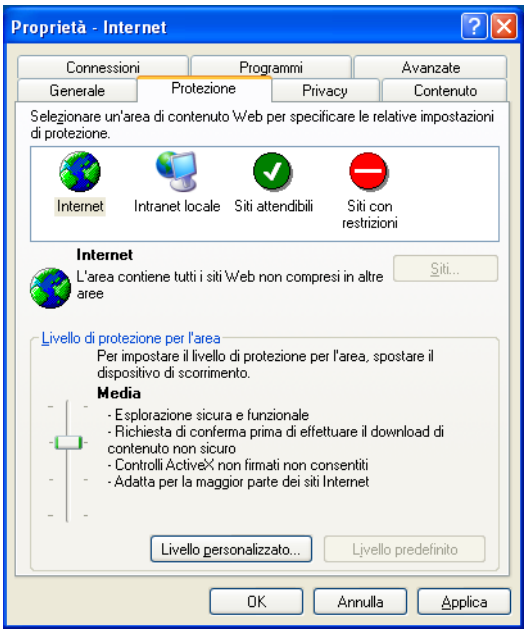
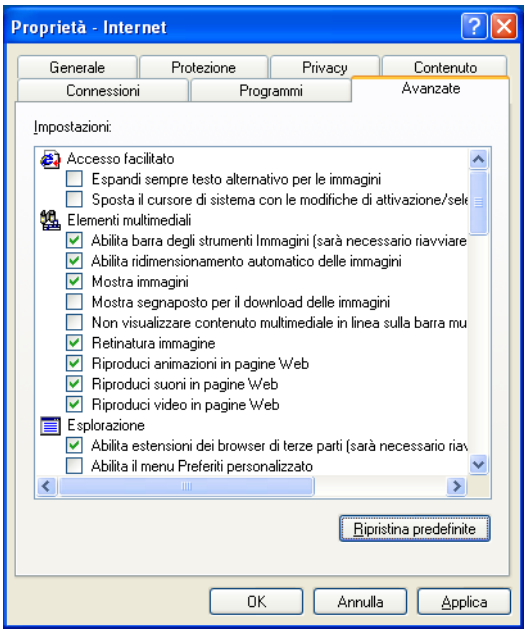


Figura 8-13. Le impostazioni avanzate



Le impostazioni valgono per utente

Tutte le impostazioni fatte in questo pannello sono relative al singolo utente attivo in quel momento. Se facciamo le modifiche da un utente, anche amministratore, queste non vengono propagate a tutti gli altri, per cui se abbiamo cinque utenti sul computer, ognuno avrà le sue impostazioni personali. Occorre tenerne conto quando si applicheranno le modifiche elencate nel seguito, da ripetere per tutti gli utenti. E' possibile modificare questo comportamento, ma ha i suoi pro ed i suoi contro.

Il pannello Protezione, già visto in precedenza (Figura 8-7), riporta quattro *zone*, cioè elenchi di siti web con differenti impostazioni. Da destra, la prima zona è quella dei siti che riteniamo assolutamente non affidabili; segue la zona dei siti affidabili, poi la zona con i computer della nostra stessa rete ed infine una zona jolly, per tutti i siti che non rientrano nelle altre categorie. Per ogni zona è disponibile un cursore che riporta quattro impostazioni di massima, ed un pulsante Livello personalizzato.... Premendolo si ottiene un ulteriore pannello con il dettaglio della configurazione (Figura 8-14), che può essere differente da zona a zona. Per prima cosa imposteremo la zona Internet con il cursore su Media, mentre la zona Siti con restrizioni avrà la protezione massima. Poi nella zona Internet modifichiamo alcune impostazioni critiche, riportate di seguito con le eventuali controindicazioni e le varianti per le altre zone:

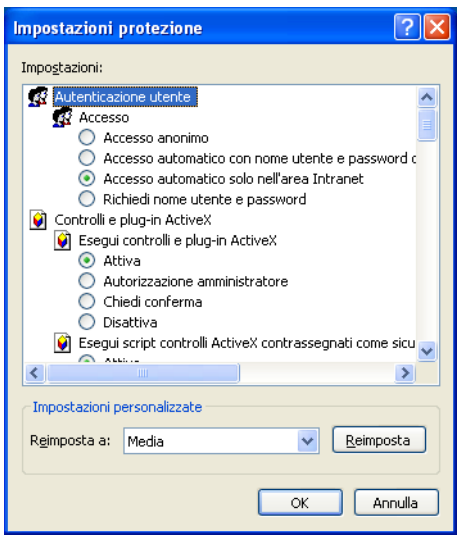
- Esegui controlli e plug-in ActiveX e Esegui script controlli ActiveX contrassegnati come sicuri - Sono normalmente impostati come Attiva. L'impostazione su Chiedi conferma causa l'apparire di un messaggio per ogni tipo di controllo ActiveX all'interno di una pagina web. Possiamo capire che la navigazione non è proprio comoda, ed in ogni caso cadiamo in quella che scherzosamente possiamo definire come "sindrome del click frenetico", in cui alla fine clicchiamo sui pulsanti di Ok senza neanche leggere, quindi è una precauzione alla fin fine totalmente inutile. Solo per la zona dei siti inattendibili li lasceremo su Disattiva.
- Inizializza ed esegui script controlli ActiveX non contrassegnati come sicuri - E' opportuno che sia impostato sempre su "disattiva". Solo le zone definite Intranet o Siti attendibili possono avere attiva questa voce, ma è comunque un azzardo. Se non abbiamo un sito interno particolare che richiede questa configurazione, è opportuno impostarlo su Disattiva in tutte le zone.
- Scarica controlli ActiveX con firma elettronica - Abbiamo visto che la presenza della firma elettronica attesta soltanto l'identità del fornitore (Sezione *Vieni a vedere cosa ho trovato!*), e che il testo che compare nel pannello di richiesta di download ed installazione è spesso usato per ingannare, quindi la migliore impostazione è di disattivare del tutto, soprattutto se le persone che

usano il computer non sono particolarmente "attente", o sono facilmente raggirabili (bambini, persone che non lavorano nel campo dell'informatica e simili). In questo non c'è alcuna accezione negativa o denigratoria, semplicemente si tratta di decidere se una persona con una cultura media all'apparire di un pannello del tipo di quelli visti è in grado di capire se è una trappola o meno, tutto qui. E dato che noi stessi possiamo essere presi da stanchezza, essere distratti o semplicemente aver fretta, è meglio metterci in una posizione di sicurezza. Solo per la zona dei Siti attendibili lo imposteremo su Attiva.

- Scarica controlli ActiveX senza firma elettronica - Tantomeno va attivato questo, a meno che non abbiamo un sito interno dell'ufficio o in casa che richieda il permesso di scaricare ed installare un controllo ActiveX non firmato, ma è una eventualità molto remota.
- Download dei caratteri - Capita di essere inviati su pagine web che per essere visualizzate necessitino di font particolari. Dato che spesso si tratta di siti in lingue con alfabeti non latini (cinese, coreano, giapponese, russo), che normalmente non sappiamo leggere, potrebbe non essere necessario scaricare font speciali. Anzi, potrebbe essere una ulteriore eventuale sicurezza: arrivati su un sito illeggibile è verosimilmente istintivo premere il pulsante Indietro nel browser, o chiudere la finestra.
- Download dei file - Se si disattiva non sarà possibile in nessun caso scaricare un file con il browser, neanche utilizzando il clic col tasto destro del mouse sul link. E' una impostazione abbastanza drastica, ma può essere utile per i bambini.
- Consenti operazioni di copia tramite script e Esecuzione script attivo - Abbiamo lo stesso scenario dei controlli ActiveX: se disabilitiamo tutto la quasi totalità dei siti web non sarà più utilizzabile, mentre l'impostazione di richiesta conferma trasforma la navigazione in un massacro del click. Possiamo lasciare su Attiva. Per la protezione conteremo di più sull'uso di utenti con diritti "giusti" e sugli eventuali aggiornamenti di sistema per chiudere le falle.
- Installazione oggetti del desktop - La possibilità di impostare direttamente da un sito web lo sfondo del desktop è comunque una porta aperta per il download e la scrittura di file all'interno del computer. Il consiglio è di impostare su Disattiva.

Queste impostazioni vanno bene per tutti gli utenti, indistintamente dal livello di privilegio. Per gli utenti amministratori possiamo lasciare il download di controlli ActiveX firmati, per permettere l'uso di Windows Update. Oppure possiamo inserire tutto il dominio Microsoft fra i siti attendibili, ma oltre ad essere una procedura complicata, non è detto che funzioni, dato che il sito da cui vengono scaricati gli aggiornamenti potrebbe cambiare per volontà di Microsoft, come è già successo al tempo dell'emergenza causata dal virus Blaster. Il miglior consiglio è sempre quello di usare un account utente non privilegiato per navigare, e di usare l'account amministratore solo per andare sul sito Microsoft.

Figura 8-14. La configurazione di una zona



Il pannello Avanzate (Figura 8-13) richiede le seguenti modifiche, anche queste da ripetere per tutti gli account utente:

- Abilita estensioni del browser di terze parti - Come sappiamo, le estensioni del browser non sono solo porte di ingresso per programmi di dubbia utilità, ma sono spesso usate da programmi "regolari". Il disabilitarle può rendere meno agevole la navigazione, e può impedire il funzionamento di programmi come la Google Toolbar™. E' questione di scelte, certamente la disabilitazione aggiunge una protezione in più, data la cattiva abitudine di molti malware di installarsi proprio come estensione.
- Abilita installazione su richiesta (altro) e Abilita installazione su richiesta (Internet Explorer) - Se il browser è correttamente configurato, non ha bisogno di molto altro per funzionare. Anche i plugin possono essere installati su nostra iniziativa, invece di vedersi presentare una richiesta al momento di entrare in un sito web. La regola è che dobbiamo decidere noi cosa e quando installare: se manca qualcosa vogliamo solo essere avvisati, niente iniziative da parte del browser.
- Verifica automaticamente aggiornamenti di Internet Explorer - Questa impostazione ha senso soltanto per gli utenti amministratori, visto che tutti gli altri non possono installare software di uso comune a tutti gli utenti.

Con questo abbiamo terminato le impostazioni aggiuntive, ma rimane da chiarire un aspetto: quanto sono efficaci le impostazioni viste fino ad ora?

Se un utente scarica volontariamente un programma e lo avvia, il programma potrà accedere e modificare le impostazioni per quell'utente stesso, rendendo inutili tutte le precauzioni e le modifiche fatte. Ovviamente, a meno di falle gravi o di utenti amministratori, il danno sarà limitato a quell'utente, ma ci sarà comunque.

Ad ulteriore aggravio della situazione, esiste la possibilità di disabilitare i pannelli visti fino ad ora, nascondendoli o impedendo la modifica delle impostazioni, tramite l'applicazione di criteri di protezione con la *Microsoft Management Console*, ma il blocco è solo verso modifiche volontarie dell'utente attraverso le interfacce grafiche. Un utente che apra l'Editor del registro, o un malware attivato dall'utente che acceda a quella parte di impostazioni potrà modificarle a piacimento. Quindi è comunque un grado di protezione insufficiente. Al limite si può usare per impedire ai bambini di modificarle, ma è comunque una misura debole, a meno di disabilitare l'editor del registro, ma anche qui c'è la tecnica per aggirare l'impedimento.

Dico io chi chiamare

Abbiamo visto che uno dei malware è in grado di far danni anche con un utente normale (Sezione *Servizi gratuiti... a pagamento*). Questo succede perché, per scelta di progetto, in XP gli utenti comuni possono configurare un collegamento a Internet privato. Ma questo apre la porta alla modifica da parte di malware dei collegamenti esistenti, o all'aggiunta di nuovi. Esiste un modo di impedire le modifiche al file, sfruttando i permessi (Sezione *Seconda linea di difesa ter: filesystem e permessi* nel Capitolo 4): dopo aver impostato i collegamenti ad Internet necessari a tutti gli utenti, o averne creato uno condiviso per tutti, si procede a bloccare l'accesso ad uno specifico file, togliendo il permesso di modifica e scrittura agli utenti normali, ovviamente usando un utente amministratore. In questo modo un dialer attivato da un utente che tenti di modificare questo file per insediarsi non riuscirà nell'intento.

Per poter applicare queste modifiche, occorre che XP sia installato su filesystem NTFS, che sia abilitata la gestione completa dei permessi (Sezione *Seconda linea di difesa ter: filesystem e permessi* nel Capitolo 4) e che siano visualizzati tutti i file nascosti e di sistema (Sezione *La terza linea di difesa: cosa mi nascondi?* nel Capitolo 4).

Il file, dal nome `rasphone.pbk`, appartiene alle impostazioni comuni a tutti gli utenti, nella directory:

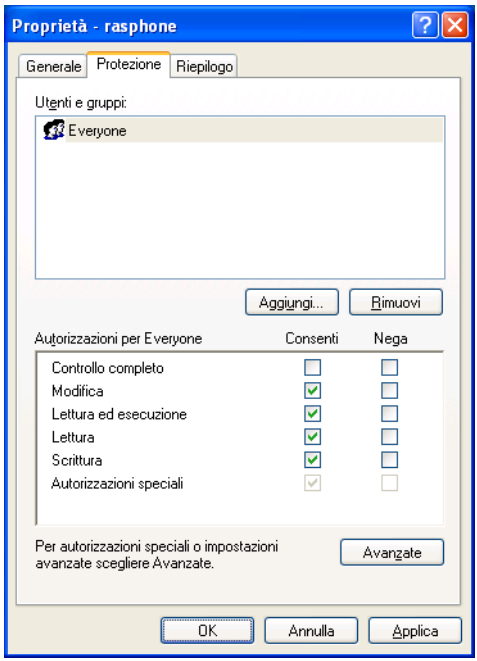
```
C:\Documents and Settings\All Users
```

ed è posizionato nella directory nascosta:

```
Dati applicazioni\Microsoft\Network\Connections\Pbk
```

Contiene tutti i dati dei collegamenti Internet via modem configurati da tutti gli utenti. Richiamando le proprietà del file, nel pannello Protezione vedremo un solo gruppo, Everyone (Figura 8-15), a cui sono assegnati permessi di lettura, lettura ed esecuzione, scrittura, modifica. Togliamo i permessi di modifica e scrittura, e confermiamo con Ok. Il file ora è intoccabile agli utenti normali.

Figura 8-15. I permessi sul file dei collegamenti Internet



Se tentiamo di avviare di nuovo il dialer visto prima (Sezione *Servizi gratuiti... a pagamento*), si blocca con un errore e non riesce a creare il collegamento a Internet. Se andiamo a vedere le proprietà di quel file dall'utente normale, troveremo che ha tutti i controlli di assegnazione dei permessi disabilitati, cioè l'utente non può modificare in alcun modo i permessi di accesso al file, e quindi acquisire la facoltà di modifica che consentiva al dialer di funzionare.

Non basta l'attributo generico di "sola lettura"

L'impostazione dell'attributo generico "sola lettura", presente nel pannello

delle proprietà generali, non è sufficiente a garantire la protezione completa, per un motivo molto semplice: questo attributo è modificabile a piacere da tutti gli utenti, per cui bloccheremo certamente i dialer più sprovveduti, ma nel momento in cui i creatori di questo malware dovessero avvedersi che si adotta questo accorgimento, per far funzionare di nuovo le loro creature dovranno soltanto controllare prima la presenza di questo attributo e cancellarlo se è impostato, dato che è una operazione non privilegiata su quel particolare file, modificabile da tutti gli utenti.

Diversamente, se l'amministratore toglie i permessi di modifica al file, gli utenti normali non potranno modificare il file, perché non hanno il livello di privilegio richiesto, anche se non ha l'attributo di "sola lettura".

Grazie alle funzioni di protezione proprie di XP, e senza programmini magici, siamo riusciti a tagliar fuori tutta questa specifica categoria di dialer. Se poi ignoriamo quanto detto fino ad ora e attiviamo un dialer da un utente amministratore, le modifiche tornano ad essere completamente inefficaci, ma questo dovremmo averlo capito.

Esplorare con il cervello

Concludiamo questo lungo capitolo riassumendo quanto abbiamo imparato. Chi costruisce malware conosce perfettamente tutti i meccanismi interni del funzionamento del sistema operativo, quindi non si può sperare di bloccarlo con strategie basate su impostazioni poco usate o poco conosciute. E' solo questione di tempo prima che il "segreto" sia scoperto e aggirato, quindi impostazioni come quelle mostrate, se applicate da sole, hanno una limitata efficacia. Abbiamo visto che un dialer ben fatto può creare una connessione via modem usando solo i diritti dell'utente standard. Poco dopo ci siamo resi conto di persona che esistono siti web creati apposta per compromettere i computer delle persone che li visitano. Siamo stati vittime, solo in modo virtuale, di piccoli raggiri che con un'esca molto semplice ci hanno convinto ad installare programmi certamente poco utili, se non dannosi. Ed abbiamo visto che per quanto possiamo tentare di proteggere il

nostro computer con configurazioni complesse e arzigogolate, queste impostazioni sono aggirabili dall'utente stesso senza troppa fatica, indipendentemente dalla sofisticazione.

L'unica strategia realmente funzionante si basa su due comportamenti assolutamente necessari:

- non navigare *mai* con un utente amministratore, se non per usare Windows Update
- non fidarsi di nessuno

in breve: teniamo acceso il cervello!

Non è una ipotesi fantascientifica che qualcuno possa compromettere un sito web affidabile e conosciuto per appestare i computer di tutti quelli che lo visitano. Il non fidarsi di nessuno deve includere anche il sito Microsoft...

Prima di salpare per l'oceano di Internet, accendiamo le nostre difese personali: scetticismo, buonsenso, realismo. Saranno i nostri dispositivi di navigazione, a prova di nebbia, scogli e pirati.

Capitolo 9. Antibiotico a largo spettro

Lo scanner antivirus, o più semplicemente antivirus, è la contromisura certamente più conosciuta, ma nel contempo la più bistrattata e male applicata. In effetti in questi ultimi anni i virus si sono molto evoluti, e come in tutti i lunghi conflitti vi è una continua *escalation* di attacchi, difese, contrattacchi e via dicendo: ogni nuovo metodo per scovare virus viene dopo qualche tempo aggirato e reso inefficace. La vita degli antivirus si è fatta molto difficile, e la responsabilità è in parte nostra. In questo settore il parallelo con gli antibiotici a largo spettro normalmente usati per la cura di noi esseri umani calza a pennello: l'abuso ed il cattivo uso di queste potentissime armi le ha rese progressivamente inefficaci, causando la selezione "innaturale" di nuove generazioni di batteri resistenti a molti tipi di antibiotici.

Allo stesso modo, l'uso poco accorto degli antivirus li rende inefficaci, ed i virus diventano immuni, trasformando uno strumento utilissimo, in molti casi insostituibile, in uno spreco di risorse di elaborazione. Vediamo di capire come funzionino, per poi renderci conto di quali siano i loro limiti e gli errori più comuni che li riducono ad un inutile peso.

Virus, firme e DNA

Il problema principale che si trova a dover risolvere un antivirus è: come distinguere un programma normale da uno dannoso. Non è un problema da poco, perché non esiste un metodo di programmazione, un algoritmo, tale che ci permetta di capire se un programma o un pezzo di programma sia capace di fare danni o no. Senza scendere in dettagli troppo matematici, ci viene in soccorso la *Teoria della computabilità*, che fornisce gli strumenti per decidere se un determinato problema sia appunto *computabile*, cioè risolvibile usando un computer. Il problema di decidere se un programma fa qualcosa di deleterio è della stessa categoria del problema di capire se un programma è errato o no. In parole povere *non è possibile in alcun modo* creare un programma che analizzando un altro programma decida in maniera definitiva se sia errato oppure no. Allo stesso modo non è possibile scrivere un programma che analizzandone un altro decida se sia dannoso in qualche modo. Fra l'altro rimane da definire anche *cosa si intenda con dannoso*, concetto molto più complicato di quanto possa sembrare.

Gli antivirus seguono una differente strategia, molto più affidabile: riconoscono i virus dalla presenza di specifiche sequenze di byte all'interno dei file in cui sono annidati, caratteristiche e uniche per ogni virus riconosciuto. Queste sequenze, chiamate *firme* (in inglese *signatures*), sono definite dal fornitore dell'antivirus, analizzando il codice del virus stesso ed estraendo una sequenza caratteristica di byte che per posizione e costituzione identifica in modo certo la presenza del virus, in maniera molto simile a quella usata per i virus biologici, la cui presenza si rileva da specifiche sequenze di DNA all'interno delle cellule infette. Ovviamente ogni virus ha la sua firma caratteristica e unica.

Questo metodo presenta, come sempre, punti di forza e inconvenienti: da un lato garantisce l'individuazione certa di virus conosciuti, prestazioni accettabili, semplicità di struttura del programma dello scanner antivirus; dall'altro può riconoscere i virus solo se ne possiede la specifica firma, non è in grado di rilevare varianti dello stesso virus, tranne in casi particolari, può segnalare per errore virus dove non ce ne sono (eventualità chiamata *falso positivo*).

Da questo discende che l'impegno del produttore dell'antivirus non si esaurisce con la sola creazione dello scanner, cioè del programma che analizza i file alla ricerca del DNA dei virus, ma deve creare e soprattutto mantenere aggiornato il database delle firme, senza il quale lo scanner antivirus è praticamente inutile.

Il laboratorio di virologia

Ogni produttore di scanner antivirus ha la necessità di allestire un laboratorio dove analizzare i virus e definirne le firme di riconoscimento. Questo è un impegno non indifferente e spesso costituisce il grosso degli investimenti, oltre a richiedere personale con elevate competenze.

La domanda principale è: come vengono in possesso degli esemplari di malware da cui poi ricavano le firme? Una delle fonti siamo noi, gli utilizzatori: professionisti del settore, amministratori di reti di computer, sistemisti di società grandi e piccole, che hanno la responsabilità della gestione di centinaia di computer e che sono spesso costretti a combattere con malware nuovi verso cui non hanno difese, ma hanno le competenze per distinguere un programma innocuo da un malware.

Alcuni dei produttori hanno addirittura una rete di trappole congegnate per attirare e catturare i malware direttamente alla fonte. Queste trappole altro non sono che normali computer dotati di programmi che simulano il comportamento di un utente: navigano, leggeno posta, scaricano file, insomma tutte le attività che di solito svolgiamo col computer. Per catturare campioni dei malware che si propagano per posta elettronica, dispongono di caselle di posta impiegate come esca, ricevendo messaggi con virus allegati.

Per quanto possa sembrare strano, è proprio questo il punto cruciale che rende un antivirus migliore di altri: la pronta risposta ai nuovi malware, con l'identificazione, la generazione delle firme di riconoscimento ed eventualmente il rila di programmi appositi per la riparazione dei danni inflitti dal malware ai computer che ne rimangono vittime, cosa non sempre possibile.

I produttori ne sono ampiamente coscienti, al punto che creano anche degli accordi di collaborazione fra loro per lo scambio dei campioni. Non solo, vengono anche stretti accordi con collaboratori "fidati" che fanno da raccoglitori dei campioni e li inviano tramite canali preferenziali.

Molti produttori incoraggiano gli utenti ad inviare i file sospetti per le analisi, assicurandosi una ulteriore fonte di materiale da analizzare, anche se con priorità inferiore.

Una volta in possesso dei campioni, persone con competenze molto particolari eseguono delle vere e proprie colture in ambiente controllato, studiando così il comportamento dei campioni inviati per l'analisi: in computer con vari sistemi operativi, con vari livelli di protezione, vengono eseguiti i programmi sospetti, e registrate accuratamente tutte le loro attività. Grazie a questo lavoro, delicatissimo, che richiede molta pazienza, vengono individuati e classificati i malware, ne viene stabilito il metodo di propagazione, il tipo di danno, le funzioni di mimetizzazione, e se possibile viene creato il programma di rimozione e riparazione. Infine vengono create le firme di riconoscimento, successivamente rilasciate per la distribuzione.

Il database del DNA

Una volta in possesso delle firme, create dal laboratorio di analisi, il produttore dello scanner antivirus rilascia un aggiornamento del database per permettere a quelli installati nei nostri computer di riconoscere le nuove minacce.

Questo database delle firme è gigantesco: è molto facile che ne contenga oltre centomila differenti, e spesso lo scanner è in grado di riconoscere varianti dello stesso malware con una singola firma. Questo database è quindi molto critico, e viene protetto sia da modifiche da parte degli stessi malware che dalla possibilità di furto da parte di altri produttori con pochi scrupoli: in fondo è la parte più preziosa dello scanner antivirus, che assorbe il grosso dei costi di produzione. Se si riesce ad entrare in possesso dell'intero database di un altro produttore si acquisisce in un colpo solo un patrimonio di anni di lavoro.

E' però anche vero che il valore di questo database diminuisce nel tempo, perché molti malware hanno vita limitata, e si estinguono ad esempio a seguito del rilascio di una patch per la falla che sfruttavano per propagarsi, o dell'abbandono del sistema operativo per cui erano stati pensati. Molti virus, ad esempio, sono spariti dalla circolazione con l'uscita di scena del sistema operativo DOS.

Di conseguenza buona parte delle firme contenute nei database degli antivirus sono ormai inutili, o quasi, vista la scomparsa dell'ambiente in cui prosperavano i virus a cui fanno riferimento. Quelle di valore sono soltanto le firme più recenti, quelle degli ultimi malware in circolazione.

Per questo motivo tutti gli scanner antivirus possiedono un meccanismo di aggiornamento, e richiedono che venga usato regolarmente. Inoltre, a differenza di qualche anno fa, i malware cambiano molto più in fretta, e l'aggiornamento deve essere tempestivo: un malware particolarmente aggressivo può fare il giro del pianeta in meno di mezzora, se si propaga direttamente via rete, in meno di una giornata se si propaga via posta elettronica, ma solo perché quando da noi apriamo la posta e attiviamo il malware allegato pensando che sia innocuo, dall'altra parte del globo è ancora notte: il malware sarà depositato nelle caselle di posta, in attesa di colpire al mattino.

Sempre, o su chiamata?

Andiamo a guardare un po' più da vicino il funzionamento dello scanner, anche per capire quali siano i suoi punti di forza, i suoi punti deboli e i motivi per cui un antivirus può essere più o meno efficace, più o meno pesante, più o meno invasivo.

L'antivirus scanner più semplice (per comodità lo chiameremo d'ora in poi solo antivirus) è quello su richiesta: si avvia il programma passandogli una lista dei file, di directory o l'intero disco da controllare. L'antivirus percorre tutto l'elenco ed analizza ogni file alla ricerca dei segni di presenza di un malware. Per maggiore efficienza non controlla tutti i file, ma seleziona solo quelli che per tipo e formato sono conosciuti per essere veicolo o vittima di malware. Si può comunque imporre il controllo di tutti i file, indipendentemente dal tipo. Per cercare la presenza delle firme non viene fatto un semplice controllo di corrispondenza delle sequenze di byte all'interno del file, anche perché comporterebbe il confronto di decine di migliaia di firme per ogni singolo file. Vengono usati metodi molto sofisticati, che ad esempio controllano se in un certo punto del file c'è un particolare valore, ed in base alla risposta scartano un intero gruppo di firme. Il metodo è in ogni caso *certo*: se la sequenza di byte c'è, viene rilevata *sempre*.

Il passo successivo è l'attivazione indiretta dalle applicazioni: il programma di posta elettronica che utilizziamo passa gli allegati dei messaggi all'antivirus per un controllo, prima di presentarceli. Oppure il browser può avere una estensione che passa all'antivirus ogni programma che scarichiamo da Internet, e lo rende disponibile solo se l'antivirus non rileva nulla di sospetto.

In questi due casi l'antivirus è molto leggero e poco invasivo. Non si intromette, si attiva solo se chiamato, non consuma continuamente risorse per controlli non richiesti.

Il passo ancora successivo è di agganciare un modulo al sistema operativo, e inserire la scansione antivirus in una serie di procedure che possono portare all'attivazione di un malware: lanciare un programma, inserire un floppy o un supporto removibile, aprire un documento, cliccare su un link nel browser, sfogliare la rete. Ogni singolo file che viene toccato dal sistema operativo o da una qualsiasi applicazione diventa oggetto di attenzione dall'antivirus. E' facile immaginare come questo comportamento sia molto invasivo, e sia causa di un

forte consumo di risorse. Questa particolare funzione viene chiamata protezione in tempo reale, con varie denominazioni commerciali a seconda del produttore, ma intendendo sempre la stessa modalità di scansione.

La protezione in tempo reale, la protezione per gli allegati di posta elettronica e la scansione su richiesta sono le tre principali funzioni di un antivirus, ma non sempre sono tutte necessarie, e, al solito, c'è un prezzo da pagare per ogni funzione aggiunta.

Reazioni immunitarie

Come il sistema immunitario umano, anche un antivirus non è infallibile, anzi, qualche volta fa più danni della malattia. Ricordiamo che è in ogni caso un programma, quindi come tutti i programmi è soggetto ad errori. Può contenere falle, può avere comportamenti imprevedibili, può essere incompatibile con altre applicazioni. Inoltre difficilmente convive con un altro antivirus.

Tanto per fare un esempio, tutti gli antivirus possono controllare i file anche se contenuti all'interno di un archivio compresso: in alcuni antivirus vi era un errore che li mandava in tilt in presenza di file compressi in un certo modo. Il risultato era che l'antivirus si sarebbe disattivato nel momento del controllo di quel file ed un eventuale malware sarebbe passato senza colpo ferire.

Può capitare che per un errore su una firma di un virus, l'antivirus segnali come malware file e documenti assolutamente innocui. I casi sono documentati ed hanno fatto molta sensazione (ci fu un caso in cui un noto antivirus segnalava come infetti file di note applicazioni o del sistema operativo, dettagli sul sito McAfee[1]), ma in fondo sono incidenti che possono capitare, vista l'estrema complessità dell'argomento e la criticità del fattore tempo: il rilascio degli aggiornamenti con le nuove firme deve essere il più rapido possibile, ed a volte la fretta gioca brutti scherzi.

Il succo del discorso è che anche l'antivirus, quale che sia, ha i suoi limiti, e non può essere visto come la soluzione unica e definitiva del problema malware.

1. http://vil.nai.com/vil/content/v_138884.htm

L'analizzatore portatile

Nel tentativo di fornire una "marcia in più", qualche produttore ha inserito una funzione particolare nel suo antivirus, chiamata *scansione euristica*. La sua azione è molto simile al laboratorio di cui parlavamo prima: il file sospetto viene analizzato in un ambiente controllato e chiuso, e in funzione di particolari indicazioni viene deciso se sia un malware o meno. E' chiaro che il tipo di analisi è piuttosto limitato, come pure le decisioni possibili, viste anche le risorse impiegate, ma se il sistema è ben fatto può dare utili indicazioni su malware nuovi e relativamente semplici.

I sistemi più sofisticati arrivano ad eseguire il programma sospetto in una sorta di "bunker" virtuale per capire cosa faccia, e se tenti di toccare parti vitali del sistema operativo.

Quanto detto va preso con le dovute precauzioni, perché proprio per questa caratteristica di analisi automatizzata le segnalazioni di potenziali malware a carico di programmi o file innocui potrebbero essere moltissime. Ad esempio quasi tutti i malware di ultima generazione vanno a modificare alcune voci del registro di sistema, ma lo stesso fanno molti programmi di installazione delle applicazioni, quindi operazioni che per un programma sono perfettamente legali non lo sono per altri, e il distinguere le due situazioni non può essere automatizzato.

L'analisi euristica si può quindi usare con molta cautela e solo su file già gravati dal sospetto di essere o celare un malware. Un'applicazione a tappeto, oltre ad essere onerosa, è sicuramente fonte di falsi positivi e di confusione.

Perché non ha funzionato?

Capita che una delle lamentele più frequenti sia su questo tono: il mio antivirus non aveva rilevato il virus X, ho installato un altro antivirus e mi ha trovato anche il virus Y.

Se abbiamo letto attentamente i capitoli precedenti, dovremmo avere la risposta: il virus X è entrato per mancanza di tutta una serie di accorgimenti, che avrebbero dovuto impedirgli qualsiasi accesso, è riuscito a installarsi e attivarsi nel computer, molto probabilmente sfruttando i diritti di un account amministrativo.

Il povero antivirus non aveva ancora le firme per riconoscerlo, una passata della scansione in tempo reale non ha trovato nulla di sospetto, quindi ha lasciato fare. A questo punto, avendo libero accesso al computer ed a tutti gli organi vitali del sistema operativo, il malware ha per prima cosa bloccato il sistema di protezione in tempo reale dell'antivirus, poi ha applicato alcune modifiche che vedremo fra breve per impedirgli di ricevere gli aggiornamenti delle firme. Una volta che il malware si è barricato dall'interno, l'antivirus installato nel computer non ha più modo di rilevarlo.

Installando un altro antivirus, di solito qualche giorno *dopo* l'intrusione del virus, questo avrà un database delle firme più aggiornato, ed all'attivazione troverà immediatamente il virus. Ignorando il motivo reale, apparirà chiaro che il secondo antivirus *è più potente* di quello installato nel computer, che viene disinstallato immediatamente con una espressione di disgusto dipinta in faccia.

Avendo però ignorato quanto sia realmente successo, a distanza di poco tempo anche il secondo antivirus sarà vittima dello stesso equivoco, e subirà la gogna e l'onta della cancellazione con disonore.

Il file HOSTS

Nell'elenco dei file bersagliati dai malware ce n'è uno in particolare che è fra i preferiti. Il file è `C:\windows\system32\drivers\etc\hosts`, un semplice file di testo il cui contenuto significativo è una sola linea che recita:

```
127.0.0.1           localhost
```

Il file serve ad assegnare una corrispondenza fra un nome ed un indirizzo IP in modo statico, un po' come un server DNS, ma visibile solo dal nostro computer. Se aggiungiamo una riga in questo modo:

```
127.0.0.1           localhost
192.168.41.152      mioserver
```

poi apriamo Internet Explorer e digitiamo **http://mioserver/**, il browser tenterà di connettersi al computer con indirizzo IP 192.168.41.152. I malware aggiungono righe in questo modo:

```
127.0.0.1           localhost
```

```
127.0.0.1          www.google.it
127.0.0.1          www.microsoft.com
```

Quale può essere il risultato? Quando tentiamo di contattare Google o Microsoft con il browser o con qualsiasi altro programma, il computer chiamerà l'indirizzo IP 127.0.0.1, che come abbiamo visto è il nostro computer. Non riusciremo più a raggiungere i due siti di Google e Microsoft.

I malware mettono in questo file i siti web da cui i produttori di antivirus distribuiscono sia i programmi che gli aggiornamenti: non riusciremo a scaricare più nessun antivirus, e quello che abbiamo non aggiornerà più il database delle firme.

Ovviamente i più attenti fra noi avranno capito che questo file è accessibile in modifica *solo agli utenti amministratori*, per cui gli utenti normali non possono toccarlo. Se il malware viene attivato con un utente non amministratore non potrà modificare questo file.

La sequenza installa/virus/disgusto/installane-un-altro si ripeterà fino a che un altro virus entrerà per la porta da cui tutti gli altri virus sono entrati, mai chiusa, ma stavolta sarà un virus di quelli veramente cattivi: non solo fermerà la scansione in tempo reale e l'aggiornamento delle firme, ma installerà un servizio di sistema che controllerà l'arrivo di altri programmi ed impedirà l'insediamento di qualsiasi altro antivirus e personal firewall noto; modificherà alcune chiavi di registro per impedire l'uso del Task Manager e dell'Editor del registro di Windows; modificherà il browser per impedire l'uso di motori di ricerca per non far reperire informazioni su Internet; bloccherà Windows Update per impedire gli aggiornamenti di XP. Poi cifrerà tutti i documenti presenti sul computer e ci mostrerà una finestrella con un messaggio sul genere di "se vuoi rivedere tutti i tuoi documenti, versa immediatamente 1000 euro su questo conto".

Se siamo spaventati è un buon segno. Non esiste ancora un virus simile, ma ne esistono molti che ci si avvicinano, e di parecchio:

- *Gaobot*. Abbiamo già fatto la sua conoscenza (Sezione *La seconda linea di difesa bis: password* nel Capitolo 4), ma non avevamo elencato tutte le sue *features*. Oltre 590 programmi differenti appartenenti agli antivirus e personal firewall più noti, se trovati in esecuzione, vengono terminati o ne viene impedita l'installazione; modifica il file `C:\windows\system32\drivers\etc\hosts` aggiungendo una quarantina di siti web di produttori di antivirus; cerca altri computer sulla rete e tenta di accedervi usando i nomi degli utenti connessi in quel momento, o attingendo da un elenco di 50 nomi utente e opera un attacco sulle password prelevandole da un dizionario di 170 elementi; si installa come servizio di sistema; si connette ad un server in cui chi ha creato il virus può controllarne il funzionamento, ed eventualmente inviare aggiornamenti del virus stesso; attraverso la stessa connessione invia tutti gli indirizzi di posta elettronica che trova nel computer ed i codici di registrazione delle licenze di alcuni programmi, se installati. Alcune varianti del virus possiedono la capacità di portare attacchi a siti web su comando, e di rimbalzare connessioni verso altri computer, col risultato che l'indirizzo IP del computer che contiene il virus sembra essere l'origine degli attacchi.
- *Ahker.b*, analisi completa sul sito Sophos[2]: l'elenco di programmi antivirus e personal firewall che conosce è di "solo" 350 elementi; modifica anche lui il file `hosts`, disabilitando l'accesso ad una combinazione di siti (Microsoft, Google, Yahoo, Symantec, CNN, ecc.); disabilita il Ripristino della configurazione di sistema, gli aggiornamenti ed il firewall di Windows, togliendo anche gli avvisi del Centro di sicurezza del PC; disabilita l'Editor del registro, Notepad, Write e Wordpad, il servizio di notifica degli aggiornamenti automatici, il Messenger di MSN; si autospedisce per posta elettronica a tutti gli indirizzi che trova nella rubrica di Outlook Express.
- *PGPcoder*, analisi completa sul sito McAfee[3]: diversamente da quello che suggerisce il nome, non ha nulla a che vedere con il noto programma di crittografia e firma digitale. Ha una sinistra caratteristica: aggredisce tutti i documenti che trova nel computer, cifrandoli con un algoritmo relativamente semplice. Poi nelle stesse directory dove sono i file modificati, crea un file con le istruzio-

2. http://www.sophos.com/virusinfo/analyses/w32ahkerb.html
3. http://vil.nai.com/vil/content/v_133901.htm

ni per rimettere a posto i documenti. Le istruzioni riguardano l'invio di un messaggio ad un indirizzo di posta elettronica per acquistare il decoder. Praticamente un ricatto.

Adesso dovremmo essere spaventati. Mettiamo insieme le caratteristiche di questi tre malware, e abbiamo uno di quelli cattivi.

Altra situazione paradossale che mi è capitata personalmente riguarda una funzione chiamata *quarantena*. Al rilevamento di un virus dobbiamo scegliere cosa debba fare l'antivirus del file che lo contiene: di solito cancellarlo o tentare la rimozione del virus. Nel caso si scelga la rimozione e l'antivirus non può farlo perché in effetti il file è il virus stesso, e non un file modificato dal virus, viene offerta la possibilità di spostare il file in una directory da dove non può fare danni, in attesa che decidiamo cosa farne. Ho visto personalmente directory di quarantena con 41.000 file *tutti dello stesso virus*. Il virus entrava, veniva riconosciuto dall'antivirus e messo in quarantena, ed immediatamente ne arrivava un altro dallo stesso computer, compromesso dal medesimo virus e costretto a comportarsi da untore, e finiva anch'esso in quarantena, e così via. Questo è un altro esempio, se mai ce ne fosse ancora necessità, di cosa porta l'affidarsi solo all'antivirus, quando invece andrebbe cercata e chiusa la falla che permette l'ingresso al malware.

Ora chiediamoci di nuovo: è veramente colpa dell'antivirus? O forse è un capro espiatorio per tutta una serie di problemi che sono a monte e che devono prima essere risolti, per poi permettere all'antivirus di fare il suo dovere?

Scanner antispyware

Gli scanner antispyware hanno un funzionamento molto simile a quello degli antivirus, solo che il tipo di malware oggetto delle loro attenzioni è differente, nel senso che fa danni di altra categoria, non che è meno dannoso. Ne abbiamo già visto alcuni esempi nel capitolo del browser (Sezione *Un secchio d'acqua per una goccia di olio* nel Capitolo 8).

Gli antispyware rivolgono la loro attenzione alle estensioni del browser, ad alcune parti del registro di sistema, alla configurazione della navigazione Internet. Ma, allo stesso modo degli antivirus, per trovare segni della presenza di qualche schi-

fezza hanno bisogno di un database con i segni distintivi degli spyware conosciuti. Il motivo è lo stesso di cui parlavamo sopra: il fatto che un programma modifichi alcune specifiche porzioni del registro di sistema, o si inserisca come estensione del browser, non è da solo sufficiente per affermare che sia un programma malevolo.

Di conseguenza anche per gli antispyware siamo nella stessa situazione degli antivirus: abbiamo bisogno di aggiornamenti tempestivi delle firme, e se un malware entra prima che siano disponibili siamo nella stessa condizione di pericolo.

Molti malware ora prendono di mira non solo gli antivirus ma anche gli antispyware, al solito terminandoli se sono in esecuzione o impedendone l'installazione, quindi il metodo migliore rimane la prevenzione, ossia impedire al malware di entrare ed attivarsi.

Voglio il migliore!

Se andiamo in un newsgroup o in un forum dedicato agli antivirus, e pretendiamo di sapere quale sia il migliore, è molto facile ricevere delle risposte poco gentili, ed a ragione. Dovendo acquistare un'automobile nuova, chiedere ai nostri amici e conoscenti quale sia la migliore si risolverà in una confusione totale. Il motivo è che solo noi sappiamo quali siano le caratteristiche che desideriamo dall'antivirus, e spesso molte sono in contrasto fra loro. Un'automobile non può fare trecento all'ora e consumare poco, né può trasportare cinque persone con i bagagli per un mese di vacanze sulla neve e parcheggiare in un fazzoletto. Quindi la domanda è posta male. Un quesito sensato può invece essere: esiste un antivirus per uso personale gratuito che abbia la scansione in tempo reale e il controllo degli allegati di posta elettronica? Oppure: ho un vecchio computer con poche risorse, esiste un antivirus che non sia troppo invasivo e che faccia solo il controllo su richiesta?

La risposta è affermativa per tutte e due le domande, e con un po' di pazienza si trova l'antivirus adatto. Ce ne sono per tutti i gusti, per tutte le esigenze e per tutte le tasche. Ve ne sono parecchi che permettono l'uso a scopo personale gratuito, senza altro vincolo di una registrazione via Internet con nome, cognome e indirizzo di posta elettronica. Ce ne sono con solo il controllo su richiesta, e con la scansione in tempo reale di tutto quello su cui mettiamo le mani. Ovviamente,

ve ne sono di complessi, con centinaia di funzioni, e di semplici che fanno lo stretto indispensabile. Ma se vogliamo un fuoriclasse non possiamo pretendere di averlo gratis, se vogliamo che controlli tutti i file su cui spostiamo la freccia del mouse non possiamo pretendere che sia leggero e consumi poche risorse.

Personalmente ho notato che alcuni antivirus hanno dei comportamenti che confondono e sgomentano chi usa il computer per lavoro e non è un informatico di professione, mostrando ad ogni aggiornamento del database delle firme un pannello a tutto schermo che *urla*, o avvisi minacciosi quando lo stesso database non è aggiornato da più di 24 ore. Ho visto persone rimanere impietrite senza capire cosa fare, domandandosi se sia tutto a posto o ci siano problemi. La semplice lettura della parola "Antivirus" le rende ansiose e incerte, ed un pannello che appare all'improvviso prendendo tutto lo schermo non facilita certo le cose. L'antivirus, come detto a suo tempo per il firewall, deve fare il suo lavoro in silenzio, e deve *agire* più che suonare l'allarme, e soltanto quando effettivamente il pericolo c'è.

Per un uso personale o in piccole reti di computer, a patto che vengano applicate tutte le contromisure elencate in questo testo, uso con molta soddisfazione ClamWin[4], un antivirus scanner con licenza Open Source, derivato dall'antivirus ClamAV[5], sviluppato per essere impiegato sui server di posta elettronica per filtrare i messaggi con virus allegati, bloccandoli prima che giungano a destinazione.

L'installazione è molto semplice e non pone particolari problemi. Il programma è distribuito senza il database delle firme, che va aggiornato al primo avvio dell'antivirus dopo l'installazione. E' dotato di un plugin di controllo della posta elettronica solo per Outlook (non Express), ma il funzionamento è molto discreto, leggero e poco invasivo.

Un uso efficace

Se abbiamo applicato tutte le contromisure elencate fino ad ora, e quelle che vedremo in seguito, l'antivirus avrà vita molto tranquilla, e dovrà intervenire solo

4. http://www.clamwin.com/
5. http://www.clamav.net

su nostra esplicita richiesta in pochi indispensabili casi:

- Controllo dei file scaricati da Internet. Ogni file proveniente da Internet dovrebbe essere controllato prima di essere dato in pasto alla relativa applicazione. Documenti di Word, di Excel, file compressi, filmati e brani audio dovrebbero essere tutti controllati prima del fatidico doppio clic. Nessun file è *sicuro*, tutti possono essere portatori sani di malware.
- Controllo di tutti i programmi scaricati da Internet prima di installarli o eseguirli, anche se provenienti da siti fidati. Può succedere (ed è successo) che un sito affidabile venga manomesso da qualcuno e infestato di malware, che poi verranno scaricati ed installati senza timore dalle vittime, ignare che il sito è stato compromesso. La prudenza non è mai troppa.
- Controllo di tutti gli allegati di posta elettronica prima dell'apertura. Nessuno escluso. Anche quella che sembra una semplice immagine può nascondere insidie. Ed il controllo deve essere fatto anche se il messaggio viene da persone fidate.
- Controllo di file e programmi ricevuti da amici e conoscenti, prima dell'apertura o dell'installazione, quale che sia il supporto su cui ci viene consegnato. Non perché la fonte sia dubbia, ma proprio perché potrebbe essere una vittima ignara anche il nostro amico.

In breve, tutto quello che entra nel computer, prima di essere avviato, aperto, attivato, deve essere al di sopra di ogni sospetto. Dopo è *sempre* troppo tardi. Ed ora che sappiamo anche il perché, quindi non abbiamo più scusanti o attenuanti. Se non lo facciamo è solo negligenza, pigrizia e incoscienza.

Capitolo 10. Il postino suona N-volte

La posta elettronica ha gradualmente preso il posto di altre forme di comunicazione, ed oggi costituisce buona parte del traffico di dati su Internet. Immancabilmente anche la posta elettronica è diventata una fonte di diffusione di malware, oltre ad essere veicolo per alcune forme di truffa.

Lettere e pacchi

In origine, la posta elettronica era pensata per l'invio di messaggi di testo, e prevedeva la possibilità di trasportare altri tipi di dati, opportunamente codificati, allegati al messaggio. Col tempo si è sfruttata questa possibilità per usare come formato dei messaggi altri tipi di codifica, principalmente HTML e RTF, per arricchire il contenuto e soprattutto la forma grafica dei messaggi. Oggi i messaggi possono apparire come una pagina di un sito web, con immagini, animazioni, suoni, e possono essere in una certa misura interattivi.

Come in tutti gli altri casi che abbiamo visto, ogni funzione aggiunta ed ogni "abbellimento" possibile viene sfruttato per divenire veicolo di propagazione di malware, e la posta elettronica offre una gamma notevole di oppotunità di nuocere.

Inoltre, dato il carattere personale e diretto, il messaggio è inviato *proprio a noi*, si presta all'applicazione di tecniche derivate dalla psicologia di comunicazione, in particolare quello che con un termine molto di moda viene chiamato *social engineering*, un termine tecnico che indica semplicemente l'arte di indurci a fare qualcosa con la persuasione o l'inganno.

Questo aspetto è aggravato quando il messaggio è in formato HTML, che consente di inserire anche del contenuto *attivo*, ossia in grado di compiere operazioni nel momento stesso in cui il messaggio è visualizzato per la lettura: praticamente è come aprire una lettera esplosiva. In Outlook Express ed in Outlook, come pure in molti altri programmi di posta elettronica, la visualizzazione del contenuto in HTML è operata attraverso lo stesso gruppo di funzioni usate da Internet Explorer per mostrare una pagina web, col risultato che la presenza di una falla in Internet Explorer spesso apre una falla anche in tutti i programmi che permettono di

visualizzare la posta in formato HTML.

Il genere di pericoli che può trasportare un messaggio di posta elettronica è molto ampio, e vanno dal semplice virus all'esca per una truffa, con una buona fetta di *spam*, la posta spazzatura che infesta le nostre caselle di posta con ogni genere di pubblicità di prodotti improbabili e servizi irriferibili.

Vedremo esempi per tutti questi pericoli con cui ci dobbiamo confrontare ogni giorno, vedremo cosa si può fare e quali difese e contromisure siano efficaci, mentre constateremo che con alcuni di essi l'unica difesa è il nostro buonsenso.

Aprimi, non aver paura...

La prima fonte in assoluto di pericolo sono gli allegati, per motivi non sempre puramente tecnologici. In tempi non remoti, la sola visualizzazione di un messaggio composto in modo particolare causava l'attivazione dell'allegato per un errore in Outlook, allegato che ovviamente era un malware. Chiusa questa falla, insieme a molte altre, i malware si sono evoluti verso forme molto meno tecnologiche, ma più efficaci: allegati che si presentano come innocui documenti o file multimediali da aprire, con icone rappresentanti immagini, filmati, brani musicali. Chi si trova davanti il messaggio non sospetta nulla ed apre l'allegato, attivando il malware.

L'inganno è operato anche su un altro fronte: se il messaggio viene da una persona conosciuta, cade la naturale diffidenza e si è più propensi ad aprire allegati senza troppe precauzioni. Una volta attivi, i malware di questo tipo collezionano gli indirizzi di posta elettronica dalle varie rubriche di contatti sparse per il computer e dalle pagine dei siti web che abbiamo visitato, per poi spedire, senza il nostro intervento, messaggi ingannevoli con l'allegato dannoso. Chi riceve il messaggio vede che il mittente siamo noi, ed apre messaggio e allegato senza sospettare che si tratta di una trappola.

Fino ai primi anni 2000 c'era un minimo di salvezza per la differenza di lingua: arrivando messaggi in lingua inglese da persone di lingua italiana, potevamo sospettare qualcosa, ma ora questa salvezza non c'è più, dato che i malware cambiano la lingua del messaggio in funzione della nazione a cui appartiene il destinatario, ricavata dall'indirizzo di posta elettronica.

Nel periodo di Natale 2004 un virus si presentava come un messaggio di auguri con allegata una cartolina. Se il destinatario aveva un indirizzo di posta elettronica terminante in *.it*, il virus creava il massaggio in lingua italiana, se finiva in *.es* lo creava in lingua spagnola, ed aveva anche la versione francese, inglese, tedesca, russa, svedese, insomma ce n'era per tutti. Il virus era denominato Zafi.D (analisi disponibile sul sito F-Secure[1]) e una volta attivato eseguiva le solite operazioni: terminare antivirus e firewall e cancellarne i file copiandoci sopra il virus stesso; impedire l'accesso al Task Manager ed all'editor del registro; predisporre una porta d'accesso per ricevere ordini dall'esterno; collezionare indirizzi di posta e spedire copie di se stesso senza passare dal programma di posta elettronica.

C'era ancora una salvezza: il mittente era la persona che aveva contratto il virus, e lo si poteva avvertire del problema. Molti server di posta con l'antivirus integrato avvisavano automaticamente il mittente di aver inviato messaggi con virus allegati. Poi i malware si sono adattati, ed oggi non usano più il mittente vero, ma lo falsificano prendendolo dalla stessa collezione di indirizzi fatta in precedenza, o generandolo casualmente, producendo due effetti: non è più possibile individuare chi ha contratto il malware, e nel caso di server che avvisano automaticamente il mittente, *viene avvisata la persona sbagliata*, che presa dal panico inizia a cercare virus sul suo computer, che invece è molto probabilmente pulito poiché non è lui il vero mittente.

Un successivo adattamento porta i malware a spacciarsi per server di posta che avvisano di non poter recapitare un nostro messaggio, che in realtà non abbiamo mai inviato, e ce lo rimandano indietro in allegato scusandosi per il disguido. Inutile dire che l'allegato non è un messaggio ma il malware stesso.

Altre tecniche, che coinvolgono sempre l'inganno, riguardano messaggi che ci accusano di aver fatto qualcosa di illegale. Ad esempio il virus Sober.K (analisi sul sito Symantec[2]), in una delle sue false e-mail si spaccia per un messaggio di richiesta informazioni proveniente dall'agenzia investigativa americana FBI che ci accusa di aver navigato in oltre 40 siti illegali, e chiede di rispondere alle domande contenute nel documento allegato; che non è un documento, ma il virus stesso. Qualcosa di simile faceva il virus Sober.C (analisi sul sito F-Secure[3]), che

1. http://www.f-secure.com/v-descs/zafi_d.shtml
2. http://www.symantec.com/avcenter/venc/data/w32.sober.k@mm.html
3. http://www.f-secure.com/v-descs/sober_c.shtml

ci ricordava l'illegalità dello scaricare musica e film con il *peer to peer*, ci avvisava che il contenuto del nostro computer era da considerarsi sequestrato come prova e in allegato mandava la lista dei file scaricati illegalmente. Che non era una lista, ma il virus camuffato da documento di testo.

Altra tecnica è quella di presentarsi come qualcuno che ci vuole dare una mano, come faceva lo stesso virus Sober.C visto or ora: si presentava come il messaggio di un *pirata buono* che durante una operazione non proprio legale si era imbattuto nelle prove che il nostro computer conteneva un pericoloso virus e ci mandava un programmino per eliminare il malware cattivo. C'è bisogno di dirlo che era il virus stesso, in allegato?

Un altro metodo è quello di presentarsi come un messaggio inviato a un'altra persona e recapitatoci per errore, contenente qualcosa di appetibile. Video divertenti, immagini "piccanti" di procaci donnine, falsi avvisi di aggiornamento di Windows, giochini, tutto fa brodo, basta che sia plausibile e ci induca ad aprire l'allegato.

In quasi tutti i casi l'antivirus è inutile perché il virus è sconosciuto, mentre il firewall fa molto presto una brutta fine, disattivato o reso inoffensivo dal virus. Rimane solo la corretta gestione dei diritti utente, al solito usando un utente non privilegiato per la nostra attività al computer, ed una buona dose di scetticismo: se il messaggio non è diretto a noi, oppure arriva da sconosciuti, o da persone note ma non sembra appartenere alla persona, per via dello stile e del contenuto, e soprattutto contiene allegati *vuol dire che siamo ad un clic dal disastro*: basta aprire l'allegato e il malware colpirà.

Banche, pesci ed esche

Una nuova categoria di minacce per la nostra tranquillità viene dalla possibilità di avere lo sportello bancario via Internet, cioè effettuare gran parte delle operazioni sul nostro conto corrente da casa, con un normale collegamento a Internet: il cosiddetto *home banking*. Per accedere occorre avere l'abilitazione del servizio da parte del nostro istituto di credito, oltre allo strumento scelto dalla banca stessa per l'accesso e l'identificazione. Il metodo varia, ma le caratteristiche di base sono le stesse: c'è un primo livello di accesso tramite una coppia nome/password

che ci viene fornita all'atto dell'attivazione del servizio, ed un secondo livello che deve essere usato quando le operazioni coinvolgono movimenti di denaro. Questo secondo livello di sicurezza è fatto con password particolari che possiamo usare una sola volta, ad esempio leggendole da un foglio prestampato, o da un generatore che visualizza sei-otto cifre casuali che cambiano ogni minuto, sempre fornito dalla banca.

Alcune banche richiedono questa ulteriore password solo per importi superiori ad un minimo, mentre altre lo richiedono per qualsiasi importo. Questa forma di identificazione è molto difficile da aggirare, a meno di falle nell'organizzazione dell'istituto bancario stesso. Per i malfattori questo non è un ostacolo, dato che più che i nostri soldi vogliono la nostra identità, intesa come nome, indirizzo e coordinate bancarie, da usare per i loro scopi. Inoltre, sfruttando proprio il fatto che non tutti gli istituti di credito richiedono la password aggiuntiva per tutte le operazioni di movimento di denaro, possono puntare a piccoli trasferimenti per un gran numero di conti bancari. Ma per far questo hanno bisogno di sapere la coppia nome/password di ingresso.

In una produzione cinematografica tipica la situazione sarebbe stata rappresentata con un personaggio, il classico supergenio cattivo del computer, che alla tastiera del proprio notebook, ovviamente dotato di qualche marchingegno di propria invenzione, avrebbe catturato le informazioni volute con un programma ultrasofisticato da lui stesso sviluppato. Nella realtà le cose sono molto più semplici, ed in un certo senso deludenti. Il malfattore si avvale del nostro tanto volonteroso quanto inconsapevole aiuto: siamo noi a fornirgli tutti i dati su un piatto d'argento.

La procedura è grossomodo questa: il malfattore crea un messaggio di posta elettronica particolare che invia a milioni di persone. Questo messaggio, infarcito con il giusto grado di termini tecnici, contiene una spiegazione plausibile anche se inverosimile, ed una richiesta specifica, che è la vera trappola. Più o meno il succo è questo: caro cliente, a causa di un rinnovo dei computer (di un potenziamento della sicurezza, di strani tentativi d'accesso fatti a nome nostro, insomma di un problema con qualsiasi cosa con un nome d'effetto) le chiediamo di confermare la sua identificazione con il nuovo sistema di accesso che può trovare qui (*questo è il link trappola*), grazie per la collaborazione. Il messaggio riporta il logo ufficiale della banca, sembra provenire proprio dall'istituto di credito ed il testo è in

lingua italiana. Dato che il malfattore non sa in anticipo chi ha un conto in quella banca, si affida al numero: mandando cento milioni di messaggi è statisticamente molto probabile imbroccare le caselle di posta di molte persone che ne sono effettivamente clienti.

La trappola è proprio nel link, che non porta affatto sul sito della banca, ma porta sul sito del malfattore che ha creato una pagina di accesso identica in tutto e per tutto a quella della banca, con le due caselle dove inserire nome e password. Se digitiamo i nostri dati in queste due caselle siamo fritti, abbiamo consegnato i nostri dati di accesso al conto bancario ad uno sconosciuto che non ne farà un uso benevolo, almeno per noi.

Ci sono poi varie finezze impiegate dal malfattore per non far capire che non siamo sul sito della banca: nascondere l'indirizzo, camuffarlo, usare falle del browser per mostrare un indirizzo invece di un altro, oltre ovviamente ad una serie di altri trucchi per non essere scoperto, ma questo non ci interessa.

La stessa tecnica può essere impiegata per ottenere l'accesso a servizi online, come le aste, la stessa posta elettronica, gli accessi a siti che richiedono la registrazione per offrire un servizio. Lo scopo è di entrare in possesso dell'identità digitale di qualcuno per poi sfruttarla a scopi truffaldini. Ad esempio se il malfattore riesce ad avere i dati di accesso alla nostra posta elettronica può mandare messaggi effettivamente a nome nostro, e sarà poi difficile dimostrare che non siamo noi gli autori.

Questa modalità di truffa è chiamata *phishing*, un termine intraducibile che si pronuncia in modo identico a *fishing*, pescare, perché come nella pesca si getta alla cieca una grossa rete dove sicuramente rimarranno impigliati i poveri pesci.

Il motivo principale per cui questo sistema funziona, è una combinazione di fattori psicologici e di tecnologia: la richiesta di aiuto, o la minaccia di bloccare l'accesso ad un servizio spingono a fare quanto viene richiesto, e la possibilità di usare HTML per il messaggio permette di nascondere il contenuto del link, completando l'inganno. Ecco perché da molti viene consigliato l'uso del testo semplice per il contenuto dei messaggi: le stesse aziende si stanno adeguando, perché è molto più difficile nascondere cose in un testo semplice, che non può avere per definizione un contenuto attivo, diversamente dal formato HTML.

I link nei messaggi di posta sono anche un metodo per indurre le persone a visitare un sito con lo scopo di diffondere malware. A partire dalla prima metà del 2006 hanno preso a circolare messaggi che usano tutti i metodi visti qui e nel paragrafo precedente per indurre chi li riceva a cliccare su un link all'interno dei messaggi stessi, solo che il link non porta al falso portale di una banca, ma a siti trappola che tentano di infilare malware attraverso il browser. Il contenuto dei messaggi varia: un avvocato che minaccia le vie legali invitando a rimandare un documento firmato (disponibile al link); un invito a vedere dei filmati divertenti sul sito (link verso il sito trappola), dove una volta arrivati al momento di scaricare i filmati ci viene detto che occorre un driver per aprire il filmato, disponibile su un altro sito (il driver è il malware vero); un'amica anonima che ci accusa di essere dei porci (link alle foto di una nostra ipotetica malefatta visibili su un sito web, che invece cerca di rifilarci un virus). La tecnica è sempre la stessa: incuriosire, spaventare, fare appello ad istinti primari come il sesso e l'avidità, usare la leva del senso di colpa, per indurre chi riceve il messaggio ad andare su un sito web che contiene la trappola.

Spam spam spam spam

Il nome viene da una scenetta del *Monty Python's Flying Circus*, in cui due poveretti in un ristorante ascoltano il cameriere che elenca il menù, in cui tutti i piatti contengono dosi più o meno massicce di *spam*, un tipo di carne in scatola, e tutti i loro sforzi per ottenere qualcosa senza questo ingrediente sono vani. Esattamente come succede con la pubblicità che piove a quintali nelle nostre cassette postali, che è impossibile da rifiutare, allo stesso modo ogni giorno nelle nostre caselle di posta elettronica piovono messaggi pubblicitari di prodotti verso cui non abbiamo alcun interesse e servizi che non ci verrebbe mai in mente di fruire. Ma non possiamo rifiutare, restituire o impedire la consegna di questi messaggi.

Anche se a prima vista non sembra una minaccia per la sicurezza, nasconde problemi gravi ed insidie subdole. Si è calcolato che il traffico generato da questi messaggi costituisce una fetta consistente di tutti i messaggi di posta elettronica recapitati ogni giorno (alcune stime parlano di oltre il 60%), e che il carico di alcuni server di posta è costituito quasi totalmente da spam. Il fenomeno è complesso, e non è ben chiaro quale sia il vero guadagno di questi individui, dato che

il ritorno è veramente minimo: si parla di un cliente guadagnato ogni centomila messaggi inviati, una cifra veramente irrisoria. Ma questo non ferma gli *spammer* (termine che indica i malfattori che generano spam).

I prodotti e servizi più pubblicizzati sono:

- medicinali venduti tramite carta di credito, attraverso siti web che dichiarano di praticare sconti consistenti per via della vendita di farmaci generici, cioè non di marca. Il problema maggiore è che nessuno garantisce i prodotti, e dato il metodo con cui viene fatta la pubblicità, personalmente non mi sentirei tanto tranquillo.
- ausili sessuali, come pillole miracolose per aumentare le prestazioni sessuali o ingrandire "certe parti". Qui, oltre ai dubbi espressi sopra per i medicinali, c'è anche da chiedersi cosa si stia effettivamente comprando.
- prodotti dietetici. Come sopra, occorre domandarsi cosa effettivamente si acquista, e soprattutto quali siano le garanzie.
- lauree universitarie senza frequenza e senza esami. Si tratta di università sconosciute che assegnano diplomi di laurea semplicemente dietro pagamento di un compenso. Ovviamente non hanno alcun valore effettivo, e sono più una truffa che un vero titolo.
- software a prezzi stracciati. Si tratta in realtà o di software pirata, quindi privo di qualsiasi valore, o di particolari licenze che però non potrebbero essere vendute in questo modo, per cui non hanno valore legale: anche pagando il software si viola comunque la licenza.
- prodotti di lusso: orologi, cravatte, borse, penne stilografiche. Sono tutti prodotti contraffatti, repliche di bassissima qualità, il cui prezzo è alto anche per una replica.
- siti per "cuori solitari": dietro la facciata spesso si nascondono sfruttamento della prostituzione e pornografia.
- notizie di borsa: vengono diffusi bollettini in cui si millantano previsioni di crescita per titoli praticamente privi di valore, consigliando massicci acquisti con la chimera di facili guadagni. Ovviamente il valore di questi bollettini è

meno che nullo, visto che si corre il rischio di acquistare azioni che non valgono nulla.

In generale i siti web pubblicizzati hanno una vita brevissima, pochi giorni, per via della palese illegalità in cui operano.

La domanda che dobbiamo avere sempre in mente è: che garanzie può offrire un sito pubblicizzato con un metodo, quello dello spam, indice della assoluta mancanza di scrupoli? Usare la nostra carta di credito, fornire i nostri dati personali (indirizzo, coordinate bancarie) ad uno sconosciuto che ha un comportamento certamente non all'insegna della trasparenza non è il massimo della prudenza.

NO SPAM, please!

E' possibile in qualche modo combattere lo spam? Occorre accettare il fatto che è praticamente impossibile impedirlo alla fonte, oggi, per via del modo in cui è generato: gli spammer usano i computer di tanti ignari utenti di Internet, compromessi da un malware su cui hanno il controllo e che operano come spedizionieri. Il virus annidato in questi computer riceve una lista di indirizzi, il messaggio da inviare ed esegue la spedizione, usando un suo programma interno, quindi senza passare per il normale programma di posta elettronica. Se i server di posta ufficiali riconoscono questi computer ed iniziano a rifiutare l'invio dei messaggi in arrivo, agli spammer basta propagare il virus su altri computer, o usarne un altro gruppo di quelli già compromessi, e ripartire con l'invio. Spesso gli spammer hanno a disposizione gruppi di decine di migliaia di computer compromessi da sfruttare, quindi sia il volume di messaggi che il numero di spedizionieri è in grado di sfondare qualsiasi barriera. L'unica possibilità sarebbe di impedire ai virus di prendere possesso dei computer, ma al momento è piuttosto difficile. Speriamo che la lettura di questo testo serva a qualcosa...

Il secondo problema riguarda l'uso del nostro indirizzo di posta elettronica: da dove viene prelevato? Lo trovano su Internet. Basta fare una ricerca usando il nostro indirizzo: newsgroup, siti web personali, mailing list, forum, son tutte fonti per reperire milioni di indirizzi validi, usando un programma automatizzato chiamato in gergo *harvester* (raccoglitore, mietitore). E' questo il motivo per cui molti

servizi come forum e mailing list nascondono o camuffano gli indirizzi di posta elettronica degli utenti, come forma di protezione.

Gli spammer, a fronte di questo ostacolo, si sono adattati ed invece di collezionare indirizzi dal web li generano, usando un metodo abbastanza semplice: conoscendo i domini di provider, di siti che offrono la posta elettronica gratuita, di aziende, ed avendo a disposizione un elenco di cognomi e nomi comuni li combinano in vari modi, spedendo un messaggio per ogni indirizzo generato: il server di posta corrispondente risponderà con un errore quando l'indirizzo non esiste, mentre accetterà l'invio se esiste un indirizzo coincidente con quello generato. Avendo a disposizione migliaia di spedizionieri *senza alcun costo* non hanno nessun problema di prestazioni o di tempo.

Configurando i server di posta elettronica per non rispondere in caso di indirizzo inesistente, viene a cadere per gli spammer l'indicazione di aver raggiunto un indirizzo valido, ma anche qui esiste la corrispondente strategia, anzi ne esistono due. La prima è di includere nel messaggio un indirizzo o un link a una pagina web per permettere al destinatario di cancellarsi dalla lista di invio: scrivendo all'indirizzo indicato o inserendo il proprio indirizzo sul sito, pensando di essere cancellati, confermiamo invece allo spammer di aver imbroccato un indirizzo valido. L'altra strategia è di includere nei messaggi, confezionati in formato HTML, un link a una piccola immagine, di un solo pixel, da visualizzare all'apertura del messaggio. Il link contiene un codice che identifica il nostro indirizzo, generato casualmente, negli archivi dello spammer: nel momento in cui apriamo il messaggio e il programma di posta elettronica va a chiedere l'immagine al sito dello spammer, gli comunica anche il codice, confermando di aver trovato un indirizzo, e dato che qualcuno apre il messaggio, è un indirizzo valido.

In definitiva, non c'è modo di impedirlo in origine, e non c'è neanche la possibilità di proteggere il nostro indirizzo di posta, perché comunque lo spam arriverà. L'unica possibilità è quella di eliminare tutti i computer compromessi dai virus asserviti agli spammer, ma non è semplice. L'unica possibilità rimasta è quella di ignorarla quando arriva.

Filtri, chiavi e liste

Lo spam non costituisce un problema fin quando non supera una certa quantità, oltre la quale diventa faticoso distinguere i messaggi buoni dal marasma di quelli inutili. A questo punto occorre un automatismo affidabile che possa distinguere almeno in linea di massima i messaggi buoni dallo spam, ma, come possiamo immaginare, anche qui diventa una lotta perenne fra metodi per riconoscere e trucchi per aggirare.

Il metodo più semplice è quello dei filtri: un filtro altro non è che una regola applicata ad ogni messaggio in arrivo che permette di fare alcune operazioni in base alle caratteristiche del messaggio, come mittente, oggetto, parole nel messaggio, presenza di allegati. In origine i filtri erano pensati per organizzare la nostra posta, ad esempio per spostare i messaggi provenienti da una mailing list in una cartella dedicata.

L'impiego di filtri come rilevatori di spam è in realtà una estensione, ed ha avuto vita piuttosto breve. Nei primi tempi era sufficiente crearne uno che trovando parole particolari nel testo del messaggio lo cestinasse. Gli spammer si sono immediatamente adattati scrivendo i messaggi in modo differente, spezzando le parole o scrivendole con errori di ortografia in modo da aggirare i filtri: se la parola era *sesso*, gli spammer la scrivevano *ses so*, con uno spazio in mezzo, oppure *sess0* con lo zero al posto della ultima vocale, oppure *sezso*. E' impossibile prevedere tutte le perverse varianti di una parola, per cui i filtri basati solo sulle parole chiave non funzionano praticamente più.

Stessa fine hanno fatto i filtri sul mittente, le cosiddette *blacklist*: tutti i messaggi provenienti dagli indirizzi in questa lista vengono rifiutati. Anche le *whitelist* hanno subito la stessa sorte: accettare messaggi solo dai mittenti contenuti in una specifica lista. Dato che il mittente è facilmente falsificabile, ed i server di posta non hanno modo di verificarne l'autenticità, ora il mittente viene generato a caso, rendendo inutili le blacklist, o viene messo il nostro indirizzo, sfruttando il fatto che è sicuramente in whitelist.

Il passo successivo è quello di verificare il server di partenza, che non può essere falsificato: alcuni siti web su Internet forniscono la lista aggiornata dei server di posta noti per aver inviato spam, se il messaggio proviene da uno di questi

è altamente probabile che sia spam. Ma anche qui c'è la possibilità di aggirare l'ostacolo: avendo a disposizione molti computer con virus all'interno che fa da spedizioniere anonimo, è facile cambiare il computer di origine ogni pochi messaggi, senza quindi superare la soglia che fa classificare un computer come server di spam, oppure una volta perso un computer per via della identificazione spammer, basta usarne un'altro.

Il modello di filtro attualmente più efficace usa invece una strategia differente: oltre ad includere tutte le regole elencate fino ad ora, ne applica molte altre che riguardano l'aspetto del messaggio stesso: il formato usato (testo o HTML), se include immagini, se contiene caratteri in lingue straniere, se ha mittente palesemente fasullo, se il nostro indirizzo non compare nelle intestazioni. Inoltre usa una sofisticatissima analisi che permette al programma di controllo di apprendere, passandogli esempi di spam ed esempi di messaggi buoni. Questo particolare metodo è chiamato *filtro bayesiano*, dal nome del matematico settecentesco Thomas Bayes. Questo tipo di filtri si basa su metodi statistici e prevede l'adattamento, cioè la capacità di cambiare il proprio comportamento in funzione del verificarsi di eventi nuovi. Ad esempio se improvvisamente gli spammer iniziano a mandare messaggi composti in un certo modo, e indichiamo questi messaggi come spam, il filtro bayesiano aumenterà il punteggio per tutti i messaggi che hanno questa caratteristica. Da quel momento in poi ogni messaggio composto nello stesso modo avrà un punteggio di probabile spam più alto.

E' importante capire che questi filtri funzionano su base statistica e probabilistica, quindi possono indicare come spam messaggi buoni e viceversa. Inoltre, vista l'estrema capacità degli spammer di adattarsi, un filtro tende a funzionare per poco tempo, poi lo spammer cambia il modello dei messaggi e siamo daccapo. Inoltre i filtri bayesiani presentano una elevata complessità, quindi richiedono molte risorse, sia come memoria che come capacità di elaborazione.

In conclusione, lo spam è purtroppo un fastidio con cui dobbiamo convivere, ma almeno non rendiamo la vita troppo facile a questi signori: se abbiamo un indirizzo gratuito, scegliamo un nome non facilmente prevedibile (il tipico nome.cognome@server.it è indovinato in brevissimo tempo dagli spammer); non pubblichiamo sul nostro sito personale l'indirizzo di posta come link, ma se possibile come immagine in cui viene scritto l'indirizzo, per non farlo trovare dagli

harvester; allo stesso modo dobbiamo camuffarlo quando scriviamo messaggi nei newsgroup; controlliamo e pretendiamo che il nostro indirizzo sia protetto quando scriviamo nei forum o nelle mailing list; se arriva dello spam, non rispondiamo né andiamo a chiedere di togliere il nostro indirizzo dalla loro lista, visto che invece andiamo a confermare che non solo l'indirizzo esiste, ma che qualcuno legge anche lo spam; configuriamo il nostro programma di posta elettronica per non andare a prendere immagini o altro contenuto dal web quando apriamo un messaggio; se il nostro programma lo prevede, usiamo un filtro antispam.

Lo spam arriverà comunque, è praticamente inevitabile, ma almeno non renderemo il lavoro facile a questi rompiscatole. Infine, un pensiero molto personale: usare lo spam per pubblicizzare un prodotto è quanto di più idiota possa esistere, per il semplice fatto che obbligarmi a leggere un messaggio pubblicitario per un prodotto a cui non sono interessato non mi farà certo cambiare idea e correre a comprarlo. Quindi lo spam è del tutto inutile, proprio come il cosiddetto *cold call marketing*, il chiamare qualcuno al telefono per informarsi se serve un certo prodotto: per caso il nostro medico ci chiama tutti i giorni per informarsi se serve il suo intervento? Ma, ripeto, è un pensiero assolutamente personale, e non dissuaderà certo uno spammer dallo spedire duecento milioni di messaggi per un prodotto che forse venderà a venti persone.

Opportunità da mancare

Sempre per rimanere in tema, esistono delle truffe piuttosto ingegnose che usano la posta elettronica come veicolo per agganciare il "pollo". Ne vediamo alcuni esempi, analizzando il meccanismo, e scherzosamente assegneremo un punto per ogni caratteristica del messaggio esca che lo rende sospetto: se supereremo i tre punti, vuol dire che il messaggio è con buona probabilità un tentativo di truffa.

Il nigeriano generoso

Un bel giorno ci arriva un messaggio da uno sconosciuto, pezzo grosso di una banca, o avvocato (dice lui) di un ex funzionario di un governo, o parente di un ex pezzo grosso, che con tono molto confidenziale ci racconta una storia plausibile, a prima vista, e, sapendo che siamo persone affidabili, chiede il nostro aiuto

per "sdoganare" una consistente somma di denaro, dichiarando di essere disposto a ricompensarci per il disturbo, di solito con una fetta generosa del malloppo. Il messaggio termina con un invito urgente a comunicare il nostro indirizzo, il numero di telefono e di fax, le nostre coordinate bancarie.

Vediamo cosa dice il nostro manuale antitruffa: qualcuno di sconosciuto chiede aiuto (1 punto, sollecitazione ai buoni sentimenti); lo sconosciuto dice di essere un pezzo grosso (1 punto, falsa autorità); il messaggio afferma che siamo persone affidabili (1 punto, tentativo di guadagnare fiducia con l'adulazione); ci offre dei soldi, tanti per l'aiuto (1 punto, tentativo di far leva sull'avidità); occorre agire in fretta (1 punto, tentativo di non far riflettere usando l'urgenza); ci vengono chiesti dati personali piuttosto riservati (1 punto, tentativo di ottenere informazioni). In totale sei punti: il campanello d'allarme suona, è certamente una truffa.

La trappola scatta dopo che abbiamo risposto mostrando interesse e disponibilità: per qualche motivo ci saranno sempre problemi risolvibili solo dietro un nostro anticipo in denaro: ci verrà detto che serve per "ungere" qualche funzionario, per richiedere un documento, per sbloccare una pratica o una scusa simile. Alla fine, quando ci avranno spillato tutto il denaro che siamo disposti ad anticipare a fronte di un possibile guadagno milionario, spariranno senza lasciare traccia.

Questo tipo di truffa è chiamato *truffa nigeriana* (in inglese *nigerian scam*), in quanto i primi truffatori si presentavano come rifugiati politici in qualche modo correlati alla guerra civile di quel paese, che fra alterne vicende non conosce pace da decenni.

Il sito web Scam-o-rama[4] raccoglie tutti i casi conosciuti di tentativi di truffa appartenenti allo stesso genere, e dei tentativi delle potenziali vittime di mettere nel sacco i truffatori, con un pizzico di umorismo. Ma c'è poco da scherzare: il governo americano ha dovuto emettere dei bollettini per avvertire i propri concittadini di non cadere nella trappola. Ci sono persone che hanno perso centinaia di migliaia di dollari, ed altri che nel tentativo di recuperare il denaro direttamente in Nigeria sono stati uccisi dai truffatori. Quindi attenzione: si parla di individui privi di scrupoli.

4. http://www.scamorama.com/

Fra l'altro, conoscendo le leggi italiane sui movimenti di denaro e quelle internazionali per contrastarne il riciclaggio, è piuttosto difficile far transitare milioni di dollari dentro e fuori l'Italia con semplici trasferimenti fra banche: legalmente sarebbe impossibile fare le operazioni richieste dai truffatori.

Ne esistono numerose varianti, tutte comunque che parlano di tanti soldi che giacciono da qualche parte, e in tutte le varianti siamo chiamati a fare da ponte per il recupero del denaro.

Uomo fortunato!

Un messaggio arriva *urlando* nella nostra casella di posta: abbiamo vinto milioni di dollari, sterline, dobloni, sesterzi e chi più ne ha, a una lotteria nazionale! Il nostro indirizzo di posta elettronica è stato selezionato per essere abbinato al biglietto che ha vinto il primo premio. Per reclamare il nostro premio occorre contattare al più presto il funzionario della lotteria ad un indirizzo per comunicargli i nostri dati: indirizzo, telefono, fax, coordinate bancarie.

Il manuale antitruffa dice: qualcuno ci vuole dare milioni di dobloni (1 punto, leva dell'avidità o del guadagno facile); il qualcuno dice di essere un funzionario della organizzazione che gestisce la lotteria (1 punto, falsa autorità); occorre agire in fretta (1 punto, metter fretta per non far riflettere); chiedono nostri dati riservati (1 punto, tentativo di ottenere informazioni); l'indirizzo di posta elettronica da contattare non appartiene all'organizzazione ufficiale della lotteria, cioè il server di posta è di solito di un fornitore di caselle di posta elettronica gratuite (1 punto, un organismo statale non ha un suo dominio? Molto improbabile). Totale 5 punti: è truffa.

La trappola è identica a quella vista prima: ci saranno sempre dei problemi per ottenere i soldi della vincita, e occorrerà anticipare soldi nostri, che finiranno in tasca a qualcuno che si dileguerà nel nulla appena capirà che sentiamo puzza di bruciato.

Ora, il buonsenso dovrebbe per prima cosa farci riflettere sul perché la notizia che il nostro indirizzo di posta è abbinato ad una lotteria ci giunge sempre *dopo* l'estrazione del premio. Per seconda cosa, riflettere sul come sia possibile vincere

senza giocare. Questi individui non vanno minimamente sottovalutati, quindi mai rispondere, né tantomeno comunicare dati personali.

Un lavoro facile facile

Il messaggio è di un manager di una società giovane e dinamica, e recita (qualche volta nell'italiano zoppicante dei traduttori automatici, ma sempre più messaggi sono in italiano perfetto) che se siamo disponibili per un lavoretto facile, possiamo guadagnare soldi extra. Il lavoro è di tipo manageriale, occorre prendere decisioni in fretta. Non occorre altro che un indirizzo di posta elettronica che consultiamo abitualmente, ed un contro corrente bancario gestito via Internet per i movimenti di denaro. Occorre fornire indirizzo, telefono, fax, coordinate bancarie.

Vediamo il manuale antitruffa: soldi facili (1 punto, leva del guadagno facile o dell'avidità); manager o funzionario (1 punto, falsa autorità); occorrono doti da manager (1 punto, tentativo di abbassare le difese con l'adulazione); tentativo di acquisire informazioni (1 punto); nessuna domanda su precedenti lavori, né sul tipo di competenze specifiche richieste (1 punto). Il totale è basso, solo quattro punti, ma è senza dubbio truffa.

Il sistema è usato dagli stessi che adoperano il phishing (Sezione *Banche, pesci ed esche*) per ottenere accesso all'home banking. La procedura è più o meno la seguente:

- dopo essere penetrato nella gestione del conto di qualche malcapitato, vittima del phishing, il malfattore apre un conto bancario on-line con i dati personali di una delle vittime, sfruttando la possibilità offerta da alcuni istituti di credito di aprire conti accettando come "identificazione" soltanto le coordinate di un altro conto bancario.
- dai conti bancari di altri malcapitati sposta piccole somme sul conto corrente di chi risponde all'annuncio per il lavoro, e via posta elettronica gli comunica i dati del conto appena aperto su cui trasferire il denaro
- quando ha raggiunto la somma voluta, o prima di essere individuato dalle forze dell'ordine, il truffatore preleva tutto il contante che è riuscito a spostare

e lo trasferisce all'estero usando uno dei servizi di spedizione del contante e sparisce nel nulla

Per essere precisi, si tratta più di un furto che di una truffa, ma chi accetta il "lavoro" si trova invischiato in un reato piuttosto grave: riciclaggio di denaro.

I soldi provenienti dal furto su un conto bancario transitano sul nostro conto, per poi finire, "ripuliti", sul conto gestito dal truffatore, che è a nome di una persona che non ha niente a che vedere con la truffa. Alla fine, quando le forze dell'ordine arrivano, il ladro e truffatore si è dileguato, lasciando noi e l'ignaro titolare del conto, aperto dal truffatore, a spiegare ad un giudice come mai soldi rubati sono finiti nel nostro conto bancario. Ovviamente del truffatore e ladro non vi sarà traccia e dovremo dimostrare di aver agito in perfetta buona fede, ma sarà molto difficile.

Ne esistono varianti che parlano di fare da ponte per i pagamenti dei clienti di una multinazionale emergente che ancora non ha filiali dalle nostre parti, o di professionisti che debbono riscuotere denaro da clienti che hanno difficoltà a mandarlo direttamente a destinazione per motivi tanto fantasiosi quanto inverosimili. Il metodo è sempre lo stesso: vogliono il conto bancario di qualcuno che sia "pulito" dove far transitare i proventi di qualche malefatta per ripulirli.

Il copertone farcito

Solita e-mail: in una operazione di alto valore etico, ma sempre riguardante problemi di sesterzi, qualcuno ha nascosto un milione di dollari in un copertone d'auto per non destare sospetti, e lo ha spedito tramite corriere a un'altra persona. Chi ci scrive è il funzionario di una agenzia realmente esistente, e che sta operando in incognito, usando un indirizzo di posta privato. La persona che doveva ricevere il copertone pieno di soldi ha avuto un problema (morta, trasferita, il pacco è bloccato alla frontiera per problemi doganali, ecc.), ed occorre in fretta qualcuno di affidabile che si presti per ricevere il pacco per poi recuperare il milione di dollari, di cui può trattenere una parte. Occorrono il nostro indirizzo postale, il nostro telefono e fax.

Vediamo il manuale: operazione a fini umanitari (1 punto, appello al buon cuore); ci scrive il funzionario (1 punto, falsa autorità); occorre qualcuno di affidabile (1 punto, tentativo di guadagnare fiducia con l'adulazione); occorre agire in fretta (1 punto, metter fretta per non far riflettere); ci regalano soldi (1 punto, appello a guadagno facile o all'avidità); servono i nostri dati (1 punto, tentativo di acquisire informazioni). Il totale è sei punti, truffa sicura.

La truffa è ingegnosa: non ci chiedono soldi, ma solo un indirizzo dove deviare una consegna. La truffa scatta alla ricezione del pacco, che è gravato da un contrassegno di alcune centinaia di dollari. Ovviamente, visto che dentro il pacco (che non possiamo aprire senza prima pagare il corriere) c'è un milione di dollari, pagheremo senza battere ciglio. Il pacco contiene appunto un vecchio copertone, vuoto, o al più pieno di ritagli di giornale per fare peso.

Campanelli d'allarme

Chiudiamo qui questa breve carrellata sull'argomento, anche se ci sarebbe ancora molto da dire. Esistono delle caratteristiche comuni a tutti questi metodi di truffa, che occorre essere pronti a individuare, per non caderne vittima:

- Sono in ballo molti soldi. Proviamo a ragionare al contrario. Abbiamo tanti soldi a disposizione su un conto bancario a cui non possiamo accedere per qualche motivo. Secondo quale astruso ragionamento possiamo pensare di darli ad uno sconosciuto reperito su Internet, nella speranza che li restituisca tutti meno il cinque percento? Possiamo pensare che sia una grande trovata?
- Chi scrive spesso lo fa adducendo motivi gravi per non poter disporre direttamente del denaro: perché è in un campo profughi, o è esiliato in un'altra nazione. Ed ovviamente ha a disposizione un collegamento Internet, una linea telefonica, e spesso anche un telefono satellitare? Strano campo profughi.
- Altre volte dichiara di essere un pezzo grosso di qualche governo o organizzazione. E' possibile che non sappia a chi rivolgersi? Un politico, soprattutto se di una nazione con gravi problemi di stabilità, ha tantissimi agganci dentro e fuori dal suo paese. E deve rivolgersi proprio ad uno sconosciuto?

- Un funzionario di banca, abile abbastanza da far uscire milioni di dollari da un conto bancario "inattivo" senza farsi scoprire, che ha bisogno di appoggiarsi ad uno sconosciuto, per di più mettendogli in mano un mucchio di soldi senza alcuna garanzia. Che razza di banca gestisce?
- Nei messaggi praticamente sempre si parla di confidenzialità, segretezza, riservatezza. Per come è oggi, la posta elettronica è forse il mezzo meno confidenziale in assoluto, soprattutto in nazioni con problemi di salvaguardia dei più elementari diritti umani. In più, quasi mai il messaggio è diretto, ma ha tutte le caratteristiche tipiche di quelli spediti ad una lista immensa di indirizzi.

Insomma, per chiudere: se ci troviamo davanti un messaggio di uno sconosciuto che promette soldi facili, deve immediatamente squillare un campanello d'allarme. E', sotto altra forma, lo sconosciuto che offre caramelle, avvelenate come sempre.

E' vero! L'ha detto mio cugino...

E' capitato a tutti, prima o poi. Arriva un messaggio da un conoscente che afferma di recare notizie estremamente importanti e si chiude quasi invariabilmente con l'invito a diffondere il più possibile il verbo.

Il contenuto dell'avviso varia, ma riguarda in generale questi argomenti:

- Un virus terribile si aggira per la rete - Gli appelli parlano di ipotetici virus che sarebbero in grado di fare i danni più disparati, compresi danni *fisici* al computer, come rompere il processore o il disco fisso. Oltre ad essere totalmente falso, non serve proprio a nulla, visto che i virus sono troppo veloci per essere battuti sul tempo da un avviso diramato in questo modo. L'unico virus di cui si abbia notizia che sia effettivamente capace di fare danni al computer era quello denominato Cernobyl o CIH (analisi sul sito Cert[5]), che poteva in certe condizioni cancellare il BIOS in alcuni specifici modelli di computer, in modo da renderli totalmente inutilizzabili. Il computer colpito non partiva più,

5. http://www.cert.org/incident_notes/IN-99-03.html

mostrando uno schermo nero all'avvio, senza dare alcun segno di vita. Non era un danno fisico vero e proprio, ma costringeva chi ne era colpito a rivolgersi all'assistenza qualificata.

- Qualcuno regala oggetti o soldi se si fa qualcosa. In particolare il metodo riguarda l'invio del messaggio ad un numero minimo di persone, a seguito del quale un nome noto dell'industria, del commercio o dei servizi, tracciando i messaggi spediti per verifica, regala un oggetto o soldi. E' un metodo totalmente impossibile, dato che non esiste un sistema (legale) di tracciamento della posta elettronica. Alcune varianti promettono soldi, altre un telefonino di ultima generazione, altri ancora una ricarica telefonica. In qualche caso, per rendere più credibile la favoletta, avvisano di mandare copia dei messaggi ad un determinato indirizzo di posta elettronica, che sembra appartenere a qualcuno che rappresenta effettivamente l'organizzazione in vena di regali. Di solito o è un indirizzo inesistente, o è la casella di qualche malcapitato, vittima di uno scherzo di cattivo gusto.
- Qualcuno ha bisogno del nostro aiuto. L'appello cita rare malattie o gravi problemi di salute, tali che servono trasfusioni di sangue o donazione di organi. Pochi di questi appelli sono veri, la maggior parte è falsa, o peggio scaduta. E' il caso di un padre, che usò questo metodo disperato alla ricerca di un miracolo, putroppo non verificatosi. Ad anni di distanza dal tragico appello, continua a ricevere messaggi di persone che offrono il loro aiuto, rinnovando all'infinito un dolore terribile come può essere quello della perdita di un figlio, per via di qualcuno che, incomprensibilmente, rimette in circolazione copie del messaggio prive della data originale.
- Un appello umanitario. I fatti riguardano persone che stanno per essere giustiziate o che subiscono maltrattamenti, oppure animali trattati in modo barbaro e incivile. L'azione proposta dall'appello è la raccolta di firme per posta elettronica, operazione priva di qualsiasi valore. Spesso l'appello è corredato di immagini, o di link a siti web. Nella maggioranza dei casi sono storie totalmente inventate, o burle di cattivo gusto.
- Complotti politici o dei servizi segreti. I fatti dell'11 settembre 2001 sono i preferiti nel momento in cui scrivo. I sostenitori della teoria del complotto sembrano aver ragione per il semplice fatto che usano un ragionamento circolare:

il complotto c'è ed il fatto che non si trovano prove lo dimostra, dato che qualcuno le ha nascoste, insabbiate, falsificate. Intendiamoci: non ci interessa qui sapere se il complotto esiste o meno, ma non sarà certo con un messaggio contenente affermazioni campate in aria e senza alcuna prova che si sveglieranno le coscienze.

Prima di premere il pulsante Inoltra nel nostro programma di posta elettronica, facciamo un breve controllo sul sito web di Paolo Attivissimo[6], consultando le sue preziose indagini *Antibufala*. Poi decideremo, ma quasi sempre si risolverà con il cestinamento del messaggio.

La regola è di ignorare ogni messaggio che termini con l'appello di inoltrare la comunicazione a tutti quelli che si conoscono. Inoltrare senza documentarsi è un comportamento inutile, irritante ed incivile.

Catene scatenate

Durante la Prima Guerra Mondiale presero a circolare lettere che invitavano a pregare per la pace, contenenti l'invito a farne copie e distribuirle a più gente possibile. Negli anni 50 circolavano lettere che iniziavano con la frase "Recita tre Ave Maria a Sant'Antonio" e poi l'invito a continuare la catena minacciando improbabili sventure se la si interrompeva. Dato che l'invito era di spedire "a tutti quelli che si conoscono", la diffusione era spesso elevata. Il fenomeno delle e-mail che riportano simili inviti ha guadagnato lo stesso nome, *catene di santantonio*, anche se il contenuto varia.

Il flagello si presenta anche per gli SMS e per altri sistemi di comunicazione, dato che per la distribuzione conta sulla credulità o su altre leve come la superstizione o i buoni sentimenti. La differenza con gli appelli visti in precedenza è che non c'è un motivo particolare a scatenare la catena, ma un semplice messaggio che augura fortuna se si continua la catena e sventure se la si interrompe. Tutto qui.

Penso che non sia necessario aggiungerlo: l'inutilità di queste lettere a catena è palese, come palese è la credulità di chi le perpetua.

6. http://www.attivissimo.net/

Il comportamento da tenere è lo stesso degli appelli visti poco sopra, semmai più deciso e diretto: cestinare. Per i curiosi, Paolo Attivissimo, sul suo sito web già citato, riporta alcune delle più diffuse, mentre il sito web Chain Letters[7] ne riporta un campione storico. Unica eccezione può riguardare le versioni umoristiche, che facendo al verso alle catene "vere" diffondono storielle divertenti, ma alla lunga stancano anch'esse.

C'è il postino, apro?

Per ridurre i rischi di contrarre malware, di rimanere sommersi di spam o di essere truffati, possiamo adottare alcune strategie che a costo di un minimo disagio iniziale, ci possono poi aiutare a leggere i nostri messaggi senza l'ansia addosso. Molte le abbiamo già viste strada facendo: allegati da considerare sempre pericolosi; link nei messaggi da non cliccare mai; non credere ad avvisi che la nostra banca non ha mai mandato; impedire agli spammer di avere troppo facilmente il nostro indirizzo; non credere ai colpi di fortuna, rimanendo vittime di un truffatore.

Un aiuto viene dalla scelta del metodo di gestione della posta, che si riduce a due possibilità: usare un programma che scarica la posta sul nostro computer o usare un servizio di *webmail*, cioè il servizio messo a disposizione da molti siti web che offrono una casella di posta gratuita, con tanto di controllo antivirus e filtro per lo spam incorporato.

Nel primo caso tutto il lavoro di prevenzione dobbiamo farcelo in casa, quindi il programma di gestione della posta dovrà essere affiancato da un antivirus che controlla gli allegati, o eseguire noi manualmente il controllo prima dell'apertura, e di un filtro antispam da tenere aggiornato. Nel secondo caso il lavoro viene svolto dal gestore del servizio, a noi rimane solo il compito di tenere acceso il cervello, per i motivi che sappiamo.

Se scegliamo di farci il lavoro in casa, esistono molti programmi ottimi sotto tutti gli aspetti, a pagamento o gratuiti, che incorporano funzioni avanzate come il filtro antispam. Uno di questi è Thunderbird[8], completamente gratuito anche

7. http://www.chainletters.net/
8. http://www.mozilla.com/

per usi aziendali. Possiede un sofisticato sistema antispam con filtri bayesiani, un sistema per impedire agli allegati di aprirsi senza il nostro specifico consenso, un metodo per impedire a chi tenta una truffa con il phishing di camuffare gli indirizzi verso cui vorrebbe deviarci. La posta è conservata in semplici file che è facile sottoporre a backup e ripristinare, il cui formato è noto e disponibile a tutti.

Se invece preferiamo lasciare il lavoro al servizio di posta, sceglieremo un gestore che offra sia il servizio antivirus che il servizio antispam. Ovviamente questo non ci farà dimenticare le più elementari regole di comportamento, come aprire allegati o cliccare link nei messaggi senza fermarsi prima a pensare.

Se confidiamo sempre nella magia tecnologica per essere salvati dal pericolo, saremo prima o poi delusi e scottati: i malfattori sono sempre un passo avanti a tutte le diavolerie automatiche. L'unica cosa che non possono e non devono a fare è impedirci di *pensare*. Ma questo sta a soltanto a noi.

Capitolo 11. Tenere la destra

Saper guidare l'auto non basta. Per circolare sicuri, e avere una qualche garanzia di arrivare a destinazione tutti interi, dobbiamo rispettare delle regole di comportamento, che nello spirito servono a impedire il crearsi di situazioni di pericolo che portano a incidenti. Un buon comportamento di guida, fra l'altro, diminuisce il consumo di carburante e l'usura di motore, freni ed altri organi meccanici, oltre ad alleggerire lo stress di conducente e passeggeri.

Usare il computer, sia su Internet che non, richiede delle regole di comportamento della stessa natura, ossia tese a diminuire il rischio di farsi male o di danneggiare le nostre cose. Queste regole non nascono semplicemente perché qualcuno si è svegliato una mattina e ha deciso di mettere un po' di divieti a caso, tanto per complicare la vita alle persone o per limitarne la libertà, ma scaturiscono dall'esperienza, spesso acquisita a proprie spese, e dal conoscere il comportamento e le motivazioni dei malfattori, sempre in agguato e sempre pronti a cogliere le occasioni che la nostra distrazione, la nostra pigrizia o il nostro non sapere mette loro a disposizione.

Ricapitoliamo brevemente le principali regole, dettate dalla nostra conoscenza dei pericoli circolanti in rete e dal riconoscere con un po' d'umiltà le nostre stesse cattive abitudini.

Sii ordinato

Il nostro computer, semplicemente perché è nostro, spesso diventa un deposito rottami, in senso non solo metaforico: software installati e mai usati, file sparsi per tutto il disco, icone che coprono tutto il desktop, ciarpame mai buttato "perché non si sa mai".

La pratica comune di essere amministratori permette di scrivere file a caso in tutto il computer, anche in punti che normalmente non dovrebbero essere toccati, col risultato che fare un backup è impossibile. Un altro brutto vizio è quello di installare tutti i programmi su cui mettiamo le mani, anche senza sapere se ci serviranno mai, o magari solo perché li abbiamo. Il sistema operativo in queste condizioni si trova intasato da tutti i componenti aggiuntivi installati dalle applicazioni, che fra

l'altro non sempre vengono eliminati con la rimozione del programma. L'effetto tipico che viene lamentato è che dopo qualche settimana il computer diventa lento, lentissimo.

Il comportamento corretto è di installare solo e soltanto le applicazioni che siamo sicuri di usare almeno una volta al mese. Inoltre non dobbiamo cedere alla tentazione di prendere la più completa e piena di funzioni, solo perché più sofisticata: ovviamente la sofisticazione si paga in tutti i termini, come velocità, spazio occupato, compatibilità, complessità, non ultimo il costo. Meglio scegliere una versione che fa proprio quello che ci serve, e poco altro. Un utente medio usa meno di un quinto delle funzioni di una qualsiasi applicazione, e spesso non conosce neanche tutte le possibilità di un programma. Lo stesso risultato si può ottenere con un programma più semplice e meno costoso. Se poi abbiamo problemi di bilancio, meglio scegliere una versione Open Source, gratuita. Ne esistono per tutte le esigenze e sono quasi sempre compatibili con le corrispondenti applicazioni commerciali. Eccone alcuni esempi:

- OpenOffice[1] per le applicazioni tipiche da ufficio: videoscrittura, foglio elettronico, presentazioni, grafica, database. Compatibile con la suite per ufficio di Microsoft.
- Firefox e Thunderbird[2] come browser e programma per la posta elettronica: potenti, flessibili, dotati di tantissime funzioni, sono una validissima alternativa a programmi commerciali.
- The Gimp[3], per l'elaborazione grafica: non ha nulla da invidiare a programmi molto più costosi, ed opera su decine di formati grafici differenti.
- Eclipse[4], per chi crea software: un ambiente di sviluppo completo e molto sofisticato, totalmente gratuito.
- Inkscape[5], per la grafica vettoriale: usa il formato standard SVG (*Scalable Vector Graphic*), e possiede una collezione di clipart per uso libero, senza restri-

1. http://it.openoffice.org/
2. http://www.mozilla.com/
3. http://www.gimp.org/
4. http://www.eclipse.org/
5. http://www.inkscape.org/

zioni.

- Audacity[6], per editing audio: niente da invidiare a programmi più complessi (e costosi), fa tutto quello che ci si aspetta, con una interfaccia utente professionale.
- VLC[7], VideoLan Client, un riproduttore multimediale: brani audio, video, DVD, CD audio, praticamente può aprire qualsiasi cosa conosciuta, e possiede anche i codec in formato Ogg Media, non coperti da brevetto, di libero impiego.

Ce ne sarebbero molte altre, ma ci fermiamo qui, e rinnoviamo l'invito ad aver cura del nostro computer e del suo sistema operativo, come con la nostra automobile: se lo maltrattiamo prima o poi ci lascerà per strada.

Attento a non sporcarti

Abbiamo visto come navigando in Internet sia possibile incappare in siti di malaffare, che sono là in attesa di vittime. Dobbiamo imparare a diffidare della parola *gratis*, soprattutto quando abbiamo a che fare con cose appetibili: musica, film, suonerie e giochini per cellulari e, inutile nascondercelo, il sesso (non possiamo ignorare che una fetta consistente del fatturato delle aziende su Internet proviene dallo sfruttamento legale della pornografia). Pur sapendo che musica e film sono protetti da leggi sul diritto d'autore, non esitiamo a girare per i peggiori siti web alla ricerca di un film, che in fondo neanche ci interessa. Chi crea malware conosce benissimo questa inclinazione, saper attirare vittime è il suo lavoro, se così vogliamo dire. Se cediamo alla futile tentazione di ottenere un misero profitto, come il vedere (male) un filmino pirata, non dobbiamo poi stupirci di trovare il computer appestato.

Altra cattiva abitudine è di usare software senza averlo acquistato. I produttori proteggono il proprio software con vari metodi, ma dei "benefattori" in Rete ci offrono dei programmini che ci permettono di infrangere questa protezione e ci fanno godere appieno di questi programmi "faticosamente" ed illegalmente ac-

6. http://audacity.sourceforge.net/
7. http://www.videolan.org/

quisiti. I *crack*, termine in gergo che identifica questi programmini, spesso sono polpette avvelenate: nascondono al loro interno malware pronti a devastare il nostro computer per metterlo al servizio di altri. Oppure usano la tecnica del "vuoi questo? Allora prendi anche questo!" (Sezione *Un secchio d'acqua per una goccia di olio* nel Capitolo 8): per scaricare il crack occorre installare un plugin, che altri non è che un malware della stessa genìa dei peggiori mai visti. Per non parlare dei vari malware che sfruttano questa propensione mascherandosi sotto forma di crack per le applicazioni più richieste.

Un paio di mesi di questo comportamento ed il nostro computer è diventato una fogna: popup, toolbar, finestrelle, avvisi, pubblicità, e per di più sarà diventato inesorabilmente lento. Ora il perché lo sappiamo, come sappiamo che a quel punto il computer non esegue solo i nostri ordini, ma anche quelli di qualcun altro.

Prevenire è meglio che curare

Dopo aver battuto per tanti capitoli sulle impostazioni del computer e sulle modifiche alla configurazione necessarie per rendere XP sicuro quanto basta, dovrebbe essere ormai chiaro che per evitare problemi è meglio premunirsi. Purtroppo la strategia più comune è al contrario, nel senso che si cercano gli antibiotici più potenti e le medicine più aggressive, invece di coprirsi bene prima di uscire in un giornata fredda. Il risultato è che il computer si trasforma in un campo di battaglia, con cadaveri e devastazioni, perché lo scanner antivirus e antispyware, pur ammettendo che sia in grado di riconoscere il malware e di eliminarlo, spesso non può o non è in grado di rimettere tutte le cose al suo posto, lasciando pezzi di programma, chiavi del registro e impostazioni dopo la rimozione del malware.

Non lo ripeteremo più: i malware non devono avere possibilità di entrare, senza eccezioni. Una volta dentro, anche l'antivirus o l'antispyware più sofisticato e furbo che possa esistere non potrà mai dare garanzia di aver rimesso tutto come prima.

Ho seguito tutto, ma è successo lo stesso...

Come abbiamo detto fin dal principio, niente e nessuno può metterci al riparo da

un problema di malware, o da un semplice guasto, possiamo soltanto ridurre il rischio che succeda o l'entità del danno, mai azzerare entrambi.

Può comunque succedere di essere vittime di un malware, nonostante tutte le nostre precauzioni ed un comportamento irreprensibile. Se il nostro antivirus non è in grado di porre rimedio, anche accedendo come amministratore, e non riusciamo a capire come sia entrato o dove sia annidato, occorre scegliere una strategia di intervento che, oltre a rendere *certa* la rimozione del malware e di tutte le sue modifiche, ci metta al sicuro da ricadute.

Questo non sempre è alla portata dell'utente medio, e la strategia solita è di vagare per la Rete in cerca dello strumento giusto, consigliato dall'amico "smanettone" o letto su un forum in Internet. A questo punto è solo questione di fortuna.

La strategia migliore sarebbe di ricorrere a una persona competente, qualcuno che sappia dove mettere le mani. Non sempre è possibile, e il difficile è capire *quanto* il qualcuno sia effettivamente competente in questo specifico campo. L'altra possibilità è di ripensare a quello che abbiamo detto fino ad ora e cercare quale fra le ultime operazioni al computer sia quella dannosa, direttamente o indirettamente. Di solito è la mancanza di un aggiornamento del sistema operativo o di qualche applicazione, o una manovra fatta in un momento di distrazione. Avendo il backup, possiamo sempre operare in modo *certo*: eliminare l'account utente compromesso dal computer, ricrearlo pulito e ripristinare i dati dall'ultimo backup.

Se il problema coinvolge l'amministratore siamo in situazione critica: niente nel computer è più affidabile, ogni indicazione o programma diagnostico potrebbe mostrare risultati fasulli, o non funzionare del tutto, ostacolato dal malware stesso. In questo caso una reinstallazione del sistema operativo sarebbe la procedura più sicura, anche sapendo che è un lavoraccio.

Una contromisura alternativa è di creare una immagine della partizione del disco su cui risiede il sistema operativo e le applicazioni, appena dopo aver aggiornato XP, installato quello che serve e configurato il sistema come spiegato nei capitoli precedenti. Per far questo esistono anche dei programmi gratuiti che funzionano egregiamente. Uno di questi è Partimage, compreso nel System Rescue CD[8], una

8. http://www.sysresccd.org/

distribuzione Linux orientata al recupero da disastri di vario genere.

Con Partimage è possibile creare una fotografia della partizione del disco su cui risiede XP e masterizzarla su un DVD registrabile, o copiarla su un disco USB esterno. Nel momento in cui fossimo vittime di un disastro di qualsiasi tipo, potremmo ripristinare l'immagine ed evitare la trafila di tutta l'installazione e configurazione. Ovviamente è utile in questo caso avere i dati su un backup separato, in modo da averli sempre aggiornati e mantenere l'immagine del sistema operativo più snella possibile.

Prima di proseguire dal punto in cui siamo stati vittime del disastro, faremo un rapido controllo su tutte le nostre difese, verificando che non vi siano punti deboli, cosa probabile se un malware è riuscito ad entrare.

Io? Non ho fatto niente!

Lo abbiamo già detto, ma lo ripetiamo: chi ha interesse a diffondere malware parte dal presupposto che il nostro computer sia blindato ed a prova di falle, per cui agisce su un altro componente, molto più semplice da colpire: noi.

Nelle prove fatte in precedenza (vedi Capitolo 8) il computer era dietro *tre* firewall in cascata: quello del router (di una nota marca), quello del laboratorio (un computer Linux attrezzato per fare da firewall/router) e quello software incluso nel computer di prova. L'antivirus e l'antispyware erano aggiornati ed attivi, l'utente in uso non aveva diritti da amministratore, e il sistema operativo era correttamente aggiornato. Eppure nessuno mi ha impedito di scaricare ed avviare un malware che poi si è rivelato un dialer (Sezione *Servizi gratuiti... a pagamento* nel Capitolo 8). Come nessuno mi ha impedito di scaricare ed installare due spyware (Sezione *Un secchio d'acqua per una goccia di olio* nel Capitolo 8).

Possiamo avere il castello più inaccessibile e fortificato immaginabile, ma siamo noi i signori del castello, e se invitiamo a corte una banda di assassini armati fino ai denti nessuno potrà impedircelo. Come niente e nessuno potrà poi impedire agli assassini di fare il loro comodo. Dare la colpa alle guardie o al costruttore del ponte levatoio servirà a poco.

Quando mettiamo qualcosa dentro il nostro computer dobbiamo pensare *a priori* che possa nascondere una insidia. Dobbiamo diventare pieni di pregiudizio e sospettosi, soprattutto verso i doni inaspettati. E' l'unica strategia che ci può salvare.

Ad ognuno il suo

Se abbiamo necessità di far lavorare più persone con lo stesso computer, è buona norma separare lo spazio di ogni utente, e tenere un solo utente come amministratore. Questo darà la sensazione a tutti di avere un angolo privato in cui nessuno mette il naso, personalizzabile a piacere, e metterà al sicuro il computer da tutti i disastri derivanti dalla situazione in cui tutti comandano.

Inoltre ognuno sarà responsabile della tenuta dei propri dati e dell'esecuzione di backup regolari. In caso di disastro, si potrà reintegrare lo spazio del singolo utente, o di tutti se il problema è causato da un guasto distruttivo.

Senza trascurare il fatto che con un solo amministratore il computer sarà sempre sotto controllo, costringendo tutti ad adeguarsi al metodo di lavoro scelto.

Ci saranno sempre problemi con qualcuno che non vuole sentire ragioni, ma a quel punto potrebbe essere meno costoso dotarlo di un computer dedicato, dove l'utente potrà pasticciare a piacimento, con l'accortezza di metterlo in condizione di non appestare gli altri computer con le porcherie che esso stesso si tirerà addosso, ad esempio isolandolo su una subnet dedicata, o configurando i firewall degli altri utenti per non accettare nulla da quel particolare computer: potrà condividere file e stampanti, ma non deve poter arrivare dentro i computer degli altri.

E' certamente una misura estrema, ma è meno onerosa che dover reinstallare sistema operativo, applicazioni, ripristinare dati di tre-quattro utenti ad ogni disastro, tenendo tutti fermi nel frattempo. In questo modo, in caso quasi inevitabile di contaminazione, solo l'utente indisciplinato dovrà attendere l'intervento di recupero sul suo computer, mentre gli altri potranno lavorare tranquillamente.

La *checklist*

Non è fondamentale, ma può essere un aiuto considerevole avere una lista delle cose da fare per mettere in sicurezza il proprio computer e soprattutto i propri dati.

Per questo motivo mettiamo qui di seguito una breve lista delle cose che abbiamo detto fino ad ora, con il riferimento allo specifico paragrafo, indicando quando sia una misura facoltativa.

Installando il sistema operativo:

- □ Prima di iniziare l'installazione, o di accendere il computer per la prima volta, scolleghiamo cavi di rete, modem normali, ADSL e disabilitiamo le reti senza fili se il computer ha la relativa interfaccia.
- □ Installiamo Windows XP usando il filesystem NTFS (Sezione *Seconda linea di difesa ter: filesystem e permessi* nel Capitolo 4).
- □ Creeremo un account utente che sarà amministratore e tanti altri quanti sono gli utilizzatori reali del computer. Se lo usiamo solo noi, creeremo due account, uno amministrativo ed uno normale (Sezione *La seconda linea di difesa: diritti e gerarchie* nel Capitolo 4).
- □ Installiamo solo i driver e le applicazioni effettivamente utilizzate.

Terminata l'installazione:

- □ Cambiamo il tipo di utenti che useranno il computer in utenti "limitati" dal Pannello di controllo, lasciandone uno solo come amministratore (Sezione *La seconda linea di difesa: diritti e gerarchie* nel Capitolo 4).
- □ Assegnamo password robuste a tutti gli utenti (Sezione *La seconda linea di difesa bis: password* nel Capitolo 4).
- □ Disabilitiamo la "condivisione semplice" per accedere alla gestione completa dei permessi del filesystem (Sezione *Seconda linea di difesa ter: filesystem e permessi* nel Capitolo 4).

- ☐ Configuriamo XP per mostrare tutto quello che normalmente ci tiene nascosto, fra cui i file e le cartelle, senza eccezioni (Sezione *La terza linea di difesa: cosa mi nascondi?* nel Capitolo 4).
- ☐ Disabilitiamo i servizi inutili e chiudiamo le relative porte (Sezione *La quarta linea di difesa: porte murate* nel Capitolo 5).
- ☐ Se non intendiamo condividere file o stampanti, disabilitiamo del tutto il servizio Server (Sezione *I servizi server bis: porte 445/TCP e 445/UDP* nel Capitolo 5).
- ☐ In alternativa, disabilitiamo le condivisioni amministrative (Sezione *Condivisioni amministrative* nel Capitolo 5).
- ☐ Attiviamo il firewall di XP su tutte le interfacce di rete, o ne installiamo uno di nostro gradimento, controllandone regole ed eccezioni (Capitolo 6).
- ☐ Configuriamo il metodo per gli aggiornamenti con Windows Update (Capitolo 7).
- ☐ Applichiamo le modifiche alle impostazioni di Internet Explorer ed alle proprietà Internet, ripetendole per tutti gli utenti (Sezione *Se sembra complicato, forse lo è* nel Capitolo 8).
- ☐ Se usiamo un collegamento Internet con modem connesso direttamente al computer, installiamo e configuriamo quello che serve e creare l'icona in "Rete e connessioni Internet" del collegamento che useranno tutti gli utenti.
- ☐ Applichiamo la protezione contro i dialer al collegamento appena creato (Sezione *Dico io chi chiamare* nel Capitolo 8).

Arrivati qui possiamo avviare il collegamento Internet.

- ☐ La prima operazione in assoluto è un aggiornamento completo del sistema operativo mediante Windows Update (Capitolo 7).
- ☐ Di seguito passiamo ad aggiornare le applicazioni che usiamo più assiduamente, controllando sul sito del produttore che non siano usciti aggiornamenti mirati per problemi di sicurezza.
- ☐ (Facoltativo) Ci iscriviamo al servizio dei bollettini di sicurezza Microsoft (Sezione *Cliccare informati* nel Capitolo 7).

- □ Scegliamo ed installiamo un antivirus (Capitolo 9 e Sezione *Voglio il migliore!* nel Capitolo 9). Opzionalmente possiamo scegliere ed installare uno scanner antispyware, tenendo presente quanto detto.
- □ Scegliamo il metodo di gestione della posta elettronica: locale o remoto (Sezione *C'è il postino, apro?* nel Capitolo 10), in funzione delle nostre preferenze e del tipo di impegno che ci vogliamo assumere.

Ora il nostro computer è un gioiellino: ordinato, pulito, veloce e soprattutto ragionevolmente sicuro.

Possiamo a questo punto passare al backup, in modo da poter recuperare situazioni di disastro. Quindi, prima di iniziare ad usare normalmente il computer:

- □ (Facoltativo, ma caldamente consigliato) Tramite il System Rescue CD, citato in precedenza, facciamo una immagine del nostro disco di sistema operativo nella sua attuale condizione di perfetto stato. In caso di disastro totale (un guasto al disco fisso, un errore di manovra: ricordiamo che non sono solo i malware a fare danni), potremo ripartire senza troppa fatica con un computer perfettamente in ordine.
- □ Ci imponiamo, ed imponiamo a tutti coloro che usano il computer, di fare un regolare backup dei dati, secondo le esigenze (Sezione *La prima contromisura: il backup* nel Capitolo 4) e secondo la regola che ognuno è responsabile dei propri dati.

Basta così

Chiudiamo qui. Ci sono molti argomenti che non abbiamo trattato per limiti di spazio, come altri che abbiamo tralasciato perché ci avrebbero portato lontano e fuori tema.

Siamo pronti per usare il computer, con qualche differenza rispetto alla situazione tragicomica rappresentata nell'introduzione:

- Siamo maggiormente coscienti dei pericoli: abbiamo imparato che Internet è un luogo ostile e che nessuno regala nulla.
- Siamo più responsabili e più attenti a quello che facciamo, non contando più sulle magie tecnologiche per la nostra sicurezza. Sappiamo che dare la colpa agli strumenti non risolve il problema: un automatismo non può competere con un essere intelligente. Il punto debole dei programmi "magici" è proprio questo: una volta spiegata la magia, diventano inutili. Il nostro scetticismo ed il nostro senso critico, questi sono i migliori dispositivi di sicurezza che esistano.
- Il nostro computer è ragionevolmente al riparo dai pericoli, e possiamo usarlo senza avere l'ansia addosso per ogni mossa, per ogni click, per ogni messaggio di avvertimento che ci si presenta.

Non è poco. E se ripercorriamo la strada fatta fino ad ora, possiamo scoprire che non abbiamo usato programmi "magici" del quale nulla sappiamo, non abbiamo fatto strani riti o alchimie senza comprendere cosa facciamo. Per ogni operazione ora sappiamo il perché, per ogni minaccia abbiamo messo in atto una strategia specifica e mirata.

Nel percorrere la strada che ci ha portato qui, abbiamo conosciuto il nemico, le sue motivazioni e le sue mire. Certamente scoverà nuovi metodi e nuove trappole sofisticate ed efficienti, ma ora avrà vita infinitamente meno facile.

Abbiamo imparato che occorre seguire delle regole, semplici e lineari, e che un piccolo sacrificio ci ripaga con un aumento considerevole della nostra tranquillità.

E' la differenza fra muoversi a caso e *possedere un metodo*, un insieme di conoscenze e di procedure che ci permette di rendere ragionevolmente sicuro il nostro computer, e soprattutto i nostri dati, quali che siano.

Agli insofferenti per le regole e le restrizioni, possiamo rispondere con una delle frasi preferite di mia moglie: *le regole servono di più proprio a chi non sa regolarsi*.

Nessuno ci obbliga a fare tutto il percorso descritto fin qui, siamo liberi di scegliere quello che ci pare, e di decidere del nostro computer. Ma non per questo andiamo a buttarlo dalla finestra solo perché possiamo.

Capitolo 12. Il finale

Siamo alla conclusione del nostro breve, e mi auguro fruttuoso, incontro. Tiriamo le somme e vediamo cosa rimane.

Approfondire

In alcuni punti abbiamo parlato di tecniche di inganno, di social engineering, di psicologia della comunicazione in altri di teoria della computabilità. Abbiamo visto ed esaminato casi reali di problemi di sicurezza del computer, analisi di malware reali e di truffe veicolate dalla posta elettronica. Gli argomenti sono veramente tanti, e se siamo curiosi e desiderosi di approfondirne qualcuno, ecco un elenco di fonti a cui attingere:

- Libro: "Mindfucking. Come fottere la mente" di Stefano Re (ed. Castelvecchi) - Stefano Re è un criminologo, e nel suo libro parla dei metodi usati in una vasta gamma di situazioni in cui si vuole convincere qualcuno a fare qualcosa contro la propria volontà. In dettaglio analizza i meccanismi che sono dietro alle tecniche di controllo mentale e psicologico, molto utilizzate da sette pseudoreligiose, da maghi e venditori televisivi. E' molto utile per capire come una persona, anche se addestrata alle condizioni peggiori, viene portata al cedimento completo anche senza uso di violenza fisica.
- Libro: "L'arte dell'inganno" di Kevin Mitnick (ed. Feltrinelli) - Mitnick è un personaggio controverso e sicuramente molto particolare. Incarcerato per crimini informatici, ed evaso con l'uso di un misto di strategie psicologiche e tecnologiche, è oggi un noto consulente per la sicurezza dell'informazione. In questo libro mostra quanto sia teoricamente semplice ottenere la collaborazione di sconosciuti per i propri scopi.
- Libro: "Computer a responsabilità limitata" di David Harel (ed. Einaudi) - E' un testo introduttivo su un argomento di livello universitario. Scritto in modo molto leggero e leggibile, spiega molto efficacemente i limiti dei moderni computer e della scienza del calcolo automatico. In particolare tratta argomenti come la teoria della computabilità, la complessità dei programmi, i problemi

insolubili.

- Sito web di Paolo Attivissimo[1]: noto divulgatore informatico, ha il merito di aver sfatato molti miti a carattere non solo informatico. E' un agguerrito cacciatore di "bufale", informatiche e non, e nel suo sito ne ha una collezione notevole e costantemente aggiornata. Da non perdere.
- Libro elettronico: "Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP V2.0", reperibile sul sito Microsoft[2] - Un manuale su come configurare Windows XP e Windows Server 2003 allo scopo di ridurre il rischio di essere vittime di attacchi di malware di vario genere. Molte delle strategie presentate sono impiegate nelle procedure spiegate in questo libro.
- Libro elettronico: "Guida per la protezione di Windows XP", in italiano, reperibile sul sito Microsoft[3] - Il titolo dice tutto. Gran parte delle impostazioni riferite in questo libro vengono da qui. Si può prelevare la versione in inglese[4], con tutti i file di supporto citati nella guida.
- Libro elettronico: "Step-by-Step Guide to Securing Windows XP Professional with Service Pack 2 in Small and Medium Businesses" - Reperibile sul sito Microsoft[5], solo in inglese.
- Sito web di SecurityFocus[6]: il punto di raccolta delle mailing list più famose e frequentate dagli esperti di sicurezza dell'informazione. La più nota è forse *Bugtraq*, dove vengono divulgate informazioni di prima mano su errori e falle all'interno di applicazioni e sistemi operativi, passibili di diventare porte per l'ingresso di malware. Purtroppo è solo in inglese, ma ne vale la pena.
- Sito web di Bruce Schneier[7], un affermato esperto di sicurezza e crittografia. Nel suo sito affronta in modo spesso *eretico* e controcorrente molti temi riguar-

1. http://www.attivissimo.net/
2. http://go.microsoft.com/fwlink/?LinkId=15160
3. http://www.microsoft.com/italy/technet/security/prodtech/windowsxp/secwinxp/default.mspx
4. http://go.microsoft.com/fwlink/?LinkId=14840
5. http://www.microsoft.com/windowsxp/using/security/learnmore/smbsecurity.mspx
6. http://www.securityfocus.com
7. http://www.schneier.com

danti la sicurezza dell'informazione. Anche questo è solo in inglese, anche se la sua *newsletter* viene tradotta in italiano da volontari.

- Sito web Scam-o-rama[8]: raccolta semiseria di tutti i campioni circolanti di truffa nigeriana, vista nel capitolo dedicato alla posta elettronica.
- I siti web dei produttori di antivirus - Tutti i produttori mantengono un database aggiornato di tutti i malware conosciuti dai loro prodotti. Per ogni malware vi è un breve sunto delle caratteristiche peculiari, ed eventualmente le indicazioni specifiche per rimuovere ogni traccia dello sgradito ospite.

Questo solo per cominciare. Alcune di queste fonti sono prettamente specialistiche, e certo non adatte a chi informatico non è, ma sono riportate per chi vuole verificare personalmente il contenuto di questo libro.

Dediche

Questo libro è dedicato a miei nonni, gente semplice che ha passato la vita lavorando duramente senza mai lamentarsi. Oggi non ci sono più, e troppo tardi ho capito quanto dei loro involontari insegnamenti mi hanno reso una persona migliore.

Ringraziamenti

Un sentito ringraziamento a mia moglie, che tollera le ore passate dal sottoscritto al computer, e che per fortuna non si occupa di informatica.

Non potrò mai ringraziare abbastanza Lorenzo, titolare di Nobug srl, per avermi sostenuto e consigliato durante la scrittura e pubblicazione di questo libro.

Senza l'ottimo lavoro fatto dal team di sviluppo di Fedora[9]), la mia distribuzione Linux di riferimento, questo documento non avrebbe potuto vedere la luce. La stessa gratitudine va agli innumerevoli individui che contribuiscono alla realizzazione di tutto il software Open Source.

8. http://www.scamorama.com
9. http://fedoraproject.org/wiki

Un grazie, si fa per dire, alla programmazione televisiva, in virtù della quale ho recuperato tante ore che passo in modi più piacevoli e costruttivi, almeno per me.

Glossario

Aa

account

In inglese *conto*, nel senso di conto bancario. Con questo termine si indica lo spazio di qualcuno che ha accesso al computer ed all'uso delle risorse disponibili.

ADSL

Acronimo di *Asymmetric Digital Subscriber Link*, linea abbonato digitale asincrona. Metodo di connessione che sfrutta un sistema molto simile a quello dei modem a 56k, ma invece di usare la banda audio telefonica, sfrutta le frequenze sopra i ventimila Hertz. E' denominato asimmetrico perché di solito la velocità verso l'abbonato è molto maggiore della velocità verso la centrale. Questo perché è pensato per il tipico accesso Internet, piuttosto passivo in quanto la quantità di dati inviati è sempre molto inferiore a quella dei dati ricevuti. Vedere anche la voce su Wikipedia[1], in inglese.

antivirus

Più esattamente *antivirus scanner*. Programma preposto al rilevamento ed eliminazione di virus e di equivalenti categorie di malware.

antispyware

Oppure *spyware scanner*. Simile come funzionamento e impiego all'antivirus, serve al rilevamento ed eliminazione degli spyware.

1. http://en.wikipedia.org/wiki/Adsl

attacco informatico

La sequenza di operazioni compiute da chi tenta di scardinare le difese di un sistema informatico. Gli scopi di un attacco possono essere i più disparati: dall'accesso non autorizzato al semplice danneggiamento, al furto di dati o risorse.

attacco a dizionario

Metodo per scoprire una password tentanto sistematicamente tutte quelle contenute in una lista predefinita, il dizionario appunto.

attacco brute force

In inglese *pura forza*. Metodo per scoprire una password tentando tutte le combinazioni possibili di caratteri che possono essere usati per la sua composizione.

Bb

backup

Letteralmente "copia di riserva". Una copia di un oggetto o di dati da usare in caso di indisponibilità dell'oggetto principale

BIOS

Acronimo per *Basic Input/Output System*, un programma di base per permettere l'accesso alle periferiche principali del computer. E' allocato su una

memoria a stato solido a sola lettura per essere disponibile anche se il computer viene spento.

Cc

catena di santantonio

In inglese *chain letters*, lettere a catena (Sezione *Catene scatenate* nel Capitolo 10).

condivisione

Nel gergo tipico di Windows, una directory resa disponibile da un computer, accessibile attraverso la rete, eventualmente fornendo una password.

Oppure l'operazione stessa di rendere accessibili vie rete alcune risorse di un computer, come stampanti, file e spazio disco.

crack

Dall'inglese *spezzare*. Programma usato per aggirare o eliminare la protezione di un altro programma. Alcuni software hanno un meccanismo per impedire la copia o per limitare l'uso di copie non originali, e, al di là della efficacia di questi sistemi, spesso la protezione è aggirabile in modo banale usando uno di questi programmi distribuiti da circuiti non ufficiali ed ovviamente illegali.

cracker

Chiunque tenti di guadagnare un accesso non autorizzato ad un computer oppure ai dati in esso contenuti.

credenziali

La coppia nome utente e password usate per l'identificazione e l'accesso ad un servizio o ad uno spazio personale in un computer. A volte invece della password può essere usato un metodo differente, come una scheda magnetica o l'impronta digitale, ma il senso non cambia.

Dd

DNS

Acronimo di *Domain Name System*. Metodo di conversione fra i nomi dei siti Internet ed il loro indirizzo IP e viceversa. Senza questo servizio sarebbe impossibile navigare su Internet, perché occorrerebbe sapere gli indirizzi IP di ogni sito web.

driver

Dall'inglese *pilota*. Software che permette al sistema operativo di pilotare appunto una periferica usando comandi predefiniti, indipendentemente dalla costituzione fisica e logica. Ad esempio se si tratta di un disco, il driver mette a disposizione comandi per leggere e scrivere dati, se è una stampante i comandi per prendere un foglio, stampare caratteri o immagini ed espellere il foglio. Esistono anche driver di protocollo, che permettono al sistema operativo di comunicare con periferiche intelligenti o con altri computer, usando comandi semplificati tipo "apri la comunicazione", "manda questi dati", "prendi dati", ecc. senza occuparsi dei dettagli della comunicazione.

DVD-R, DVD-RW

E' un DVD registrabile che nella versione -RW è possibile cancellare e riscrivere un numero limitato di volte, tipicamente qualche migliaio.

Ee

Ethernet

Standard di connessione di rete. Pur essendo stato inventato parecchi anni fa, nel 1976, continua ad essere il più usato, ed è ormai arrivato alla velocità di 10 gigabit al secondo su un singolo collegamento.

Ff

filesystem

Il metodo e la codifica interna con cui i dati sono memorizzati su una porzione di disco. In Windows ne esistono di vari tipi, e due famiglie principali: FAT (acronimo da *File Allocation Table*, usato fin dai primi anni ottanta nel Microsoft MS-DOS, ed evolutosi fino alla versione FAT32) ed NTFS (usato in Windows NT, Windows 2000, Windows XP e Windows 2003). NTFS è un sistema evoluto che permette di gestire anche proprietà come appartenenza di un file ed un utente e permessi di scrittura, lettura, esecuzione per utenti o gruppi di utenti.

firewall

Programma, o dispositivo contenente un programma che esamina il traffico in una rete locale e consente o nega il passaggio sulla base di regole presta-

bilite.

firme

dall'inglese *signatures*. Sequenza contenuta all'interno del programma di un malware che ne rende certa l'identificazione. Ogni programma antivirus ed antispyware ha bisogno di un database di firme, e deve tenerlo aggiornato per svolgere la sua funzione.

formattazione

Operazione di inizializzazione di un supporto dati, costituito dalla scrittura di dati particolari, invisibili all'utente, che servono a definire l'organizzazione dei dati all'interno del supporto stesso.

FTP

Acronimo di *File Transfer Protocol*. servizio di trasferimento file via Internet.

Hh

HTTP

Acronimo di *HyperText Transfer Protocol*. Sistema di distribuzione degli ipertesti su Internet.

hacker

Termine intraducibile, indicante un individuo che ama capire il funzionamento delle cose e di seguito trovarne nuovi usi, non sempre previsti in origine. Ad esempio chi per primo ha usato il trucco degli squilli a vuoto del cellulare è un hacker. Il termine non ha nessuna connotazione negativa, anche se i media a grande diffusione hanno definitivamente associato il termine alla nozione di pirata informatico. Una buona definizione:

> uno che ami programmare, e a cui piaccia essere bravo a farlo
>
> —R. Stallman, fondatore del progetto GNU

home banking

Sistema che sfrutta il web per permettere ai clienti di un istituto bancario di effettuare operazioni sul proprio conto corrente e sui propri titoli senza andare fisicamente allo sportello.

Ii

ipertesto

Un testo normale ha una struttura lineare, e la sua lettura è di solito sequenziale. Un ipertesto invece contiene elementi di connessione logica fra temi, la cui lettura può essere anche secondo una sequenza scelta dal lettore. Il formato HTML definisce proprio un tipo di ipertesto.

IP

Acronimo di *Internet Protocol*. Protocollo base di Internet, nato da un progetto universitario alla fine degli anni 70.

incidente informatico

Un evento riguardante la compromissione di un computer o di una rete di computer con conseguente perdita di funzionalità, dati e servizi. Detto anche *computer incident*.

intrusione

La sequenza di azioni che porta qualcuno ad accedere dati e risorse in un computer su cui non ha titolo né diritto alcuno, sia operando direttamente che per il tramite di strumenti automatizzati.

IRC

Acronimo di *Internet Relay Chat*, un protocollo per conversazioni di gruppo o individuali in tempo reale attraverso Internet.

LI

libreria

In campo informatico, una raccolta di funzioni di uso comune richiamabili da altri programmi. In Windows sono sotto forma di file con estensione *.dll*, acronimo per *Dynamic Link Library*. Ad esempio, la funzione di visualizzazione delle immagini di tipo JPEG è contenuta in un file DLL, che viene utilizzato da tutti i programmi che hanno necessità di manipolare file di questo tipo.

Mm

malware

Neologismo derivato dalla contrazione di *Malicious Software*, nato per indicare in generale tutti i tipi di software malevolo. Data la continua espansione e diversificazione della categoria, si è coniato questo termine omnicomprensivo.

Oo

Open Source

Letteralmente "sorgente aperto". E' un modello di distribuzione del software dove, diversamente da quello comunemente applicato, il sorgente è distribuito insieme al programma. Spesso viene distribuito soltanto il sorgente, lasciando all'utilizzatore il compito di crearsi la versione eseguibile. Esistono varie licenze di distribuzione del software che si classificano come Open Source.

Pp

PPP

Acronimo per *Point to Point Protocol*. Protocollo di comunicazione pensato per far comunicare in modo esclusivo due computer. Usato per i collegamenti a Internet via telefono.

pacchetto

Unità di trasmissione dati, riferita ai protocolli di comunicazione. Su canali di comunicazione che possono presentare errori di trasmissione, il trasferimento di grandi quantità di dati può essere resa difficoltosa e ci si trova costretti a ripetere la trasmissione. Suddividendo i dati in piccole quantità alla volta, in caso di errore basta ripetere solo il gruppo errato e non tutti i dati.

Rr

router

Apparato di rete che si occupa di instradare i pacchetti fra reti appartenenti a differenti subnet.

Ss

scheda madre

Componente la cui funzione è di fornire alimentazione e connessione a tutti i dispositivi che costituiscono il computer stesso: CPU, memoria, scheda video, dischi. Di solito non ha capacità elaborative o di memorizzazione, ma fornisce il supporto fisico e logico per tutti gli altri componenti.

sniffer

Lo *sniffer* è un programma capace di catturare tutto il traffico di dati che risulta visibile da una interfaccia di rete del computer, anche se non è destinato al computer stesso. E' chiaramente una minaccia alla sicurezza, in

quanto con uno sniffer si possono spiare tutti i dati che transitano su quella porzione di rete.

sniffing

Sniffing è l'operazione di spiare il traffico usando uno sniffer. Il termine è inglese e significa "annusare", quindi sniffer sta per "annusatore".

spam

E' un tipo di carne in scatola. Il termine è usato per indicare la posta spazzatura. In genere si tratta di messaggi spediti a milioni di indirizzi, il cui mittente è falsificato e quindi praticamente impossibile da rintracciare (Sezione *Spam spam spam spam* nel Capitolo 10).

spammer

Individuo che genera e diffonde spam.

Spyware

Contrazione dei termini *spy software*, *programma spia*. Un malware che ha come funzione principale la raccolta di informazioni ad insaputa della vittima. Queste informazioni sono poi trasmesse al creatore del malware per gli scopi più vari, principalmente commercio di informazioni di marketing e spionaggio.

Uu

USB

Acronimo per *Universal Serial Bus*, uno standard di connessione per periferiche di computer. Usato per archiviazione e trasmissione dati.

utente

Nel campo dell'informatica è un termine con cui si indicano varie cose a seconda del contesto. Normalmente ci si riferisce all'identificativo con cui ci si fa riconoscere dal sistema operativo, ed a cui viene associato uno spazio di lavoro, detto *home directory*. L'utente è anche un oggetto che ha dei permessi e dei diritti che definiscono cosa può fare e quali parti del sistema operativo può toccare.

Vv

virus

Organismo molto semplice che si riproduce soltanto tramite infezione di altri organismi, usandone i meccanismi e le risorse interne e riprogrammandone il codice genetico. Il termine è passato al mondo dell'informatica per il forte parallelo con il meccanismo di diffusione.

Ww

Worm

Dall'inglese *verme*. Un tipo di malware che si propaga senza intervento dell'utente del computer, solitamente attraverso il collegamento in rete. A

differenza del virus propriamente detto, non ha bisogno di attaccarsi ad un altro programma, ma è un programma indipendente.

Zz

zombi

Morto vivente. Termine usato per indicare un computer infetto con un tipo di malware capace di prendere ordini da una fonte esterna e di usarne le risorse di elaborazione e di connessione per compiere azioni di disturbo o attacchi informatici.