



# Computer e Internet in sicurezza



Mario Pascucci

Copyright © 2012 Mario Pascucci

## **Presentazione**

Sono passati alcuni anni dalla pubblicazione di “Windows XP in sicurezza”, e lo scenario è certamente cambiato: alcune minacce sono state quasi completamente debellate, più spesso estinte, ma altre ne sono spuntate, sia grazie alle differenti abitudini di noi utilizzatori, sia per la innaturale evoluzione tecnologica, spinta da un mercato in cui chi non presenta novità ogni tre mesi è destinato a non sopravvivere.

Sul fronte dei sistemi operativi, Windows XP è stato dato per morto parecchie volte, ma ad oggi è ancora vivo e vegeto, nonostante l’uscita di Vista prima e di Windows 7 poi. Mac OSX si sta ritagliando una sua fetta di utenti, affezionati ed entusiasti. In quanto a Linux, è sufficiente nominarlo per provocare discussioni interminabili, con opinioni totalmente contrastanti.

Da un diverso punto di vista, Internet sta diventando sempre più indispensabile per tutti, fra il proliferare di social network, servizi online, siti personali e l’impiego sempre più popolare di applicazioni web. Prontamente, parte delle attività criminose si sta spostando in Rete e le vittime siamo sempre noi utilizzatori.

Non è più questione di proteggere il proprio computer, ma anche di proteggere la nostra identità digitale, i nostri preziosi dati personali e, non ultimo, il nostro portafogli, che rimane uno dei bersagli preferiti, non il solo.

Il nostro computer può essere blindato e inattaccabile, ma ogni volta che inseriamo i nostri dati di identità in qualche sito Internet siamo un potenziale bersaglio. I pericoli sono tanti, in continua evoluzione, quindi ecco la necessità di realizzare una nuova versione di questo libro, meno orientata al nostro computer, in ogni caso importante, e maggiormente dedicata alle attività in Rete.

Questo libro è distribuito sotto licenza Creative Commons: Attribuzione-Non commerciale-Non opere derivate 3.0 Italia (CC BY-NC-ND 3.0)<sup>1</sup>. Per tutti gli altri usi contattatemi.

L’immagine di copertina è realizzata con il LEGO® Digital Designer da Mario Pascucci.

Il marchio LEGO® appartiene al Gruppo LEGO con sede in Danimarca.

---

1. <http://creativecommons.org/licenses/by-nc-nd/3.0/it/deed.it>



# Sommario

<b>Un libro nato vecchio .....</b>	<b>xi</b>
<b>1. Prima di iniziare .....</b>	<b>1</b>
Introduzione.....	1
Perché .....	4
Cosa c'è e cosa non c'è .....	5
Cose di cui non voglio parlare .....	6
Cosa occorre .....	7
Legalese .....	8
Come leggerlo .....	8
<b>2. Ri-conosci il Nemico .....</b>	<b>9</b>
I problemi di qualsiasi sistema operativo .....	9
Anatomia dei malware .....	9
Mitologie pericolose .....	12
Niente virus (leggi malware) per Linux .....	12
Perché Windows è l'unico colpito?.....	14
Unix è più sicuro di Windows.....	15
Il Mac è invulnerabile a tutto .....	17
Un sistema operativo sicuro segnerà la fine dei malware .....	20
Nuove strategie di attacco, nessuna di difesa .....	20
L'esercito delle scimmie mutanti.....	24
C'è da scherzare ancora meno .....	25
<b>3. Il fallimento della sicurezza .....</b>	<b>26</b>
La parabola degli antibiotici .....	26
Qualcosa del genere.....	27
Non ci siamo ancora .....	29
Si dice il peccato.....	30
... non il peccatore.....	32
Investire in un bravo SysAdmin .....	33
Manager "2.0", gestione della sicurezza "0.1beta" .....	36
A me non capita.....	37

<b>4. Cosa rimane valido.....</b>	<b>39</b>
Le basi sono sempre attuali .....	39
RAID non è backup .....	40
Porte, firewall e antivirus .....	42
Internet, sempre più Internet.....	44
Valido sempre .....	46
<b>5. Service Pack 1.....</b>	<b>48</b>
SPAM, l'immortale.....	48
Una raccomandata da 200kg .....	48
SPAM, un ottimo investimento.....	49
Phishing for Dummies .....	50
Il colpevole sbagliato .....	53
<b>6. Malware per tutti i gusti.....</b>	<b>56</b>
Evoluzione e selezione .....	56
Software criminale.....	57
Zbot, il <i>full optional</i> .....	58
Le sorprese non sono finite.....	61
Non tutto è perduto .....	62
Continuiamo ad autoregolarci .....	69
<b>7. L'albero della cuccagna .....</b>	<b>71</b>
Malintesi e sottintesi.....	71
Openche?!? .....	74
Non è questo che cercavo... ..	78
Chi cerca trova, pure troppo .....	80
Sensi di colpa.....	94
Incubi senza risveglio .....	95
BitTorrent Vs eMule .....	99
<i>Digital divide</i> e pessime idee.....	103
La tecnologia è neutra .....	104
<b>8. Nebbiaware .....</b>	<b>107</b>
Scaricami, SONO GRATIS!!! .....	107
Ecco eMule Free e eMule Plus.....	114
Disinfetta, PRESTO! .....	121

Computer lento? Velocizzalo! .....	130
Le cattive abitudini sono dure a morire .....	149
Follie sparse.....	153
<b>9. Il web delle meraviglie .....</b>	<b>155</b>
L'ha detto Internet! .....	155
Lei non sa chi sono io.....	158
Antisocial Network.....	159
Servizi 2.0 con fregatura 1.0.....	163
Il mio regno per una password .....	164
Una spia in tasca.....	166
Un file è per sempre.....	169
L'assenza di prove è una prova.....	171
Crimini reali nel mondo virtuale .....	173
Bello perché vario, forse troppo .....	174
I milioni son fatti di centesimi .....	175
Cuccagna? Mah.....	177
<b>10. Gestisco un sito web, io!.....</b>	<b>178</b>
Non costa niente, non subito, almeno.....	178
Webmaster, in un attimo!.....	178
Demolire le false certezze, al solito.....	180
Spam, spam ovunque .....	180
Ma io mi prendo un hosting blindato.....	182
Windows, Linux o PincoPallo, non cambia nulla .....	182
L'Open Source è meno sicuro .....	182
I siti li “bucano” gli hacker per farsi pubblicità .....	183
Vulnerabilità e aggiornamenti, anche qui .....	183
Non esageriamo!.....	184
Solo io so come funziona la mia applicazione .....	185
Va bene, ma ti pare che.....	186
Un infernale circolo vizioso .....	189
La zappa sui piedi.....	190
Fai da te, danni compresi.....	191
Il sito è mio e ci metto quello che mi pare .....	192
Calma, respira e rifletti .....	195

<b>11. Il bello di Internet.....</b>	<b>197</b>
Informarsi .....	197
Imparare.....	198
Divertirsi .....	200
Acquistare su Internet? MAI! .....	201
<b>12. Per finire.....</b>	<b>204</b>
Che succederà, dopo? .....	204
Per proseguire il percorso .....	204
Dediche.....	205
Ringraziamenti .....	205
<b>Glossario .....</b>	<b>206</b>



## Lista delle Figure

2-1. Le immagini mostrate da <i>MaWi</i> .....	18
2-2. Il Virus Sensor nell'aprile 2006.....	20
2-3. Qui nel gennaio 2009.....	21
6-1. L'attacco di Zbot in Windows XP.....	64
6-2. La reazione di Windows <i>Seven</i> .....	65
6-3. Le regole inserite automaticamente per bloccare Zbot.....	66
6-4. Il Task manager con il PID visualizzato.....	66
6-5. La lista delle porte aperte.....	67
6-6. Zbot sotto mentite spoglie.....	69
7-1. The GIMP: c'è anche il <i>crack</i> e la versione <i>live</i> .....	82
7-2. OpenOffice: versione <i>mobile</i> e versione in alta qualità.....	83
7-3. Con Linux Ubuntu le cose non è che siano differenti.....	85
7-4. Cerco qualsiasi cosa, e la trovo!.....	87
7-5. Le icone che appaiono sul desktop.....	87
7-6. Il “gratta-e-perdi”, invece di OpenOffice.....	88
7-7. Il solito ActiveX, e l'inferno è servito.....	89
7-8. Ma insomma, che film è?.....	92
8-1. Metà dei link sponsorizzati.....	108
8-2. Termini diversi, anche peggio.....	109
8-3. eMule: quelli con l'asterisco sono fasulli.....	110
8-4. La pubblicità in uno dei siti in Figura 8-1.....	111
8-5. Pubblicità in un sito che parla di un altro “velocizzatore”.....	112
8-6. Il sito ufficiale di eMule.....	114
8-7. Il sito ufficiale di Emule Plus.....	115
8-8. Un falso sito di eMule.....	116
8-9. Un altro, solo con eMule.....	117
8-10. Un altro, leggermente differente.....	118
8-11. Il solito secchio d'acqua per la goccia d'olio.....	119
8-12. L'ennesima <i>toolbar</i> .....	120
8-13. Un esempio di falso scanner.....	121
8-14. Notare la somiglianza con la grafica di Windows.....	123
8-15. Sono 159 o $18+23+158$ ? Come fanno a starci tutti?.....	123
8-16. Dopo l'installazione, solo un pallino verde.....	125

8-17. Inutilizzabile, per via dell'antivirus fasullo però .....	125
8-18. In effetti un antivirus mancava.....	126
8-19. Veramente non ho alcuna chiave, io .....	127
8-20. Finalmente, non ci speravo più .....	128
8-21. Qui c'è anche un grafico animato .....	133
8-22. Questo ha i "bollini" di certificazione .....	135
8-23. Altra versione dello stesso .....	135
8-24. Questo mette anche fretta a chi lo visita.....	136
8-25. ... non perdere tempo a leggere, scarica, PRESTO!.....	137
8-26. Solo la scansione è gratuita, questo almeno lo dice.....	138
8-27. All'avvio una bella scansione .....	140
8-28. I risultati sono disastrosi, naturalmente.....	141
8-29. ...sempre e comunque disastrosi .....	142
8-30. Ma i numeri sono praticamente a caso .....	143
8-31. Ben quattro programmi per ottimizzare e verificare.....	144
8-32. Per sicurezza, disabilita Windows Defender.....	146
8-33. Una serpe in seno .....	148
8-34. Dopo il velocizzatore, il rallentatore.....	150
8-35. In cinque hanno tentato, in cinque hanno fallito.....	151

## Un libro nato vecchio

Il libro che state leggendo è nato nella sua forma definitiva nella prima metà del 2011, frutto di un lavoro di scrittura e revisione partito nel 2009. Le ragioni per cui sia successivamente rimasto nel limbo per oltre un anno, invecchiando e perdendo di “novità” sono complesse e non mi sono ancora del tutto chiare.

Fatto sta che il tempo passa, e il contenuto di questo libro viene ogni giorno sorpassato dagli eventi. Uno dei punti cardine che vado ad evidenziare nel resto del libro è che l’obiettivo non è più soltanto il nostro computer, ma sono i nostri dati, ovunque siano presenti, soprattutto quando sono concentrati in un unico punto: i fornitori di servizi. Le innumerevoli prodezze di *LulzSecurity* e di *Anonymous*, due gruppi di attivisti nel campo politico e della sicurezza, hanno non solo dimostrato, ma reso obsoleto quello che dicevo.

Un capitolo è dedicato alle capacità distruttive di un malware piuttosto sofisticato, ZeuS, che oggi viene lentamente rimpiazzato da alcuni agguerriti concorrenti, il cui scopo rimane però lo stesso: collezionare e trafugare informazioni.

Un altro capitolo è dedicato all’allegria e spensierata famiglia degli utenti di *peer-to-peer*, sia esso Emule o BitTorrent. L’avvento del *cloud*, che in tutte le declinazioni inventate dal marketing nasconde un computer che ne contiene altri, virtuali, ma con tutti i problemi reali di un normale computer, ha dato vita al fenomeno del *file sharing* tramite i tanti siti di scambio file diretto. Il caso di Megaupload ha dimostrato quanto il *cloud* sia evanescente, facendo letteralmente evaporare terabyte di dati regolarmente e legalmente memorizzati da utenti che impiegavano in modo corretto questi servizi (per backup, distribuzione file personali, foto di famiglia) quando la Legge si è abbattuta su di esso.

Le varie società di sicurezza stanno lentamente accorgendosi del pericolo dei software “apparentemente” utili, mentre il caso di Italia-Programmi.net ha dimostrato al di là di ogni dubbio che siamo pronti a rivelare qualsiasi informazione ci venga chiesta da uno sconosciuto nel modo giusto, informazione che non riveleremo al nostro migliore amico.

Insomma, non tutto è da buttare, di questo libro, sicuramente per chi non ha “il polso della situazione” è un buon aggiornamento. Per chi segue da vicino le vicende del mondo dei bit non è certamente una primizia.

Per questi motivi, e per altri con cui non sto a tediarvi, ho deciso di rendere pubblico questo lavoro a costo zero, per chi lo vorrà leggere. Per me il costo è stato alto, si tratta di parecchio lavoro per cercare, selezionare, verificare ed incrociare fonti e notizie, oltre a una notevole dose di esperienza personale, sudata e guadagnata anche a prezzo di una gastrite, ma a volte le cose vanno così e c'è poco da fare se non accettarle come sono.

Ho riscoperto con gioia una vecchia passione che mi sta dando molte soddisfazioni: i mattoncini LEGO®. Se pensate che questo libro valga la pena di essere letto, potete ringraziarmi con un sacchetto di mattoncini, anche usati, purché originali LEGO®.

# Capitolo 1. Prima di iniziare

## Introduzione

Pomeriggio di un lunedì non proprio qualsiasi. Fra poco il Presidente della Repubblica Napolitano si collegherà con la Stazione Spaziale Internazionale<sup>1</sup> per salutare due astronauti italiani, Paolo Nespoli e Roberto Vittori. Due Italiani nello spazio, nello stesso momento, fatto a dir poco storico. In un momento come quello attuale, sento il bisogno di sapere che abbiamo persone come loro, per restituirmi un po' della dignità di essere Italiano.

E' tutto pronto: computer acceso, cuffia stereo per non perdere neanche una sillaba, due finestre aperte sul desktop, una sul sito dell'ESA<sup>2</sup>, una sulla televisione web in alta definizione della NASA<sup>3</sup>.

Squilla il telefono.

“Pronto?”

“Sono io.”

Alzo gli occhi al cielo: chiunque, ma non *lui*, non proprio adesso. Rassegnato: “Dimmi, che succede?”

Polemico: “Non deve mica succedere qualcosa per chiamarti. Ti chiamo anche senza che sia successo niente. Qualche volta.”

Non mi faccio ingannare, solo che non ho voglia di mettermi a giocare a gatto e topo, il collegamento sta per iniziare. “Va bene, se non c'è urgenza possiamo sentirci fra mezzora?”

Ignora completamente la mia richiesta: “No, dai, seriamente, ho un problema.”

*Ma non mi dire!* - penso, ma mi mordo la lingua. Taccio, per non incoraggiarlo. Invece lui prende il mio silenzio come un invito a proseguire: “Sai come si fa a togliere i soldi dalla carta di credito?”

- 
1. [http://www.esa.int/esaCP/SEMFUYMSNNG\\_Italy\\_0.html](http://www.esa.int/esaCP/SEMFUYMSNNG_Italy_0.html)
  2. <http://www.esa.int/esaCP/Italy.html>
  3. <http://www.ustream.tv/nasahdtv>

“Comprandoci le cose. Ma che razza di domanda è?!”

“No, aspetta, mi sono spiegato male. Ho una carta ricaricabile, come faccio a recuperare i soldi che ci ho messo?”

Un sospetto prende forma: “Se il tipo di contratto che hai con la carta lo permette, puoi andare ad uno sportello bancomat e prendere i soldi lì, ma c’è un massimo che puoi prelevare ogni giorno ed ogni mese.”

“E quant’è il massimo?”

Sto per spazientirmi, e sulla web-tv della NASA si vedono gli astronauti prendere posizione per il collegamento. “E che ne so? Il contratto lo hai tu, la carta ce l’hai tu, perché lo chiedi a me?”

Finalmente ci siamo: “No, niente, è che dopo che *ci hai messo le mani tu*, il computer mi sembrava un po’ lento, allora ho scaricato un programma per verificare il registro di Windows...”

Eccola, la frase chiave: non importa quanto devastato sia un computer, dopo che ci metti le mani qualsiasi cosa succeda nei successivi due anni è *perché lo hai toccato*. Lo interrompo: “Lento? Beh, certo, prima non andava proprio, ora almeno qualcosa riesci a fare. Ci ho fatto le due di notte, mentre gli altri facevano conversazione, non so se ti ricordi...”, poi il significato di quello che ha appena detto mi arriva a pieno: “Tu hai fatto *cosa?!?*”

Inizia a parlare a precipizio: “No, aspetta, guarda che il programma mi ha trovato un sacco di problemi nel registro, proprio tanti, e molti li segnala come problemi di *privacy*. Allora ho comprato la versione completa, quella gratuita faceva soltanto la scansione, tanto costava poco. Il problema è che mi sono arrivati in breve tempo altri due addebiti sulla carta di credito, non molti euro per volta, ma in tutto siamo già a quasi centocinquanta euro. E se poi questi continuano?”

Sullo schermo il Presidente Napolitano sta parlando, ed io non ho la cuffia indosso. “Fammi capire, dopo che ho lavorato per una intera serata sul tuo computer per rimmetterlo in condizione di essere usato, tu decidi che è troppo lento, per fare cosa non si sa, e ti affidi al primo programma scaricato da Internet che ti promette di far tornare il computer come appena comprato? Mi pareva di averti già spiegato, più di una volta, che l’unico sistema per far tornare il tuo computer co-

me appena comprato è cancellare tutto e ripartire da zero, installando un decimo dell'immondizia che c'è ora.”

“Sono tutti programmi che uso, mi servono. E poi guarda che il programma funziona, adesso quando navigo in Internet è velocissimo. Anche se trovo spesso le pagine dei siti non aggiornate...”

“Certo, ti ha impostato il browser per controllare solo una volta se la pagina che ha in *cache* è più vecchia di quella remota. E scommetto che ti ha messo il tema del desktop come se fosse Windows 2000, giusto?”

“...sì, ma che c'entra? Pensavo fosse una mia manovra sbagliata.”

“L'unica manovra sbagliata è stata quella di aver scaricato quel programma.”  
*L'errore vero è aver comprato il computer* penso, ma non è il caso di infierire. “Ti ha eliminato tutti gli effetti grafici aggiuntivi, una cosa che potevi fare da solo senza spendere un centesimo. Ora sarà anche difficile rimuoverlo, il programma, vedrai.”

“In effetti ho provato a rimuoverlo e mi ha dato un errore. L'iconcina vicino all'orologio è ancora lì, ma mi dice che il programma non può essere rimosso. Non è che puoi venire...”

Sullo schermo i due astronauti stanno mostrando una bandiera italiana. “NO. Chiama il numero per bloccare la carta. Aspettati altri addebiti a breve.”

Insiste: “E' che mi stanno arrivando parecchie e-mail di notifica da Facebook di amici che si lamentano per un link che avrei inviato, ma io non ho inviato niente. Solo che appena provo ad entrare su Facebook 'sto cavolo di programma che ho comprato blocca tutto, segnalando dei pericoli per la *privacy*.”

Stavolta non ce la faccio a trattenermi: “Da non credere, l'ha capito anche un programma pensato per svuotare le carte di credito ai polli.”

Attraverso il telefono sento un trillo. Un momento di silenzio, poi: “Mi hanno preso altri cinquanta euro! Scusa, ci sentiamo dopo” e la telefonata termina.

Sullo schermo, nel sito dell'ESA c'è un monoscopio, mentre la televisione web della NASA mostra l'interno della Stazione, ma non c'è nessuno in vista. Il collegamento è finito e l'equipaggio ha ripreso le proprie occupazioni.

Sipario.

Dell'episodio raccontato, naturalmente, l'unica cosa successa realmente è il collegamento fra il Presidente Napolitano e i due astronauti a bordo della stazione, che ho potuto seguire in tutta tranquillità, avendo preventivamente staccato i telefoni.

In ogni caso, nessuno dei fatti che ho raccontato è del tutto inventato. Programmi che spaventano e confondono le persone per farsi acquistare, rivelandosi quanto meno di dubbia utilità per chi li compra e strane epidemie di *like* su Facebook sono purtroppo due delle tante forme che hanno assunto i rischi per la nostra sicurezza al computer.

## Perché

A distanza di alcuni anni dalla pubblicazione del mio precedente libro, “Windows XP in sicurezza”<sup>4</sup>, vari motivi mi hanno spinto a riprendere in mano il testo e vedere cosa è ancora valido e cosa non lo è più.

Il primo motivo è sempre l'aura magica che circonda in generale tutto quello che ha a che fare con i computer, immutata nonostante gli anni trascorsi, a cui si aggiunge la novità relativa di Internet, almeno per molte persone, anch'essa con il suo contorno di miti: su Internet si trova tutto, basta scovare il sito giusto.

Anche stavolta la risposta a questa affermazione è un sonoro *NO*. Internet non è l'albero della cuccagna. Non lo è mai stato e non lo sarà mai. Chi offre beni e servizi su Internet lo fa per soldi, quindi anche le cose che *sembrano* gratuite, in qualche modo, non lo sono. Se poi quello che andiamo a cercare è illegale, o comunque non è qualcosa di cui si può conversare a cena con i bambini presenti, siamo destinati a cadere vittime di chi conosce perfettamente questa inclinazione umana ed è pronto a sfruttarla, senza scrupolo alcuno, per i propri scopi.

Un altro motivo è l'esplosione dei cosiddetti *social network*, con la grave sottovalutazione relativa ai dati personali diffusi da ognuno di noi, consapevolmente o meno. Pochissime persone hanno coscienza di quante informazioni lasciano volontariamente in giro sui tanti servizi disponibili in Internet. Questi dati sono

---

4. <http://www.apogeonline.com/libri/88-503-1008-0/scheda>



preziosissimi, come vedremo, e tante sono le trappole congegnate per convincerci a rivelare spontaneamente cose che non diremmo ai nostri vicini di casa.

Nella precedente versione eravamo concentrati su Windows XP e su come renderlo ragionevolmente sicuro: molte delle regole e delle strategie sono tuttora valide ed applicabili, ma non è più sufficiente. Le nostre abitudini si stanno modificando: il nostro computer rimane un bersaglio primario, ma si aprono nuovi fronti, con nuove falle e nuove vulnerabilità, su cui non abbiamo alcun controllo, né possiamo rimediarvi direttamente.

Stavolta il nemico è molto più pericoloso: non si tratta solo di programmi automatizzati, le cui risposte sono limitate e prevedibili. Abbiamo di fronte delle trappole pensate per l'essere umano: il principale bersaglio siamo diventati noi. Trappole che possono assumere centinaia di forme differenti, e che sono in continua evoluzione. Non esiste una risposta per tutte, anche perché, al tempo in cui forse questa nuova versione vedrà la pubblicazione, ve ne saranno altre di trappole, a cui nessuno poteva pensare.

C'è una ragione di cauto ottimismo, però: le strategie di attacco non sono infinite, come invece lo sono gli strumenti. Se arrivassimo a identificare i principali bersagli e gli schemi di attacco, potremmo definire un ristretto numero di segnali da trattare come un allarme, a rivelare un potenziale tentativo di attacco. Questa è la nuova sfida.

## **Cosa c'è e cosa non c'è**

Se stiamo cercando un libro pieno di belle schermate a colori, con procedure passo-passo e di "sicuro successo", beh, mi dispiace, non è questo che avete per le mani: anche in questa nuova versione rimarremo delusi. Qui non si vendono ricette o strumenti magici: talismani e incantesimi li possiamo trovare presso qualsiasi esperto di magia, non qui.

Le immagini ci saranno, ma spesso serviranno a mostrare il risultato di manovre sconsiderate o di operazioni che di solito facciamo nella modalità "cervello spento".

Se qualcuno ci proponesse l'acquisto di un particolare portafogli, presentato come capace di sventare qualsiasi tentativo di borseggio, è probabile che gli ri-

deremmo in faccia, e sonoramente. Eppure in informatica la sicurezza è vista in questo modo: l'acquisto dello strumento giusto. Ho usato deliberatamente il verbo *acquistare* e non il verbo *impiegare* per un motivo preciso: troppo spesso vedo strumenti di sicurezza acquistati e mai utilizzati a dovere.

Il compito è arduo: se per proteggere il nostro computer si possono adottare comportamenti e strategie di provata efficacia, con il supporto di alcuni strumenti basilari, in Internet tutto questo non vale più: le regole sono totalmente differenti. E' più facile cadere vittima di qualche trappola ben congegnata, non si può oggettivamente sapere tutto.

Occorre trovare nuove strategie e soprattutto capire cosa vogliono da noi i tanti mentecatti che girano in Rete. Come abbiamo già detto, anche questa volta sarà una bella sfida.

## Cose di cui non voglio parlare

Vi sono poi delle cose di cui proprio non intendo parlare, in parte perché esulano dallo scopo di questo libro, ed in parte perché trovo che non possano aggiungere nulla a quanto verrà detto, o a quanto altri hanno già trattato.

Non parlerò di:

- Wi-Fi e sicurezza. E' un tema abbastanza ampio da meritare un testo a parte. Ne hanno parlato in tanti, meglio di quanto possa fare io. L'argomento diventerà sempre più attuale, in funzione di quanti punti di accesso liberi verranno installati, ma al momento, almeno in Italia, è un argomento tabù.
- Stuxnet. E' un malware molto particolare e, paradossalmente, rappresenta per gli utenti un pericolo veramente ridotto, dato che, da voci che si fanno sempre più insistenti in questo periodo, era una particolare arma di attacco puntata a certi impianti di raffinazione del combustibile nucleare.

Il pericolo è molto più grave per l'allegria sottovalutazione che i protagonisti diretti ed indiretti stanno dando all'accaduto: un malware in grado di cercarsi il bersaglio (un determinato sistema di controllo di una specifica installazione industriale) e *comprometterne il funzionamento*. Generatori di energia, impian-

ti di raffinazione carburanti, industrie chimiche, tanto per fare qualche esempio, rientrano tutti nella categoria “installazione industriale”. Quali sicurezze vengono attuate perché un malware come Stuxnet non possa spegnere una decina di centrali elettriche, magari nell’ora di punta?

- Tablet, smartphone e iCosi. Sotto altra forma, sono computer connessi a Internet, niente di più, niente di meno. Al momento non c’è motivo di dedicargli uno spazio distinto rispetto ad un normale computer. Il *phishing* funziona indipendentemente da come leggo la posta.

Ed uno smartphone colpito da un malware che riconosce un numero di carta di credito scandito a voce per telefono<sup>5</sup>, negli effetti, in cosa è differente da un computer in cui è annidato un keylogger?

- Crittografia come strumento di sicurezza. Nelle mani di chi non capisca a fondo funzionamento e limiti di questa tecnologia, per molti versi meravigliosa, non aggiungerebbe un grammo di sicurezza in più, ma alimenterebbe falsamente la sensazione di essere in una botte di ferro.
- Sistemi di autenticazione biometrici. E’ una mia opinione assolutamente personale, quindi criticabile a piacere: c’è un problema di fondo con questi sistemi, ossia che si basano su qualcosa che non è segreto, ma anzi lasciamo come una scia ovunque passiamo. Impronte digitali, DNA, la nostra faccia, il fondo della retina, il timbro di voce e innumerevoli altre “peculiarità” del nostro corpo sono certamente uniche, ma assolutamente note e riproducibili, spesso con poco sforzo e nessuna spesa. Se seguite Bruce Schneier<sup>6</sup>, vedrete che spesso pubblica articoli di ricercatori che con pochissimo impegno hanno ingannato i più disparati sistemi basati sulla biometria.

## Cosa occorre

Un computer con qualsiasi sistema operativo. Faremo comunque un ripasso delle regole di base e delle principali strategie difensive, generalizzandolo per

5. [http://www.schneier.com/blog/archives/2011/01/trojan\\_steals\\_c.html](http://www.schneier.com/blog/archives/2011/01/trojan_steals_c.html)

6. <http://www.schneier.com/>

qualsiasi sistema operativo.

Si presume che il lettore conosca il proprio sistema operativo, in particolare sappia effettuare le normali operazioni di gestione e configurazione del computer. E' inutile ripetere qui quello che si trova nelle guide fornite con i sistemi operativi.

## Legalese

Nel testo saranno spesso mostrati siti web il cui contenuto è da considerarsi ad alto rischio. In qualche punto saranno mostrate alcune procedure, il cui uso fuori contesto e senza coscienza di cosa esattamente si stia facendo 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 *dieci minuti* potrebbe non valere più.

Infine: 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, tanto meno, lo posso fare con questo testo: ogni giorno qualcuno inventa 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

A computer spento e cervello acceso, niente altro. Fine delle raccomandazioni.

## Capitolo 2. Ri-conosci il Nemico

Siamo già in guerra. Il nemico appare mutevole e pieno di risorse. Ogni giorno una tecnologia, un servizio o un protocollo usato da decenni diventa un'arma di offesa. Non c'è limite alla fantasia perversa di chi vuole mettere le mani nel nostro portafogli e nella nostra vita privata. Sappiamo che il nemico c'è, il problema è riconoscerlo.

### I problemi di qualsiasi sistema operativo

Mi capita troppo spesso di assistere a discussioni sulla presunta superiorità di questo o quel sistema operativo, questo o quel programma, questa o quella tecnologia. Ho sempre sostenuto e sostengo che la presenza di discussioni interminabili è la più lampante dimostrazione che *non vi sono elementi definitivi* per determinare chi sia il migliore, per cui le discussioni e le prese di posizione sono solo un inutile dispendio di energia. Senza contare che nella quasi totalità dei casi gli argomenti portati a sostegno delle varie tesi sono inconsistenti, a voler essere buoni.

Semmai la discussione dovrebbe essere orientata su argomenti del tutto differenti, come ad esempio la libera utilizzazione e la trasparenza nel trattamento delle informazioni, ma questa è una storia totalmente differente, e ne parleremo più volte nel seguito.

Questa lunga premessa è per dire che nessun programma, quindi nessun sistema operativo, che è in definitiva un programma molto grande e complesso, è esente da errori e difetti. Proprio come non esiste un sistema operativo, per quanto ben progettato e realizzato, tale da non poter essere usato talmente male da essere una vera e propria calamita di catastrofi. Come sempre non è la racchetta che crea il tennista, l'ho già detto e lo ripeterò fino alla nausea.

Quindi, assunto numero uno: qualsiasi computer che esegua un programma può nascondere uno o più probabilmente molti difetti, alcuni dei quali possono diventare porte di ingresso per il Nemico.

## Anatomia dei malware

Ne parliamo in continuazione, li nominiamo, li combattiamo e spesso li sperimentiamo sulla nostra pelle, ma poco sappiamo di come siano fatti i malware. Vediamo di mettere qualche punto fermo, prima di proseguire: servirà a impedire fraintendimenti e incomprensioni.

Prima di tutto, un malware è un software. Quale che sia il linguaggio, quale che sia la funzione, quale che sia lo scopo, si tratta di un programma, niente di più, niente di meno.

Questo programma ha differenti funzioni, progettate per lo scopo che il creatore si è prefisso e, per quante possano essere, le possiamo dividere in un numero non troppo esteso di categorie:

- Propagazione. L'insieme delle funzioni previste per la diffusione del malware, ossia il mezzo con cui si propaga da un computer colpito ad uno integro.
- Attacco. Il sistema con cui oltrepassa le difese del computer bersaglio.
- Innesadimento. Le operazioni eseguite per consolidare la propria presenza nel computer "conquistato"
- Carico bellico (in inglese: *payload*). L'attività che intraprende una volta innesadito nel computer conquistato.
- Contromisure. Strategie con cui impedisce sia la rilevazione sia la rimozione dal computer colpito.

Non è detto che un malware possieda tutte le funzioni elencate. Vediamo qualche esempio reale, per capire come la nostra classificazione si sposa con i malware conosciuti:

- SQL Slammer/SQLExp<sup>1</sup> - Propagazione: si trasferisce via rete da un computer infetto all'altro. Attacco: sfrutta una vulnerabilità del software per far eseguire codice arbitrario. Innesadimento: unicamente in memoria, nessun file viene crea-

---

1. [http://www.symantec.com/security\\_response/writeup.jsp?docid=2003-012502-3306-99](http://www.symantec.com/security_response/writeup.jsp?docid=2003-012502-3306-99)

to o modificato nel computer colpito. Carico bellico: soltanto la propagazione, diffusione verso altri computer. Contromisure: nessuna.

- Conficker C<sup>2</sup> - Propagazione: rete, supporti removibili. Attacco: via rete, sfrutta una vulnerabilità del sistema operativo; se il sistema operativo è aggiornato, tenta un attacco a dizionario sulle cartelle condivise; nei supporti removibili usa il meccanismo di *autorun*. Insediamento: crea file dal nome casuale nel disco del computer colpito, modifica alcuni servizi di sistema, apre una backdoor attraverso il firewall del computer. Carico bellico: aggregazione ad una botnet, compiti aggiuntivi decisi da chi controlla la botnet, attraverso aggiornamenti automatici del malware. Contromisure: occultamento in particolari chiavi di registro delle istruzioni per l'avvio; modifica dei permessi di accesso alle aree modificate del registro; ricerca attiva e terminazione di un nutrito elenco di applicazioni di sicurezza (antivirus, programmi di gestione ed aggiornamento, programmi di configurazione, ecc.); blocco degli aggiornamenti degli antivirus; blocco della navigazione Internet verso determinati siti web, tramite inquinamento del servizio di *cache* DNS.
- Zbot<sup>3</sup> (ZeuS Bot)<sup>4</sup> - Propagazione: campagne di spam, server trappola, *social engineering*; il malware non ha capacità di diffusione autonoma. Attacco: iniettato attraverso vulnerabilità nel browser o inducendo la vittima (umana) ad attivarlo; il malware non ha capacità di attacco in sé, necessita di un meccanismo esterno per essere depositato nel computer vittima. Insediamento: se avviato da un account amministrativo, si inserisce nelle cartelle di sistema, altrimenti in quelle dell'utente che lo ha attivato; modifica chiavi di registro per essere avviato alla partenza del computer; apre una backdoor, ed attraverso il protocollo UPnP tenta la configurazione di un eventuale router locale; scarica la configurazione dal server da cui dipende. Carico bellico: aggregazione in botnet; furto di informazioni; furto di credenziali bancarie; controllo remoto del computer. Contromisure: usando tecniche da rootkit, rende invisibile la propria esecuzione, tanto da non apparire nell'elenco dei processi attivi.

---

2. <http://mtc.sri.com/Conficker/addendumC/>

3. <http://www.fortiguard.com/analysis/zeusanalysis.html>

4. <http://www.symantec.com/connect/blogs/brief-look-zeuszbot-20>

Con solo tre malware piuttosto conosciuti abbiamo un quadro di come possano essere costituiti i malware e di come funzionino, a grandi linee. Possiamo anche vedere la grande varietà di tecniche e di strategie per ottenere il risultato voluto, quale che sia. Torneremo più avanti su Zbot, dedicandogli un intero capitolo.

Per intanto, possiamo prendere spunto da quanto detto qui per notare innanzitutto che parlare genericamente di virus o di malware non è soddisfacente. Data la grande varietà di funzioni e comportamenti, pensare ai malware soltanto come programmi dannosi che si propagano via rete sfruttando vulnerabilità del sistema operativo è oggi estremamente riduttivo: esistono malware che non sfruttano nessuna vulnerabilità, o che comunque sono in grado di diffondersi in assenza di esse.

Altra cosa degna di nota: per operare a piacimento, i malware sfruttano in gran parte di casi le funzioni messe a disposizione dal sistema operativo, ossia non fanno nulla di “illegale”, dal punto di vista dell’integrità del sistema operativo stesso.

## **Mitologie pericolose**

Ora che abbiamo chiarito, a grandi linee, come sono fatti e quali funzioni possiedono i malware, passiamo ad esaminare alcune convinzioni che mettono a repentaglio la sicurezza dei nostri computer, snocciolate come verità assodate ed incontestabili. Ecco le più pericolose.

### **Niente virus (leggi malware) per Linux**

Possiamo sostituire “Linux” con altro nome a piacere, purché diverso da Windows. Per prima cosa occorre definire esattamente cosa si intenda con “virus”. Come spesso fa chi vuol avere ragione a tutti i costi, ci si mette a cavillare sul termine, dicendo che il virus è quello che si “attacca” ai programmi, modificandoli, e replicandosi all’interno di un computer fino a conquistare tutti i file eseguibili disponibili, affermando poi che non ne esistono per Linux, perché l’architettura non lo permette. Ebbene, abbiamo una serie di brutte notizie. I virus



di questo tipo sono perfettamente realizzabili<sup>5</sup> anche in Linux, in Rete si trovano vari articoli<sup>6</sup> anche non troppo vecchi sull'argomento<sup>7</sup>.

Quindi, virus ve ne sono e si possono creare. Vogliamo, per amore di discussione, considerare nulli i virus per Linux, perché nessuno ne ha mai sentito parlare o perché non hanno fatto grandi danni? Linux (e Unix in generale) ha un paio di primati che Windows non ha. Il primo worm (malware che si propaga e replica via rete senza intervento umano) che ha fatto grandi danni era il Morris worm<sup>8</sup>, nel 1988, che prendeva di mira alcuni servizi di Unix per trasferirsi da un computer all'altro. Colpì circa 6.000 computer sull'allora nascente Internet, che contava un totale di 60.000 computer collegati: a conti fatti ne colpì il dieci per cento. Si stima che il costo della rimozione sommato al costo dei disservizi abbia superato il milione di dollari. I servizi colpiti facevano capo a programmi ancora oggi utilizzati in Linux, fra cui **sendmail**, il server di invio posta elettronica tuttora presente in molte installazioni (naturalmente la versione usata oggi non ha più le falle che permisero la creazione del worm).

Il secondo primato è quello dei *rootkit*. Questo tipo di malware nasce proprio nei sistemi operativi Unix/Linux, e, come suggerisce il nome stesso, serve a far guadagnare il livello amministrativo massimo, *root* appunto, all'attaccante, ottenendo un controllo pressoché completo sul computer colpito. Oltre questo, molti *rootkit* mettono in atto sofisticatissime tecniche per nascondersi agli occhi dell'amministratore legittimo, che praticamente non ha più la reale disponibilità del computer, ma non ha modo di rendersene conto. Questo metodo di attacco, che mira a poter gestire il computer colpito come se fosse il proprio, rende perfettamente l'idea del perché un computer colpito da un rootkit sia definito in gergo *owned* (di proprietà, che appartiene), a volte scritto *Own3d* o *pwned*: chi attacca si appropria del computer colpito.

Entrambi questi primati appartengono a Linux e Unix, non a Windows. Per cui, dato che stiamo parlando di informatica, in cui le cose sono o vere o false, non vi sono vie di mezzo, la risposta è che non solo esistono e possono esistere virus per Linux, ma anche volendo dar ragione a chi la vuole a tutti i costi, pos-

---

5. <http://vx.netlux.org/>

6. <https://help.ubuntu.com/community/Linuxvirus>

7. <http://linuxmafia.com/~rick/faq/index.php?page=virus>

8. [http://en.wikipedia.org/wiki/Morris\\_worm](http://en.wikipedia.org/wiki/Morris_worm)

siamo dire che anche i soli *rootkit* non ci fanno sentire la mancanza dei semplici virus. Quindi, a parte i virus, alcune delle categorie di malware più pericolose e sofisticate hanno visto la luce proprio in Unix/Linux.

Inoltre vi è un problema non da poco: nelle recenti versioni di Windows (da Vista in poi, ma anche in Windows XP il sistema era parzialmente implementato) tutti i file vitali del sistema sono firmati crittograficamente (applicazioni, driver, librerie, ecc.) e qualsiasi modifica ad uno di essi viene immediatamente rilevata e segnalata, arrivando a rifiutare l'avvio del sistema se il file modificato è particolarmente importante. Questo taglia fuori i virus dal poter attaccare direttamente punti vitali del sistema modificando gli eseguibili, come vuole la definizione esatta di *virus* (naturalmente, tutti gli altri file eseguibili restano attaccabili, è sufficiente che il virus eviti quelli con la firma crittografica).

In Linux questa firma crittografica è riservata soltanto al kernel ed ai propri moduli, nessun eseguibile o libreria è firmata crittograficamente, né viene controllata all'avvio per verificare modifiche fraudolente.

Tutto questo per dire quello che per un esperto di sicurezza è già evidente: il problema non riguarda solo i virus propriamente detti, anche perché negli ultimi anni questo specifico tipo di malware ha avuto pochissimo successo, perché troppo complicato da realizzare e troppo facile da scoprire. Il problema ben più grande è che i malware più pericolosi sono programmi indipendenti, che hanno un proprio file eseguibile (spesso più d'uno), capaci di fare di tutto e di più senza nessuna necessità di andare a modificare i file di sistema o delle applicazioni. Non c'è proprio alcun bisogno di complicarsi la vita andando a spaccare il cappello in quattro per iniettare specificamente un virus nel computer delle vittime. Tutto può essere realizzato in modo molto più semplice con programmi di attacco indipendenti ed autosufficienti.

## **Perché Windows è l'unico colpito?**

La domanda è sbagliata. Per prima cosa perché non è vero che sia l'unico colpito, basta cercare in Rete per convincersi. E prima che qualcuno se ne esca col ragionamento "ma ne esistono pochissimi e vecchissimi per il mio sistema operativo (o programma) preferito", qui siamo purtroppo nella zona binaria del

“o è vero, o è falso”. Per citare un noto film: “se sanguina, allora può essere ucciso”, cioè: se il sistema è inattaccabile non ne deve esistere nemmeno uno. Se ne esiste anche uno solo, allora non è più possibile usare la parola inattaccabile.

Supponiamo di essere molto abili nel capire come aprire una cassaforte. In una città di un milione di abitanti, tutti egualmente ricchi, sono in uso tre differenti modelli di cassaforte: il modello A è usato dal novantasei per cento degli abitanti, il modello B è usato dal tre per cento ed il rimanente un per cento usa il modello C. Domanda: dovendo acquistare un modello per capirne i punti deboli, e quindi poter aprire tutti gli esemplari dello stesso tipo con poco sforzo, quale prenderò?

Sì, è un argomento desolatamente banale, ma se l'interesse del Nemico è colpire nel mucchio più grosso, perché conta il numero e niente altro, le discussioni sono solo aria fritta. E possiamo star certi che al Nemico interessa conquistare molti computer, per gli scopi che si prefigge, e che vedremo più avanti.

C'è anche un altro argomento, a sostegno di questa tesi: in una particolare categoria di attacchi, i computer più colpiti usano proprio Linux: sul web, dove le applicazioni fatte con il linguaggio PHP mostrano spesso gravi falle, i nostri amici mentecatti ne fanno strage. Perché in questo specifico caso il più diffuso è proprio PHP su piattaforma Linux. Soltanto che per un sito web, ed il rispettivo server, esistono centinaia di migliaia di computer che usano Windows. Nel seguito scopriremo anche che i due mondi saranno uniti nello stesso destino: web server Linux compromessi e usati come veicolo di infezioni per Windows.

Il bersaglio dipende dall'uso che il Nemico ha in mente. Tutto qui.

## **Unix è più sicuro di Windows**

Questa affermazione era certamente valida per le versioni di Windows 95/98/ME, che non prevedevano né una qualsiasi forma di multiutenza reale, né, di conseguenza, una reale separazione dei privilegi, per cui qualsiasi cosa arrivasse a mettere i piedi nel computer era automaticamente ed immediatamente in grado di operare con i massimi privilegi, quindi fare il comodo suo.

Con Windows XP (in realtà già a partire da Windows NT) le cose erano già cambiate parecchio, tanto che utilizzando le strategie e le regole esplicitate nel libro precedente, si poteva raggiungere un livello di sicurezza simile a quello di

un sistema Unix. Oggi i due sistemi operativi sono tutto sommato paragonabili, tanto che le strategie e le tecniche usate da uno le possiamo trovare implementate nell'altro.

Unix, e quindi anche Linux, risente del fatto che parte del suo codice è stato scritto in anni lontani, informaticamente parlando, quando l'attenzione alla sicurezza non era alta come oggi, e purtroppo questo potrebbe riservare brutte sorprese. Proprio nei giorni in cui sto scrivendo questo capitolo, Joanna Rutkowska<sup>9</sup>, una ricercatrice di sicurezza che mi sentirete nominare spesso, ha scoperto un problema di sicurezza molto grave in Linux<sup>10</sup>, presente fin dall'introduzione del kernel 2.6, di cui nessuno si era ancora accorto. Un problema che sfrutta una falla progettuale, non un bug, quindi molto più grave, e che è presente dal 2004, anno di introduzione della serie 2.6 del kernel. Per sfruttare questa falla, però, è necessario utilizzare il server grafico, l'*X server*, il cui progetto è molto più vecchio. Quando siano presenti questi due componenti, e lo sono sempre in distribuzioni Linux che hanno un desktop grafico, è possibile usare un processo lanciato da un utente non privilegiato per acquisire i diritti amministrativi massimi, quindi aggirare del tutto la separazione dei privilegi, fulcro della sicurezza in Linux. L'eventuale presenza di SELinux in questo specifico caso *non pone alcun ostacolo alla conquista dei privilegi di root*. Quindi, se mai vi fosse bisogno di ulteriori dimostrazioni che nessun software, per quanto sofisticato e ragionato, è esente da problemi, questa forse è la migliore.

Tornando all'affermazione nel titolo, è oggi passibile di essere trattata come mal posta. La domanda chiave oggi è diventata: cosa rende un sistema operativo più o meno sicuro rispetto ad un altro? La risposta sta sempre più diventando: quello che sta fra la tastiera e la sedia, ossia l'essere umano.

Mia moglie ha usato Windows XP per sette anni, sullo stesso computer. Per sette anni ha navigato in Internet, letto posta elettronica, scritto documenti e realizzato lavori nel suo campo di specializzazione, che sono le menti umane (è psicologa). Usava Internet Explorer per navigare, visto che alcuni siti web istituzionali che visitava per lavoro non funzionavano con alcun altro browser. Il suo computer, configurato e gestito con tutte le strategie descritte nel libro precedente,

---

9. <http://invisiblethingslab.com/>

10. <http://theinvisiblethings.blogspot.com/2010/08/skeletons-hidden-in-linux-closet.html>

aveva un antivirus installato che non ha mai avuto un solo giorno di lavoro: nel computer non è mai arrivato un singolo malware, di alcun tipo.

Di contro, conosco persone che non usano Windows da anni e che se mai dovesse diffondersi un malware dei più semplici per il loro sistema operativo sarebbero i primi a caderne vittime.

Ancora, di nuovo, non è la racchetta che fa il tennista, non è il bisturi che fa il chirurgo, non è il sistema operativo che fa la sicurezza.

## Il Mac è invulnerabile a tutto

Il sistema operativo di Mac, OS X, pur presentandosi in modo molto elegante e assolutamente amichevole all'utente, è una variante di Unix. Il fatto che non sia attaccabile dalla pleora di virus che invece assedia i computer con Windows rende gli utilizzatori di Mac piuttosto confidenti nelle capacità del proprio computer.

Forse eccessivamente confidenti, tanto da arrivare ad altezze inarrivabili di ingenuità. Per quanto sofisticato, per quanto differente da Windows e da Linux, Mac OS X non ha realmente nulla di diverso da qualsiasi altro sistema operativo, dal punto di vista della sicurezza. Ha i suoi bug, i suoi aggiornamenti periodici, le sue vulnerabilità ed i suoi malware.

Per spiegare meglio quale sia il pericolo di una convinzione errata di tale portata, la cosa migliore è andare a vedere una situazione reale che ci permetta una dimostrazione per assurdo.

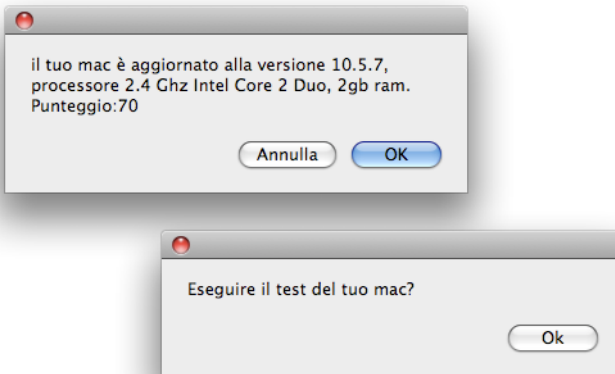
L'azione si svolge nel giugno 2009, in un forum per gli utenti italiani di Mac<sup>11</sup>. Uno di essi, che chiameremo *MaWi* da ora in poi, offre un programmino "autocostruito" che, testuali parole, "praticamente con una scala da 1 a 10 valuta la potenza del mac eseguendo 2 test". Inserisce un messaggio con un link al file, e prontamente interviene uno dei moderatori del forum, che elimina il link e ammonisce l'utente, attenzione, non proibendo di offrire file, ma impostando la reprimenda su una questione di correttezza, chiedendogli poi se abbia un sito web personale dove rendere disponibile il file. Alla risposta negativa di *MaWi*,

---

11. <http://www.italiamac.it/forum/showthread.php?t=333757>

il moderatore chiede di inserire qualche schermata del programma. Intervengono altri utenti che chiedono di avere maggiori dettagli sul programma, e suggeriscono di mostrare schermate e descrivere meglio le funzioni del programma. Lo stesso moderatore rinnova la richiesta di inserire immagini del funzionamento del programma. Altri utenti, incuriositi, insistono per provare l'applicazione. *MaWi* inserisce prima due piccole immagini, che mostrano due pannelli anonimi con messaggi relativamente generici, chiedendo se può mettere il link al file. Altri utenti incalzano, ansiosi di provare l'applicazione. Il link ricompare. Sono passati in tutto poco più di quaranta minuti. Nei minuti successivi almeno tre utenti del forum scaricano e provano l'applicazione.

**Figura 2-1. Le immagini mostrate da *MaWi***



Il risultato è facile da immaginare, ed è la migliore dimostrazione possibile che nessuno strumento di sicurezza, nessun sistema operativo e nessuna contromisura può salvare l'utente sprovveduto. Per chi non ha voglia di andarsi a leggere tutta la conversazione sul sito (al momento in cui scrivo, l'intera discussione non è più accessibile pubblicamente), riassumo brevemente quello che avviene dopo: l'applicazione si rivela essere un programma dannoso, che si limita a cancellare

tutto quello che trova nello spazio dell'account utente da cui viene avviato, terminando tutte le applicazioni prima di uscire. Il computer diviene inutilizzabile fino al riavvio, per la mancanza di interfaccia utente, terminata dal programma. Dopo il riavvio, l'account utente è vuoto, vergine, come su un computer appena acquistato.

L'utente viene "bannato" dal forum, si elimina il link al programma, ma il danno è fatto.

Se e come ci si poteva rendere conto che era una trappola? Beh, siamo alle basi: è il più stereotipato modello dell'accettare caramelle da uno sconosciuto. L'utente si era iscritto poco prima al forum, quindi uno sconosciuto a tutti i frequentatori abituali del forum stesso, nel limite della possibilità di considerare "conoscenza" il leggere messaggi praticamente anonimi su un sito web. Ha usato una tecnica psicologica semplice ma efficace: la richiesta d'aiuto e consiglio.

Assolutamente emblematica la discussione che ne segue, sul forum stesso, dove appare potentemente il livello di impreparazione degli utenti, ed il livello mitologico delle certezze:

"si ma tutti dicono che il mac non prende virus"

"Ma prima di cancellare tutto, vi ha chiesto la pwd di root?"

"vi ha chiesto la password di root immagino...e vi fidate così al volo di tutti?"

"non l'ha chiesta!!"

"ma sbaglio o senza password dovrebbe metterti tutto nel cestino?"

"mah in teoria basta avere disabilitato l'utente root no?"

"allora sarà bene informare qualcuno, tipo inviare una email alla apple, e sperare che questo tipo di cose non sarà più fattibile"

L'applicazione era un semplicissimo script shell che si limitava a cancellare le principali directory nella *home* dell'utente. Usando soltanto i privilegi dell'utente che lo avviava, era perfettamente in grado di cancellare tutto, senza alcun ostacolo.

Pure in questo caso il problema si trova fra la tastiera e la sedia. Ed a questo tipo di problemi non c'è rimedio.

## Un sistema operativo sicuro segnerà la fine dei malware

Anche qui, niente di più fuorviante. Questa fede nella tecnologia è disarmante, ed è difficile far capire che quando hai contro un essere pensante, qualsiasi tecnologia è destinata a soccombere.

Quello che succederà quando finalmente sarà disponibile un sistema operativo totalmente sicuro *per progetto*, e sarà privo di falle utilizzabili come porte di ingresso da parte dei malware, è in parte visibile già oggi: Linux, Windows e Mac OS X hanno livelli di sicurezza che solo pochi anni fa erano impensabili. Se pensiamo che questo abbia scoraggiato minimamente chi crea malware, o che abbia reso meno efficaci i suoi prodotti, beh, dobbiamo ricrederci.

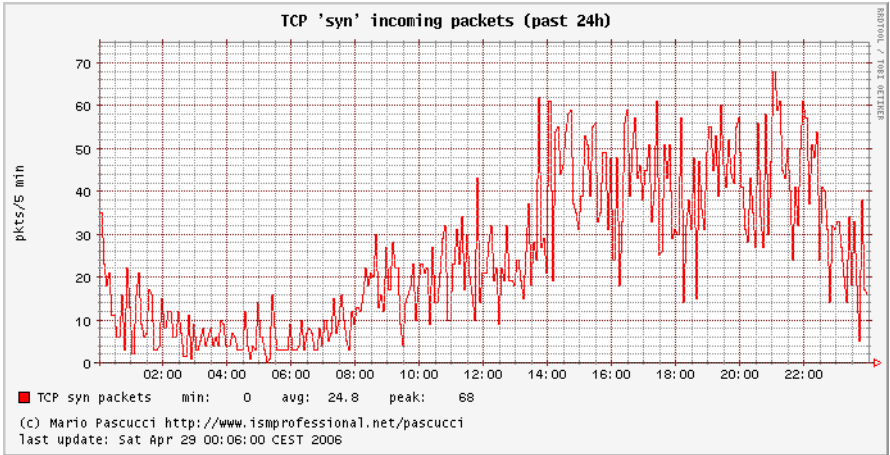
Supponiamo che finalmente i sistemi operativi diventino totalmente inattaccabili. Gli utenti dovranno sempre poter installare una applicazione o lanciare un programma preso da un supporto o da Internet, altrimenti verrebbe meno il senso stesso di uso del computer. Questa sarà la via per attaccare. Già oggi è così, e lo sta diventando sempre di più: molti malware non hanno alcuna capacità di propagazione, e quando la hanno, non sfrutta falle nel sistema operativo, ma falle nel modo in cui l'utente usa il computer. Inoltre non compiono operazioni "illegali" per il sistema operativo o per i suoi componenti: l'insediamento, l'occultamento, il contrasto alla rimozione sono realizzati sfruttando normali e legittime funzioni del sistema operativo stesso.

## Nuove strategie di attacco, nessuna di difesa

Dal 2007, fra aggiornamenti, Service Pack, bollettini di sicurezza e via andare, sono pochissimi ad oggi i computer non protetti da una qualche forma di firewall e da un sia pur modesto antivirus. Tanto è che gli attacchi tipici di alcune famiglie di malware non sono praticamente più efficaci, e lo testimonia la ridottissima quantità di scansioni casuali rilevabili su una qualsiasi connessione Internet.

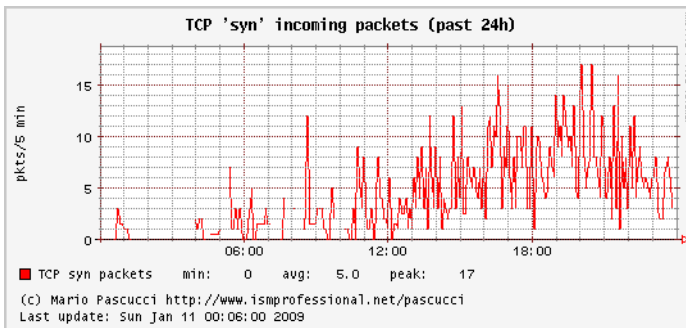


Figura 2-2. Il Virus Sensor nell'aprile 2006



Se avete letto il vecchio libro, ricorderete il Virus Sensor, mostrato a pagina 19, nel capitolo 3. Riporto la figura di allora, che mostrava le scansioni casuali in arrivo da Internet sulla mia ADSL, risultato di innumerevoli computer colpiti da un qualche malware che si propagava via rete.

Figura 2-3. Qui nel gennaio 2009



A distanza di tre anni, la situazione era molto cambiata: da picchi di oltre sessanta scansioni in cinque minuti, con una media sulle 24 ore di quasi 5 scansioni al minuto, siamo passati a picchi di 17 scansioni in cinque minuti, con una media sulle ventiquattro ore di una scansione al minuto. Tanto è che poco dopo ho provveduto a rimuovere il Virus Sensor: non forniva più indicazioni utili, ed andiamo a vedere perché.

La presenza di un firewall in tutti i computer, più la maggiore attenzione e tempestività nel correggere errori nei sistemi operativi e nelle applicazioni, ha reso molto poco vantaggiosa la realizzazione di un malware che sfrutti come sistema di propagazione soltanto attacchi ai servizi di rete: la presenza del firewall ha reso irraggiungibili i servizi vulnerabili, e comunque le vulnerabilità tendono a durare sempre meno tempo, vista la continua diminuzione del tempo che intercorre fra la scoperta della vulnerabilità ed il rilascio della correzione. Anzi, molti ricercatori di sicurezza, responsabilmente, rilasciano informazioni sulle vulnerabilità scoperte solo *dopo* che il produttore, notificato in anticipo, ha rilasciato la correzione.

Questo non ha per nulla scoraggiato i nostri amici mentecatti, che si sono dedicati a fare i compiti a casa, cercando altre vie per infilarsi nei nostri computer. I risultati non sono per nulla confortanti, per noi.

Pochi se lo aspettavano: sono ritornati in grande stile i malware che si propagano attraverso i supporti removibili, dati per estinti dopo l'archiviazione definitiva dei floppy, spinti dalla grandissima diffusione dei *pen drive* USB.

Altri hanno ripiegato su metodi di attacco che non assicurano il successo certo, ma consentono di raggiungere il risultato statisticamente, lavorando su grandi numeri: ecco quindi i malware che partono dal presupposto che nel computer non vi siano falle da sfruttare, contando invece sul fatto statisticamente provato<sup>12</sup> che molti utenti tendono a scegliere una password debole.

Il famigerato Conficker<sup>13</sup>, in tutte le sue varianti, sta eguagliando e sorpassando la diffusione degli storici Blaster e Sasser, usando come principale vettore

---

12. <http://www.schneier.com/crypto-gram-0612.html>

13. <http://mtc.sri.com/Conficker/>

di diffusione proprio i supporti USB, combinato con un attacco a dizionario sulle password di accesso al computer.

Altra strategia, resa efficace dal ritardo con cui gli utenti applicano gli aggiornamenti al sistema operativo e soprattutto alle applicazioni: attendere l'uscita di un aggiornamento di un sistema operativo o di un qualsiasi altro programma sufficientemente diffuso, esaminare dove interviene la correzione e da lì risalire alla vulnerabilità. In meno di 48 ore ecco in libertà, pronto a fare la sua porzione di devastazioni, un nuovo malware che sfrutta l'errore prima che tutti gli interessati applichino la correzione.

Quando nessuna di queste strategie funziona, si passa ad un altro metodo di attacco, infinitamente più semplice, ma non per questo meno efficace, ed in più trasversale, potendo applicarsi a tutti i sistemi operativi, senza eccezioni. Un click di troppo, un "Accetta" senza leggere con attenzione il testo riportato sopra il pulsante, un **Invio** senza pensare. Ed il Nemico ringrazia.

Se poi aggiungiamo la mancata applicazione dei più elementari concetti di "corretto uso", il gioco è fatto. L'uscita di Windows Vista, seguito a poca distanza da Windows 7, ha segnato di nuovo la sconfitta della strategia detta dei *privilegi sufficienti*. Ossia, l'account utente normalmente utilizzato deve avere i privilegi per l'attività ordinaria, niente di più. Detto in altre parole, *non serve un account amministrativo per scrivere una lettera*, o per navigare in Internet. Eppure, anche in questo caso si è preferito aggiungere una magia tecnologica, il famigerato User Account Control o UAC, per impedire, in teoria, che un programma tentasse di fare più di quello che dichiarava. Peccato che nel momento in cui UAC rilevi un comportamento "a rischio" di un programma *chieda all'utente cosa fare*. Un utente che di solito ne sa meno di lui. Una strategia che non ha molto senso, detta così.

Lo vedremo più avanti, quando studieremo il funzionamento di alcuni malware: nessuno sforzo è impiegato per ottenere i diritti amministrativi. Chi ha creato il malware *sa di averli già* nella quasi totalità dei casi. Perché perderci tempo?

Possiamo star certi che i nuovi malware sanno sfruttare i diritti amministrativi meglio di chiunque altro: all'epoca del libro precedente, antivirus e firewall venivano disattivati e resi inoffensivi. Ora i malware di ultima generazione configurano il firewall a puntino per i loro scopi senza disattivarlo, quindi niente più

segnalazioni che il firewall è disattivato, che almeno ci potevano avvertire di qualcosa che non andava.

L'antivirus, dal suo canto, si è evoluto, e non opera solo con la ricerca di firme, ma esamina anche il comportamento dei programmi una volta in esecuzione: se all'avvio un programma tenta qualcosa di poco pulito o sospetto, l'antivirus lo blocca e segnala l'anomalia. Naturalmente i malware sono preparati anche a questa evenienza: stanno buoni buoni, aspettano che l'antivirus termini il periodo d'osservazione e sferrano l'attacco. Intere famiglie di malware sono in grado di nascondersi efficacemente, e l'antivirus non è in grado di scovarli: quando l'antivirus chiede di esaminare la memoria dove risiede il malware, o di leggere il contenuto del file che lo contiene, il malware prontamente mostra all'antivirus dati innocui, presi da altri file o da altre zone di memoria.

Il prodotto è che l'attacco e l'insediamento di un malware sono silenziosi, senza conseguenze immediate e, soprattutto, senza sintomi. Una volta dentro, le strategie di occultamento e di opposizione alla rimozione messe in atto sono sofisticatissime. Il risultato finale è che nel computer violato niente è più affidabile, ma *non possiamo saperlo*, non abbiamo più nessun indizio.

Qui sta uno dei punti deboli della lotta alla diffusione del crimine informatico: mentre i criminali studiano continuamente nuove strategie di attacco, dall'altro lato si assiste solo alla produzione di strumenti di sicurezza, senza una reale strategia, organica e ragionata.

## L'esercito delle scimmie mutanti

La tendenza mostrata dai malware in questi ultimi tempi è inquietante: le funzioni con cui viene rilasciato un qualsiasi esemplare si limitano a insediamento, occultamento e contrasto alla rimozione. Nessun altro compito, neanche la propagazione, se non quello di "chiamare casa" una volta giunto a destinazione. E' a questo punto che il suo creatore decide cosa fare del computer conquistato, che per prima cosa sarà aggregato ad una *botnet* in cui condividerà lo stato di "zombificazione" con decine di migliaia di altri.

Spam, phishing, keylogger, open proxy, spionaggio, *cyberwar*, niente è impossibile. Basta fornire al malware il plugin giusto e subito il computer partirà,

diligentemente, mandando spam a mezzo mondo o collezionando dati sull'attività del proprietario.

Nessuno sa cosa ne sarà del computer conquistato, nessuno ha idea di come verranno usati i dati che nel frattempo vi transitano, soltanto una cosa è certa: niente di salutare.

## **C'è da scherzare ancora meno**

Nell'attuale mondo sempre più digitale, il Nemico ha bisogno di dati e di risorse per fare i suoi affari. Qualsiasi dato ha un valore, anche soltanto un indirizzo di posta elettronica, o un numero di telefono. Parimenti, qualsiasi risorsa ha un valore: tempo processore, spazio disco, connessione a Internet.

La vecchia scusa, “nel mio computer non tengo nulla di importante”, non regge più. Il computer stesso è importante. La connessione a Internet è importante. L'indirizzo IP della nostra connessione è fondamentale. Il Nemico lo sa, e sa come sfruttarli. E' come una partita a Risiko, il famoso gioco di guerra e conquista: più territori possiedi, più diventi difficile da sconfiggere, o anche solo da contrastare.

Non abbiamo più nessuna scusa per non correre ai ripari, *subito*. Il problema è che non sappiamo come.

## Capitolo 3. Il fallimento della sicurezza

Tempo addietro leggevo molto di più. In alcuni dei libri letti, di divulgazione scientifica, scritti da scienziati autorevoli e riconosciuti a livello internazionale, si parlava dell'efficacia della medicina moderna. Contrariamente a quanto si creda, la fortissima riduzione delle malattie infettive epidemiche non è dovuta all'impiego degli antibiotici, o almeno, non solo, ma alla maggiore attenzione a pratiche di prevenzione (igiene personale e dei luoghi pubblici, profilassi sanitaria, ecc.) ed alla migliore alimentazione. In pratica, un sistema immunitario più efficiente, dovuto alla abbondanza di cibo, e minore contatto con agenti patogeni, dovuto alla maggior cura dell'igiene. Gli antibiotici hanno ridotto la mortalità in caso di infezione, non la quantità di infezioni in sé, diminuita invece dalla *riduzione dei comportamenti a rischio*.

### La parabola degli antibiotici

Facendo un parallelo con il nostro argomento, invece, non possiamo certo dire che le cose stiano così bene. I miglioramenti nei nostri computer e nelle interconnessioni hanno solo aumentato la rapidità di diffusione e la pericolosità dei malware, oltre a rendere molto più attuale il rischio di cadere vittime di truffe.

Non posso fare a meno di pensare che ci siano numerosi punti di contatto con la strategia d'uso degli antibiotici in medicina. Quando ero bambino (diciamo che sono passati circa 40 anni), i medici prescrivevano antibiotici praticamente alla stregua di ricostituenti, per non dire come acqua fresca. Il risultato lo abbiamo sotto gli occhi: i germi, che sono una cosa viva, si evolvono, anche grazie alla selezione innaturale imposta dai nostri antibiotici. L'antibiotico non li elimina totalmente e matematicamente. Ne sopravvive sempre una piccola percentuale, immuni all'antibiotico, o resi semplicemente meno aggressivi. Il nostro sistema immunitario dovrebbe fare il resto. Ma a volte qualcosa non va per il verso giusto: cure interrotte troppo presto, convalescenze troppo brevi, e i germi sopravvissuti si fanno di nuovo avanti, solo che stavolta sono immuni all'antibiotico.

Oggi, prima di prescrivere un antibiotico, i medici ci pensano due volte, e fanno mille raccomandazioni. Non è troppo tardi per fortuna, ma abbiamo azzerato l'efficacia di gran parte degli antibiotici del passato in questo modo.

Nei nostri computer abbiamo antivirus sofisticatissimi, firewall che nel 2000 erano disponibili solo in dispositivi di classe *Enterprise*. Eppure, l'incidenza di malware e annessi non è diminuita di molto. Anzi, con l'ingresso in Internet di molti più computer è diventato possibile infettare centinaia di migliaia di computer, senza usare particolari magie, senza impiegare tecniche da stregone.

Il problema è che abbiamo completamente trascurato la prevenzione, o meglio, non ce l'hanno mai insegnata, quando si tratta di computer. Il semplice lavarsi le mani appena entrati in casa, operazione che molti di noi fanno automaticamente, tanto da non farci più caso, non ha equivalenti nell'universo informatico. Nessuno penserebbe di ingurgitare del cibo trovato in strada, mentre facciamo ingoiare al nostro computer qualsiasi cosa trovata in Internet, neanche tanto figurativamente parlando.

I moderni sistemi operativi non hanno un sistema immunitario integrato, ma deve essere aggiunto a posteriori. Sono stati fatti dei passi in questo senso, ma spesso lo scopo prefissato è un altro. Si veda quello che successe al tempo del famigerato *Trusted Computing*. L'idea era quella di far sì che il computer eseguisse e accettasse software e dati solo da fonti attendibili. In breve, la cosa si rivelò per quello che realmente era: un meccanismo per tenere sotto controllo quello che le persone facevano coi propri computer, in particolare impedire l'uso di software pirata e la fruizione di contenuti senza pagare i diritti d'autore. A questo proposito, materiale interessante è disponibile sul sito del progetto No 1984<sup>1</sup>. Il problema maggiore era che alla fine l'utente non aveva nessun peso nel processo di decidere se un qualcosa era affidabile o no, lo decidevano i produttori di software e di contenuti.

L'assenza di un sistema immunitario, o anche solo di un controllo di integrità, conduce alla situazione in cui un malware che riesca ad attivarsi con i permessi amministrativi (e questo non è quasi mai un problema) possa fare il suo comodo e compromettere fin nelle strutture più intime il sistema operativo, senza alcun indizio di quello che stia succedendo, inquinando a tutti i livelli i sistemi di autocontrollo e autoverifica, al punto che niente sarà più credibile.

---

1. <http://www.no1984.org/>

## Qualcosa del genere

L'uscita di Windows Vista fu accompagnata da una scia interminabile di proteste degli utenti, tanto da far sospettare che il rilascio di Windows 7 a breve distanza sia stato in un certo senso forzato dalle polemiche (Vista fu rilasciato a gennaio 2007, *Seven* seguì nell'ottobre 2009, meno di tre anni dopo). Fra l'altro il numero di versione di *Seven* non è 7, ma 6.1, mentre quello di Vista è 6.0, cosa che, dal punto di vista della numerazione convenzionale delle versioni di software, qualifica *Seven* una *minor release* rispetto a Vista. In effetti la lista di modifiche apportate da *Seven* è costituita quasi interamente da miglioramenti ai componenti introdotti con Vista.

Personalmente, ritengo che sia stato sottovalutato pesantemente il ruolo delle abitudini degli utenti (e non solo loro), ormai cristallizzate da oltre sette anni di uso ininterrotto di Windows XP (uscito nell'ottobre 2001, che riceverà aggiornamenti di sicurezza fino al 2014). Il semplice aver spostato alcune funzioni del pannello di controllo ha prodotto il panico in molti utenti che non sapevano più trovare le cose, non essendo nel posto in cui sono state per anni. Molte persone di cui mi sono trovato per le mani il computer nuovo con installato Vista si lamentavano di non riuscire a fare più niente.

Pigrizia mentale? Incapacità? No, più semplicemente: abitudini acquisite che è faticoso cambiare. Ho avuto più volte dimostrazione di quanto sia deleterio e controproducente sottovalutare le abitudini delle persone. Qualche anno fa, mi sono trovato a lavorare su un impianto piuttosto complesso, per il completo rinnovo. Uno dei componenti era una DAW (*Digital Audio Workstation*) con una console di comando dedicata, fatta da pulsanti, manopole, interruttori, indicatori, cursori. Essendo ormai impiegata per parecchi anni oltre la vita dichiarata dal produttore, era necessario sostituirla con qualcosa di più moderno e flessibile. La scelta, presentata e condivisa inizialmente con gli utilizzatori dell'impianto, cadde su un software commerciale e una console di controllo generica, ma altamente configurabile dal software.

Al rilascio del nuovo impianto successe il finimondo. Niente andava bene, niente. Dopo alcuni mesi di sofferenza generale, la luce venne da un commento di una cara amica: parlando della console della vecchia DAW, ne definì "naturale" l'uso. I pulsanti erano esattamente dove dovevano essere, la si poteva usare anche



al buio.

Alla mia domanda se per caso stesse parlando di abitudine, rimase silenziosa. Ci pensò su per un po', poi concluse, molto onestamente, che gli anni di uso erano la ragione principale per cui sapesse manovrare l'apparato ad occhi chiusi. Dopo qualche mese in cui le proteste si fecero via via più rade, tutto finì come era cominciato.

La storia si è ripetuta immutata dopo quattro anni, al successivo rinnovo dell'impianto: di nuovo proteste e resistenze al cambiamento ma, indovinate un po', le obiezioni addotte erano le stesse a suo tempo mosse all'impianto che ora si era trasformato nel vecchio.

Penso che prima o poi i produttori dovranno venire a patti con questa umanissima inclinazione, o ci troveremo a fronteggiare il rischio del rifiuto dei cambiamenti da parte degli utilizzatori.

## Non ci siamo ancora

In ogni caso, è innegabile che, sempre prendendo ad esempio l'evoluzione di Windows, i progressi nella gestione della sicurezza vi siano stati. Le strategie di sviluppo del software, i controlli alla correttezza formale del codice, le contro-misure per rendere più difficile lo sfruttamento di falle nel software, hanno avuto il loro effetto.

Vediamo qualche esempio:

- Internet Explorer viene eseguito con diritti limitati, indipendentemente dal livello dell'utente che lo avvia; non ha accesso ad altro che i file temporanei, in più ha i famigerati controlli ActiveX disabilitati.
- Vi è una speciale applicazione di sicurezza, chiamata UAC (*User Account Control*, "Controllo Account Utente" nella versione italiana), che si attiva al verificarsi di certe condizioni, indice di un probabile accesso indesiderato di un programma a parti vitali del sistema operativo, bloccando l'esecuzione del software responsabile.

- L'aggiornamento del sistema operativo è eseguito da una applicazione apposita, non tramite Internet Explorer, che così torna al mestiere di browser e basta.
- Uso di crittografia e firme digitali per le verifiche di integrità del sistema e dei suoi componenti.

Oltre queste modifiche, vi sono strategie poco visibili nell'immediato all'utente finale, utilizzate al momento dello sviluppo del software, fra cui un costante ed accurato controllo alla ricerca di errori tali da pregiudicare la sicurezza e l'integrità del sistema operativo.

Gli altri sistemi operativi non sono da meno.

Quello che sto notando, sempre più spesso, è il progressivo convergere verso un modello in cui l'account utente utilizzato normalmente ha sempre meno limitazioni e sempre più potere, al punto da rendere inutile la distinzione fra account amministrativo e normale, inteso alla maniera tradizionale.

L'effetto collaterale è che nessuno educa gli utenti, cioè noi, alle semplici regole minime che erano alla base dell'uso del computer.

Nelle reti aziendali sta divenendo sempre più complicato mantenere un livello accettabile di affidabilità, proprio a causa dei comportamenti sempre più imprevedibili degli utenti, che ne inventano di tutti i colori per installare il programma bellissimo che hanno anche a casa (portato con un *pen drive* USB in cui c'è molto più di quanto sospettano), o per scaricare l'ultimo film da eMule, anche se il firewall aziendale blocca il traffico correlato.

Niente mi toglie dalla testa che alla fine si spendono più soldi per impedire agli utenti di fare il proprio comodo di quanti effettivamente ne vengano spesi per contrastare pericoli e minacce reali.

E questo è un palese indizio di fallimento dell'intero concetto di sicurezza applicata. L'utente medio vede le limitazioni come un ostacolo da aggirare senza farsi troppi problemi, se non un'alzata di spalle e una mezza imprecazione diretta a "quei rompiscatole della sicurezza", che poi sarebbero quelli che comunque fanno da capro espiatorio quando, a causa di qualche trovata geniale di un utente, l'intera rete aziendale collassa.

## Si dice il peccato...

Sia chiaro, non è responsabilità di un sistema operativo se le persone pretendono di essere amministratori anche per usare i giochini in Flash, non è questo che sto dicendo. La tendenza a deresponsabilizzare l'utente è la vera causa di tutto. Può sembrare strano ma, a differenza di quanto si creda, il metodo di infezione che fa enormemente più danni di qualsiasi altro è "il doppio clic della morte", ossia l'utente che apre documenti o lancia programmi dei quali non conosce il reale contenuto, lo sottovaluta o lo ignora volontariamente. Certamente, pestilenze come quella di Conficker o quella di Blaster fanno sensazione, anche perché ne parlano i media generalisti con soliti toni catastrofici, ma esistono pestilenze più o meno silenziose che fanno molti più danni, e li fanno per tempi molto più lunghi. Al momento opportuno ne vedremo degli esempi, che posso assicurare toglieranno il sonno a più d'uno, e dei quali difficilmente si sentirà parlare in televisione. Ogni strumento ed ogni strategia vista in questi anni è tesa a togliere un altro piccolo pezzo di responsabilità all'utente, convincendolo che difficilmente potrà autoinfliggersi danni. Peccato che nella quasi totalità dei disastri che mi sono capitati sotto mano, l'invariabile situazione era del tipo "Io? Io non ho fatto niente!", seguita immancabilmente da una o più varianti del "Ho solo aperto installato cliccato inserito cercato scaricato ecc."

Altro malinteso da superare definitivamente è quello che sia l'utente inesperto, il novizio, a tirarsi addosso le pestilenze peggiori. Manco per niente. Proprio perché novizio ed inesperto, ci pensa due volte prima di fare qualsiasi operazione con cui non ha confidenza, soprattutto perché ha paura di rompere qualcosa, e di solito chiede a chi ne sa più di lui. Il problema è che, purtroppo, spesso capita in mani sbagliate, chiedendo consiglio all'amico "che ne capisce".

Che è la vera calamità, quello che chiamo "esperto definitivo", quello che ne sa "abbastanza", che ha un intero disco (della massima capacità disponibile al momento sul mercato) pieno di programmi per tutti gli usi, che ha sempre un consiglio su quale sia "il più migliore" prodotto per ogni campo dell'informatica.

Si riconosce abbastanza facilmente per il sorrisetto di compatimento con cui accoglie consigli che non riguardino l'installazione di un qualche software di uso professionale costosissimo e sovradimensionato, ma va bene comunque, visto che è probabilmente "rimediato" da qualche circuito *peer to peer* (ovviamente

l'acquisto non è una soluzione contemplata), o l'andare a pasticciare nel Registro di Windows in qualche oscura chiave "non documentata".

Scherzi a parte, è proprio l'esperto autoproclamato, che pensa, purtroppo, di aver capito tutto quello che c'era da capire, che si attira i disastri peggiori.

Ne ho parecchi di aneddoti che riguardano questa categoria di utenti, e nel seguito verranno fuori quelli più appropriati all'argomento. In questo momento ci interessa discutere su come sia possibile che anni di ricerche e di sforzi congiunti di sviluppatori e ricercatori di sicurezza non abbiano prodotto la definitiva scomparsa dei malware, ma, al contrario, ne abbiano prodotti di più pericolosi.

## ... non il peccatore

La chiave di lettura della mancata sconfitta definitiva dei malware va cercata proprio nella apparente capacità di aggirare e invalidare ogni precauzione ed ogni strategia. Di progressi nella progettazione e nella realizzazione di software con elevati standard di sicurezza ve ne sono stati, oltre all'impiego di strategie e tecniche molto sofisticate per rendere la vita più difficile a chi tenti di sfruttare falle nel software. Quello che è rimasto invariato in tutti questi anni è l'utente, l'essere umano.

Finché l'utente non entrerà a far parte della equazione, ogni possibile avanzamento nella prevenzione e contrasto ai malware vedrà il vanificarsi degli sforzi.

L'essere umano è lento ad adattarsi, e fatica ad accettare le novità, soprattutto quando non ne vede il vantaggio immediato, in termini di minor impegno personale. Il giorno che finalmente avremo i software per la dettatura, gli utenti faranno fatica a parlare, e l'invenzione della scrittura tramite il pensiero provocherà una epidemia di assenza di pensiero. Questo è uno dei motivi per cui applicazioni di sicurezza come lo *User Account Control* di Vista e *Seven* e gli avvisi di sicurezza di alcuni firewall commerciali hanno come risultato, certamente non desiderato, la disattivazione *in toto* dell'applicazione. Qualcosa di simile succede in Linux, con le distribuzioni che implementano SELinux (*Security Enhanced Linux*), una versione di Linux con il kernel "irrobustito" per garantire un controllo più esteso e granulare sul comportamento di applicazioni e utenti. SELinux permette di stabilire ad esempio che un certo servizio non possa aprire connessioni con l'esterno,

o che non possa mandare in esecuzione file al di fuori di una certa directory. La strada più rapida scelta in caso di opposizione di SELinux ad una particolare operazione voluta dall'utente è quella di disabilitarlo, anche in server esposti al traffico Internet, perché SELinux viene visto come un ostacolo, non come una protezione verso comportamenti indesiderati e abusi.

Se l'utente è lento ad adattarsi, possiamo invece star certi che sia rapidissimo e diretto nel trovare modi per aggirare gli ostacoli, o meglio, quelli che vede come ostacoli. E, aggiungo, è capace anche di mostrare una vivace inventiva per raggiungere lo scopo.

Poi, almeno per noi Italiani, il riuscire a “fregare” un sistema di sicurezza o aggirare un divieto è fonte di piacere quasi orgasmico.

## Investire in un bravo SysAdmin

Il *sysadmin* (contrazione delle parole *system administrator*, persona che gestisce il corretto funzionamento dei sistemi informatici) è un personaggio del quale molti di noi non conoscono neanche l'esistenza. Eppure è una figura chiave in qualsiasi organizzazione che abbia la propria attività in qualche modo dipendente dai computer. Un buon *sysadmin* è invisibile, perché il suo intervento è sempre preventivo: qualsiasi evento disastroso accada ai sistemi informatici, un buon *sysadmin* è sempre in grado di fronteggiarlo senza troppi disagi per gli utenti, perché ha pronta l'alternativa.

Stiamo naturalmente parlando di una situazione ideale, quindi irreali. La realtà è fotografata in modo sintetico in questa frase:

Devi sapere che l'Universo può essere visto come una battaglia fra i sistemisti, che cercano di realizzare sistemi a prova d'idiota, e Dio che crea idioti sempre più sofisticati.

Inutile dire che, per ora, Dio sta vincendo.

—Leonardo Serni

Il lavoro di un *sysadmin* è spesso infernale, dovendo confrontarsi da un lato con la complessità in continua evoluzione dei sistemi informatici, dall'altro con le esigenze degli utenti, a dir poco contraddittorie e schizofreniche.

Cosa succede se il *sysadmin* non è all'altezza? La domanda è pleonastica. Il problema è capire se un *sysadmin* sia competente o meno.

Iniziamo con lo sgombrare il campo dai miti:

- Il bravo *sysadmin* sa tutto. Manco per niente: la materia è estremamente complessa ed in continuo aggiornamento, quindi il poveretto deve studiare in continuazione. Se volete che il vostro *sysadmin* rimanga efficiente ed efficace *dovete dargli il tempo di studiare*. Se passa la giornata a fare la trottola in breve tempo sarà obsoleto, come i computer su cui lavora.
- Il bravo *sysadmin* conosce tutto di tutto. Se qualcuno si presenta in questo modo, va cacciato a pedate, senza indugi. Il campo dell'informatica è talmente vasto e complesso che è impossibile per chiunque padroneggiarlo interamente. Naturalmente occorre sapere un po' di tutto, ma non si può essere contemporaneamente esperti di ogni cosa. Un bravo *sysadmin* è specializzato e, soprattutto, conosce i propri limiti e non ha nessun problema ad ammetterli.
- Il bravo *sysadmin* può risolvere ogni problema. Altra trappola infernale, innescata purtroppo dalla umana inclinazione a considerare magia quello che non si capisce o non si conosce. Mi è capitato di essere guardato con timore reverenziale perché ho recuperato dati da dischi che Windows considerava vuoti e da formattare. Ma non ho fatto nulla di strano o soprannaturale, ho solo applicato quello che sa ogni sistemista degno di questo nome: dati e metadati sono due cose diverse.

Per non incappare in problemi senza soluzione, occorre fornire mezzi e risorse al *sysadmin*. Costringerlo a lavorare con roba vecchia e mezzi limitatissimi porta solo al disastro.

- Il bravo *sysadmin* non sbaglia mai. E' un essere umano, e come tale fa la sua parte di errori. La differenza è che di solito è in grado di rimediare senza addossare la colpa ad altri.

Il problema più grosso è che i bravi *sysadmin* non sono facili da trovare e non sono economici. La competenza costa, e paga.

Se poi andiamo a parlare di sicurezza, il *sysadmin* è una figura fondamentale per l'implementazione di strategie efficaci. Solo che la maggior parte delle volte

è liquidato come rompiscatole paranoico.

I risultati si vedono: gente capace solo di usare programmi preconfezionati, con una interfaccia di tipo *wizard* (avete presente, no? Avanti, Avanti, Avanti, Avanti, Fine) è impiegata correntemente come *sysadmin*, senza alcuna valutazione sulla reale competenza e sulla effettiva capacità di gestione. Tenere sincronizzate due directory su due server differenti? Scarico il programmino (pirata) e via. Codificare decine di migliaia di file MP3 da 256 kilobit a 192 kilobit? Programmino da *peer to peer*. Il database server è lento? Aggiungiamo memoria, mettiamo un server a 4 processori.

Soluzioni *pret-a-porter*, pericolose, costose e inefficaci. Dovrebbe ricordarci qualcosa. Proprio i problemi di sicurezza di cui tanto ci preoccupiamo, nella maggior parte dei casi, sono aggravati, se non originati, da persone senza le necessarie competenze messe a fare un lavoro delicatissimo.

La presenza di tante interfacce utente semplificate ha creato la convinzione che basti leggere quello che c'è nel pannello che si ha di fronte per saper fare qualsiasi cosa. La scarsa alfabetizzazione informatica di chi fa formazione di base nelle scuole ha alimentato la convinzione che i giovani siano “naturalmente portati” per l'informatica. Queste due false certezze, insieme, portano molte persone a ritenersi “esperti informatici”, ed a convincere chi gli sta intorno della stessa cosa.

Se per risolvere un qualsiasi problema la strategia è andare a cercare il programma giusto, allora siamo di fronte ad un *sysadmin* che tale non è. Sarebbe come affermare che tutti siano in grado di fare il meccanico in Formula 1, basta individuare l'attrezzo giusto.

Molti responsabili di aziende e di piccole e medie imprese, al momento di assumere un *sysadmin*, hanno in mente il ragazzino “mago del computer” che passa le ore incollato ad un monitor, non si sa bene a quale scopo, che accetta di fare il lavoro per poca paga, visto che gli è sufficiente “divertirsi coi computer”. Niente potrebbe essere più deleterio e niente è più simile a buttare i propri soldi. Il *sysadmin* preparato è una persona ben differente, che difficilmente ha soluzioni belle e pronte, e che studia a fondo i problemi prima di fare alcunché.

Quando poi si tratta di sicurezza, andiamo a finire nel ridicolo, con *sysadmin*

che non riescono ad eliminare Conficker dalla loro rete perché non hanno ancora capito che l'antivirus non basta, o che prendono i loro software di sicurezza dal *peer to peer*, stupendosi che l'antivirus, poveretto, segnali che c'è un malware dentro.

Non sono esempi inventati, sono cose successe realmente. Giorni persi dietro ad una infezione generalizzata di malware per poi scoprire che era uno dei *sysadmin* che installava una *inutility* presa dal *peer to peer* perché "era carina". Web server, su macchine quadriprocessore e memoria a tonnellate, che sembrano tartarughe con il Parkinson perché il *sysadmin* non sapeva che il server database nell'installazione predefinita *non ha nessuna ottimizzazione*, quindi usava solo una frazione delle risorse a disposizione.

Quindi, va bene investire in strumenti di sicurezza, ma occorre anche investire sulle competenze e su persone capaci e preparate, senza le quali gli strumenti sono inutili.

## Manager "2.0", gestione della sicurezza "0.1beta"

E' pieno di manager che si riempiono la bocca di termini che suonano bene, pregni di significati positivi: *forward thinking*, *user experience*, *community driven*, *weak links*, *long tail*, e chi più ne ha...

Quando si tratta di investire in sicurezza, però, la versione del management che entra in campo è la pre-beta, per continuare il parallelo con il versionamento del software.

Acquisto al miglior prezzo ed al massimo ribasso, sono le parole d'ordine. E quando non lo sono, vengono sostituite da "più è grosso, meglio è".

C'è un bel parlare sulla sicurezza che non è determinata dagli strumenti ma deve essere considerata un processo: belle parole e basta purtroppo.

Quando si parla di sicurezza in relazione a qualsiasi cosa, sia essa un sistema di computer o altro, l'impostazione mentale è quella di comprare il servizio e gli strumenti giusti, al miglior prezzo, per non pensarci più.

Quello che possiamo dire, è che si può certamente imparare dagli incidenti di sicurezza, ma potrebbe darsi il caso che non vi sia possibilità di mettere a frutto



la lezione: alcuni incidenti di sicurezza sono fatali, dopo l'evento non rimane più niente da difendere...

Se un malware entra in una rete privata aziendale e riesce a trafugare i dati di tutte le carte di credito dei clienti, o i progetti del nuovo aggeggio rivoluzionario in procinto di essere prodotto su larga scala, hai voglia a rimediare.

Esistono normative che obbligano le aziende a tenere in considerazione alcune misure di protezione dei dati (vedi il Testo Unico sulla Protezione dei Dati Personali, o la legge 231 sulla responsabilità amministrativa delle società), ma spesso questo si traduce in un semplice gioco a scaricabarile dove la responsabilità viene suddivisa e frammentata in modo da rendere legalmente ineccepibile la posizione aziendale, senza però aumentare di un epsilon (in matematica, una quantità piccola a piacere) il livello di sicurezza generale.

## **A me non capita**

Tornando al nostro discorso, non ho una soluzione per convincere l'utente medio che alcune limitazioni e alcune regole siano essenziali per la sua stessa sicurezza, magari: sarei ricco sfondato, e probabilmente sulle strade vi sarebbe una consistente riduzione di incidenti e vittime. Che c'entra? E' un differente aspetto dello stesso problema.

E' lo schema mentale del "guidatore sopra la media", immagine che ogni conducente di mezzo a motore ha di sé stesso. E' spesso associato al pensiero sottostante: "a me non succede".

L'unico mio possibile contributo è quello di mostrare alcuni pericoli nell'uso troppo disinvolto del computer e soprattutto di Internet, e di come alcuni "guidatori sopra la media" vi si siano imbattuti ricavandone qualche grattacapo. Naturalmente, vi saranno quelli che scuoteranno la testa ridacchiando e sentendosi superiori ai malcapitati, ma è proprio questo il pensiero del "guidatore sopra la media", ed è quello che gli fa abbassare la guardia.

Nessuno è autorizzato a sentirsi "al riparo", perché è "un esperto". Sono innumerevoli i casi di esperti veri, caduti vittime di incidenti di sicurezza. E il "guidatore sopra la media", prontamente, è là ad additare e deridere, non renden-

dosi conto che se anche ad un esperto può capitare, allora, a maggior ragione, *non c'è proprio nulla da ridere.*

## Capitolo 4. Cosa rimane valido

Le notizie, le strategie e le procedure presenti nel libro precedente sono in parte ancora valide, con i dovuti aggiustamenti e tagli. Negli anni trascorsi dal 2006 a oggi, Microsoft ha mandato in pensione Windows XP, anche se a tutt'oggi, acquistando un computer di categoria *business* si trova inclusa una licenza di Windows XP per fare il *downgrade* da Windows 7, segno evidente di un fenomeno con cui in futuro faremo sempre più i conti: la tecnologia avanza più velocemente di quanto le persone riescano ad adattarsi. Tuttora (prima metà del 2011) Windows XP è il sistema operativo più usato, con una fetta di utenti intorno al 40%, anche se Windows 7 sta lentamente guadagnando terreno, ma è ancora lontano dal sorpassare XP (fonti: W3Schools<sup>1</sup>, NetMarketShare<sup>2</sup>, Wikipedia<sup>3</sup>).

In questo capitolo faremo una cernita dei contenuti del vecchio libro ancora validi e utilizzabili. Nei successivi capitoli vedremo di fare un aggiornamento per gli argomenti che ne necessitano, poi passeremo alle cose nuove. Credetemi, ce ne sono anche troppe.

### Le basi sono sempre attuali

Nei primi tre capitoli del libro precedente, dato che era orientato a Windows XP, i paragrafi che ne parlano specificamente non sono più applicabili nei dettagli, conservando però validità per le informazioni di carattere generale. Ad esempio, nel Capitolo 2 i paragrafi “Senza fare nulla”, “Antivirus? Firewall? Che fanno, dormono?”, “L'esercito delle infinite scimmie” e “C'è poco da scherzare” contengono informazioni di carattere generale assolutamente attuali.

Il Capitolo 4 è invece totalmente applicabile, anche se in alcune parti va generalizzato. I concetti sono gli stessi, quale che sia il sistema operativo impiegato, oltre che su Internet. Il discorso sulla robustezza delle password (“La seconda linea di difesa bis: password” a pagina 31) è validissimo anche sui servizi online. Ci sono alcune differenze, che vedremo nel seguito. Fra le cose peggiorate, sia con Windows Vista che con *Seven*, abbiamo quanto detto in “La terza linea di

- 
1. [http://www.w3schools.com/browsers/browsers\\_os.asp](http://www.w3schools.com/browsers/browsers_os.asp)
  2. <http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10>
  3. [http://en.wikipedia.org/wiki/Usage\\_share\\_of\\_operating\\_systems](http://en.wikipedia.org/wiki/Usage_share_of_operating_systems)

difesa: cosa mi nascondi?": i nomi delle cartelle di sistema non corrispondono ai nomi reali sul disco.

Questo “vizio” è presente anche in altri sistemi operativi: nelle distribuzioni Linux che usano Gnome<sup>4</sup> come ambiente di desktop le cartelle mostrate come “Scrivania”, “Immagini”, “Documenti” in lingua italiana, non è detto che abbiano lo stesso nome delle directory corrispondenti sul disco.

Non solo, sempre nelle stesse distribuzioni Linux, vi sono discussioni riguardo la possibilità di permettere all’utente non privilegiato alcune operazioni potenzialmente pericolose senza richiedere alcuna autenticazione aggiuntiva, cioè senza neanche richiedere una qualsiasi password.

La mia personale paura è che per semplice pigrizia, o per un malinteso concetto di *user-friendliness*, si stiano mandando al diavolo le più elementari regole di prudenza.

Tornando a noi, ed al Capitolo 4, backup e separazione dei privilegi sono le due strategie basilari valide per qualsiasi sistema operativo e per qualsiasi uso si faccia del computer.

## RAID non è backup

Il basso costo dei dischi fissi, e la continua dilatazione della capacità, stanno orientando molti a installare più dischi nel proprio computer, usando una configurazione RAID (da *Redundant Array of Independent Disks*, oppure, nella forma più vecchia *Redundant Array of Inexpensive Disks*), tipicamente due dischi con i contenuti in replica (RAID 1 o *mirroring*).

I più intraprendenti (e con qualche soldino in più), installano tre dischi e usano configurazioni RAID 5 (3 o più dischi, dei quali uno è per ridondanza), che permettono di sommare la capacità dei dischi fino a valori impensabili fino a qualche tempo addietro.

La dura realtà è che avere due dischi in RAID 1 non mette al sicuro dalla perdita di dati. Anzi, paradossalmente, avere una configurazione RAID 5 con 4

---

4. <http://www.gnome.org/>

dischi implica il *quadruplo di possibilità* di un guasto (statisticamente, la probabilità di guasto è la somma delle probabilità di guasto del singolo disco). Quindi, con due dischi non si annulla la probabilità di perdere i dati, ma si diminuisce solo la probabilità di perdere i dati in caso di guasto dei dischi, guasto che però diventa *due volte* più probabile.



### **Due guasti contemporanei: non è impossibile**

La probabilità che i due dischi si guastino contemporaneamente è il prodotto delle probabilità del guasto del singolo disco. Dato che la probabilità è espressa come un numero decimale compreso fra zero (probabilità nulla) e uno (probabilità certa), il prodotto dei due numeri risulta più piccolo di entrambi. Per esempio se la probabilità di guasto è una su mille, la probabilità di guasto contemporaneo è di una su un milione. Piccola, ma non nulla.

Questi calcoli non tengono però conto di vari fattori: la vecchiaia dei dischi, la presenza di eventi esterni e la pura casualità. Il calcolo quindi non è così semplice.

Con il RAID 5 le cose vanno anche peggio. Quando i dischi hanno qualche anno, nel momento in cui se ne guasta uno, gli altri saranno sottoposti ad uno stress maggiore durante la ricostruzione dei dati, obbligatoria ed automatica dopo la sostituzione del disco guasto. Non è infrequente che durante quella fase si schianti un *secondo disco*, provocando la perdita irrecuperabile di tutti i dati. Credetemi sulla parola, ne ho vissuto le conseguenze più volte di quelle che avrei voluto.

Tutto questo senza considerare la maggiore criticità e delicatezza di queste configurazioni, in cui basta a volte pochissimo per avere disallineamenti fra i dischi e perdere tutti i dati, anche senza chiamare in causa guasti o eventi catastrofici.

In ogni caso c'è un pensiero che deve farci riflettere sempre sulla salvezza dei nostri dati: se il computer o il supporto dove sono memorizzati in questo momento viene bruciato in un incendio, o da un fulmine che colpisce la rete elettrica, o semplicemente rubato, dove posso recuperare i miei dati? Se, come spesso suc-

cede, la risposta è il silenzio, i nostri dati non hanno una grande aspettativa di vita.

Non ricordo chi, diceva:

Le persone si dividono in due categorie: quelli che hanno perso i dati e quelli che li perderanno.

Per quanto mi riguarda, appartengo a tutte e due le categorie. Li ho persi, più volte (un furto, un problema con l'alimentatore del computer, una password dimenticata), e li perderò di nuovo in futuro, è inutile illudersi. La perdita però riguarda una sola delle copie, sparse in quattro posti differenti.

Forse sono esagerato, ma immaginatevi in questa situazione: il computer in cui avete installato una coppia di dischi in RAID 1, ed in cui avevate tutte le foto ed i filmati di vostro figlio dalla nascita (ora ha 5 anni) ha preso una sovratensione dalla rete di alimentazione durante un temporale e entrambi i dischi sono andati. Ora spiegatele a vostra moglie ed ai nonni del pargolo.

## Porte, firewall e antivirus

Il Capitolo 5 (“Vietato l’accesso”) è decaduto come validità specifica. Sono cambiate molte cose e, sinceramente, non saprei dire se in meglio o in peggio. Fatto sta che ormai anche sulle principali distribuzioni Linux, oltre che su tutte le versioni recenti di Windows e su Mac OS X, il firewall è di serie ed è attivato fin dalla prima installazione.



### **In Linux il firewall c'è *sempre***

Il sistema di firewall di Linux è integrato nel kernel, quindi è presente per definizione. L'unico problema è che la sua configurazione predefinita corrisponde alla completa trasparenza: niente viene bloccato.

Quello che avviene da qualche anno è che le principali distribuzioni includono una interfaccia grafica per la configurazione, ed al momento dell'installazione del sistema operativo il firewall viene fornito di un ristretto gruppo di regole per aprire solo le porte necessarie in funzione del tipo di utilizzo che si sceglie al momento dell'installazione stessa.

Seppure in Linux è ancora perfettamente possibile disabilitare i servizi inutili, quindi chiudere le porte aperte in modo definitivo, non è comunque una operazione a portata di principiante. E' però doveroso ricordare che una installazione standard di una distribuzione fra le più diffuse ha una esposizione realmente minima (tipicamente solo la porta del servizio *Secure Shell* è aperta in attesa).

Windows, d'altro canto, non è rimasto indietro: le versioni server dalla 2003 in poi si avviano con tutti i servizi disabilitati e fermi, per cui una macchina appena installata è potenzialmente invulnerabile agli attacchi provenienti dalla rete. Rimane il fatto che non è per nulla facile avviare e configurare i servizi, certamente non alla portata di chiunque.

C'è anche un altro problema: buona parte delle applicazioni per Windows sfrutta alcuni servizi fra quelli elencati nel capitolo, a volte anche senza apparente correlazione specifica, per cui capita molto spesso che applicazioni installate smettano di funzionare dopo le modifiche ai servizi attivi. Peggio, al momento dell'installazione la procedura fallisce con messaggi di errore realmente arcani, o fuorvianti, per cui è diventato non solo macchinoso, ma anche dannoso applicare quanto descritto nel capitolo. Per non parlare di applicarlo a versioni differenti di Windows, cosa altamente sconsigliata.

Ed ancora: un'altra fetta consistente di applicazioni apre porte sulle interfacce di rete, o installa servizi di sistema che lo fanno, anche se non hanno alcuna funzione esplicita di comunicazione con l'esterno, per i motivi più disparati: controllo aggiornamenti, verifica licenze, statistiche d'uso. Per questo motivo, anche fermando tutti i servizi di cui ho parlato nel libro precedente, non si otterrà mai dal comando **netstat** un elenco vuoto ma, al contrario, vi saranno tante più porte aperte (e sconosciute) quante saranno le applicazioni aggiunte.

La tecnica mostrata nel Capitolo 5 è comunque valida nel metodo: elencare le porte aperte, cercare i servizi che vi fanno capo, disabilitare quelli inutili e spostare sull'interfaccia di *loopback* quelli necessari che non devono essere contattati dall'esterno.

E' pur vero che molti dei malware che si propagavano autonomamente usando falle sui servizi esposti in Internet sono praticamente estinti, ma in particolari

ambienti, tipicamente le reti *intranet* di grandi e piccole aziende, dove alcune porte devono essere tenute aperte per la gestione e l'assistenza, alcune categorie di malware che si propagano via rete la fanno da padrone, ma siamo fuori dal nostro campo di interesse.

I concetti esposti nel Capitolo 6 sono ancora tutti pienamente validi. I firewall integrati nei moderni sistemi operativi bastano ed avanzano nell'uso quotidiano che facciamo del computer. Stiamo naturalmente sempre parlando di un uso tipicamente personale del computer. Se abbiamo per le mani un server, esposto a Internet, quanto detto non vale, ma non è neanche lo scopo di questo libro.

Il Capitolo 9, sugli antivirus, è valido e pienamente attuale. Mi permetto una nota assolutamente personale: l'efficacia dei software antivirus è, secondo la mia esperienza, in costante diminuzione, mentre invece aumentano i comportamenti indesiderati e i falsi allarmi: eliminano file del sistema operativo, convinti che siano pericolosi malware, segnalano pericoli in pagine web assolutamente innocue, bloccano l'accesso a documenti solo perché contengono stringhe "sospette". Sempre più spesso mi trovo a fronteggiare ostacoli posti dai sistemi di rilevamento dei malware per impedire l'accesso a minacce inesistenti. Oppure a recuperare i danni fatti da un antivirus troppo zelante. Di contro, i malware godono di ottima salute, e di continuo vedono la luce nuove famiglie o varianti più o meno dannose di famiglie ben note.

Il punto che desidero sottolineare è che non è ammissibile affidare l'intera sicurezza di dati e computer alla sola coppia firewall/antivirus. Occorre una corretta gestione del computer e delle sue funzioni: diritti utente, permessi, servizi, applicazioni e via così. Come avevo detto al Capitolo 2 (Conosci il Nemico) alla sezione "Antivirus? Firewall? Che fanno, dormono?", l'antivirus è l'ultima spiaggia, semmai, non la prima ed unica linea di difesa, mentre il firewall nulla può quando siamo noi ad invitare in casa il nemico.

## Internet, sempre più Internet

Portali, *Social Network*, *blog*, Internet non è mai stata tanto ricca di cose da vedere, leggere, sperimentare. In questi giorni ho letto un commento da qualche parte che diceva, pressappoco: in Internet tutti scrivono talmente tanto e su



qualsiasi argomento che inizia a scarseggiare chi legge.

Ironia, certo, ma è indice di una espansione e di una diffusione che è difficile arginare o negare. Quello che però non cambia, mai, è la presenza inalienabile di chi cerca di trarre profitto da tutto questo, lecitamente o illecitamente che sia. *Niente è realmente gratis* in Internet. Niente. Anche il software “libero”, Open Source, indipendentemente dalla licenza, non è del tutto gratuito: spesso la documentazione è appena sufficiente ad avviare il programma, mentre per usi più approfonditi occorre rivolgersi a chi lo ha creato, il software. Oppure, semplicemente, le competenze richieste per utilizzare o anche solo per far funzionare il software gratuito sono costose e non facilmente reperibili.

Fatto sta che i pericoli vanno dove vanno i bersagli appetibili. Il rapinatore che voleva fare il “colpo sicuro” andava nei pressi degli uffici postali nei giorni in cui venivano pagate le pensioni. Oggi che è sempre più frequente l’accredito diretto su un conto corrente, il rapinatore si è spostato davanti gli sportelli bancomat, per derubare direttamente chi preleva o per clonare le carte magnetiche usando falsi lettori e telecamere.

Sta succedendo la stessa cosa con Internet: i nostri dati sono sempre più presenti in Rete e sempre meno sui nostri computer, come pure la nostra attività si sta spostando sempre più su Internet. Pagare bollette, tasse o abbonamenti, fare acquisti, accedere a servizi, leggere giornali, mantenere i contatti con amici e conoscenti: per queste attività sempre più spesso ricorriamo alla Rete, come chi ha intenzione di trarre vantaggio da questa tendenza, non sempre in modo legale e rispettoso dei diritti altrui.

Ecco il motivo per cui occorre focalizzare l’attenzione, oltre che sul proprio computer, anche su tutti i servizi che usiamo in Internet. Il nostro computer può essere totalmente ed assolutamente sicuro, ma non abbiamo alcun controllo sui computer dove andiamo a memorizzare i nostri dati in Internet. E’ questa la strada principale seguita dai falsari di carte di credito, ad esempio. Lo sforzo per rubare un singolo numero di carta dal computer di uno di noi è uguale (se non maggiore) a quello necessario per trafugare l’intero database dei clienti di un sito di e-commerce. Solo che nel secondo caso, in un colpo solo, si mettono le mani su centinaia o migliaia di numeri di carte di credito, verificati e corredati di tutti i dati anagrafici degli utenti.



### 100 milioni in un colpo solo

Una dimostrazione, per chi fosse ancora dubbioso, è data dal caso Sony Playstation Network<sup>5</sup>: alla fine di aprile del 2011 Sony divulgò la notizia che erano stati trafugati i dati dei 77 milioni di utenti della Sony Playstation Network, a cui il 2 maggio si aggiunse la notizia che anche i dati degli utenti della Sony Online Entertainment erano stati trafugati, per un totale di *oltre 100 milioni di utenti*. Tali dati consistevano in nome, cognome, indirizzo, data di nascita ed e-mail, e qualcuno ha ipotizzato che vi fossero dati riguardanti le carte di credito, anche se Sony ha smentito categoricamente. Violando un paio di server qualcuno ha messo le mani sui dati di 100 milioni di persone: perché perdere tempo con i singoli computer?

Appena rimessa in linea la rete, Sony ha fatto cambiare a tutti gli utenti le password di accesso. Supponiamo che fra i dati trafugati vi siano anche le password. Una sola domanda: quanti dei 100 milioni di utenti usano la stessa password dei servizi Sony per altro?

Non ho dimenticato l'argomento: i capitoli 7 ("Difetti di fabbricazione"), 8 ("Clicca QUI!") e 10 ("Il postino suona N-volte") del libro precedente non solo sono quanto mai attuali, ma necessitano di una robusta integrazione, perché il Nemico si è evoluto ed adattato. Tocca a noi evolvere ed adattare le nostre strategie e le nostre difese, in questa corsa agli armamenti perenne, alla quale è impossibile sottrarsi.

## Valido sempre

Il Capitolo 11 ("Tenere la destra") riporta delle semplici regole di comportamento sempre e comunque valide, quale che sia il proprio computer, il sistema operativo, le applicazioni utilizzate e l'impiego che ne facciamo.

Rimane fuori la sola sezione "La *checklist*" che elencava i passi da fare per mettere in sicurezza il proprio computer. Orientata a Windows XP, non è molto utile, anche se alcune delle operazioni riportate e l'ordine di esecuzione rimarranno praticamente sempre valide.

---

5. <http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/>

Al di là delle esclusioni e inclusioni, il messaggio contenuto nell'intero capitolo è molto semplice, anche se in un certo senso "eretico": è il nostro comportamento a metterci in pericolo, non la tecnologia e gli strumenti (o la loro assenza). Per modificare il nostro comportamento niente di meglio di una robusta dose di conoscenza: quando ho la consapevolezza che installando un software pirata, scaricato da un circuito "peer to peer", molto probabilmente installerò anche altro nel computer, allora ho due alternative: o continuo imperterrito a scaricare ed installare, ben sapendo che per installare devo essere amministratore, e che un malware eseguito come amministratore può fare di tutto con il mio computer, oppure decido di provare ad usare un software libero e gratuito, che forse fa qualcosa in meno, ma tanto a me non serve, o di acquistare un software commerciale in versione ridotta, che non fa tutte quelle cose iperfantastiche che comunque non uso mai, e che costa cifre ragionevoli.

Lascio decidere a voi quale sia il comportamento più adatto alla sopravvivenza. Naturalmente non mancano quelli che continueranno a scaricare ed installare, lamentandosi poi che il sistema operativo che usa è una schifezza, che l'antivirus XYZ non funziona, che il proprio computer è pieno di immondizia e lento. E, ovviamente, cercheranno nello stesso *peer to peer* un antivirus "più potente", un "ottimizzatore del registro", un "velocizzatore del computer".

## Capitolo 5. Service Pack 1

Prima di iniziare gli argomenti nuovi, diamo uno sguardo ad alcune delle cose che avevamo esaminato a suo tempo, per vedere se qualcosa è cambiato.

Nel precedente capitolo abbiamo visto cosa era ancora valido, qui andiamo ad aggiornare ed integrare quanto già detto nel libro precedente. In un certo senso, questo capitolo è un *update* del libro precedente, di qui il titolo.

### SPAM, l'immortale

Nonostante gli anni trascorsi, e le innumerevoli strategie messe in atto dai vari fornitori di servizi Internet, lo spam, la posta indesiderata, continua a intasare le nostre caselle di posta elettronica. Non solo, continua ad essere uno dei veicoli preferiti per tutta una serie di attività truffaldine e criminali in genere. Non so voi, ma io continuo a ricevere messaggi di gente che mi vuole vendere medicinali, orologi, software, diplomi di laurea, direttori di banca che vogliono regalarmi milioni di dollari, ragazze russe che vogliono conoscermi, vincite alle lotterie più strane, banche che vogliono proteggere la mia sicurezza, cartoline elettroniche da ammiratori sconosciuti, proposte di lavoro part-time. Per non parlare delle richieste di aiuto di chi soffre il freddo e dei miracolosi rimedi per “diventare irresistibili con le donne”.

Per quanto riguarda la vendita di medicinali, accessori di moda, software e diplomi, vale quanto detto: tutta roba contraffatta o priva di qualsiasi valore. Lotterie e proposte di affari milionari sono sempre le famose “truffe nigeriane”, i lavori part-time sono operazioni di riciclaggio di denaro.

I messaggi da varie banche e servizi online (eBay, PayPal, Facebook, ecc.) sono tutti tentativi di *phishing*.

Sull'argomento truffe, le cose sono un po' più articolate.

### Una raccomandata da 200kg

La fantasia dei truffatori si è dimostrata fervida, inventandosi di tutto. La tecnica che si è mostrata più promettente è quella delle richieste di aiuto da parte di ragazze madri povere, giovani e carine. In sostanza le poverette, all'approssimarsi

dell'inverno, mandano spam a mezzo mondo per sapere se c'è un'anima buona, in possesso di una stufa a legna che non usa più, disposto a spedirgliela in Russia. Ora, a parte considerazioni sul costo del trasferimento tramite corriere di 200 e passa chilogrammi di ghisa, appare strano che in una casa russa non ci sia un caminetto *ma vi sia un computer ed un collegamento ad Internet*.

La truffa ha lo scopo di sfilare pochi euro ad ognuna delle persone di buon cuore che rispondono, inducendole ad abbassare le difese con la storia lacrimevole del freddo e della famigliola di sole donne, con tanto di foto della figliola di sette anni e della nonna malata.

Per chi si vuole divertire un po', in Rete si trova un po' di tutto su questa vicenda, anche qualcuno<sup>1</sup> che si è messo in contatto con una di queste "povere ragazze" e le ha dato un po' di corda per vedere dove andava a parare. Sul suo sito ha pubblicato tutta la sequenza, vale la pena leggerla, anche per capire la tecnica impiegata per "agganciare" la vittima.

Naturalmente, dietro tutto questo non c'è alcuna ragazza russa, né persone in difficoltà. E' la solita pletora di truffatori<sup>2</sup> che sfrutta Internet per raggiungere tanta gente e tentare di carpirne la buona fede.

## SPAM, un ottimo investimento

Nel 2008, un gruppo di ricercatori dell'università di Berkeley ha portato a termine uno studio<sup>3</sup> con lo scopo di capire quanto renda effettivamente in termini economici lo spam. Lo studio era molto complesso, e verteva su un tipo specifico di spam, quello sui medicinali venduti online.

In breve, per rendere verificabile e verosimile il risultato, i ricercatori si sono infiltrati in una *botnet* dedicata a questo scopo, che forniva tutti i componenti necessari per l'organizzazione di vendita: i generatori di spam, i siti delle farmacie e i server di controllo.

Nel periodo di osservazione i generatori di spam hanno inviato due tipi di messaggi differenti, in periodi diversi: quelli con la pubblicità alle farmacie online

1. <http://www.falsomagro.com/2008/11/la-ragazza-stufa.html>
2. [http://www.attivissimo.net/antibufala/valentin/valentin\\_russia.htm](http://www.attivissimo.net/antibufala/valentin/valentin_russia.htm)
3. <http://www.icsi.berkeley.edu/cgi-bin/pubs/publication.pl?ID=002358>

e quelli con le cartoline animate. In pratica, i messaggi con le cartoline animate inducevano gli utenti a seguire un link, che li avrebbe portati ad autoinfettarsi con il malware che costituiva la *botnet* stessa. I messaggi con la pubblicità portavano sui siti con il catalogo, per permettere agli interessati di fare gli acquisti.

Tutti i server, sia quelli dei siti infettanti con le cartoline animate che quelli delle farmacie, appartenevano all'organizzazione che controllava la *botnet*, ma non erano individuabili in quanto non venivano contattati direttamente dalle vittime, ma vi era un consistente numero di computer membri della *botnet* che operava da *open proxy*, nascondendo di fatto i veri server.

Al termine del periodo di studio i risultati furono sorprendenti: in 26 giorni i server infiltrati dai ricercatori maneggiarono *350 milioni* di messaggi spam; di questi solo 28 portarono ad un acquisto di medicinali, che solo in un caso non riguardavano "pillole blu"; l'importo medio degli acquisti era intorno a 100 dollari. Dato che i server infiltrati costituivano l'1,5% del totale dei server della *botnet*, una proiezione conservativa dei dati al totale dell'attività della rete criminale indica introiti lordi per 3,5 milioni di dollari l'anno, non un ricco bottino ma, sicuramente, una attività fiorente.

Periodicamente, venivano intraprese campagne di spam volte a infettare nuovi computer per il mantenimento della *botnet*. In questo caso furono maneggiati altri *120 milioni* di messaggi in quindici giorni, che portarono all'infezione con il malware della *botnet* di 500 computer. Anche qui, proiettando il risultato all'intera *botnet*, il numero di computer *zombificati* e aggregati ogni giorno varia da 3.500 a 8.500 a seconda delle stime, comunque numeri di tutto rispetto.

La conclusione è che lo spam rende, eccome. Almeno per le farmacie online. Questo ci fa essere relativamente sicuri che, almeno per i prossimi anni, non vedremo un declino dello spam, anzi.

La pubblicazione dello studio, purtroppo solo in inglese, è comunque da leggere per via della grande densità di informazioni, come ulteriore conferma di quanto già in gran parte riportato in questo libro e nel precedente: le strategie di creazione e gestione delle *botnet*, l'uso di malware per creare ed accrescere la *botnet* stessa, le tecniche di propagazione, basate quasi esclusivamente sull'inganno.

## Phishing for Dummies

Anche questa forma di attacco alla nostra tranquillità non vede alcuna battuta d'arresto: al classico tentativo di sottrarre i nostri dati di accesso per la banca online si sono aggiunti tentativi di rubare le credenziali di accesso ad innumerevoli servizi online: dalla posta elettronica ai *social network*, da eBay<sup>4</sup> a Poste Italiane, niente si salva.

Molti sono i progetti che tentano di fornire una qualche protezione a chi naviga per il web, ma, effettivamente, i tentativi sono realmente troppi per contrastarli tutti, ed alla fine qualcuno sfugge alle maglie della rete di difesa.

Il fulcro è sempre lo spam, attraverso cui vengono inviati i messaggi trappola. Se si impiega un servizio di posta elettronica via web, come Gmail, gran parte dei messaggi viene bloccata e segnalata come appunto *phishing*. Gmail stessa, inoltre, offre una ulteriore forma di protezione disabilitando tutti i link del messaggio, che diventano inattivi. Per aggirare questo tipo protezione, nei messaggi viene allegato un file HTML da aprire. In questo modo il filtro anti-phishing non interviene, *perché quello che vediamo non è un sito web*, ma un file locale al computer. Solo che il pulsante *Invia dati* che possiede è attivo e spedisce effettivamente i dati al criminale che ha inviato i messaggi.

Anche Facebook, il noto *social network*, non è indenne da questa minaccia: i messaggi trappola appaiono come e-mail di notifica delle *richieste di amicizia* da parte di sconosciuti, funzione realmente offerta dal noto *social network*. Se la curiosità ha il sopravvento, come spesso succede, il danno è presto fatto: il link da seguire per vedere la richiesta di amicizia porta da tutt'altra parte, e i dati di accesso da noi inseriti (e-mail e password) saranno utilizzati per andare a curiosare nel nostro profilo. Cosa ci può essere di così importante in un account Facebook? Proviamo ad immaginare che chiunque possa accedere a tutti i dati da noi inseriti: tanto per fare un esempio, qui in Italia sarebbe semplicissimo calcolare il codice fiscale di una persona con i dati di Facebook. Ed il codice fiscale è spesso l'unico dato verificato al momento dell'attivazione di un qualsiasi contratto per telefonia, Internet o fornitura di energia elettrica. Traete da soli le conclusioni.

---

4. <http://www.ebay.it/>



### Furto d'identità: l'abc

Usando questa locuzione altisonante, la cosa ci sembra lontana anni luce. Invece, purtroppo, questa pratica è in uso da anni, e non solo in Rete. Nel maggio del 2010 sono stato vittima proprio di un furto di identità: qualcuno aveva stipulato a mio nome due contratti per il passaggio a differenti gestori per l'energia elettrica e per il gas metano. Me ne sono accorto all'arrivo delle prime bollette con l'indicazione del nuovo gestore, con inclusi i ringraziamenti per aver sottoscritto il contratto. Come era successo? Semplicemente qualcuno aveva letto nome e cognome dal citofono ed i numeri dei contatori, purtroppo esposti nella scala condominiale. Con quelli aveva potuto compilare le richieste. Ecco: un caso lampante di furto di identità. E senza usare Internet.

Quindi, non pensiamo che il furto d'identità sia qualcosa di remoto ("a me non capita", ricordate?) o connesso soltanto all'uso di Internet.

La facilità con cui è possibile sottrarre dati alle persone con questo sistema attira molti, desiderosi di fare soldi facili con poco rischio. In effetti il rischio corso da questo tipo di criminali è realmente basso, per vari motivi:

- La campagna di spam per l'invio dei messaggi è impossibile da tracciare all'indietro, visto che vengono usate delle *botnet*.
- Il sito fasullo su cui sono dirette le vittime, come pure il sito a cui vengono inviati i dati, appartiene a due categorie: o è uno spazio web gratuito, acquisito con dati falsi da provider che non fanno troppe formalità per assegnarlo, oppure, molto più spesso, è nascosto dentro un sito web regolare, violato a causa di qualche vulnerabilità, senza che il legittimo proprietario ne abbia alcun sospetto.
- Le operazioni vengono eseguite dai criminali usando computer membri di *botnet*, che operano come *open proxy*, quindi gli eventuali indirizzi IP che siano rilevati portano a vittime inconsapevoli ed innocenti.

Questi motivi hanno portato molti a ritenere che la pratica del *phishing* fosse il sistema ideale per arricchirsi in breve tempo. Immediatamente qualcuno ha colto



l'occasione, creando un mercato di servizi per gli aspiranti criminali informatici: un kit per creare il proprio sito di *phishing*, un servizio per mandare spam alle vittime che vende messaggi un tanto al chilo<sup>5</sup>, siti web violati dove ospitare il sito fasullo, *open proxy* per operare sotto copertura. *Et-voilà*, la truffa è servita.

Come oramai possiamo aspettarci, sono comparsi anche dei kit gratuiti per approntare il sito fasullo, con tanto di web application per la collezione dei dati e l'invio per posta elettronica al truffatore, e altri kit per mandare i messaggi di spam, sempre da un sito web il cui reperimento è a carico del truffatore. Questi kit<sup>6</sup> hanno quasi sempre<sup>7</sup> la sorpresa dentro<sup>8</sup>: quelli di phishing normalmente usano inviare i dati inseriti dalle vittime ad un indirizzo di posta elettronica, da configurare a piacere, e di nascosto ad un secondo (e spesso anche ad un terzo, un quarto, ...) indirizzo di posta elettronica, sepolto all'interno del codice; quelli per lo spam nascondono una *backdoor* da cui il creatore del kit apprende su quali server viene piazzato il kit, e che gli permette di eseguire codice a piacere, tramite una funzione nascosta nel codice dell'applicazione di invio spam. Quindi, l'aspirante Arsenio Lupin del crimine informatico si accolla tutti i rischi, mentre il creatore dei kit da un lato riceve i dati inseriti dalle vittime nel sito fasullo creato dal novello criminale, dall'altro può usare il server, reperito da quest'ultimo per diffondere spam, per altro scopo, certamente molto più dannoso. Il tutto sarà accolto ai vari Diabolik in erba, mentre il creatore del kit sfrutterà tranquillamente i dati che possiede senza correre alcun pericolo.

## Il colpevole sbagliato

Per chi ha chiaramente in testa come funzioni il *phishing* è immediato capire che la responsabilità in caso di truffa con questo sistema *non è mai* dell'istituto bancario o del servizio online di cui l'utente truffato si serve. Se sono cliente di Poste Italiane, mi arriva un messaggio trappola, spontaneamente digito i miei dati ed il criminale usa quei dati per togliere dei soldi dal mio conto corrente postale, Poste Italiane non solo non può impedirlo in alcun modo, ma non può

---

5. <http://www.darkreading.com/security/management/showArticle.jhtml?articleID=208803799>

6. <http://www.ismprofessional.net/pascucci/index.php/2008/11/ando-per-fare-phishing-e-rimase-allamo/>

7. [http://www.theregister.co.uk/2008/08/07/scammers\\_con\\_naive\\_phishermen/](http://www.theregister.co.uk/2008/08/07/scammers_con_naive_phishermen/)

8. <http://blog.imperva.com/2010/07/gnarley-new-phishing-kit.html>

neanche opporsi all'esecuzione della transazione, che viene da qualcuno che si è identificato per noi, *usando i dati che noi stessi gli abbiamo fornito*.

Per fare un esempio calzante, è come se, passando davanti alla nostra banca, un tizio con un cartellino col logo della banca stessa ci fermasse e chiedesse di controllare la nostra carta di credito. A nessuno verrebbe in mente di dare in mano ad uno sconosciuto la carta di credito, quale che sia il cartellino che espone. Ma se qualcuno lo facesse, gli impiegati all'interno della banca non avrebbero alcuna possibilità di accorgersi di cosa stia succedendo.

Eppure ogni anno parecchi truffati fanno causa a istituti bancari e altri servizi finanziari per essere caduti vittime del *phishing*, adducendo la motivazione che i sistemi di sicurezza non hanno protetto il cliente dalle truffe. Ebbene, sono soldi e tempo buttato: gli istituti non hanno alcuna colpa in questo e hanno poche possibilità di opporsi, in quanto non possono accorgersi dei tentativi di phishing che subiscono i clienti, non direttamente. Non ho particolarmente in simpatia alcun istituto bancario o finanziario in generale, ma occorre dare a Cesare quel che è di Cesare.



### **Qualcosa si può fare**

Un caro amico, Denis Frati, sta portando avanti da un po' di mesi una iniziativa assolutamente personale di *intelligence* sul *phishing*, catalogando le e-mail, le caratteristiche dei siti utilizzati per ingannare le vittime e di quelli che operano la raccolta dei dati.

La mole di dati raccolta è interessante, ed interessanti sono le sue indagini sui vari gruppi che probabilmente si celano dietro alcune campagne di *phishing*. Peccato che il suo lavoro non riceva più attenzione dai diretti interessati. Vale la pena sfogliare un po' il suo sito<sup>9</sup>.

Costituisce eccezione, fino ad ora, l'istituto bancario, o assimilato, non si adegua agli standard tecnologici e di mercato al fine di combattere il fenomeno delle truffe tramite *phishing*. Una decisione dell'Arbitro Bancario Finanziario del

---

9. <http://www.denisfrati.it/>

febbraio 2010, di cui parla Denis nel suo sito<sup>10</sup>, ha assegnato una buona parte della responsabilità, per un episodio di phishing, all'istituto bancario, dato che, parole testuali: “all'epoca dei fatti ... la tecnologia aveva già messo a disposizione dispositivi più raffinati, sicuri ed affidabili di quelli in concreto adottati e perciò maggiormente adeguati rispetto all'obiettivo suddetto in quanto capaci di offrire al cliente un terzo livello di protezione, come le serie numeriche casuali e random, generate da dispositivi automatici quali chiavette o token, digipass, et similia”, ossia, detto con altre parole, la banca non si era adeguata a sistemi più efficaci per generare password dispositive che non potessero essere trafugate.

Situazione differente è quella in cui la persona si accorge di essere caduta vittima di *phishing*, sporge denuncia alle Forze di Polizia, notifica l'istituto bancario che però continua a permettere operazioni con le credenziali trafugate.

Vi sono anzi alcuni istituti che hanno implementato sistemi per individuare non i tentativi di *phishing*, cosa pressoché impossibile, ma i tentativi di utilizzare i dati di accesso trafugati. Poste Italiane<sup>11</sup> ha un sistema per tracciare accessi sospetti agli account dei propri clienti, ad esempio segnalando picchi di attività o accessi multipli da posizioni geografiche differenti. Inoltre possiede una rete di controllo con cui rileva i siti di *phishing*, ma spesso l'intervento, seppur velocissimo, non è sufficiente a impedire che qualche utente ne rimanga vittima.

---

10. <http://www.denisfrati.it/2011/06/06/il-confinne-delletica/>

11. <http://download.microsoft.com/download/9/2/7/927113A8-F6CB-4AF8-9406-D9E2B2074089/DMARIANI.pdf>

## Capitolo 6. Malware per tutti i gusti

Nel libro precedente, al Capitolo 9, dove parlavamo degli antivirus, alla sezione “Perché non ha funzionato?”, ipotizzavo un malware di quelli cattivi, sommando le caratteristiche di alcuni di quelli conosciuti.

Non è che mi faccia molto piacere l’essermi sbagliato sulla previsione: infatti alcuni malware in circolazione al momento in cui scrivo sono *molto peggio* di quello che avevo inventato al tempo. Il Nemico si è evoluto ben oltre le aspettative più nere.

### Evoluzione e selezione

Nel 2006 affermavo che quasi nessuno sforzo era posto nel guadagnare i privilegi amministrativi da parte dei malware. Oggi possiamo asserire che lo sforzo in questa direzione è proprio nullo. Nessun malware per Windows di quelli più noti e diffusi usa tecniche di *privilege escalation*, ossia lo sfruttare falle per guadagnare i privilegi amministrativi. Eppure continuano a colpire computer su computer, macinando cifre da nausea.

Cercando in Rete, la quasi totalità dei siti riguardanti specifici malware tratta di come rimuovere l’ospite indesiderato, quasi mai di come prevenire l’attacco, e le procedure di rimozione stanno aumentando di complessità ogni giorno che passa, tanto da apparire più simili a incantesimi.

Questa situazione è un chiaro indice di quale sia la direzione di maggior impegno per chi crea pestilenze: renderne silenzioso il funzionamento e difficile la rimozione. Non è l’insediamento o l’attacco a preoccupare. Non è un buon segnale di come stiano evolvendo le cose: vuol dire che le nostre misure preventive sono inefficaci, per cui non occorre molto per aggirarle.

Ogni nuova versione di un particolare malware usa tecniche sempre più sofisticate per nascondersi in profondità nel sistema operativo e per impedirne la rimozione, sia inibendo gli strumenti propri del sistema operativo che impedendo l’uso di strumenti più o meno noti forniti da terzi. Si sta avvicinando il momento in cui dopo un attacco da parte di un malware l’unica soluzione sarà un completo *wiping* di tutti i dischi interni al computer per rimuovere ogni traccia del codice

iniettato e debellare definitivamente l'intruso. Ci sono segnali che forse non sarà sufficiente neanche quello, in un futuro non troppo lontano.

Se poi andiamo a vedere le funzioni svolte dal malware una volta insediato, c'è di che rimanere basiti. I tempi dei *dialer*, del *browser hijacking* o degli *spambot* sono finiti.

Per capire fino a che punto si è evoluto il panorama funesto dei malware, niente di meglio che dare uno sguardo ad un esempio reale.

## Software criminale

Se qualcuno vuol cambiare mestiere, e diventare un criminale informatico, ci sono ottime notizie per questo novello Diabolik del bit. Per una cifra tutto sommato contenuta (si va da qualche centinaio a qualche migliaio di dollari) si può acquistare il generatore di malware con tutti gli optional, oppure, rinunciando alla documentazione ed al supporto tecnico, vi sono le versioni gratuite, con meno funzioni di quelle a pagamento. Per le versioni a pagamento viene garantita l'assoluta immunità a tutti i maggiori antivirus al momento del rilascio per ogni malware creato dal kit. Naturalmente, i servizi a disposizione non finiscono qui: c'è il servizio di diffusione del malware, con sito web camuffato da cartoline animate o da raccolta di video porno, associato al servizio di spam per notificare milioni di utenti di computer dell'esistenza del sito; c'è il pannello di controllo per la rete di computer compromessi, per dominare il proprio esercito di scimmie mutanti, la *botnet*; c'è l'accesso al database di informazioni trafugate dai singoli computer compromessi.

Il malware ha una serie di caratteristiche degne dei marchingegni in dotazione al miglior agente di spionaggio. Niente processi sospetti, niente segnali anomali, niente attività insolite. Firewall e antivirus funzionano regolarmente e non segnalano stranezze, il computer non ha rallentamenti di sorta e l'accesso a Internet è regolare e senza incertezze.

Sto parlando dell'organizzazione che fa capo al *crimeware* denominato *Zeus*. Si è dovuto coniare un neologismo, perché non siamo di fronte ad un semplice malware, ma ad un sistema completo e complesso, a più livelli.

Chi voglia crearsi la propria *botnet* deve per prima cosa attrezzarsi con un server, detto *C&C*, da *Command and Control*. Il necessario per crearne uno è compreso nella versione commerciale del kit, con tutta la documentazione necessaria. Le versioni di libera distribuzione non comprendono la documentazione approfondita. Naturalmente il server deve essere accessibile via Internet a tutti i membri della *botnet*, per cui occorre cercare un servizio di hosting, cioè un posto dove mettere tutto il necessario per creare il server *C&C*, come fosse un normale sito web. Il server permetterà di impartire ordini ai membri della propria *botnet*, tramite un pannello di controllo utilizzabile con un normale browser. Sempre nel kit vi è lo strumento che crea la parte “client” del malware, denominata *Zbot*, dalla contrazione di *Zeus Bot*, quella che va nei computer delle vittime e che sarà strettamente associata allo specifico server *C&C* di gestione.

Se non si vuole spendere troppo, si possono acquistare lotti di computer già compromessi, oppure accessi al database di informazioni trafugate. Se invece si dispone di risorse economiche maggiori si può puntare a creare la propria *botnet*, acquistando il kit per creare i malware “client”.

Se ancora non basta, possiamo aggiungere che la parte “client”, quella che si insedia nei computer compromessi, lo *Zbot*, ha caratteristiche di tutto rispetto. Una volta attivata nel computer vittima, si registra come applicazione da avviare quando l’utente esegue il *logon*, ed inietta il proprio codice in memoria agganciandolo ad alcune librerie di sistema utilizzate da praticamente tutti i servizi del sistema operativo e da tutte le applicazioni. Da quel momento ogni informazione estratta da quel computer non è più credibile ed ogni dato inserito dall’utente non è più privato. L’antivirus non lo trova, perché il malware intercetta i tentativi di leggere e controllare sia i file che lo costituiscono che la zona di memoria che lo contiene, presentando dati innocui all’antivirus. Ogni strumento di sistema è controllato dal malware che modifica a piacimento i dati di lavoro del sistema operativo: la lista dei processi non mostra nulla di sospetto e la lista delle connessioni di rete è pulita.

Il computer è completamente inaffidabile, ma l’utente *non ha alcun modo per saperlo*.

Per finire, il colpo di grazia: il “client” funziona perfettamente *anche se avviato da un account non amministrativo*. Scacco matto.

## Zbot, il *full optionals*

Cosa rende *Zbot* così particolare, e soprattutto così pericoloso?

Il malware è progettato per il furto di informazioni, in particolare il furto di credenziali. Una volta attivo, passa in rassegna l'area dati personali nell'account in cui si è insediato controllando se siano installati software specifici, in particolare client di posta elettronica e di accesso FTP, ma anche le aree dove i browser salvano le password dei servizi a cui accediamo (se abbiamo attiva l'opzione di salvataggio password). Contemporaneamente, si attrezza per intercettare il traffico di rete, specificamente quello relativo al protocollo HTTP, iniettando il suo codice nelle funzioni del sistema operativo preposte alla gestione del protocollo stesso. Dato che l'intercettazione è fatta ad un livello molto basso, nelle funzioni che usano tutte le applicazioni che accedono a Internet, ha un punto di osservazione diretto per tutte le informazioni che riceviamo, ma, soprattutto, alle informazioni che inviamo.

Al momento dell'attivazione, e per ogni avvio, scarica un file specifico da uno dei server *C&C*, quello da cui dipende la *botnet* a cui è associato. Questo file è la configurazione, ed è cifrato con una chiave che è specifica per ogni esemplare creato dal kit *Zeus*, quindi è praticamente impossibile da decifrare.

La configurazione decide il comportamento del malware, in particolare quali informazioni deve cercare nel computer. La parte più importante è quella che determina per quali siti web viene operata l'iniezione di codice allo scopo di sottrarre credenziali di accesso, elencati sotto forma di URL.

Il malware opera in questo modo: durante la navigazione web tiene sotto controllo quali siti e quali pagine vengono richieste dal browser. Nel momento in cui uno degli URL coincide con quelli nella configurazione, opera una iniezione *nel codice HTML ricevuto dal server*, modificando la pagina web prima che venga visualizzata dal browser. In questo modo l'utente non ha alcun indizio di quello che sta per succedere: il server non viene in alcun modo toccato; il sito visitato è proprio quello voluto, non una copia contraffatta come nel *phishing* classico; il codice iniettato colleziona i dati inseriti dall'utente, senza che il server possa accorgersene. Il risultato è che i dati inseriti finiscono in mano anche a chi gestisce quella particolare *botnet*, con le ovvie conseguenze del caso: se è un account bancario, per trafugare i dati o compiere operazioni di movimentazione del dena-

ro sotto la soglia di autorizzazione; se è un altro tipo di account (PayPal, eBay, Facebook, ecc.) per operare con l'identità di qualcun altro.

Non c'è limite alla operatività con questo metodo: se la banca prevede l'immissione di una ulteriore password detta "dispositiva" per autorizzare alcune operazioni, chi controlla il malware potrebbe deviare la password e non farla mai arrivare al server originale, per usarla lui stesso. Il proprietario del conto si vedrebbe rifiutare l'operazione perché la password è già stata usata, o perché scaduta, e difficilmente si insospettirebbe: nessuno di questi comportamenti è riportato negli avvisi antifrode periodicamente emanati dalle banche, perché non si tratta di *phishing* vero e proprio.

Pensare di aggirare il problema con trucchi tipo mettere la password in un file di testo e operare di copia&incolla, usare una tastiera a video o altre trovate più o meno ingegnose, possiamo darle già per inutili. Il malware è in grado di intercettare i dati che passano per il copia&incolla, e può catturare immagini del contenuto del video in qualsiasi momento, allegandole al flusso di dati intercettato.

Se poi quel computer non è proprio utilizzato per accedere a nessun servizio in Internet, può essere usato per rimbalzare traffico di rete, addossandolo alla nostra connessione Internet. Il risultato di questa funzione, detta di *proxy*, è che colui che controlla il malware può tranquillamente fare qualsiasi birbonata senza paura di essere rintracciato, tanto l'indirizzo IP che apparirà alla vittima sarà il nostro.

Il firewall di Windows è praticamente inutile per evitare questo tipo di abuso, visto che il malware può controllarne il funzionamento senza problemi. L'aver un router recente, che opera come firewall e permette di filtrare il traffico, potrebbe essere inutile se non è stato disattivato il servizio *UPnP*. Questo servizio permette alle applicazioni sui computer "dietro" al router di comunicare autonomamente quali porte aprire all'accesso da Internet verso il computer. Se il servizio è attivo, *Zbot* istruisce il router per inoltrare le porte che gli servono, silenziosamente e senza avvisare nessuno. Il risultato è che il computer diventa raggiungibile come se il router/firewall fosse trasparente.

Se ancora qualcuno ha dei dubbi sulla pericolosità e determinazione di que-



sta gente, nell'aprile del 2009 un ricercatore di sicurezza di S21sec.com<sup>1</sup> ha scoperto che *Zbot* possiede una funzione a dir poco inquietante: *kill OS* (uccidi il sistema operativo). Il comando, come suggerisce il nome, rende inutilizzabile il computer distruggendo il sistema operativo, probabilmente cancellando parti vitali di esso dal disco di sistema. Un altro ricercatore (di Abuse.ch<sup>2</sup>) pochi giorni dopo, esaminando un server *C&C* acquisito integro ed ancora col suo database completo di informazioni trafugate (155 gigabyte di dati, scusate se è poco), ha scoperto che il gestore di una botnet con oltre 100.000 computer aveva usato il comando **kos** (*kill OS* appunto) su di essi, provocando una ecatombe. In un colpo aveva ridotto a pezzi di ferro 100.000 computer, costringendo i proprietari a reinstallare completamente il sistema operativo e tutte le applicazioni.

Al momento in cui scrivo, il sito Abuse.ch<sup>3</sup>, nelle statistiche di rilevamento della rete di *Zeus*, elenca poco meno di 200 server *C&C* attivi, oltre milleottocento differenti versioni di *Zbot*, di cui solo il quaranta per cento è riconosciuta dagli antivirus.

Nello stesso momento, *niente* fa supporre che la rete criminale sia in pericolo o in declino.

## Le sorprese non sono finite

Per motivi che non sono immediatamente evidenti, *Zbot* non possiede un suo meccanismo di propagazione. Non sfrutta falle del sistema operativo per propagarsi via rete, né si trasferisce su *pen drive* USB, né si spedisce via posta elettronica, sfruttando i contatti della rubrica. Niente di tutto questo.

La propagazione è affidata a campagne di spam, riportanti link a siti web attrezzati per scodellare il malware nei computer delle vittime, oppure il malware è allegato al messaggio stesso, camuffato da qualcosa d'altro.

I vantaggi sono molteplici:

1. <http://blog.s21sec.com/2009/04/when-bot-master-goes-mad-kill-os.html>
2. <http://www.abuse.ch/?p=1327>
3. <http://www.abuse.ch/>

- la diffusione è limitata e mirata: solo chi riceve i messaggi trappola o chi viene attaccato direttamente con varie tecniche, verrà infettato. Questo permette di tenere sotto controllo non solo il numero di computer colpiti, ma anche ad esempio la nazionalità delle vittime: se i messaggi di spam sono diretti ai residenti di una particolare nazione, basta usare la lingua giusta, o fabbricare il sito web trappola nella lingua desiderata;
- si può decidere con estrema precisione chi attaccare, ad esempio fabbricando messaggi trappola indirizzati solo ai dipendenti di una determinata azienda;
- il malware è meno rilevabile dalle reti di controllo delle varie organizzazioni e aziende che si occupano di sicurezza: il fatto che la propagazione sia controllata, rende meno probabile la cattura di esemplari per caso. Una volta raggiunto il numero di elementi voluti nella propria botnet, si può eliminare il sito trappola e terminare l'invio dello spam, diventando di fatto invisibili;
- la necessità di campagne di spam e di siti trappola crea un mercato per chi offre questi servizi usando botnet già esistenti. Non dimentichiamo che lo scopo di questa gente è fare soldi;

La mancanza di un sistema di propagazione integrato sembra più un vantaggio che un problema, nel complesso.

Il messaggio più inquietante, in ogni caso, è che la propagazione conta sul fatto che sia l'utente ad autodanneggiarsi, sia avviando volontariamente il malware propinatogli come *codec* per vedere filmati "anatomici", sia andando a visitare i siti "pubblicizzati" dallo spam, i quali tenteranno di sfruttare una qualche vulnerabilità del browser o di uno dei suoi plugin per iniettargli il malware.

Il metodo preferito è e rimane sempre lo stesso: ingannare l'utente ed indurlo a fare qualcosa che ha come risultato l'infezione.

## Non tutto è perduto

Le caratteristiche di *Zeus* sono certamente di tutto rispetto, e giustificano l'attenzione che molte società di sicurezza e di ricerca gli dedicano. Per fortuna ci sono delle ragioni per non essere del tutto pessimisti.

E' vero che *Zbot* ha elevate capacità di occultamento ed evasione, operando con molte tecniche tipiche dei *rootkit*. Ma è anche vero che per poter applicare queste tecniche deve poter disporre dei privilegi amministrativi nel momento in cui si attiva.

Se l'account utente in cui viene avviato *non ha* i privilegi amministrativi, è vero che il malware continua a funzionare, ma con parecchie limitazioni e qualche segnale, anche se molto labile, che sia successo qualcosa al computer.

Utilizzando la consueta tecnica delle macchine virtuali, si possono condurre test sul comportamento di *Zbot* nelle varie situazioni.

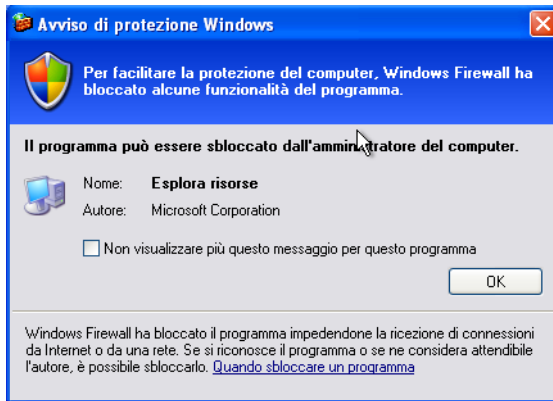
Partiamo da Windows XP: se l'account in cui viene attivato è di tipo amministrativo, ossia con privilegi massimi, non c'è scampo e il disastro è certo. L'intero computer è compromesso, ed occorre operare tempestivamente, sempre che ci si renda conto di qualcosa.

Se invece l'account è di tipo limitato, come dovremmo aver sempre fatto dopo aver letto il primo libro, le cose non proprio facilissime per il malware. Riesce ad insediarsi, riesce a intercettare il traffico e trafugare credenziali, ma al momento dell'insediamento vanno storte un po' di cose:

- non può insediarsi nelle directory di sistema di Windows, deve accontentarsi di infilarsi in qualche directory poco visibile dell'account utente da cui è stato attivato, di solito nella directory nascosta `Dati Applicazioni`, in una sottodirectory con un nome casuale e improbabile. Il file eseguibile stesso si rinomina con una sequenza casuale di caratteri. Usando un account amministrativo, i file sono perfettamente visibili ed eliminabili.
- non può iniettare codice nei processi di altri utenti, in quanto non possiede i privilegi necessari.
- nel momento in cui va ad aprire porte in ascolto sulla interfaccia di rete, il firewall di Windows se ne accorge e lo blocca, mostrando un avviso di sicurezza.
- non può interferire con l'antivirus, per cui se in uno degli aggiornamenti del database delle firme vi è compresa la variante che si è introdotta nel computer, verrà rilevato ed eliminato dall'antivirus stesso.

- se ci si accorge dell'intruso, è relativamente indolore eliminarlo, basta entrare con un account amministrativo e cancellare file e riferimenti nel registro, naturalmente sapendo dove mettere le mani.

Figura 6-1. L'attacco di Zbot in Windows XP



Al momento dell'attivazione, in un account non amministrativo, viene mostrato un messaggio del Centro di Sicurezza, relativo a un tentativo di accesso a Internet da parte di tutt'altro programma, Esplora risorse, che sarebbe il gestore del desktop di Windows. Mai, per nessun motivo, Esplora risorse (o meglio l'eseguibile che lo rappresenta, `Explorer.exe`) necessita di accedere a Internet, quale che sia l'attività che stiamo eseguendo al computer. La comparsa di un messaggio di questo tipo è sicuramente indice di qualcosa che vale la pena approfondire. Se questo messaggio appare appena dopo aver visitato un sito web, indicato in un messaggio di posta elettronica o trovato in altro modo, oppure all'apertura di un allegato di posta elettronica, anche se si tratta di un documento PDF, siamo in presenza di un attacco da parte di un malware.

Con Windows 7 le cose sono abbastanza simili, può cambiare solo la directory in cui il malware va a nascondersi, poco altro. Il messaggio del Centro di

Sicurezza è leggermente differente, ed il pannello mostra una opzione a suo modo pericolosa.

**Figura 6-2. La reazione di Windows Seven**



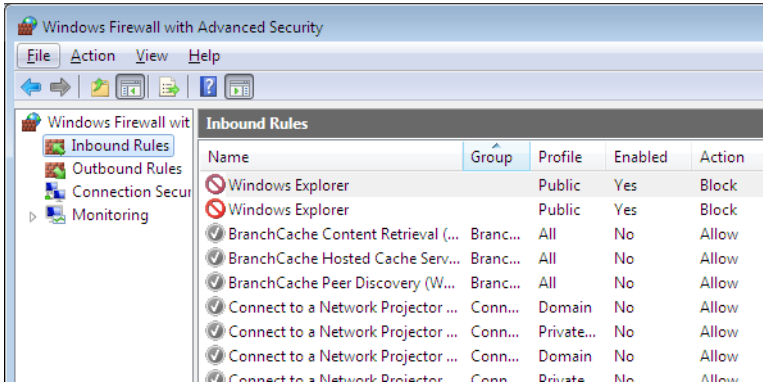
Il pericolo è rappresentato dalla “scorciatoia” per l’abilitazione. Mentre su Windows XP occorre cambiare account e passare ad uno amministrativo, con una operazione piuttosto lunga e laboriosa, che maggiormente può indurre l’utente medio a riflettere, in Windows 7 abbiamo un pulsante di autorizzazione già nel pannello. Un click, la password, e abbiamo lasciato fare al malware il suo sporco lavoro.

E’ pur vero che l’utente che non riflette *in toto*, non viene scoraggiato da una procedura più laboriosa, ma quello che non può l’assenza di pensiero potrebbe la pigrizia. Quel pulsante dovrebbe essere premuto solo dopo aver riflettuto accuratamente sul perché sia apparso il messaggio, ma una riflessione condurrebbe alla determinazione che quel pulsante *non va premuto affatto*.

Altra differenza fra Windows XP e Windows 7 è che il messaggio appare ad

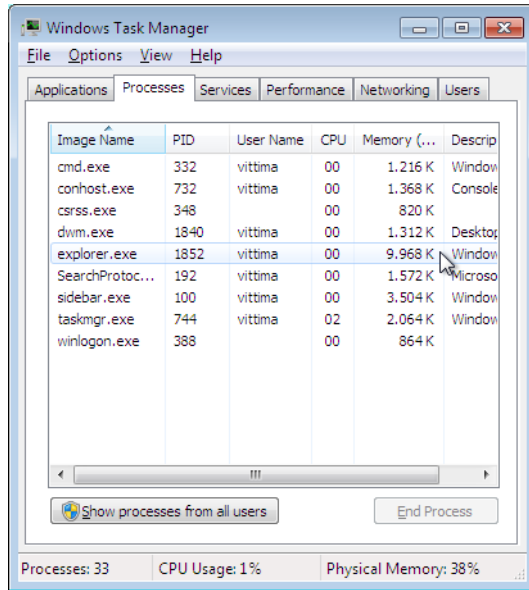
ogni avvio con XP, mentre con *Seven* appare solo la prima volta, poi più nulla, anche se il firewall continua a bloccare qualsiasi connessione sulle porte aperte dal malware.

**Figura 6-3. Le regole inserite automaticamente per bloccare Zbot**



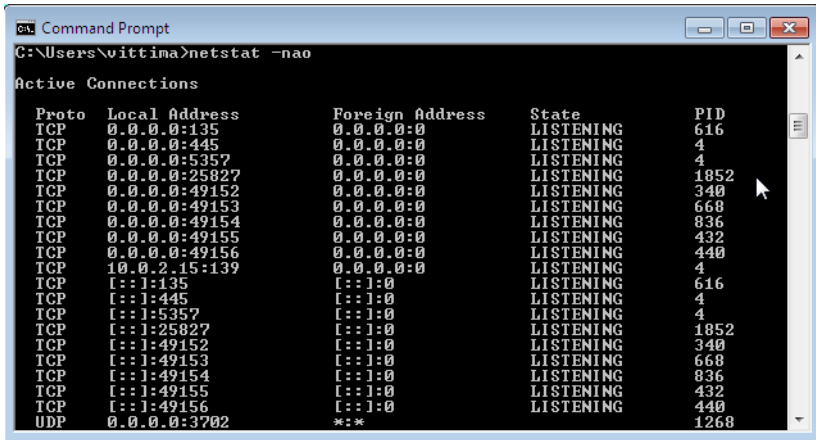
Per capire cosa stia succedendo, occorre incrociare i dati di tre differenti strumenti di Windows: il Task Manager, l'output del comando **netstat -nao** e il pannello di configurazione avanzata del firewall, dal Centro sicurezza nel Pannello di controllo. Da quest'ultimo abbiamo visto che vi sono delle regole nella categoria *inbound* (in arrivo) che riguardano `Explorer.exe`, il gestore del desktop (Figura 6-3).

Figura 6-4. Il Task manager con il PID visualizzato



Nel Task Manager occorre andare nella lista dei processi ed abilitare la vista della colonna del *PID* (*Process ID*) e si ottiene quanto mostrato in Figura 6-4. Poi dal Prompt dei comandi elencare le porte di rete aperte (Figura 6-5).

Figura 6-5. La lista delle porte aperte



```

C:\Users\vittima>netstat -nao

Active Connections

Proto Local Address          Foreign Address        State                   PID
TCP   0.0.0.0:135             0.0.0.0:0              LISTENING               616
TCP   0.0.0.0:445             0.0.0.0:0              LISTENING                4
TCP   0.0.0.0:5357            0.0.0.0:0              LISTENING                4
TCP   0.0.0.0:25827           0.0.0.0:0              LISTENING               1852
TCP   0.0.0.0:49152           0.0.0.0:0              LISTENING               340
TCP   0.0.0.0:49153           0.0.0.0:0              LISTENING               668
TCP   0.0.0.0:49154           0.0.0.0:0              LISTENING               836
TCP   0.0.0.0:49155           0.0.0.0:0              LISTENING               432
TCP   0.0.0.0:49156           0.0.0.0:0              LISTENING               440
TCP   10.0.2.15:139           0.0.0.0:0              LISTENING                4
TCP   [::]:135                [::]:0                  LISTENING               616
TCP   [::]:445                [::]:0                  LISTENING                4
TCP   [::]:5357               [::]:0                  LISTENING                4
TCP   [::]:25827              [::]:0                  LISTENING               1852
TCP   [::]:49152              [::]:0                  LISTENING               340
TCP   [::]:49153              [::]:0                  LISTENING               668
TCP   [::]:49154              [::]:0                  LISTENING               836
TCP   [::]:49155              [::]:0                  LISTENING               432
TCP   [::]:49156              [::]:0                  LISTENING               440
UDP   0.0.0.0:3702            *:.*                    LISTENING               1260

```

Nel caso mostrato, Explorer ha PID 1852, e nella lista delle porte aperte la 25827 risulta in attesa di connessione dall'esterno, cosa assolutamente anomala per un computer in buona salute.



### Niente panico!

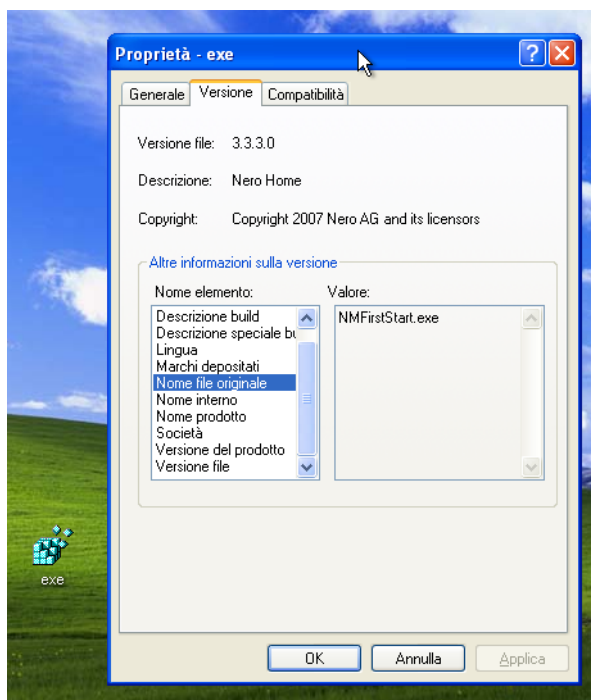
Naturalmente quanto mostrato non deve indurre a frugare freneticamente fra PID e lista porte per capire se abbiamo ospiti indesiderati nel computer. E' soltanto un esempio teso a mostrare un metodo, più che una ricetta. Nella vita reale, tale sequenza di controlli viene fatta solo dopo un evento insolito ed anomalo come il messaggio di avviso di cui parlavamo (Figura 6-2).

L'eseguibile in oggetto era stato catturato il 13 luglio 2010, e solo 2 antivirus su 42 lo classificavano come malware, senza però identificarlo. Soltanto due settimane dopo, il 27 luglio, veniva riconosciuto come *Zbot* da appena 9 antivirus su 42, mentre altri 18 antivirus lo identificavano come malware generico e altri 6 come sospetto. Il file si chiamava `exe.exe`, come icona aveva la stessa di un file



.REG e si autoproclamava prodotto dalla nota casa di software per masterizzazione Nero.

Figura 6-6. Zbot sotto mentite spoglie



## Continuiamo ad autoregolarci

In conclusione, quindi, è vero che l'uso di un account utente non amministrativo non rappresenta la panacea contro ogni malware: *Zbot*, anche da un account limitato riesce a fare il suo sporco lavoro. Ma è anche vero che l'uso di un account non amministrativo circoscrive grandemente il campo di azione di qualsiasi malware. Se *Zbot* riesce ad attivarsi da un account con privilegi elevati può usare

tutto il suo sofisticato arsenale di tecniche da *rootkit*, e possiamo essere certi che diventerà molto più difficile accorgersi della sua presenza, come pure sarà complicatissimo procedere alla sua rimozione, senza ricorrere ad una formattazione completa.

Se anche è nostra abitudine rivolgerci all'amico "che ne capisce" per riparare i danni fatti al nostro computer dai vari intrusi, l'uso abituale di un account limitato renderà il suo compito di pulizia molto meno faticoso, e con maggiori probabilità di successo.

## Capitolo 7. L'albero della cuccagna

“Stasera mi scarico un film da Internet”

“Hai un *ciddi* di Office?” “No. Senti, ma perché non provi OpenOffice, che è gratuito e funziona bene?” “Naaaa. Per carità, ogni volta che l’ho scaricato da eMule ho preso solo virus...”

“Mi hanno detto che Linux è meglio di Windows. Tu cosa usi?” “Uso Fedora, mi ci sono abituato e fa tutto quello che mi serve.” “Me la consigli? La trovo su eMule? Col crack?”

Frammenti di innumerevoli conversazioni che mi capitano e che rendono vagamente l’idea della gran confusione che regna in testa alle persone su questo argomento. Confusione colpevolmente e consapevolmente sfruttata da chi vende connessioni a Internet, abbinando neanche tanto implicitamente la fruizione a volontà di film, musica e videogiochi con la semplice connessione a Internet.

Tanto c’è eMule.

### Malintesi e sottintesi

Il *peer to peer* (in inglese “da pari a pari”) nasce come soluzione per la diffusione e lo scambio di file di grandi dimensioni senza accollarsi l’onere di un server con una connessione di rete veloce (e costosa). L’idea è quella di condivisione diffusa: se mi serve un file particolare, ne prendo un pezzetto da ognuno di quelli che ce l’hanno. Così anche con connessioni limitate e lente i tempi di attesa sono ragionevoli per ottenere quello che cerco.

Da qui allo scambio di qualsiasi cosa sotto forma di file il passo è brevissimo, come è brevissima l’evoluzione verso una sorta di archivio diffuso globale.

Il problema principale è che quello che viene scambiato *quasi mai* è farina del proprio sacco, o comunque qualcosa che si può diffondere liberamente. Musica, film e software, i tre “prodotti” più gettonati, sono praticamente sempre diffusi illegalmente: perché ognuno di questi prodotti è protetto da leggi in tutto il mondo il cui fine esplicito è di far avere un “giusto compenso” al creatore per la sua fatica.

Quando acquistiamo un software, un film o un brano musicale, non acquistiamo l'opera in sé, ma acquistiamo soltanto il diritto di fruirla in prima persona. E' tutta qui la chiave di lettura. Del software acquistiamo la licenza d'uso, dei film acquistiamo il diritto per la visione privata, per la musica l'ascolto. Qualsiasi altro uso è vietato. Per capirci, il prestare un DVD col film ad un amico, originale naturalmente, è in teoria vietato. Il diritto alla visione privata è personale e non cedibile.

Non ho intenzione alcuna di addentrarmi nel ginepraio di leggi e leggine che regolano la questione, ci basti saperne l'effetto finale: scambiare software, film e musica tramite un circuito *peer to peer*, anche se possediamo un supporto originale, è illegale. Ed è illegale al punto che il proprietario dell'opera può, per legge, chiederci i danni per il mancato guadagno a causa della distribuzione da parte nostra, secondo il ragionamento molto comune che ogni copia scaricata da Internet equivale a una copia originale in meno venduta regolarmente.



### **I danni all'industria musicale e cinematografica? Tutti da dimostrare**

Nell'aprile del 2010 il *Government Accountability Office* (qualcosa di molto simile alla nostra Corte dei Conti, ossia un istituto che controlla come vengono spesi i soldi pubblici e con quale efficacia) ha rilasciato il risultato di uno studio<sup>1</sup>, commissionatogli dal Congresso, per vedere se era possibile migliorare i risultati nella protezione della proprietà intellettuale. Il punto centrale dello studio era che in realtà nessuno dei metodi e delle statistiche usate per mostrare i danni della pirateria era affidabile, quindi era impossibile valutare correttamente il danno sia per i produttori, come mancato introito, sia per lo stato, per l'evasione delle imposte sui beni.

Anzi, secondo lo stesso studio, ci sono alcuni effetti positivi della pirateria, effetti che in una relazione<sup>2</sup> dell'italianissima AGCom (Autorità per le Garanzie nelle Comunicazioni) del febbraio 2010 vengono esplicitati (pag 35, paragrafo 3.1.4) citando uno studio del 2004:

[lo studio sostiene come attraverso il file sharing, N.d.A.] il consumatore possa venire a conoscenza di musica che altrimenti non avrebbe

1. <http://www.gao.gov/products/GAO-10-423>

2. <http://www.agcom.it/default.aspx?DocID=3790>

conosciuto e come questo possa promuovere le vendite a seconda che il consumatore abbia apprezzato o meno la musica ascoltata.

Personalmente ritengo sia la pura verità. Non sapevo dell'esistenza della versione cinematografica del fumetto "V for Vendetta"<sup>3</sup> (in Italia col titolo "V per Vendetta") e non avevo potuto vedere al cinema la trasposizione del videogame "Max Payne"<sup>4</sup>, e di entrambi ho acquistato il DVD originale dopo aver visto una versione scaricata via *peer to peer*. E' anche probabilmente non troppo distante dal vero quello che affermano alcuni studi citati dal rapporto della AGCom: non è assolutamente detto che un film o un brano musicale scaricati via *peer to peer* equivalgano ad un biglietto cinematografico, ad un DVD o ad un CD venduti in meno. Probabilmente la persona che si accontenta di versioni spesso di scarsissima qualità audio e video difficilmente spenderebbe una qualsiasi cifra, anche irrisoria, per avere l'originale.

Naturalmente questa non vuole essere assolutamente una difesa della pirateria, al contrario. Il punto è che non si combatterà mai con successo la pirateria e la contraffazione se non si prenderà coscienza di alcune cose:

- Far pagare a chi acquista gli originali i costi per la protezione da copia è un controsenso. Come è un controsenso ficcare i filmati con il pistolotto che copiare e scaricare da Internet è illegale negli originali e renderne obbligatoria e non interrompibile la riproduzione: quale parte di "ho comprato un originale" risulta difficile da capire a chi produce film?

Il risultato di queste due idee geniali è che chi compra un originale paga per qualcosa che gli rende difficile la fruizione (la protezione da copia spesso causa problemi con i riproduttori) e scoccante l'attesa (provatevi a far ragionare quattro bambini fra i quattro ed i sette anni che fremono per vedere l'ultimo film animato, mentre sullo schermo passano gli avvisi che scaricare un film è illegale...), mentre chi scarica un film da Internet non paga nulla e il film lo vede da subito.

---

3. [http://it.wikipedia.org/wiki/V\\_%28fumetto%29](http://it.wikipedia.org/wiki/V_%28fumetto%29)

4. [http://it.wikipedia.org/wiki/Max\\_Payne](http://it.wikipedia.org/wiki/Max_Payne)

- Se sono un fan di Star Trek<sup>5</sup> è lapalissiano che acquisterò gli originali, sempre e comunque. Se delle avventure “dove nessuno è mai giunto prima” non me ne importa nulla, può darsi che un film scaricato lo guardi pure, se non ho nulla di meglio da fare, ma comprare un DVD proprio no.
- Per una famiglia di quattro persone pagare 40 euro per vedere un film al cinema è pura follia. Pagarne 30 per il DVD un po' meno, ma ci si sente piuttosto fessi se dopo sei mesi lo stesso DVD si trova originale in offerta a 7 euro e 90. Magari con prezzi più ragionevoli, le vendite potrebbero beneficiarne.
- Ultima follia: alzi la mano chi non ha buttato decine di videocassette VHS originali ora che i videoregistratori sono storia. Dato che quello che ho pagato è il diritto alla fruizione privata, e non il supporto, perché ora dovrei acquistare le versioni in DVD per vedere qualcosa *che ho già pagato?*

Quindi, la pirateria è comunque da condannare, ma per combatterla occorre ben altro che le strategie indiscutibilmente perdenti sposate fino ad ora. Non ultima quella di combattere le tecnologie: rendere il *file sharing*, ossia l'uso del *peer to peer*, illegale *in sé* è totalmente inutile e dannoso. Le tecnologie sono neutre, come Internet, e devono essere trattate come tali.

## Openche?!?

Per il software il discorso è molto simile, con alcune differenze peculiari, che danno meno spazio a giustificazioni.

Anche per i programmi non acquistiamo la proprietà, ma la licenza d'uso, che in più ha una limitazione sul numero di computer in cui è possibile installare ed usare il software, di solito uno solo. Vi sono delle licenze che permettono di installare più copie a patto che ne sia utilizzata solo una alla volta, utile per chi ha un computer in ufficio, uno a casa ed un notebook, ma in definitiva il problema della proprietà intellettuale è lo stesso che per film e musica.

Quello che cambia è che mentre per un film non abbiamo alternative, c'è solo un “I Predatori dell'Arca Perduta”, per il software le cose cambiano, e parecchio.

---

5. <http://www.startrek.com/>

Un software, che è uno strumento per fare qualcosa, può esistere in molte versioni differenti, a cui viene associato un costo differente. Ne possono esistere differenti realizzazioni, di differenti produttori, che però consentono di fare le stesse cose, a meno di differenze minori. Infine ne può esistere una realizzazione con una licenza d'uso completamente gratuita.

Di licenze completamente gratuite ne esistono varie, da quella che permette l'uso per fini personali, ma non per impieghi commerciali, a quella che permette l'uso senza alcuna limitazione, a quella che offre in aggiunta la possibilità di modificare a piacere il programma, dato che ne mette a disposizione i sorgenti.



### **Eseguibili e sorgenti**

Ogni programma di computer è originato da un testo scritto in un linguaggio formale, il cosiddetto *codice sorgente*. Questo testo è umanamente comprensibile, e può essere modificato a piacere per aggiungere funzioni al programma, o per trasformarlo in un programma differente, riutilizzando parte del codice.

Attraverso una operazione detta *compilazione*, un codice sorgente viene trasformato in un codice eseguibile, o più semplicemente *eseguibile*, che è comprensibile solo alla macchina, e da cui è pressoché impossibile tornare indietro, nel senso che è possibile fare l'operazione inversa, ossia la *decompilazione*, ma il risultato è praticamente inutile.

Quindi, quelli che abbiamo di solito quando acquistiamo o scarichiamo un programma sono i *codici eseguibili*. In alcune licenze è possibile avere anche i *codici sorgente*.

La grande libertà offerta dalle licenze dette *Open Source* (a sorgente aperto, inteso come di libero impiego), ha tanti e tali di quei vantaggi che anche molte grandi aziende che producono software si stanno muovendo in questa direzione, spostando i costi del software dalla semplice licenza ai servizi: se prima si pagava per avere una licenza, a seguito della quale l'utente veniva lasciato solo con i suoi problemi, ora si punta a far pagare solo l'assistenza, mentre la licenza è completamente priva di costi.

Tornando al nostro discorso, esistono validissime alternative a software costosi, di uso professionale. Il problema è come conoscerle e come reperirle. Per fortuna vi sono dei siti web che si occupano di questo, a partire da *Open Source as Alternative*<sup>6</sup>, passando per SourceForge<sup>7</sup> e FreshMeat<sup>8</sup>, per arrivare agli innumerevoli siti web che pubblicano notizie ed aggiornamenti relativi al mondo Open Source.



### Open Source per tutti

Il software Open Source viene associato quasi automaticamente a Linux, ma oggi è molto riduttivo: tutti i sistemi operativi che abbiano una qualche rilevanza hanno un discreto parco di applicazioni Open Source a cui attingere. Windows, Mac OS X, Solaris, per tutti esiste almeno una raccolta di software libero e gratuito da esplorare alla ricerca di qualcosa di utile.

Anzi, da tempo esistono software Open Source nati su Windows, che non hanno versioni per Linux.

Tutto questo, naturalmente, è vero a due condizioni: che si abbia seriamente intenzione di imparare qualcosa di nuovo; che non vi siano problemi di compatibilità.

Spesso mi capita che persone che hanno installato su mio consiglio alternative Open Source tornino da me con fare vagamente accusatorio: “il programma *che mi hai fatto installare* non ha la funzione XYZ!”. Inutile dire che nella totalità dei casi la cosa si risolve semplicemente mostrando alla persona in quale menù si trova la funzione richiesta. Altre volte capita che effettivamente ci sia un problema di compatibilità, nel senso che la persona ha necessità di leggere o scrivere i dati in un formato specifico, tipicamente quello proprietario di un software commerciale. Le ragioni possono essere molte, ma in generale cerco di far capire che i produttori di software commerciale *non hanno nessun riguardo* per i nostri dati. Se abbiamo fatto un bellissimo disegno con il noto programma di grafica, sicur-

---

6. <http://www.osalt.com/>

7. <http://sourceforge.net/>

8. <http://freshmeat.net/>



mente con una versione regolarmente pagata, tre o quattro anni prima, e vogliamo riprenderlo, può accadere che non sia possibile per vari motivi:

- la versione che abbiamo non funziona più sul computer nuovo, perché il sistema operativo è troppo nuovo e non ce lo fa installare
- il produttore ha cessato l'attività, e non si trovano nuove versioni
- le nuove versioni non leggono più quel formato di file

In ognuno di questi casi i nostri lavori sono perduti.

Nelle versioni Open Source questo difficilmente avviene. Prendiamo ad esempio OpenOffice<sup>9</sup>, la suite gratuita di programmi per l'ufficio. Nel momento in cui scrivo è appena stata rilasciata la versione 3.3 e sta per uscire la versione 3.4. Ho documenti scritti con OpenOffice versione 1.1 del 2004 che sono tranquillamente riconosciuti ed utilizzabili nelle ultime versioni. Niente fa pensare che OpenOffice sarà abbandonato, né che cesserà di essere compatibile con i file delle versioni precedenti. Al contrario, il formato dei file che rappresentano i documenti creati con OpenOffice è diventato uno standard internazionale, denominato "ISO/IEC 26300:2006 Open Document Format for Office Applications (OpenDocument<sup>10</sup>) v1.0".

Se non vogliamo perdere tempo a cercare e scaricare i singoli programmi, possiamo provare il The Open CD/The Open DVD Project<sup>11</sup>, una raccolta su CD o su DVD di software Open Source per Windows.

Se in più vogliamo la comodità di poter usare i nostri software Open Source preferiti senza doverli installare, su qualsiasi computer, ci sono dei progetti come Portable Apps<sup>12</sup>, WinPenPack<sup>13</sup> e Liberkey<sup>14</sup>. Ognuno di essi offre la possibilità di crearsi il proprio *pen drive* USB pieno di applicazioni utilissime che funzionano senza bisogno di installazione.

---

9. <http://www.openoffice.org/>

10. <http://en.wikipedia.org/wiki/OpenDocument>

11. <http://linux.studenti.polito.it/>

12. <http://portableapps.com/>

13. <http://www.winpenpack.com/en/index.php>

14. <http://www.liberkey.com/en/>

A questo punto, se ancora ci ostiniamo ad usare software pirata, la ragione principale è la pigrizia, non l'assenza di funzioni, la praticità o la mancanza di compatibilità.

Non ho dimenticato che qui stiamo parlando di pericoli e sicurezza. Ci sono ancora parecchi argomenti a favore di un uso intelligente e sensato del *peer to peer*, in particolare ci interessano quelli legati ai rischi dell'uso *sportivo* (leggi superficiale e incosciente) del *peer to peer*.

## Non è questo che cercavo...

Una mattina di qualche tempo fa, una persona si presenta nel mio ufficio, in mano un CD registrabile ed un *blister* con una scheda di memoria appena acquistata: "ho bisogno di un'opera di bene", esordisce.

L'opera consiste nel trasferire nella scheda di memoria un noto software di navigazione satellitare, corredato di tutte le mappe del pianeta, cosicché sia possibile installare ed utilizzare il software nello *smartphone* di ultima generazione di un parente in visita.

A parte che per *opera di bene* intendo solitamente altre cose, quando ci si può permettere uno *smartphone* di ultima generazione, a maggior ragione si possono spendere i pochi (al confronto) euro per il software originale e le relative mappe.

Comunque, prendo il CD, la scheda e li inserisco nei rispettivi lettori. Il file nel CD è uno solo, di dimensione piuttosto corposa, 660 megabyte, con estensione RAR<sup>15</sup>. Faccio presente che difficilmente funzionerà in questo modo, occorre esplodere l'archivio compresso e scrivere sulla scheda i file non compressi. Il gestore di archivi di Linux, File Roller, si rifiuta di aprire il file RAR, affermando che è corrotto. Naturalmente ho installato l'utility **unrar**, e provo da riga di comando, ma niente da fare.

Supponendo (erroneamente) che il formato sia incompatibile per qualche motivo con la versione di **unrar** per Linux, mi sposto sul computer con Windows e avvio WinRAR. Stessa storia, archivio corrotto. Rimetto il CD nel computer con Linux, e copio il file dal CD al computer, immaginando che ci sia un errore di

---

15. <http://www.rarlab.com/>

masterizzazione. In attesa della copia, chiedo alla persona se il file fosse integro. La risposta, perentoria e sicura: “Ma certo! L’ho verificato!”. Un po’ intimidito da tanta sicurezza, rinuncio ad approfondire in cosa consista la “verifica”. Nel frattempo la copia termina regolarmente, escludendo anche errori di masterizzazione. Tento di nuovo **unrar** sia con l’opzione di test che con l’opzione di tenere i file corrotti, ma niente da fare. Prima di gettare la spugna, provo ad usare il comando **file**, che serve ad identificare il formato di un file dal contenuto e non dal nome. La risposta è abbastanza sorprendente:

```
RIFF (little-endian) data, AVI, 640 x 480, 29.97 fps,  
  video: DivX 4, audio: MPEG-1 Layer 3 (stereo, 48000 Hz)
```

ossia un file video in formato AVI. Dato che il comando **file** raramente sbaglia, soprattutto quando i parametri stampati sono coerenti come in questo caso, decido di divertirmi un po’.

“Non so come tu abbia verificato il file, ma qui non c’è un navigatore satellitare, e neanche mappe. Più che altro scommetto sia un *atlante anatomico...*” dico alla persona mentre lancio il file incriminato con `mplayer`<sup>16</sup> (un lettore multimediale per Linux, Windows e Mac OS X). Intanto giro il monitor verso di lui, e potete immaginarne la sorpresa quando appare un filmato, con scritte in ideogrammi (probabilmente cinesi o giapponesi). Inutile dire che saltando a pochi minuti dall’inizio del film il colore dominante sullo schermo si rivela essere il rosa carne.

Il nome del file era qualcosa di simile a:

```
noto-navigatore+mappe Europa+crack+keygen (OK  
FUNZIONANTE!!!).rar
```

notare i tre punti esclamativi.

Questa è una pratica abbastanza comune, nei circuiti *peer to peer*: vedere cosa le persone stanno cercando e offrirgli pronto per il download un file che ha un nome verosimile, con tanto di conferme. E’ ovvio che non c’è nulla di quanto cercato in quei file. Lo scopo è di sfruttare questa inclinazione per far sì che colui che scarica si trovi ad aver perso tempo, nella migliore delle ipotesi, o ad avere il computer compromesso da qualche malware che vi farà i propri comodi.

---

16. <http://www.mplayerhq.hu/>

La stessa strategia in questi ultimi anni è messa in atto da chi vuol proteggere i propri prodotti (film, musica e software), usando delle tecniche dette di *content poisoning*<sup>17</sup> (avvelenamento dei contenuti): ogni file che ospita contenuti illegalmente diffusi viene affiancato da un file di identica lunghezza e nome, ma disponibile in molti più server sulla rete, oppure parti del file vengono sostituite durante il download, sfruttando punti deboli nel protocollo<sup>18</sup> di *peer to peer*. Chi vuole scaricare quel file punterà a quello più facilmente reperibile, che però ha un contenuto differente o del tutto inutilizzabile.

## Chi cerca trova, pure troppo

Vediamo di persona cosa realmente ottenga chi si avventuri nel download via *peer to peer* senza avere un minimo di cognizione dei pericoli a cui va incontro.



### **Do not try at home!**

Eccesso di cautela, forse, ma mi sembra doveroso a questo punto avvisare chiunque voglia fare dei test per verificare quanto riportato. Oltre al rischio di beccarsi qualche pestilenza sconosciuta e particolarmente dannosa, il download di materiale dalle reti *peer to peer* può condurre a situazioni potenzialmente illegali. Prima di fare qualsiasi cosa, leggere fino in fondo il capitolo. Come ho già detto all'inizio, non sono e non sarò responsabile di eventuali sciocchezze commesse da alcuno.

Proviamo a cercare prima The GIMP<sup>19</sup>, il software di fotoritocco professionale Open Source, gratuito, poi OpenOffice<sup>20</sup>, la suite di programmi per l'ufficio, ugualmente gratuita. Entrambi i programmi possono essere scaricati direttamente dai rispettivi siti, probabilmente un po' più affidabili che prenderli da un completo sconosciuto, perché il *peer to peer* questo fa: recupera file in base al nome indipendentemente da chi lo detiene, quindi senza alcuna indicazione di chi sia il proprietario e quanto sia affidabile.

---

17. <http://gridsec.usc.edu/TR.html>

18. [http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?arnumber=5474821](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5474821)

19. <http://www.gimp.org/>

20. <http://www.openoffice.org/>



### eD2K, file e *hash*

Per condividere un file qualsiasi nella rete eMule è sufficiente piazzarlo nella directory scelta dal programma per i file in condivisione. Prima di condividerlo, il programma calcola un valore chiamato *hash*, strettamente legato al contenuto del file stesso, inteso come sequenza di numeri binari. Tale *hash* è calcolato con un particolare algoritmo, che tiene conto non solo dei valori dei singoli byte del file, ma anche della loro posizione. Per cui il valore dell'*hash* cambia radicalmente cambiando sia un solo bit nel file, che scambiando di posizione due byte. Altra caratteristica che dovrebbe avere è che sia impossibile “costruire” un file che abbia un determinato *hash*. Vedremo più avanti che, per quanto riguarda l'algoritmo di hash usato per eMule, ciò non sia più vero, a causa di gravi falle scoperte nell'algoritmo stesso.

Al termine del calcolo, il programma “annuncia” di avere disponibile un certo file, con un certo nome ed un certo *hash*. Quello che identifica in modo praticamente univoco un certo file è proprio il valore di *hash* associato, che viene impiegato per puntare un determinato file nell'oceano di tutti quelli condivisi, usando un link particolare, chiamato *link eD2K*<sup>21</sup>, che ha questa forma:

```
ed2k://|file|nome|1000|E610CD...505CD|/
```

dove *file* indica che il link si riferisce ad un file, *nome* è il nome con cui viene condiviso il file stesso, *1000* è la lunghezza in byte e l'ultimo gruppo di 32 caratteri è la rappresentazione in esadecimale dell'*hash*.

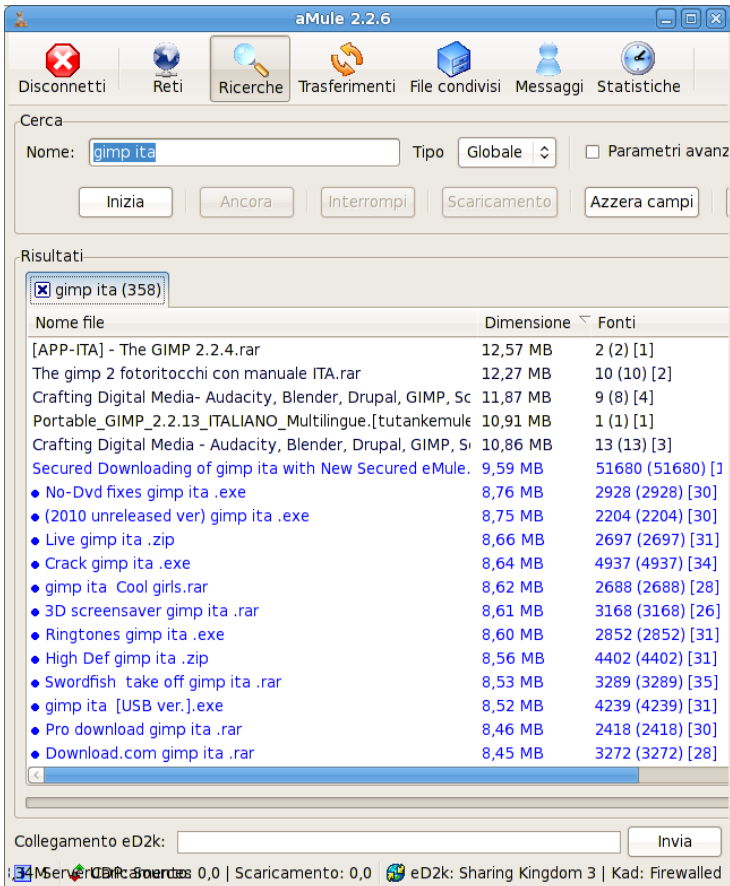
Se qualcuno scarica questo file, ne cambia il nome, rimettendolo in condivisione col nome differente, il valore di *hash* non cambia. Ecco perché è così facile trovare dei falsi: se qualcuno mette in condivisione il film “Atlante anatomico”, qualcun altro lo scarica e lo rimette in condivisione col titolo dell'ultimo film in prima visione, quando andiamo a cercare proprio quest'ultimo troveremo anche il trattato di anatomia fra i risultati delle ricerche. L'unico modo per capire se è un falso è di scaricarlo, non c'è altro da fare.

Alcuni programmi permettono di vedere tutti i nomi con cui viene condiviso un file con un determinato *hash* (vedi Figura 7-8), ma non è un sistema infallibile: se vi sono solo falsi, tutti i nomi dei file coincideranno, solo che il

21. [http://it.wikipedia.org/wiki/Link\\_ed2k](http://it.wikipedia.org/wiki/Link_ed2k)

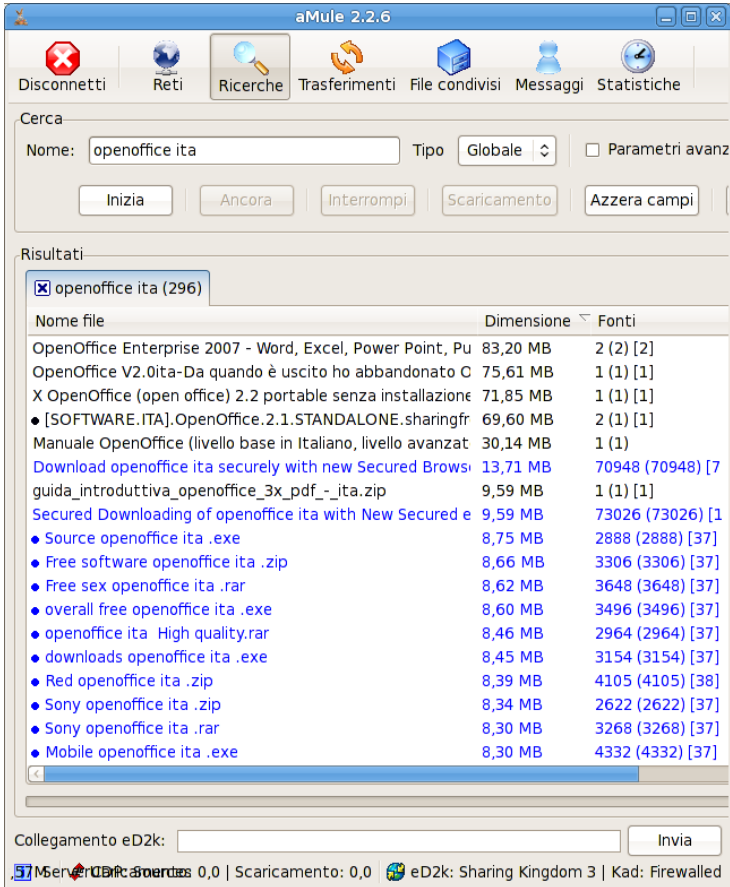
contenuto non corrisponderà mai a quanto dichiarano i nomi dei file, e non c'è modo di saperlo senza scaricare i file uno per uno.

**Figura 7-1. The GIMP: c'è anche il crack e la versione live...**



Come possiamo vedere in Figura 7-1, le cose sono piuttosto complicate. I file con più sorgenti sono *tutti fasulli*, nessuno escluso, mentre i file che potrebbero contenere veramente il software cercato ne offrono versioni vecchie di anni: al momento la versione distribuita è la 2.6.11, ed è in lavorazione la versione 2.8, mentre la versione 2.2.13, la più recente reperita tramite il *peer to peer* è dell'agosto del 2006.

Figura 7-2. OpenOffice: versione *mobile* e versione in alta qualità



Per OpenOffice le cose non vanno meglio. Oltre ad una inesistente versione *Enterprise* spacciata con i nomi di altre applicazioni più note, la versione più recente è la 2.2 del 2007, seguita dalla pletora di malware con nomi fantasiosi.

Un terzo dei file di lunghezza paragonabile a quella delle varie versioni di



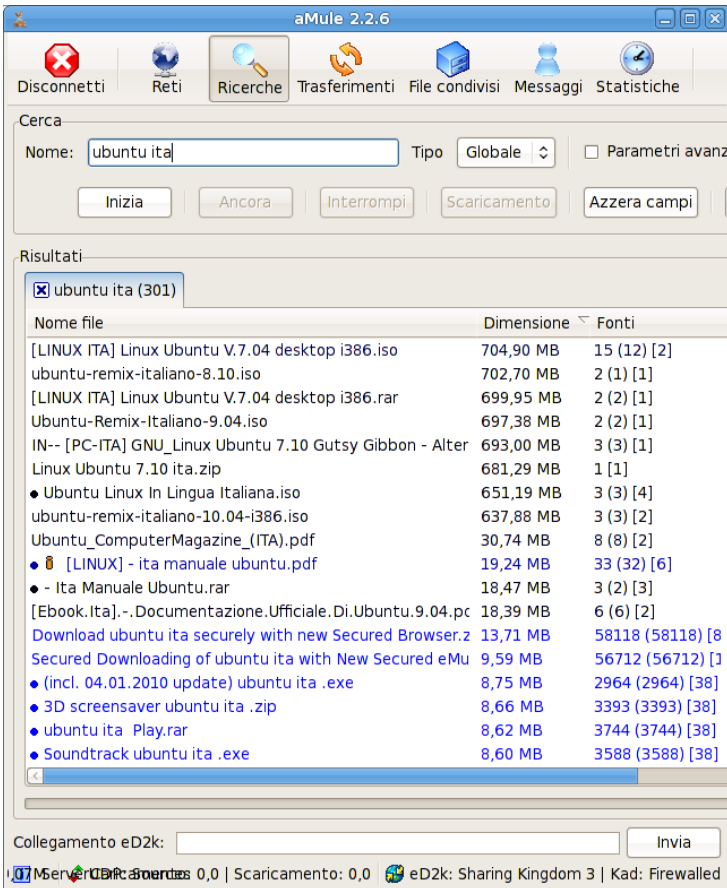
OpenOffice è costituita da filmati camuffati da archivi RAR, ZIP o immagini ISO. Naturalmente filmati decisamente poco adatti ai bambini.

Usando altri termini di ricerca i risultati sono costantemente deludenti. Cercando la distribuzione Linux Ubuntu<sup>22</sup> si ottengono vecchie versioni, unica non troppo vecchia (al momento siamo alla 11.04) la 10.04 *remix* pensata per i *net-book*, ma le dimensioni non corrispondono: l'originale scaricata dal sito è di 700 megabyte, questa è di 637 megabyte. Fra l'altro, le maggiori distribuzioni Linux includono in una unica versione tutte le lingue più comuni, per cui non ha nessun senso cercare la versione italiana, *lo sono tutte*. Altra cosa, una delle versioni fasulle dichiara la data di ultimo aggiornamento del software, ma in tutte le maggiori distribuzioni Linux il software è aggiornato continuamente e gratuitamente. Solo che molti non sanno che Linux ha queste caratteristiche, come non conoscono le caratteristiche di molti software Open Source, per cui continuano a ragionare con i parametri che conoscono: aggiornamenti a pagamento, registrazione della licenza, versioni differenti per lingue differenti, protezione da copia ecc.

---

22. <http://www.ubuntu-it.org/>

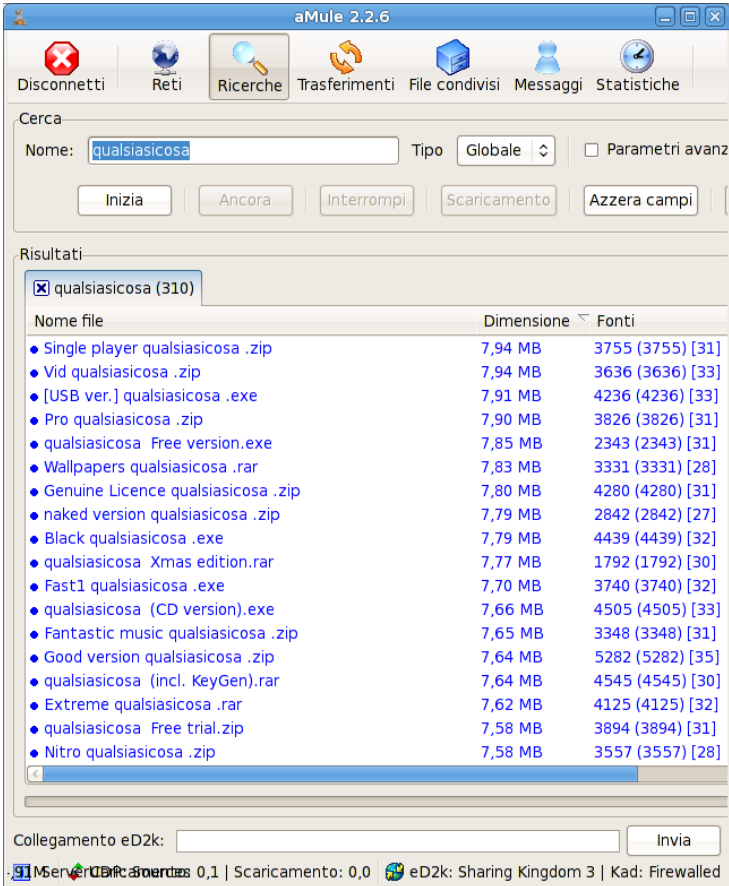
Figura 7-3. Con Linux Ubuntu le cose non è che siano differenti



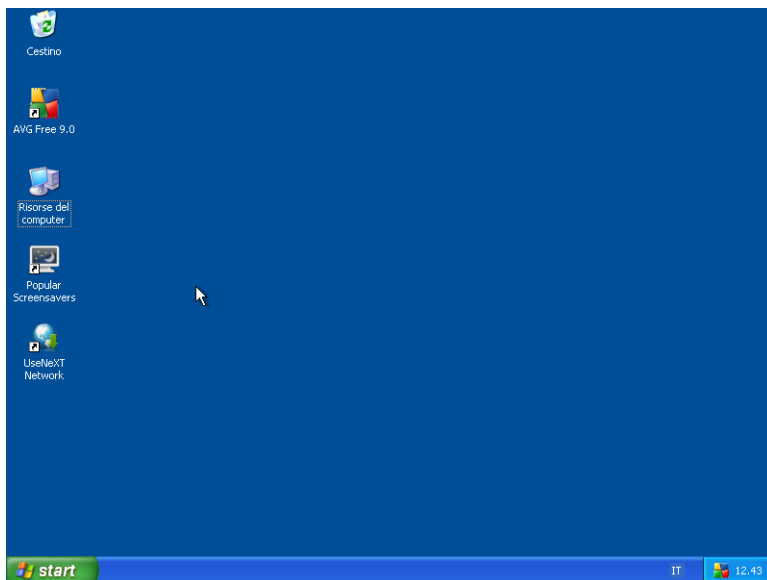
Andiamo sul ridicolo: cercando con una parola chiave improbabile, come a questo punto è facile intuire, si trova lo stesso una quantità di file. Qui siamo nel paradossale, ma serve a far capire il meccanismo che si cela dietro tutto questo: le parole chiave che digitiamo sono prese e trasformate in un nome di file, aggiungendo termini comuni nei circuiti *peer to peer*, per poi usarlo con file che

contengono tutto meno che roba utile, per noi almeno.

Figura 7-4. Cerco qualsiasi cosa, e la trovo!



**Figura 7-5. Le icone che appaiono sul desktop**



Tutti i file fasulli di questo tipo sono malware, senza eccezioni: passati al solito sito Virustotal<sup>23</sup>, in media meno di un sesto degli antivirus li identifica come tali. Eseguiti in una macchina virtuale con Windows XP e account sia amministrativo che normale, appaiono varie icone sul desktop, e viene avviato Internet Explorer, puntato su un sito di scommesse online.

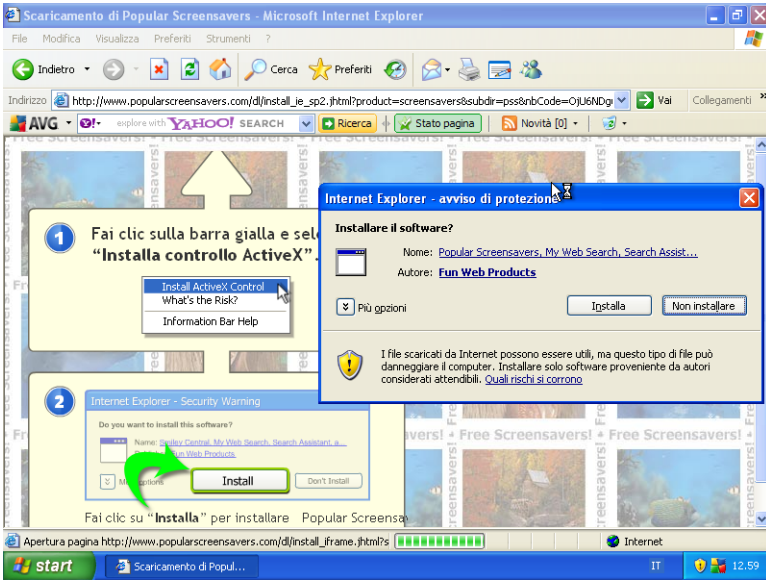
23. <http://www.virustotal.com/>

Figura 7-6. Il “gratta-e-perdi”, invece di OpenOffice



Le due icone, invece, portano a vari siti web che con la scusa di regalarci sfondi per il desktop, puntatori per il mouse, faccine per la chat e chi più ne ha, tentano di rifilarci un *adware*, ossia un bel software che ci sfinirà a forza di sparare pubblicità non richiesta mentre stiamo usando il computer per fare altro, corredato di un *search assistant* che si preoccuperà di fornirci risultati più pertinenti alle nostre ricerche su Internet. Pertinenti per chi intascherà i soldi della pubblicità, non per noi, che la subiremo.

Figura 7-7. Il solito ActiveX, e l'inferno è servito



Tutto questo andando a cercare software che è legalmente scaricabile da Internet o dai circuiti *peer to peer*: alcune distribuzioni Linux sono regolarmente distribuite in questo modo, anche se usano il circuito BitTorrent<sup>24</sup>, molto più affidabile, come vedremo, ma solo a certe condizioni.



### L'antivirus non ha fatto una piega

Ovviamente, sul computer di prova c'è l'antivirus, aggiornato al giorno del test. I malware sono stati in grado di fare i loro comodi senza alcun problema, l'antivirus non li ha mai riconosciuti, né ostacolati in alcun modo.

24. <http://it.wikipedia.org/wiki/BitTorrent>

Possiamo facilmente immaginare cosa succeda quando andiamo a scaricare un software commerciale che non sia legalmente scaricabile. Se siamo fortunati abbiamo il nostro software pirata, di cui per esperienza posso dire che ne sfrutteremo le potenzialità per meno del cinque per cento. Se, come è purtroppo molto probabile, incapperemo in una trappola, forse il software funzionerà anche, ma non saremo più i soli ad usare il computer.

Le trappole possono essere piazzate in vari punti, tutti di passaggio obbligato:

- Il programma è sotto forma di archivio compresso, una volta aperto troviamo un file eseguibile, di solito chiamato `setup.exe` o `install.exe`, ed un ulteriore archivio compresso, o una directory con molti file all'interno. La trappola è il file eseguibile, che eseguirà una installazione di ben altro che il software cercato, facile intuirlo.
- Il programma è sempre sotto forma di archivio compresso, al suo interno vi è una directory piena di file, fra cui il programma per rimuovere la protezione al momento dell'installazione (il *crack*) o per generare il codice di registrazione (il *keygen*). In questo caso la trappola è in questi due file, che eseguono il compito fino in fondo, eliminando la protezione del programma, ma anche quelle al nostro computer.
- Nel caso più fortunato, dipende dai punti di vista, il file pazientemente scaricato contiene tutt'altro, innocuo per il computer, ma potrebbe essere fonte di altri tipi di grattacapi: provatevi a spiegare alla fidanzata che in realtà cercavate un programma per farla più bella nelle foto...

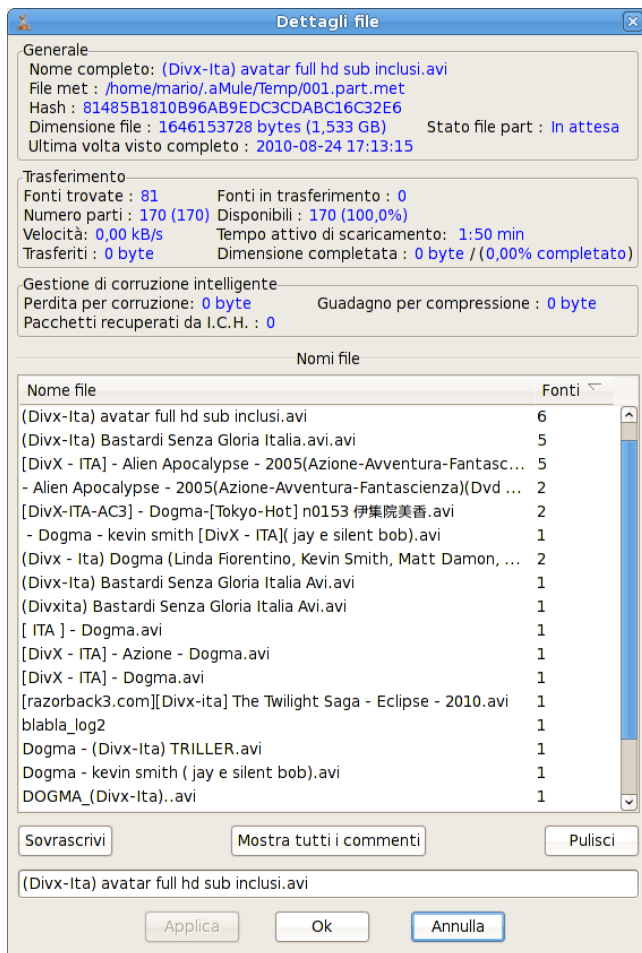
Se poi andiamo a cercare dei film o della musica, le cose peggiorano, e non poco. Ho fatto una semplice prova, cercando il noto film *Avatar* in italiano. Il numero di falsi è impressionante. Alcuni programmi mettono a disposizione una funzione che permette di vedere tutti i nomi che sono stati assegnati a quello specifico file. Impiegandola nei confronti dei risultati ottenuti, quasi nessuno è il film cercato, anche se i nomi dei file sembrano affermare il contrario: solo 5 fra i primi 20 risultati restituiscono file condivisi con il titolo cercato, gli altri sono

film di tutt'altro genere.

Non ho naturalmente verificato se quelli il cui nome è univoco siano poi effettivamente copie di Avatar, cosa che niente ci assicura. In Figura 7-8 si vede un esempio lampante della situazione: il file corrisponde ad almeno sei differenti gruppi di denominazione, è impossibile stabilire cosa effettivamente contenga.



**Figura 7-8. Ma insomma, che film è?**



Vi sono dei metodi per limitare queste sorprese, fra cui quello appena mostrato di verificare con che nomi viene condiviso un determinato file, ma non sono infallibili. In questo caso è abbastanza agevole evitare i falsi, ma il pericolo dei

malware rimane, soprattutto nella ricerca di software.

Tutto questo, naturalmente, senza entrare nel merito e senza nulla chiedere in fatto di qualità audio e video: molti film reperibili in questo modo sono effettivamente scadenti, avendo ad esempio l'audio registrato durante la proiezione del film, quando non l'intero film, audio e video.

## Sensi di colpa

Inutile nascondersi dietro un dito: il *peer to peer* è usatissimo per la ricerca e la fruizione del porno, in tutte le salse. Non ultimi i videogame a sfondo erotico, spesso di produzione orientale.

Pur essendo totalmente legale, e spesso il porno liberamente disponibile nel *peer to peer* lo è proprio perché serve da pubblicità ai siti che lo commercializzano (l'industria del porno è sempre avanti e pronta a cogliere le opportunità, ben prima dell'industria cinematografica in generale), pur essendo legalmente disponibile, dicevamo, è facile essere vittime di un sotterraneo senso di colpa nel fruire questo tipo di intrattenimento, sia per motivi culturali che sociali.

Questo è un terreno fertile per operazioni di *social engineering*: sfruttare questo indefinito, ma sempre presente, senso di colpa per “cogliere sul fatto” qualcuno e aggirarne il naturale senso critico.

E' quello che ad esempio<sup>25</sup> ha fatto una organizzazione criminale<sup>26</sup>, immettendo nei circuiti *peer to peer* un software che si spacciava per un videogame a sfondo erotico di una nota casa produttrice. Al momento della registrazione, operazione necessaria per poter giocare, venivano chieste molte notizie personali, con la scusa di rendere più coinvolgente l'esperienza ludica. Nello stesso momento, il malware esaminava il computer per estrarre alcune informazioni, fra cui siti web visitati, elenco dei file più utilizzati, versione di sistema operativo. Poi aggiungeva anche qualche *screenshot* di quello che c'era sul video del computer in quel momento.

25. [http://www.theregister.co.uk/2010/04/16/smut\\_malware\\_shakedown/](http://www.theregister.co.uk/2010/04/16/smut_malware_shakedown/)

26. <http://countermeasures.trendmicro.eu/japanese-porn-extortion/>

Dopo breve tempo, alla vittima giungeva un messaggio e-mail accusatorio, relativo ad una violazione del diritto d'autore<sup>27</sup>, in quanto nel suo computer erano presenti file audio in formato MP3 di grande valore, venduti sul sito ufficiale al prezzo di centinaia di migliaia di dollari. Naturalmente, i file MP3 erano stati scaricati dal malware, non dalla vittima, e comunque non valevano certo quella cifra, ma l'esistenza di un sito web dove il presunto proprietario effettivamente vendeva i file a quel prezzo costituiva una conferma per le vittime.

Il punto centrale del messaggio era che veniva proposto un "aggiustamento amichevole" per pochi dollari, a copertura della violazione.

Come ulteriore leva sulle vittime veniva usata la vergogna, aggiungendo nel messaggio l'indirizzo ad un sito web pubblico dove erano mostrati tutti i dati del malcapitato, insieme agli *screenshot*, a mo' di pubblica gogna.

Dato che le vittime erano in gran parte giapponesi, e che proprio in quel periodo il governo giapponese aveva inasprito le pene per le violazioni del diritto d'autore, la truffa colpì oltre 1500 vittime. Nello stesso periodo girava una truffa simile, solo che chiedeva alcune centinaia di dollari per "sistemare le cose". Non funzionò solo perché la cifra richiesta era molto alta, cadendo al di fuori della categoria dei micro-pagamenti, quindi le vittime invece di pagare iniziavano a farsi domande.

Dello stesso malware, appartenente alla categoria dei *ransomware* (software che chiedono un riscatto), sono stati rinvenute varianti per tutte le lingue più comuni, compreso l'Italiano.

Questa è una ulteriore dimostrazione di varie cose: che i malware non sono fini a sé stessi, ma vengono creati *sempre* per uno scopo; che la vulnerabilità maggiore dei computer è fra la tastiera e la sedia; che niente è gratis; che trattare il *peer to peer* come un centro commerciale è una *cattiva idea*.

## Incubi senza risveglio

A partire dal 2004, negli Stati Uniti, le case discografiche e cinematografiche hanno avviato una campagna giudiziaria contro i singoli colpevoli di aver

---

27. <http://ddanchev.blogspot.com/2010/04/copyright-violation-alert-themed.html>

scaricato o diffuso illegalmente contenuti protetti dal diritto d'autore. I risultati possiamo giudicarli da soli: negli anni dal 2006 al 2008 la RIAA<sup>28</sup> (*Recording Industry Association of America* assimilabile alla nostrana SIAE<sup>29</sup>, Società Italiana Autori ed Editori) ha speso qualcosa come 64 milioni di dollari in parcelle per avvocati ed investigatori, ottenendo in teoria risarcimenti per meno di un milione e quattrocentomila dollari, fonti: Recording Industry vs The People blog<sup>30</sup>, p2pNet News<sup>31</sup>, EFF<sup>32</sup> (*Electronic Frontier Foundation*).

Senza contare che alcuni casi<sup>33</sup> hanno avuto un effetto *boomerang* nei confronti della popolarità dell'ente:

- Tammy Lafky, una madre *single* di 41 anni, con figlia adolescente, si è vista presentare una richiesta di risarcimento danni di *mezzo milione di dollari*, per musica scaricata nel 2003. La donna guadagnava 12 dollari l'ora e non poteva neanche permettersi di pagare un avvocato.
- Cassi Hunt, una studentessa del MIT, si è sentita suggerire di mollare la scuola per pagare 3.750 dollari di danni, in quanto non poteva accollarsi un altro prestito finanziario oltre a quello già in essere per la scuola.
- Cecilia Gonzalez, madre di cinque figli, si è vista chiedere 22.500 dollari per aver scaricato musica, che possedeva già *in originale su 250 CD*, solo per risparmiarsi la fatica di trasferirli sul computer. Lei e suo marito spendevano in media 30 dollari al mese in CD originali.
- Una vedova disabile è stata accusata di aver scaricato 500 brani, da lei posseduti già in originale su CD, operazione giustificata dalla difficoltà di movimento causata dalla disabilità. Si è vista proporre un risarcimento ridotto a 2.000 dollari, a patto che *dimostrasse di essere realmente disabile*.
- Jammie Thomas si era vista addebitare 222.000 dollari di risarcimento per 24 (ventiquattro) brani musicali. La tesi che portava alla cifra, indubbiamente fuori

---

28. <http://www.riaa.com/>

29. <http://www.siae.it/>

30. <http://recordingindustryvspeople.blogspot.com/2010/07/ha-ha-ha-ha-ha-riaa-paid-its-lawyers.html>

31. <http://www.p2pnet.net/story/41631>

32. <http://www.eff.org/issues/intellectual-property>

33. <http://www.eff.org/wp/riaa-v-people-years-later>

da ogni umana logica, era che il fatto di aver messo i 24 file in condivisione sul circuito *peer to peer* automaticamente portava alla violazione della legge sul diritto d'autore, con conseguente applicazione di una penale per ogni copia distribuita, ossia per ogni volta che il file veniva scaricato da qualcuno. La tesi è poi stata smontata completamente, per fortuna.

Questi sono solo alcuni esempi di quello che capita negli Stati Uniti. Da noi in Italia le leggi sono ugualmente restrittive, se non peggio. Nel 2004, grazie al famigerato decreto Urbani si era tentato di equiparare la bancarella che vende CD e DVD duplicati illegalmente con il CD o il DVD copiato per l'amico o i file scambiati sul *peer to peer*, assimilando il guadagno dalla vendita di materiale appositamente duplicato con il risparmio sull'acquisto della singola copia da parte di un privato. Nel 2005 in un altro decreto convertito in legge<sup>34</sup> tale equivalenza cessa, e viene ripristinata la distinzione fra chi produce copie per venderle e chi ne realizza per esclusivo uso personale.

Questo non toglie però che anche da noi vi siano stati casi simili a quelli americani, come quello, nel 2007, della casa discografica tedesca che riuscì a reperire gli indirizzi IP di 4.000 utenti italiani, rei di aver scambiato materiale coperto dal diritto d'autore, chiedendo ad ognuno 330 euro a titolo di risarcimento, minacciando azioni legali<sup>35</sup>. In quello specifico caso le persone evitarono conseguenze solo perché il trattamento dei dati personali raccolti al fine della richiesta di risarcimento fu giudicato illecito dall'Autorità Garante per la protezione dei dati personali, costituitasi poi in giudizio.

Vi sono inoltre considerazioni riguardanti un altro aspetto dell'incauto uso del *peer to peer*. Nel campo della lotta alla pedofilia ed ai reati connessi, uno dei filoni di attività è quello del contrasto alla diffusione via Internet di questo tipo di materiale. I circuiti *peer to peer* sono attivamente utilizzati dai criminali per il commercio e lo scambio di foto e filmati, ed utilizzano varie tecniche per rendere difficile l'individuazione dei singoli attori: chi condivide, chi produce, chi fruisce.

Non è una remota eventualità che ci si possa imbattere in un filmato di questo tipo, cercando tutt'altro. I controlli che alcuni programmi permettono, ad esempio di poter vedere i primi minuti di un filmato in scaricamento, non sono sufficienti:

---

34. <http://www.parlamento.it/parlam/leggi/050431.htm>

35. <http://www.altalex.com/index.php?idnot=2541>

a volte il filmato è nascosto internamente ad altri insospettabili, a parecchi minuti dall'inizio; altre volte è camuffato da altro, come abbiamo visto prima.



### **Omissioni intenzionali**

Se qualcuno si domanda perché qui non si nominino plugin ed estensioni di eMule che servono a determinare il tipo di file scaricato dal contenuto e di vedere o ascoltare filmati e musica durante il download, è presto detto: è una omissione volontaria. *Non ho alcuna intenzione* di fornire appigli discutibili per permettere a chi scarica di tutto e di più di sentirsi tranquillo perché ha il plugin che gli dice se il file è un falso.

Ricordiamolo: non esistono magie tecnologiche, ed i nostri amici mentecatti sanno perfettamente come aggirare tutti questi trucchetti che, fra l'altro, sono il segreto di Pulcinella. Mostrarli qui significherebbe fornire elementi di rinforzo a quel falso senso di sicurezza che hanno tutti i "guidatori sopra la media", e che abbiamo deciso fin dall'inizio di avversare.

Il pericolo è causato da due differenti reati che possono concorrere in chi incappa nel download di un simile materiale: la detenzione (articolo 600-quater del Codice Penale) e la diffusione (articolo 600-ter del Codice Penale). La detenzione si realizza anche ospitando un singolo file sul proprio computer. La diffusione si realizza anche durante il download stesso, per come è la tecnologia *peer to peer*.



### **Come funziona il *peer to peer***

Ogni file è suddiviso in segmenti di lunghezza predefinita, ed al momento del download viene chiesto il singolo segmento, non l'intero file. I segmenti possono essere chiesti indifferentemente dalla posizione, per cui può arrivare prima la parte centrale del file, poi la parte finale e per ultimi i segmenti iniziali. Nel momento in cui un segmento del file viene scaricato, il programma diventa automaticamente "fornitore" per quel segmento, e lo distribuisce a qualunque altro programma lo richieda sulla rete, anche se è l'unico pezzo che ha del file. Questo comportamento è disabilitabile solo in alcuni programmi per il *peer to peer*, non in tutti, ed è normalmente un comportamento

predefinito. Occorre intervenire esplicitamente per negare la distribuzione dei segmenti durante il download.

Questo fa sì che se dovessimo incappare in un filmato pedo-pornografico, mentre in realtà cercavamo altro, potremmo essere accusati sia di detenzione, per il fatto di avere il file nel computer, sia di diffusione, per via della distribuzione automatica operata dal programma di *peer to peer*, reato ben più grave.

Poi, certamente, se il giudice ha gli elementi per determinare che il nostro è un comportamento assolutamente non intenzionale, potremmo cavarcela con relativamente poco visto che il Codice Penale nel reato di detenzione usa esplicitamente la parola *consapevolmente*, ma non è certo una esperienza consigliabile trovarsi accusati di diffusione di materiale pedo-pornografico in un periodo di così alta attenzione a questo tipo di reati.

## BitTorrent Vs eMule

Spendiamo due parole per definire le maggiori differenze fra i due protocolli di *file sharing* più utilizzati e conosciuti.

La rete su cui si basa eMule usa il protocollo detto *eD2K* o *eDonkey2000*, dal nome del primo client rilasciato da MetaMachine<sup>36</sup>, la società che aveva ideato il protocollo e sviluppato i primi software server e client.

Il protocollo di BitTorrent fu sviluppato nel 2001 da Bram Cohen, il quale fondò poi la BitTorrent inc.<sup>37</sup> per sfruttarne l'applicazione commerciale.

Entrambi i protocolli consentono di distribuire file di dimensioni elevate sfruttando la banda aggregata di tutti i partecipanti alla rete, ossia tutti gli utenti con un client connessi alla rete, di fatto eliminando la necessità di grandi server con connessioni veloci a Internet, dal costo elevatissimo.

Entrambi i protocolli *non proteggono l'anonimato di chi scambia file* in modo nativo. Con il protocollo *eD2K* vi è il concetto di *user ID*, una stringa esadecimale che identifica univocamente una installazione client, e che quindi è stret-

---

36. [http://en.wikipedia.org/wiki/EDonkey\\_network](http://en.wikipedia.org/wiki/EDonkey_network)

37. <http://www.bittorrent.com/>

tamente associata ad un determinato computer. Analizzando il traffico di rete è possibile determinare da quali indirizzi IP viene scaricato un determinato file, o parti di esso. Da qui, associarlo ad una specifica connessione a Internet, quindi ad un utente del provider e di seguito ad un computer di quell'utente è prassi comunemente seguita dagli investigatori per rintracciare chi scambia materiale illegale. Con il protocollo BitTorrent è ugualmente facile individuare da quali indirizzi IP è scaricato un determinato file, ma in più è banale individuare la fonte che ha diffuso il file in origine: è contenuta nel file `.torrent` che si scarica inizialmente per poter poi accedere al materiale cercato.



### **Anonimato in Rete? Una chimera.**

Occorre sfatare un mito pericoloso, quello dell'anonimato "facile" in Rete. Niente è più difficile del rimanere anonimi in Rete: ogni volta che accediamo ad un sito o apriamo una qualsiasi applicazione che accede a Internet il nostro anonimato è buttato alle ortiche. Il nostro indirizzo IP è il nostro primo punto debole: è più preciso del DNA, perché è univoco. Ogni volta che una applicazione si connette a qualsiasi servizio su Internet, che sia un server di posta, che sia un sito web, una rete *peer to peer*, il nostro indirizzo IP rimane scritto da qualche parte fuori dal nostro controllo. Ed il nostro provider Internet sa sempre, minuto per minuto, chi sta usando quel determinato indirizzo IP, anche se si tratta di una rete che usa il NAT (*Network Address Translation*), come ad esempio tutti i provider che offrono connessioni UMTS/3G, dove l'indirizzo interno della connessione a Internet è differente da quello esterno con cui ci si presenta ai server: i provider *sono obbligati* a mantenere la registrazione delle associazioni fra indirizzo interno ed esterno.

Le guide più gettonate parlano di TOR<sup>38</sup>, di *Open Proxy* e di altre diavolerie date per infallibili. Niente potrebbe essere più sbagliato. Gli *Open Proxy* non sono gratuiti, e quelli che lo sono, o sono troppo lenti per essere utilizzabili, o sono veloci in modo sospetto, e dato che se posso gestire un *Open Proxy* posso ficcare il naso in tutto il traffico che vi passa, si dovrebbero utilizzare solo *Open Proxy* "fidati", ma questo è un ossimoro. Per quanto riguarda TOR, niente e nessuno ci può garantire che alcuni nodi della rete non siano "ostili", vanificando del tutto l'effetto dell'anonimizzazione.

---

38. [http://it.wikipedia.org/wiki/Tor\\_%28software\\_di\\_anonimato%29](http://it.wikipedia.org/wiki/Tor_%28software_di_anonimato%29)



Altri software di anonimizzazione promettono molto più di quanto poi in realtà facciano, senza naturalmente tenere conto del fatto che i nostri amici mentecatti sappiano perfettamente come funzionino.

La maggiore differenza fra i due protocolli è che con BitTorrent la fonte del file può essere in un certo senso “certificata”, per cui non è possibile ricevere un falso, se il file `.torrent` è preso da una fonte affidabile, di solito il distributore originale del file. Questo accade con le distribuzioni Linux, ad esempio: se andiamo a prendere il file `.torrent` dal sito della distribuzione, i file che otterremo saranno senza dubbio quelli voluti. Lo stesso non è possibile con la rete *eD2K*, in quanto non è proprio previsto dal protocollo. Un file può essere identificato in modo pressoché univoco usando l'*hash* di tipo MD4<sup>39</sup> a 128 bit che lo individua, ma non c'è modo di sapere *da dove è partito* il file originale.



### L'*hash* non è infallibile

Esiste una limitazione per gli *hash*, tutti, quale che sia l'algoritmo utilizzato per calcolarli: le cosiddette *collisioni*, ossia due file differenti che presentano lo stesso *hash*. Tale eventualità è dimostrata e dimostrabile matematicamente, ma anche a semplice buonsenso: Un *hash* a 128 bit può identificare univocamente al massimo 2 alla 128ma file differenti, un numero enorme, ma non infinito. Un file lungo 100 byte può avere 2 alla 800ma possibili varianti di contenuto, per cui la maggior parte di questi file avrà *hash* uguali a gruppi, anche con contenuti differenti, proprio a causa delle collisioni.

Questo tipo di attacco è chiamato *collision attack*<sup>40</sup>, e ad oggi non è alla portata di tutti (almeno per i computer disponibili per i normali esseri umani al momento), ossia è complicatissimo creare un file che abbia uno specifico *hash*, a meno di gravi<sup>41</sup> vulnerabilità<sup>42</sup> nell'algoritmo di *hash*.

Con l'algoritmo utilizzato per eMule, denominato MD4, cade completamente la presunta univocità in quanto l'algoritmo stesso soffre di gravissime falle, tanto che è piuttosto facile e veloce (in alcuni articoli, citati dalla pagina su

39. <http://en.wikipedia.org/wiki/MD4>

40. [http://en.wikipedia.org/wiki/Collision\\_attack](http://en.wikipedia.org/wiki/Collision_attack)

41. <http://en.wikipedia.org/wiki/MD5#Security>

42. <http://en.wikipedia.org/wiki/MD4#Security>

Wikipedia, si parla di frazioni di secondo con un normale PC) creare un file che abbia lo stesso *hash* MD4 di un altro.

Naturalmente, escludendo un elemento intenzionale, è statisticamente improbabile che due file con contenuti differenti abbiano *per caso* lo stesso *hash*, per cui l'univocità di una coppia file-hash è praticamente sempre valida. Quindi, a meno di una manipolazione intenzionale di file allo scopo di creare collisioni di *hash*, l'univocità è abbastanza affidabile. Ma noi sappiamo che per chi ha cattive intenzioni questa è tutta manna dal cielo.

Altra differenza è che per distribuire un singolo file con BitTorrent occorre creare un file `.torrent` con all'interno l'indirizzo di un server specifico chiamato *tracker*. Tale server, che deve essere preparato appositamente, fornisce a chi lo richiama l'elenco di chi possiede i file cercati. Quindi non si può semplicemente piazzare un file con un nome "invitante" dentro la cartella dei file in condivisione come succede con eMule.



### Usare solo file `.torrent` presi da fonti affidabili

Con BitTorrent è pressoché impossibile prendere un qualcosa per poi scoprire che si tratta di altro, proprio perché è il file `.torrent` a stabilire cosa viene distribuito e dove trovarlo. Tutto questo vale, naturalmente, se e solo se il file `.torrent` è prelevato da una fonte affidabile e certificata. Ad esempio, se si vuole scaricare una distribuzione Linux via BitTorrent, il file `.torrent` deve essere prelevato dal sito ufficiale della distribuzione. Qualsiasi altro file, prelevato da qualsiasi altra fonte è potenzialmente pericoloso, e potrebbe contenere tutt'altro.

Non occorre precisare, ma lo facciamo comunque, che i vari motori di ricerca per i file `.torrent` in giro per la Rete (Pirate Bay, Mininova, TorrentReactor, ISOHunt, ecc.) *non sono da ritenere fonti affidabili*.

Niente quindi autorizza a pensare che BitTorrent sia *a priori* meno pericoloso di eMule: come su eMule basta scaricare un file affidandosi solo al nome per rimediare tutt'altro, così con BitTorrent basta andare a prendere il file `.torrent` da una fonte non verificata per scaricare immondizia, nella migliore delle ipotesi.

Perciò, è vero che non mi verrebbe mai in mente di scaricare Linux Fedora con eMule, ma non mi sogno neanche di usare un `.torrent` preso da qualsiasi altro posto che non sia il sito del progetto Fedora<sup>43</sup>.

## **Digital divide e pessime idee**

Sotto la definizione di *Digital Divide* va l'attuale situazione della diffusione della *banda larga* per il collegamento a Internet, dove nei grandi centri è abbastanza agevole trovare offerte per la connessione a svariati megabit al secondo a prezzi abbordabili, poche decine di euro al mese al massimo, mentre nei piccoli centri, nelle zone di periferia, lontani insomma dalle grandi città, è spesso impossibile trovare alternative al modem analogico. Questa situazione produce in effetti una profonda divisione fra chi ha a disposizione una connessione stabile e veloce e chi ne ha una lenta e saltuaria.

La Rete, volenti o nolenti, sta diventando un punto di convergenza notevole, sia per le attività ricreative che per quelle commerciali ed economiche. Possedere una connessione lenta significa essere tagliati fuori del tutto, basti pensare che qualsiasi sito web oggi richiede non meno di 500 kilobyte di dati per pagina per essere fruito: con un modem a 56k, nella migliore delle ipotesi, occorrono quasi due minuti per vedere una singola pagina. E' facile capire come chi non possieda una connessione ad almeno 256 kilobit al secondo sia tagliato fuori.

L'avvento della telefonia 3G ha, da un lato, aperto uno spiraglio nella cortina del *digital divide*, dall'altro ha contribuito a rallentare la diffusione di altre tecnologie, all'apparenza meno flessibili, ma in realtà molto più vantaggiose nel lungo termine. Tutti i gestori telefonici hanno in catalogo varie possibilità di connessione a Internet con le oramai famose "chiavette" 3G, anche se certo non possiamo parlare di soluzioni propriamente economiche.

Per lo più si tratta di contratti con limiti a tempo o a volume di traffico, ed in entrambi i casi le "eccedenze" sono a caro prezzo. Per come è la tecnologia è anche difficile tenerli sotto controllo, i limiti. Inoltre, la convenienza cambia in funzione del tipo di uso che si fa di Internet in generale.

---

43. <http://fedoraproject.org/>

Usare uno di questi contratti per il *peer to peer* è una *pessima* idea. Prima di tutto, ricordiamo quanto abbiamo scritto poco sopra: ogni protocollo di *peer to peer* prevede l'immediata redistribuzione di ogni singolo segmento di file ricevuto: questo vuol dire che per scaricare un file da 100 megabyte il software di *peer to peer* ne potrebbe distribuire altrettanti, come minimo. In tutti i contratti di tipo 3G viene conteggiato il traffico in generale, non il solo download, quindi se nello scaricare un file da 100 megabyte il programma ne distribuisce altrettanti, verranno conteggiati 200 megabyte.

Se poi, terminato il download, lasciamo attivo il programma di *peer to peer*, questi continuerà a inviare porzioni di file a chiunque le richieda, con ulteriore aggravio di traffico.

Nell'agosto 2010, l'Autorità per le Garanzie nelle Comunicazioni ha disposto<sup>44</sup> che i fornitori attivino dei blocchi automatici della connessione al superamento del tetto contrattuale, sia esso di traffico che di tempo, per evitare il ripetersi di situazioni più che paradossali, in cui per scaricare un film via *peer to peer* l'incauto utente possa vedersi addebitare in bolletta cifre tali che sarebbe costato meno prenotare l'intera sala di proiezione solo per sé.

Quanto detto vale sia per eMule che per BitTorrent. Inoltre c'è un problema di connettività alla base: in tutti questi contratti, l'indirizzo IP fornito dal gestore al momento della connessione è un indirizzo non pubblico, sottoposto a NAT (*Network Address Translation*), sicuramente di una rete dietro un firewall, senza eccezioni. Non c'è quindi alcun modo di ottenere il cosiddetto "ID alto" tanto cercato in eMule per avere download più rapidi.

Per questi motivi, in generale, pensare di aggirare il *digital divide* con un contratto 3G non è una idea particolarmente brillante. Naturalmente questo vale solo per chi ha intenzione di fare *peer to peer*. Se intendiamo partecipare a qualche *social network*, se vogliamo gestire un sito web nostro o fruire dei tantissimi servizi in Rete, tutto questo non vale: anzi, un contratto per una connessione 3G può effettivamente abbattere il muro del *digital divide*.

---

44. <http://www.agcom.it/default.aspx?DocID=4671>

## La tecnologia è neutra

Concludiamo qui questa parte dedicata al *file sharing*. Resta soltanto da chiarire un possibile equivoco, se ancora non lo è: il *peer to peer* non è da condannare *tout-court*, al contrario. Le mie distribuzioni Linux sono regolarmente e costantemente scaricate via BitTorrent, e mi premuro di togliere i file dalla condivisione solo dopo che ho contribuito per almeno il doppio dei byte che ho scaricato. Ma in questo caso sto usando il canale di distribuzione scelto e consigliato da chi produce la distribuzione Linux che uso, e non sto facendo un danno, ma sto contribuendo a ridurre le spese di gestione dei server e del collegamento Internet di chi lavora per mettermi a disposizione la mia versione di Linux preferita, o il mio programma Open Source preferito.

Se invece, sistematicamente, tutto quello che installo sul computer, quello che ascolto, quello che vedo e quello che leggo (ci sono anche i libri) è preso da un circuito *peer to peer*, la responsabilità è solo mia, non del programma o della tecnologia.

Vi sono esperimenti di condivisione volontaria di contenuti, tesi sia ad aggirare le limitazioni imposte dall'industria cinematografica e discografica in generale, sia a permettere l'emergere di artisti che non vedrebbero mai un qualsiasi riconoscimento, perché troppo "di nicchia" per piacere alla massa. Organizzazioni come Creative Commons<sup>45</sup> ed esperimenti come Magnatune<sup>46</sup>, Jamendo<sup>47</sup>, Vodo<sup>48</sup>, dimostrano che qualcuno sta ripensando i dogmi della distribuzione dei contenuti multimediali.

Degno di nota è l'esperimento condotto nel 2007 dal noto gruppo musicale dei Radiohead. Nell'ottobre del 2007 il gruppo offrì con la formula del "download ad offerta"<sup>49</sup> l'ultimo disco. L'offerta non aveva limite inferiore, per cui era possibile offrire anche zero, cioè non pagare nulla. Il successivo 3 dicembre il disco venne messo in vendita in una confezione lusso, con le versioni in vinile, oltre al CD, ed un ulteriore CD con alcuni brani inediti, al prezzo di 80 dollari.

---

45. <http://www.creativecommons.it/>

46. <http://magnatune.com/>

47. <http://www.jamendo.com/it/>

48. <http://vodo.net/>

49. <http://attivissimo.blogspot.com/2007/10/nuovo-album-radiohead-il-prezzo-lo.html>

Secondo la società a cui venne commissionato lo studio di verifica (com-Score), il 38% delle persone pagò<sup>50</sup> per avere qualcosa che era disponibile anche gratuitamente, e di questi quasi la metà pagò più di otto dollari. Non solo, la stessa società ha ipotizzato che il mettere a disposizione i brani gratuitamente potrebbe avere un effetto benefico sulle vendite tradizionali, visto l'aumentato il numero di persone venute a conoscenza del gruppo grazie alla versione "gratuita". Al momento in cui scrivo questo non è stato verificato, anche se verosimile.

Quindi, la Rete e le tecnologie mettono a disposizione nuove forme di comunicazione e di diffusione dei prodotti dell'ingegno umano in tutte le sue incarnazioni. Invece di rimanere attaccati ai vecchi modelli, sempre più a rischio anacronismo, sarebbe giunto il momento di cominciare a ripensare alcune strategie, anche da parte di noi utenti e fruitori.

---

50. [http://www.comscore.com/Press\\_Events/Press\\_Releases/2007/11/Radiohead\\_Downloads](http://www.comscore.com/Press_Events/Press_Releases/2007/11/Radiohead_Downloads)

## Capitolo 8. Nebbiaware

Sempre nella convinzione che su Internet vi sia tutto quello che serve, senza tenere conto che vi è anche molto che non serve e moltissimo di cui si vorrebbe poter fare a meno, qualsiasi esigenza di software sorga, ci si rivolge al proprio motore di ricerca preferito, con risultati non sempre corrispondenti alle aspettative.

Forti di questa realtà, i nostri amici mentecatti hanno immediatamente approntato innumerevoli siti web che offrono tutte le possibili meraviglie software tecnologicamente avanzate per soddisfare primariamente una esigenza vitale: riempire il loro portafogli e svuotare il nostro.

La strategia migliore si basa principalmente sulla grande ignoranza e superficialità della maggior parte di noi utenti, che operiamo principalmente con la tecnica scarico-installo-provo-cancello, a cervello spento.

Come purtroppo ho già detto e ripeterò per tutto il libro, non ci sono magie tecnologiche o ricette (leggi incantesimi) che ci mettano al sicuro. L'unica risorsa è la conoscenza, quella vera.

### Scaricami, SONO GRATIS!!!

Qualsiasi sia la nostra esigenza, esplicitata con poche parole chiave nella casella di ricerca di Google, probabilmente troveremo qualcosa che fa al caso nostro. Se però includiamo alcune parole particolari nei termini di ricerca otterremo l'esatto contrario di quello che i termini intendono, anche se non lo scopriremo immediatamente, ma dopo un po'.

Le paroline magiche sono “download”, “gratis” e “free”, con tutte le varianti e declinazioni.

Ogni software, ogni possibile prodotto disponibile in forma digitale è passibile di questo tipo di inganno, anche prodotti effettivamente gratuiti e di libera distribuzione possono essere spacciati con questo metodo. La tecnica a grandi linee può essere riassunta in questi passi:

1. I risultati della ricerca restituiscono nei primi risultati uno o più siti web confezionati appositamente che offrono proprio quello che le parole chiave da noi inserite indicano (Figura 8-3). Oppure, nei riquadri dedicati ai link sponsorizzati appaiono dei siti che offrono apparentemente quello che cerchiamo (Figura 8-1 e Figura 8-2). Oppure, visitando uno dei siti reperiti nella ricerca, uno dei riquadri di pubblicità, oramai onnipresenti, mostra un prodotto che sembra proprio fare al caso nostro. In queste ultime due ipotesi vi è sempre evidente l'indicazione che il tutto è gratuito.
2. Il sito appare graficamente ben fatto e curato, con confortanti e rassicuranti immagini, "bollini" di varie organizzazioni di certificazione e di compatibilità, frasi entusiastiche di utenti soddisfatti. Spesso è anche nella nostra lingua, e in molte altre, come testimonia la sfilza di bandiere per le varie versioni del sito. In bella mostra c'è un pulsante enorme, coloratissimo, lampeggiante, animato, che invita a scaricare.
3. In pochi secondi il download è fatto, senza altre formalità: niente registrazione, niente richiesta di indirizzi e-mail, niente iscrizioni a *newsletter* o altri vincoli di alcun genere.

Nelle figure che seguono vi sono degli esempi abbastanza comuni sia dei risultati delle ricerche che della pubblicità contenuta nei siti "innocui".



Figura 8-1. Metà dei link sponsorizzati

<input type="text" value="velocizzare computer gratis"/> <input type="button" value="Cerca"/>	
Circa 85.800 risultati (0,25 secondi) <span style="float: right;">Ricerca avanzata</span>	
<p><b>Velocizzare Computer Gratis *</b></p> <p>Uniblue.com/<a href="#">Velocizza_PC</a> Rileva ed Elimina Errori per un PC più Veloce. Scarica Software <b>Gratis</b></p>	<p>Link sponsorizzati</p> <p><b>Come Velocizzo PC Lento ? *</b></p> <p>FIXIO <b>Velocizza</b> il PC in 2 clic. Download - Scansione PC e <b>Gratis!</b> FIXIO-PC-Cleaner.it</p> <p><b>Velocizza il tuo PC</b></p> <p>Scansione gratuita degli errori qui SLOW-PCfighter <b>velocizza</b> il tuo PC <a href="#">www.spamfighter.com/slow-pcfighter</a></p> <p><b>Download Velocizza PC</b></p> <p>Ottimizza il registro del sistema Migliora le prestazioni del pc <a href="#">avs4you.com/AVS_Registry_Cleaner</a></p> <p><b>Velocizzare PC Gratis</b></p> <p>Tutto di <b>Velocizzare PC Gratis</b> <b>Velocizzare PC Gratis</b> - Adesso su Ask Ask.com</p> <p><b>Velocizza il tuo PC *</b></p> <p>Con lo strumento di Tuning No.1 Avvia ora la scansione gratuita! <a href="#">pcpitstop.com/velocizzare_windows</a></p>
<p><b>Download velocizzare il pc gratis</b></p> <p>Download <b>velocizzare il pc gratis</b> - VistaMizer 3.6.0.0: Quando Windows XP si fece Vista, e tanti altri download. <a href="#">www.softonic.it</a> » Personalizza il tuo PC - Copia cache - Simili</p> <p><a href="#">Download migliore programma per velocizzare pc free italiano</a></p> <p>Download gratuito migliore programma per <b>velocizzare pc free italiano</b> - TuneUp Utilities 2010 9.0.4200: Ripara, ottimizza e migliora il funzionamento del ... <a href="#">www.softonic.it</a> » Personalizza il tuo PC - Copia cache - Simili</p> <p><a href="#">Mostra altri risultati da www.softonic.it</a></p> <p><b>Come velocizzare il vostro pc : Mondo Gratis</b></p> <p>29 apr 2009 ... chi non vorrebbe il proprio pc sempre più veloce? si installano aggiornamenti di sistema, programmi per ottimizzare il sistema ecc ecc. <a href="#">mondogratis.myblog.it/.../come-velocizzare-il-vostro-pc.html</a> - Copia cache - Simili</p> <p><b>Velocizzare PC Gratis Con Il Programma Quad Cleaner   eDentity Coach *</b></p> <p>13 giu 2009 ... Stai cercando un programma <b>gratis</b> per <b>velocizzare</b> il PC ? Allora ti segnaliamo Quad Cleaner, un'applicazione in grado di massimizzare le ... <a href="#">www.edentitycoach.com/.../velocizzare-pc-gratis-con-il-programma-quad-cleaner/</a> - Simili</p>	

Figura 8-2. Termini diversi, anche peggio

velocizzare pc gratis

Circa 53.800 risultati (0,05 secondi) [Ricerca avanzata](#)

**Velocizzare PC Gratis** Link sponsorizzati  
[Uniblue.com/Velocizza\\_PC](#) Scarica Software **Gratis** Rileva ed Elimina Errori per un **PC** più Veloce.

**Velocizza il tuo PC**  
[PC-Fix-2010.com](#) Ripara, Correggi il tuo **PC** in 2 min Scarica Adesso Gratuitamente!

**Velocizza il tuo PC**  
[www.spamfighter.com/slow-pcfighter](#) Scansione gratuita degli errori qui SLOW-PCfighter **velocizza** il tuo **PC**

**Programmi per velocizzare Windows XP, Vista e Windows 7** ☆  
**Velocizzare** Windows, tweaking, ottimizzare sistema. ... INTERNET **GRATIS** - Connessione gratuita e velocissima ... spezzare e unire file molto grandi, manager dei processi del sistema e controllo della sequenza di avvio del **pc** (startup). ...  
[www.programmifree.com/.../ottimizzazione-sistema.htm](#) - Copia cache - Simili

**Come velocizzare il vostro pc : Mondo Gratis** ☆  
 29 apr 2009 ... chi non vorrebbe il proprio **pc** sempre più veloce? si installano aggiornamenti di sistema, programmi per ottimizzare il sistema ecc ecc ecc.  
[mondogratis.myblog.it/.../come-velocizzare-il-vostro-pc.html](#) - Copia cache - Simili

**Download velocizzare il pc gratis** ☆  
 Download **velocizzare il pc gratis** - VistaMizer 3.6.0.0: Quando Windows XP si fece Vista, e tanti altri download.  
[www.softonic.it](#) > Personalizza il tuo PC - Copia cache - Simili

**Download migliore programma per velocizzare pc free italiano** ☆  
 Download gratuito migliore programma per **velocizzare pc** free italiano - TuneUp Utilities 2010 9.0.4200: Ripara, ottimizza e migliora il funzionamento del ...  
[www.softonic.it](#) > Personalizza il tuo PC - Copia cache - Simili  
[+](#) Mostra altri risultati da [www.softonic.it](#)

**Velocizzare PC Gratis Con Il Programma Quad Cleaner | eDentity Coach** ☆  
 13 giu 2009 ... Stai cercando un programma **gratis** per **velocizzare** il **PC** ? Allora ti segnaliamo Quad Cleaner, un'applicazione in grado di massimizzare le ...  
[www.edentitycoach.com/.../velocizzare-pc-gratis-con-il-programma-quad-](#)

Link sponsorizzati

**Velocizzazione del PC**  
 Sia desktop che notebook - TuneUp Utilities **velocizza** ogni **PC!**  
[www.tune-up.it/PC\\_Velocizzazione](#)

**Come Velocizzo PC Lento ?**  
 FIXIO **Velocizza** il **PC** in 2 clic. Download, fai Scansione **PC Gratis!**  
[FIXIO-PC-Cleaner.it](#)

**Download Velocizza PC**  
 Ottimizza il registro del sistema Migliora le prestazioni del **pc**  
[avs4you.com/AVS\\_Registry\\_Cleaner](#)

**Velocizzare PC Gratis**  
 Tutto di **Velocizzare PC Gratis** **Velocizzare PC Gratis** - Adesso su Ask!  
[Ask.com](#)

**Velocizzare Windows**  
 Effetua ora una scansione del sistema gratuita con **PC Pitstop**  
[pcpitstop.com/velocita](#)

[Visualizza la tuo annuncio qui »](#)

**Figura 8-3. eMule: quelli con l'asterisco sono fasulli**

emule gratis
Cerca

Circa 1.340.000 risultati (0,05 secondi) Ricerca avanzata

[eMule - eMule Plus - download eMule gratis \\*](#)  
eMule, scarica **eMule gratis**. eMule è fra i migliori client P2P. Sono molti gli sviluppatori che contribuiscono al progetto, ragion per cui la rete diventa ...  
[0.49c](#) - [0.49b](#) - [0.49a](#) - [0.48a](#)  
[www.emule.com/it/](#) - [Copia cache](#) - [Simili](#)

[eMule 0.49b gratis \\*](#)  
1 ago 2008 ... **eMule 0.49b** migliora la velocità e l'affidabilità, per continuare ad essere la migliore applicazione P2P.  
[www.emule.com/it/emule-049b.php](#) - [Copia cache](#) - [Simili](#)  
+ Mostra altri risultati da [www.emule.com](#)

[Emule - Tutto Gratis](#)  
**eMule** e tutte le mod da scaricare **gratis**, come **eMule Plus** o **eMule Adunanza**, oltre che versioni specifiche di **eMule** per Vista. Inoltre guide, trucchi, lista ...  
[www.tuttogratitis.it](#) > ... > Internet > Software Peer To Peer - [Copia cache](#) - [Simili](#)

[Download emule 0.49c gratis : download gratuito](#)  
download **emule 0.49c gratis** : download gratuito - **eMule** a 0.50: Scarica file grazie al mulo più famoso della Rete, e tanti altri download.  
[www.softonic.it](#) > Internet > Download e upload - [Copia cache](#) - [Simili](#)

[Download Emule Gratis, scarica emule italiano, \\*](#)  
Emule è il più famoso e diffuso peer to peer, il software per scambiarsi file: musica, video, immagini programmi e videogiochi. Download **Emule gratis**.  
[downloademulegratis.com/](#) - [Copia cache](#)

[Scarica eMule Gratis \\*](#)  
Scarica eMule v5.0a. Scarica **eMule Gratis**. Licenza: Gratis. Lingua: Italiano Inglese Francese Spagnolo Tedesco. Voto: Download totali: 4727200 ...  
[www.emulegratis.net/](#) - [Copia cache](#) - [Simili](#)

[Download eMule italiano gratis, Scarica eMule gratis Freeware](#)  
25 apr 2010 ... NUOVO Download! Scarica **gratis eMule** in italiano, **eMule** download.  
[www.xnavigation.net/view/..emule/download.html](#) - [Copia cache](#) - [Simili](#)

[Download - Scarica eMule gratis](#)  
Download - Scarica **eMule gratis**. EMULE 0.48a È un programma libero P2P (ovvero da utente a utente), per la condivisione di file che utilizza la rete ...  
[downloads.phpnuke.org/it/download..EMULE.htm](#) - [Copia cache](#)

[eMule-Project.net - Sito ufficiale di eMule, Downloads, Help, Docu ...](#)  
**eMule** è completamente **gratis**. **eMule** è anche completamente libero da ogni Adware, Spyware, etc. Noi facciamo tutto ciò per divertimento e per conoscere, ...  
[www.emule-project.net/home/pert/general.cgi?!](#) - [Copia cache](#) - [Simili](#)

Link sponsorizzati

[Scarica Versione Italiana \\*](#)  
Download la Versione Gratuita del programma più usato. 100% **Gratis!**  
[www.software-net.com/OfficialEMule](#)

[Emule Italiano Gratis](#)  
Tutto di **Emule** Italiano **Gratis**  
**Emule** Italiano **Gratis** - Adesso su Ask! Ask.com

[Visualizza il tuo annuncio qui >](#)

**Figura 8-4. La pubblicità in uno dei siti in Figura 8-1**

PUBBLICITA':

**Il Tuo PC è troppo Lento?** [PC-Fix-2010.com](http://PC-Fix-2010.com)  
Correggi, Ripara Errori PC in 2 min Scarica  
Adesso Gratuitamente!

**Pc Lento?** [www.Ascentive.com/it](http://www.Ascentive.com/it)  
Rileva ed Elimina Gli Errori del PC Avvia  
Scansione Gratuita!

**Sicurezza Gratis Computer** [www.Alice.it/Alice-Tot](http://www.Alice.it/Alice-Tot)  
Difendi il PC dagli attacchi con Alice Total Security!  
Gratis 6 Mesi

Figura 8-5. Pubblicità in un sito che parla di un altro “velocizzatore”

In omaggio, anc

## Come Ottimizzare e Velocizzare il PC

17 settembre 2010 - Fonte: <http://www.becomegeek.com>

Ottimizza e velocizza il tuo PC in pochi clic

**Registry Mum** è un programma in grado di:

- Individuare, diagnosticare e riparare tutti i tipi di problema del PC
- Velocizzare l'avvio di Windows e le performance delle vostre applicazioni
- Individuare facilmente e rimuovere in modo sicuro i file inutili

Caratteristiche del programma:

- Ottimizza automaticamente le impostazioni del registro per impedire crash ...

[Leggi il seguito »](#) [Annunci Google](#) [PC Computer](#) [PC Einschalten](#) [Occasioni PC](#) [Windows XP PC](#)

Inserito in [accelerare pc](#), [BecomeGeek.com](#), [Come Ottimizzare e Velocizzare il PC](#), [computer](#), [ottimizzare pc](#), [velocizzare pc](#) Nessun commento »

**il PC è Lento, si Blocca, ha Errori?**  
FIXIO Ripara il Registro di Windows e il tuo PC Torna COME NUOVO!  
FIXIO-PC-Cleaner.it [Annunci Google](#)

GRATIS: Scan Totale PC  
**DOWNLOAD ora!**

**Smart PC: Ottimizzare e Velocizzare in 7 step il tuo PC**

2 settembre 2010 - Fonte: <http://unitragazzi.altervista.org>

[Procedura guidata di Smart PC Pro](#)

**PC Lento, si Blocca, ha Errori ?**

**FIXIO**  
PC Cleaner

**Ripara il Registro di Windows, il PC Torna COME NUOVO**

GRATIS: Scansione Totale del tuo PC  
**DOWNLOAD ora!**

Compatibile con  
Windows 7, Vista, XP

Certificato per Windows Vista™

Windows 7, Vista, XP

Da questo momento in poi la vera natura di quello che abbiamo scaricato può rivelarsi, e può succedere in una delle varie fasi:

- al momento dell'installazione viene chiesta una procedura di attivazione, o l'installazione di componenti aggiuntivi non evidenziati in precedenza
- dopo l'installazione, per avviare il programma, viene chiesta una chiave di attivazione
- dopo aver avviato il programma, a seguito di una qualche operazione ci viene notificato un problema grave nel nostro computer che può essere risolto unicamente sbloccando alcune funzionalità o usando la versione completa del programma, entrambe disponibili solo dietro pagamento di una somma non trascurabile di denaro

Tutte queste varianti nascondono una sola strategia: spillare soldi agli utenti.

Vediamo qualche esempio pratico, per capire fino a che punto dobbiamo diffidare delle cose gratuite che tali non sono.

## **Ecco eMule Free e eMule Plus**

Nel capitolo sul *peer to peer* lo abbiamo nominato spesso, e naturalmente non poteva non essere preso di mira. Vari siti con nomi verosimili appaiono nelle pubblicità di Google o nei link sponsorizzati a seguito di una ricerca. Qui si fa conto della mancanza di conoscenza dell'utente sul fatto che è un software Open Source di cui è disponibile il sorgente, e che è effettivamente gratuito. Il sito da cui scaricarlo è [www.emule-project.net](http://www.emule-project.net) (vedi Figura 8-6), con l'interfaccia utente in varie lingue.

Figura 8-6. Il sito ufficiale di eMule



In effetti il sito non è molto accattivante, e il link al download non è immediatamente visibile.

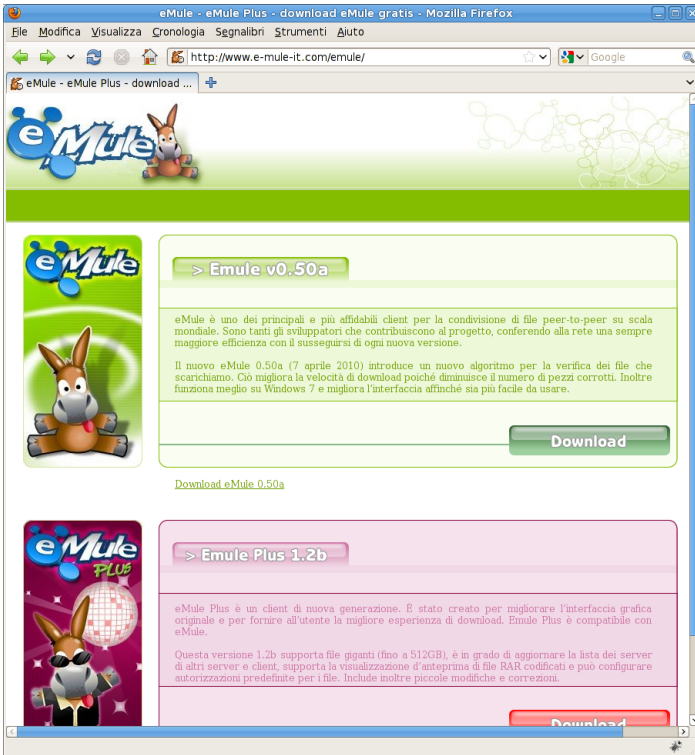
Figura 8-7. Il sito ufficiale di Emule Plus



Quello di *eMule Plus*, [emuleplus.info](http://emuleplus.info), una versione estesa con alcune delle funzioni di verifica della affidabilità dei file, più altre modifiche minori, è graficamente appena più colorato (Figura 8-7).

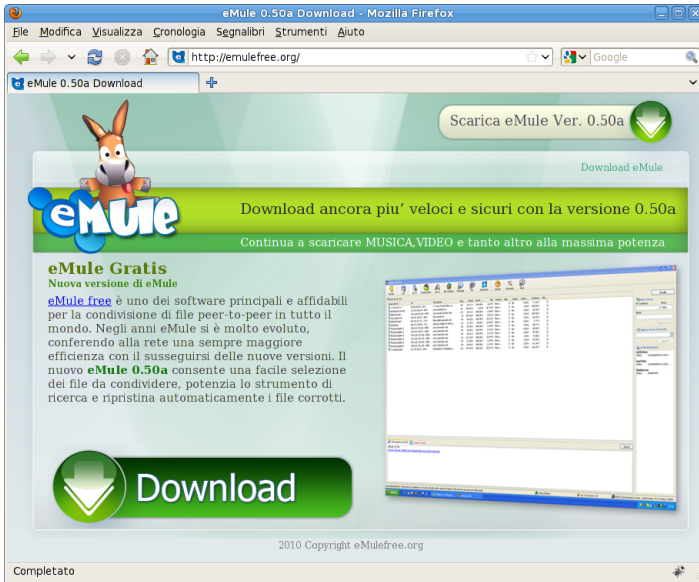


Figura 8-8. Un falso sito di eMule



Usando le parole chiave *emule gratis italiano* i primi risultati portano a siti che *non hanno niente a che vedere con eMule*. Nel senso che apparentemente vi si possono scaricare le ultime versioni di eMule, ma sono tutte differenti da quelle originali. Il file della versione “regolare” distribuita da questi siti è mediamente il 40% più grande di quello della versione ufficiale, mentre il file della versione *Plus* è di pochi kilobyte, segno che in realtà la gran parte del software sarà scaricata a nostra insaputa da chissà dove.

Figura 8-9. Un altro, solo con eMule



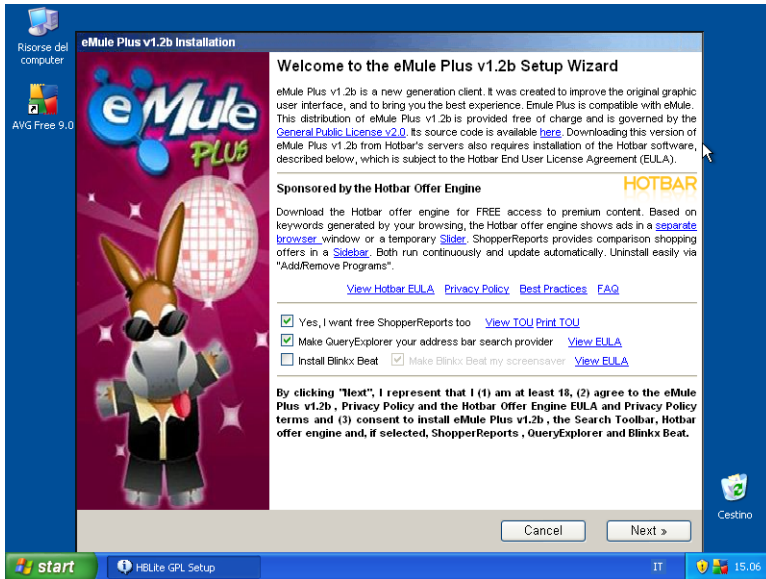
Guardando i siti fasulli, non si può dire che la grafica non sia accattivante, con i pulsanti per scaricare il software immediatamente visibili, a differenza del sito originale.

Figura 8-10. Un altro, leggermente differente



Usando la collaudata tecnica della macchina virtuale sacrificale, installiamo eMule Plus preso da uno di questi siti, e vediamo che siamo obbligati ad installare anche altra roba, assolutamente inutile, se non dannosa, che non è possibile rifiutare: spacciati per accesso a contenuti selezionati e offerte irripetibili, abbiamo ogni genere di *adware*, oltre a estensioni di Internet Explorer, tutti pronti a rendere qualsiasi attività al computer un inferno di *popup*, messaggi, finestre che si aprono e chiudono, senza parlare della possibilità per questi intrusi di collezionare a piacimento dati e informazioni su di noi a nostra insaputa.

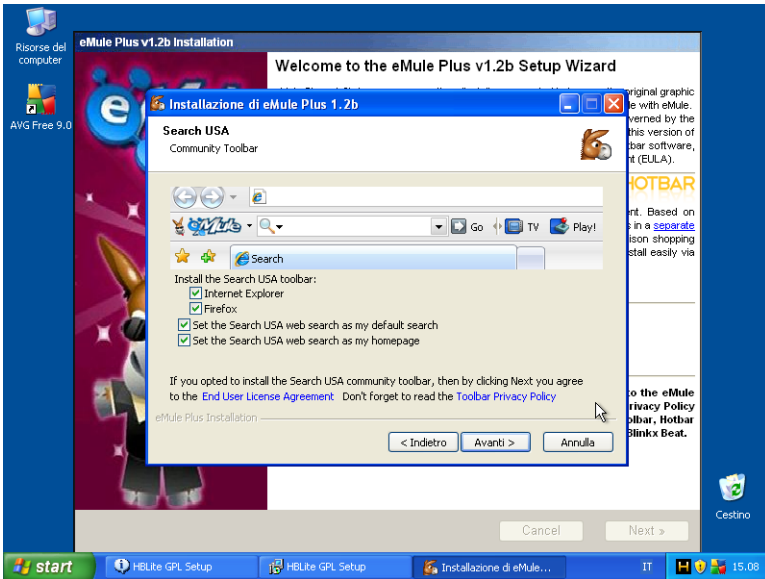
Figura 8-11. Il solito secchio d'acqua per la goccia d'olio



Come possiamo notare dalle immagini, nella macchina virtuale c'è installato un antivirus, che non è mai intervenuto a segnalare alcunché. In effetti, questi software non vengono classificati come malware, in quanto *non fanno nulla che l'utente non abbia autorizzato installando*: nella licenza e nelle schermate di installazione c'è scritto tutto quello che faranno i vari software ma, alzi la mano chi non è d'accordo, il numero di licenze lette da noi utenti globalmente in tutto il mondo ogni anno è zero. Si clicca su **Accetto** e via.

Si badi bene che *nessun antivirus* segnala come malware questi software, perché tecnicamente *non lo sono*, tanto che i pochi che lo fanno (tre su quarantadue) segnalano chiaramente che *non è un virus* ma un possibile programma di pubblicità. Peccato che però il nostro computer dopo assomigli di più ad un mercato rionale, e ci sia qualcuno che si impicci costantemente nei fatti nostri.

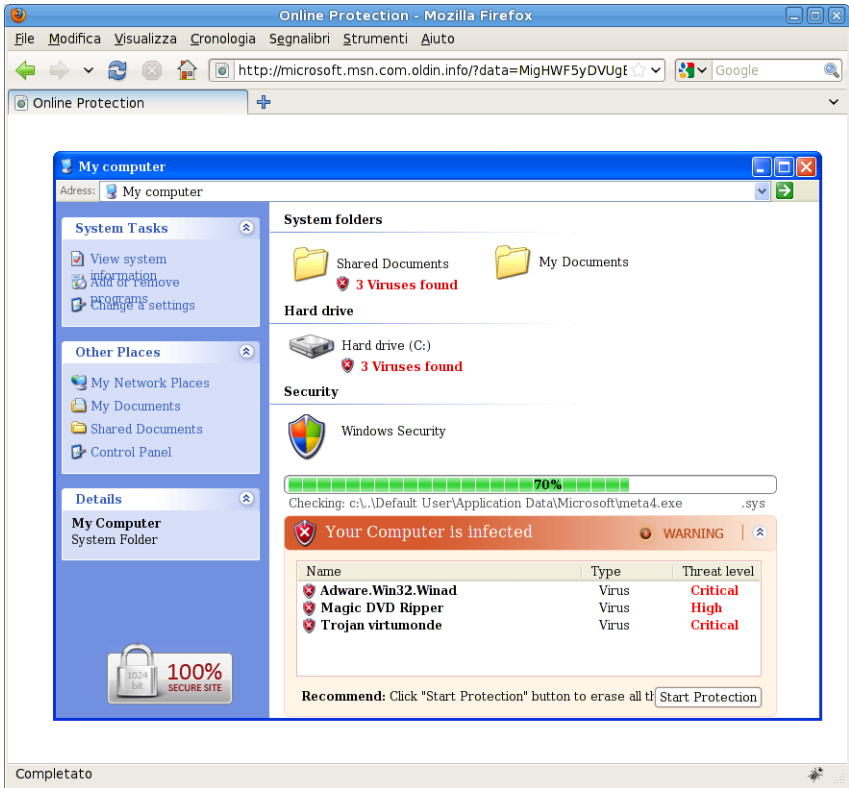
Figura 8-12. L'ennesima toolbar



## Disinfetta, PRESTO!

Capita, navigando in siti insospettabili o in uno di quelli visitati abitualmente, che si venga improvvisamente dirottati su un altro sito, che niente ha a che vedere con quello dove intendevamo andare (vedremo più avanti come possa succedere): in una frazione di secondo, appare una interfaccia simile a quella di molti antivirus, o identica ad un pannello del Centro di Sicurezza di Windows, con quella che sembra una scansione in corso, seguita a brevissima distanza da un allarmante messaggio che ci avverte di avere il computer pieno di terrificanti pestilenze.

Figura 8-13. Un esempio di falso scanner

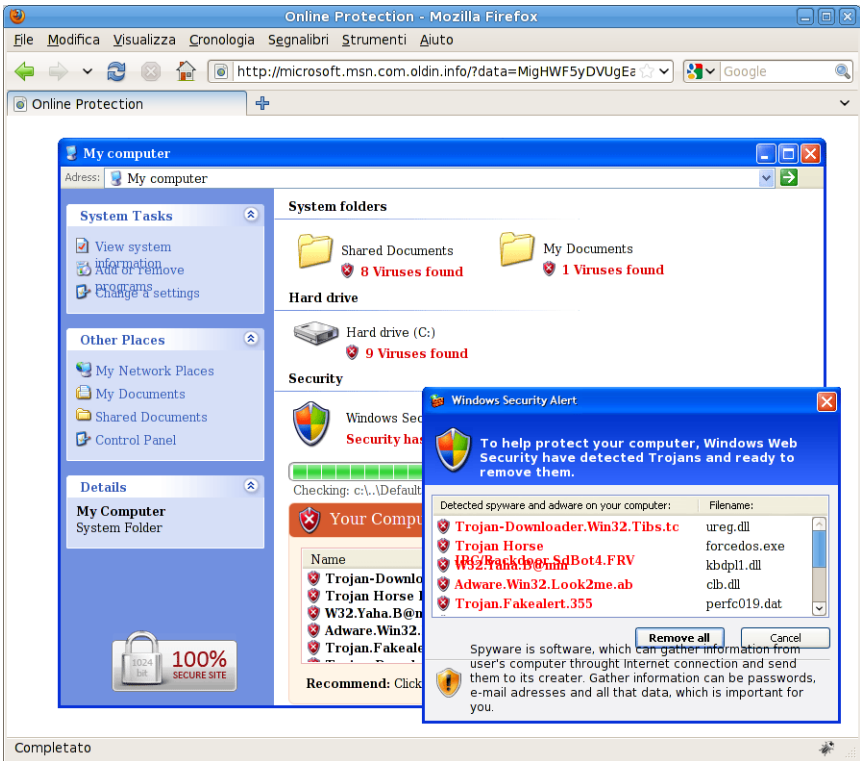


Queste immagini, che a prima vista sembrano catturate da un computer con Windows XP o Windows 7, sono prese da quello che uso per scrivere il libro che state leggendo. Il sistema operativo da me usato abitualmente è Fedora Linux<sup>1</sup>, con cui ho scritto anche il libro precedente. Il browser è Firefox, e le immagini che vedete sono tutte catturate dalla finestra di Firefox in Fedora. Il fatto che *sembrino* appartenere a Windows ci deve far riflettere su quanta cura è posta nel

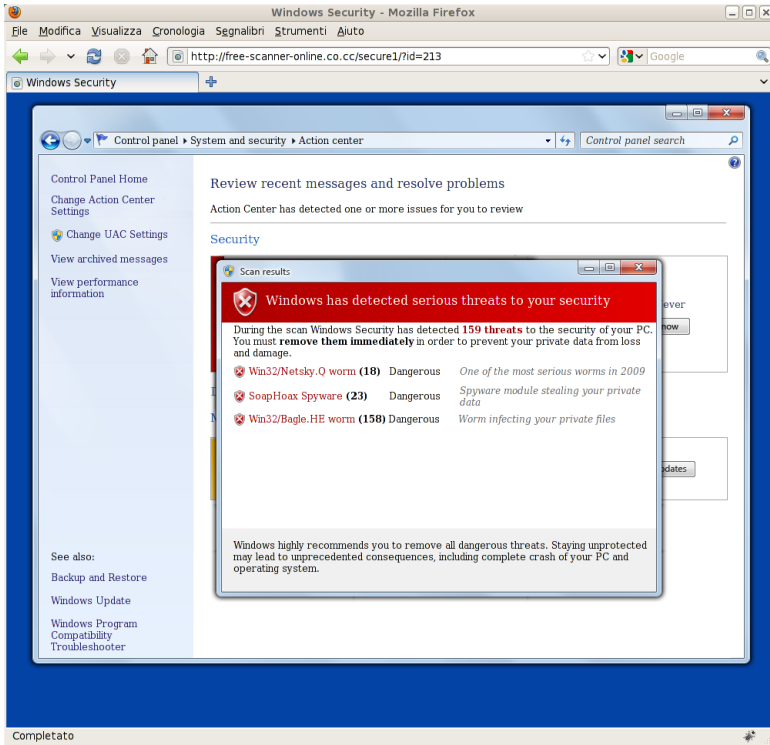
1. <http://fedoraproject.org/>

mimare interfacce e comportamenti noti del nostro sistema operativo, allo scopo di ingannare l'utente facendogli credere che sia un avviso regolare, anche se mai visto prima.

**Figura 8-14. Notare la somiglianza con la grafica di Windows**



**Figura 8-15. Sono 159 o 18+23+158? Come fanno a starci tutti?**



In Figura 8-15 un esempio piuttosto notevole: è identico in tutto e per tutto all'interfaccia del Centro di Sicurezza di Windows 7, ma è dentro Firefox su Fedora Linux (che non ha quel tipo di grafica delle finestre). Dopo questa finestra appare un messaggio che invita a scaricare un non meglio specificato aggiornamento per Windows capace di rimuovere tutti gli intrusi trovati.

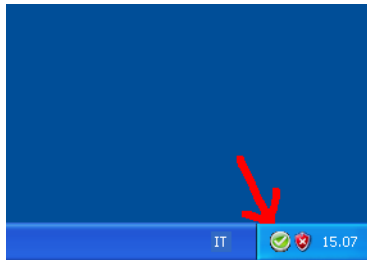
Inutile dire che tale aggiornamento è del tutto fasullo e nasconde varie sorprese. Per prima cosa, di qualsiasi cosa si tratti, si avvia e si installa anche da un utente non amministratore: questo dovrebbe in teoria renderlo meno dannoso,



non potendo opporsi ad un intervento di un utente amministratore che ne operi la rimozione. In realtà, dovrebbe farci riflettere abbastanza, visto che un aggiornamento di sistema operativo deve *necessariamente* essere installato da un account amministrativo. Dato che lo scopo vero è un altro, non certo l'aggiornamento, possiamo star certi che per portare a termine il suo compito si accontenti di essere lanciato da chiunque.

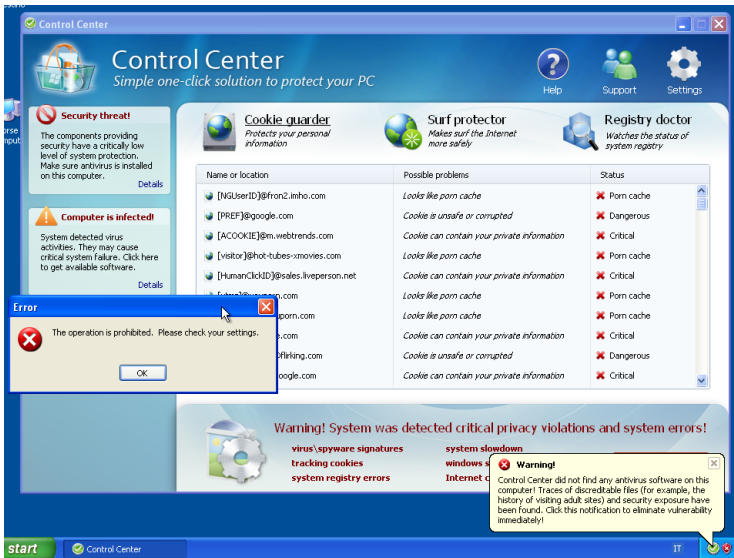
L'installazione è velocissima e silenziosa. Appare soltanto una piccola icona vicino l'orologio, in basso a destra, di colore verde ad indicare che è tutto in ordine.

**Figura 8-16. Dopo l'installazione, solo un pallino verde**



Al primo riavvio o al primo clic del mouse sopra l'icona si rivela la trappola: appare un centro di controllo tuttofare, dall'antivirus al controllo del Registro di Windows, al controllo della cache del browser. Naturalmente è un disastro su tutta la linea: centinaia di avvisi critici, segnalazioni di navigazione in siti poco raccomandabili, virus, malware, errori nel registro. Periodicamente salta fuori una notifica che ricorda gli innumerevoli problemi del computer, e *non si può chiudere il pannello*, come conferma anche il messaggio di avviso (Figura 8-17). Solo andando nelle impostazioni, dopo aver abilitato una voce che dice pressappoco: "Permettere l'avvio insicuro di Windows", si riesce a chiudere il pannello di avviso.

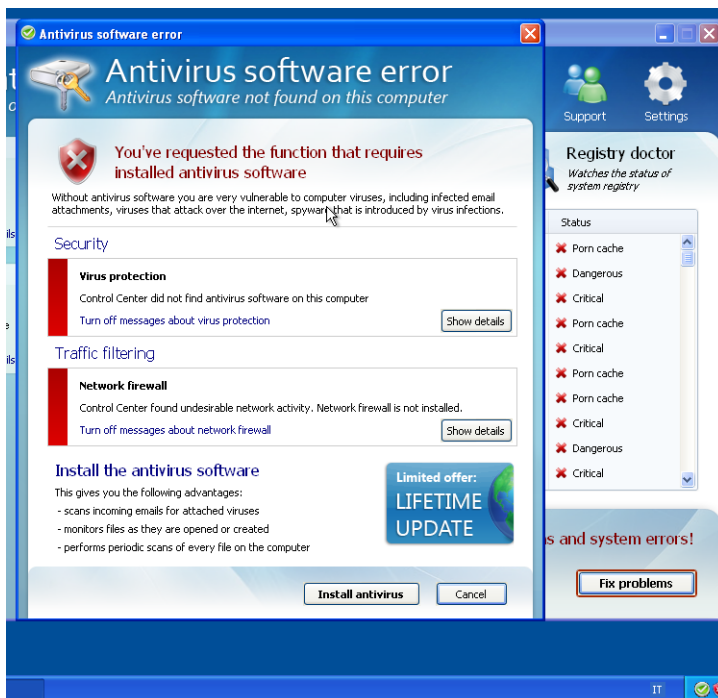
Figura 8-17. Inutilizzabile, per via dell'antivirus fasullo però



Tutto ciò in un computer appena installato, che *non ha mai navigato in Internet*, in quanto il file è stato scaricato da Linux e poi copiato nella macchina virtuale, proprio per evitare interferenze e inquinamento dell'ambiente di analisi.

Sotto la notifica, c'è un bel pulsante col bordo lampeggiante che dice Fix problems (sistema i problemi). Cliccandolo abbiamo una finestra che riepiloga i problemi del nostro computer (che in effetti non aveva un antivirus installato), e ci propone di installare l'antivirus, con tanto di aggiornamenti a vita.

**Figura 8-18. In effetti un antivirus mancava...**



La finestra successiva ci avverte che la nostra chiave di attivazione è purtroppo scaduta, tre mesi prima dell'installazione, e che occorre acquistarne una nuova (Figura 8-19).

Figura 8-19. Veramente non ho alcuna chiave, io

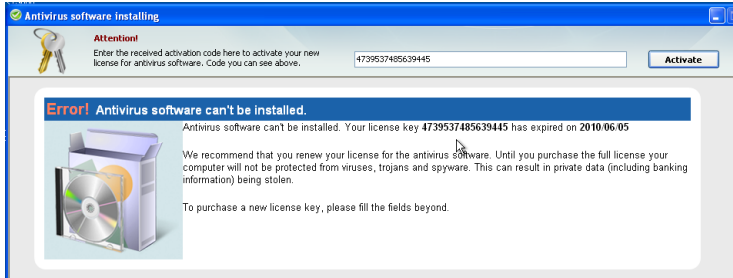
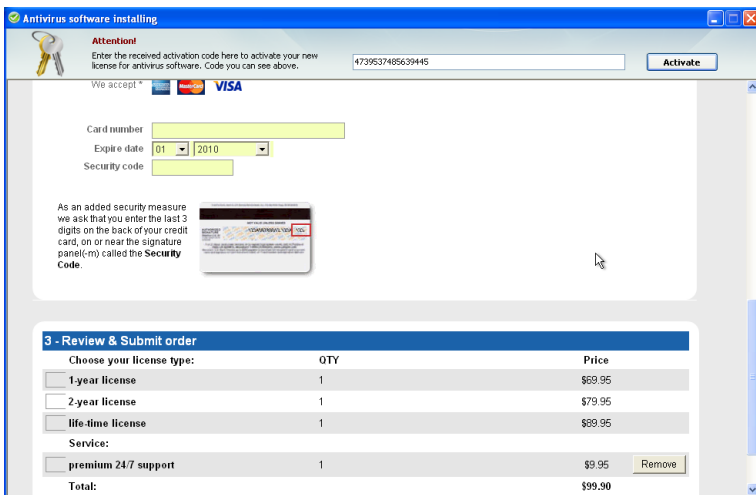


Figura 8-20. Finalmente, non ci speravo più



In fondo alla pagina esce finalmente il modulo per pagare la nuova licenza, per la modica cifra di 99 dollari, però, per fortuna, c'è il supporto e la licenza a vita.

Fino a questo momento il "software utile" non si è mai lamentato di essere

eseguito da un utente non amministrativo. Questa cosa dovrebbe essere abbastanza indicativa perché, per prima cosa, molte aree del sistema non sono accessibili agli utenti non amministratori, e per seconda è impossibile modificare alcunché nelle aree di sistema del registro o nelle impostazioni di sicurezza di Windows se non si accede con un account amministrativo: ossia il software *non potrà correggere un bel niente*.

Tutto questo, lo ricordiamo, in una macchina virtuale isolata, appena installata, mai connessa a Internet. Se questo non è un sistema per togliere i soldi alle persone facendo leva sulla paura, non so cosa altro possa esserlo.

Per questo motivo questi software sono classificati come *rogue antivirus* (antivirus disonesti), e fanno parte di una categoria più ampia denominata *scareware* (contrazione delle parole inglesi *scare software*, software che spaventa), o anche *scam software* (software truffa).

La tecnica è propria del *social engineering*: adottando strategie tese a spaventare l'utente, ad esempio avvisandolo di pericoli estremi ma esposti in modo vago, ed offrendogli la soluzione a portata di clic (e carta di credito).



### **Niente di illegale**

Qui occorre precisare che questi programmi non sono segnalati come malware dagli antivirus, perché non lo sono. Tecnicamente non fanno nulla di illegale e niente che l'utente non abbia autorizzato in precedenza. Si tratta solo di forme di marketing molto aggressivo ed eticamente discutibile, ma nulla di illegale.

Appena pagata la licenza, magicamente, tutti i pericoli scompaiono ed il software diventa silenzioso, lasciando in pace l'utente. Naturalmente, se si spaccia per un antivirus, la protezione effettiva che offre è pressoché nulla, non avendo aggiornamenti né database delle firme. Analisi condotte da molte parti<sup>2</sup> dimostrano che tali software, nella maggior parte dei casi, non hanno alcuna efficacia reale<sup>3</sup>,

2. [http://www.spywarewarrior.com/rogue\\_anti-spyware.htm](http://www.spywarewarrior.com/rogue_anti-spyware.htm)

3. <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=7a827fbd-c2a1-48bc-9e85-6b805d3e7e26>

ed anche quando possiedano le capacità di operare come antivirus, hanno una efficacia limitata nei confronti dei malware reali, mentre spesso segnalano come malware file del tutto innocui, eventualità nota come *false positivo*.



### Per chi ha un computer Apple

Chi ha un Mac non si senta escluso, affatto. Proprio nei giorni in cui sto terminando la prima revisione del libro, un malware con identiche caratteristiche, ossia che si offre come “antitutto” per inesistenti pericoli, chiamato *MacDefender* nella prima versione e *MacGuard* nella seconda, sta creando qualche grattacapo. La seconda versione si installa anche se l’utente non appartiene al gruppo degli amministratori, quindi anche se non è privilegiato. Sul sito di Intego<sup>4</sup>, una società di sicurezza che si occupa anche di Mac OSX, vi sono schermate che non hanno nulla da invidiare ai corrispondenti *scareware* per Windows.

## Computer lento? Velocizzalo!

Altro esempio di sfruttamento della disinformazione e dell’ignoranza di noi utenti, è la pletora di programmi e programmini che promettono miracoli nel rendere il nostro computer più veloce, “proprio come appena installato” recita una delle pubblicità.

Per prima cosa, sarebbe corretto operare una distinzione sulla effettiva velocità del computer e sulla *percezione* della velocità da parte dell’utente, cosa ben diversa. La sensazione di velocità è in realtà la combinazione di diversi fattori, pochi dei quali hanno effettivamente a che fare con la velocità in senso stretto. Il primo fattore, probabilmente il più importante, è la reattività ai comandi, seguita dalla prontezza di risposta. Sembrano la stessa cosa, ma la distinzione c’è: la prima è la risposta immediata ai comandi impartiti con mouse, tastiera o qualsiasi altro dispositivo di input: una freccia del mouse che procede a salti; una casella di testo in cui i caratteri digitati appaiono con uno-due secondi di ritardo. La seconda è la risposta del programma al comando: un clic del mouse su un link lo

---

4. <http://blog.intego.com/2011/05/02/intego-security-memo-macdefender-fake-antivirus/>

evidenzia, ma il browser non reagisce che dopo 5-10 secondi; doppio clic su un file lo evidenzia, ma il computer inizia a far “frullare” il disco per 4-5 secondi prima di mostrare una qualche reazione.

Un computer che mostri tutti questi “ritardi” e lentezze è perfettamente in grado di ricodificare un file video con gli stessi tempi di elaborazione di uno che invece appare velocissimo. Questo perché una codifica video richiede velocità oggettiva, più che reattività.

E’ sufficiente installare un antivirus, regolare e legittimo, per rendere meno reattivo un computer: questo perché l’antivirus, nel momento in cui andremo ad aprire un file, ne vorrà fare la scansione di controllo, introducendo un leggero ma avvertibile ritardo fra il doppio clic e l’apparire della finestra con il file voluto.

Mi trovo continuamente per le mani computer che sono praticamente catatonici: ogni operazione, anche la più stupida, guardare cosa c’è nei dischi, diventa faticosa. Un notebook capitatomi in questi giorni (depositatomi sul tavolo da un conoscente con la frase faticosa: “Vedi un po’ tu, è diventato lento”) aveva *quattro* differenti antivirus installati, uno solo dei quali conservava una parvenza di efficacia, gli altri non erano aggiornati da mesi, quindi inutili. Ad ogni clic su un qualsiasi file, quattro antivirus pretendevano di fare la scansione di controllo. Esasperante, più che lento.

Il punto è che sono proprio questi ritardi a comunicare la sensazione di lentezza, che però lentezza non è.

I motivi più comuni dell’apparire di questi ritardi possono essere riassunti nei punti seguenti:

- *Troppi programmi installati* - Ogni software installato porta con sé elementi che tendono ad accumularsi: librerie, servizi, chiavi di registro, oltre, naturalmente, a file e directory dell’applicazione stessa. Molte librerie vengono caricate in memoria anche se l’applicazione non viene avviata, e comunque il sistema operativo è costretto ad esaminarle tutte per elencare le funzioni che offre ognuna, in modo da renderle disponibili ad ogni programma che le richieda, anche se nessuno ne farà mai uso. I servizi sono applicazioni eseguite fin dalla partenza del computer, ed occupano risorse, anche se non svolgono attivamente nessuna

funzione. Alcuni sono semplici scadenziari, che ci ricordano di registrare una licenza, o di fare un aggiornamento. Chiavi di registro, file e directory rallentano in generale tutto il lavoro al computer: più ve ne sono e maggiore diventa il tempo per reperirne uno, anche se l'impatto sulle prestazioni è realmente minimo, e l'ingolfamento deve raggiungere numeri consistenti per essere avvertibile.

- *Computer sottodimensionato* - Dopo un paio d'anni dall'acquisto, in media, un computer inizia a non essere adeguato all'esecuzione delle applicazioni più recenti rilasciate dai produttori. Poca memoria, processore troppo lento o mancante di alcune funzionalità, schede video inadeguate, disco lento. Se poi andiamo a fare un aggiornamento del sistema operativo ad una nuova versione la cosa diventa evidente, con situazioni limite in cui il software stesso rifiuta di installarsi per carenza di risorse.
- *Strumenti di sicurezza invasivi* - quasi tutti gli antivirus offrono protezione continua, controllando ogni singolo file a tiro dell'utente, esaminando ogni pagina web caricata, ispezionando ogni supporto di memorizzazione inserito. Tutta questa attività, anche se eseguita senza intervento dell'utente, impegna molte risorse e tende a rendere meno reattivo il computer, inducendo anche la sensazione di rallentamento generale.
- *Malware* - in determinate circostanze, ed in funzione della categoria di malware, il rallentamento generale del computer può essere consistente al punto da rendere penosa qualsiasi operazione, anche banale. Questo in parte non è più vero, in quanto da qualche tempo i malware mirano ad essere silenziosi ed a operare in modo molto discreto per non attirare l'attenzione e soprattutto per ritardare l'insorgenza di sospetti nell'utente, e quindi allungare i tempi di permanenza nel computer.

Il comportamento tipico di noi utenti quando il computer diventa lento oltre un certo limite, che per la mia esperienza è estremamente soggettivo, è di cercare in Rete qualcosa per far diventare più veloce il computer.

Premesso che l'ottimizzazione delle prestazioni è un argomento non proprio alla portata di tutti, e che non esiste una ottimizzazione universale, dato che ogni applicazione ha esigenze differenti, la tipica ricerca fatta con Google con le parole chiave "velocizzare computer gratis" restituisce un numero consistente di link, fra cui almeno tre sponsorizzati: questi ultimi portano tutti, senza eccezioni, a siti che



espongono programmi esplicitamente offerti come capaci di svolgere una quantità di funzioni, tutte tese a rendere il computer più veloce. In tutti i siti restituiti dalla ricerca nei link non sponsorizzati appaiono pubblicità e link sponsorizzati agli stessi siti, con l'aggiunta di altri ancora, differenti.

A questo punto è inevitabile andare su uno di essi e scaricare il software cliccando sul pulsante in cui c'è in bella vista **Scarica GRATIS!**. Di seguito una carrellata di siti che offrono queste magie tecnologiche.

**Figura 8-21. Qui c'è anche un grafico animato**

**ASCENTIVE PC SpeedScan Pro**

### Cosa posso fare per migliorare le prestazioni del mio PC?

Se utilizzi regolarmente, quasi tutti i PC vengono colpiti da numerosi errori che, con il tempo, ne riducono le prestazioni. Con pochi clic del mouse, PC SpeedScan Pro rileva e rimuove questi errori e [migliora notevolmente le prestazioni del tuo computer.](#)

- Ottimizza al massimo le prestazioni del PC
- Rileva ed elimina gli errori del PC
- Consente di aprire più applicazioni simultaneamente
- Stabilizza il tuo sistema operativo Windows
- Rapido e intuitivo sia per i principianti sia per gli esperti

**Migliora le prestazioni del PC**  
- fai clic qui -

#### Influenza negativa dei file di errore sulle prestazioni del PC

File di errore	Velocità
500	Alto
400	Medio
300	Basso
200	
100	

In media un PC contiene almeno 432 file di errore

Indicatore livello prestazioni computer

**Esegui la scansione GRATUITA per conoscere gli errori che stanno rallentando il tuo PC - [Fai clic qui per avviare una scansione GRATUITA!](#)**

#### Problema

Con il passare del tempo, il computer accumula file non necessari che possono creare problemi. Ciò succede perché il sistema operativo Windows non gestisce bene i propri file.

Non importa se il tuo PC ha due mesi o due anni di vita, più hai ignorato questo problema, più grave è il disordine, che inizia a crearsi dalla prima volta che utilizzi il computer.

#### Soluzione

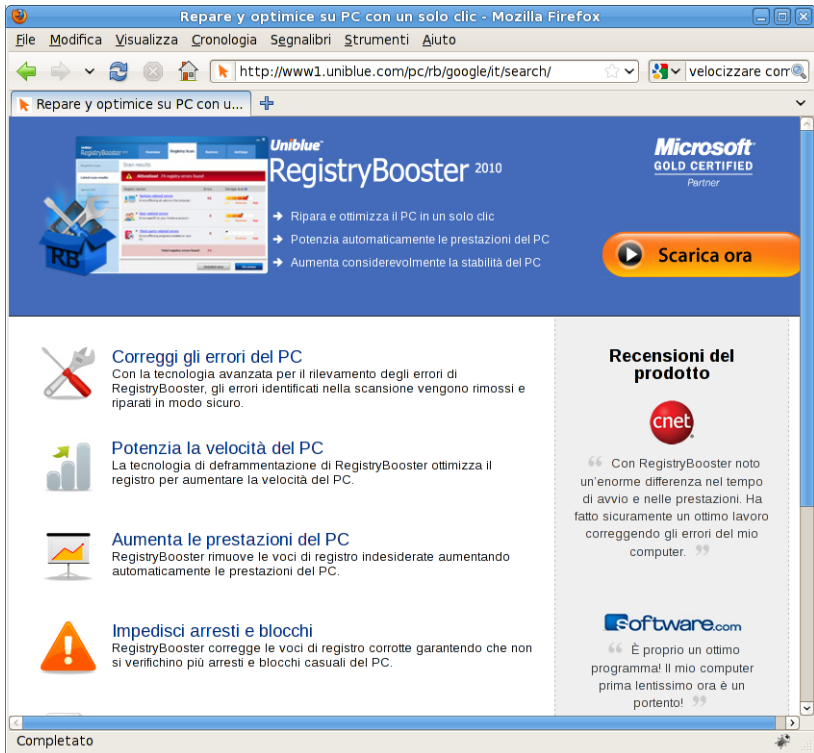
Puoi eseguire subito una scansione rapida e rilevare i file inutili e le voci di comando incorrette che sono all'origine di questi problemi. PC SpeedScan Pro è il programma più rapido ed efficace di rilevamento degli errori disponibile sul mercato. Inoltre, una volta trovati gli errori, hai la possibilità

Completato

Nell'immagine appena mostrata, addirittura viene fornita una spiegazione del perché il computer rallenti col tempo, nella sezione "Problema". Tale spiegazione è inesatta, fuorviante e tendenziosa, addossando genericamente la colpa a Windows. Non è per nulla vero che "Windows non gestisce bene i propri file". Quello che è vero è che molte applicazioni usano malissimo gli strumenti che

Windows mette a disposizione per la gestione di installazione, configurazione e rimozione. Ma questo diventa un problema quando sul computer viene installata troppa roba, come diciamo da tempo.

Figura 8-22. Questo ha i “bollini” di certificazione



Alcuni di questi programmi sono pubblicizzati in più siti differenti, con differenti grafiche di presentazione, ma tutti portano allo stesso programma. Questo per via di una strategia di marketing chiamata “affiliazione”, che in sé non ha nulla di negativo: se fai pubblicità al programma sul tuo sito, per ogni copia venduta per tuo tramite prendi una piccola percentuale sul guadagno.

Figura 8-23. Altra versione dello stesso



Figura 8-24. Questo mette anche fretta a chi lo visita...

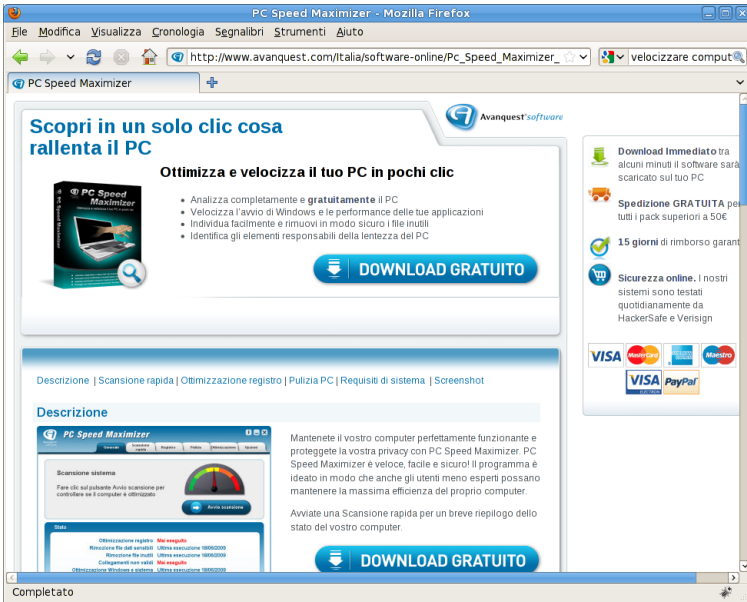


Figura 8-25. ... non perdere tempo a leggere, scarica, PRESTO!



Notare che in tutti i siti non è immediatamente evidente che *solo la scansione è gratuita*, l'ottimizzazione comporta *sempre* l'acquisto di un qualcosa, che sia una licenza, che sia un servizio di assistenza, che sia l'aggiornamento a vita. L'unico che nel pulsante scrive esplicitamente "Scansione gratuita" è quello in Figura 8-26.

**Figura 8-26. Solo la scansione è gratuita, questo almeno lo dice.**



Naturalmente, niente vieta di produrre un software che aiuti le persone a tenere un po' più ordinato il computer ed a correggere automaticamente errori evidenti nella configurazione del computer. E niente vieta di chiedere un equo compenso per la fatica di creare e mantenere aggiornato il database delle impostazioni "corrette" per le versioni di Windows in commercio e per le principali applicazioni.

Purtroppo, molti di questi programmi non fanno quanto promettono o, se lo fanno, le impostazioni che propongono sono assolutamente banali ed inefficaci, tipo aumentare la cache del browser e disabilitare gli effetti grafici dell'interfaccia utente di Windows, operazioni che è possibile fare anche dalle interfacce di gestione native del sistema operativo, senza dover scomodare un software apposito. Di contro, sono molto insistenti nel richiedere la registrazione (ed il pagamen-

to della relativa quota), continuando a mostrare messaggi allarmanti e ripetitivi. Per questi motivi, ed altri che vedremo fra poco, questi software sono denominati *grayware*, software grigi, sia per indicare la natura indistinta e nebbiosa del loro operato, sia per indicare l'incerta classificazione: non sono propriamente malware, ossia neri, né effettivamente utili, cioè bianchi.

Ne avevo parlato a suo tempo nel mio blog, prendendo in esempio due programmi fra quelli proposti dalle pubblicità nei vari siti web, ed i risultati erano stati piuttosto rivelatori<sup>5</sup>.

Ripetiamo l'esperimento a distanza di quasi due anni, usando al solito la nostra macchina virtuale, stavolta con *Windows Seven*.

Dopo averne provati ben quattro, possiamo dire che il comportamento è simile in tutti. Vi sono le eccezioni: una quinta applicazione permette un periodo di prova di 15 giorni, in cui tutte le funzioni sono attive.

L'installazione è rapida e senza opzioni da selezionare: solo l'accettazione della licenza e la scelta se posizionare le due classiche icone sul desktop o sulla barra di avvio veloce. Al riavvio, appare una icona vicino all'orologio e parte una scansione automatica che porta via da poche decine di secondi a qualche minuto. Tale scansione è disattivabile, ma occorre vagare alla ricerca dell'impostazione nelle opzioni del programma.

---

5. <http://www.ismprofessional.net/pascucci/index.php/2009/07/ripara-velocizza-e-pulisci-cosa-non-si-sa/>



---

**Figura 8-27. All'avvio una bella scansione**



---

I risultati della scansione sono *sempre* allarmanti, con comportamenti di due tipi: o vengono esagerati i problemi, ad esempio segnalando come errori critici semplici chiavi di registro vuote o impostazioni poco usate, o vengono praticamente inventati, segnalando ad esempio come problemi per la privacy i file ed i cookies contenuti nella cache del browser, tutti indistintamente. Naturalmente, entrambi i comportamenti sono tesi a spaventare e provocare ansia nell'utente, per predisporlo a quello che succede quando si preme il pulsante di correzione.

Figura 8-28. I risultati sono disastrosi, naturalmente...

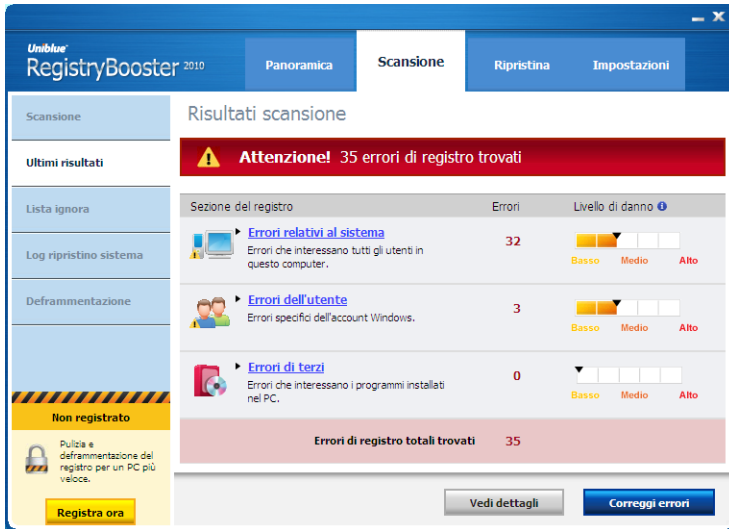
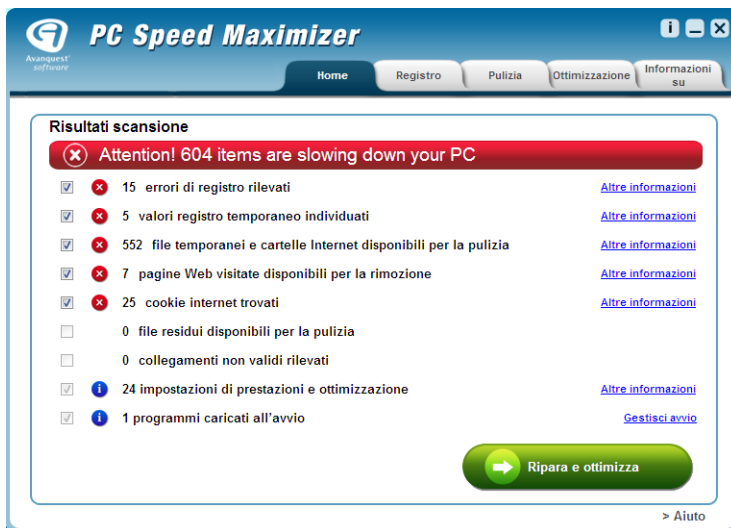


Figura 8-29. ...sempre e comunque disastrosi



Eseguendo i differenti programmi appaiono discrepanze macroscopiche fra i risultati. Alcuni segnalano pochi errori, dell'ordine delle decine, altri vanno tranquillamente sulle centinaia. Esaminando i rapporti di scansione ci si trova spesso di fronte ad elenchi generici: chiavi di registro segnalate come errate, ma non viene specificato il motivo specifico; vengono riportati elenchi sterminati di file, senza definire il problema.

Quando invece gli elenchi sono dettagliati le segnalazioni appaiono imbarazzanti ad un occhio appena più competente dell'utente medio: la pagina iniziale predefinita di Internet Explorer, chiavi di registro vuote appartenenti a impostazioni predefinite, file della cache di Internet Explorer *appartenenti al sito Microsoft* definiti come *privacy threat* (un pericolo per la riservatezza).

**Figura 8-30. Ma i numeri sono praticamente a caso**



Alcune versioni offrono pacchetti aggiuntivi, sempre con lo stesso metodo della scansione gratuita, per aumentare la velocità del computer, per fare scansioni anti-spyware, per ogni sorta di “ottimizzazioni”.

Figura 8-31. Ben quattro programmi per ottimizzare e verificare



Ad ogni download ed installazione viene chiesto l'acquisto di una nuova licenza. L'importo è relativamente contenuto, in genere, e compreso fra 20 e 40 euro. La cifra non è casuale, nel senso che probabilmente è scelta per essere abbastanza alta da garantire adeguati profitti, ed abbastanza bassa per cui un cliente "scontento" possa essere messo di fronte ad ostacoli sufficienti a farlo desistere dal richiedere i soldi indietro: un *call center* che non risponde mai, le e-mail che rimangono a lungo senza risposta, le richieste di rimborso che richiedono procedure assurdamamente complicate. Cercando i nomi delle applicazioni di ottimizzazione su Internet si trovano innumerevoli forum dove frotte di utenti si lamentano fondamentalmente di:

- non riuscire a disinstallare le applicazioni in versione di prova
- dopo aver pagato, l'applicazione non offre i risultati promessi
- le richieste di rimborso cadono nel vuoto

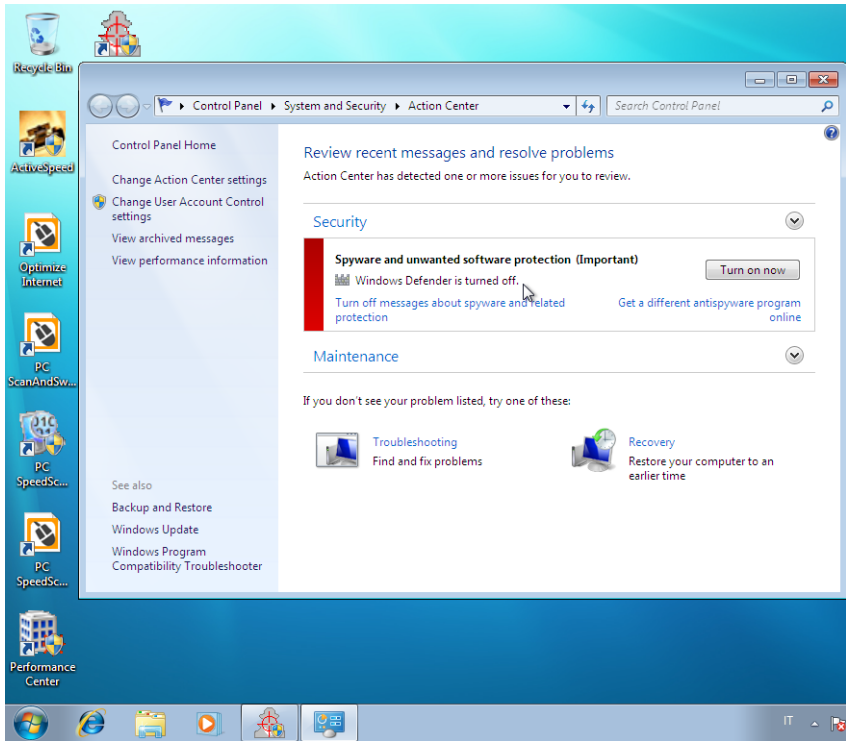
- nessuna risposta a e-mail e chiamate al numero dell'assistenza.

In alcuni casi viene lamentato l'addebito su carta di credito di cifre superiori a quelle dichiarate, senza alcuna risposta alle richieste di chiarimento da parte degli utenti. In un sito web dedicato ai reclami<sup>6</sup>, basta inserire il nome di uno di questi software per leggerne di cotte e di crude: vi sono decine di utenti che lamentano di aver pagato per non ricevere nessuno dei benefici promessi, di aver visto prelevate cifre superiori a quelle pattuite dalla propria carta di credito, ed infine di non aver ricevuto indietro il denaro a seguito di una richiesta di rimborso.

---

6. <http://www.complaintsboard.com/>

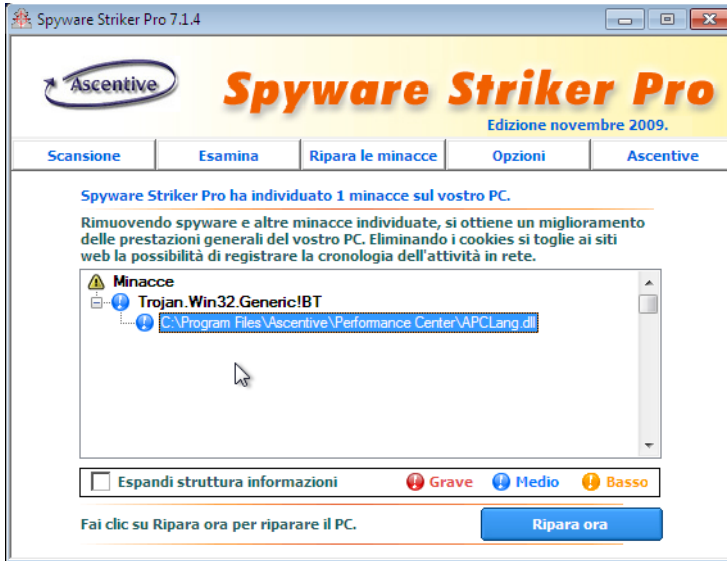
**Figura 8-32. Per sicurezza, disabilita Windows Defender...**



Terminiamo la carrellata con qualche chicca. Uno di questi prodotti, con funzione dichiarata di antispyware, al momento dell'installazione ha per prima cosa disattivato Windows Defender, l'antispyware integrato in Windows Vista e 7 (Figura 8-32), poi, dopo aver scaricato quasi 70 megabyte di "database degli spyware", al termine della scansione, durata parecchi minuti, ha indicato come critico un singolo *cookie*, proveniente dalla società di pubblicità di Microsoft. Per rimuovere *un singolo cookie* occorre pagare 36 euro e 90 centesimi. Cosa che si può fare a costo zero e senza installare nulla semplicemente cancellando la cronologia di navigazione di Internet Explorer, dopodiché il numero di problemi

rilevati è stato esattamente zero.

Figura 8-33. Una serpe in seno



Infine: dopo una scansione approfondita ha segnalato come spyware di media pericolosità un file appartenente al centro di controllo delle prestazioni *appartenente alla sua stessa suite di programmi* (Figura 8-33).



### Anche qui niente di illegale

Non si tratta di malware. Non eseguono operazioni che l'utente non abbia prima autorizzato. Non costringono nessuno a mettere mano al portafogli. E' marketing aggressivo ed eticamente discutibile, basato sull'ignoranza e sull'incompetenza cronica degli utilizzatori.



Per concludere questa parte, possiamo andare a vedere anche le ottimizzazioni pensate per rendere il computer e la navigazione Internet una vera freccia. Si tratta *per la totalità dei casi* di impostazioni assolutamente banali che è possibile fare da Windows stesso: aumentare la dimensione della cache di Internet Explorer, verificare solo una volta per sessione gli aggiornamenti delle pagine visitate, disabilitare gli effetti visivi del desktop, disattivare l'*antialiasing* dei caratteri a schermo, disabilitare l'aggiornamento della data di ultimo accesso ai file nel disco, dare maggiore priorità alle applicazioni in primo piano, e via così. Ognuna di queste impostazioni può avere effetti positivi sulla velocità *percepita* del computer, ma ognuna ha delle controindicazioni.

Inoltre, per come è la struttura del file registro di Windows, *non è cancellando chiavi qua e là che si ottimizza*. Cancellando una sola sottochiave non si guadagna un solo byte di spazio su disco, in quanto il registro usa blocchi da 4 kilobyte, che riempie di volta in volta con gruppi di sotto-chiavi. Cancellandone una nel gruppo non si guadagna alcunché. C'è un vecchio articolo di Mark Russinovich<sup>7</sup> su TechNet (il sito Microsoft dedicato agli sviluppatori ed ai sistemisti) che spiega come è fatto il file registro, e dove è evidente che l'impiego di "ottimizzatori di registro" è del tutto inutile.

Ricapitolando: se il computer è lento, la soluzione va cercata altrove. L'ottimizzazione delle risorse di un computer è un argomento estremamente specialistico, e deve essere operata da persone competenti. Usare programmi a pagamento per operare modifiche minime e banali, dalla dubbia efficacia, che è possibile operare senza intermediari *usando direttamente le interfacce di gestione native di Windows*, oltre che di dubbia efficacia, è uno spreco di soldi. Come suggerito più volte, occorre documentarsi e soprattutto evitare di trasformare il proprio computer in una discarica, installando qualsiasi cosa capiti a tiro.

## Le cattive abitudini sono dure a morire

Nel settembre del 2008 avevo mostrato un sito web<sup>8</sup> dove si potevano cercare programmi creati per spezzare le protezioni del software commerciale, che

7. <http://technet.microsoft.com/it-it/library/cc750583%28en-us%29.aspx>

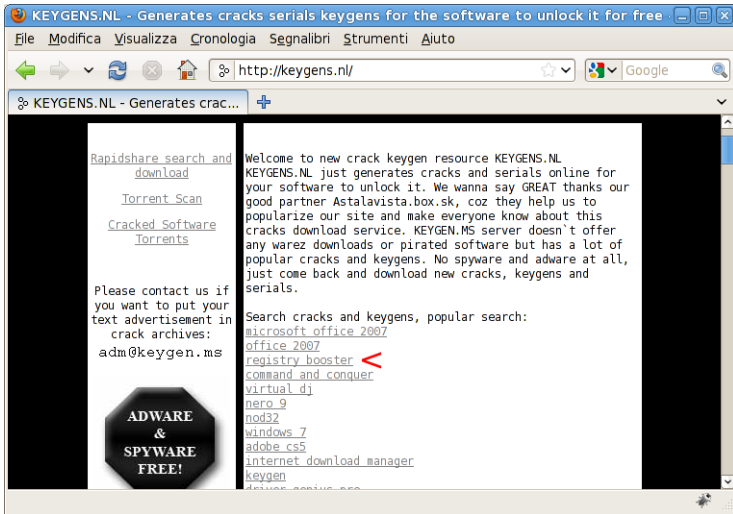
8. <http://www.ismprofessional.net/pascucci/?p=283>

in realtà, con la tecnica ben collaudata delle caramelle dagli sconosciuti, rifilava malware di vario tipo. Il sito manteneva una lista delle ultime ricerche fatte dai visitatori, ed una di queste puntava ad un noto falso antivirus, Antivirus XP 2008, dello stesso tipo trattato fino ad ora. Ricapitoliamo brevemente: chi aveva fatto quella ricerca aveva in realtà già contratto una pestilenza abbastanza fastidiosa, quella del falso antivirus, che chiedeva continuamente la registrazione (più propriamente, il pagamento di una “tassa”) per eliminare malware inesistenti. La strategia di risoluzione scelta dall’ignoto visitatore era stata quella di cercare un generatore di chiave di registrazione del software (in gergo un *keygen*) su un sito assolutamente privo di qualsiasi garanzia. Il probabile risultato era che se il visitatore aveva scaricato il programma, aveva contratto *una seconda pestilenza*, visto che il sito in questione era stato creato apposta per questo.

Tutto ciò è indicativo di un modello di pensiero persistente e radicato in molti utenti. Piombo su un sito che mostra una scansione del mio computer, assimilabile a quella di un normale antivirus, al termine della quale mi viene proposto di scaricare un antivirus, che io diligentemente installo *senza farmi domande*. La successiva scansione riporta di nuovo una estesa infezione del computer. Potrei avere un antivirus già installato che non ha segnalato niente di tutto questo, o potrei non averne, non fa differenza: *accetto i risultati senza farmi domande*. Alla pressione del pulsante Disinfetta mi viene presentata una richiesta di registrazione con un codice, da ottenere a pagamento. Invece di pagare, mi metto a cercare il codice di registrazione in Rete, o mi rivolgo ad uno di questi siti messi a disposizione da tanti “benefattori”, *senza domandarmi cosa ci guadagnino*.

Tutta la sequenza implica che la persona ne sappia quanto basta di computer e Internet, probabilmente più della media degli utilizzatori, ma anche che stia operando con la convinzione che su Internet si trovi tutto, basta cercarlo *nei posti giusti*, e comunque a cervello spento. Questa è la combinazione principe di assunti e comportamenti per cadere vittime di tutti i trabocchetti e le possibili truffe che costantemente sono architettate e messe in pratica da chi sa come trarne profitto.

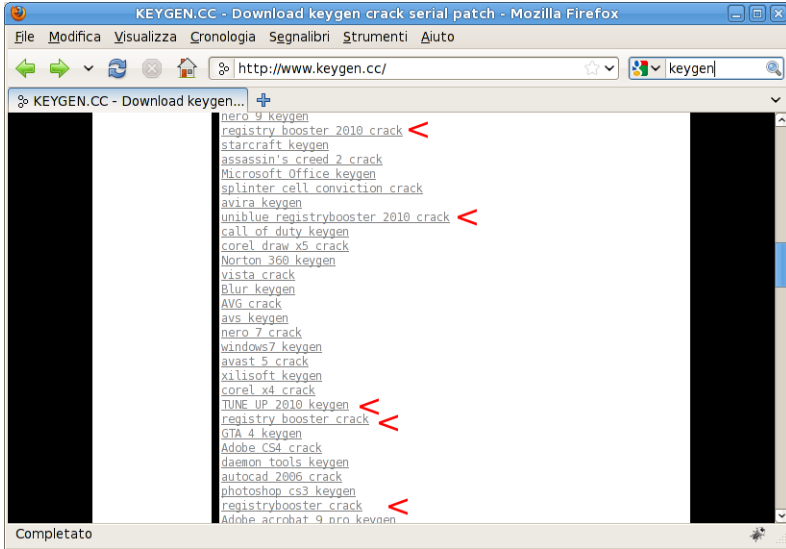
Figura 8-34. Dopo il velocizzatore, il rallentatore



Nel momento in cui scrivo il sito di cui parlavo nel blog non è raggiungibile, ma ve ne sono molti altri che fanno lo stesso lavoro, e, come possiamo aspettarci, ora che abbiamo iniziato a capire come veniamo ingannati e colpiti, troviamo le solite sorprese. Ne mostriamo qualcuno.

In Figura 8-34 qualcuno ha cercato il codice per registrare il “velocizzatore” in Figura 8-22 (il link indicato con la freccia rossa). Peccato che il programma magico, una volta scaricato a passato a Virustotal<sup>9</sup> venga identificato da 30 antivirus su 42 come un malware non esattamente utile.

9. <http://www.virustotal.com/>

**Figura 8-35. In cinque hanno tentato, in cinque hanno fallito**

In Figura 8-35 è anche peggio. Sono ben cinque le ricerche fatte, e in tutti e cinque i casi hanno trovato molto più di quanto speravano, anche se non nel senso voluto.

Il significato di quanto mostrato è proprio nella totale ignoranza che rivela questo comportamento. Ignorare che quei software sono dei falsi, o nella migliore delle ipotesi inutili; ignorare che l'uso di un *keygen* non solo è illegale ma, praticamente sempre, porta a casa molto più di quanto desiderato; ignorare l'uso corretto di Internet, cercando un software pirata invece di rivolgersi alla comunità di esperti che ogni giorno mettono in guardia gli utenti sia su questi software inutili sia su quanto le cattive abitudini siano pericolose per chi le pratici.

Per arrivare poi ad altezze inarrivabili di ingenuità con altri utenti altamente confidenti nella loro esperienza che su vari forum consigliano “di controllare con l'antivirus” i vari *keygen* scaricati, o ridicolizzano l'utente che evidentemente, dal loro punto di vista, non lo ha fatto prima di lanciare il programma sospetto.

Ingenuità doppiamente pericolosa, che mostra da un lato quanto poco sappiamo dell'argomento, dall'altro quanto si credano al sicuro perché hanno l'antivirus, dimostrando di non aver capito nulla di come l'antivirus funzioni: nel momento in cui ho scaricato la prima volta il programmino, per passarlo a Virustotal, solo 7 antivirus su 42 lo segnalavano come potenzialmente pericoloso, senza riuscire ad identificarne categoria o famiglia. Dopo un mese ho fatto controllare di nuovo lo stesso file, che avevo conservato appositamente, ed il tasso di rilevamento è salito a 30 su 42, anche se pochissimi lo identificano per quello che realmente è: un malware per il furto di credenziali. Non si provi a barare affermando che i più noti e blasonati mettono al sicuro: nei 12 che non lo riconoscono ci sono molti nomi eccellenti.

## Follie sparse

Quelle elencate fino ad ora sono solo alcune delle strategie poste in essere da chi ha come unico scopo il mettere le mani nel nostro portafogli. La sempre maggiore diffusione di strumenti di pagamento su Internet ha certamente dato un grande impulso al commercio elettronico ma, come c'era da attendersi, ha reso possibile ad ogni sorta di mentecatti il raggiungere milioni di persone con poco sforzo, trasformando di fatto ogni minima operazione truffaldina in una vera e propria piaga.

Per un periodo, nel 2008, era possibile imbattersi in siti web che vendevano l'installazione<sup>10</sup> del plugin Flash Player di Adobe<sup>11</sup>, disponibile da sempre gratuitamente. La tecnica era quella di costringere l'utente a chiamare via cellulare un numero a tariffazione maggiorata per ottenere un "codice di attivazione" del tutto inutile per l'installazione regolare del plugin. Il plugin installato era per fortuna identico a quello liberamente disponibile. In questo caso non era neanche necessario mettere mano alla carta di credito, facilitando l'abbozzare delle vittime ed allargando enormemente la platea di possibili vittime. Il numero da chiamare era un 899, segno che dietro la truffa c'era probabilmente una mano italiana.

---

10. <http://www.ismprofessional.net/pascucci/index.php/2008/08/flash-player-plugin-attenti-alle-versioni-a-pagamento/>

11. <http://get.adobe.com/it/flashplayer/>

Simile sorte era toccata ad eMule e non è detto che non succeda per qualche altra applicazione nota.

La tecnica è efficace anche per via della mancanza di percezione da parte dell'utente del pagamento in sé: chiamare un numero di telefono non ha effettivamente nessuna connotazione di volontà di acquisto, perché il telefonare è una cosa differente, è un comunicare.

Quando sentiamo la parola “gratis”, da oggi in poi, dobbiamo esercitarci a trovare l'inghippo, subito. Perché non è detto che ci sia, ma basta riuscire ad evitarne uno solo e ci saremo ripagati ampiamente della fatica.

Vedremo fra poco come anche cose apparentemente prive di valore monetario, come i nostri interessi e i nostri hobby, diventino strumenti per mettere le mani nelle nostre tasche, direttamente ed indirettamente.

## Capitolo 9. Il web delle meraviglie

Che differenza passa fra un articolo pubblicato su una rivista scientifica ed un sito web che parla della stessa cosa?

Il non saper rispondere a questa domanda contiene il primo indizio del perché le persone cadano vittime di ogni genere di truffa, disinformazione, scherzi, complottismi più o meno fantasiosi.

Per pubblicare un articolo su una rivista scientifica occorre non solo dimostrare che chi scrive sappia di cosa parli, ma anche passare una particolare procedura chiamata *peer review*<sup>1</sup>, che in italiano può essere grossolanamente tradotta con “revisione paritaria”. Prima di essere pubblicato, l’articolo viene esaminato da un gruppo di persone la cui competenza nel campo è riconosciuta ed accettata, che rimangono anonime per motivi di indipendenza del giudizio.

Questo meccanismo ha vari effetti positivi: se la trattazione non è rigorosamente scientifica, ossia non segue i dettami di ripetibilità e riproducibilità dei risultati da parte di altri, o non riporta dati oggettivi risultato di esperimenti, viene scartata per ovvie ragioni. Altro effetto, spesso determinante, è che consente di correggere e migliorare i risultati di una ricerca grazie ai suggerimenti e alle critiche mosse da chi opera la revisione. Non ultimo, costringe chi vuole presentare i propri lavori ad attenersi al metodo scientifico, quindi ad essere rigoroso, dovendo dimostrare con i fatti le proprie idee.

Come tutte le cose umane, il meccanismo è certamente migliorabile, ma ha l’indiscusso effetto di stroncare da subito ricerche inutili, vicoli ciechi, false scoperte e simili. Tanto è che funziona da secoli, ormai.

Su Internet tutto questo non vale più. Chiunque può prendersi uno spazio web per pochi centesimi, o addirittura senza spendere nulla, e pubblicarci qualsiasi cosa gli passi per la testa, raggiungendo potenzialmente centinaia di milioni di persone senza alcuno sforzo.

Sommando questo alla pressoché totale assenza di senso critico di molti di noi, oltre all’implicita autorevolezza della frase “l’ho letto su Internet”, è facile immaginare quanto sia frequente abboccare a qualsiasi scemenza letta in Rete.

---

1. [http://it.wikipedia.org/wiki/Revisione\\_paritaria](http://it.wikipedia.org/wiki/Revisione_paritaria)

## **L'ha detto Internet!**

E' la frase che, in varie forme e declinazioni, sta pian piano prendendo il posto della mitica "l'ha detto mio cugino", pronunciata nel tentativo di avvalorare una affermazione altrimenti insostenibile sotto qualsiasi punto di vista.

Nessuno controlla niente su Internet (per fortuna), per cui ogni singola cosa letta va verificata accuratamente, prima di prenderla per buona. Il fatto che qualcuno scriva su un sito web che si possa ricavare energia pulita a costo zero dall'acqua non lo rende vero automaticamente. Il fatto che qualcuno mostri immagini di gatti cresciuti in bottiglie di vetro<sup>2</sup>, non significa che qualcuno l'abbia fatto realmente.

Assurde, le cose che ho citato, eppure sono anni che cose simili circolano in Rete, nonostante ci siano innumerevoli siti web di persone autorevoli e conosciute per la loro serietà che ne abbiano dimostrato la totale falsità.

Perché succeda questo nessuno lo sa, anche se molti hanno ipotizzato spiegazioni verosimili. Per quello che ci interessa qui, basti sapere che alla maggior parte di noi il semplice leggere qualcosa scritto in una pagina web lo fa assimilare per vero. Che poi lo sia sul serio, è tutto un altro paio di maniche.

Il risultato funesto è che diventa sempre più difficile trovare contenuti validi e verificati, mentre aumenta a dismisura la disinformazione. L'effetto finale è quello di ascoltare musica a mezzo metro da una turbina di un aereo a reazione accesa: la musica c'è, ma nessuno è in grado di sentirla.

Questa situazione è in parte mitigata dall'altro aspetto, ancora poco sfruttato, di Internet, dove tutti siamo in un certo senso uguali. Se nel mio blog scrivo una palese cretinata, in poco tempo mi si riempie di commenti che vanno da quello che fa notare gentilmente che ho scritto una fesseria a quello che mi invita senza tanti complimenti a dedicarmi ad un altro mestiere.

Il problema, non proprio banale, è quindi assegnare un livello di affidabilità ad ogni singola cosa che leggiamo e vediamo.

Facciamo un esempio vicino ai nostri argomenti, anche per mostrare alcuni meccanismi non sempre chiari ai più. Il proprietario e autore di un sito web che

---

2. [http://it.wikipedia.org/wiki/Bonsai\\_Kitten](http://it.wikipedia.org/wiki/Bonsai_Kitten)



tratta di argomenti legati a Windows ed al suo uso quotidiano decide di provare un diverso sistema operativo. Dopo qualche tentativo relativamente infruttuoso, scrive una recensione sul suo sito dove definisce il sistema operativo provato in termini fortemente negativi. In poco tempo, l'articolo pubblicato riceve una quantità enorme di commenti che fondamentalmente accusano l'autore di mancanze ben precise, in particolare: di aver scritto di cose su cui non ha specifica competenza; di aver presentato argomentazioni fortemente discutibili a sostegno delle proprie tesi; di non aver approfondito a sufficienza l'argomento con qualcuno più esperto, prima di avventurarsi nel test. Buona parte dei commenti ha un tono piuttosto aggressivo, qualche volta ingiurioso.

Il problema si presenta quando qualcuno, volendo fare la stessa prova, usa Google per cercare recensioni sul sistema operativo scelto e capita su questa pagina. Chi ha ragione? L'autore dell'articolo o gli innumerevoli commentatori imbufaliti per la denigrazione del loro sistema operativo preferito?

Non è certamente il numero a fare la ragione, come non è certamente chi grida più forte ad averla, per cui risulta effettivamente ostico decidere se prendere in considerazione la recensione negativa.

Fondamentalmente è una variante di un problema molto più vasto: capire se chi scrive (o parla) sappia di cosa stia parlando. Purtroppo, nella maggior parte dei casi, occorre saperne più di chi scrive per poter rispondere al quesito.

Vi sono però dei segnali, piuttosto evidenti se cercati esplicitamente:

- Assenza di dettagli specifici e di procedure per replicare autonomamente i risultati esposti. Quando viene affermato qualcosa e non viene esplicitata la sequenza di azioni o di ragionamenti che portano all'affermazione stessa, siamo di fronte ad una di queste situazioni: o chi scrive sta esponendo una opinione personale, e quindi come tale va considerata, o sta parlando di qualcosa che non ha sperimentato di persona.
- Nessuna indicazione delle fonti. Gran parte delle informazioni che si usano per scrivere qualcosa, soprattutto in campo tecnico, non vengono dal nulla ma sono prese da fonti note e verificabili. Se quello che leggiamo non ha nessuna indicazione della fonte, o la fonte non è verificabile, siamo di fronte a notizie

potenzialmente inaffidabili.

- La risposta alle critiche o ai dubbi sollevati da altri è costituita unicamente da attacchi personali. Gli attacchi non sempre sono diretti ed espliciti, ma spesso sotto forma di svalutazione dell'interlocutore. La svalutazione e le minimizzazione sono due strategie tipiche delle tecniche per "avere ragione a tutti i costi".
- Nel caso si tratti di un sito che permetta i commenti dei visitatori, vi è la totale assenza di commenti negativi. Il proprietario del sito ha il completo controllo di quello che vi appare, e può selezionare a piacimento i commenti, naturalmente senza alcun segno visibile dall'esterno.

Questi sono i segnali più palesi e naturalmente ne esistono molti altri, ma andremmo oltre lo scopo di questo libro. Quello che ci preme puntualizzare qui è che quello che si legge in Internet, in senso molto ampio, va preso con molte precauzioni: verificare sempre fonti, autorevolezza e competenza di chi scrive.

## Lei non sa chi sono io

Strettamente legato al punto appena discusso, vi è il problema dell'identità del o dei nostri interlocutori su Internet.

Il primo ed unico assunto da tenere sempre a mente è che su Internet *nessuno sa chi ha di fronte realmente*. E' certamente valido anche nella vita reale, in senso lato, ma su Internet diventa un aspetto estremamente importante. Per chi conosce i meccanismi, è semplicissimo costruire una identità digitale totalmente slegata dalla realtà. Ed è semplicissimo usarla per acquistare credito ed estendere il numero di potenziali vittime dell'inganno.

Oltre gli innumerevoli casi di truffatori e malviventi che hanno adescato le proprie vittime proprio basandosi su questa strategia, vi è un caso, in particolare, che ha reso evidente questo aspetto della Rete: quello di Amina<sup>3</sup>, la blogger siriana<sup>4</sup> che si batteva per i diritti dei gay, dichiaratasi apertamente gay lei stessa.

3. <http://damascusgaygirl.blogspot.com/>

4. <http://english.aljazeera.net/news/middleeast/2011/06/201161345554900720.html>

Ebbene, nel giugno del 2011, un uomo di nazionalità americana<sup>5</sup> ha ammesso di essersi inventato il personaggio e tutta la storia.

Il tutto è andato avanti per mesi, da febbraio 2011, culminando con l'annuncio del rapimento di Amina da parte delle forze di sicurezza siriane, nel bel mezzo della rivolta popolare per chiedere più democrazia, i primi di giugno.

Pochi giorni dopo l'inganno viene svelato dallo stesso autore, che ne spiega le ragioni in un articolo nel blog stesso<sup>6</sup>.

La stampa internazionale, gli organi d'informazione, tutti sono caduti nell'inganno, pur se perpetrato a fin di bene, e con nessuna velleità di trarne profitto.

In Rete è praticamente impossibile verificare l'identità di chi abbiamo "di fronte", se non ha intenzione di farsi identificare. Un truffatore esperto riuscirà a crearsi una identità qualsiasi, credibile e verosimile, con tanto di "prove" tangibili al contorno: foto dei luoghi in cui vive, facce, persone, relazioni.

Tutte "prove" che possono essere costruite a tavolino combinando materiale liberamente disponibile in Internet: un indirizzo e-mail, un profilo Facebook, farcito con le giuste foto e qualche decina di amici, ed il gioco è fatto.

La realtà è che niente e nessuno ci può assicurare che il nome sia quello, che la persona abbia quella faccia, che viva in quella città, che faccia quel lavoro.

L'unica realtà, in questi casi, è l'inganno.

## **Antisocial Network**

Il fenomeno di questi anni sono i cosiddetti "social network". L'idea di base è che fornendo un adeguato supporto alla comunicazione, negli aggregati casuali di persone vengono a formarsi autonomamente delle reti di relazioni.

Di qui, la nascita di innumerevoli piattaforme per la creazione di queste reti, con varia funzionalità e scopo. Ci sono quelle orientate alle reti lavorative e

---

5. <http://www.unita.it/mondo/la-blogger-amina-era-un-falso-br-un-40enne-confessa-ero-io-1.303601>

6. <http://damascusgaygirl.blogspot.com/2011/06/apology-to-readers.html>

professionali (LinkedIN, Xing), quelle generiche (Facebook, Orkut, MySpace) e quelle con usi particolari (FourSquare, Ping, Flickr). Naturalmente, non ci interessa fare recensioni dei servizi, il nostro punto di vista è un altro, il solito: dov'è il pericolo?

Partiamo da una semplice domanda: cosa ci guadagna chi offre questo servizio? Perché, al solito, è tutto apparentemente gratis, ma abbiamo imparato a diffidare di questa parola.

Per aderire ad uno di questi servizi, di solito, occorre fornire una quantità di dati personali che variano da un semplice nomignolo ed una password, a tutta una serie di informazioni sulle nostre attività lavorative e personali. Poi, dopo l'adesione, veniamo continuamente sollecitati ad arricchire il nostro "profilo" con altre informazioni ed a "connetterci" con altri utenti presenti. Ad esempio su Facebook veniamo sollecitati a cercare ed aggiungere "amici", su LinkedIN siamo spinti ad aggiungere colleghi, clienti e collaboratori.

Queste sono tutte informazioni e nel mondo attuale hanno un valore, anche quando non siano direttamente riconducibili a noi.

Immaginiamo di essere una società di ricerche di mercato, e di essere interessati ai gusti di una certa fascia di persone. Quale migliore fornitore di un *social network* con oltre cinquecento milioni di iscritti?

Potrebbe sembrare inverosimile, dato che molte informazioni non sono esplicitamente richieste, o non sono disponibili per via delle impostazioni di riservatezza scelte dagli utenti. Aggirare queste limitazioni è relativamente facile: basta offrire all'utente una contropartita. Su Facebook esistono le cosiddette "applicazioni", ossia delle funzioni aggiuntive sviluppate sia dal team di Facebook stesso che da terze parti. Un esempio sono gli innumerevoli quiz, come "che tipo di donna sei" o "che personaggio dei fumetti ti assomiglia di più", oppure alcuni giochi che è possibile usare solo all'interno di Facebook.

Queste applicazioni chiedono espressamente all'utente di poter accedere ai dati del profilo per essere usate. Il risultato è che per fare un banale quiz diamo il permesso di curiosare a piacere nei fatti nostri a chi ha creato l'applicazione. Quello che dobbiamo tener presente è che *nessuno* può dire che cosa ne faranno.

Il risultato finale è che abbiamo perso il controllo dei nostri dati. Magari

abbiamo anche perso ore a documentarci su come impostare i permessi di accesso: un singolo clic può vanificare del tutto i nostri sforzi, *senza che ne abbiamo coscienza*.

Altro problema, non certo di minore importanza, è che pur adottando un controllo ferreo dei nostri dati e di come vengano utilizzati all'interno dell'applicazione che costituisce il *social network* stesso, non abbiamo alcun controllo su quello che i nostri "amici" rendono pubblico su di noi. Possiamo impedire di essere "etichettati" (in inglese *tagged*) in una foto di gruppo, se però il nostro nome appare nel commento della foto, o un nostro amico commenta con frasi del tipo "Ti sei fatto crescere la barba!" e noi siamo gli unici in foto con la barba, possiamo esserci impegnarci a morte per non far associare la nostra faccia al nostro nome, ma basta questo per rendere inutili gli sforzi.

Alcune impostazioni sono poi sibilline, e non sempre ci si rende conto di quale portata abbiano: dicendo che le nostre foto sono visibili solo agli amici, possiamo averne un certo controllo, ma lasciare l'impostazione di base, che permette anche agli "amici degli amici" di vedere le nostre foto, porta in definitiva al fatto che ne abbiamo perso del tutto la gestione: anche usando politiche estremamente rigorose di concessione delle "amicizie" non potremo mai sapere con certezza chi siano gli amici dei nostri amici.

Capitolo a parte deve essere dedicato alle trappole. In Facebook, ad esempio, è possibile creare delle "pagine", ossia qualcosa di simile ad un normale profilo, non legato obbligatoriamente ad una specifica persona. Vi sono le pagine dei fan dei personaggi dei fumetti, degli appassionati di un piatto particolare, di un modo di dire, e via così. Per diventare fan occorre dare la propria adesione volontaria, usando il pulsante *Mi piace* (nella versione in inglese è *Like*).

Esistono pagine trappola: di solito hanno un nome che fa leva sulla curiosità e su sentimenti di sdegno, disgusto, condanna e, naturalmente, sul sesso. Qualche esempio: pagine dal titolo "Incredibile! Guardate cosa fa questa ragazza in discoteca!", "Nessuno riesce a guardare questo video per più di 20 secondi!", "Guardate come è diventato questo big mac dopo due settimane!!" e via così. In tutti i casi per poter accedere al contenuto fonte di tanta emozione occorre dare il *Like* alla pagina. E qui scatta la trappola: il *Like* in realtà provoca l'aggiunta di questa pagina ai nostri interessi e la segnalazione ai nostri amici, tramite un

messaggio di stato sulla nostra bacheca, che li induce a seguire il link ed a cadere nella stessa trappola. In altri casi, la trappola appare sotto forma di un link ad un video, che porta in realtà ad una applicazione trappola, autorizzandola ad accedere al nostro profilo, quindi a tutti i nostri dati. Ci sono pagine che in breve tempo hanno superato il mezzo milione di *Like*. Ne hanno parlato alcune società<sup>7</sup> di sicurezza<sup>8</sup> e Paolo Attivissimo<sup>9</sup> nel suo sito<sup>10</sup>.

Autorizzare una applicazione equivale a lasciarle libero accesso a tutti i nostri dati. Possiamo star certi che quelli che hanno approntato applicazione e trappola non ne faranno un uso benevolo.



### Ecosistemi e parassiti

Esattamente come in natura, quando il numero di individui in un qualsiasi aggregato, come gli utenti di un servizio, supera un certo livello, il tutto assume le caratteristiche di un ecosistema: alcuni individui si specializzano nel sopravvivere a spese di quella parte della popolazione che ha caratteristiche “adatte” a cadere vittima di predazione o parassitosi. I truffatori si nutrono di soldi, i *troll* delle reazioni alle provocazioni, gli *stalker* della sofferenza delle proprie vittime.

La somiglianza non è solo apparente. Esistono varie scienze che si occupano dei fenomeni legati ad aggregazioni di individui, dalla Psicologia di Comunità all'Ecologia per finire con le teorie sui sistemi caotici e sui comportamenti emergenti.

Per questo motivo, probabilmente, nelle comunità online si sta bene quando si è pochi ed i problemi iniziano ad apparire quando c'è abbastanza “cibo” per i parassiti.

Personalmente, ho avuto un account Facebook per alcuni mesi. Dopo l'ennesimo cambiamento di regole per la gestione della riservatezza delle

7. <http://thompson.blog.avg.com/2010/07/remote-control-facebook.html>

8. <http://nakedsecurity.sophos.com/2010/05/31/viral-clickjacking-like-worm-hits-facebook-users/>

9. <http://attivissimo.blogspot.com/2010/07/facebook-qualche-trappola-da-evitare.html>

10. <http://attivissimo.blogspot.com/2010/06/facebook-oltre-100000-vittime-del.html>

proprie informazioni, totalmente arbitrario e imposto dall'alto, e l'introduzione dell'ennesima "feature" che sembrava pensata deliberatamente per diffondere ulteriori fatti personali, ho deciso di staccare la spina. Non ho perso un solo contatto, non ho perso amici, meno che mai ho perso occasioni di alcun genere.

## Servizi 2.0 con fregatura 1.0

Seguendo il paradigma del cosiddetto *Web 2.0*, molti sono i siti web che offrono servizi gratuiti, i più disparati: ritoccare foto, gestire mailing list, connettersi al proprio computer di casa dall'ufficio, condividere file di grandi dimensioni, inviare messaggi cifrati, raccogliere firme per una petizione, convertire il formato dei file, e chi più ne ha.

Tutto sempre, rigorosamente, gratis. E, come sempre, noi invece ci facciamo la domanda di rito: cosa ci guadagnano oltre la gloria, che come sappiamo non riempie la pancia?

Torniamo al nostro assunto: ogni informazione ha un valore. Per fruire un servizio di questo tipo, nella quasi totalità dei casi, ci viene chiesto di fornire qualche dato personale, il minimo è un indirizzo di posta elettronica.

In pratica, chi voglia operare una raccolta di indirizzi di posta elettronica verificati, si inventa un bel sito web, tutto colorato e pieno di animazioni ed effetti, che offra una qualsiasi funzione gratuitamente, anche la più semplice: togliere gli occhi rossi dalle foto col flash, fare caricature dalle nostre foto, convertire un file da un formato all'altro. Basta caricare il file, inserire il nostro indirizzo di posta elettronica (valido e funzionante, se vogliamo ricevere il file col risultato), ed in breve riceveremo il file voluto, mentre chi ha creato il sito avrà un indirizzo di posta elettronica valido e verificato. Se poi vuole fare le cose per benino, offrirà la possibilità di pubblicare la foto su un qualsiasi *social network*, basta fornire le nostre credenziali di accesso.

Per capirci: qualsiasi dato noi digitiamo in una pagina di un sito web, quale esso sia, una volta inviato al server (e non c'è bisogno di premere un pulsante per farlo, state pur certi) *non è più sotto il nostro controllo*, e non vi è alcun modo per sapere se e come sarà impiegato.

Quindi, se anche solo fornire un indirizzo e-mail è poco consigliabile, figuriamoci usare le *nostre* credenziali di accesso ad un altro sito.

Di esempi del genere è pieno il web, e i siti che offrono servizi con simili modalità sono innumerevoli. Ovviamente, questo non vuol dire che *tutti* siano collettori di dati personali, quello che però dobbiamo sempre chiederci è se il gioco vale il prezzo: quanto vale il nostro indirizzo e-mail?

Se per ritoccare una foto ci viene chiesto l'indirizzo di posta elettronica, basta cercare un altro sito che offra lo stesso servizio senza chiedere niente in cambio. Non è difficile trovarne, basta cercarli.

## Il mio regno per una password

Posta elettronica, foto online, social network, acquisti in Rete, ormai chiunque usi Internet da qualche mese ha almeno quattro differenti accessi ad altrettanti servizi. Per ognuno di essi ci viene chiesto di creare una password, che poi dovremo ricordarci, naturalmente.

Questo apre la porta a una serie di problemi, diretti ed indiretti. Primo fra tutti, ricordarle, le password, con le relative le associazioni password-sito.

Se siete arrivati a leggere fin qua, avrete compreso che spesso le soluzioni proposte in questo libro sono controcorrente, e in un certo "eretico". Ragioniamo sopra questa storia delle password:

- Siti differenti, password differenti. Per quanto possa essere scoccante e fastidioso, occorre usare una password differente per ogni sito. I motivi sono essenzialmente due. Il primo è che se ci venisse sottratta una password (anche qualcuno che guarda da sopra le spalle può farlo, e non deve essere un *hacker* per forza...), la password sarà applicabile solo per il sito corrispondente.

Il secondo motivo è più difficile da spiegare, ed implica alcune conoscenze sul funzionamento delle applicazioni dei siti web. Le password vengono memorizzate usando un meccanismo di *hash*, per cui, in teoria, è impossibile risalire alla password avendo l'*hash*. Se però la password non è adeguatamente complessa, o si basa su un termine a dizionario, esiste un metodo che permette



di risalire alla password conoscendo l'*hash*, sfruttando le cosiddette *rainbow tables*<sup>11</sup>, ossia una sorta di database di *hash* con associata la password che lo genera. Se l'applicazione web non usa dei metodi per rendere meno efficace l'uso delle *rainbow tables*, chiunque riesca a mettere le mani sul database degli utenti (è meno difficile di quanto si possa pensare) potrebbe avere in mano la chiave di accesso a tutte le nostre attività in Rete, se la stessa password la usassimo per tutto.

- Password non prevedibili e complicate quanto basta. Sul web valgono le stesse regole che a suo tempo vedemmo nel libro precedente, nel capitolo “La seconda linea di difesa bis: password” a pagina 31. E' certamente vero che gli attacchi a dizionario o esaustivi sul web sono più difficili da realizzare, e potrebbero essere più facilmente rilevati per l'intensa attività generata dall'attacco, ma quando l'attaccante riesca a trafugare il database delle password del sito, l'attacco è infinitamente più fattibile, e destinato ad avere successo in gran parte dei casi, proprio a causa della scelta poco ragionata delle password. Per questo motivo è importante scegliere con cognizione di causa qualsiasi password da usare in Rete. Soprattutto quella usata per la posta elettronica, che sta diventando il servizio più importante di tutti.
- Non memorizzare le password nel computer, mai. Abbiamo tre modi possibili di memorizzare una password nel nostro computer: scriverla in un file, usare la funzione di memorizzazione password del browser o impiegare uno di quei programmi per la gestione disponibili in Rete. In tutti e tre i casi un malware potrebbe in un colpo solo rubarci tutte le password: se sono in un file, quando lo apriamo per leggerlo un malware come Zbot può prendere uno *screenshot*; se sono nel browser o in un programma tutto sta nella robustezza della password scelta per proteggere le altre, la “master password”. In ogni caso un malware potrebbe portarsi a casa i file e poi applicarvi con comodo un attacco alla fine del quale avrebbe in mano tutte le nostre password.

La cosa più semplice è *scrivere su un foglietto da mettere nel portafogli*. Assurdo? Pazzesco? Quanto è più probabile essere colpiti da un malware rispetto all'essere derubati da qualcuno che non sia interessato ai soldi ed alle carte di credito ma sappia come utilizzare un foglietto con cinque-sei parole prive di senso?

---

11. [http://it.wikipedia.org/wiki/Tabella\\_arcobaleno](http://it.wikipedia.org/wiki/Tabella_arcobaleno)

Naturalmente, non dobbiamo scrivere sullo stesso foglietto *a cosa appartengono le password*, altrimenti è inutile. Se, per un malaugurato evento, ci dovessero rubare il portafogli *sapremmo immediatamente* che qualcuno ha in mano le nostre password, ed avremmo il tempo di correre ai ripari, cambiandole.

Se invece teniamo le password nel computer, potrebbero passare giorni prima di accorgerci della presenza di un malware, messo lì *con lo scopo di rubare informazioni*.

La stessa Microsoft<sup>12</sup>, in uno dei suoi scritti sulla sicurezza e la riservatezza, afferma: “Le password sono più al sicuro da Internet se scritte su un pezzo di carta piuttosto che memorizzate in un software di gestione delle password, su un sito Web o con altri strumenti di memorizzazione.”

In un panorama dove lo scopo principale dei malware in circolazione è il furto di informazioni, dove siamo sempre più tutti connessi, dove sempre più le nostre informazioni sono affidate alla Rete, oltre che al nostro computer, forse il posto più sicuro torna ad essere il mattone, sotto il quale nascondere le chiavi di accesso.

## Una spia in tasca

Per poche decine di euro è possibile acquistare un telefono cellulare sofisticato (uno *smartphone*), dotato di fotocamera e di ricevitore GPS.

L'accoppiamento di questi due strumenti è micidiale per i nostri fatti privati, ma viene commercializzato, naturalmente, in modo che il telefono che non possieda tali funzioni è da scartare perché arretrato. Vediamo: “Scatta le tue foto e pubblicale su tutti i *social network* più noti del momento, in un clic!”. Oppure: “Basta con le foto che non ricordi dove le hai scattate: il telefono inserisce automaticamente nella foto data, ora e luogo in cui è stata ripresa!”.

Come questo sia possibile, è facile da spiegare per chi conosca un minimo i formati per memorizzare le immagini: nel formato JPEG<sup>13</sup>, utilizzato da praticamente tutte le fotocamere, comprese quelle nei telefoni cellulari, è possibile

12. <http://www.microsoft.com/italy/athome/security/privacy/password.msp>

13. <http://it.wikipedia.org/wiki/JPEG>

includere una quantità di dati relativi alla foto, alla fotocamera ed alla posizione geografica in cui la ripresa viene fatta, grazie a Exif<sup>14</sup>.

Nel momento in cui la foto viene scattata, la fotocamera inserisce informazioni su sé stessa (marca, modello, condizioni di funzionamento), sulla foto (data e ora, caratteristiche dell'esposizione) e, se dotata di GPS, coordinate geografiche esatte della ripresa. In alcuni modelli evoluti viene inserito anche il numero di serie della fotocamera, arrivando ad identificare *uno specifico esemplare di quel modello*.

Tradotto: la foto si porta appresso dati che permettono di identificare in modo quasi certo il proprietario. Il peggio deve ancora venire: tutta l'enfasi nella commercializzazione di questi aggeggi è sul mostrare ai propri amici sul *social network* di turno dove siamo stati in vacanza in modo automatico. Scatta la foto ed il tuo aggeggino farà il resto, includendo tutte le informazioni indispensabili e inviandolo alla tua pagina personale: in un colpo solo si manda al diavolo riservatezza e sicurezza, comunicando al mondo chi siamo e dove siamo.



### **Geolocalizzazione**

Questa caratteristica di individuare la posizione geografica di un oggetto (un telefonino, una fotografia, un veicolo) si chiama appunto geolocalizzazione<sup>15</sup>.

Visto che la precisione dei ricevitori GPS è praticamente di metri, significa che se scattiamo una foto in casa nostra e la pubblichiamo con i dati intatti, chiunque può accedervi *saprà dove abitiamo*.

Al di là delle iperboli pubblicitarie, basta indagare un po' per scoprire che è sì possibile disabilitare l'inserimento di queste informazioni nelle foto, come pure è possibile configurare la maggior parte dei *social network* per scartarle, ma occorre una azione specifica preventiva da parte dell'utente, dato che nella maggior parte dei casi queste informazioni sono a priori inserite dai dispositivi che generano foto e mantenute dai servizi in Rete, se l'utente non specifica diversamente.

14. [http://it.wikipedia.org/wiki/Exchangeable\\_image\\_file\\_format](http://it.wikipedia.org/wiki/Exchangeable_image_file_format)

15. <http://it.wikipedia.org/wiki/Geolocalizzazione>

Se poi possediamo un sito personale autogestito, l'attenzione deve essere maggiore nel momento in cui pubblichiamo foto e filmati, perché normalmente i software per i siti personali non possiedono controlli specifici per questo tipo di informazioni.

Facendo un giretto sui principali *social network* e sui servizi di pubblicazione delle foto (Flickr, Picasa, ecc.) è abbastanza comune imbattersi in foto con i dati Exif intatti.



### **Modificare la foto non modifica i dati Exif**

Non è detto che operando delle modifiche alle foto i dati Exif siano persi, anzi. Molti software di fotoritocco non toccano affatto questi dati, e qualunque operazione si applichi alla foto (rotazione, taglio, riduzione, rimozione dettagli, applicazione di filtri, ...) non modifica in alcun modo i dati Exif.

Quasi tutti i software possiedono una qualche forma di controllo di questi dati, anche se non ne permettono la modifica, consentendo all'utente di scegliere se mantenere o eliminare del tutto i dati. Per rimanere sul software libero, GIMP<sup>16</sup> consente di eliminare i dati Exif al momento del salvataggio di una immagine, che altrimenti rimangono intatti.

L'esame dei dati Exif di una foto digitale viene usato comunemente nei casi in cui si voglia indagare sulla storia di una foto, ad esempio per capire se è stata scattata da una persona in particolare, o se è stata modificata successivamente: fra i dati vi è spesso una miniatura della ripresa originale.

Paolo Attivissimo ne ha parlato nel suo blog all'inizio del 2010<sup>17</sup>, evidenziando i pericoli e le trappole subdole che questa tecnologia nasconde.

Le cose sono destinate a peggiorare, vista la sempre maggiore pervasività della tecnologia e il suo sempre minore costo. Ricevitori GPS sono inseriti ormai in dispositivi con prezzo intorno ai cento euro, ed il costo scenderà ancora. Sempre più *social network* offrono la possibilità di sfruttare queste informazioni

---

16. <http://www.gimp.org/>

17. <http://attivissimo.blogspot.com/2010/03/attenti-alle-foto-con-coordinate-gps.html>

(vedi ad esempio FourSquare<sup>18</sup> e Facebook Places<sup>19</sup>), non sempre con implicazioni chiare ai più.

## Un file è per sempre

Un argomento, più di ogni altro, mostra la profonda rivoluzione che la Rete ha portato e, insieme, quanto poche persone ne abbiano piena coscienza: il cosiddetto diritto all'oblio. La voce corrispondente in Wikipedia<sup>20</sup> non è molto dettagliata nel momento in cui scrivo, ma c'è un link ad un articolo molto più esaustivo, anche se un po' difficile da leggere, sul sito Difesa dell'Informazione<sup>21</sup>. Detto in parole povere, è il diritto per ogni persona a vedere dimenticata sé stessa e fatti che la riguardano, diventati di dominio pubblico, ad esempio per essere stata oggetto di vicende di cronaca o giudiziarie. E' ritenuto talmente importante da essere annoverato fra quei *diritti inviolabili dell'uomo* citati nel secondo articolo della Costituzione della Repubblica Italiana.

Su Internet, questo diritto ha qualche problema ad essere rispettato, proprio per la natura diffusa, capillare e fuori dalla dimensione temporale della Rete. Pubblicare una foto su un qualsiasi sito web accessibile al pubblico significa perdere il controllo per sempre. La foto può essere duplicata all'infinito, modificata, ripubblicata per decenni, senza che sia possibile intervenire minimamente sul fenomeno.

A giudicare dalla quantità di foto di gente ubriaca fotografata da amici, o dalla quantità di filmati di ragazzi oggetto di scherzi in giro per Internet, non sembra un problema molto sentito.

Eppure, una delle tante piccole truffe che girano in Rete<sup>22</sup>, per fare un esempio, utilizza foto che incaute ragazzine si sono scattate in abbigliamento "ridotto" ed hanno pubblicato su qualche *social network* affidandosi alla misera protezione data dall'accesso "riservato ai soli amici", che equivale a stamparne cento milioni

---

18. <http://foursquare.com/>

19. <http://www.facebook.com/places/>

20. [http://it.wikipedia.org/wiki/Diritto\\_all%27oblio](http://it.wikipedia.org/wiki/Diritto_all%27oblio)

21. <http://www.difesadellinformazione.com/113/il-diritto-all-oblio/>

22. <http://protezioneaccount.blogspot.com/2010/06/la-mia-ragazza-mi-ha-traditoe-questa-la.html>

di copie ed a fare volantinaggio da un aereo sopra tutte le capitali europee. La truffa si basa al solito su una semplice operazione di *social engineering*: sotto la frase “La mia ragazza mi ha tradito... e questa è la mia vendetta!”, seguita da un raccontino abbastanza scontato, vi è una immagine di una ragazza molto giovane mentre si scatta una foto, tipicamente da un cellulare, e la promessa: guardatevi pure le sue foto nuda!

La truffa esiste in parecchie versioni, in cui cambiano nomi e foto. Quelle foto vengono proprio dalla totale ignoranza di questo aspetto di persistenza in Rete.

Se cercate il mio nome con un qualsiasi motore di ricerca, troverete tracce della mia attività su Internet che risalgono al 2000, e non si tratta di cose “interessanti” come una fanciulla poco vestita... Fatte le dovute proporzioni, immaginiamo quanti anni possa persistere una foto particolarmente “appetibile” in giro per la Rete.

Il tutto riguarda *qualsiasi tipo di informazione*, sotto qualsiasi forma, sia divulgata su Internet. Alcuni ricorderanno il caso dei file con tutti i dati di reddito<sup>23</sup> pubblicati incautamente dall’Agenzia delle Entrate nell’aprile del 2008<sup>24</sup> per poche ore e poi immediatamente ritirati. In quelle poche ore i file sono finiti sui principali circuiti *peer to peer* e sono ancora lì: una ricerca fatta nei primi giorni del 2011, a distanza di quasi tre anni, elenca alcune centinaia di file relativi all’elenco, da quelli completi a quelli riguardanti una sola provincia.

Oppure il caso del ricercatore di sicurezza<sup>25</sup> che aveva scaricato i dati di *cento milioni* di profili utente da Facebook<sup>26</sup>, ed il file era “finito” sui circuiti *peer to peer*, dove è ancora tranquillamente reperibile.



### **Vale anche per gli insulti**

A maggior ragione, quanto detto vale per gli insulti, siano essi scritti nel

23. <http://www.rainews24.rai.it/it/news.php?newsid=81390>

24. [http://www.corriere.it/economia/08\\_aprile\\_30/fisco\\_redditi\\_internet\\_916ff390-1694-11dd-8b67-00144f02aabc.shtml](http://www.corriere.it/economia/08_aprile_30/fisco_redditi_internet_916ff390-1694-11dd-8b67-00144f02aabc.shtml)

25. <http://www.skullsecurity.org/blog/2010/return-of-the-facebook-snatchers>

26. <http://www.itespresso.it/28-gb-di-privacy-violati-cento-milioni-di-utenti-di-facebook-su-bittorrent-47303.html>

nostro sito, nel nostro *social network* preferito, come commento a qualcosa scritto da altri o come messaggio in forum pubblici.

Con la differenza che insultare qualcuno su Internet è sì reato come insultarlo nel mondo fisico, ma l'insulto rimane scritto per un tempo indefinito e leggibile da chiunque passi di là, a differenza dell'evento nel mondo reale, dove l'insulto lo senti solo se sei presente *in quel preciso istante*. Quindi le probabilità di far arrabbiare qualcuno sono infinitamente più alte. Tenendo conto di quanto detto sull'anonimato in Internet (vedi Sezione *BitTorrent Vs eMule* nel Capitolo 7), è anche abbastanza scontato che l'insulto sia associato correttamente all'autore, con tutte le conseguenze del caso. Perciò, attenzione a cosa si scrive *in qualsiasi posto di Internet*. Inoltre, un insulto o uno scritto denigratorio pubblicato su Internet viene assimilato in molti casi al reato di diffamazione, molto più grave della semplice ingiuria.

Quindi, se non possiamo fare a meno di esibirci per sfogare i nostri irrefrenabili impulsi "artistici", prima di pubblicare qualsiasi cosa, in qualsiasi posto di Internet, ragioniamo un attimo: andiamo a fare un colloquio di lavoro ed il nostro futuro capo sta ammirando il nostro prodotto sul suo monitor *full-hd* da 42 pollici. Se immaginare questa situazione ci imbarazza, allora è il caso di verificare se la prodezza sia chiaramente riconducibile a noi, e nel caso soprassedere.

## L'assenza di prove è una prova

Dai fatti dell'undici settembre 2001, alle scie di condensazione lasciate dagli aerei, alle missioni lunari Apollo, ogni avvenimento o fenomeno universalmente noto è preso di mira dai teorici del *Grande Complotto*, che trovano in Internet il terreno migliore dove esporre le teorie e le presunte prove di incredibili ed enormi macchinazioni ad opera delle entità più disparate.

Non importa quanto bislacca sia la teoria, non importa quanto sia inverosimile, non importa che esistano prove a sostegno del contrario, come non esistano prove a favore, c'è sempre pronta una risposta a tutte le obiezioni. E quando la risposta non c'è, ecco partire l'attacco alla persona che muove i rilievi al complotista di turno.

Paolo Attivissimo<sup>27</sup> (credo che gli dovrò una parte del successo di questo libro, se mai neavrà), con il suo servizio “Antibufala”, indaga sulle più note teorie, e puntualmente viene preso di mira con argomentazioni più vicine a quelle che userebbe un credente a cui si vanno a toccare i dogmi di fede, piuttosto che con costrutti sensati e fondati su prove verificabili.

L’obiezione, tautologica, che i complottisti muovono a chi fa notare l’assenza di prove è che “l’assenza di prove è una prova” dell’esistenza complotto stesso, nella sottintesa conseguenza che gli autori del complotto siano talmente potenti e capillarmente presenti da controllare tutte le possibili fughe di notizie e le fonti in modo talmente perfetto da non riuscire a trovare neanche una prova diretta, solo indizi.

Non è facile per niente combattere questo fenomeno, che in più occasioni ha avuto anche ricadute economiche, vedi il caso delle sostanze chimiche schiumogene<sup>28</sup> presenti in una serie di dentifrici e prodotti per la cura della persona. Il messaggio di fondo era: questi prodotti sono cancerogeni. Peccato che, mentre è stata accertata la possibilità di irritazioni (possibilità presente *per qualsiasi cosa entri in contatto con il nostro corpo*), mai è stata dimostrata una relazione con tumori di alcun tipo. Eppure i produttori sono stati costretti a eliminarli da molti cosmetici, ed a cercare dei sostituti. Con il rischio, neanche tanto lontano, di sostituire sostanze i cui effetti sono noti ed accertati, oltre che minimi, con sostanze di cui poco si conosce.



### **Cosa si guadagna ad inventare complotti?**

Sicuramente, se il “complotto” è sufficientemente intrigante, vi è il consistente “rischio” di essere chiamati da giornali, radio o televisioni per raccontare nei dettagli presunti fatti e presunte prove del *Grande Complotto*.

A parte le trasmissioni televisive e radiofoniche specificamente dedicate a questi argomenti, basta andare sui siti web dei complottisti più noti per vedere che spesso sono più ricercati di chi invece tenta di smentirli.

---

27. <http://attivissimo.blogspot.com/>

28. [http://www.attivissimo.net/antibufala/sls/dentifrici\\_cancerogeni.htm](http://www.attivissimo.net/antibufala/sls/dentifrici_cancerogeni.htm)



Lo stesso Paolo parla della *metafora della montagna di merda*: creare un mucchio di escrementi richiede infinitamente meno sforzo e fastidio di quanto ce ne voglia a smaltirlo. Questo è l'effetto delle varie teorie complottiste: basta poco a crearle (soprattutto l'ignoranza), ma ci vuole tempo e tanto impegno per smontarle.

E' tempo di smettere di credere *a vista* a qualsiasi cosa si legga su Internet.

## Crimini reali nel mondo virtuale

Il fatto che Internet sia un mondo virtuale non deve ingannarci: le azioni ivi compiute hanno ricadute sul mondo reale, e non sono meno importanti.

Nel novembre 2010<sup>29</sup> l'FBI ha arrestato un trentunenne con l'accusa di estorsione dopo *due anni* di indagini. Il tipo impersonava amiche di ragazze molto giovani e le induceva a vedere un video pauroso, inviato come allegato in posta elettronica o offerto via *social network* o chat. Il file era in realtà un malware che prendeva il controllo del computer della vittima, operando come "telecontrollo". Se nel computer trovava foto e video personali della vittima, le usava come arma di ricatto per ottenerne altre, naturalmente in pose "specifiche". Se il computer aveva una webcam collegata, veniva utilizzata per riprendere di nascosto le vittime nell'intimità della propria camera, ed ancora foto e filmati erano utilizzati per ricattare le vittime ed ottenerne di più.

Sempre nel 2010, da noi, la Polizia Postale ha arrestato un ventottenne<sup>30</sup> che attraverso un noto *social network* contattava ragazzine con la scusa della selezione per la campagna pubblicitaria dei costumi di un noto personaggio per bambini. Peccato che poi le facesse spogliare e le fotografasse in pose erotiche. In casa del tipo la Polizia ha trovato una quantità ingente di materiale, segno che tanti genitori erano caduti nell'inganno senza sospettare alcunché.

In un altro caso, un marito tradito ha pensato bene di tirar su qualche soldino mettendo su un sito creato appositamente foto e filmati intimi della moglie fedifraga, raccogliendo poi "testimonianze" di altri mariti e fidanzati traditi, per

29. <http://attivissimo.blogspot.com/2010/11/estorsione-sessuale-via-web-arresto.html>

30. [http://bologna.repubblica.it/cronaca/2011/01/05/news/emilia\\_attenzione\\_alle\\_trappole\\_online\\_dai\\_mariti\\_traditi\\_al\\_falso\\_casting\\_hello\\_kitty-10874004/](http://bologna.repubblica.it/cronaca/2011/01/05/news/emilia_attenzione_alle_trappole_online_dai_mariti_traditi_al_falso_casting_hello_kitty-10874004/)

vendetta, e mettendo a disposizione il materiale a chiunque, dietro pagamento di poche decine di euro come “abbonamento”.

Per commettere questi reati, i protagonisti non hanno avuto bisogno di essere esperti di computer, né particolarmente astuti. Tanto è che non sono criminali già noti alle forze dell’ordine, ma tutti incensurati. Il fatto che in tanti ci siano caduti dimostra sia che la percezione di quello che si fa in Internet sia in qualche modo “distante” da noi, sia che il livello di diffidenza è molto inferiore, probabilmente perché manca il contatto diretto. Nessuno di noi accetterebbe di far posare la figlia in costume da bagno con uno incontrato per strada, mentre se il tipo contatta la figlia via Internet il tutto assume una forma di ufficialità che fa sottovalutare le implicazioni della situazione.

## Bello perché vario, forse troppo

Come ho già detto qualche paragrafo fa, ogni aggregato, reale o virtuale che sia, quando superi una certa dimensione mostra la comparsa spontanea di “forme di vita” la cui sopravvivenza è strettamente legata alla consistenza ed alla composizione dell’aggregato.

Detto in altri termini: i truffatori compaiono solo quando c’è abbastanza gente da truffare e le truffe che è possibile portare a termine sono in numero e valore tale da valerne la pena.

Sono forme parassitiche, e tipicamente richiedono che l’aggregato di cui fanno parte sia sufficientemente grande. Alcuni esempi:

- Spam e spammer. La pubblicità è l’anima del commercio, ma quando è capillare e onnipresente forse stanca un po’. Ogni *social network*, ogni comunità virtuale esistente, ogni piattaforma ed ogni applicazione è affetta in varia misura dalla pubblicità parassita, tanto più utenti vi sono, tanto più è presente lo spam.
- Troll e provocatori. Il *troll* non è quello nei racconti di Tolkien<sup>31</sup>, si riferisce alla pesca fatta prima buttando esca a secchiate in acqua, poi passando con la rete a traino, modalità chiamata in inglese *trolling*, appunto. Il troll è un provocatore,

---

31. [http://it.wikipedia.org/wiki/John\\_Ronald\\_Reuel\\_Tolkien](http://it.wikipedia.org/wiki/John_Ronald_Reuel_Tolkien)

un professionista nello scatenare discussioni accesissime e battaglie a suon di commenti in forum e blog. Discussioni che nella totalità dei casi niente hanno a che fare con l'argomento che in teoria le avrebbe scatenate, e che come scopo hanno proprio quello di allontanare l'attenzione dall'argomento stesso.

- Persecutori e stalker. A differenza dei troll, i persecutori si concentrano su un solo bersaglio, persona o sito web che sia. Il fastidio può andare dal commento puntuale ad ogni nuova aggiunta sul blog della vittima alla persecuzione vera e propria, senza la necessità di attività della vittima, con e-mail, messaggi nei vari *social network*, forum, chat. La persecuzione può migrare dal mondo virtuale a quello reale, diventando una fonte di preoccupazione. Oppure, molto più spesso, il persecutore si sposta su Internet trovando terreno facile per denigrare e danneggiare la vittima, pensando di essere "protetto" dal presunto anonimato, cosa che sappiamo essere un pio desiderio (vedi Sezione *BitTorrent Vs eMule* nel Capitolo 7).

La fauna presente in Internet è molto varia, e rappresenta tutte le possibili varianti della persona umana, da tutti i punti di vista. Ne vengono quindi rappresentati anche gli estremi, nel bene e nel male.

Una volta capito questo, si può smettere di demonizzare lo strumento (Internet appunto), e iniziare a dare il giusto valore alle cose. Che in ogni caso non deve farci dimenticare la presenza di chi in qualsiasi modo tenta di trarre profitto da qualunque cosa, e ad ogni costo.

## I milioni son fatti di centesimi

Anche di questo avevo parlato a suo tempo nel mio blog<sup>32</sup>, ma riassumo per praticità. Ci si imbatte spesso in pubblicità su vari siti web, in particolare quelli dedicati ai videogames, che mostrano proprio giochi con le ambientazioni più varie. In tutte le pubblicità campeggia in bella mostra la parola "gratis", in tutte le sue declinazioni.

Al netto delle tecnologie impiegate, che sono in generale collaudate e note, quindi niente di nuovo, il meccanismo del gioco ha una doppia personalità: una

---

32. <http://www.ismprofessional.net/pascucci/index.php/2009/09/gioca-e-gratis-piu-o-meno-anzi-no/>

realmente gratuita ed una a pagamento. Naturalmente, nulla obbliga il giocatore a pagare niente, né in modo esplicito, né implicito.

Il meccanismo che induce il giocatore a ricorrere al portafogli è duplice: da un lato vi sono le personalizzazioni, dall'altro la possibilità di progredire nei vari livelli del gioco.

In altre parole, se si tratta ad esempio di un gioco a tema spaziale, la nostra astronave ha una dotazione standard, nome, forma e colore predefiniti. Se invece è a tema bellico, il nostro soldato avrà uniforme, stemma e dotazione assolutamente standard. Se vogliamo dare un nome personalizzato alla navicella, colorarla di rosso, far indossare al nostro soldato una mimetica o usare una differente forma del mirino a video dobbiamo acquistare la personalizzazione. L'acquisto si perfeziona usando una moneta virtuale, che si acquisisce in due modi: giocando o acquistandola con denaro reale.

Per acquistare la moneta virtuale vi è un vero e proprio tasso di cambio, tipicamente un euro per mille "crediti" del gioco. Mille crediti possono sembrare tanti, ma basta scorrere il "listino prezzi" per capire che ci si fa ben poco: cambiare il colore di un dettaglio del personaggio può costare alcune migliaia di crediti, acquistare le munizioni sufficienti per una sola missione, altrettanto.

Di solito, la parte iniziale del gioco è pienamente fruibile senza spendere un euro. Le prime missioni sono abbastanza impegnative da stimolare la competizione, ma abbastanza facili da non scoraggiare il giocatore. Una volta che ci si prende gusto, però, i livelli successivi sono un po' più difficili, e diventa sempre più necessario il ricorso all'acquisto di potenziamenti. Ecco che mettere mano al portafogli diventa facile.

Difficile diventa smettere: al termine di una sessione di gioco è facile spendere alcune decine di euro, senza rendersene conto. Questo è il meccanismo che qualcuno ha definito<sup>33</sup> "il marketing di un caffè al giorno".

Sia chiaro a tutti: nessuno fa nulla di illegale. Assolutamente no. Le clausole sono chiaramente indicate nel testo che appare all'atto di accettare la partecipazione al gioco, e niente viene fatto di nascosto o con la forza. Anzi, è illegale tentare di forzare il software o il server che lo gestisce per ottenere dei vantaggi.

---

33. <http://personalitaconfusa.splinder.com/post/21145855#21145855>

Anche qui si tratta soltanto di tecniche di marketing, magari non particolarmente aggressive, ma possono diventare pericolose se chi gioca è un bambino con disponibilità di denaro. Quindi massima attenzione, al solito, alla parola gratis.

## Cuccagna? Mah...

Chiudiamo qui questo capitolo denso di informazioni. Ce ne sarebbe ancora per un ulteriore libro, e nel momento in cui leggerete questo, di libro, molte altre ne verranno fuori di trappole. E' una rincorsa impari, ma, per fortuna, c'è una chiave di lettura che può aiutarci a discriminare comportamenti pericolosi e trappole.

Il primo pensiero che ci deve guidare sempre è: mai dare troppe informazioni. Mai. Se per scaricare una suoneria ci viene chiesto il numero di cellulare, possiamo star certi che vi sia qualcosa sotto, "chiaramente" riportato nei termini di utilizzo del servizio, scritti in carattere lillipuziano, in perfetto burocratese: all'esaurimento del credito telefonico avremo poco di cui lamentarci. Se per accedere ad un servizio qualsiasi, dobbiamo fornire la data di nascita, dobbiamo diffidare. Se andiamo a pubblicare una foto, dobbiamo chiederci se può essere usata contro di noi, o se la foto non contenga troppe informazioni, non solo nascoste nei dati EXIF.

Il secondo pensiero deve essere "tu chi diavolo sei?". Internet è un luogo privo di controlli, e tale *deve* rimanere. Ma proprio per questo motivo ogni singola affermazione, notizia e informazione deve essere verificata e trattata fin dall'inizio come "da verificare". E' questi giorni la notizia della morte di Osama Bin Laden per mano delle forze speciali statunitensi, e le ripetute gaffe di giornali e giornalisti con la pubblicazione di foto taroccate dimostra al di là di ogni necessità di come ogni singola informazione sia passibile di smentita, anche quando venga da fonti "affidabili" (non metto volontariamente i link perché gli articoli contengono tutti foto dal contenuto orribile a vedersi).

Un po' di sano scetticismo è la migliore arma di difesa. L'unica su Internet.

## Capitolo 10. Gestisco un sito web, io!

E' facile, alla portata di chiunque, al punto che proprio *chiunque* si improvvisa webmaster. Sarebbe da chiarire prima quali siano i compiti di chi gestisce un sito web. E no, la grafica c'entra assai poco.

Acquisire uno spazio web e metterci il sito è alla portata di qualsiasi tasca, anche quelle vuote. Ma, parlando in questi termini, stiamo riducendo tutto ad una mera questione pecuniaria. Non è così, e molti ne hanno fatto le spese, per fortuna quasi sempre senza gravi conseguenze, fino ad ora almeno.

### Non costa niente, non subito, almeno...

Lo sappiamo tutti, ormai: essere presenti in Rete non costa praticamente nulla. A partire dallo spazio web, passando per la registrazione del nome del sito, per finire con la scelta dell'applicazione da usare per creare e pubblicare i contenuti, tutto può essere fatto con una manciata di euro, o del tutto gratis se si rinuncia a qualcosa.

A parte il non trascurabile dettaglio di *cosa* mettere sul sito, il resto è alla portata di chiunque sappia usare un po' il computer, niente di più.

Chi vuole fare le cose professionalmente si affida ad una società di marketing sul web, una *web-agency*. Ci si preoccupa dell'aspetto grafico, dei contenuti, dell'indicizzazione del sito da parte dei principali motori di ricerca, della pubblicità da accogliere sulla prima pagina, della promozione sui principali *social network*, della rilevazione delle statistiche sulle visite e sui "click".

La sicurezza è una postilla, un ripensamento tardivo nel contratto, aggiunto in fretta, che si rivolge quasi esclusivamente alla protezione dei contenuti, che, per inciso, è una contraddizione in termini: se è pubblicato in Internet lo scopo è proprio la più ampia diffusione possibile, e la diffusione passa anche per lo scambio di link, immagini e contenuti fra i visitatori del nostro sito.

Là fuori, purtroppo, una pletora di mentecatti non aspetta altro che siano messi in linea siti web dove la sicurezza è trattata come una postilla, per farne il proprio comodo.

## **Webmaster, in un attimo!**

Vediamo di contestualizzare un po' il discorso. Un sito web, per esistere, deve essere ospitato su un server, su cui vi è uno spazio dedicato allo scopo. Il server non è altro che un normale computer, con caratteristiche particolari per quanto riguarda l'affidabilità e la resistenza ai guasti. Tipicamente, avrà una configurazione di dischi in RAID, il doppio alimentatore, due o più schede di rete, e via così, per ridurre la possibilità di un fermo totale in caso di guasto di uno dei componenti più fragili.

Il software può essere in varie configurazioni. La più comune è quella del cosiddetto "hosting condiviso", dove in un unico server sono ospitati centinaia (a volte migliaia) di siti web differenti ed indipendenti. Il server che ospita il mio sito ne contiene alcune centinaia di altri, i più disparati. Ogni sito ha il suo spazio ed il software del server è pensato per impedire interferenze di qualsiasi sorta fra siti web differenti, pur se ospitati sullo stesso server. A seconda della quantità dello spazio disco disponibile e dei servizi aggiuntivi di cui si fruisce, un tale tipo di sito web può essere del tutto gratuito, o può arrivare a costare un paio di centinaia di euro l'anno.

Una configurazione meno comune, anche perché molto più costosa, è quella del server dedicato, che può essere "fisico", ossia proprio una macchina a noi dedicata, o virtuale, una configurazione in cui un server fisico ospita, tramite un software apposito, un numero consistente di server virtuali, isolati ed indipendenti, indistinguibili da normali computer, che condividono le risorse del computer reale.

Naturalmente, la complessità di gestione dei due casi è totalmente differente: nel primo caso, ossia in "hosting condiviso", la gestione riguarda la scelta ed il mantenimento della sola applicazione web che costituisce il nostro sito e del relativo database; nel secondo caso la gestione è dell'intero server e, come possiamo ben immaginare, è sostanzialmente più complessa e delicata.

Un errore di manovra nel primo caso può essere recuperato al massimo reinstallando l'applicazione web, nel secondo caso potrebbe essere necessario reinstallare a partire dal sistema operativo, o addirittura potrebbe essere necessario un intervento tecnico da parte del servizio di gestione.

Fin qui, stiamo parlando di normale amministrazione, siamo umani e capita di sbagliare, i backup esistono *anche* per questo. I problemi nascono in presenza di problemi di sicurezza, e quello che accade è cosa nota a chi si occupa di questo.

Vi sono numerosi miti da sfatare anche in questo ambito, in primo luogo: *nessun sito web è troppo poco importante per non essere violato*. Esattamente come per i nostri computer, quello che interessa ai mentecatti è proprio il poter disporre di server, puliti e con una buona reputazione, da impiegare per i loro scopi. Naturalmente, la responsabilità di quello che verrà fatto con il server ricadrà su chi crea e gestisce il sito, visto che gli appartiene.

## Demolire le false certezze, al solito

Oltre al fatto che nessun sito è al sicuro, *nessuno*, dobbiamo sgombrare il campo da vari dogmi, che saranno anche utili in altri ambiti della umana esperienza, ma in campo scientifico e tecnologico sono solo un ostacolo al progresso della conoscenza.

## Spam, spam ovunque

Chi ha provato a gestire un blog in proprio se ne è accorto ben presto: non esiste solo lo spam nelle e-mail. Ogni possibile strumento a disposizione di chi gestisce un blog per comunicare con i lettori e con il resto dell'ambiente in Rete è veicolo di una o più forme di spam, tanto che il primo e sovente unico plugin installato in un qualsiasi blog è proprio un filtro per lo spam.

La principale porta d'ingresso allo spam è la possibilità per i visitatori del sito di lasciare commenti agli articoli pubblicati: dato che è consentito a chi commenta l'inserimento di un link al proprio sito web, oltre che l'inserimento di link nel commento stesso, gli spammer infilano secchiate di commenti contenenti secchiate di link, annullando il valore dello scambio di opinioni fra i visitatori del sito.

Altra porta di ingresso sono i cosiddetti *trackback* e *pingback*: quando un altro sito pubblica un articolo che contiene uno o più link ad un nostro articolo, questo viene notificato con uno scambio di dati fra i due siti, direttamente. E' un modo per riconoscere le fonti delle citazioni, e per dare in qualche modo visibilità



alle connessioni fra i vari siti, equivalenti a relazioni di conoscenza e di stima fra persone. Vengono inviati messaggi per notificare un *trackback* da siti che invece non contengono nessun link verso il nostro. Oppure vengono creati interi siti pieni di link ad altri, per evitare alcuni filtri intelligenti, che vanno a verificare che effettivamente i link relativi ai *trackback* ci siano.

L'ultima diavoleria è il cosiddetto *referrer spam*<sup>1</sup>: quando un visitatore del sito A clicca su un link al sito B, il sito B apprende che il visitatore è giunto sul sito grazie al link messo nel sito A. Il sito A è chiamato *referrer*<sup>2</sup> (o *referer*) del sito B. Alcuni siti mostrano appunto un riquadro dove viene esposta la provenienza dei visitatori, un modo per “ringraziare” chi porta visitatori al sito.

Lo scopo di tutti questi trucchi è duplice: il primo è attuare un inquinamento dei database dei motori di ricerca attraverso link che conducono ai siti degli spammer stessi, che normalmente nessuno si sognerebbe di inserire nel proprio sito (il termine tecnico è *spamdexing*<sup>3</sup>); il secondo è pubblicare link verso siti pericolosi per i visitatori in siti web al di sopra di ogni sospetto.

Nel primo caso i motori di ricerca vengono inquinati da questi link fasulli, e quando cerchiamo alcuni particolari termini è possibile che appaiano nelle prime pagine i siti degli spammer, prima di quelli che magari offrono quello che cerchiamo in maniera più onesta ed affidabile: non si tratta solo di vendita di medicinali, ma anche di agenzie che offrono voli economici, auto usate, mutui, case in affitto. Tutto è passibile di essere “pubblicizzato” in questo modo, anche alcuni programmi non proprio utili (vedi Capitolo 8).

Nel secondo caso, il visitatore che segue quel link si trova in un sito web fabbricato appositamente per infilargli un qualche malware nel computer. Inutile dire che a nessuno verrebbe in mente di andare su un sito del genere, ma quando il link parte da un sito affidabile e conosciuto è più difficile che la diffidenza prenda il sopravvento.

Una parte consistente del lavoro di chi gestisce i principali motori di ricerca è proprio il contrasto a queste forme di inquinamento, sempre più sofisticate e sempre più difficili da combattere. Per avere una qualche possibilità in più, in molti

---

1. [http://en.wikipedia.org/wiki/Referrer\\_spam](http://en.wikipedia.org/wiki/Referrer_spam)

2. <http://it.wikipedia.org/wiki/Referer>

3. <http://it.wikipedia.org/wiki/Spamdexing>

casi anche il sito web su cui appaiono i link fasulli viene penalizzato, abbassando il suo indice di affidabilità, quando non addirittura eliminandolo dal database, questo per dare un robusto incentivo ai webmaster meno attenti.

## **Ma io mi prendo un hosting blindato**

Ecco che ci risiamo. Non esiste un hosting blindato, come non esiste un computer blindato. La ragione è semplicissima: il livello di “blindatura” di un sito dipende da quello che il webmaster ci infila dentro.

Se l’applicazione ha un problema di sicurezza, nessuna “blindatura” impedirà ad uno dei tanti mentecatti di farne l’uso che vuole, perché sarà indistinguibile dalla normale attività di un sito web.

## **Windows, Linux o PincoPallo, non cambia nulla**

Continuando sul tema “hosting blindato”, non ha quasi nessuna influenza il tipo di sistema operativo del server che ospita i siti web, per quanto riguarda la possibilità di avere il sito violato o meno.

Alcune applicazioni web richiedono specifici sistemi operativi per il server su cui vengono ospitate, mentre altre funzionano con tutti i sistemi operativi: entrambe vengono violate, indipendentemente dal sistema operativo impiegato dal server.

Le applicazioni web Open Source sono spesso sviluppate per Linux, e sono molto diffuse per la mancanza di problemi di licenze ed oneri di vario tipo: succede che, al contrario di quanto avviene per i nostri computer di casa, le applicazioni web ospitate su server Linux siano colpite più frequentemente, unicamente per la maggiore diffusione.

Attenzione, è l’applicazione web a rappresentare il punto debole, non il server o il suo sistema operativo. Tanto è che può succedere che, nei casi in cui su un singolo server siano ospitati molti siti web differenti, se un sito viene violato può costituire una porta di ingresso per violare l’intero server, in casi particolari.

## L'Open Source è meno sicuro

Le applicazioni web Open Source non sono più vulnerabili di quelle commerciali. Nessuno è mai riuscito a dimostrare una sostanziale differenza nelle vulnerabilità a favore di una o dell'altra tipologia.

Quello che succede è che le applicazioni Open Source, essendo di libero uso, quindi gratuite, sono molto utilizzate dai webmaster “fai-da-te”, che spesso mancano delle nozioni di base, come ad esempio la necessità di seguire il rilascio degli aggiornamenti dell'applicazione, finendo per alimentare il girone infernale dei siti web violati per mancanza di aggiornamenti e manutenzione.

Lo stesso accade nelle applicazioni commerciali, dove gli aggiornamenti sono a pagamento. Chi ne acquista una per il proprio sito spesso si limita ad acquistare il servizio di aggiornamento solo per il primo anno, per vari motivi, per cui è facilissimo trovare siti web violati a causa di applicazioni commerciali non aggiornate.

## I siti li “bucano” gli hacker per farsi pubblicità

E' una convinzione errata, e pericolosissima. La quasi totalità dei siti violati mostra pochissimi sintomi, o niente del tutto: l'intrusione è silenziosa e invisibile. Se fosse per vantarsi (“guarda quanti siti ho demolito”), rendere le violazioni così elusive sarebbe un controsenso.

Lo scopo delle violazioni è tutt'altro, e lo vedremo fra poco. Pensare che il tutto si riduca al *defacement* (in inglese sfregiare, deturpare) per motivi ideologici è, al solito, una pericolosa sottovalutazione.

## Vulnerabilità e aggiornamenti, anche qui

Se avete letto fino a questo punto, avrete intuito che sta per arrivare la prima di una serie di brutte notizie, per chi pensava di avere la vita facile: le applicazioni web soffrono di tutti i problemi delle normali applicazioni. Per chi è del mestiere, non è una sorpresa: le applicazioni web sono software, e come tutti i software possono contenere errori di vario genere. Quindi vanno corrette, aggiornate e controllate esattamente come tutte le altre applicazioni.

Molto dipende da che tipo di applicazione si è scelta, da come viene gestito il sito e da chi. L'applicazione può essere preconfezionata, commerciale o Open Source, oppure realizzata su misura. Nel secondo caso può essere creata da zero o, molto più frequentemente, adattata a partire da una preconfezionata, spesso Open Source. Nel caso di applicazione preconfezionata non ci dovrebbero essere problemi con gli aggiornamenti e la correzione degli errori, il problema, semmai, è scegliere qualcosa di adeguatamente supportato e diffuso. Ovviamente, se andiamo a scegliere una applicazione che usano in tutto il mondo non avremo una grande aspettativa di vita per il nostro sito.

Il sito stesso può essere gestito direttamente dal proprietario o da un professionista, oppure da una società, può essere semplice o complesso come un portale, insomma le varianti sono infinite.

Se si tratta di una applicazione sviluppata “su misura”, occorre anche accertarsi di poter avere un supporto adeguato per la correzione di errori e di possibili vulnerabilità. Ma serve anche che lo sviluppatore abbia competenza nel campo della cosiddetta programmazione sicura, ossia le tecniche e le strategie per realizzare applicazioni che siano meno vulnerabili a tutta una serie di attacchi noti ed a quelli che potrebbero sorgere in futuro.

Naturalmente, questo presuppone l'aver a che fare con qualcuno che sappia di cosa parliamo.

## **Non esageriamo!**

Minimizzare il problema non lo renderà meno presente e meno grave. Abbiamo già (o dovremmo avere) coscienza di quanto sia pericoloso usare un computer con applicazioni vulnerabili, a maggior ragione dovremmo porre attenzione alle applicazioni sul web. Due cose rendono le vulnerabilità delle applicazioni web molto più pericolose di quelle delle applicazioni nel nostro computer:

- un sito web non si può spegnere o scollegare dalla rete. Se il sito contiene una applicazione con un problema di sicurezza, non c'è modo di metterlo al riparo da violazioni, se non quello di correggere le falle.

- là fuori è pieno di mentecatti attivamente e continuamente alla ricerca di siti web con applicazioni vulnerabili. A differenza delle applicazioni nel nostro computer, dove è possibile in un certo senso chiudere la porta a chi viene da fuori, un sito web è esposto 24 ore al giorno al pericolo.

Per rendere l'idea, il mio sito, non particolarmente noto e visitato, meno di 150 visite al giorno, viene sondato da una media di dieci-quindici mentecatti differenti ogni giorno, alla ricerca di varie vulnerabilità, tutte per fortuna ampiamente corrette.

Se questo è quello che succede ad un sito da poco come il mio, è facile capire quale aspettativa di vita possa avere un sito basato su una applicazione web non aggiornata da un anno, senza dover ricorrere ad esagerazioni.

## **Solo io so come funziona la mia applicazione**

Le applicazioni web fatte su misura, o commerciali, non sono meno soggette per il semplice fatto che il codice sorgente non sia disponibile ad un potenziale attaccante, secondo la convinzione, del tutto infondata, che le falle di sicurezza siano individuabili solo dal codice sorgente.

La bruttissima notizia è che non ne ha alcun bisogno, l'attaccante, del codice: è in grado di scoprire le falle semplicemente visitando il sito che ospita l'applicazione. Nei primi mesi del 2011 ho dovuto esaminare i log di due differenti web server, entrambi ospitanti una applicazione web fatta su misura, entrambi violati: il primo era stato "farcito" di Javascript che tentavano di rifilare malware ai visitatori, il secondo apriva dei popup con pubblicità di siti per il gioco d'azzardo e per "ausili sessuali".

In entrambi i casi l'incursore aveva utilizzato dei programmi automatizzati per portare l'attacco, che si era realizzato in tre fasi distinte:

- Ricerca della vulnerabilità: l'attaccante aveva esplorato tutti i link interni del sito, alla ricerca di quelli che accettavano parametri, o di pagine contenenti moduli compilabili dai visitatori. In entrambi i casi, aveva individuato che la

vulnerabilità era nella gestione dei parametri, che venivano usati senza controlli appropriati in interrogazioni al database dell'applicazione.

- Analisi e mappatura del database: un secondo automatismo, lanciato poco dopo, sfruttava le vulnerabilità scoperte nel primo giro per creare l'elenco delle tabelle del database dell'applicazione web, con tanto di definizione completa della struttura delle singole tabelle. Attraverso questi dati l'attaccante è riuscito a capire quali tabelle contenevano i dati pubblicati sul web, e come poteva sfruttarle per iniettarci i propri, di dati.
- Attacco vero e proprio: fino a questo punto nulla era stato toccato nell'applicazione e nel database. Un terzo automatismo iniettava in una o più tabelle specifiche del database i dati necessari per far apparire un brevissimo frammento di codice HTML, il cui scopo era prelevare da un altro sito del codice Javascript, quello che poi effettivamente operava le azioni nei confronti dei visitatori (iniezione di malware o popup di pubblicità).

Ad ogni pagina visitata, il contenuto veniva costruito prelevandolo dal database, come è normale in tutte le applicazioni web, e presentato ai visitatori, insieme al codice iniettato che invece operava l'apertura del popup o il rilascio del malware.

Lo svolgersi di tutte le azioni ha richiesto all'attaccante poco tempo, in entrambi i casi: un paio d'ore al massimo. Gli automatismi hanno lavorato velocemente, pochi minuti ciascuno, con pause prima del lancio del successivo, verosimilmente mentre l'attaccante esaminava e selezionava sito, vulnerabilità e tabelle più adatte allo scopo.

Il pensiero che un attaccante non possa violare un sito se non ha il codice sorgente dell'applicazione appartiene al modello di pensiero detto *security through obscurity*, sicurezza attraverso la segretezza: se nessuno sa come funziona l'applicazione, nessuno può violarla. Modello di pensiero che è errato a molteplici livelli, ma dato che soddisfa il senso di sicurezza di molti, continua ad essere applicato diffusamente, anche a fronte di continue ed evidenti smentite.

## Va bene, ma ti pare che...

...proprio il mio sito riescano a trovare, fra milioni di altri? Questo state pensando, lo so. E questo è proprio un pensiero che bisogna levarsi subito dalla

testa: i siti vulnerabili vengono scovati impiegando gli stessi strumenti che usiamo per far trovare il nostro sito web ai potenziali visitatori.

Inutile negarlo, se abbiamo un sito web è perché vogliamo che sia visitato da più gente possibile, per cui ci preoccupiamo di fare più pubblicità possibile, attraverso i principali motori di ricerca, gli elenchi ragionati, le classifiche web. Esattamente gli stessi strumenti utilizzati per trovare i siti da violare.

Non voglio entrare troppo nei dettagli, ma ogni applicazione web lascia delle tracce inconfondibili, anche se non riporta esplicitamente il suo nome nel codice che mostra ai visitatori. Neanche le applicazioni sviluppate in proprio sono esenti, perché viene cercato uno specifico schema nel modo in cui il sito stesso presenta i suoi contenuti.

La violazione del sito può avere differenti scopi, questi elencati sono alcuni di quelli che ho verificato personalmente:

- Inserimento di pubblicità. Nelle pagine del sito viene nascosto del codice Javascript che fa apparire un popup quando arriva un visitatore. Per evitare che l'intrusione venga scoperta troppo presto vengono applicate varie tecniche: in un caso il popup era programmato per apparire quando il visitatore lasciava il sito per andare su un altro, così il popup sembrava venire da quest'ultimo.
- Iniezione di malware ai visitatori. Questa è una delle motivazioni più frequenti. Viene inserito un brevissimo frammento di codice che con vari trucchi tenta di rifilare un malware ai visitatori. E' la strategia usata per spacciare i finti antivirus (vedi Sezione *Disinfetta, PRESTO!* nel Capitolo 8): appena un visitatore capita nel sito vede partire la finta scansione (Figura 8-13). La "colpa" dell'infezione ricadrà sul sito violato e sul suo proprietario, che in realtà non ha nessuna responsabilità diretta, se non quella di avere un sito vulnerabile.
- Inserimento di un intero sito "parassita" all'interno di quello legittimo. Questa è una strategia molto utilizzata da chi pratica il *phishing*, in modo da rendere impossibile risalire al responsabile della truffa. Ne ho parlato nel mio blog<sup>4</sup> e Denis Frati ne parla da tempo nel suo<sup>5</sup>.

---

4. <http://www.ismprofessional.net/pascucci/index.php/2009/08/tre-mesi-di-phishing/>

5. <http://www.denisfrati.it/>

Nel 2008 mi occupai di una vera e propria tempesta riguardante i siti basati su Wordpress. La storia completa, per chi fosse interessato, è disponibile sul mio sito sotto la categoria apposita<sup>6</sup>. Faccio un breve riassunto: tutto originò dai venditori di farmaci online, gli stessi responsabili di praticamente quasi tutto lo spam che riceviamo. Avevano scoperto che nascondere dei link alla propria farmacia online in siti web con una buona reputazione avrebbe portato molti più visitatori, proprio per il meccanismo di promozione basato sui link. Cercando su Google, ad esempio, un medicinale specifico, il sito con la farmacia “pubblicizzata” dai link nascosti veniva mostrato per primo nei risultati.

Il meccanismo è piuttosto complesso da spiegare, e coinvolge concetti tipici della SEO, acronimo di *Search Engine Optimization*, ossia l’insieme di tecniche e di strategie per far sì che il proprio sito risulti più visibile nei risultati presentati agli utenti dai motori di ricerca. Per quanto ci interessa, basti accettare che più siti riportavano i link, più la “farmacia” riceveva visite.

Di qui la vera e propria epidemia di siti violati, tutti basati su Wordpress, in tutto il mondo. Epidemia che durò per parecchi mesi, fino a quando tutti i motori di ricerca non riuscirono a riconoscere i link illegalmente piazzati nei siti web compromessi, e passarono all’attacco, operando in vari modi: cancellando del tutto i link dal proprio database, assegnando rilevanza bassissima ai siti violati, cancellando del tutto qualsiasi riferimento alle farmacie online.

L’epidemia terminò semplicemente perché chi violava i siti non aveva più nessun vantaggio nel piazzare i link alle farmacie, non certo per la pronta risposta dei proprietari dei siti, che in molti casi non si accorsero di nulla, almeno fino a quando non furono in qualche caso cancellati dal database dei motori di ricerca, o avvertiti che il sito tentava di iniettare malware ai visitatori: chi aveva violato il sito ne aveva il controllo al punto da poter cedere l’accesso ad altri che lo sfruttavano per infilarci di tutto.

Personalmente tentai di avvisare più di un centinaio di persone il cui sito era stato violato e presentava tutti i segni dell’intrusione. Approntai un test online che esaminava il sito e cercava i segni della presenza dei link abusivi. Il test venne usato per controllare oltre 5000 siti web, di cui oltre 450 presentavano i segni della violazione.

---

6. <http://www.ismprofessional.net/pascucci/index.php/category/wordpress/>



La lezione che ho imparato è che la percezione dell'utente comune riguardo le violazioni dei siti web è assolutamente fuori dalla realtà. Tutti pensano che ad essere violati siano solo i più famosi, o i più frequentati. Ed ancora, la preparazione tecnica di chi gestisce i siti web lascia molto all'improvvisazione, al pressappochismo ed al caso.

I dati parlano chiaro<sup>7</sup>: i due terzi delle repliche contraffatte di portali bancari, utilizzate per il *phishing*, sono ospitate su siti web violati, con situazioni in cui lo stesso sito è utilizzato più volte, spesso contemporaneamente. Sovente il sito rimane violato per settimane, quando non mesi, senza che il proprietario e gestore si accorga di nulla.

## Un infernale circolo vizioso

L'avevo annunciato qualche capitolo addietro (vedi Sezione *Perché Windows è l'unico colpito?* nel Capitolo 2), ma vediamo in dettaglio cosa accomuna siti web vulnerabili, malware, spam, grayware e *phishing*:

- Un sito violato viene modificato per rifilare malware ai visitatori.
- Il malware viene iniettato con successo in un certo numero di computer, che vanno a costituire una botnet.
- Nello stesso sito violato viene nascosto un sito per il *phishing*.
- I computer della botnet vengono istruiti per inviare messaggi e-mail allo scopo di attirare vittime al sito di *phishing*, quindi diventano spedizionieri di spam.
- La stessa botnet viene utilizzata per cercare e violare altri siti vulnerabili e ripartire dal primo punto, solo che stavolta, invece del *phishing* sul sito violato verrà inserito un falso antivirus, per rifilare un *grayware* o qualche altra amenità dello stesso tenore.

E' più chiaro ora perché non è solo un problema di computer vulnerabili, ma anche di siti web gestiti male: malware e siti web vulnerabili sono parte dello stesso disegno criminale. Non basta bloccare i malware sui computer, occorre anche rendere più difficile trovare siti da violare e sfruttare.

---

7. <http://www.ismprofessional.net/pascucci/index.php/2009/08/tre-mesi-di-phishing/>

## **La zappa sui piedi**

Quando non è l'applicazione web ad avere problemi, è il webmaster a crearli, naturalmente involontariamente. Assumendo che le applicazioni web siano prive di falle, esiste una strada differente per conquistare un sito web: convincere il proprietario a installare qualcosa che funziona come un cavallo di troia.

Non è difficile, ricorrendo ad un meccanismo pensato da chi crea le applicazioni web per permetterne la personalizzazione e l'estensione delle funzionalità: la possibilità di aggiungere temi grafici e plugin.

Con i temi grafici si può personalizzare l'aspetto del sito web, conservando la piena compatibilità dell'applicazione originale. La personalizzazione può essere molto spinta, al punto di non riuscire a riconoscere l'applicazione di partenza, o addirittura mimare l'aspetto di una differente applicazione web, o di una normale applicazione del computer. Vi sono temi che mimano l'aspetto delle finestre di un sistema operativo, altri che sembrano schermi di videogiochi, praticamente il limite è la fantasia.

Con i plugin si possono aggiungere funzioni nuove, estendere quelle già presenti o cambiare totalmente il funzionamento dell'applicazione, senza perdere la totale compatibilità.

Prendendo come esempio Wordpress, solo perché è l'applicazione che conosco meglio, ma ne esistono tante altre che offrono le stesse possibilità, esistono plugin per una infinità di funzioni, dal controllo dei commenti indesiderati alla creazione di siti multilingue, mentre per i temi grafici esiste solo l'imbarazzo della scelta: qualsiasi colore, impostazione e aspetto del sito può essere personalizzato.

Arrivando al dunque: quale migliore porta di ingresso per un intruso di quella dei temi grafici o dei plugin?

Come succede per i software grigi (Capitolo 8), basta cercare temi per Wordpress in Rete usando i motori di ricerca e troviamo decine di siti che ne offrono, gratuitamente.

Nella quasi totalità dei casi i temi riportati non hanno nulla di originale, sono copie di temi già offerti da altri, modificate ad arte per includervi del codice

in grado di compiere azioni all'insaputa del legittimo proprietario del sito, azioni che vanno dal semplice mostrare link pubblicitari a siti web di dubbia reputazione, allo scaricare, includere ed eseguire codice preso da un altro sito, anche questo sicuramente di dubbia fama ed utilità.

Anche di questo avevo parlato nel mio blog<sup>8</sup>, e a distanza di tre anni niente è cambiato. Anzi, le strategie di offuscamento e occultamento del codice nei temi sono diventate sofisticatissime, tanto che solo un programmatore esperto riesce ad identificarne le tracce.

## Fai da te, danni compresi

Non sempre un sito che smette di funzionare o inizia a fare cose strane è indice di una violazione da parte di uno dei tanti mentecatti in giro per la Rete. A volte è lo stesso webmaster che incappa in situazioni che per un sysadmin (vedi Sezione *Investire in un bravo SysAdmin* nel Capitolo 3) sono normale amministrazione, solo che quando si difetta di alcune nozioni basilari tutto diventa oscuro e penoso.

Quasi tutte le web application necessitano di un database per il proprio funzionamento, e normalmente questo viene incluso in tutte le offerte di hosting, anche le più economiche. Per venire incontro agli utenti, vi è di solito una interfaccia di gestione del database via web, che permette tutte le principali operazioni di manutenzione: backup e ripristino, operazioni sulle tabelle, visualizzazione e modifica dei dati e via così.

Lo stesso avviene per la gestione dei file nello spazio web: il servizio di hosting mette a disposizione una interfaccia simile ad un *file manager* per operare sui singoli file.

E' uno dei tipici casi in cui una interfaccia grafica illude l'utilizzatore di poter fare qualsiasi cosa con uno strumento che nasconde tutto quanto c'è "sotto il cofano", di cui non conosce neanche il funzionamento di base e le principali nozioni teoriche.

---

8. <http://www.ismprofessional.net/pascucci/index.php/2008/06/wordpress-bello-il-tuo-tema-e-un-trojan/>

Se suona familiare, è perché appartiene alla stessa categoria di situazioni che vedono coinvolti tanti “guidatori sopra la media”, di cui abbiamo parlato più volte.

Ed ecco allora siti che espongono un penoso messaggio di errore (PHP Parse error: syntax error, unexpected ...), o un più oscuro HTTP 500 - Internal Server Error. Siti che sembrano funzionare perfettamente, ma negano l’accesso a chiunque, webmaster compreso, o che improvvisamente si presentano come se fossero appena stati installati, vuoti e vergini.

Non è detto che si tratti di una violazione, i nostri amici mentecatti, quando riescono a violare un sito, hanno interesse a che l’applicazione originale ed il proprietario subiscano meno danno possibile, per due motivi: poter utilizzare il sito con piena funzionalità e ritardare il più possibile un intervento di pulizia del proprietario, che vanificherebbe il lavoro fatto per entrare nel sito abusivamente.

Nella maggior parte dei casi in cui un sito inizia a fare i capricci la ragione va ricercata in qualche operazione compiuta dal proprietario o webmaster. A volte si tratta di reali sciocchezze, come una coppia di virgolette dimenticate o di uno spazio di troppo, una inezia agli occhi umani, un errore irrecuperabile per la macchina, che ha solo risposte predeterminate e limitate.

## **Il sito è mio e ci metto quello che mi pare**

Al tempo. Anche quando si tratti di materiale di propria produzione, non possiamo pubblicare qualsiasi cosa ci passi per la mente.

Esistono una serie di problemi legali a cui si va incontro, correlati con il tipo di contenuti e con la forma con cui sono pubblicati, che non è permesso ignorare.

Per prima cosa non si possono scrivere cose ingiuriose, offensive o caluniose nei confronti di chicchessia. E’ capitato che qualcuno si sia lamentato del comportamento di una ditta o di un commerciante, facendo nomi e cognomi sul suo sito, e si sia visto querelare per diffamazione. Al di là delle ragioni che possiamo avere, le perdiamo immediatamente nel momento in cui andiamo a fare cose come questa.

Sta benissimo che Internet e la Rete siano libere e senza censori, sono il primo ad affermarlo, ma una grande libertà richiede una più grande responsabilità nel farne uso. Poi, non tutti sono pronti a cogliere le nuove modalità di confronto online e le potenzialità della libera circolazione delle informazioni, per cui ci si deve aspettare che il signor Nomeinventato Chenonesiste, di cui vado a raccontare le poco onorevoli azioni nel mio blog, si inalberi e mi quereli per diffamazione. Non è lui che è cattivo, sono io che gli ho offerto il fianco.

Per non parlare poi dei reati in cui possiamo incappare con affermazioni incaute o pubblicando materiale *che non ci appartiene* o, peggio, illegale.

Per capirci, non è detto che la bellissima foto di paesaggio che abbiamo trovato in un sito la possiamo usare nel nostro. Potrebbero esserci dei vincoli (citare l'autore della foto, non modificarla, non utilizzarla in altre opere, per nominarne qualcuno), o potrebbe essere del tutto proibito.

Ora, so benissimo che in Rete l'uso che si fa dei contenuti multimediali è largamente *sportivo*, ed in un certo senso tale uso è sperato da parte di molti autori (più si diffonde la mia opera, più divento noto e conosciuto), per cui alla fin fine nessuno sembra preoccuparsi più di tanto. Il confine però è molto sottile e soggettivo, per cui è facile oltrepassarlo. Il comportamento migliore sarebbe quello di chiedere il permesso all'autore, prima di pubblicare una copia del contenuto scelto sul proprio sito.

Comprendendo quanto possa essere difficoltoso per tutti, si è arrivati a diverse strategie per regolare l'uso dei materiali reperiti in Rete, dal *fair use*<sup>9</sup> americano, alle licenze Creative Commons<sup>10</sup>.

Il *fair use* è la possibilità di utilizzare materiale reperito in Rete con certi vincoli, tipicamente la citazione della fonte e senza fini di lucro, sempre che non sia diversamente specificato dal proprietario dell'opera.

Le licenze Creative Commons permettono di pubblicare le nostre opere su Internet informando puntualmente chi voglia riutilizzarle sulle modalità che abbiamo scelto per la diffusione. Naturalmente, molto sta alla buona volontà ed alla civiltà di chi decide di riutilizzare le nostre produzioni. Sia chiaro: le licenze

---

9. [http://it.wikipedia.org/wiki/Fair\\_use](http://it.wikipedia.org/wiki/Fair_use)

10. <http://www.creativecommons.it/>

Creative Commons non proteggono il cosiddetto *diritto d'autore*, cosa che vale dal momento della creazione dell'opera, a prescindere da qualsiasi altra cosa, ma semplicemente ad agevolare la diffusione dell'opera.

In entrambi i miei siti web diffondo materiale di mia produzione usando una licenza Creative Commons, e lo stesso faccio con altro materiale che produco per corsi e seminari.

Quello che non si può assolutamente fare è prendere un brano musicale o un film e pubblicarlo integralmente sul proprio sito web, come pure il testo di una opera di letteratura o una fotografia, quando non sono io l'autore e non ho acquisito gli specifici diritti di uso, che *non corrispondono* all'aver acquistato il CD musicale o il DVD del film, proprio no (vedi Sezione *Malintesi e sottintesi* nel Capitolo 7).

Chiudo con un esempio di quanto sia un argomento sconosciuto ed ignorato, esempio che mi riguarda direttamente. Il precedente libro, "Windows XP in Sicurezza"<sup>11</sup>, fu pubblicato nel 2007 dalla casa editrice Apogeo con un contratto che ne prevedeva la distribuzione in forma di testo elettronico (un file PDF) ad un costo di zero euro. Esatto, era, ed è, totalmente gratuito, chiunque può tutt'ora andare sul sito e scaricarlo una copia senza pagare nulla (questo implica naturalmente che non ho ricevuto alcun compenso di alcun tipo).

A distanza di quattro anni, una decina di siti distribuisce una copia del file PDF, non usando il link al sito di Apogeo, ma direttamente o tramite uno dei tanti siti di condivisione file. Il danno è indiretto, perché non percepisco nulla per ogni copia scaricata ma, se il libro non viene scaricato dal sito originale, vengono falsate le statistiche di diffusione dell'editore, una delle chiavi per ottenere pubblicazioni di altre opere o per convincere l'editore stesso a distribuirne una copia stampata a pagamento, cosa implicitamente prevista nel contratto esistente fra me e l'editore.

Fra l'altro, vista la facilità con cui è possibile modificare un file PDF, non è detto che il contenuto sia lo stesso, come non è detto che qualche simpaticone ne metta in giro versioni opportunamente farcite di script per rifilare malware, cosa che con i PDF è diventata la norma.

---

11. <http://www.ismprofessional.net/pascucci/index.php/2007/06/windows-xp-in-sicurezza/>

Tutto questo per un testo che è completamente gratuito. Per un po' ho provato a notificare "l'indelicatezza" a chi lo faceva, poi ho lasciato perdere: è difficile riuscire a farsi ascoltare e comunque le risposte che si ricevono sono abbastanza scoraggianti.

## Calma, respira e rifletti

La domanda a cui dovremmo rispondere per prima è se proprio abbiamo necessità assoluta ed indifferibile di avere un sito web personale. Mantenere un sito significa avere la capacità e la costanza di creare contenuti originali per parecchio tempo, e vi posso assicurare che è una faticaccia. Un buon articolo sul blog può costare un paio di pomeriggi di lavoro, fra stesura, ricerca dei riferimenti, verifica delle fonti e correzioni varie. Se poi intendiamo scrivere una sorta di manuale, possono volerci giorni, settimane, per un singolo articolo.

Dopo aver scritto il tutto, conviene spendere un po' di tempo per verificare di essere dentro limiti legali, non avendo offeso, diffamato o danneggiato nessuno. No, non è impossibile, è più facile di quanto si possa pensare, e ci sono delle regole ben precise da tenere a mente.



### Una lettura utile

Per avere le idee un po' più chiare, e per evitare di fare le cose in modo approssimato e poco professionale, conviene affidarsi a chi ne sa più di noi. A questo scopo possiamo riferirci all'ottimo "Minottino" dell'avv. Daniele Minotti<sup>12</sup>. E' un testo breve, leggibilissimo, ma denso di informazioni sui temi legali relativi alla tenuta di un blog, ed in generale di un sito web.

Se a questo dobbiamo aggiungere l'impegno per tenere in ordine le interiora del sito, possiamo facilmente immaginare che sia una vera rottura di scatole, perdonate il francesismo, perdere una quantità indecente di tempo a scegliere e mantenere aspetti in definitiva del tutto secondari rispetto alla principale attività, che dovrebbe essere la creazione di contenuti da pubblicare.

---

12. <http://www.minotti.net/il-minottino/>

Dopo aver fatto gli opportuni esami di coscienza, analizzato spassionatamente cosa abbiamo da dire e per quanto ne abbiamo, se proprio dobbiamo, possiamo prendere in considerazione uno dei tantissimi servizi gratuiti che offrono non lo spazio web, ma l'applicazione completa: in questo modo la parte di gestione puramente tecnica è lasciata al fornitore del servizio, mentre a noi rimane da decidere l'aspetto grafico e naturalmente i contenuti.

Per la scelta c'è veramente l'imbarazzo, basta cercare in Rete. L'offerta va dal blog, al forum, al wiki (un sistema per creare siti di documentazione in forma collaborativa, esattamente come Wikipedia), tutti gratuiti e con pochissime limitazioni, che tali non sono per chi inizia.

Se poi la nostra avventura ha molta fortuna, e il nostro sito inizia a diventare famoso, possiamo valutare altre alternative, fra cui un sito in proprio, che ci consenta molta più libertà, ma a questo punto sarà d'obbligo valutare una forma di collaborazione con un professionista del settore che si occupi di tutti gli aspetti tecnici per l'amministrazione e la manutenzione del sito, sollevandoci dal compito ma, soprattutto, mettendoci al riparo da catastrofi e disservizi.



## Capitolo 11. Il bello di Internet

Onestamente, leggendo fino a qui, è probabile che il primo pensiero di una persona normale sia di disdire l'abbonamento ad Internet e vendere il computer.

Se possedere un computer e collegarsi ad Internet deve essere solo fonte di guai, allora tanto vale rinunciarvi.

Non è tutto da buttare, al contrario. Ma per poter fruire delle reali potenzialità di uno strumento così potente da aver rivoluzionato più aspetti della nostra vita, più volte, occorre prima allenarsi a riconoscere le trappole, per poi godersi gli aspetti positivi. E' un po' come andare per funghi: occorre conoscere le specie velenose, per poter poi gustare appieno un piatto di funghi selvatici trifolati, il cui profumo è indimenticabile.

### Informarsi

A differenza di televisione, radio e giornali, dove le notizie sono razionate e selezionate, vuoi per motivi di spazio, ma anche per motivi di comodo e di opportunismo, in Internet è possibile scegliere come e dove informarsi.

La stessa notizia può essere letta da differenti fonti, verificata all'origine, controllata nella sostanza e nella coerenza, anche semplicemente confrontando le varie versioni disponibili.

Non sono rari i casi in cui le notizie vengono smentite dai lettori in Internet, anzi, ed è questo a rappresentare una delle grandi potenzialità della Rete: non è più una informazione a senso unico, dove siamo costretti ad ascoltare e basta. Ne avevo già parlato, ma il caso delle foto di Bin Laden taroccate si è ripetuto più volte e puntualmente persone normali hanno non solo dimostrato che erano dei falsi, ma hanno anche mostrato da dove erano originati e come erano stati prodotti.

Altra grande caratteristica è che si possono selezionare le notizie in funzione degli argomenti, i più disparati. Se siamo appassionati di cinema o di robotica abbiamo letteralmente centinaia di siti che ne parlano, dal sito amatoriale a quello professionale.

Non ultimo, possiamo vedere quello che succede “altrove”, fuori dai confini nazionali o continentali. Le recenti sollevazioni popolari nei paesi dell’area del Mediterraneo hanno avuto grandissima risonanza in Internet, anche grazie a particolari iniziative di alcuni *social network* che hanno permesso di diffondere notizie fuori dai canali “ufficiali”, controllati da apparati governativi.

Se siamo appassionati anche di argomenti poco noti e diffusi, troveremo comunque notizie relative ai nostri interessi, basta cercarle.

Qualche esempio:

- Sapere cosa fanno i nostri politici. Il sito OpenPolis<sup>1</sup> tiene un aggiornatissimo archivio di deputati, senatori, proposte di legge, interrogazioni, risultati di votazioni, presenze ed assenze. Per sapere se colui che abbiamo votato non solo ci rappresenta adeguatamente, ma anche l’uso che fa del potere che gli è stato delegato.
- Statistiche sulla popolazione mondiale, l’incidenza delle malattie ed infinite altre. Gapminder<sup>2</sup>, un sito creato dalle Nazioni Unite, mette a disposizione statistiche su centinaia di indicatori sociali e di sviluppo della popolazione mondiale. Consumo di alcool, percentuale di adulti malati di AIDS, emissioni di anidride carbonica, percentuale di colesterolo nel sangue, praticamente ogni aspetto è coperto da una qualche statistica. I dati sono reali, e lo scopo è quello di demolire i miti su sviluppo e benessere attraverso i fatti ed i numeri.
- Mappa dei veleni versati in mare. InFondoAlMar<sup>3</sup> è un sito costruito a partire da dati oggettivi (notizie di affondamento, registri navali, rapporti delle Capitanerie di Porto) che mostra dove è riportato l’affondamento e che tipo di inquinante è stato versato in mare.

---

1. <http://www.openpolis.it/>  
2. <http://www.gapminder.org/>  
3. <http://www.infondoalmar.info/>

## Imparare

Simile, se non migliore, la situazione per chi voglia imparare qualcosa di nuovo. Il panorama è vastissimo ed estremamente variegato.

Informatica, chimica, fisica, medicina, geologia, filosofia, arte, letteratura, cucina, fai da te, tutti i campi dello scibile umano trovano amplissima trattazione in Internet.

La novità è che sempre più spesso sono i protagonisti a trasmettere direttamente le proprie conoscenze a chiunque voglia imparare. Molti sono gli scienziati ed i ricercatori che mantengono un sito dove parlano delle proprie ricerche, condividendole direttamente, senza intermediari.

Anche le organizzazioni dedite alla ricerca ed alla formazione stanno sempre più rendendo disponibile materiale didattico di qualsiasi genere, dai libri ai filmati, senza alcun onere e con la clausola esplicita dell'uso a fini didattici.

Alcuni esempi:

- Idee da diffondere. Il sito TED<sup>4</sup> raccoglie video di presentazioni di personaggi della scienza e della cultura in generale. I video sono in inglese, ma in gran parte sono sottotitolati anche in lingua italiana, per cui si possono fruire senza troppe sofferenze, anche se non si conosce l'inglese. Gli argomenti spaziano per tutto lo scibile umano, e le persone che parlano hanno una grande capacità di intrattenere.
- La biblioteca della National Academies Press<sup>5</sup> (in inglese). Una raccolta di oltre 4000 volumi su salute, energia, scienze della terra, tecnologia, tutti di altissimo livello, disponibili gratuitamente in formato PDF.
- Un database di 7000 piante utili (in inglese). Il sito Plants For A Future<sup>6</sup> riporta le schede complete di piante commestibili, medicinali ed utili in genere, con tutte le informazioni per la coltivazione e l'uso.

---

4. <http://www.ted.com/>

5. <http://www.nap.edu/>

6. <http://www.pfaf.org/>

- L'accademia della Crusca<sup>7</sup>. E' il riferimento assoluto per la lingua italiana. Qualsiasi dubbio sulla ortografia, sulle regole grammaticali, su un termine o un neologismo trova la risposta in questo sito. Offrono anche consulenza gratuita attraverso il forum.

## **Divertirsi**

Una fetta enorme del tempo passato su Internet è, naturalmente, speso per il divertimento, dal videogioco, al filmato, per finire con i fumetti.

Di tutta l'umana produzione relativa all'intrattenimento, Internet è stracolma. E la relativa novità è che molto di quello che si può fruire è assolutamente e totalmente gratuito, ed il fatto che lo sia non è per nulla sinonimo di bassa qualità, al contrario.

Prendendo ad esempio i disegnatori di fumetti, vi sono molti casi di incredibile produttività e qualità, disponibili liberamente e senza dover sborsare un centesimo.

La ragione è che nell'editoria classica un disegnatore viene pubblicato su carta solo se in qualche modo l'editore conosce già in anticipo l'estensione del possibile pubblico interessato all'acquisto. Alla fine è un serpente che si morde la coda: se il disegnatore non è conosciuto non vende, ma non può essere conosciuto finché qualcuno non pubblica i suoi lavori.

Con Internet, un disegnatore, anche assolutamente sconosciuto, può prendersi uno spazio web e pubblicare i suoi lavori, raggiungendo un pubblico che diversamente non avrebbe mai avuto.

Qualche esempio:

- Musica scaricabile legalmente e gratuitamente. Il sito Jamendo<sup>8</sup> nasce con lo scopo di offrire una vetrina per artisti che sono fuori dal giro della musica commerciale, vuoi perché poco noti, vuoi perché votati a generi musicali di

---

7. <http://www.accademiadellacrusca.it/>

8. <http://www.jamendo.com/>

nicchia. Gli artisti sono migliaia, e ci vuole pazienza per selezionare qualcosa vicino ai nostri gusti, ma vale la pena perderci tempo.

- I fumetti di Marco Dambrosio, in arte Makkox<sup>9</sup>. Se servisse una dimostrazione di come Internet cambia le prospettive e sovverte i dogmi in molti campi, Marco è una delle migliori. Ha iniziato pubblicando fumetti in vari suoi siti web. Il suo tratto è molto particolare, come pure la sua vena ironica e graffiante, e suscita sempre reazioni estreme: o si ama o si odia, non ci sono vie di mezzo. A distanza di qualche anno è riuscito a pubblicare su carta parecchi suoi lavori, compiendo il percorso inverso: da Internet alla carta stampata.
- La web TV della NASA<sup>10</sup>, in alta definizione. Documentari sulle missioni spaziali passate, presenti e future, interviste con i personaggi, immagini spettacolari della Terra e dello spazio. In occasione delle principali missioni offre trasmissioni in diretta, con collegamenti alla Stazione Spaziale Internazionale ed ai veicoli spaziali in viaggio. Se siete appassionati di spazio ed esplorazione spaziale, qui c'è tutto. Le immagini sono spettacolari quanto basta per rimanere senza fiato, grazie anche all'alta definizione.
- L'Independent Game Festival<sup>11</sup>. E' una competizione annuale che premia i creatori di giochi per computer secondo varie categorie. E' una vetrina per sviluppatori e piccole software house, tipicamente fuori dal giro dei grandi numeri. Vi si possono trovare giochi da provare ed altri da scaricare ed usare liberamente. Il tema principale è l'originalità e l'esplorazione di nuove forme di gioco interattivo. Uno dei vincitori del 2011 è Minecraft<sup>12</sup>.

## **Acquistare su Internet? MAI!**

Una delle possibilità più controverse e più allettanti è quella di fare acquisti senza muoversi da casa.

---

9. <http://makkox.it/>

10. <http://www.ustream.tv/nasahdtv>

11. <http://www.igf.com/>

12. <http://www.minecraft.net/>

La demonizzazione in questo settore è, a mio parere, esagerata e immeritata. Sono quasi dieci anni che acquisto vari tipi di merce via Internet, e fino ad ora non mi sono mai dovuto pentire. E da quando uso la carta di credito non ho mai avuto un singolo problema di furto o truffa.

Libri, giocattoli, materiale elettronico, software e hardware, fotocamere, DVD, biancheria per la casa, addirittura le bomboniere di quando mi sono sposato, tutto acquistato via Internet e consegnato a casa senza problemi.

E' sufficiente seguire alcune regole semplici per avere la ragionevole certezza di non rimanere scottati:

- Non fidarsi di offerte troppo allettanti. Il telefonino ultima generazione da 500 euro venduto a 200? O un software del valore di 1500 euro venduto a 200? Troppo bello per essere vero, e troppo allettante per non essere una trappola.
- Attenzione ai metodi di pagamento. Sono da evitare i sistemi poco tracciabili, quali le ricariche di carte di credito o mediante i servizi di trasferimento contante, soprattutto se la cifra supera i 50 euro. Preferire i pagamenti mediante carta di credito (tramite un istituto bancario o Paypal), con bonifico bancario o alla consegna.

Se si tratta di pochi euro, o abbiamo già avuto a che fare con il venditore, allora possiamo pensare di allentare questa regola, altrimenti è da considerare inderogabile.

- Usiamo una carta di credito prepagata. La caricheremo ogni volta con la cifra necessaria e la spenderemo immediatamente, così, anche se dovesse essere trafugata (non a noi, ma al venditore) difficilmente perderemmo più di qualche euro.
- Diffidare dei servizi che offrono di “memorizzare i dati della carta di credito” per rendere più facile il prossimo acquisto. E' proprio questa la strada per perderne il controllo: un malintenzionato che volesse fare incetta di carte di credito per usarle a sbafo rivolgerà le sue attenzioni verso chi detiene i dati di centinaia o migliaia di carte, piuttosto che tentare di sottrarre i dati ad ogni singolo proprietario.

- Verificare tutte le informazioni relative a garanzia, diritto di recesso, consegna, resa della merce difettosa o errata. Di solito, se il sito è affidabile, offre informazioni dettagliate e precise per queste eventualità, proprio perché il venditore non ha nessun interesse a complicarsi la vita, se è onesto: dare poche informazioni ai clienti significa poi avere continui scontri e contrasti che prendono tempo e denaro.
- Verificare la presenza dei dati identificativi della società, quali codice fiscale, partita IVA e iscrizione alla camera di commercio, dati che è *obbligatorio* pubblicare sul sito di vendita.

Tali dati possono essere controllati, dato che i registri sono pubblici.

Tutto qui. Niente di trascendentale o troppo complicato da applicare. Semplice buon senso e un pizzico di conoscenza del variegato universo di Internet.

## Capitolo 12. Per finire

Siamo di nuovo al termine della nostra chiacchierata. Ci sarebbero ancora tanti argomenti di cui parlare, ma il tempo stringe, e se continuo ad aggiungere cose finisce che non lo pubblicherò mai, anche perché il tempo passa e molto di quello che ho scritto l'ho dovuto aggiornare, più volte. Il tempo corre, in Rete, e stargli dietro è difficile.

### Che succederà, dopo?

Cosa ci aspetta, di qui in avanti, nessuno lo sa e nessuno può permettersi di fare previsioni certe. Ci sono alcune tendenze, però, che mostrano l'evoluzione dei pericoli per noi e per i nostri dati.

I malware saranno sempre più sofisticati, e questa non è certo una previsione difficile, ma, da quello che si vede in giro, non altrettanto sofisticati dovranno essere anche i metodi per infilarli nei nostri computer, visto che il principale bersaglio saremo noi, davanti al computer.

Sempre più i nostri dati personali saranno trafugati da servizi su Internet, più che dai nostri computer. Lo sforzo è infinitamente minore, e si ottengono in un colpo solo i dati di milioni di individui.

L'evoluzione dei supporti, l'evoluzione dei servizi online e l'evoluzione della tecnologia, ci indurranno a concentrare sempre più dati in forma digitale in un unico contenitore, con il risultato di rischiare sempre più di perdere tutto in un colpo solo.

Occorrerà essere un po' più smaliziati e meno inclini a pensare la tecnologia come "la" soluzione. La leva tecnologica è spesso soltanto uno strumento per vendere, indipendentemente da quanto effettivamente esista un bisogno. Tipicamente, dopo l'acquisto siamo soli con i nostri problemi.

### Per proseguire il percorso

Di materiale in Rete ve ne è in quantità mostruosa. Troppo per chiunque, tanto che occorre specializzarsi e selezionare le fonti.



Se non avete letto il libro precedente<sup>1</sup>, andatelo a prendere e leggetelo, tanto è gratuito. Tenete conto delle avvertenze su quello che è valido e quello che non lo è più (vedi Capitolo 4), ma i riferimenti e gli approfondimenti sono ancora validi.

## Dediche

Stavolta la dedica è per un cucciolo di nome Luigi che oggi ha quattro anni. Curioso, testardo, affettuoso come solo un bambino può esserlo. Gioca col computer, è appassionato di LEGO e di missioni spaziali ed adora leggere e sentir leggere. E sa già godersi il bello di Internet.

## Ringraziamenti

Sono di nuovo a ringraziare mia moglie, che non solo continua a tollerare le ore che dedico al computer, ma è una convinta sostenitrice degli acquisti via Internet. Libri e DVD sono i suoi preferiti.

Lorenzo, titolare di Nobug srl, con cui collaboro ormai da oltre sei anni, continua ad offrirmi occasioni di crescita professionale e personale, nonostante il mio caratteraccio.

Fedora<sup>2</sup> continua ad essere la mia distribuzione Linux di riferimento, come pure tutto il software Open Source.

Televisione? A chi serve?

---

1. <http://www.apogeonline.com/libri/88-503-1008-0/scheda>  
2. <http://fedoraproject.org/wiki>

# 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<sup>1</sup>, in inglese.

### adware

Software la cui licenza d'uso è subordinata alla presentazione all'utente di messaggi pubblicitari durante il funzionamento del programma. Inizialmente una normale forma di licenza, è diventata impopolare al punto da essere considerata sinonimo di malware, per l'uso indiscriminato da parte di persone senza scrupoli, il cui software rendeva impossibile fare qualsiasi altra cosa che subire la pubblicità.

---

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

## **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.

## **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 tentando sistematicamente tutte quelle contenute in una lista predefinita, il dizionario appunto.

## **attacco esaustivo, attacco brute force**

In inglese "pura forza", ossia facendo affidamento solo sulla forza. Metodo per scoprire una password tentando tutte le combinazioni possibili di caratteri che possono essere usati per la sua composizione, senza nessun'altra considerazione o strategia per abbreviare il lavoro di ricerca.

## **autorun**

funzione disponibile nei sistemi operativi più diffusi, applicata ai supporti removibili, per far avviare un programma contenuto nel supporto al momento dell'inserimento nel lettore o della connessione al computer, come nel caso di periferiche USB.

E' diventata una delle strategie preferite per favorire la propagazione di malware, tanto da essere progressivamente disabilitata in tutti i sistemi operativi che la prevedono.

## **Bb**

### **backdoor**

Letteralmente, la porta sul cortile o sul retro. Una funzione nascosta in un software, spesso destinata ad usi poco etici.

### **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.

## **blog**

Neologismo coniato a partire dalle parole *web log*, traducibile grossolanamente come “diario sul web”. Si riferisce ad un sito web che permette di pubblicare un diario, con possibilità di inserire contenuti multimediali e di relazionarsi con i lettori.

## **BlueTooth**

Tecnologia di comunicazione senza fili a breve distanza per mezzo di onde radio. Usato in molti modelli di telefono cellulare, in computer portatili e ultimamente anche su alcuni modelli di vetture.

## **botnet**

Rete di computer colpiti da uno specifico malware, aggregati e controllati da una unica entità. Possono raggiungere dimensioni di tutto rispetto, fino a decine di milioni di computer, i cui legittimi proprietari possono continuare per mesi ad utilizzare i loro computer, senza accorgersi che qualcun altro li usa per ben altri scopi.

Maggiori dettagli alla voce corrispondente di Wikipedia<sup>2</sup>.

## **Cc**

### **catena di santantonio**

In inglese *chain letters*, lettere a catena.

---

2. <http://it.wikipedia.org/wiki/Botnet>

## **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 usata 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.

## **crittografia a chiave pubblica**

Sistema crittografico che usa due differenti chiavi, strettamente correlate fra loro, una segreta ed una liberamente distribuibile, detta anche chiave

pubblica. E' impossibile risalire alla chiave segreta a partire dalla chiave pubblica.

Maggiori dettagli alla voce corrispondente su Wikipedia<sup>3</sup> o sul breve manuale disponibile sul mio sito<sup>4</sup>.

## 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.

### downgrade

L'operazione inversa di installare un programma (o uno dei componenti del computer) con migliori prestazioni. Il passare ad una versione precedente di un software.

*Vedi Anche:* upgrade.

### 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,

---

3. [http://it.wikipedia.org/wiki/Crittografia\\_a\\_chiave\\_pubblica](http://it.wikipedia.org/wiki/Crittografia_a_chiave_pubblica)

4. <http://www.ismprofessional.net/pascucci/documenti/gpg/>

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 versioni successive). NTFS è un sistema evoluto che permette di gestire anche proprietà come appartenenza di un file ad 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 prestabilite.

## **firma (virus)**

Dall'inglese *signature*. 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 efficacemente la sua funzione.

## **firma crittografica**

Sistema con cui è possibile verificare autenticità e integrità di un qualsiasi file, entro certi limiti e vincoli.

*Vedi Anche:* hash, crittografia a chiave pubblica.

## **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.

*Vedi Anche:* filesystem.

## **FTP**

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

## Gg

### grayware

Un software che non si può classificare come malware (black, nero), ma neppure come utile (white, bianco). Lo sono programmi che vengono venduti con tecniche di marketing molto aggressive.

*Vedi Anche:* scareware.

## Hh

### hash

Funzione matematica usata per trasformare una sequenza di dati di lunghezza qualsiasi in un numero di lunghezza prefissata e limitata. Una semplice funzione di hash può essere il resto della divisione per 256 della somma di tutti i valori in codice ASCII dei caratteri di un testo: il risultato sarà sempre compreso fra 0 e 255, indipendentemente dalla lunghezza del testo.

In crittografia, le funzioni di hash devono possedere alcune caratteristiche particolari per essere usate: ad esempio non deve essere facile "costruire" sequenze di dati tali da restituire lo stesso hash.

Per maggiori informazioni vedere la voce corrispondente su Wikipedia<sup>5</sup>.

## HTTP

Acronimo di *HyperText Transfer Protocol*. Sistema di distribuzione dei contenuti su Internet.

---

5. <http://it.wikipedia.org/wiki/Hash>

## 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.

## hosting

Per pubblicare pagine web su Internet occorre che siano su un server connesso alla Rete. Dato che i costi per possedere e gestire un server sono piuttosto alti, ci sono società di servizi che offrono fette di spazio su server propri, su cui pubblicare siti web. In questo modo è possibile suddividere il costo fra molti clienti, che rimangono indipendenti fra loro, rendendo i prezzi del servizio estremamente accessibili. In qualche caso può essere addirittura gratuito, a patto di accettarne alcune limitazioni.

## li

### 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*.

### **intranet**

Termine usato per definire il “lato interno” di una rete aziendale, la cui struttura, insieme ai servizi offerti, è praticamente identica ad Internet, solo che non è aperta all’accesso pubblico, ma riservata agli usi aziendali.

### **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.

### **inutility**

Parola scherzosa, contrazione di “utility inutile”, ossia un programma che pur dichiarandosi utile a qualcosa è in realtà del tutto inutile, se non dannoso, spesso per la cattiva qualità del codice sviluppato e la scarsa competenza del programmatore.

### **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.

## 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 dannoso. Data la continua espansione e diversificazione della categoria, si è coniato questo termine omni-comprendivo.

## **mirror, mirroring**

Dall'inglese specchio, copia speculare. E' un metodo per ridurre le probabilità di perdita dei dati a seguito di un guasto nel disco di un computer. Vengono installati due dischi, identici, il cui contenuto è tenuto allineato dal sistema operativo o dal sistema di controllo dei dischi. Ogni variazione viene immediatamente riportata su entrambi i dischi. In caso di guasto di un disco, il rimanente contiene tutti i dati.

*Vedi Anche:* RAID.

## **Nn**

### **netbook**

Termine che designa una particolare categoria di computer portatili, più piccola e leggera dei notebook, pensata per la navigazione e l'uso intensivo dei servizi disponibili su Internet (social network, blog, posta elettronica, chat e via così).

## **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.

### **permessi**

Riferito ad un file nel computer, è l'elenco delle azioni che un utente può compiere su quel file. Ad esempio un file può essere letto e modificato da uno, mentre un altro può solo leggerlo.

### **porta TCP o UDP**

Sistema per individuare ed indirizzare correttamente un collegamento vie rete fra computer. Serve a definire con quale specifico servizio si vuole dialogare. Molti servizi hanno dedicata una particolare porta: ad esempio il servizio HTTP (quello dei server web) è sulla porta 80, mentre il servizio di invio posta elettronica è sulla porta 25.

## **portale**

Sito web molto articolato e complesso. Dalla prima pagina del portale si può accedere alle varie sezioni, che possono essere ospitate addirittura su computer differenti.

## **privilegi**

Livello di accesso alle funzioni ed ai componenti di un computer. E' relativo al singolo utente, e definisce fino a che punto può intervenire sul computer e sui suoi componenti. In un normale sistema operativo esistono almeno due livelli di privilegi: quello utente e quello amministrativo. Il primo è dedicato al normale uso del computer, il secondo è destinato a tutte le operazioni riguardanti la configurazione e il regolare funzionamento del computer, del sistema operativo e delle applicazioni.

## **proxy, open proxy**

Un server contenente un programma che opera come un intermediario nelle comunicazioni fra un client ed un server. Ne esistono di vari tipi, con scopi differenti. Principalmente è uno strumento di sicurezza.

Normalmente un proxy richiede una forma di autenticazione per essere usato. Quando non avviene, è chiamato *open proxy*, per evidenziare il fatto che l'uso è aperto a chiunque.

Maggiori dettagli alla voce corrispondente su Wikipedia<sup>6</sup>.

---

6. <http://it.wikipedia.org/wiki/Proxy>



## Rr

### RAID

Acronimo di *redundant array of independent (o inexpensive) disks*. E' una tecnica che permette di combinare in vari modi due o più dischi, che verranno usati dal sistema operativo come un solo disco. A seconda del numero di dischi e della configurazione (detta anche livello del RAID) si privilegia la capacità o la sicurezza.

Per maggiori dettagli alla voce corrispondente su Wikipedia<sup>7</sup>.

### router

Apparato di rete che si occupa di instradare i pacchetti fra reti appartenenti a differenti subnet.

## Ss

### scareware

Neologismo coniato a partire dai termini inglesi *scare software*, programma che spaventa. E' una tecnica per vendere programmi agli utenti meno preparati, convincendoli ad esempio di avere un qualche problema grave, ma descritto vagamente, nel computer.

### 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.

---

7. <http://it.wikipedia.org/wiki/RAID>

## Search Engine Optimization

L'insieme di tecniche e di strategie per far sì che il proprio sito risulti più visibile nei risultati presentati agli utenti dai motori di ricerca.

## Security Enhanced Linux

Una versione del kernel Linux modificata dalla NSA (National Security Agency) americana per aumentarne il livello di sicurezza e la granularità nella gestione di permessi e privilegi. Maggiori dettagli nella pagina di Wikipedia<sup>8</sup>.

## smartphone

Un telefono cellulare dotato di funzioni estese, paragonabile ad un computer palmare.

## sniffer

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".

---

8. [http://it.wikipedia.org/wiki/Security-Enhanced\\_Linux](http://it.wikipedia.org/wiki/Security-Enhanced_Linux)

## **social network**

Un aggregato di persone che condividono un qualche tipo di legame sociale. Ad esempio rapporti di lavoro, vincoli di parentela, passione per una particolare attività.

Maggiori dettagli alla voce su Wikipedia<sup>9</sup>.

## **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.

## **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.

## **sysadmin**

contrazione delle parole *system administrator*, persona che gestisce il corretto funzionamento dei sistemi informatici.

---

9. [http://it.wikipedia.org/wiki/Social\\_network](http://it.wikipedia.org/wiki/Social_network)

## Uu

### **upgrade**

Il passaggio ad una versione più recente o con maggiori prestazioni di un software o di un componente del computer.

### **USB**

Acronimo per *Universal Serial Bus*, uno standard di connessione per periferiche di computer.

### **user-friendly**

Amichevole verso l'utente. Pensato per essere utilizzato anche da persone con una formazione non tecnica.

### **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

### wiping

Operazione di completa e definitiva cancellazione del contenuto di un supporto, al punto da non poter recuperare nulla. Un esempio è scrivere su un disco una sequenza di valori casuali, o tutti uguali, per l'intera capienza del disco stesso.

E' una operazione fatta principalmente per motivi di riservatezza (nessun dato può essere recuperato da un supporto cancellato in questo modo), ma può essere utilizzata per avere la sicurezza di disporre di un supporto pulito e senza alcun residuo dei dati precedenti, cosa che può tornare utile in presenza di un malware che non si riesce ad eliminare in altro modo.

### 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.