

Sbarre alle finestre

Qualche giorno fa mi stavo dedicando a una delle mie attività ahimè meno remunerative ... stavo, infatti, ripulendo il computer di un amico da virus, trojan e dialer vari, raccattati in mesi di navigazione sul web praticamente senza alcuna protezione (nessun firewall, antivirus non aggiornato, visite piuttosto disinvolute a certi siti, diciamo così, un po' al peperoncino eccetera).

Di amici ne ho diversi e tutti, prima o poi, si sono rivolti a me con le faticose parole: "Mario, il mio PC non funziona bene (oppure "è lento", o anche "mi si aprono continuamente pagine pornografiche" e simili) ... potresti dargli un'occhiata? penso che ci sia un virus". Dopo essermi fatto portare il "malato", ho cominciato quella che è una procedura ormai standard, fatta di scansioni con diversi programmi, installazione e aggiornamento dei software adeguati, pulizia delle chiavi di registro e così via. Ebbene, l'altro giorno, mentre stavo eseguendo queste operazioni, ho pensato: "Cos'hanno in comune tutti questi miei amici, a parte il fatto di essere degli sciagurati? (informaticamente parlando, s'intende). Usano tutti una delle diverse versioni di Windows", che è il sistema operativo sicuramente più diffuso sui personal computer.



Illustrazione 1: La finestra di avviso di un antivirus)

Ho iniziato a riflettere ... Microsoft Windows è installato su circa l'ottanta per cento dei personal computer al mondo, mentre la restante quota di mercato è ripartita tra MacOS (il sistema operativo dei PC della Apple) e Linux, con una prevalenza di quest'ultimo. Il fatto che i virus e gli altri programmi nocivi abbiano una netta predilezione per Windows si può sicuramente spiegare con la statistica: se è il sistema operativo più diffuso è

anche il più colpito ... è più facile colpire un elefante piuttosto che una mosca, logico, no?

Le cose, però, non stanno proprio così: i sistemi operativi concorrenti, infatti, sono praticamente immuni da virus e schifezze simili, e non può essere dovuto solamente a una questione di diffusione: cerchiamo allora di capire cosa succede e se c'è qualche accorgimento che ci può permettere di limitare i rischi.

Un dato, un po' obsoleto, ci aiuta a capire meglio le dimensioni del problema: è stato stimato che il codice sorgente (le istruzioni così come sono scritte, prima di essere adattate all'uso sull'elaboratore) di Windows 2000 sia composto da un numero di righe compreso tra 35 e 50 milioni e, probabilmente, da questo numero sono escluse quelle appartenenti a Internet Explorer, Windows Media Player e altri programmi che sono installati assieme al sistema operativo. Ritengo che Windows XP conti un numero di righe di codice sorgente molto più grande. Naturalmente la grande complessità del sistema operativo è un punto debole: più è grande il codice sorgente, maggiori sono le probabilità che contenga talloni d'Achille ... ma anche i concorrenti non scherzano quanto a dimensioni ... no, ci deve essere qualcos'altro.

Tutti questi sistemi operativi sono caratterizzati da un'interfaccia grafica, cioè si possono comandare a vista, con il mouse, e non usando sequenze di comandi da tastiera: questa innovazione, che ha raggiunto una larga diffusione ormai da molti anni, ha facilitato l'uso del computer anche agli utenti meno esperti. Il mouse comanda un puntatore, che si muove sul monitor del PC, e ci permette di eseguire programmi e di compiere altre operazioni. Uno degli elementi principali di un'interfaccia grafica è dato dalle finestre, nelle quali, almeno in Windows, avviene l'esecuzione dei comandi.

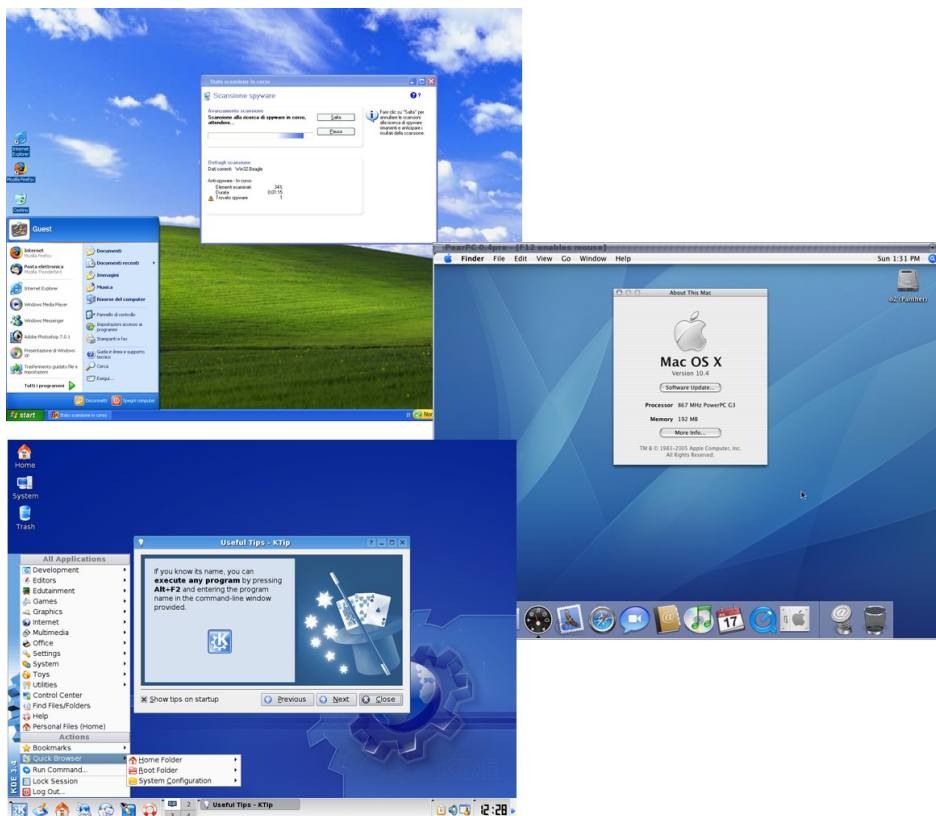


Illustrazione 2: In senso orario l'interfaccia grafica di Windows XP, di Mac OS X e di Linux

Ebbene, molti software ostili basano i loro attacchi proprio su alcuni accorgimenti adottati dai programmatori per aumentare la facilità d'uso del personal computer. Vediamone alcuni esempi.

Quante volte abbiamo messo un CD-Rom nel lettore e questo immediatamente si è avviato, facendoci vedere un film, ascoltare musica, oppure installando un gioco o un programma? È più raro che accada il contrario: quasi tutti i CD-Rom, infatti, sono dotati di un programma di avvio automatico (autorun) che si attiva non appena sono inseriti nel lettore. Facciamo un'ipotesi: un amico ci porta un CD contenente una copia dell'ultimo film di cassetta, scaricato da Internet (chi è senza peccato scagli la prima pietra). Lo inseriamo nel lettore e, immediatamente, parte il player che ci consente di vederlo ... peccato che, nel frattempo, l'autorun ha provveduto ad installare sul nostro PC un trojan. Esaminiamo le differenze tra i tre sistemi operativi sopra citati: in Windows XP la funzione di autoavvio è **attiva**, a meno che non la disattiviamo, in Mac OS X è **inattiva** a meno che non la attiviamo, in Linux non esiste.

Come si può fare per risolvere il problema? Abbiamo due possibilità: o premiamo il tasto Maiusc (quello che ci permette di scrivere una lettera maiuscola) mentre inseriamo il CD, oppure, ma qui il gioco si fa duro e occorre essere degli esperti, modifichiamo il registro di sistema, che è un file che contiene tutte le impostazioni di Windows.



Illustrazione 3: I tasti Maiusc (o Shift) sono evidenziati da un bordo rosso

Vediamo un'altra possibile fonte di insidie: siamo abituati a riconoscere i file dalla loro icona, che, di solito, identifica anche il programma che li ha creati o li può aprire. Cosa fa sì che il sistema operativo riconosca un file di Word da uno di Excel? Il loro contenuto? In Windows no: il riconoscimento del tipo di file è basato sulla sua estensione, una sorta di cognome. Come dite? Non avete mai sentito parlare delle estensioni? È possibile, infatti Windows le tiene nascoste per evitare che possano essere accidentalmente modificate. Abbiamo scoperto un secondo spiffero nelle nostre finestre: possiamo usare questo fatto per ingannare Windows e fargli credere una cosa per un'altra.

Facciamo un piccolo esperimento: apriamo una qualsiasi cartella e, nel menù *Strumenti*, scegliamo il comando *Opzioni cartella*; nella finestra che si apre clicchiamo sulla scheda

Visualizzazione e scorriamo l'elenco fino a che non troviamo una voce che recita "Nascondi le estensioni per i tipi di file conosciuti": normalmente è spuntata. Con un clic togliamo il segno di spunta e premiamo il tasto *Ok* per uscire dalla finestra. Osserviamo attentamente i file contenuti nella nostra cartella: accanto al nome sono spuntate delle strane sigle, le estensioni, appunto, che identificano il tipo di file.

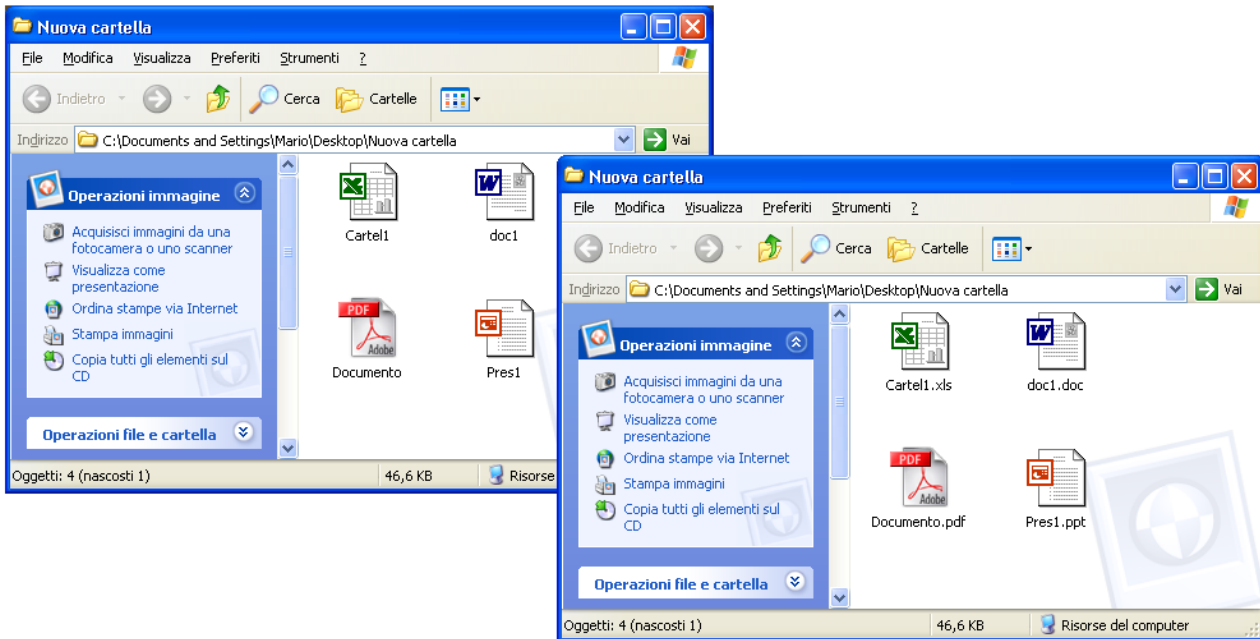


Illustrazione 4: Abbiamo scoperto le estensioni dei file

Adesso farò un piccolo esperimento: seguitemi ma non imitatemi. Seleziono il file *Doc1.doc*, che, secondo quanto mi dice l'icona è un documento di Word, premo il tasto destro del mouse e, dal menù contestuale, scelgo il comando *Rinomina*. Cambio l'estensione del file da *.doc* a *.xls*, ignoro il messaggio di avvertimento che mi informa dei rischi terribili ai quali andrò incontro, et voilà: il mio file di testo adesso presenta l'inconfondibile icona del foglio elettronico. Al doppio clic Excel cercherà, inutilmente, di aprire il mio documento.

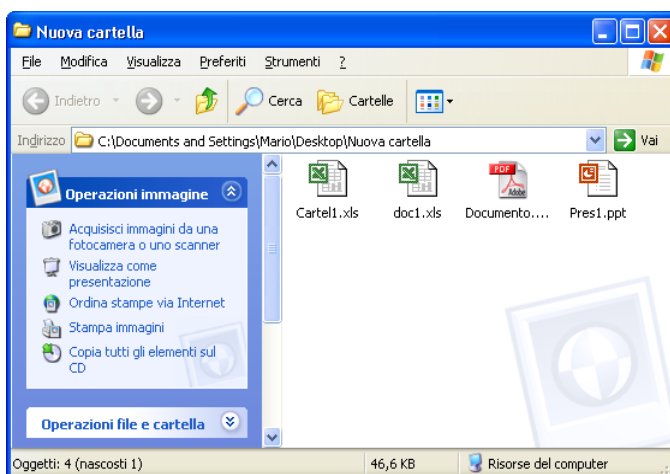


Illustrazione 5: Il file trasformista

Occhio non vede, cuore non duole: Windows ci nasconde le estensioni per evitare che le andiamo a pasticciare, magari per errore, e rendiamo inservibili i nostri file. Dietro a questo lodevole intento, però, si nasconde un'insidia: sono un malintenzionato, creo un virus, gli do un'estensione abitualmente ritenuta innocua e un nome allettante (che so sottoladoccia.jpg, e qui torna in

ballo l'ingegneria sociale) e lo mando per posta elettronica. L'incauto lo vede, riconosce l'icona che è associata ai file di immagine e, spensieratamente, lo apre. A tutto ciò, aggiungiamo il fatto che modificare l'icona di un file non è che sia impresa titanica e capiamo perché uno dei comandamenti esposti nello scorso articolo ci consiglia di diffidare di tutti gli allegati ai messaggi di posta elettronica.

Negli altri sistemi operativi le estensioni o non esistono o sono delle semplici appendici mnemoniche: il file è riconosciuto sulla base del suo contenuto, non di quello che dice il suo nome.

Prima di concludere, fatemi fare un ultimo esempio: vi ho parlato dei cavalli di Troia e dei rischi connessi. Ebbene, in Windows esiste, ed è attivo per impostazione predefinita, una sorta di Trojan horse. Non ci credete? Seguitemi ancora: fate un clic col tasto destro del mouse sull'icona delle *Risorse del computer* e scegliete, nel menù contestuale, la voce *Proprietà*. Nella finestra che si apre scegliete la scheda *Connessioni remote*; cliccate sul pulsante *Avanzate*: dovrebbe esserci un segno di spunta accanto alla voce "Consenti il controllo del computer da postazioni remote" che, tradotto in italiano, significa "Permetti che qualcuno, dall'esterno, controlli il tuo computer". Questa opzione di solito serve a garantire l'assistenza da remoto ma, salvo casi eccezionali (organizzazioni complesse, manutenzione software affidata ad esterni e simili) è assolutamente inutile e costituisce solo una possibile porta d'accesso al vostro sistema.

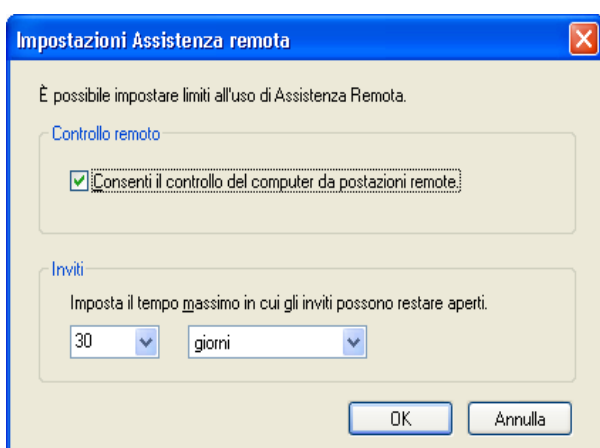


Illustrazione 6: La finestra per attivare/disattivare il controllo remoto

Il problema non è tanto nella possibilità di controllo remoto: è possibile su tutti i PC ed è presente in tutti i sistemi operativi. Quello che costituisce una potenziale fonte di rischio è il fatto che sia attiva senza che l'utente lo sappia.

Oltre a queste vulnerabilità, che sono le più macroscopiche, ogni mese se ne scoprono di nuove: è questo il motivo per cui, con cadenza, appunto, mensile, la Microsoft

rilascia aggiornamenti di sicurezza per i propri programmi.

La morale di questa storia è una sola: lasciare le finestre troppo aperte può farci entrare i ladri in casa. Forse è meglio mettere delle robuste sbarre che ci aiutino a bloccarli. Fuori di metafora, cerchiamo di adottare dei comportamenti attenti nell'uso del computer, quali

quelli indicati in questo articolo. Premiamo il tasto Maiusc ogni volta che inseriamo nel lettore un CD del quale non siamo certissimi, non pensiamo che ci siano allegati a rischio e altri innocui, disabilitiamo il controllo remoto e manteniamo costantemente aggiornato il nostro sistema operativo, oltre, naturalmente, ai nostri software di protezione.

Alla prossima.

Articolo pubblicato per gentile concessione della rivista "Porto e Diporto" della AM editori Srl - Napoli