

- 7 Ritornare in Risorse del computer, fare click col tasto destro su **Z**, scegliere Proprietà >> Protezione. Nel riquadro “Gruppi e utenti” dovrebbe esserci solo Everyone. In “Autorizzazioni per Everyone” lasciare le spunte solo per “Lettura ed esecuzione”, “Visualizzazione contenuto cartella” e “Lettura”; quindi confermare con OK.



La memoria esterna ora può considerarsi immune. Non è possibile in alcun modo scrivere nella *root* né per l'utente né per un eventuale virus; da adesso però i dati possono essere salvati solo nella cartella creata, in questo esempio “Corsi serale”, poiché è stata interdetta la possibilità di scrivere nella *root* della memoria.

Questa procedura è utile soprattutto a chi utilizza un sistema operativo Windows in quanto per chi utilizza sistemi operativi Mac OSX o GNU/Linux, le possibilità di infettare il sistema sono irrilevanti. Anzi, per chi utilizza Mac OSX è una procedura addirittura svantaggiosa in quanto questo sistema operativo può leggere da NTFS ma non scrivervi.

IMPORTANTE: non eseguire mai questa procedura su partizioni del disco rigido perché il computer non si avvia in caso rilevi delle protezioni interne.

Adattamento da un'idea di Gregorio Geppino, Univ. Federico II di Napoli

**I.T.I.S. «Carlo Zuccante»
CORSO SERALE PER ADULTI
corsi di Informatica e di Elettronica**

LE PICCOLE GUIDE PRATICHE

INFORMATICA

4

IMMUNIZZARE UNA PENDRIVE USB PER NON TRASPORTARE VIRUS SUL PROPRIO COMPUTER

sede del corso serale:

Via Astorre Baglioni 22 – 30173 Mestre-Venezia

<http://serale.zuccante.it>

serale@zuccante.it

È ormai diffuso l'uso di memorie di massa USB (pendrive, dischi rigidi esterni...), molto pratiche per trasportare dati da un computer ad un altro. Spesso però oltre ai file questi dispositivi trasportano anche malware e virus.

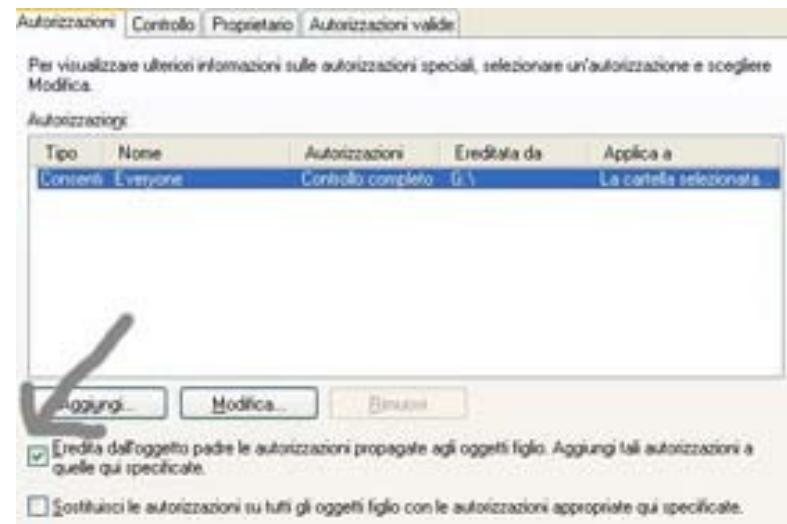
Nulla può essere totalmente sicuro e definitivo in questo campo, anche perché le novità sono quotidiane. Comunque la soluzione qui proposta riduce al minimo la possibilità di infezione, in quanto la memoria viene protetta in maniera ottimale dai virus che si propagano per auto-esecuzione. In altre parole non si può impedire al virus di annidarsi nella pendrive ma, inibendo la sua esecuzione, non può provocare danno, se ne impedisce il replicarsi e, dunque, può essere cancellato definitivamente da qualsiasi software antivirus. La soluzione proposta sfrutta una caratteristica del file system NTFS: le ACL (Access Control List).

Di seguito si descrivono i passaggi per “immunizzare” i dispositivi USB. Si presume l'uso di WinXP Pro, il sistema operativo Windows che utilizziamo nei nostri corsi serali; comunque la procedura è simile anche su Vista. Invece per chi utilizza una Home Edition è necessario avviare il sistema in modalità provvisoria, tenendo premuto il tasto F8 al momento dell'avvio. Per tutti è necessario autenticarsi come Amministratore. Nell'esempio si immagina che il sistema abbia assegnato al dispositivo USB la lettera **Z**.

- 1 Formattare il dispositivo su un computer “sano”, cioè che non sia già infettato, altrimenti si inficia l'intera procedura, scegliendo come file system NTFS.
- 1a Se si lavora su un disco rigido esterno non vi sono problemi; se invece si vuole formattare una pendrive di modeste dimensioni (2 o 4 Gb) Windows non permette di formattare in NTFS. Per aggirare il problema formattare la pendrive in FAT. Quindi avviare la funzione **Terminale** (Programmi >> Accessori >> Prompt dei comandi) e digitare la seguente linea di comando: `CONVERT Z: /FS:NTFS` (dove **Z** è la lettera assegnata).



- 2 Entrare in **Z** e creare una nuova cartella (per esempio “Corsi-serale”).
- 3 Accedere alla **Proprietà** della cartella “Corsi-serale” e scegliere **Protezione**.
- 3a Se **Protezione** non è visibile, allora dal menù a tendina **Strumenti** >> **Opzioni cartella** >> **Visualizzazione** >> togliere la spunta a “Utilizza condivisione file semplice” e quindi OK.
- 4 Dopo aver scelto il tab **Protezione** selezionare il pulsante **Avanzate**
- 5 Selezionare la linguetta **Autorizzazioni** ed eliminare la spunta dalla casella “Eredita dall'oggetto padre le autorizzazioni”; fare click su **Copia** e quindi OK.



- 6 Nel riquadro “Utenti e gruppi” deve esserci solo Everyone e nel riquadro “Autorizzazioni per Everyone” dovrebbero esserci delle spunte sulle varie voci di “Consenti” (Controllo completo - Modifica...). Se così non fosse, eliminare tutte le voci da “Utenti e gruppi” lasciando solo ‘Everyone’ a cui assegnare “Controllo completo”. Confermare con OK.

