

Come eliminare Disk Knight

Inserendo la chiavetta USB appare un'icona nell'area di notifica di Windows: UNO SCUDETTO. Si tratta di un'applicazione autoinstallante in VB6 creata da **Ariful Islam** chiamata **Disk Knight**. Gli Antivirus e antispyware non lo vedono!! (con me ha funzionato, ma non mi prendo alcuna responsabilità! **Leggete tutto con attenzione prima di iniziare e attenti alla dattiloscrittura**).

PASSO 1

Eliminazione dalla chiavetta USB

Selezionare il percorso Start -> Programmi -> Accessori -> Prompt dei comandi.
Appare la finestra DOS

1. supponendo che la vostra chiavetta sia riconosciuta come disco E:\, una volta inserita da DOS digitare con le esatte **maiuscole** e **spazi** (ve li ho indicati con **_**): **dir_E:\A:_h**.
2. In questo modo verranno visualizzati i *files* della chiavetta e, se infetta, anche la presenza di due *files*: "**autorun**" e "**knight**".
3. come eliminare **autorun**: si digita sempre in DOS **del_/f_/P_/A:H_E:*autorun***, quindi si da conferma con "**S**".
4. come eliminare **knight**, si digita sempre in DOS **del_/f_/P_/A:H_E:*knight***, quindi si da conferma con "**S**".
5. a questo punto la chiavetta è pulita, **ma non reinseritela** nel PC che è ancora infetto!!

oppure

Se non visualizzate i file nascosti e di sistema dovete eseguire il percorso Strumenti -> Opzioni Cartella -> Visualizzazione e selezionate "Visualizza Cartelle e File Nascosti" e deselezionate "Nascondi File Protetti di Sistema".

A questo punto se avete **Disk Knight** nella vostra chiavetta dovreste visualizzare un eseguibile chiamato **Knight** e un **Autorun.inf**: eliminate questi file, estraete la chiavetta e NON reinseritela.

PASSO 2

Eliminazione dal PC:

Premendo contemporaneamente CTRL+ALT+CANC si attiva la finestra Protezione di Windows controllate in Task Manager i processi in esecuzione e se esiste un processo che si chiama **Knight** terminatelo;

1. andate in Pannello di Controllo -> Installazione Applicazioni cercate Knight e se c'è rimuovetelo;
2. andate in Start -> Cerca -> File o cartelle ed inserite **Knight**. Rimuovetene tutti i *files* trovati;
3. **attenzione** a questa procedura: andate in Start -> Esegui e digitate **regedit** quindi INVIO, dalla finestra che appare si seleziona il percorso Modifica -> Trova e si scrive **knight**. Eliminate tutte le chiavi di registro con scritto **knight** o **disk knight** .
4. Leggete con attenzione non quelle con scritto, per esempio, "knightj" o cose simili altrimenti si potrebbero bloccare altri programmi di sistema.

Dovete fare tutti questi passaggi perchè altrimenti il programma non si disinstalla completamente !!

Per ulteriori informazioni:

http://www.mikeyleung.ca/mikiwiki/index.php?title=Disk_Knight

<http://www.sophos.com/virusinfo/analyses/diskknight.html>

<http://www.mikeyleung.ca/2007/08/07/disk-knight/>