

DEBELLARE IL VIRUS GUARDIA DI FINANZA, POLIZIA



Ultimamente è molto diffuso un virus relativo ad un falso annuncio della **Guardia di Finanza** o della **Polizia**. Dopo avere preso l'infezione, avviando il computer resterete bloccati in una finestra che riporta:

Il logo della guardia di finanza o della polizia

Una scritta che ci accusa di avere nel computer contenuti illegali.

La richiesta di un pagamento di 100 euro per ripristinare le funzionalità del PC.

Non vi sarà possibile andare avanti ed il computer resterà bloccato.

In questo caso sappiate che si tratta di un virus (dal nome Trojan.Win32.FakeGdF.A) e che stanno cercando di truffarvi. Non dovete assolutamente PAGARE NULLA. Per eliminare il virus seguite le istruzioni sotto riportate.

A) Se il pc parte e subito dopo compare la schermata del virus:

1. Scollegate il pc dalla rete e da internet, quindi avviate lo;
2. Bisogna essere veloci, **prima** che il pc carichi tutto il sistema, appena compare la schermata del desktop premere ctrl-alt-canc e attendere che si apra il Task manager, portarsi **subito** nel tab "Processi", e se notate qualche nome strano tipo: wgwkgwkgwg.exe o simile, selezionatelo **immediatamente** e premete "Termina". Potrebbero essere anche più di uno;
3. Se siete riusciti a non far caricare il virus, eliminiamo tutte le altre tracce del malware entrando nell'utilità *Ripristino configurazione di sistema* di Windows (Start – tutti i programmi – accessori – utilità di sistema). Qui possiamo ripristinare il pc alle impostazioni di qualche giorno prima dell'infezione. Fine.

B) Se non è possibile entrare nel task manager (ctrl-alt-canc), bisogna far partire il pc da modalità provvisoria, avviate lo e dopo il controllo del bios premete F8. Caricata la modalità

provvisoria, andate nel registro di sistema (start – esegui – scrivete regedit e poi premete invio), e verificare queste chiavi di registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system

se presente, il valore DisableTaskMgr deve essere impostato a 0 altrimenti non si potrà aprire il task manager di Windows. Poi controllare le seguenti voci:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunEx

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunEx

Verificare che non ci siano file strani in avvio tipo WPBT0.dll, Oxxxxxxx.exe, wgwgggw.exe, etc. Poi posizionarsi su:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

controllate che il valore “Shell” sia solo Explorer.exe.

Se non c’è dovrete inserirlo voi manualmente.

Più sotto, sempre nel ramo “shell” trovate un’altra voce denominata **Userinit**. Deve avere come valore **SOLO** C:\Windows\system32\userinit.exe, (con la virgola).

Fatto questo riavviate il pc e il virus dovrebbe essere debellato.

C) Se non funziona ctrl-alt-canc e non funziona la modalità provvisoria in quanto visualizziamo una schermata blu, abbiamo bisogno di un altro strumento per far partire il pc anziché il nostro disco fisso. Dobbiamo preparare un CD autopartente o meglio una chiavetta USB autopartente che carichi in RAM un Sistema Operativo di Emergenza che ci consenta di modificare il sistema bloccato.

Da un altro computer funzionante scarichiamo [questo file ISO](#), successivamente preleviamo il software aggiuntivo *Rescue2USB* ([cliccare qui](#) per il download).

Rescue2USB è un programma che consente di preparare una qualunque chiavetta USB rendendola avviabile e memorizzandovi il file ISO di Kaspersky Rescue Disk. Così facendo, lasciando inserita all'avvio del personal computer la chiavetta, si potrà avviare Kaspersky Rescue CD.

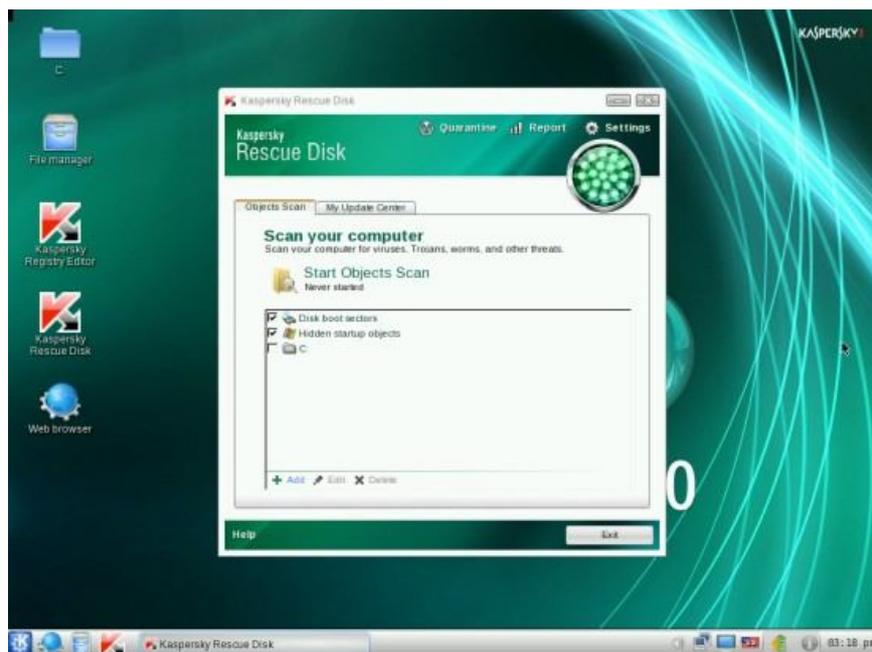
Una volta scaricato ed avviato *Rescue2USB*, si potrà inserire automaticamente il Rescue Disk di

Kaspersky in una chiavetta USB: basta selezionare il file ISO di Kaspersky Rescue Disk precedentemente scaricato, l'unità USB di destinazione quindi fare clic sul pulsante *Start*. *Rescue2USB* cancellerà tutto il contenuto della chiavetta USB, perciò usate una chiavetta vuota.



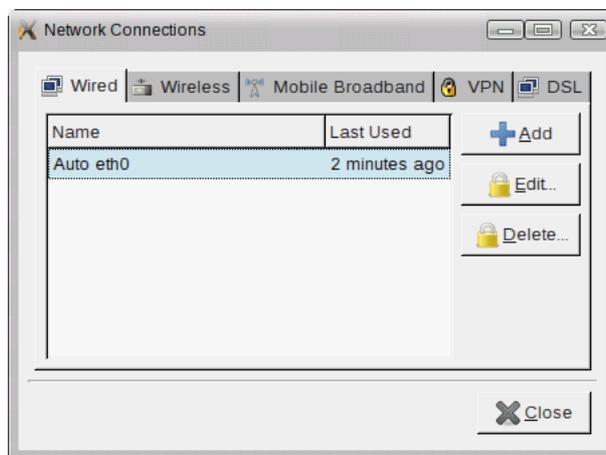
Una volta concluso il procedimento di creazione della chiavetta autopartente, inserirla in una porta USB del computer, avviatelo da supporto USB (controllare dal BIOS **la corretta sequenza di avvio: unità USB prima**, hard disk poi).

Così facendo al boot del sistema ci ritroveremo la schermata di Kaspersky Rescue Disk, premiamo un tasto qualsiasi e scegliamo la lingua, poi premiamo 1 per accettare la licenza, scegliamo *Kaspersky Rescue Disk Graphic mode*. Al termine della fase di caricamento dell'ambiente di lavoro, ci si troverà dinanzi ad una finestra simile al desktop di windows.



Premiamo il tasto in basso a sinistra (al posto di start di windows), e dal menù a tendina verificiamo la correttezza delle impostazioni di rete, premendo web browser. Proviamo a navigare in qualche sito e verificiamo che funzioni internet.

In caso contrario, è necessario cliccare sulla voce *Network setup* del menù di avvio quindi selezionare l'interfaccia di rete da impostare (wired o wireless):



Facendo clic sul pulsante *Edit*, si potranno eventualmente assegnare in modo manuale le impostazioni di rete (indirizzo IP, gateway, DNS).

Dopo aver completato quest'operazione, si dovrà tornare alla schermata iniziale, fare clic sulla scheda *My Update Center* quindi su *Start update*:



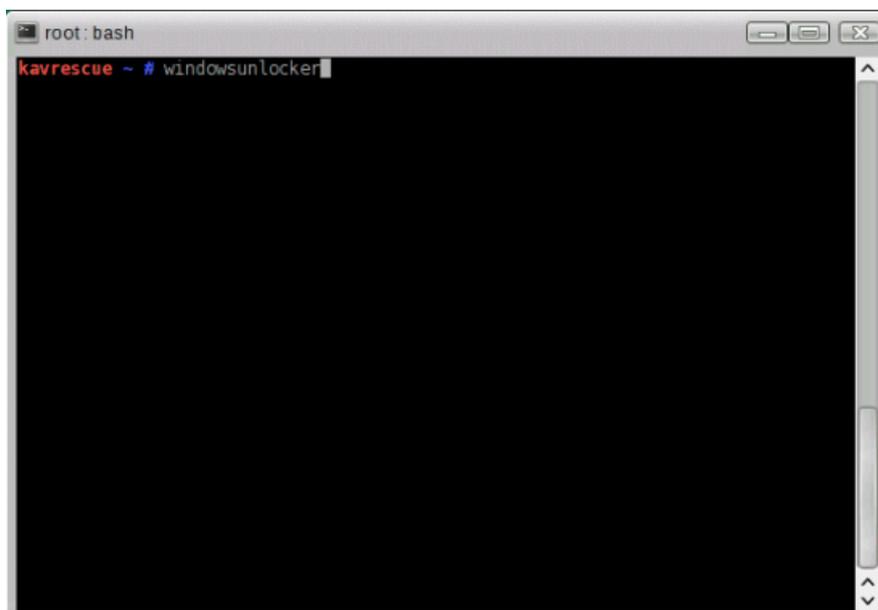
Così facendo aggiorneremo i database delle firme di Kaspersky. Queste informazioni verranno automaticamente salvate, all'interno di C:\Kaspersky Rescue Disk 10.0. In questo modo, ogniqualevolta si riutilizzerà il supporto di Kaspersky Rescue Disk, non saremo costretti a ricaricare manualmente gli aggiornamenti dell'antivirus.

Per avviare una scansione antimaleware, si dovrà tornare alla scheda *Objects scan*, selezionare tutte

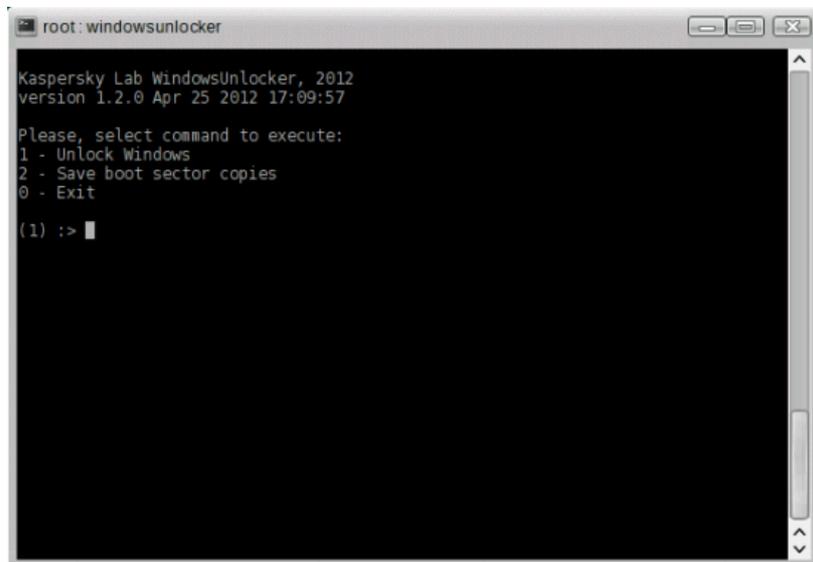
le voci in elenco (*Disk boot sectors*, *Hidden startup objects* e la lettera identificativa di unità corrispondente al disco C:):



Dopo aver spuntato le caselle corrispondenti premiamo *Start objects scan*. Al termine della scansione potremo anche stampare il report della stessa sotto forma di file. A questo punto suggeriamo di avviare lo strumento *Kaspersky Windows Unlocker* eseguibile cliccando sul pulsante in basso a sinistra, scegliendo *Terminal* quindi digitando `windowsunlocker`:



Questa applicazione provvederà a controllare il registro di sistema rilevando e rimuovendo ogni traccia di eventuali infezioni da malware. Alla comparsa del menù seguente, si dovrà premere semplicemente il tasto Invio:

A screenshot of a terminal window titled "root : windowsunlocker". The text inside the terminal reads: "Kaspersky Lab WindowsUnlocker, 2012", "version 1.2.0 Apr 25 2012 17:09:57", "Please, select command to execute:", "1 - Unlock Windows", "2 - Save boot sector copies", "0 - Exit", and "(1) :>". The cursor is positioned at the end of the prompt line.

```
root : windowsunlocker
Kaspersky Lab WindowsUnlocker, 2012
version 1.2.0 Apr 25 2012 17:09:57
Please, select command to execute:
1 - Unlock Windows
2 - Save boot sector copies
0 - Exit
(1) :>
```

Sugeriamo quindi di premere il tasto "2" ed Invio (*Save boot sector copies*) ed uscire dall'utilità premendo "0" quindi ancora Invio.

A questo punto, dal desktop di Kaspersky Rescue Disk, fare doppio clic sull'icona *Kaspersky Registry Editor*, una utilità che permette di aprire il registro di sistema di Windows, verificarne la configurazione ed eventualmente modificarne chiavi e valori.

Ora possiamo fare un'ultima verifica alle chiavi descritte nel punto B) e debellare finalmente il virus.