La rimozione dei virus della famiglia “ZBOT” tramite il “Kaspersky Removal Tool”

Introduzione

In seguito ad alcune segnalazioni di frodi ricevute da nostri clienti, il Nucleo Frodi Internet di BNL informa che alcune case di produzione di software antivirus mettono a disposizione strumenti mirati per la rimozione dei virus, che i clienti possono scaricare per bonificare i propri PC.

In questo documento ci limitiamo a dare alcune semplici indicazioni per aiutare i nostri clienti a difendersi da un virus o da una variante della famiglia di virus “ZBOT” (rilevato anche come "PWS-Zbot", "Win32/Ursap", "Trojan-Ransom.Win32.PornoAsset", "Trojan-Ransom.Win32.Gimemo").

Lo strumento di rimozione di questo virus è il “Kaspersky Removal Tool”, disponibile online gratuitamente.

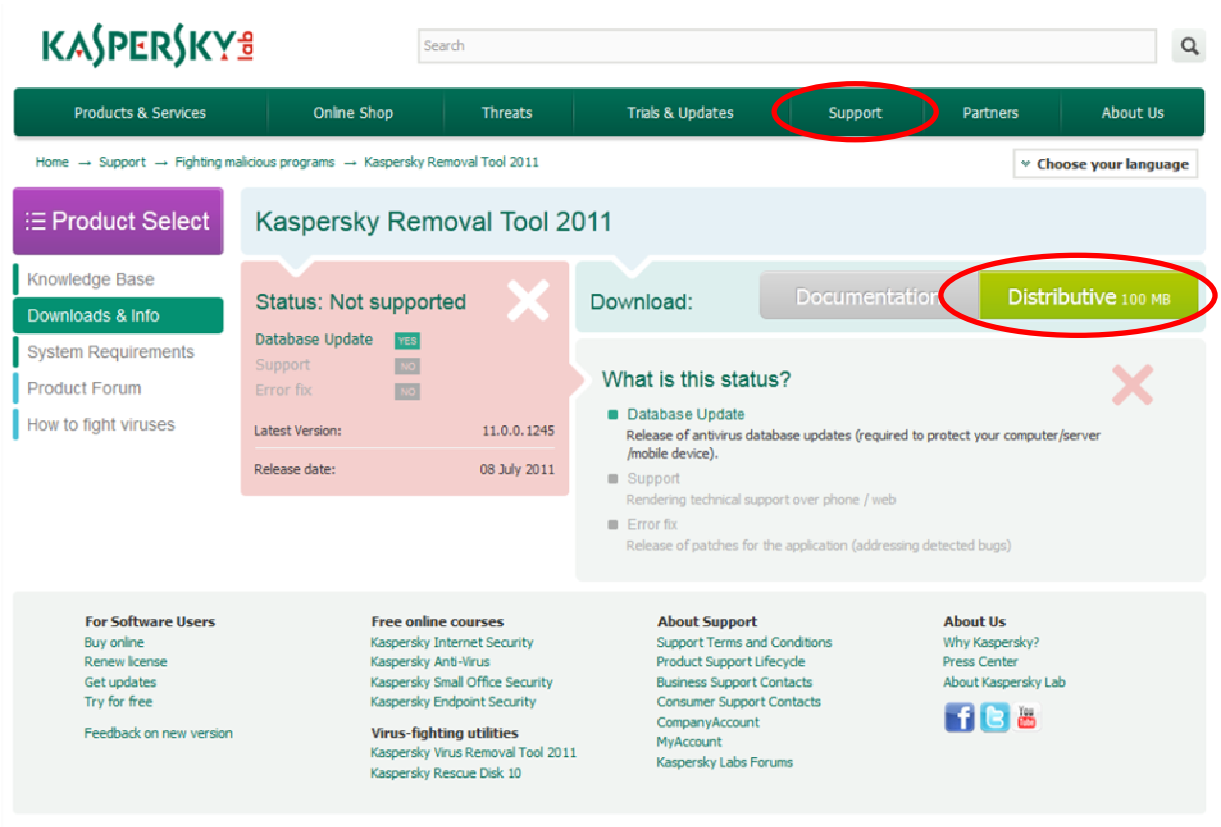
Link

Il link al Kaspersky Removal Tool che suggeriamo di utilizzare è il seguente:

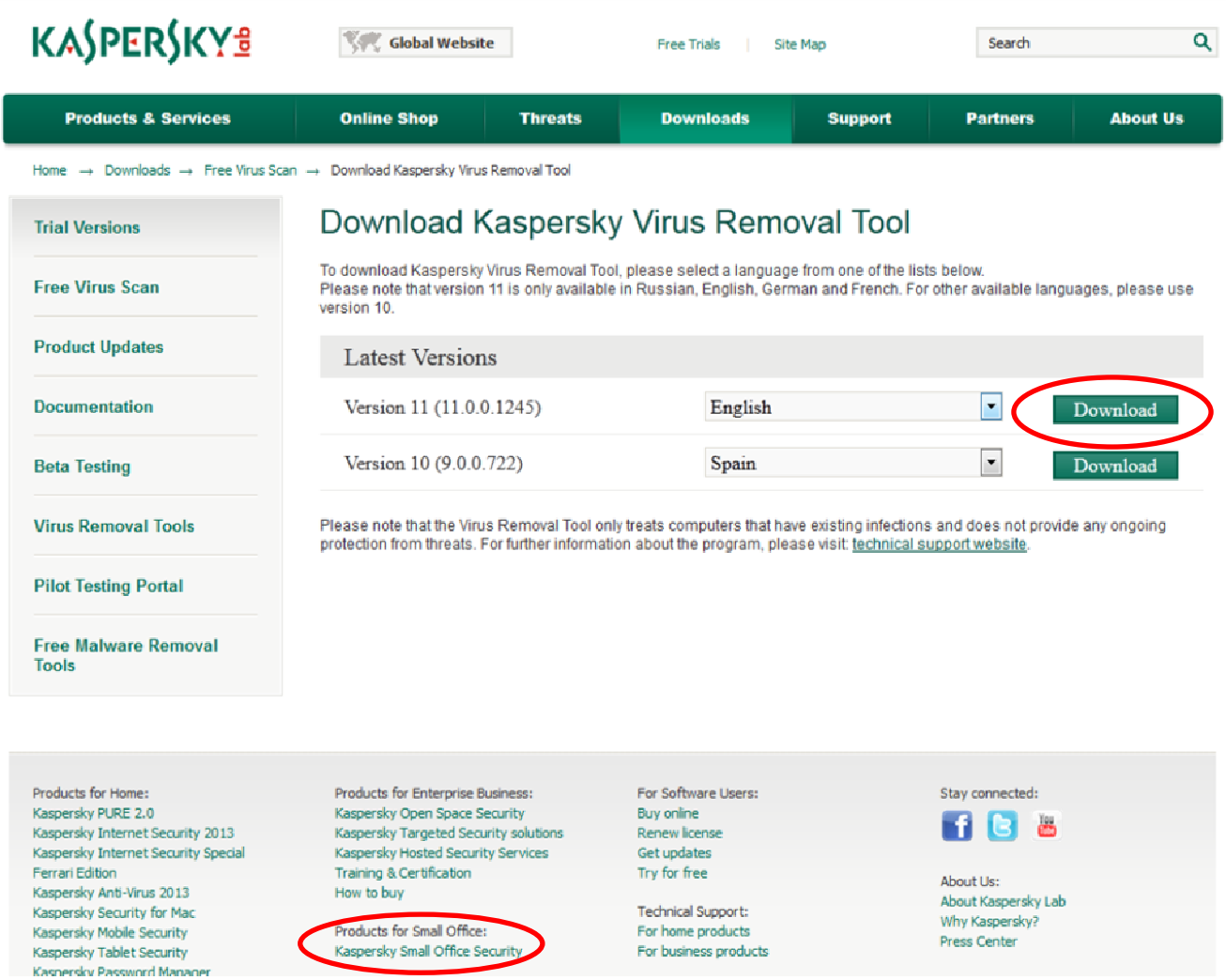
http://support.kaspersky.com/viruses/avptool2011?level=2#downloads

Questo link potrebbe cambiare nel tempo e rendere di fatto non raggiungibile il file così come da noi indicato. Consigliamo quindi di entrare nella sezione di SUPPORTO del sito http://www.kaspersky.com/ cliccando su **SUPPORT** o recandosi direttamente all'indirizzo: http://support.kaspersky.com/ e cercando in basso nella pagina la sezione "**Virus-fighting utilities**" nella quale è presente il link al "Kaspersky Virus Removal Tool 2011"

Da questa pagina, cliccare sul pulsante "DISTRIBUTIVE"



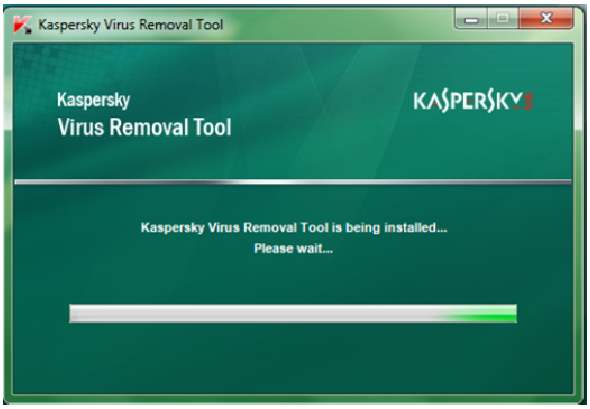
Sulla pagina seguente selezionare la versione da scaricare. Consigliamo di scaricare l'ultima versione disponibile, che spesso non è in lingua italiana ma INGLESE. Cliccare a questo punto sul relativo pulsante "**DOWNLOAD"**:



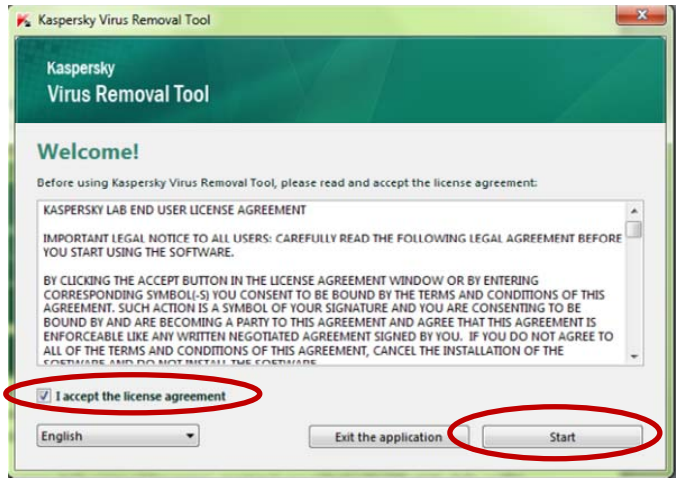
Il file è di grandi dimensioni (circa 150 megabytes). Specificare un percorso nel quale salvare il file e attendere il completamento del DOWNLOAD.

Istruzioni di utilizzo

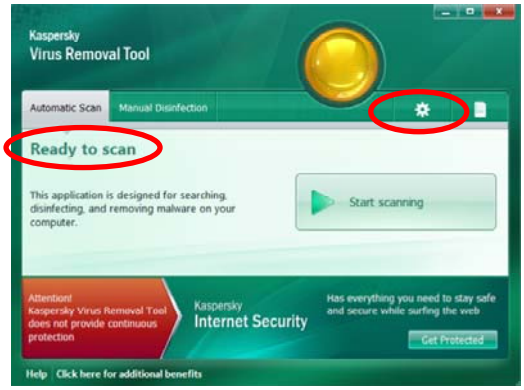
1. Eseguire il programma di installazione facendo doppio click sul file appena salvato (setup_11.0.0....etc). Il software installerà dei file temporanei.



2. Attendere che l'applicazione mostri la schermata di benvenuto: "Welcome!" e accettare le condizioni di utilizzo selezionando la casella "I accept the license agreement" e quindi avviare l'applicazione cliccando sul tasto "Start".

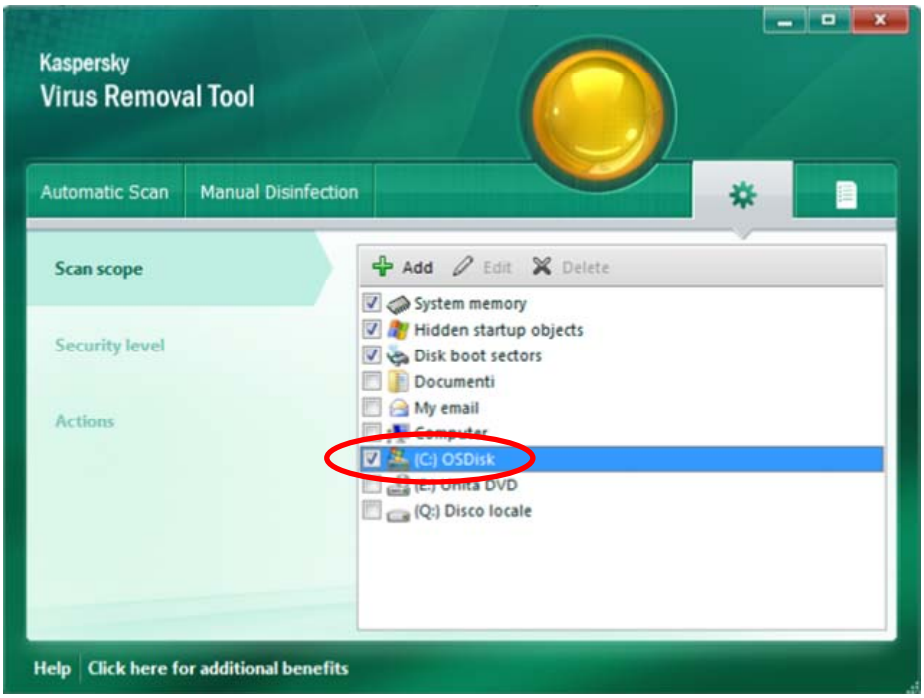


3. Il programma, al termine delle prime elaborazioni, mostrerà una videata identificabile dalla scritta "Ready to Scan".

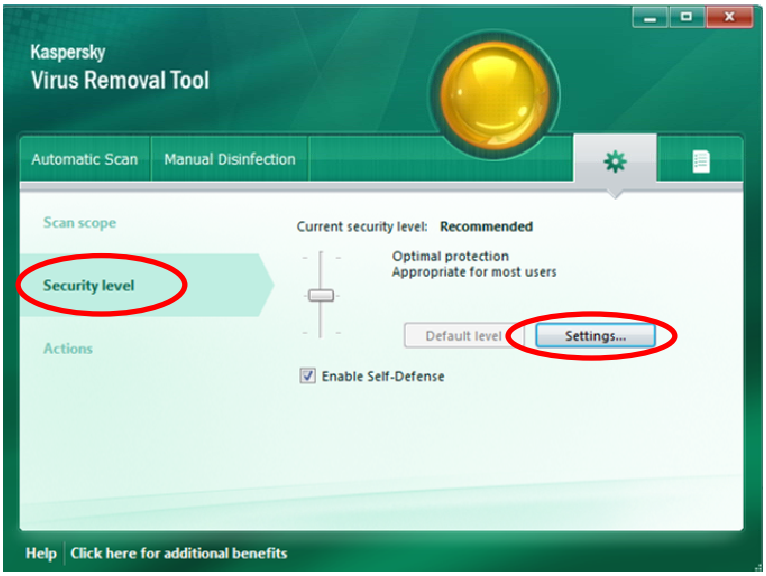


4. In questa schermata, cliccare in alto a destra sul tasto con il simbolo dell'ingranaggio.

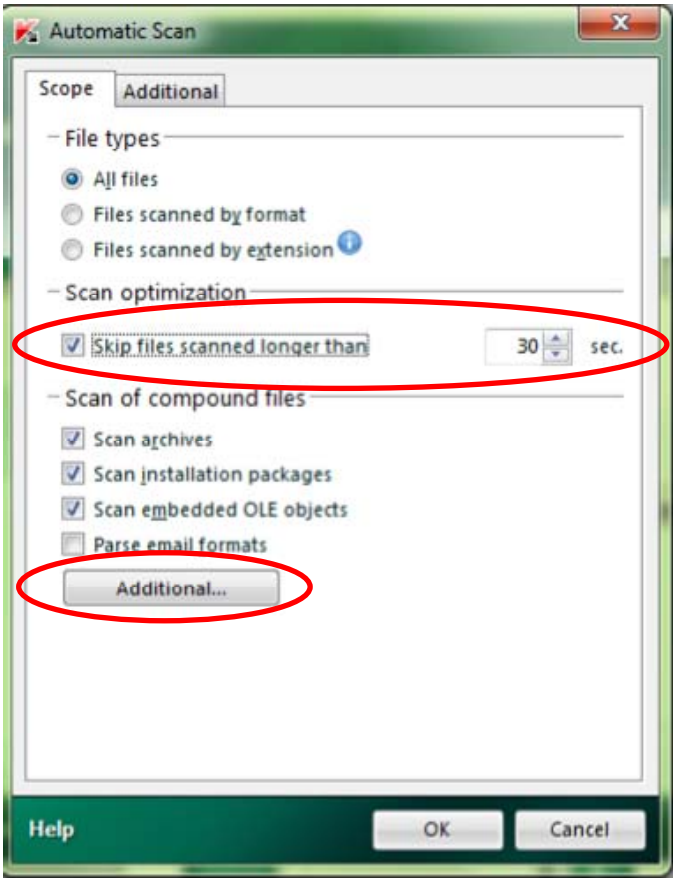
5. Nella schermata successiva, selezionare le unità da verificare (mediante il flag "visto") nella casellina relativa al proprio disco di sistema "C:"



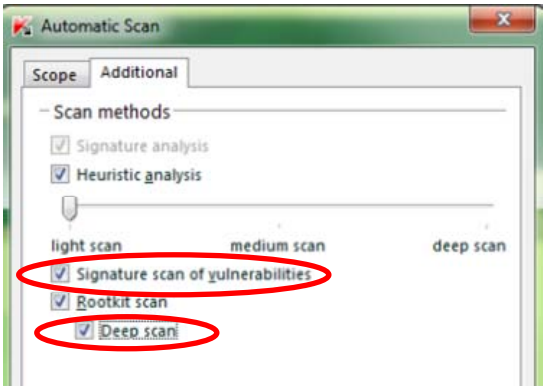
6. Sulla sinistra selezionare “**SECURITY LEVEL**” e cliccare a questo punto su “**SETTINGS**”



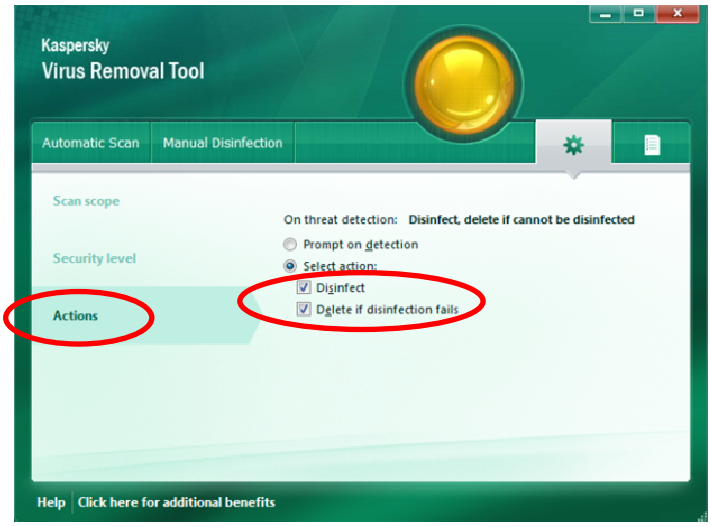
7. Nelle impostazioni selezionare la voce “Skip files scanned longer than” e “30” sec. Cliccare poi sul pulsante “**Additional**”



8. Selezionare “Signature scan of vulnerabilities” e “Deep scan”

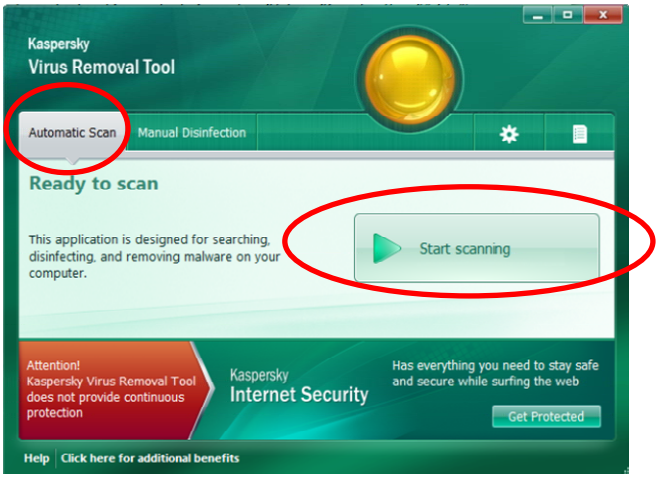


9. Selezionare sulla sinistra “**Actions**” e cliccare sulle opzioni “DISINFECT” e “DELETE IF DISINFECTION FAILS”.
   In questo modo il software procederà automaticamente senza richiedere l’intervento di un operatore.

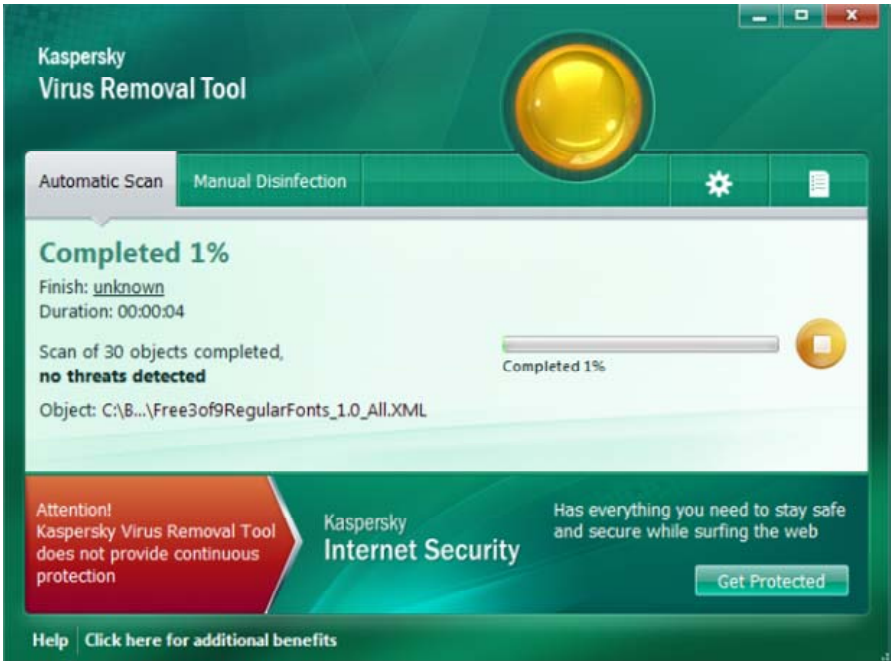


10. Cliccare in altro a sinistra su “**Automatic Scan**”

11. Cliccare a destra a metà schermo sul tasto verde “Start scanning”:



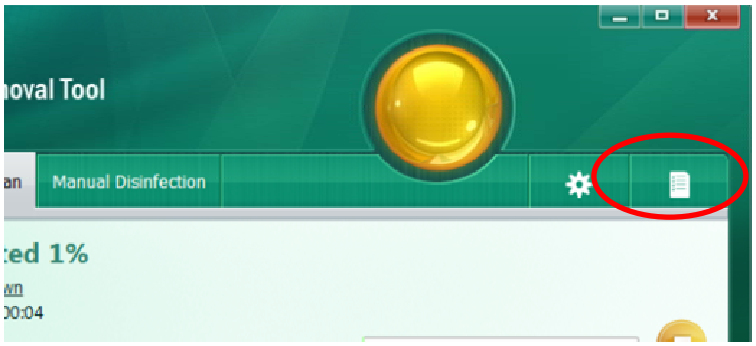
A questo punto inizierà la scansione completa del disco C: (a sinistra verranno indicati quanti file sono stati scansionati, il tempo trascorso dall’inizio della scansione, etc).



Ad ogni virus rilevato, il programma farà apparire in basso a destra una finestra di ALERT con i bordi rossi dove verranno indicati il nome del file infetto, il nome del virus e l’azione che si intende intraprendere.

IMPORTANTE: chiediamo gentilmente a questo punto di **PRENDERE NOTA** dei virus identificati in modo da comunicarli a BNL (v. oltre) per eventuali indagini.

Nel caso in cui si sia scelta la rimozione automatica, la lista dei virus e delle vulnerabilità trovate sarà presente in un log al quale si può accedere cliccando sull'icona "documento" posta accanto all'ingranaggio:



In tal modo è possibile SALVARE i file di log cliccando su SAVE e inviarli via mail a NucleoAntifrodeInternet@bnlmail.com.

Se non si è scelta la rimozione automatica, il programma termina con la lista di file e di virus presenti e a questo punto è possibile scegliere come azione **DELETE** ed eliminare il VIRUS dal proprio disco fisso.

Per alcuni virus, la procedura di pulizia potrebbe richiedere un riavvio del computer.

Consigliamo di riavviare il PC ed eseguire nuovamente l'applicazione di rimozione.

NOTA IMPORTANTE

Nonostante in molti casi la procedura sopra descritta funzioni correttamente, consigliamo comunque di **ripristinare il sistema operativo** reinstallando completamente il computer infetto, formattando e azzerando tutti i dati presenti sul disco del computer. Solo in questo caso si infatti può avere la certezza di aver eliminato ogni traccia del virus.

SUGGERIMENTI

Consigliamo inoltre, successivamente alla reinstallazione del computer, l'installazione di un **antivirus commerciale**, meglio se in versione "Internet Security" e meglio se una versione a pagamento.

Di seguito alcuni degli antivirus che ci sentiamo di consigliare:

- McAfee “Internet Security”
- Kaspersky “Internet Security 2012”
- Trendmicro “Maximum Security 2012”

Ricordiamo inoltre che qualsiasi software antivirus può non essere in grado di bloccare le infezioni se non correttamente aggiornato. Invitiamo quindi tutti i clienti ad **aggiornare regolarmente il proprio software antivirus** ad ogni utilizzo del PC o ad impostare il software in modo da scaricare gli aggiornamenti ad ogni riavvio del PC.