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.

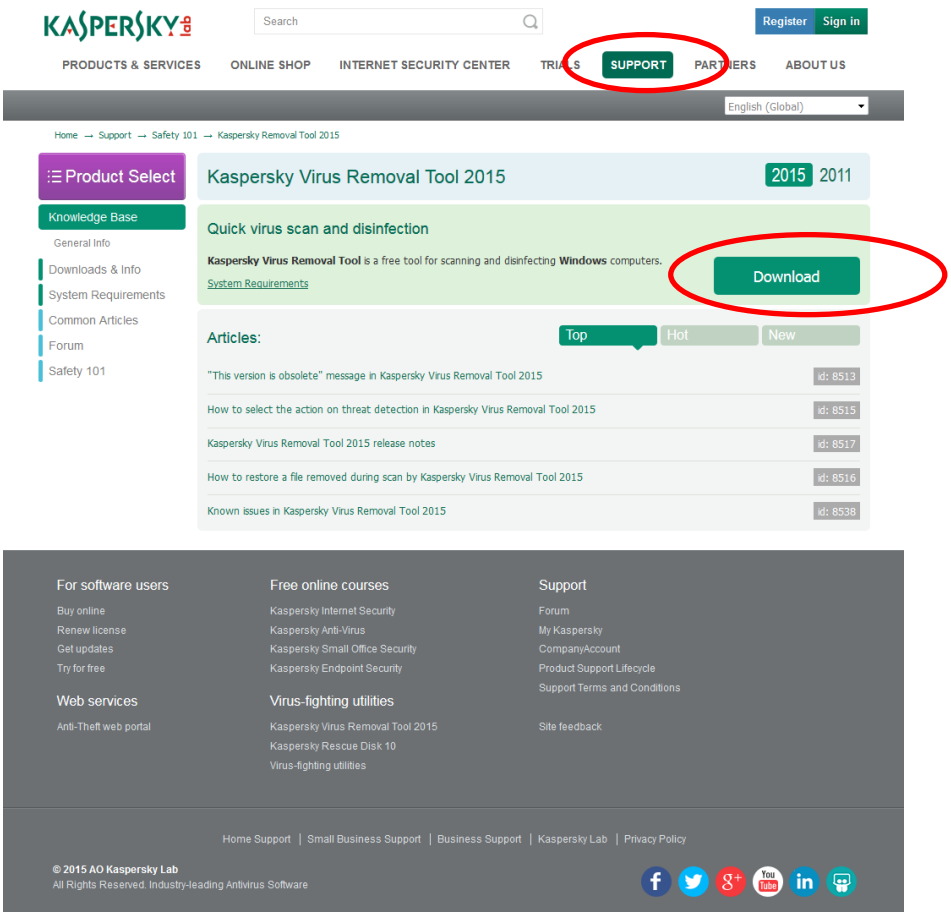
Link

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

http://support.kaspersky.com/viruses/kvrt2015

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 2015"

Da questa pagina, cliccare sul pulsante "Download"

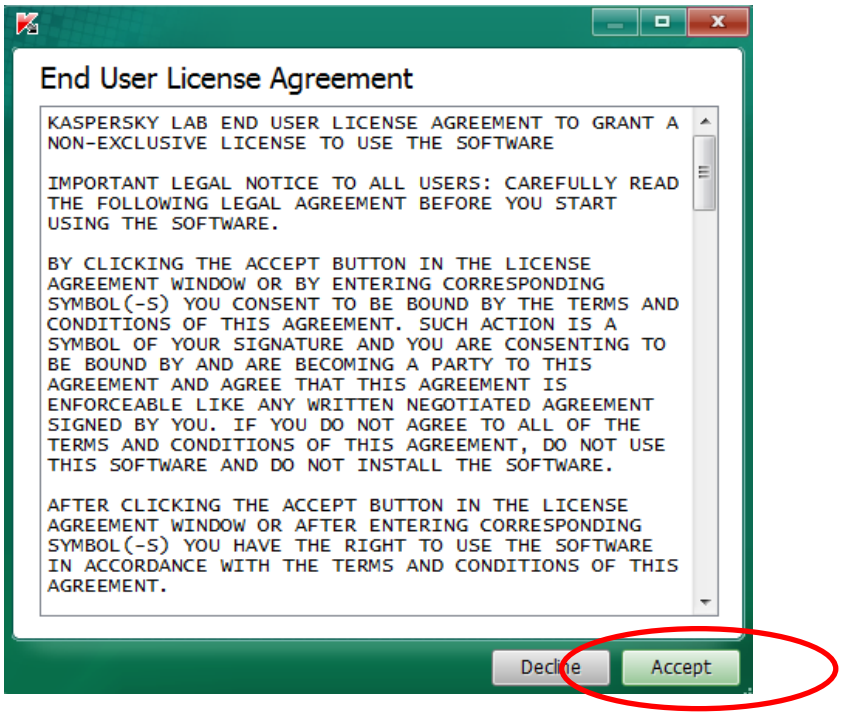


Il file è di grandi dimensioni (circa 150 megabytes). Specificare un percorso nel quale salvare il file e attendere il completamento del DOWNLOAD.

Istruzioni di utilizzo

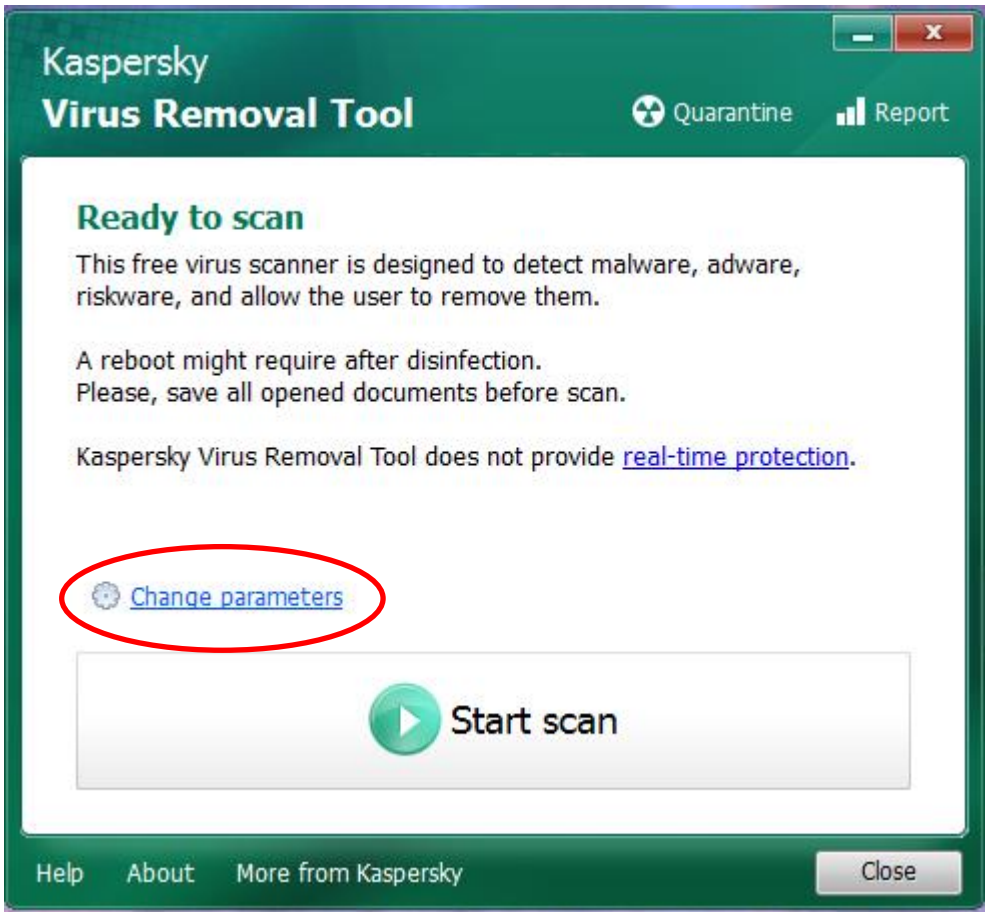
1. Eseguire il programma di installazione **KVRT.EXE** facendo doppio click sul file appena salvato, il software installerà dei file temporanei.

2. Attendere che l'applicazione si avvii e accettare poi le condizioni di utilizzo cliccando su tasto "Accept"



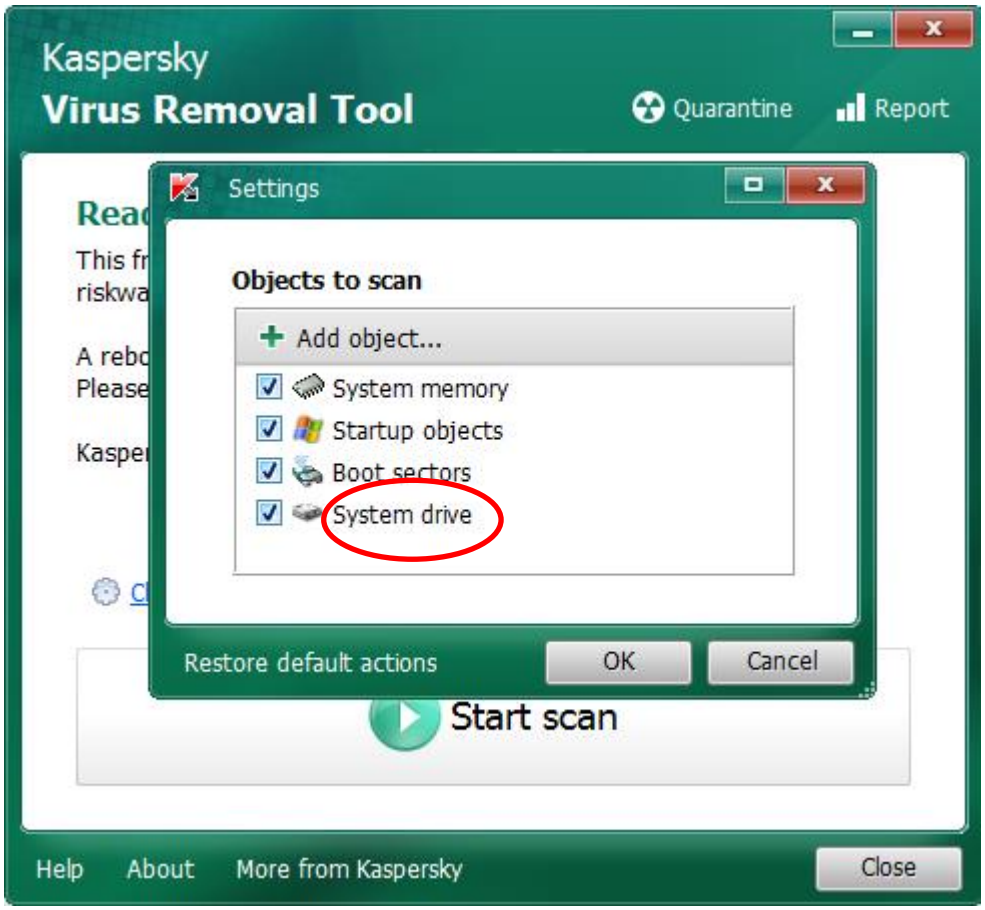
Il programma si avvierà mostrando una barra di progresso:

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

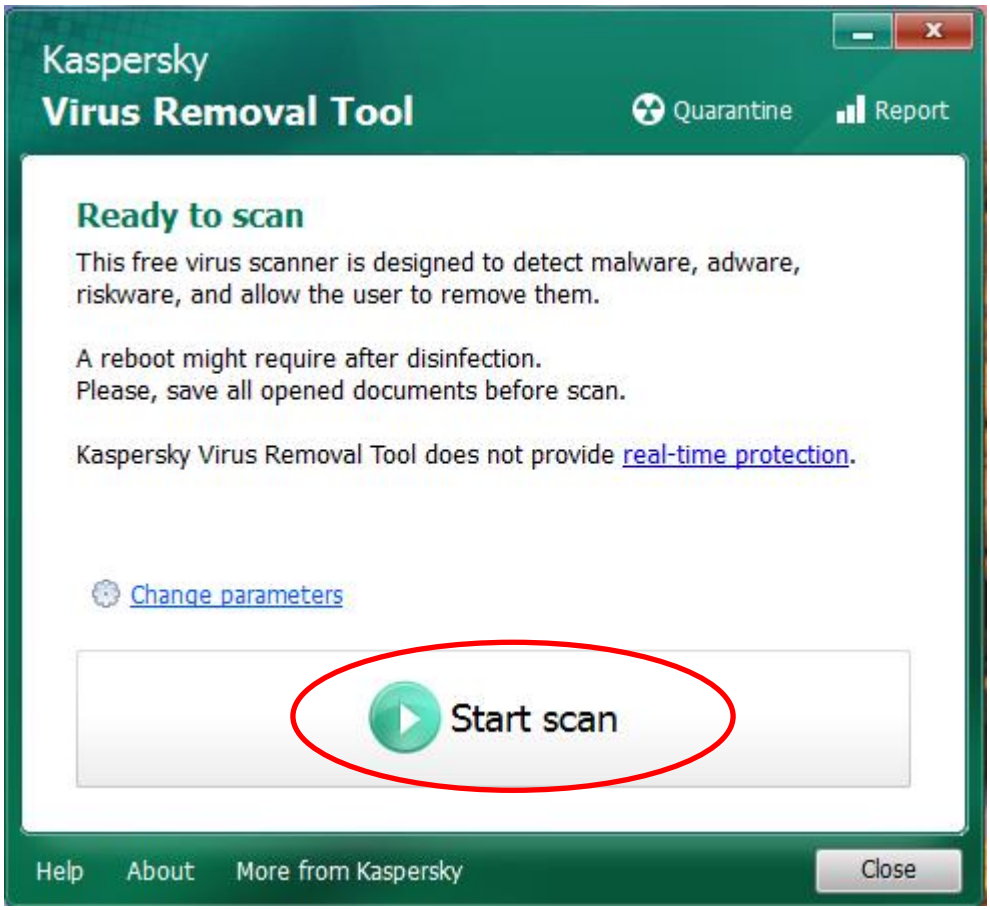


In questa schermata, cliccare sul link in basso con il simbolo dell’ingranaggio “CHANGE PARAMETERS”

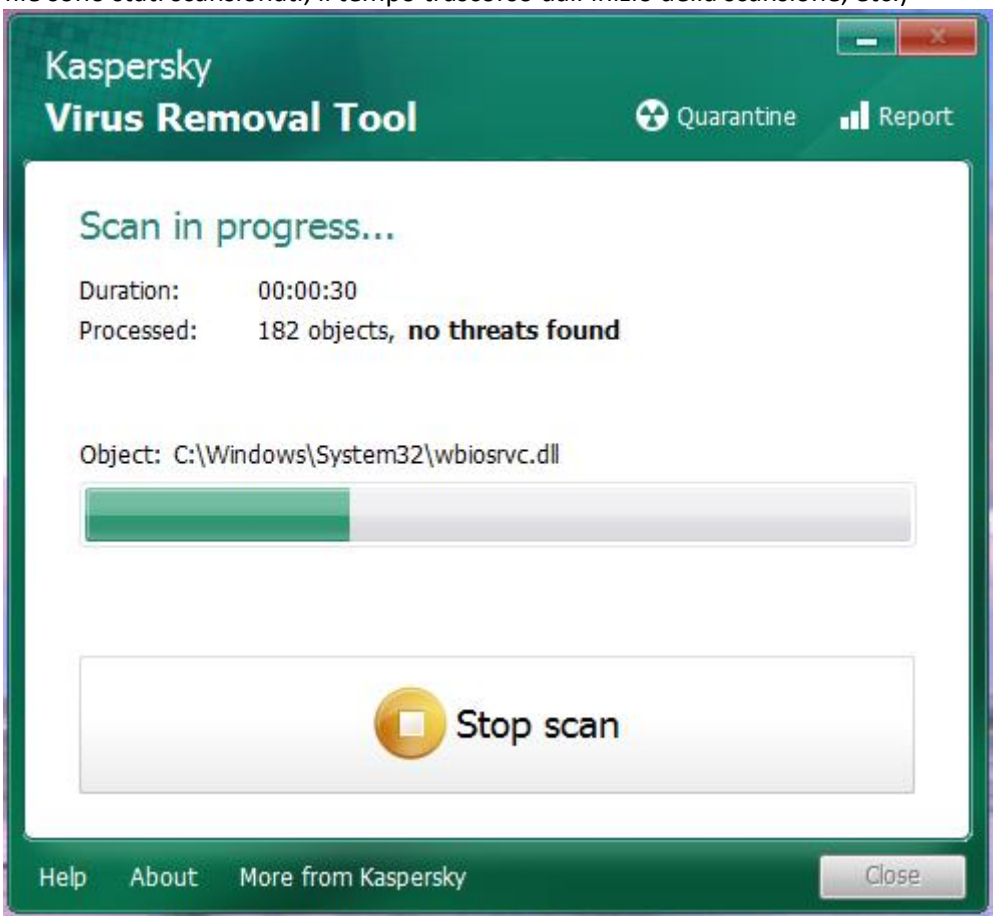
4. Nella schermata successiva, selezionare le unità da verificare (mediante il flag “visto”) nella casellina relativa al proprio disco di sistema “System drive”



5. Cliccare sul pulsante “START SCAN”

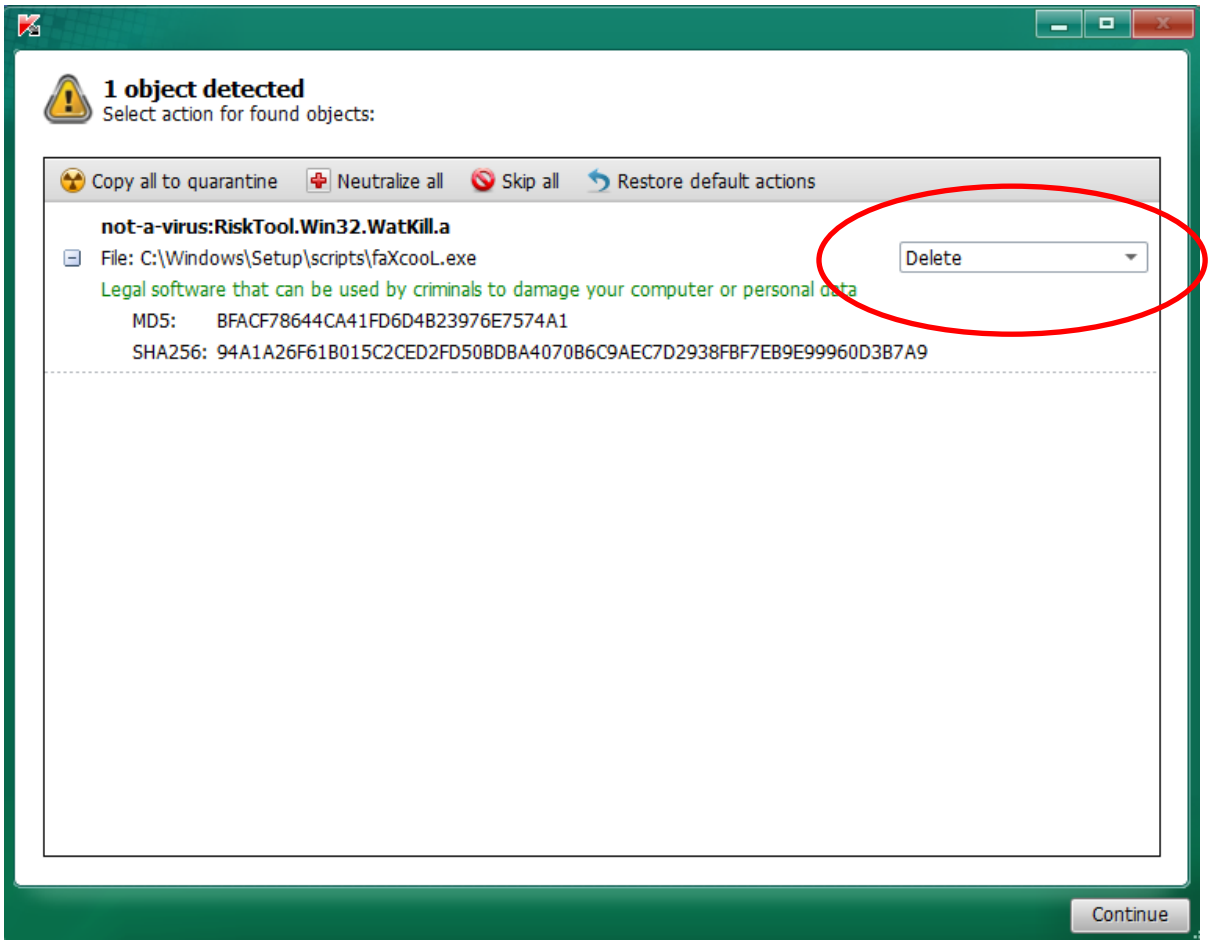


6. A questo punto inizierà la scansione completa del sistema (a sinistra verranno indicati quanti file sono stati scansionati, il tempo trascorso dall'inizio della scansione, etc.)

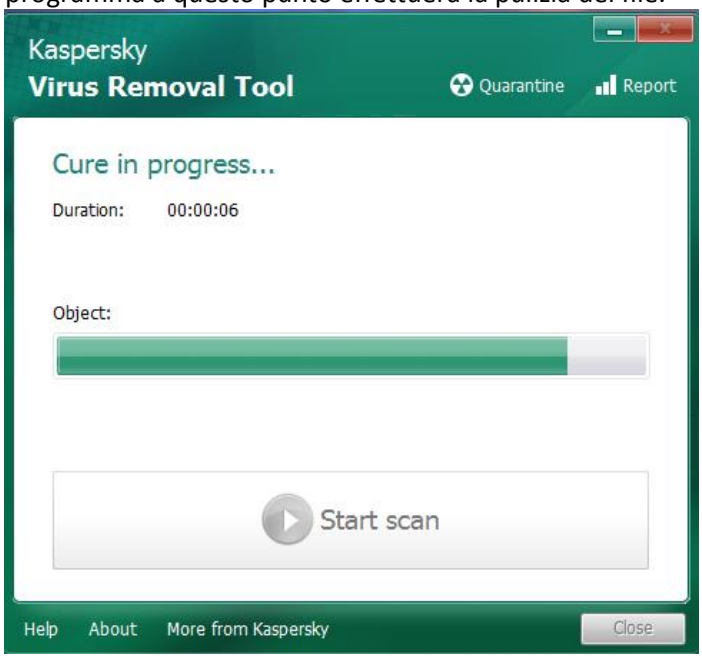


Ad ogni minaccia rilevata, il programma farà apparire accanto ai file scansionati, un progressivo dei file compromessi o infetti.
Cliccando sul pulsante in alto a destra "REPORT" verranno mostrati dettagli dei file individuati come infetti o pericolosi.

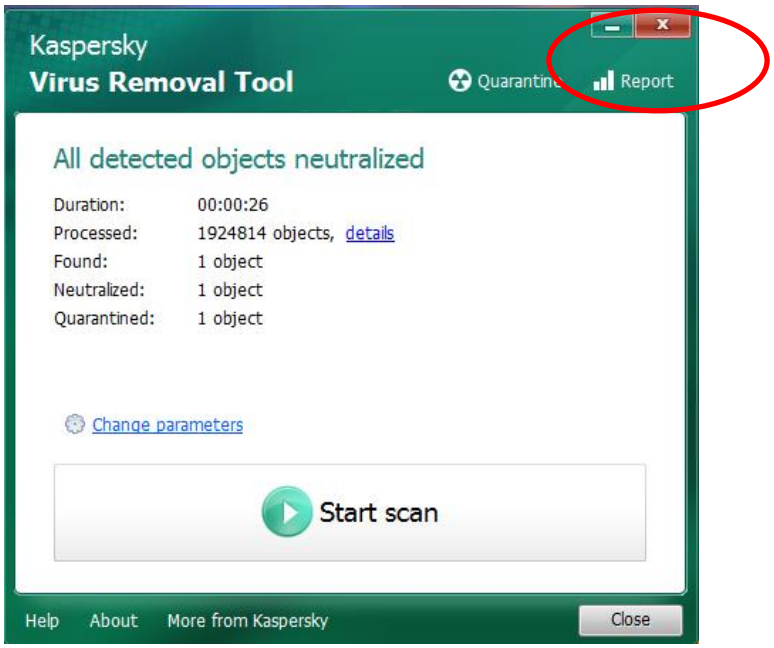
7. Accanto ad ogni file verrà mostrato un menù a tendina nel quale bisognerà selezionare la voce “DELETE” e infine cliccare sul tasto “CONTINUE” in basso a destra.



8. Il programma a questo punto effettuerà la pulizia dei file.

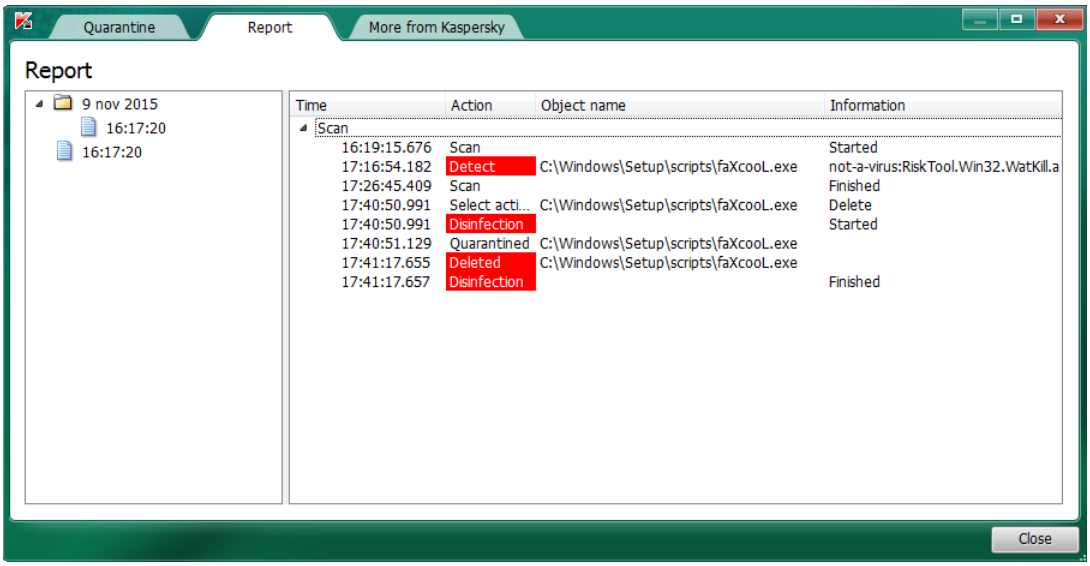


9. Al termine della pulizia, verrà mostrata una videata riepilogativa dove viene indicato il numero di files infetti rilevati, il numero dei files neutralizzati o messi in quarantena



Al termine della disinfezione, cliccando sul tasto REPORT in alto a destra nella videata di riepilogo, viene mostrata l'attività svolta dal programma per neutralizzare la minaccia.

10. 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 per eventuali indagini.

Se possibile, acquisire la schermata come immagine ed inoltrarli via mail al seguente indirizzo:

NucleoAntifrodeInternet@bnlmail.com.

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 "
- Trendmicro "Maximum Security"

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.