

CRYALA – programma di verifica presenza crypto-virus Ver 3.0.0 - 17 aprile 2016

Il programma testa l'eventuale presenza nel PC di un cryptovirus usando la tecnica delle 'esche'.

Questa tecnica permette di sapere solo se nel PC è presente il virus. Non evita l'infezione.

Quando il programma segnala la presenza del virus, i dati utente nel PC possono essere già stati criptati.

Questa tecnica serve solamente a prevenire di sporcare i backup con files cifrati dal virus.

Tutte le altre precauzioni per evitare che il virus possa inocularsi nel PC rimangono indispensabili.

IL BACKUP DEI DATI UTENTE RIMANE IL SISTEMA MIGLIORE PER NON PERDERLI COMPLETAMENTE A CAUSA DEL LAVORO DI UN VIRUS DI QUESTA FAMIGLIA.

Il programma si compone di due moduli, due eseguibili:

- 1) CRYA_Console.exe – la console di settaggio e controllo.
- 2) CRYA_Engine.exe – il modulo di verifica singola, ciclica e di lancio del Backup.

La tecnica

Dato che i cryptovirus attaccano i files dell'utente rendendoli inutilizzabili, la tecnica prevede di creare e distribuire nel PC una serie di files 'esca' che verranno controllati costantemente dal modulo di verifica.

Se un cryptovirus comincia a lavorare sui files utente è altamente probabile che modifichi anche le 'esche', soprattutto se queste sono state ben posizionate nelle aree utente e sono di tipo 'adatto' per essere considerate Dati Utente.

In quest'ottica è consigliabile creare le esche nelle cartelle delegate ad accogliere i dati utente per default, cioè:

- Documenti
- Immagini
- Video
- Desktop

In ciascuna di queste cartelle conviene posizionare un file coerente con l'area stessa, quindi nella cartella Documenti creare per es. un file PDF opp. DOC, nella cartella Video un file AVI o FLV, nella cartella Immagini un file JPG e sul Desktop un file ancora PDF o DOC o di qualsiasi altra estensione che richiami un dato utente.

Le estensioni sopra citate al momento sono di sicuro usate dai cryptovirus per considerare un file come ostaggio.

E' inutile usare files esca grossi. Bastano files di pochi KB, qualche centinaio al massimo, anche se il programma può utilizzare qualsiasi file di qualsiasi dimensione.

Una dimensione non eccessiva impegna per poco tempo la verifica ed è quindi consigliabile.

Quando avviene la verifica

Il modulo CRYA_Engine.exe può lavorare in tre modi diversi:

- 1) Verifica le esche quando viene lanciato il programma e se le esche sono a posto, si chiude automaticamente, mentre se ci sono degli Allerta o degli Allarmi, viene presentata la finestra con le informazioni del caso.
- 2) Quando viene lanciato il programma, questo rimane attivo e residente in memoria e verifica le esche con un intervallo di tempo prefissato, configurato dall'operatore. Alla verifica delle esche il comportamento è lo stesso del modo 1)

- 3) Il programma quando viene lanciato verifica le esche. Se queste sono a posto viene lanciato il programma di Backup configurato dall'utente e CryAla_Engine si chiude da solo. Se ci sono degli Allerta o degli Allarmi, viene presentata la finestra con le informazioni del caso e NON VIENE LANCIATO IL PROGRAMMA DI BACKUP.

L'utente può scegliere la modalità operativa che ritiene più idonea al proprio caso.

Come preparare il PC

Per prima cosa preparare e posizionare i files esca.

Utilizzare files esistenti sul PC oppure crearli appositamente.

Se si utilizzano files esistenti, verificare che questi non siano già stati cifrati, aprendoli con l'applicazione opportuna e verificando che siano leggibili o visibili.

Il numero di files esca non è obbligato da nulla. Uno o due files per tipo sono sufficienti alla bisogna. Partiamo dal presupposto che il virus attacchi tutti i files utente che trova nelle aree specifiche, esche comprese.

Una volta distribuiti i files esca, creare una cartella dove si desidera (es: C:\CRYA\) e copiare all'interno i due files del programma: CRYA_Console.exe e CRYA_Engine.exe.

Il programma utilizza anche altri due file che crea da solo appena lanciato il modulo di configurazione:

CRYA_LOG.LOG : file di log degli eventi

CRYA_CFG.CFG : file di configurazione del programma.

In base alla modalità scelta, è possibile aggiungere all'Esecuzione Automatica di Windows il lancio del modulo di verifica, creando il link nella cartella :

C:\Users\nomeutente\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

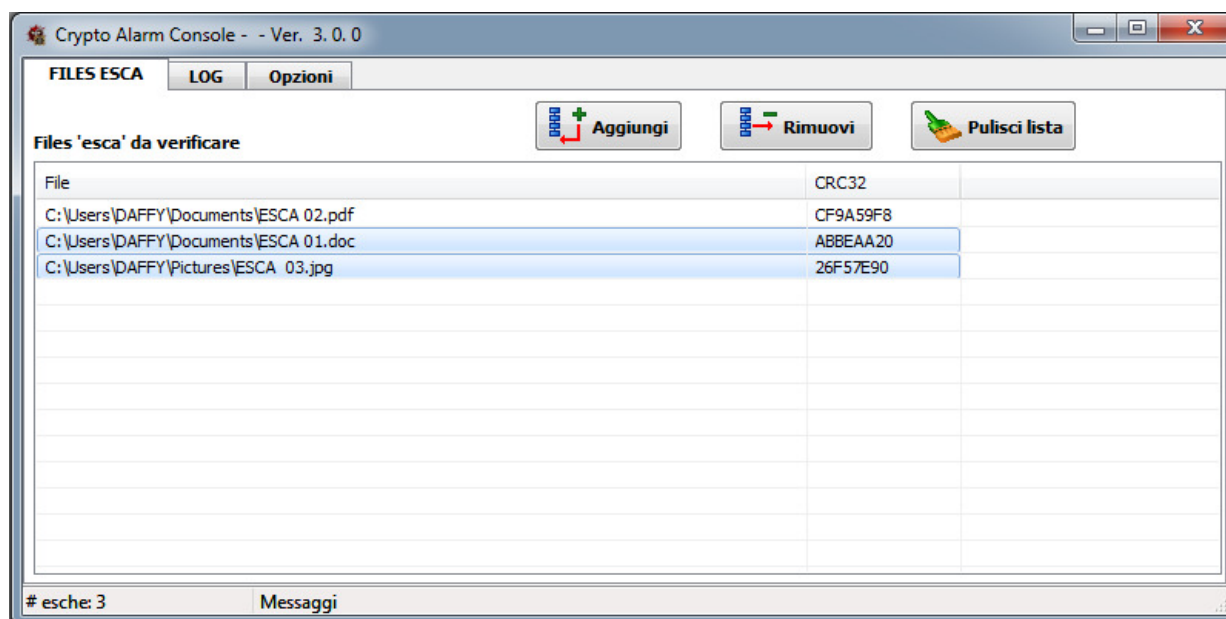
(usare la voce Apri del menu contestuale sulla voce Esecuzione Automatica del menu di Start).

Questo permette di avviare automaticamente il controllo ad ogni avvio del PC.

(Per la modalità di avvio automatico del Backup, vedere anche il parametro su linea di comando : NOBKU).

Per prima cosa occorre configurare il programma con il modulo CRYA_Console.exe, per informarlo su quali sono i files di esca.

Il modulo CRYA_Console.exe



Questo modulo permette di configurare le esche, vedere il LOG delle attività e settare le opzioni.

Nella pagina **FILES ESCA** con i tasti **AGGIUGI**, **RIMUOVI** e **Pulisci Lista** possiamo informare il programma su quali sono le esche da verificare.

Il tasto **AGGIUNGI** apre una finestra di navigazione del PC con cui possiamo indicare i files esca da usare.

Il tasto **RIMUOVI** permette di rimuovere dalla lista i files selezionati.

Il tasto **Pulisci Lista** permette di rimuovere tutti i files esca dalla lista.

Si possono aggiungere e rimuovere più file contemporaneamente con il solito metodo di Windows attraverso i tasti Control e Shift per la selezione multipla.

Ogni variazione alla lista viene automaticamente salvata dal programma nel file CRYA_CFG.CFG, creato al primo lancio di questo modulo.

Appena viene scelto un file esca, il programma calcola il CRC32 (Cyclical Redundancy Check a 32 bit), cioè la firma univoca di quel file.

Il CRC32 è un numero che identifica in modo assoluto un file. Modificando anche un solo bit del file, il CRC32 cambia.

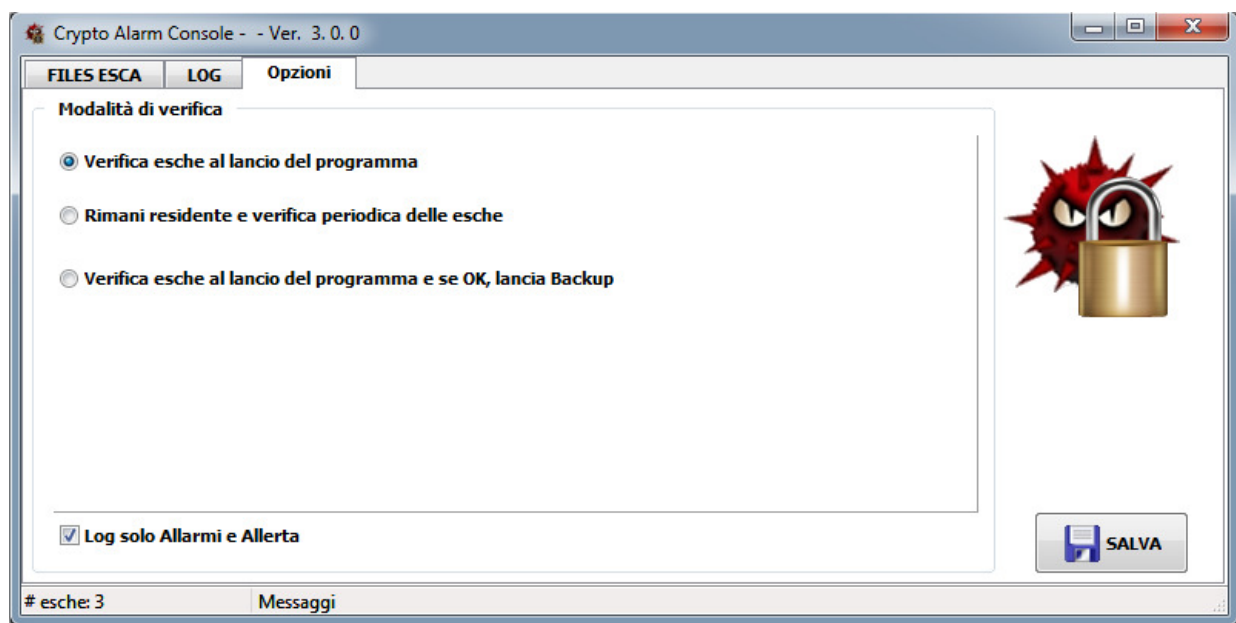
L'uso del CRC32 permette quindi di capire istantaneamente se quel file è stato modificato, nel nostro caso da un cryptovirus.

Il valore del CRC32 calcolato sul file scelto come esca viene rappresentato nella relativa colonna e costituirà la base di comparazione per stabilire se quel file è stato modificato o meno.

La pagina **Opzioni** permette di configurare le varie opzioni.

Modalità di verifica

La modalità di verifica è una di tre, univoca.



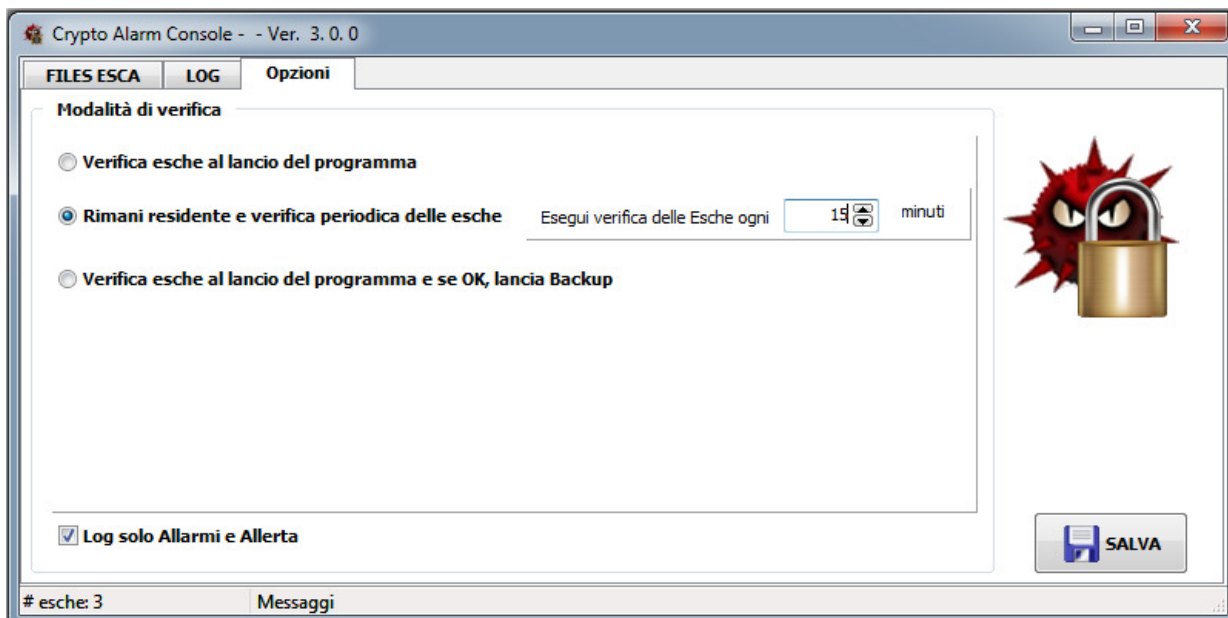
Verifica Esche al lancio del programma

In questa modalità il programma CRYAla_Engine verifica le esche appena viene lanciato.

Se le esche sono a posto, il programma si chiude senza segnalare nulla all'utente.

Se configurato dalla relativa spunta, viene compilato il LOG.

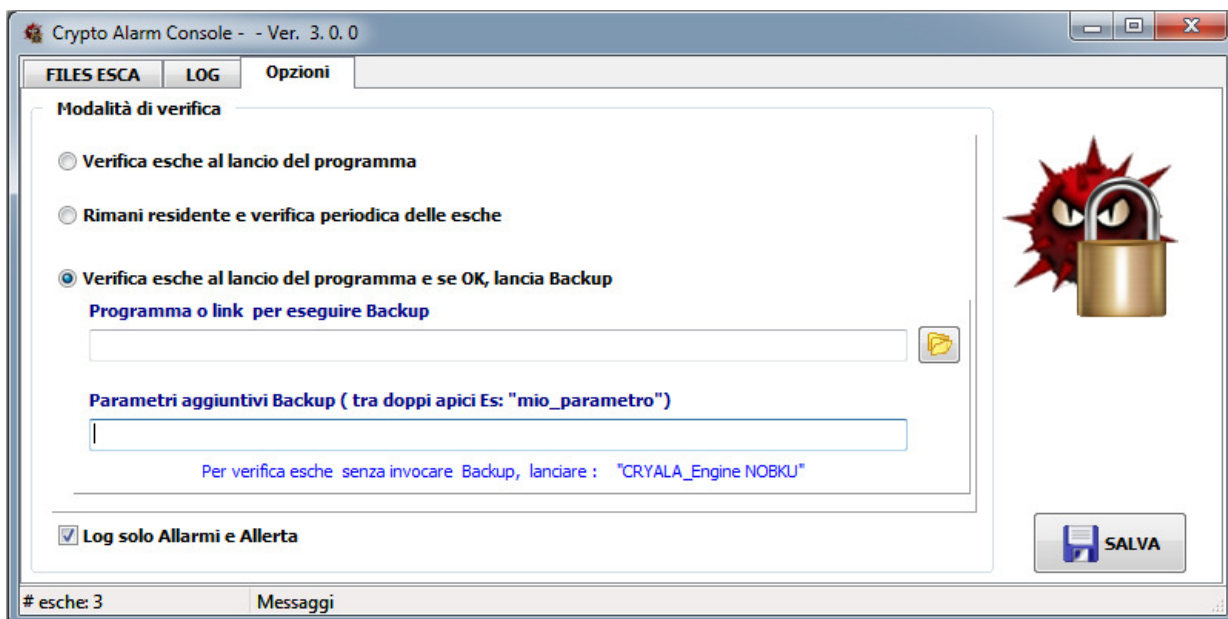
Se le esche sono state modificate o ci sono delle Allerta sul file di configurazione, il programma apre la propria finestra e mostra lo stato delle cose. In questo caso viene comunque compilato il LOG degli eventi.



Rimani residente e verifica periodica delle esche

In questa modalità il modulo di verifica, quando lanciato la prima volta (magari all'avvio del PC), rimane residente in memoria e verifica periodicamente le esche con un intervallo di tempo configurato con l'apposita voce.

Al momento della verifica il programma usa lo stesso comportamento della modalità precedente.



Verifica esche al lancio del programma e se OK, lancia Backup

In questa modalità il modulo di verifica si comporta come nella prima modalità, ma se le esche sono a posto, lancia il programma per eseguire il Backup, configurato dall'utente nell'apposito campo. Con il tasto previsto si apre una finestra di navigazione che permette di indicare il programma usato dall'utente per eseguire il Backup.

E' anche possibile fornire una serie di parametri da passare al programma di backup nel caso questo li richiedesse. (per es. il nome di un profilo di backup o altro).

Nota:

Se si configura questa modalità, è possibile anche chiamare il programma CryAla_Engine con un parametro : **NOBKU** (tutto maiuscolo) per fare in modo che anche se configurato, verifichi le esche ma non lanci il programma di Backup.

Questo è utile se si configura il programma anche al boot di Windows solo per verificare lo stato del sistema, senza però innescare anche il backup.

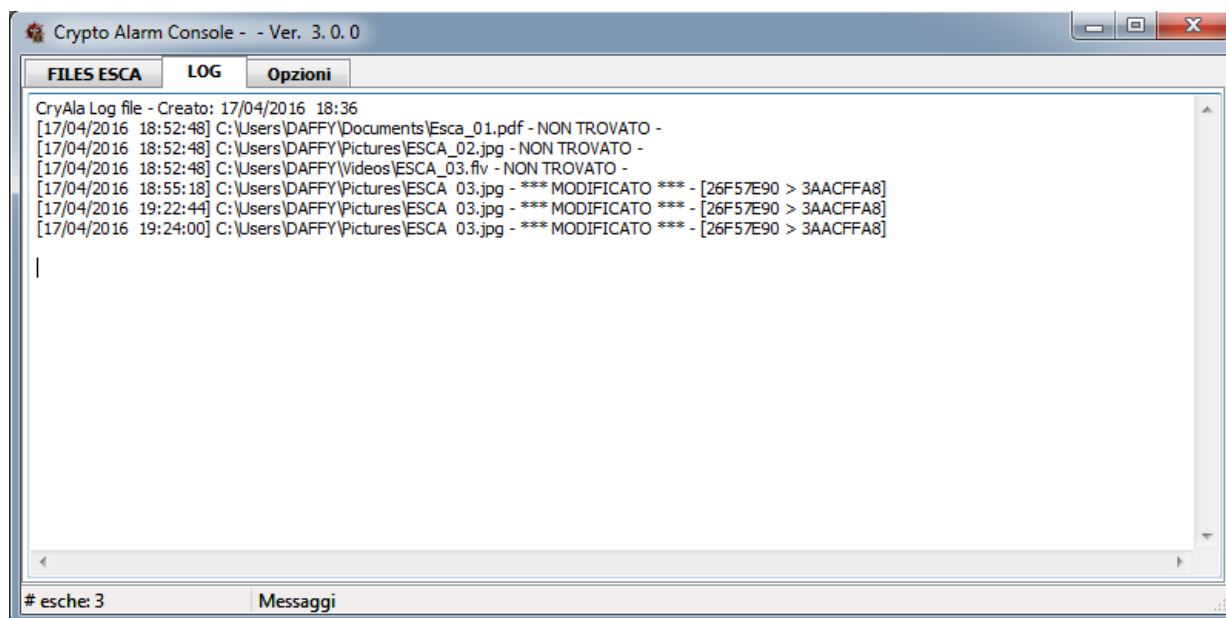
Per lanciare il modulo di verifica con questo parametro, basta creare un link il cui argomento sia: "...Percorso...\CryAla_Engine.exe" "NOBKU" (con le doppie virgolette incluse).

Log solo Allarmi e Allerta

Questa spunta permette di scegliere se il modulo di verifica deve registrare nel LOG degli eventi solo eventi di Allarme e Allerta oppure tutti gli eventi, anche quelli di controllo con risultati positivi.

Il tasto SALVA permette di salvare lo stato delle opzioni nel file di configurazione.

L'utente deve salvare con questo tasto per rendere permanenti le modifiche alle opzioni.

La pagina LOG

Questa pagina permette di visionare il file di LOG degli eventi, aggiornato ad ogni lancio del modulo di verifica.

Nota: I messaggi di Allerta e Allarme vengono anche presentati in tempo reale dal modulo di verifica (vedere più avanti).

Il file di LOG

Questo file, benché abbia estensione .LOG (i files .LOG non sembrano essere attaccati dai cryptovirus), è un file di tipo TXT che può essere visto e gestito da qualsiasi editor di testo.

Per azzerare il file di LOG è sufficiente cancellarlo. Sia il modulo Console che quello di verifica creano un nuovo file di LOG se non ne trovano uno esistente.

I messaggi previsti nel LOG per segnalare eventi sono i seguenti:

... Nessuna segnalazione ...

Aggiunto al LOG solo se la spunta *Log solo Allarmi e Allerta* non è presente.

Segnala un ciclo di verifica delle esche senza nessun allarme o allerta.

Messaggi di Allerta:

Nessun File Esca configurato

Non è stato configurato nessun file di esca. Provvedere.

File configurazione non compatibile

e

File configurazione non trovato

Il file di configurazione CRYA_CFG.CFG non è stato trovato o non è stato riconosciuto come compatibile.

Entrambe le condizioni sono sospette. Dato che il file di configurazione viene creato automaticamente dal modulo CRYA_Console, il fatto di non trovarlo o trovarlo non compatibile potrebbe significare che un cryptovirus ha cifrato anche il file di configurazione.

Al momento nessuna famiglia di cryptovirus sembra aggredire files di tipo .CFG e .LOG, ma non si sa mai cosa succederà domani.

Messaggi di Allarme:

NomefileEsca -*** MODIFICATO *** - [CRC32 originale > CRC32 corrente]

Questo messaggio indica che il modulo di verifica ha trovato il CRC32 corrente di un file esca diverso dal CRC32 presente nel file di configurazione.

Il file è stato modificato.

NomefileEsca - NON TROVATO -

Questo messaggio indica che il file esca non è stato trovato. Se nessuno ha cancellato il file involontariamente, può significare che è stato rinominato da un cryptovirus.

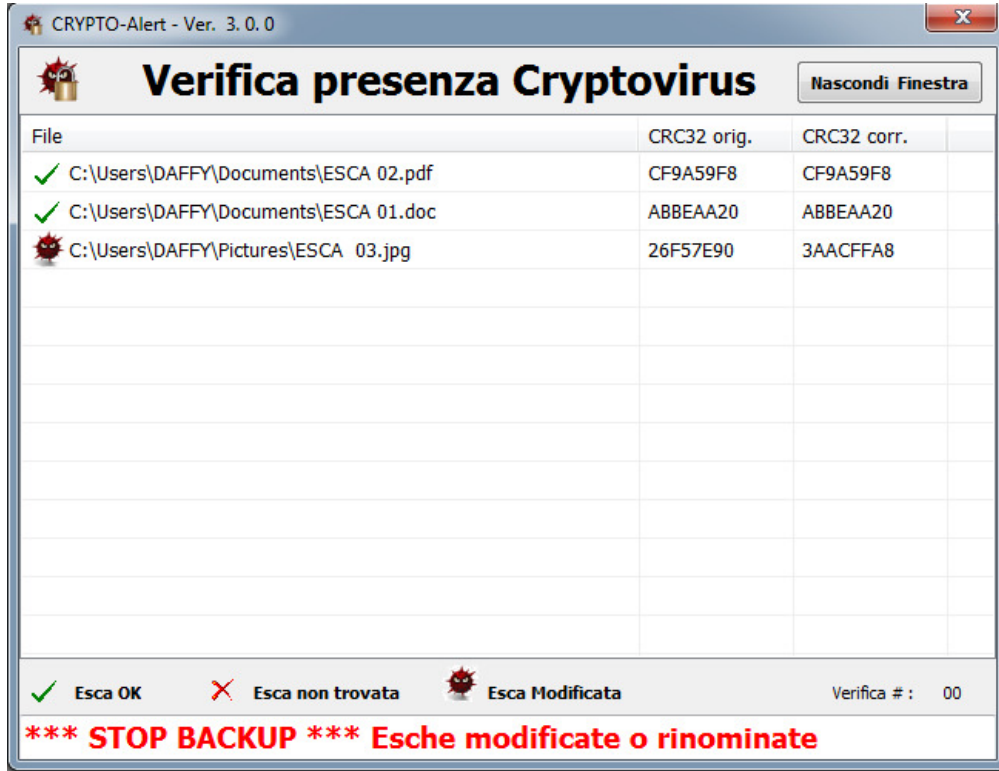
Al momento 3 famiglie su 4 di questi virus rinominano o cambiano estensione ai files utente che hanno cifrato.

Il modulo CRYA_Engine.exe

Il modulo di verifica, se non trova ne Allarmi, ne Allerta, non si mostra all'utente in nessuna delle modalità operative.

Esegue il proprio lavoro in modo nascosto e aggiorna il file di LOG in modo coerente alla spunta relativa presente nel modulo Console.

Se invece la verifica trova Allerta o Allarmi, il modulo mostra all'utente la finestra qui sotto, estesa per tutta l'altezza del Desktop e centrata nello stesso.



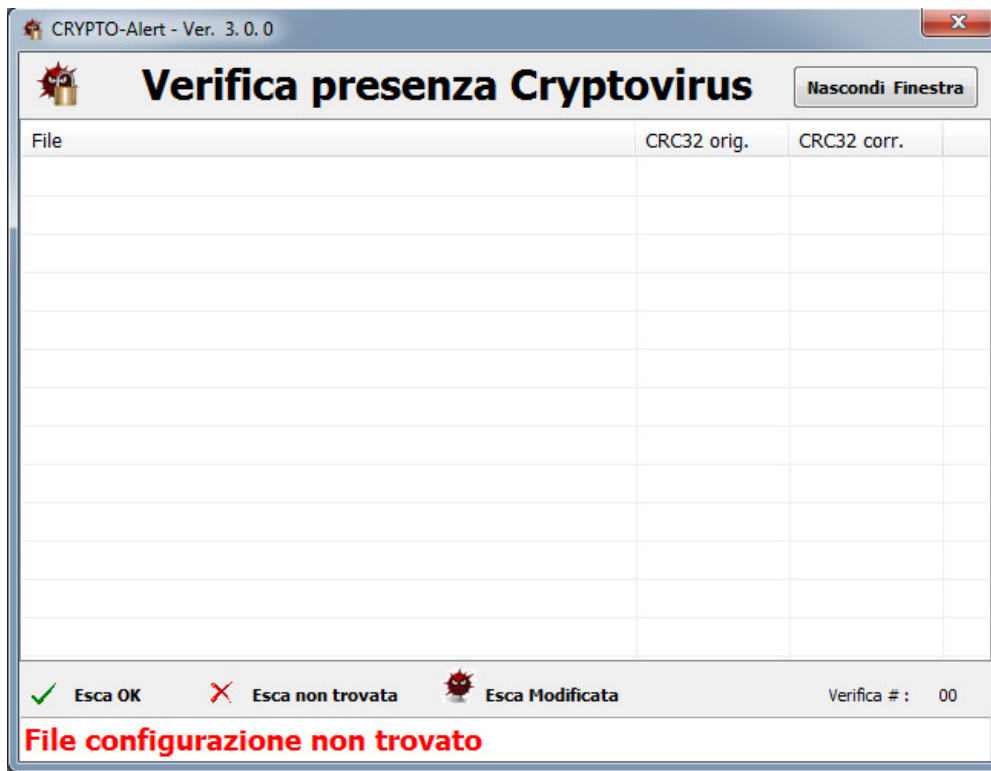
In questa finestra vengono rappresentate le condizioni trovate di allarme o allerta.

La figura qui sopra mostra la segnalazione di allarme nel caso in cui venga trovato un file esc modificato.

Se è stata configurata la modalità Verifica esche al lancio del programma e se OK, lancia Backup il modulo NON lancia il programma di Backup quando trova Allarmi o Allerte.

Il campo **Verifica #:** **xx** in basso a destra, indica il numero dell'ultima verifica eseguita in caso di modalità operativa con verifica ciclica.

In caso di Allerta la finestra ha il seg. formato:



I messaggi di Allerta sono rappresentati sulla riga di stato in colore rosso.

Se qualcuno trova migliorie o problemi, per favore segnalatele. Grazie.

Non posso non ringraziare pubblicamente **Franco Gastaldi di Imperia** che ha contribuito alla ideazione e verifica sul campo di questo programma. Ha contribuito e continua a farlo. Grazie per la collaborazione.

Ing. Alberto Sozzi sozzia@sozzi-a.com