

Configura Dr.Web contro i cryptolocker!

Raccomandazioni per ridurre al minimo il rischio di un'infezione dal trojan del riscatto



I cryptolocker (la famiglia Trojan.Encoder) – programmi malevoli che cercano su dischi del computer infetto o nella memoria del dispositivo mobile i file dell'utente, dopodiché li criptano e chiedono alla vittima il riscatto per la decriptazione dei file.

Tutti i cryptolocker appartengono ai file dannosi (trojan) che **non sono in grado di diffondersi e avviarsi in maniera autonoma**. Secondo le statistiche Doctor Web

In oltre il 90% dei casi	Soltanto nel 10% dei casi
gli utenti avviano i cryptolocker sul loro computer con le proprie mani	la decriptazione è possibile

Bisogna saperlo

Le comunità criminali che si occupano dello sviluppo dei programmi malevoli li testano **contro il rilevamento** da tutte le soluzioni antivirus correnti. Pertanto, vengono rilasciati nella "natura selvatica" soltanto quei programmi malevoli che garantitamente non vengono rilevati dagli antivirus (fino a quando questi ultimi non riceveranno gli aggiornamenti).

Un cryptolocker potrebbe penetrare persino in un computer protetto da un (qualsiasi) antivirus – se il trojan non è ancora conosciuto dal database dei virus o se l'antivirus non include le tecnologie di protezione preventiva. Nessun antivirus riconosce tutti i programmi malevoli in un momento.

E questo significa che nessuno è al sicuro dall'infezione da un cryptolocker nuovo sconosciuto — se non è stato configurato il sistema di protezione

Configura Dr.Web

Le regole di configurazione Dr.Web di base aiutano a prevenire l'infezione da un cryptolocker – persino da uno non conosciuto dal motore antivirus.

Dr.Web dovrebbe essere sempre attivato

Se il computer è connesso alla rete Internet o se ad esso è collegato un supporto di memoria esterno non precedentemente sottoposto a una verifica antivirus – in questo momento non si può assolutamente disattivare Dr.Web.

Questa è l'icona di agent Dr.Web nella tray di sistema che segnala che Dr.Web è attivato e protegge il PC.



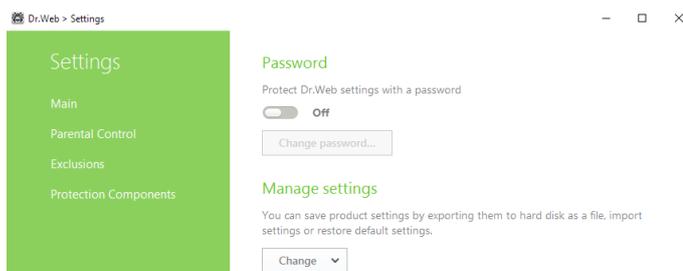
Se l'icona di agent è assente o porta il punto esclamativo o una croce, significa che Dr.Web è disattivato e il computer è rimasto senza la protezione antivirus. In questo caso riavviare immediatamente il computer. Se il problema persiste – [contattare immediatamente il servizio di supporto tecnico Doctor Web](#).

E il Suo Dr.Web è adesso attivato?

La password di Dr.Web dovrebbe essere impostata

L'impostazione di una password garantisce l'impossibilità di disattivare l'auto-protezione Dr.Web — compreso il caso di violazione.

Per impostare una password di accesso a Dr.Web



Fare clic sull'icona  (l'icona cambia aspetto a ) e facendo clic sull'icona comparsa  selezionare nel menu **Impostazioni** la voce **Principali**. Premere l'interruttore e quindi il pulsante **Modifica la password**.

Attenzione! Non è consigliabile impostare una password che corrisponda alla password di accesso al computer o dispositivo. La password Dr.Web non dovrebbe essere memorizzata sullo stesso computer.

E al Suo Dr.Web è impostata la password?

Tutti i componenti di protezione Dr.Web dovrebbero essere sempre attivati

Ciascun componente di Dr.Web Security Space partecipa a proteggere dai trojan-ransomware.

La disattivazione — se solo di uno dei componenti e anche temporaneamente — significa un inevitabile abbassamento di protezione.

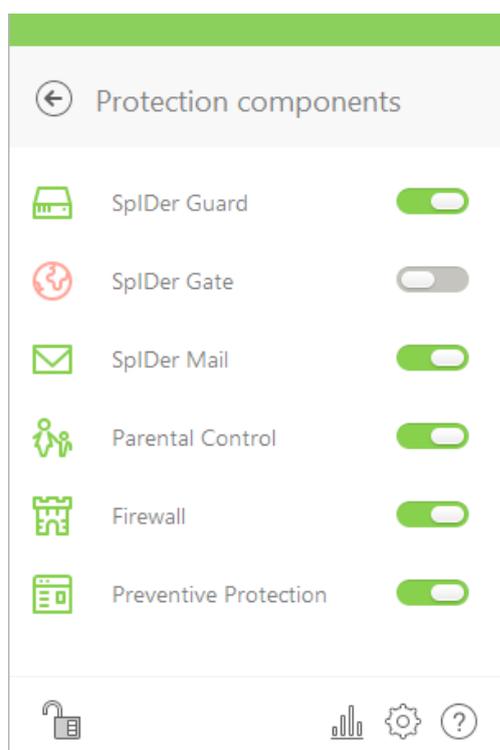
- **Dr.Web SpIDer Guard** rileverà programmi malevoli al momento quando si avviano — persino se i componenti malevoli sono stati ricevuti criptati e non sono stati rilevati al momento del caricamento
- Un cryptolocker potrebbe infiltrarsi nel computer anche attraverso un messaggio di posta elettronica. Di regola, tale email contiene un allegato malevolo o un link appositamente creato. **Antispam** Dr.Web filtra email con contenuti malevoli sulla base delle caratteristiche specifiche delle email dei malintenzionati — anche se il motore antivirus non ha ancora ricevuto un aggiornamento che contiene informazioni sulla minaccia più recente.
Antispam Dr.Web non ha bisogno di essere istruito — lui stesso sa come agire!

- **Dr.Web SpIDer Gate** e **Parental control** non lasceranno che l'utente vada a un sito pericoloso se un link di download di un trojan verrà ricevuto in un'email. Il servizio di scansione del traffico email e web, che fa parte di Dr.Web Security Space, è costruito su algoritmi unici che assicurano l'altissima velocità di verifica e l'ottima qualità del rilevamento dei programmi malevoli.
- Firewall Dr.Web consente di configurare limitazioni per programmi che hanno l'accesso a Internet.

E questi sono lungi dall'essere tutti i componenti Dr.Web che rilevano virus e trojan!

Per scoprire se nel Suo Dr.Web ci sono componenti disattivati

Attenti alla tray di sistema – se in Dr.Web ci sono componenti disattivati, l'icona Dr.Web si presenterà così: 



Per vedere quali componenti sono disattivati

Fare clic sull'icona di agent Dr.Web e quindi sulla voce **Componenti di protezione** – si aprirà il relativo menu di agent Dr.Web.

E nel Suo Dr.Web tutti i componenti sono attivati?

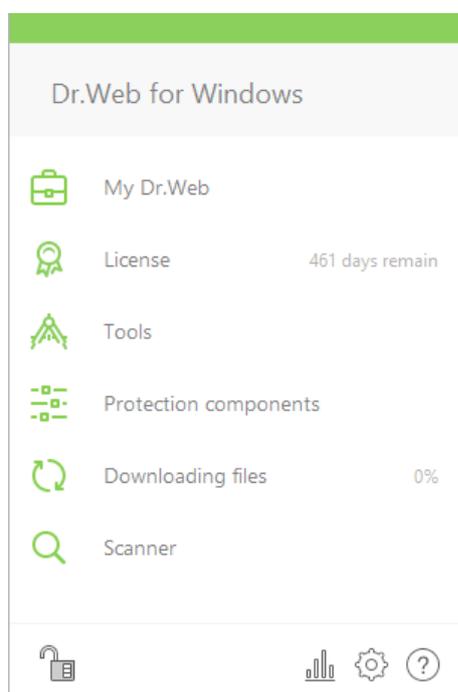
Bisogna aggiornare spesso l'antivirus

Bisogna aggiornare l'antivirus subito dopo la ricezione degli aggiornamenti.

A tale scopo basta lasciare invariate le impostazioni di aggiornamento impostate dallo sviluppatore di Dr.Web – e l'antivirus verrà aggiornato in autonomo e in tempo.

Ma è anche molto importante RIAVVIARE IL PC dopo un aggiornamento che richiede un riavvio – a prescindere da quanto spesso Dr.Web chiede di farlo. Perché solo dopo il riavvio vengono installati nuovi driver di intercettazione di programmi malevoli precedentemente sconosciuti e inoltre correzioni per le potenziali vulnerabilità di sicurezza Dr.Web.

Attenzione! Solo in un giorno il laboratorio antivirus Doctor Web riceve fino a un milione di nuovi file potenzialmente malevoli. Se Dr.Web non viene aggiornato persino durante alcune ore – questa è la possibilità di saltare centinaia di file malevoli precedentemente sconosciuti (anche dall'analisi euristica Dr.Web). Nel frattempo, a solo un trojan-banker bastano da 1 a 3 minuti per rubare denaro da un conto dell'utente.



Per verificare la data e lo stato aggiornato degli aggiornamenti

Fare clic sull'icona  nella tray di sistema. Lo stato di aggiornamento sarà mostrato nella finestra che si è aperta.

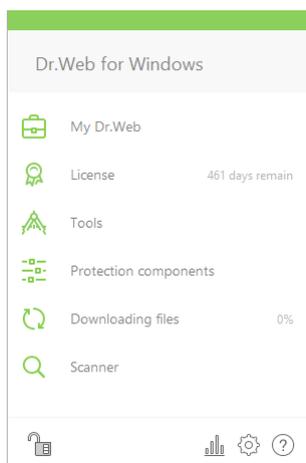
E quando è stato l'ultimo aggiornamento nel Suo Dr.Web?

Si possono utilizzare eccezioni dalla scansione soltanto in casi rari

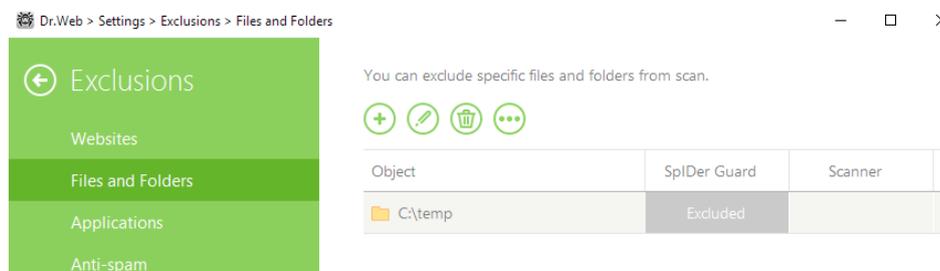
Le eccezioni dalla scansione possono accelerare la scansione, ma il più spesso a scapito del livello di sicurezza. Autori dei virus sanno CHE utenti tendono a impostare eccezioni e sfruttano questa circostanza ai loro scopi criminali.

I nostri programmi sono massimamente ottimizzati e risparmiano le risorse del computer. Non consigliamo di escludere qualche cosa dalla scansione Dr.Web in quanto non ogni utente ha le conoscenze sufficienti per valutare i rischi di tale impostazione. Le eccezioni sono un metodo per aggirare qualche situazione problematica. Come si fa a farlo correttamente, lo possono consigliare soltanto gli esperti di supporto tecnico Doctor Web.

Per verificare se in Dr.Web sono utilizzate delle eccezioni dalla scansione che abbassano il livello di protezione



Fare clic sull'icona  nella tray di sistema. Nel menu comparso fare clic sull'icona  (l'icona cambia aspetto a ) e cliccando sull'icona comparsa , selezionare **Impostazioni** → **Esclusioni**.



Attenzione! Se nelle eccezioni sono impostate le maschere di tipo *.exe o *.dll, la scansione Dr.Web salterà tutti gli oggetti che corrispondono a tale maschera – cioè tutti i file eseguibili e tutte le librerie software!

Attenzione! Non è consigliato escludere dalla verifica il traffico dei programmi in uso – in seguito a tale impostazione non verrà controllato nessun software malevolo caricato da tali programmi.

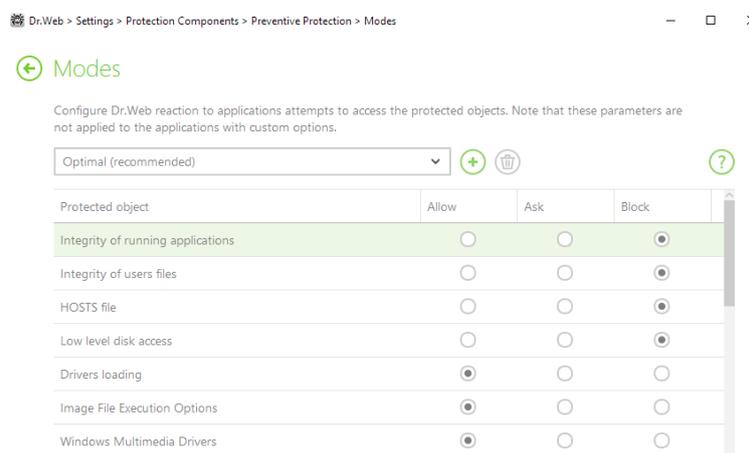
E nel Suo Dr.Web è impostata qualche eccezione dalla scansione?

La Protezione preventiva dovrebbe essere attivata

Oggi la Protezione preventiva è uno dei componenti più importanti nel sistema di protezione completa Dr.Web.

In base alla somiglianza del comportamento di un software sospetto (non ancora conosciuto da Dr.Web) ai noti modelli di comportamento dei programmi malevoli già conosciuti, la Protezione preventiva Dr.Web è in grado di riconoscere e bloccare tali software grazie a un'intera serie di diverse [tecnologie](#) che agiscono sull'anticipo e non sono dipendenti dalla presenza delle relative firme antivirali nel database Dr.Web.

Si raccomanda di non disattivare la Protezione preventiva – il suo funzionamento ostacola notevolmente la possibilità di furto dei dati e soldi dell'utente da parte dei cryptolocker, winlocker, trojan-banker e di altri programmi malevoli pericolosi.



IMPORTANTE! Per una protezione aggiuntiva dai cryptolocker nelle impostazioni del componente Protezione preventiva dovrebbe sempre essere impostato "Proibisci" per le voci "Integrità delle applicazioni in esecuzione" e "Integrità dei file degli utenti".

E nel Suo Dr.Web è attivata questa impostazione?

Se il PC è connesso a Internet, la Protezione preventiva ottiene dal servizio online basato su cloud Dr.Web Cloud le conoscenze circa i più recenti algoritmi per contrastare le minacce sconosciute. Questo fornisce la protezione dai programmi malevoli che sono giunti agli analisti Doctor Web già dopo che l'antivirus sul computer aveva ricevuto l'ultimo aggiornamento.

Di regola, gli aggiornamenti tradizionali giungono sul computer non più spesso di una volta l'ora. Le informazioni in Dr.Web Cloud invece sono sempre le più recenti in quanto vengono aggiornate non appena sono state ricavate dagli analisti Doctor Web. L'utilizzo del database cloud aumenta significativamente la protezione dalle minacce che sfruttano le vulnerabilità "zero day".

E nel Suo Dr.Web è attivato Cloud Dr.Web?

Di default, nella Protezione preventiva Dr.Web è impostato il livello di protezione **Ottimale**. Le impostazioni della Protezione preventiva Dr.Web sono descritte dettagliatamente [qui](#).

La Protezione preventiva ha un sistema di profili attraverso cui è possibile creare regole flessibili per applicazioni attendibili e così prevenire conflitti durante il funzionamento della Protezione preventiva Dr.Web. Le impostazioni dei profili della Protezione preventiva Dr.Web sono descritte dettagliatamente nella [documentazione](#).

E nel Suo Dr.Web è attivata la Protezione preventiva?

La Prevenzione della perdita di dati dovrebbe essere attivata e configurata

La "Prevenzione della perdita di dati" salva i file dell'utente più importanti in uno specifico storage protetto Dr.Web.

A differenza dei soliti programmi di backup, Dr.Web crea e protegge lo storage con le copie dei file contro l'accesso non autorizzato dei malintenzionati. Anche se un trojan più recente (non ancora conosciuto da Dr.Web) si infiltrerà nel PC, l'utilizzo della "Prevenzione della perdita di dati" preserverà i file dell'utente. E persino se il trojan cripterà i file, l'utente potrà ripristinarli in autonomo senza contattare il servizio di supporto tecnico Doctor Web.

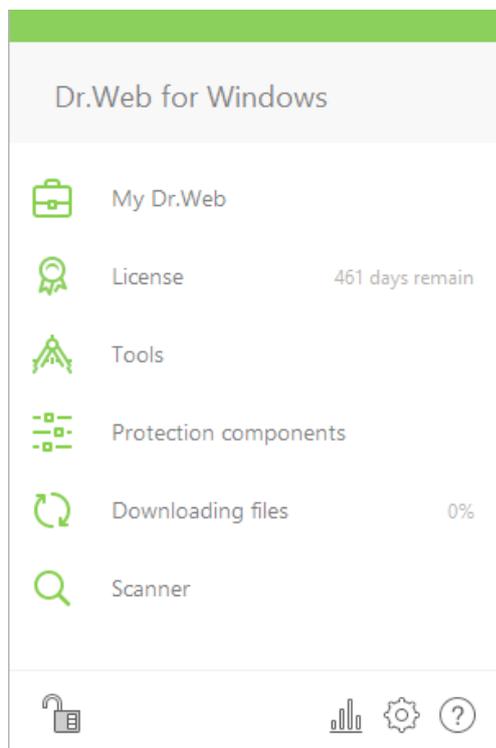
Di default questo componente non è attivato in quanto per il suo funzionamento occorre indicare i dati che vanno memorizzati e configurare percorsi e il metodo di conservazione dei dati.

E nel Suo Dr.Web è attivata e configurata la "Prevenzione della perdita di dati"?

La licenza Dr.Web dovrebbe essere attuale

Affinché Dr.Web protegga il PC, la licenza deve essere attiva (valida).

Dopo la scadenza di una licenza tutti i componenti Dr.Web cessano di funzionare.



Per scoprire fino a quando è valida una licenza Dr.Web

Fare clic sull'icona  nella tray di sistema. Se la licenza è valida, nel menu aperto è mostrato il numero di giorni mancanti alla scadenza della licenza.

Inoltre, è possibile scoprire la scadenza di una licenza Dr.Web nella [Gestione licenze sul sito](#).

E nel Suo Dr.Web c'è adesso una licenza valida?

Regole di comportamento in caso di infezione da un cryptolocker

Affinché per gli specialisti Doctor Web sia possibile ripristinare file criptati, l'utente DEVE EVITARE DI:

- modificare l'estensione dei file cifrati;
- reinstallare il sistema operativo;
- utilizzare qualche programma per la decifrazione/rispristino dei dati;
- eliminare/rinominare qualche file e programma (compresi file temporanei);
- eseguire azioni definitive di cura/eliminazione di oggetti.

Come risultato di queste azioni i dati si potrebbero perdere completamente – neppure l'apposita utility di decifrazione potrà ritrovarli e ripristinarli.

Pertanto, è meglio evitare tutte le azioni con il computer infetto prima di ricevere una risposta da Doctor Web circa la possibilità di ripristinare i file.

[Regole di comportamento in condizioni di un'infezione dal trojan-ransomware](#)

[Informazioni giuridiche](#)

Il ripristino gratuito di file criptati da un trojan-ransomware

è disponibile ai proprietari delle licenze commerciali valide [Dr.Web Security Space](#), [Dr.Web Enterprise Security Suite \(Protezione completa\)](#) e agli abbonati al servizio "Antivirus Dr.Web" (il piano tariffario [Dr.Web Premium](#)) – se queste [condizioni](#) sono soddisfatte al momento del verificarsi dell'incidente informatico.

Il servizio è a pagamento per gli utenti degli altri antivirus – a questo scopo è necessario acquistare una licenza per Dr.Web Rescue Pack.

Cosa è incluso nella licenza

- Utility di decriptazione
- Una licenza Dr.Web Security Space per 1 PC per 2 anni

Fai una richiesta di decriptazione

La conoscenza è un'arma potente contro i trojan-cryptolocker

Di come configurare correttamente il sistema di protezione dai trojan-ransomware racconta il corso di formazione **DWCERT-070-6 "Protezione di postazioni e file server Windows dalle attività dei programmi cryptolocker"** che può essere scaricato al link <https://training.drweb.com/users?lng=it>.

L'inganno è tutt'intorno? Ma c'è "The Anti-virus Times!"

Leggete di quello come affrontare i trojan-cryptolocker sulle pagine del progetto di informazione "The Anti-virus Times" nella rubrica "Encrypt everything".



[Tutte le edizioni della rubrica "Encrypt everything"](#)

Regole di igiene

I cryptolocker vengono massicciamente distribuiti per email – in messaggi che sarebbero quelli dalla polizia tributaria, dal tribunale o dai propri conoscenti, sotto forma di un curriculum vitae, documenti contabili ecc. Se si è ricevuta un'email sospetta con un allegato a cui Dr.Web non ha reagito, potrebbe esserci dentro un cryptolocker non ancora conosciuto dall'antivirus.

Inviare questo allegato per l'analisi nel laboratorio antivirus Doctor Web <https://vms.drweb.com/sendvirus?lng=en> e attendere la risposta di uno specialista.

Ciò aiuterà non solo l'utente stesso (ad impedire la crittografia dei dati), ma anche migliaia di potenziali vittime dei criminali informatici.

Potete aiutare a fermare i criminali informatici

La criptazione di dati è una pericolosa minaccia e i file corrotti sono un serio problema. Ma affrontare questo problema è possibile ed è necessario. Sugeriamo agli utenti vittime, come parte lesa, di rivolgersi alle forze dell'ordine denunciando l'accesso non autorizzato al computer, la distribuzione di programmi malevoli e l'estorsione. È possibile consultare inoltre la sezione delle informazioni giuridiche sul nostro sito: <http://legal.drweb.com/?lng=en>.

L'azienda Doctor Web

Doctor Web – produttore russo dei software Dr.Web di protezione antivirus delle informazioni. I prodotti Dr.Web vengono sviluppati fin dal 1992. L'azienda è un giocatore chiave nel mercato russo dei programmi studiati per soddisfare un'esigenza essenziale dell'impresa – quella della sicurezza delle informazioni.

Doctor Web è tra i pochi vendor antivirus del mondo a possedere le proprie tecnologie uniche di rilevamento e neutralizzazione di programmi malevoli. L'azienda ha il proprio laboratorio antivirus, un servizio di monitoraggio di virus globale e un servizio di supporto tecnico.

L'obiettivo strategico dell'azienda, su cui sono concentrati gli sforzi di tutti i dipendenti, è creare i migliori programmi di protezione antivirus che soddisfano tutti i requisiti moderni per questa classe di software e inoltre sviluppare nuove soluzioni tecnologiche che permettono agli utenti di essere preparati ad affrontare tutti i tipi di minacce informatiche.

Formazione

[Area dello studente a distanza Dr.Web](#) (è richiesta la registrazione)
[Corsi per ingegneri](#) | [Corsi per utenti](#) | [Brochure](#)

Informazione

["Mondo antivirus!"](#) | [Brochure](#)

Contatti

125040, Russia, Mosca, la 3° via Yamskogo polya, 2, 12A

[Numeri telefonici](#)

[Mappa per arrivare](#)

[Contatti per la stampa](#)

[Uffici al di fuori della Russia](#)

www.drweb.com | free.drweb.com | www.av-desk.com | curenet.drweb.com



© Doctor Web,
2003 – 2017



Unitevi a noi sui social network

