

# DWCERT-070-6

Protezione di postazioni e file server Windows dalle  
attività dei programmi cryptolocker



# Sommario

<b>1. In che cosa consiste la particolarità (il pericolo) dei programmi cryptolocker?</b>	<b>3</b>
<b>2. Come configurare il software antivirus per proteggersi dalle attività dei programmi cryptolocker</b>	<b>5</b>
2.1. Configurazione delle azioni che Dr.Web Security Space applica a file malevoli	6
2.2. Configurazione del sistema degli aggiornamenti di Dr.Web Security Space	8
2.3. Configurazione del componente Dr.Web Cloud	11
2.4. Configurazione dei parametri che permettono di rilevare file malevoli precedentemente sconosciuti	12
2.5. Le funzionalità "Prevenzione della perdita di dati"	16
2.6. Limitazione della possibilità di penetrazione dei programmi cryptolocker nel computer	18
<b>3. Raccomandazioni dell'azienda Doctor Web per la protezione del computer dai programmi cryptolocker</b>	<b>23</b>
3.1. Attivazione della visualizzazione delle estensioni di file	24
<b>4. Le azioni dell'utente se ha scoperto file criptati e/o una richiesta di riscatto</b>	<b>25</b>
4.1. Le utility di decifratura	25
4.2. Dove potrebbero esserci i file dei programmi cryptolocker	26

## Informazioni aggiuntive

<b>Progetti di informazione</b>	«Trojan cryptolocker – la minaccia No.1» «The Dancing Men, or the Encryption Trojan Invasion»
<b>"Mondo antivirus!"</b>	Categoria «Encrypt everything» e inoltre le altre edizioni con gli hashtag #Trojan.Encoder, #encryption_ransomware, #extortion e #decryption
<b>Opuscolo</b>	«Trojan cryptolocker – la minaccia No.1»
<b>Video</b>	Configurazione della "Prevenzione della perdita di dati"
<b>Libreria di virus</b>	Descrizioni dei trojan-cryptolocker della famiglia Trojan.Encoder

# 1. In che cosa consiste la particolarità (il pericolo) dei programmi cryptolocker?

Attualmente uno dei principali problemi che devono essere affrontati da amministratori di reti locali e singoli utenti sono le attività dei programmi cryptolocker – trojan della famiglia Trojan.Encoder.

**I cryptolocker (Trojan.Encoder)** sono programmi malevoli che cercano sui dischi del computer infetto o nella memoria del dispositivo mobile i file dell'utente, dopodiché li criptano e chiedono alla vittima un riscatto per la decifrazione dei file.

**Attenzione!** Se avete ricevuto una richiesta di pagare un riscatto, non prendete contatto con i malintenzionati. In oltre il 50% dei casi non si riceve il programma di decriptazione dopo il pagamento e si perde il denaro.

**Attenzione!** Anche se pagherete il riscatto al malintenzionato, questo non vi darà alcuna garanzia del recupero delle informazioni. C'è stato un caso quando i malintenzionati stessi non hanno potuto decriptare i file da loro criptati e hanno indirizzato le loro vittime dal servizio di supporto tecnico Doctor Web.

I primi programmi della famiglia Trojan.Encoder comparvero nel 2009. Nei successivi cinque anni il numero delle loro varietà principali aumentò di circa il 1.900%, e adesso i programmi Trojan.Encoder hanno diverse migliaia di versioni – ogni giorno il laboratorio antivirus Dr.Web riceve almeno una decina di nuovi campioni. Ci sono i trojan cryptolocker non solo per i PC (i sistemi operativi MS Windows e Linux) ma anche per i dispositivi mobili.

Di regola, i cryptolocker trovano sul computer e/o nella rete locale i file con determinate estensioni (per esempio \*.mp3, \*.doc, \*.docx, \*.pdf, \*.jpg, \*.rar, ma non solo con queste) e li criptano. Alcune versioni della famiglia encoder sono in grado di criptare anche altri file.

Non è facile ripristinare i file che un trojan è riuscito a criptare. Talvolta i file vengono decifrati tramite la selezione delle password-chiavi alla crittografia utilizzata, ma accade abbastanza spesso che i cryptolocker utilizzano i più forti metodi di crittografia. Alcuni cryptolocker possono essere decifrati dopo mesi di lavoro continuo ([Trojan.Encoder.567](#)), mentre altri ancora ([Trojan.Encoder.283](#)) non possono mai essere decifrati in un modo corretto.

*Per selezionare le chiavi manualmente per i file criptati dal Trojan.Encoder.741, ci vogliono 107902838054224993544152335601 anni.*

Il problema principale con la famiglia Trojan.Encoder è legato al sistema di sviluppo impiegato dai malintenzionati.

## **Nel corso dello sviluppo i programmi malevoli vengono testati contro il rilevamento da parte delle soluzioni antivirus attuali.**

Come risultato, fino a quando non verranno analizzati dai laboratori antivirus (con il successivo rilascio e la ricezione degli aggiornamenti), questi programmi malevoli non vengono rilevati dagli antivirus – neanche tramite i metodi euristici.

I prodotti Dr.Web eliminano con successo qualsiasi variante conosciuta dei trojan cryptolocker e anche permettono di neutralizzare le versioni non ancora analizzate dal laboratorio antivirus. Le tecnologie impiegate nei prodotti Dr.Web fanno sì che per i malintenzionati sia molto difficile creare i campioni radicalmente nuovi dei programmi malevoli che non possano essere rilevati tramite il nucleo antivirus Dr.Web.

Per ampliare le possibilità della protezione su un computer su cui è installato un antivirus basato su firme (diverso da Dr.Web), è possibile utilizzare Dr.Web Katana.

**Attenzione!** *In qualsiasi momento nessun programma antivirus può fornire la protezione contro la penetrazione dei programmi malevoli ancora sconosciuti senza impiegare mezzi di protezione addizionali (quali il sistema di limitazione degli accessi o il controllo dei processi in esecuzione).*

Le maggiori informazioni sui cryptolocker sono ritrovabili sull'indirizzo [https://antifraud.drweb.com/encryption\\_trojs/?lng=it](https://antifraud.drweb.com/encryption_trojs/?lng=it).

## 2. Come configurare il software antivirus per proteggersi dalle attività dei programmi cryptolocker

Un trojan cryptolocker non ancora conosciuto dal sistema antivirus può penetrare nella rete locale o in un singolo computer attraverso lo spam (di regola, il messaggio contiene un allegato o un apposito link), attraverso un messaggio istantaneo (che anche contiene un link), da un sito infetto o su una chiave usb infetta. L'infezione può avvenire in un modo impercettibile – i programmi malevoli odierni vengono creati in modo che l'utente non se ne accorga del loro funzionamento fino al momento “giusto” – fino a quando i file sul computer non verranno criptati e/o non apparirà il messaggio con una richiesta di riscatto.

**Attenzione!** *Se tra i vostri conoscenti e partner c'è qualcuno che non si cura della protezione dei dati personali, un'email con dentro un cryptolocker potrebbe arrivare da una persona o un'azienda che il destinatario conosce – per esempio, dalla polizia tributaria o da una banca. Più di quello, l'email potrebbe essere indirizzata proprio al destinatario!*

1. Se le varianti sconosciute dei Trojan.Encoder si infiltrano sul computer, di regola vengono riconosciute ed eliminate non prima che siano arrivati i prossimi aggiornamenti dell'antivirus. Pertanto è necessario aggiornare i database dei virus più spesso possibile – non meno di una volta ogni ora.
2. Se è disponibile una connessione Internet, attivate l'utilizzo del componente Dr.Web Cloud (fa parte dei prodotti **Dr.Web Security Space** (per Windows), **Dr.Web Desktop Security Suite** (per Windows, la licenza Protezione completa), nonché di **Dr.Web Katana**). Questo consente di trovare i file malevoli nuovi ancora più velocemente poiché le informazioni su di essi diventano disponibili nel sistema di protezione ancora prima della ricezione del relativo aggiornamento.
3. I criminali creano centinaia e migliaia di nuovi campioni dei programmi malevoli al giorno, e sarebbe ingenuo pensare che un antivirus che cerca virus sulla base delle conoscenze memorizzate nei database dei virus rilevi i malware nuovi al momento del loro arrivo. Il rilevamento dei campioni sconosciuti della famiglia Trojan.Encoder può essere assicurato da **un modulo di protezione preventiva** che tramite un'analisi comportamentale controlla i tentativi dei malintenzionati dell'esecuzione di un'azione da loro richiesta, confrontando “al volo” il comportamento dei programmi in esecuzione con quello dei trojan cryptolocker.

**Attenzione!** programmi malevoli sconosciuti potranno difficilmente penetrare sul computer se vengono configurati i parametri di funzionamento del Parental control e della Protezione preventiva. Limitando i permessi degli utenti (e quindi dei programmi che vengono eseguiti) per l'accesso a file e cartelle, impostando le limitazioni per programmi per l'accesso a varie risorse di rete, creiamo una configurazione che garantisce la salvaguardia dei nostri dati. Anche se un programma malevolo non è conosciuto dal nucleo antivirus e dalla protezione preventiva, in queste condizioni esso non potrà avviarsi o si avvierà ma verrà rilevato quando tenterà di utilizzare una risorsa di sistema controllata.

4. Purtroppo, persino l'impiego della protezione preventiva, attraverso cui Dr.Web può rilevare le varianti sconosciute dei cryptolocker, non può prevenire del tutto la criptazione dei file – su un computer protetto da Dr.Web nell'arco del tempo necessario per l'analisi di un processo sospetto un cryptolocker potrebbe riuscire a cifrare fino a una decina di file. Dunque per evitare la perdita dei file, è necessario configurare il componente "Prevenzione della perdita di dati" incluso in **Dr.Web Security Space** e in Dr.Web Desktop Security Suite (per Windows), la licenza Protezione completa.




Anche se per salvaguardare informazioni viene già utilizzato uno strumento di backup, è consigliabile utilizzare il componente "Prevenzione della perdita di dati" che permetterà di salvare più efficacemente i dati critici per l'utente. 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.

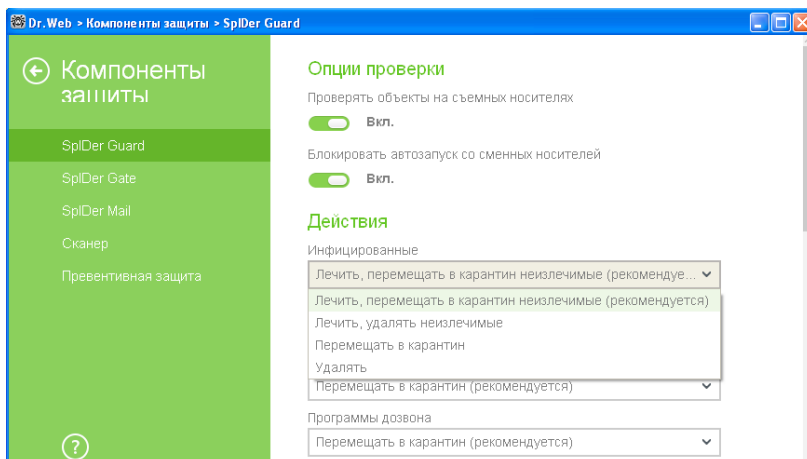
**Attenzione!** Visto che le soluzioni **Dr.Web Security Space** e **Dr.Web Desktop Security Suite** (per Windows), la licenza Protezione completa hanno le uguali possibilità di protezione dai cryptolocker, tutti gli esempi delle impostazioni verranno riportate in base a Dr.Web Security Space.

## 2.1. Configurazione delle azioni che Dr.Web Security Space applica a file malevoli

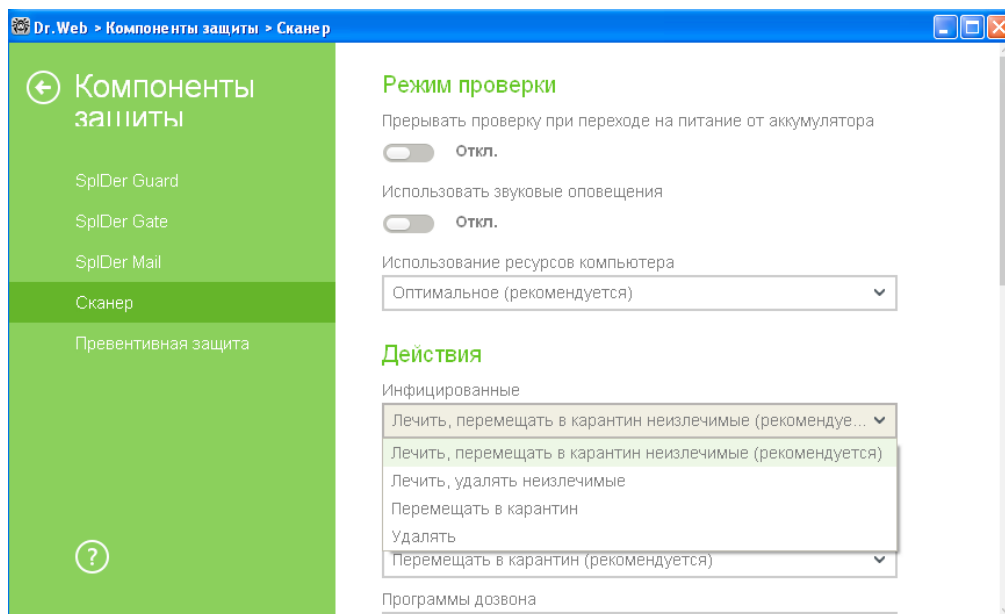
Per recuperare informazioni dai file criptati è preferibile avere il file malevolo stesso che ha eseguito la criptazione. Va notato inoltre che i file malevoli della famiglia Trojan. Encoder appartengono agli oggetti incurabili. Pertanto ad essi è necessario applicare l'azione **sposta in quarantena**.

**Attenzione!** L'avvio dello scanner antivirus può provocare modifiche nei dati e nei loro attributi disponibili sul computer. Questo a sua volta può comportare l'impossibilità di analizzare ulteriormente l'incidente informatico o di fornire i dati come prova nell'inchiesta. È consigliabile eseguire tutte le azioni per il ripristino dei dati su un'immagine del disco rigido, ottenuta conformemente alle norme procedurali.

Fate clic sull'icona  nel menu di sistema, quindi nel menu che si è aperto fate clic prima su  (Modalità amministratore) e quindi sull'icona apparsa  (Impostazioni). Nella finestra **Impostazioni** che si è aperta selezionate la voce **Componenti di protezione** e quindi **SplDer Guard**.






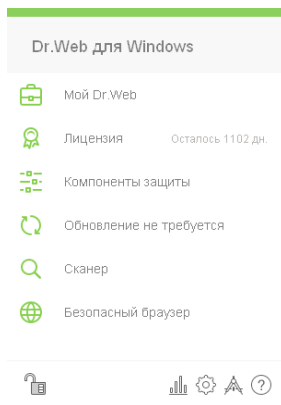
Le impostazioni simili è necessario utilizzare in una scansione antivirus. Le impostazioni vengono configurate nella stessa finestra delle impostazioni di SplDer Guard, ma nella sezione **Scanner**.



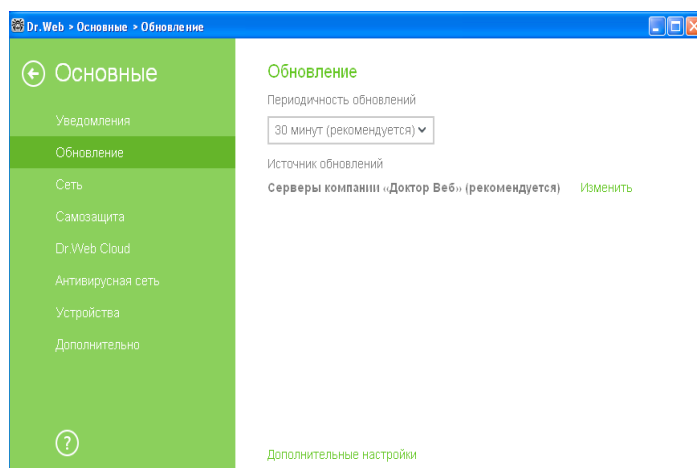
**Attenzione!** Non eliminate oggetti da quarantena perché in alcuni casi i file malevoli potrebbero contenere le chiavi che possono aiutare la decifrazione.

## 2.2. Configurazione del sistema degli aggiornamenti di Dr.Web Security Space

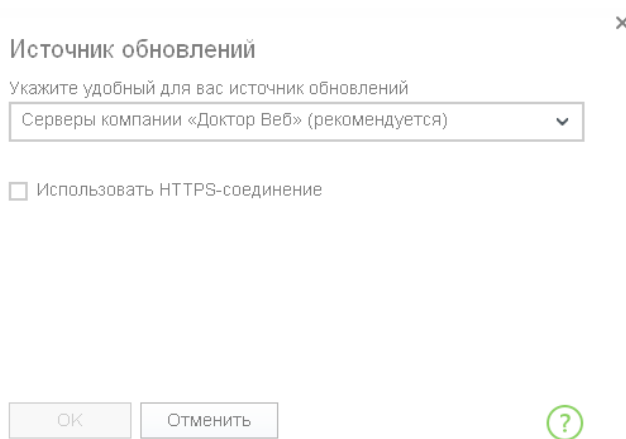
Per configurare parametri degli aggiornamenti, fate clic sull'icona  nel menu di sistema, quindi nel menu che si è aperto fate clic prima su  e quindi sull'icona apparsa .



Nella finestra **Impostazioni** che si è aperta selezionate **Principali** → **Aggiornamento**.

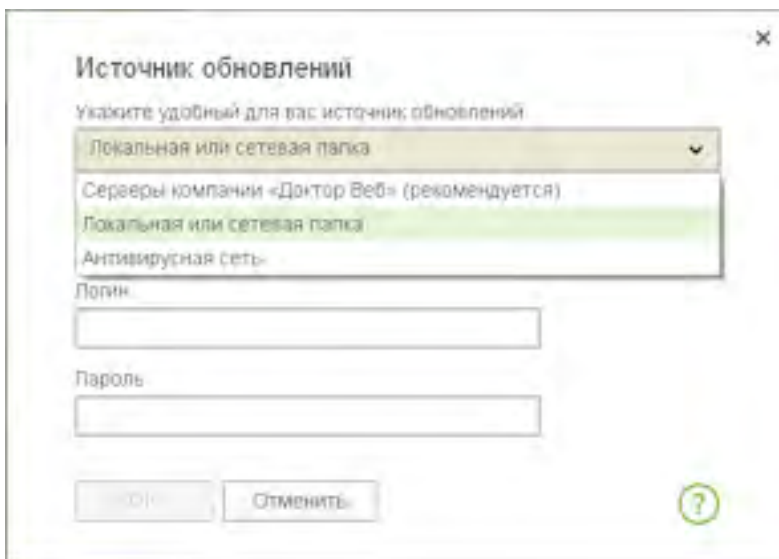


Di default, l'antivirus viene aggiornato dai server dell'azienda Doctor Web. Per cambiare la fonte degli aggiornamenti, selezionate **Modifica**.

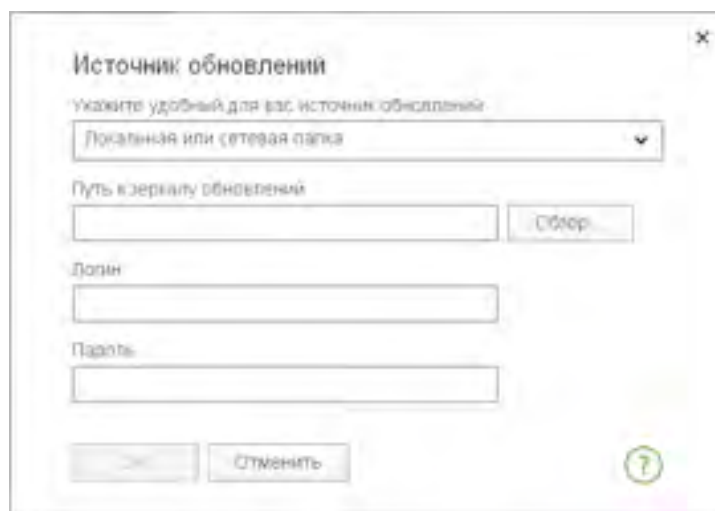






Sono disponibili tre opzioni:

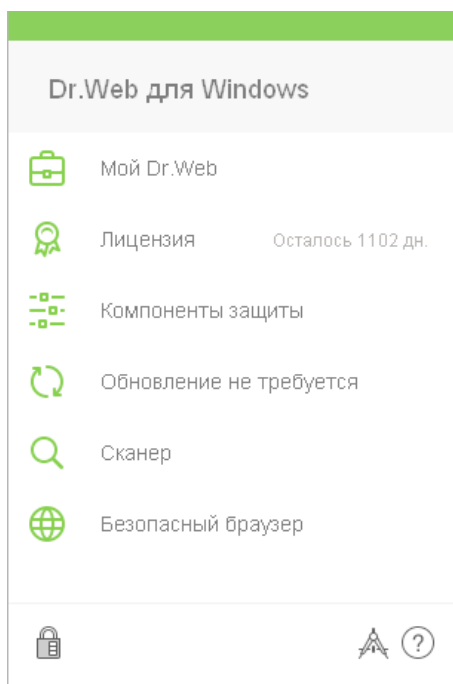


Se l'aggiornamento arriva da una cartella locale, bisogna specificare l'indirizzo della cartella e i parametri di accesso ad essa.

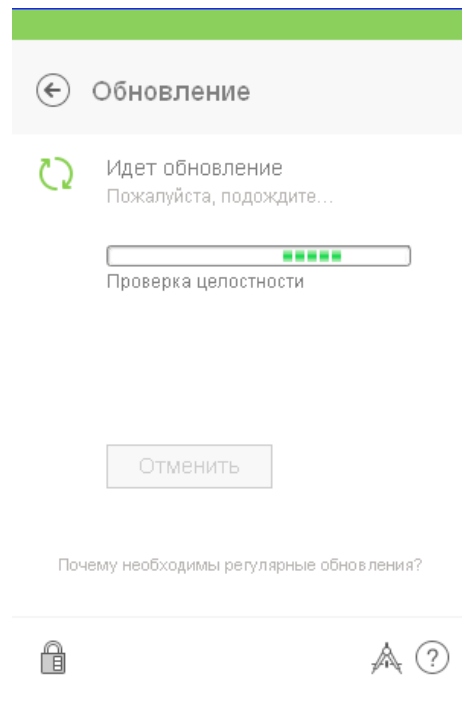
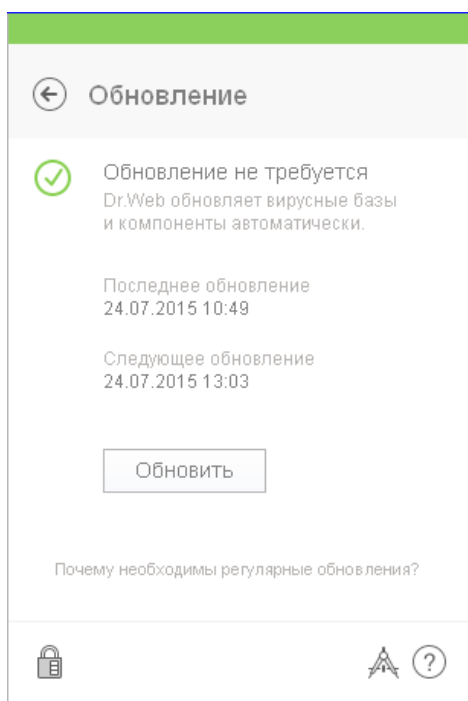


Allo stesso modo bisogna procedere se l'aggiornamento arriva da un server antivirus.

Per aggiornare l'antivirus manualmente o verificare lo stato di aggiornamento, fate clic sull'icona  nel menu di sistema e selezionate .

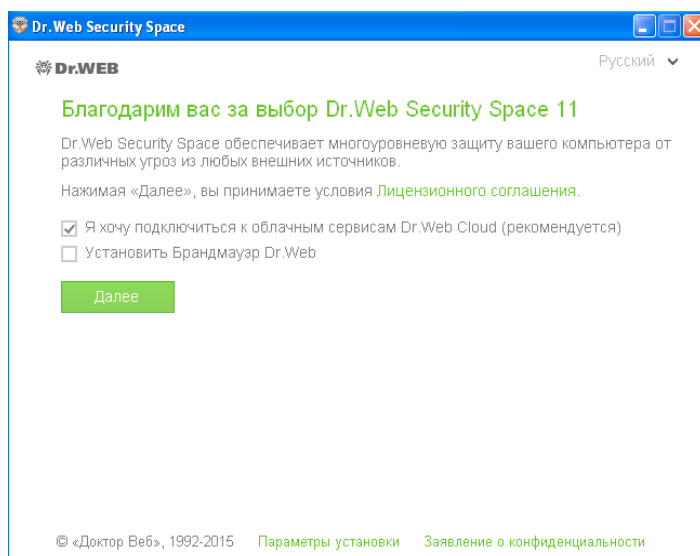





Per aggiornare manualmente, fate clic sul pulsante **Aggiorna**.

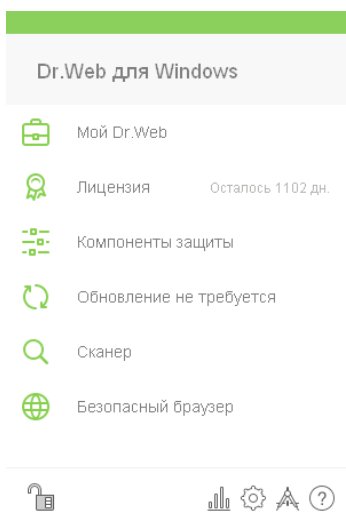


## 2.3. Configurazione del componente Dr.Web Cloud

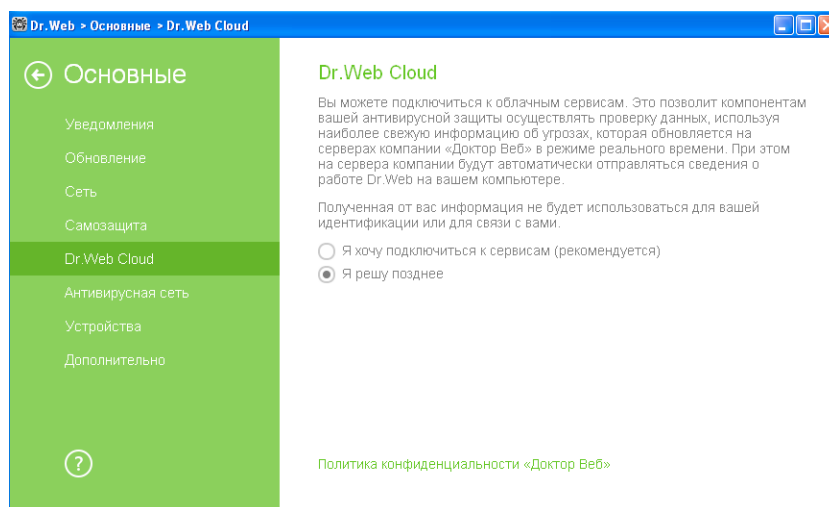
L'utilizzo del componente Dr.Web Cloud viene già offerto nel corso dell'installazione del prodotto Dr.Web Security Space. Per il funzionamento del componente, basta lasciare sul valore predefinito il parametro **Voglio connettermi ai servizi basati su cloud Dr.Web Cloud**. Dopo la fine dell'installazione, la reputazione di ogni oggetto di controllo verrà controllata in modo automatico e questo non richiede quasi nessun consumo delle risorse del computer protetto.



Se il componente Dr.Web Cloud non è stato attivato durante l'installazione, fate clic sulle icone  e  una dopo l'altra. Quindi fate clic sull'icona apparsa .



Nella finestra Impostazioni che si è aperta selezionate la voce di menu **Principali** → **Dr.Web Cloud**.






Nella finestra che si è aperta selezionate **Voglio connettermi ai servizi**.

## 2.4. Configurazione dei parametri che permettono di rilevare file malevoli precedentemente sconosciuti

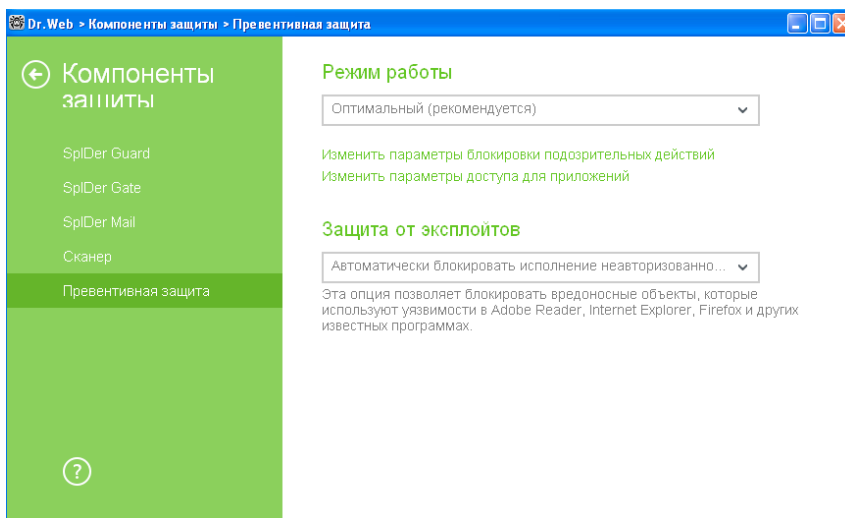
Del rilevamento dei campioni della famiglia Trojan.Encoder non ancora conosciuti si occupa il modulo **Protezione preventiva** che controlla i tentativi intrapresi dai programmi malevoli per eseguire un'azione da loro richiesta, confrontando "al volo" il comportamento dei programmi in esecuzione con il comportamento caratteristico dei trojan cryptolocker.

Il rilevamento dei programmi malevoli non conosciuti precedentemente viene assicurato dalla scansione silenziosa dei processi in esecuzione, nonché dalla scansione antivirus eseguita secondo un calendario oppure on demand.

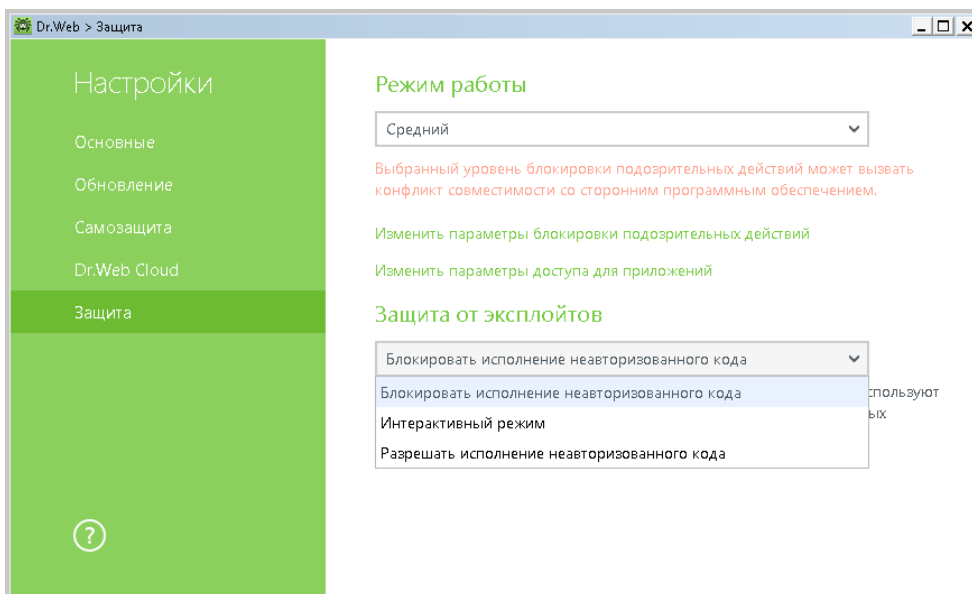
Il sottosistema di scansione silenziosa e di neutralizzazione delle minacce attive è realizzato all'interno dell'**Antirookit Dr.Web**. Questo sottosistema risiede nella memoria e cerca minacce attive nelle seguenti aree critiche di Windows: oggetti in avvio automatico, processi e moduli in esecuzione, le caratteristiche euristiche degli oggetti di sistema, la memoria operativa, i MBR/VBR dei dischi, il BIOS di sistema del computer. Se ha rilevato delle minacce, questo sottosistema può avvisarne l'utente, eseguire la cura e bloccare le influenze pericolose.

Per configurare parametri della protezione preventiva, fate clic sull'icona  nel menu di sistema, quindi nel menu che si è aperto fate clic prima su  e quindi sull'icona apparsa .

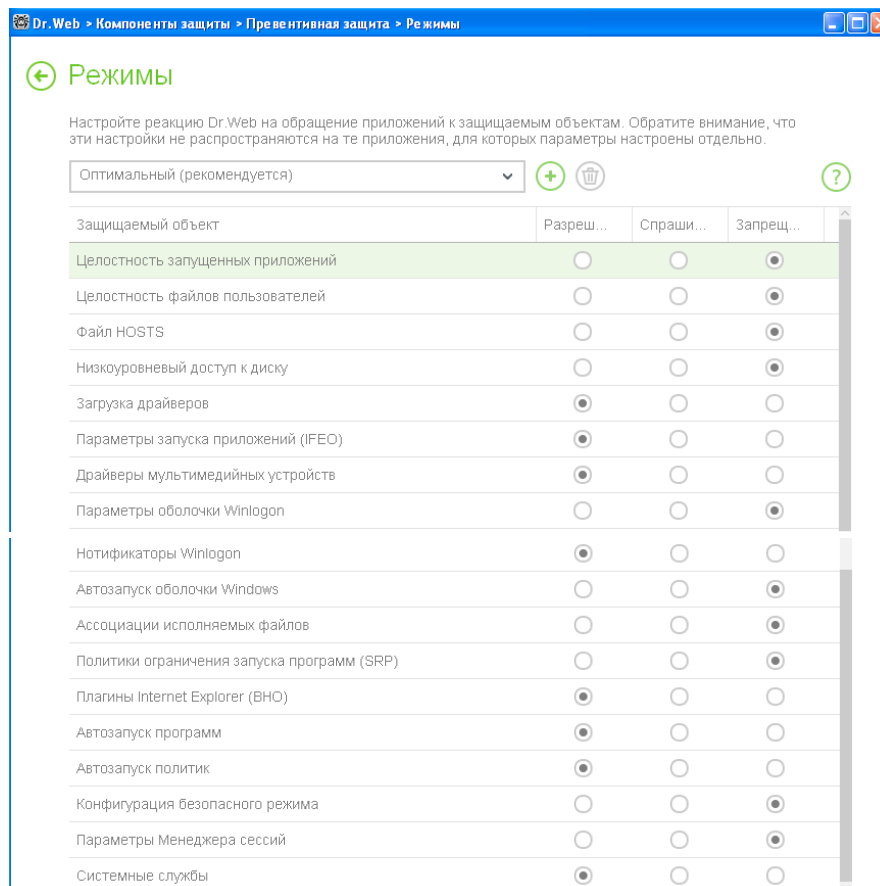
Nella finestra **Impostazioni** che si è aperta selezionate la voce **Componenti di protezione** e quindi **Protezione preventiva**.



**Attenzione!** Nel prodotto Dr.Web Katana il componente **Protezione preventiva** è stato rinominato:



Per configurare la reazione dell'antivirus alle attività di applicazioni di terzi che potrebbero portare all'infezione del computer, impostate il livello richiesto di blocco di azioni sospette. La configurazione dei parametri di protezione preventiva consente di tenere sotto controllo tutti i tentativi di modifica delle aree critiche di Windows. Per modificare le impostazioni di protezione preventiva, premete **Modifica i parametri di blocco di azioni sospette**.



Nella modalità di operazione **Ottimale**, che è quella predefinita, è proibita la modifica automatica degli oggetti di sistema, una modifica dei quali sarebbe un chiaro segno di un tentativo di influenza malevola sul sistema operativo. Inoltre è proibito l'accesso al disco a basso livello per proteggere il sistema dall'infezione dai bootkit e dai trojan-locker che infettano il master boot record del disco. È proibita anche la modifica del file HOSTS per prevenire che venga bloccato l'accesso agli aggiornamenti dell'antivirus tramite Internet e ai siti degli produttori degli antivirus.

Se c'è un elevato rischio di infezione, è necessario aumentare il livello di protezione a **Media**. In questa modalità è proibito anche l'accesso agli oggetti critici che potrebbero potenzialmente essere utilizzati dai programmi malevoli.

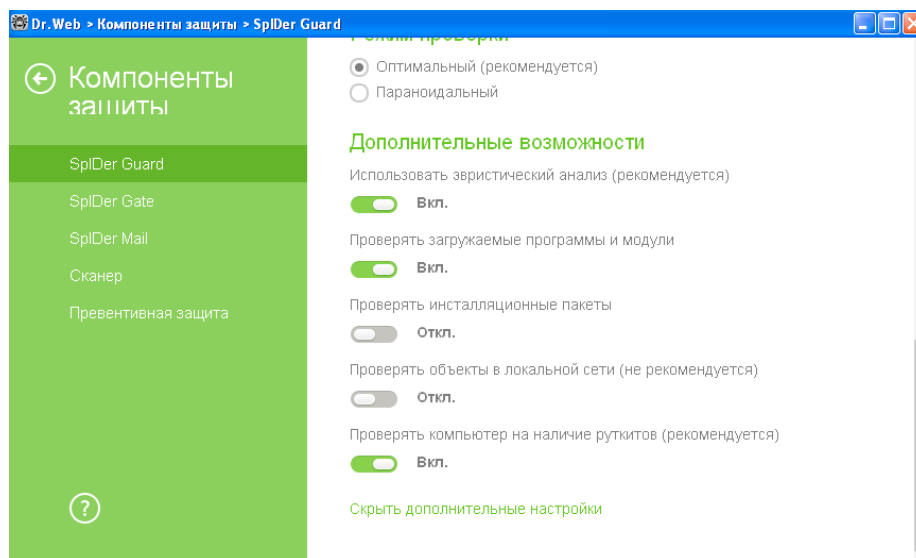
**Attenzione!** In questa modalità sono possibili conflitti di compatibilità con i software di terzi che utilizzando i rami del registro protetti.

Se necessario, per un completo controllo degli accessi agli oggetti critici di Windows, si può aumentare il livello di protezione a **Paranoicale**. In questo caso sarà disponibile un controllo interattivo del caricamento dei driver e dell'esecuzione automatica dei programmi.




Per personalizzare i parametri di funzionamento della protezione preventiva, selezionate il livello desiderato di accesso agli oggetti protetti. La modalità cambierà automaticamente a quella **Personalizzata**. La modalità personalizzata consente di configurare in modo flessibile la reazione dell'antivirus a determinate attività che potrebbero portare all'infezione del computer.

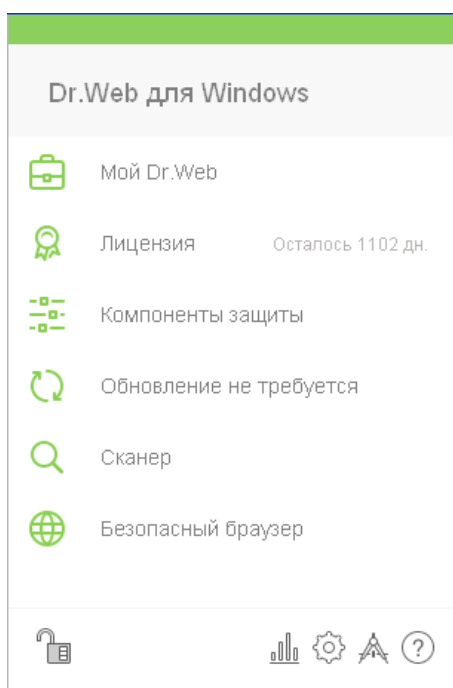
Per attivare la modalità di ricerca di rootkit, nella finestra **Impostazioni** selezionate **Componenti di protezione** → **SplDer Guard**. Nella finestra che si è aperta premete **Impostazioni avanzate**.

Di default, la funzione di scansione alla ricerca dei rootkit è attivata.

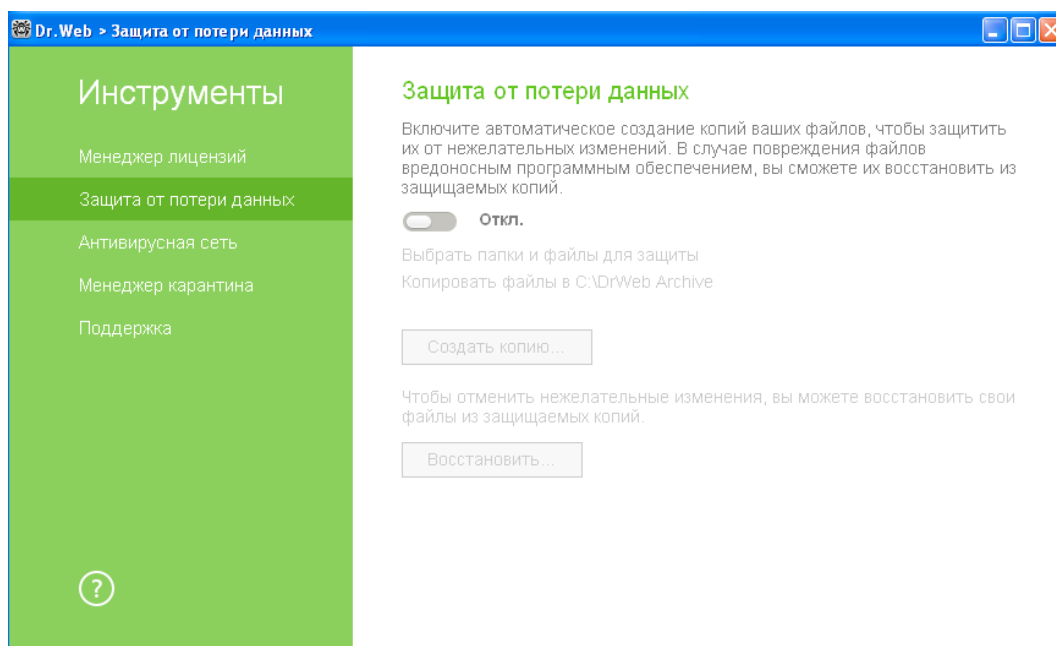


## 2.5. Le funzionalità “Prevenzione della perdita di dati”

Per configurare parametri di “Prevenzione della perdita di dati”, fate clic sull'icona  nel menu di sistema, quindi nel menu che si è aperto fate clic prima su  e quindi sull'icona apparsa .

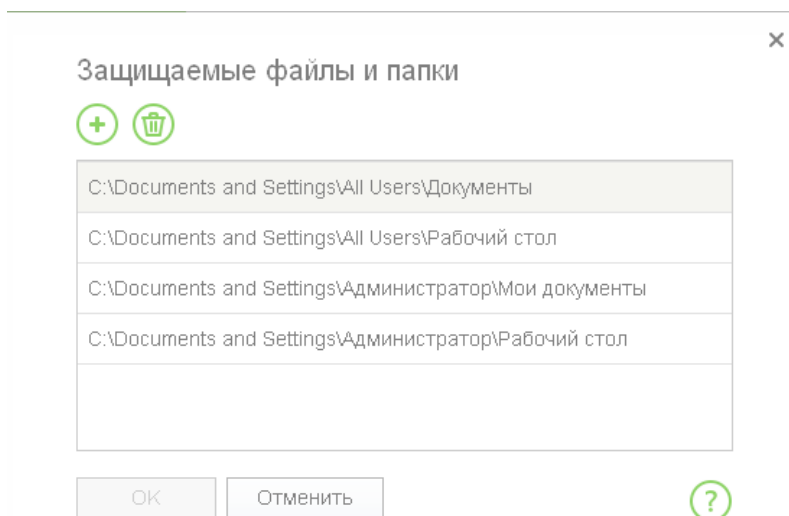


Nella finestra che si è aperta andate alla sezione **Prevenzione della perdita di dati** e premendo l'interruttore attivate la creazione automatica delle copie dei vostri dati.



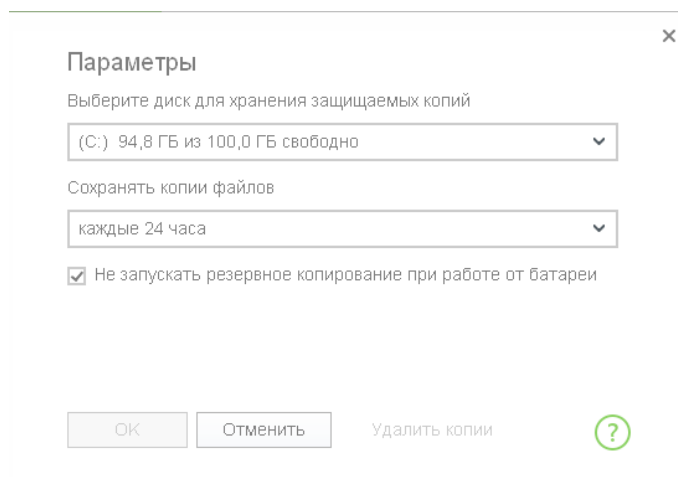


In seguito è necessario indicare i file e le cartelle di cui le copie verranno salvate.



Per aggiungere file e cartelle, fate clic sull'icona  e indicate gli oggetti da proteggere desiderati.




È possibile impostare la periodicità della creazione delle copie e il percorso di conservazione nella voce **Copia i file...**

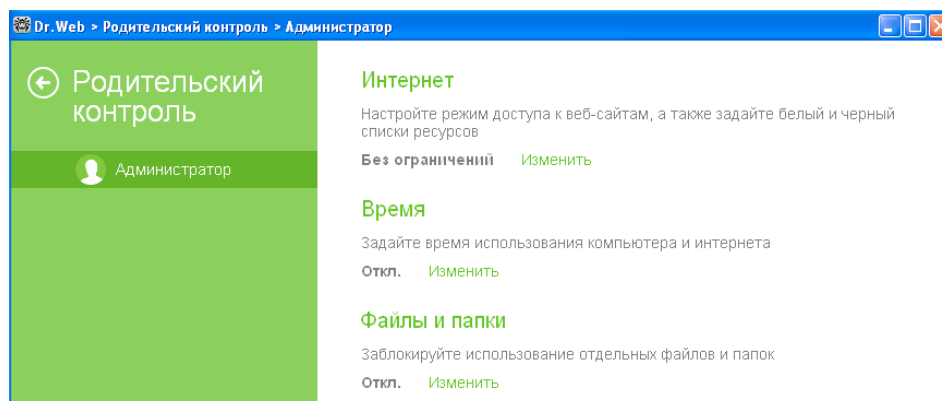


## 2.6. Limitazione della possibilità di penetrazione dei programmi cryptolocker nel computer

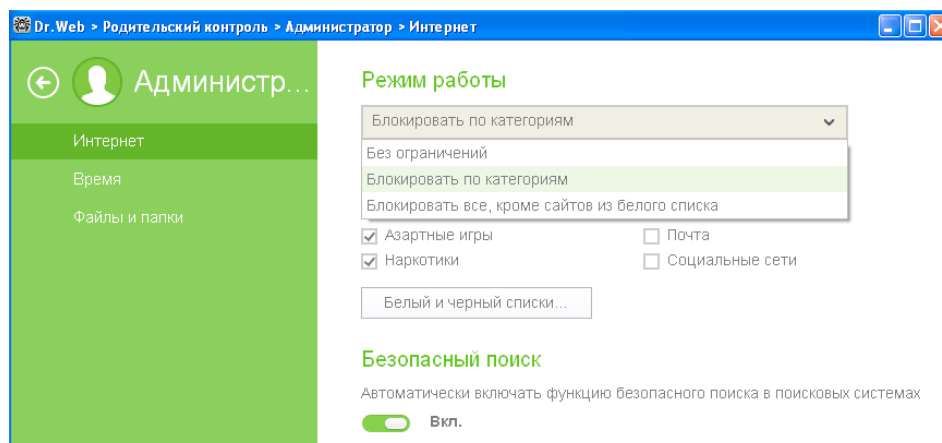
Un trojan cryptolocker potrebbe penetrare nella rete locale o in un singolo computer attraverso lo spam (di regola, il messaggio contiene un allegato malevolo o un apposito link), attraverso un messaggio istantaneo (che anche contiene un link), tramite il download del trojan da parte dell'utente stesso da un sito infetto o su una chiave usb infetta. Per ridurre il rischio dell'infezione è necessario utilizzare l'antispam e limitare la possibilità di utilizzo di risorse Internet potenzialmente pericolose e di supporti rimovibili.

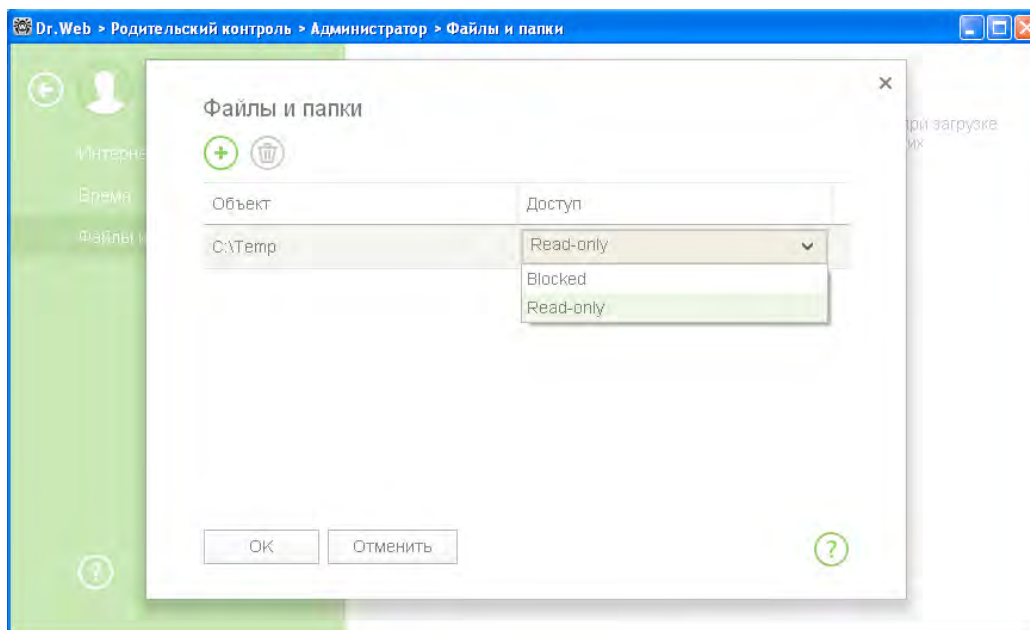
*La configurazione dell'antispam Dr.Web non rientra in questo corso in quanto l'antispam inizia a funzionare di default dal momento dell'installazione di Dr.Web Security Space e non richiede ulteriore configurazione.*

Per configurare la modalità di accesso alle risorse Internet, nonché per limitare l'accesso a file e cartelle, fate clic sulle icone  e  una dopo l'altra. Quindi fate clic sull'icona apparsa  e nella finestra **Impostazioni** andate alla voce di menu **Parental control**.



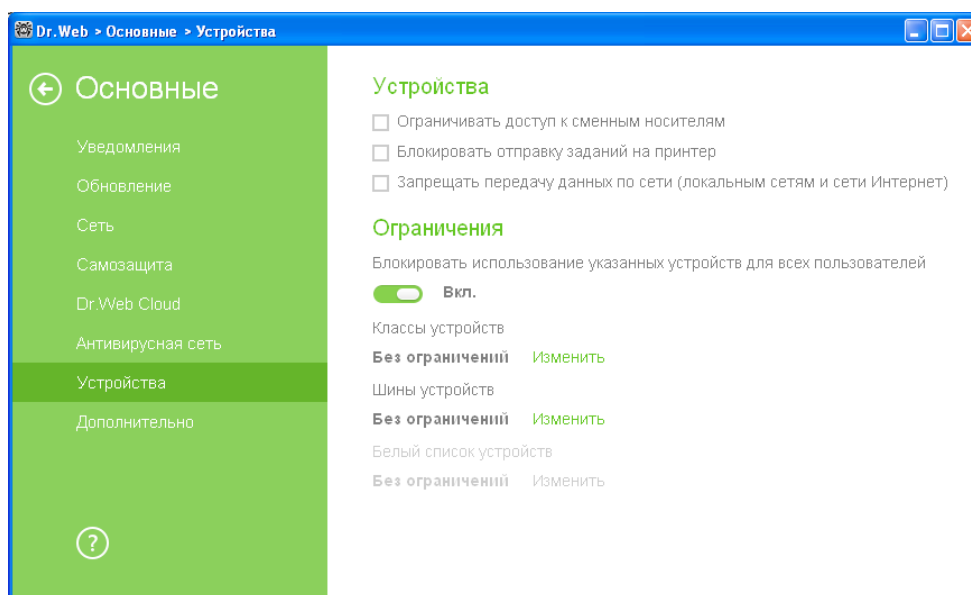
Nella finestra che si è aperta selezionate l'utente per cui volete configurare le restrizioni e fare le impostazioni necessarie.



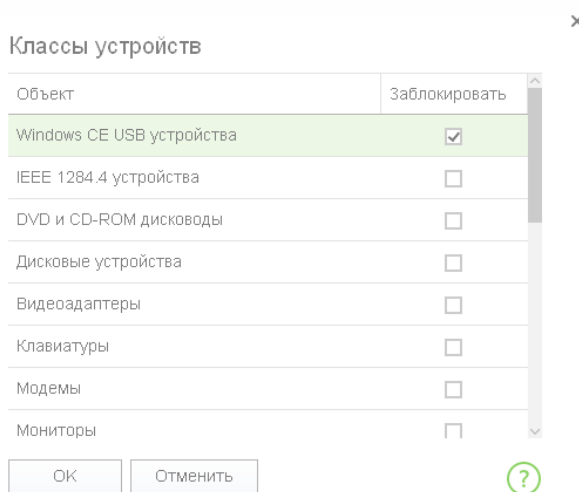



Di default, le restrizioni sono disattivate.

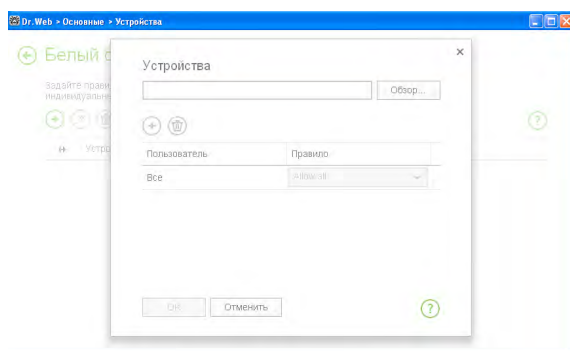
Per configurare le restrizioni riguardanti i supporti rimovibili, nella finestra **Impostazioni** selezionate **Principali** → **Dispositivi**.



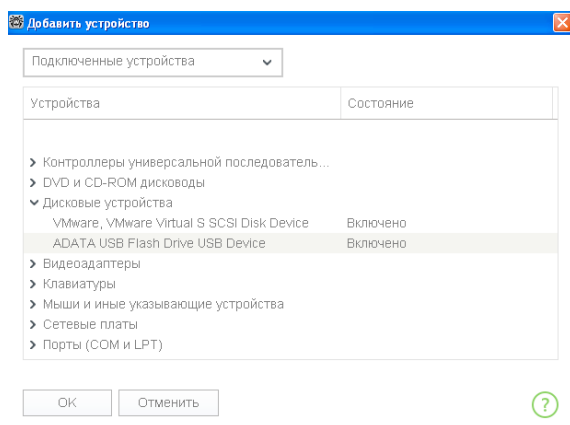
In questa finestra selezionate **Limita l'accesso ai supporti rimovibili**. Quindi premete **Modifica** per le classi di dispositivi e selezionate le classi di dispositivi desiderate.



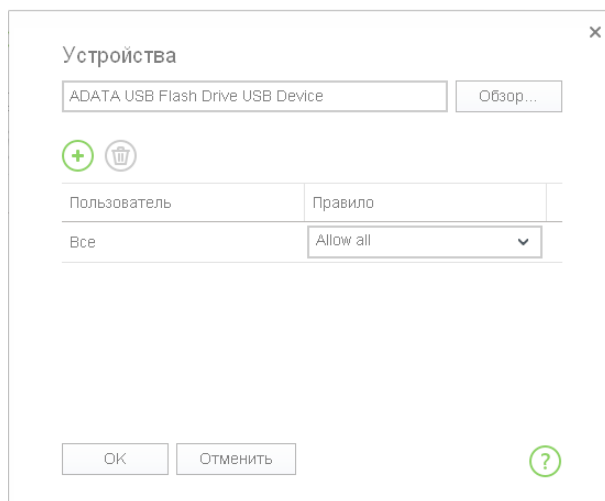
In seguito appare la possibilità di configurare la sezione **White list dei dispositivi**. Se è necessario utilizzare soltanto i supporti rimovibili consentiti, premete **Modifica** → .



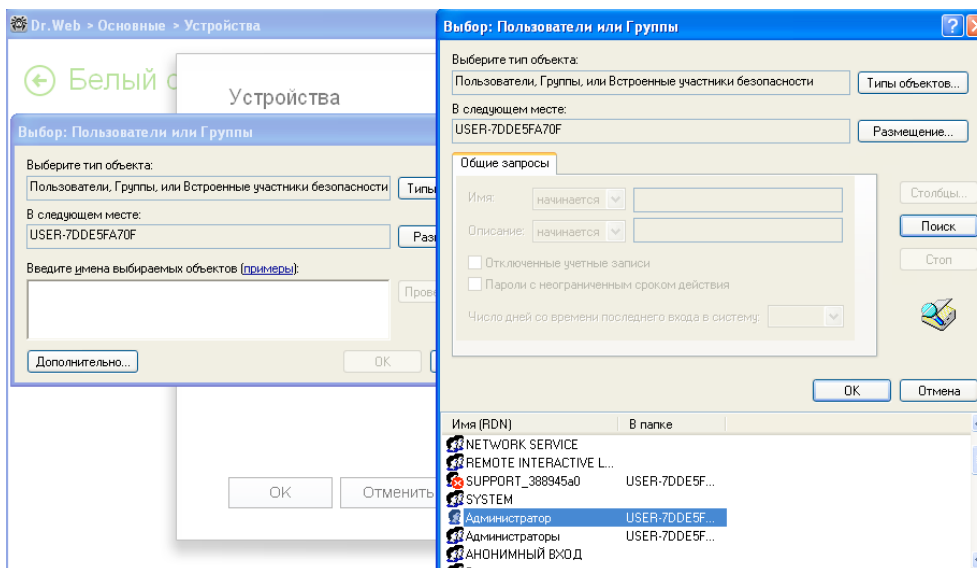
Nella finestra che si è aperta premete **Sfogliare** e selezionate il dispositivo desiderato.



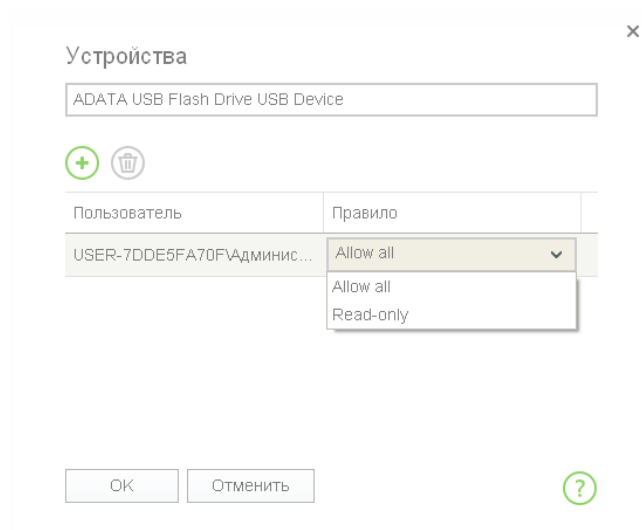
Confermate la scelta premendo **OK**.



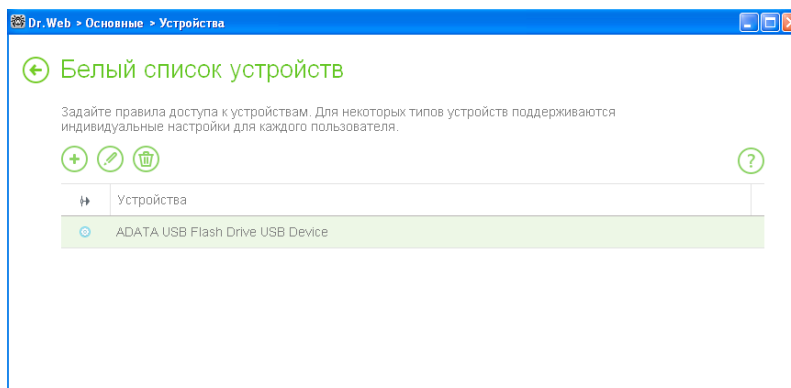
Se è necessario consentire di usare questo supporto soltanto a determinati utenti del computer, premete **+** e selezionate l'utente a cui volete consentire l'accesso al dispositivo.



Indicate i permessi di uso di questo dispositivo.



Confermate la scelta.



## 3. Raccomandazioni dell'azienda Doctor Web per la protezione del computer dai programmi cryptolocker

**Le statistiche mostrano che in oltre il 90% dei casi le vittime eseguono cryptolocker con le proprie mani.**

- Non accettate di eseguire un allegato o aprire un documento, come viene suggerito in alcune offerte in Internet (di solito sono file appositamente creati dai malintenzionati che hanno formati doc e pdf e che anche spesso sono compressi in archivi con i formati .zip, .rar, .7z e .cab. in quanto la verifica degli archivi spesso viene disattivata per migliorare le prestazioni).
- Utilizzate le soluzioni che hanno le funzionalità di backup (creano le copie dei file o di tutto il sistema). È fortemente sconsigliato creare le copie di backup copiando i file manualmente e conservare le copie di backup sul computer. Non è consigliabile conservare le copie di backup su un altro disco rigido o in una cartella di rete a cui è possibile accedere dal computer locale. È consigliabile utilizzare supporti rimovibili e/o cloud storage e creare o conservare le copie di backup nella forma criptata. In tal modo i file saranno protetti non soltanto dai programmi cryptolocker, ma anche dai guasti dell'hardware del computer.

**Attenzione!** *Prima di creare una copia di backup, bisogna assicurarsi che i file da copiare non siano già criptati e non sostituiscano le versioni normali dei file.*

A partire da Windows Vista, i sistemi operativi Windows includono il servizio di protezione del sistema su tutti i dischi che crea i backup di file e cartelle durante l'archiviazione o la creazione di un punto di ripristino del sistema. Di default, questo servizio è disponibile soltanto per la partizione di sistema.

**Attenzione!** *L'utilizzo di questo servizio non protegge dalle attività dei programmi cryptolocker visto che loro possono disattivare questo servizio e annientare i backup creati i precedenza.*

- Non aprite gli allegati alle email arrivate da mittenti sconosciuti. Nella maggior parte dei casi, i programmi cryptolocker arrivano sul computer in allegati ai messaggi elettronici. L'obiettivo del malintenzionato è quello di convincere l'utente ad aprire l'allegato all'email o a utilizzare il link riportato in tale messaggio.
- Se i vostri dati sono stati criptati da un malware, non utilizzate, senza la consulenza degli esperti, programmi per la decifrazione di dati, non modificate le estensioni dei file criptati ecc. Come risultato di queste azioni, potrete perdere completamente i vostri dati – neanche l'apposita utility di decifrazione potrà trovarli e ripristinarli.
- Attivate la visualizzazione delle estensioni dei file (v. sotto p. 3.1). Se la visualizzazione delle estensioni non è attivata, le vittime non possono vedere cosa veramente c'è all'interno degli archivi.

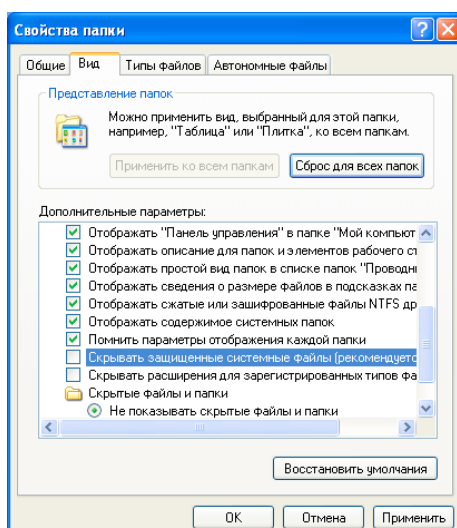
- Utilizzate soltanto software con licenza.
- Installate tempestivamente gli aggiornamenti di sicurezza del sistema operativo e di tutti i programmi installati sul computer.
- Configurate i permessi di tutti gli utenti del computer riguardanti l'accesso alle informazioni e alle cartelle di rete che loro utilizzano. Altrimenti in seguito a un'infezione del computer potrebbero risultare criptati tutti i documenti di tutti gli utenti – anche in tutte le cartelle di rete.

Per avere ulteriori informazioni su come agire in caso dell'infezione da un cryptolocker, consultate <http://legal.drweb.com/encoder?lng=en>.

### 3.1. Attivazione della visualizzazione delle estensioni di file

Per attivare la visualizzazione delle estensioni di file:

- In caso di **Windows XP**: nel menu **Start** selezionate **Impostazioni** → **Pannello di controllo** → **Proprietà cartelle** e deselezionate la casella di controllo **Nascondi le estensioni per i tipi di file conosciuti**.



- in caso di **Windows 7**: sulla tastiera premete il tasto Alt sinistro. Nel menu apparso premete **Servizio** → **Opzioni cartella**, nella finestra che si è aperta passate alla scheda **Visualizzazione** e nell'elenco delle impostazioni avanzate deselezionate la casella di controllo **Nascondi le estensioni per i tipi di file conosciuti**.
- in caso di **Windows 8/8.1**: aprite qualsiasi cartella o avviate Esplora risorse di Windows 8 premendo i tasti Windows + E. Nel menu principale di Esplora risorse passate alla scheda **Visualizza** e mettete il segno di spunta accanto alla voce **Estensioni nomi file** – se è contrassegnata, le estensioni di file vengono mostrate (non soltanto nella cartella selezionata, ma dappertutto sul computer) se no, le estensioni sono nascoste.



## 4. Le azioni dell'utente se ha scoperto file criptati e/o una richiesta di riscatto

Per aumentare le chance di recupero dei dati crittografati, in nessun caso si deve:

- modificare l'estensione dei file cifrati;
- reinstallare il sistema operativo;
- utilizzare per conto proprio – senza avere le raccomandazioni degli specialisti di supporto tecnico Doctor Web – qualche programma per la decifrazione/recupero di dati;
- eliminare/rinominare qualche file e programma (compresi file temporanei);
- se è stata avviata una scansione antivirus – non si devono eseguire alcune azioni definitive di cura/eliminazione di oggetti malevoli.

### 4.1. Le utility di decifrazione

La decifrazione dei file criptati dai malintenzionati è possibile tramite le apposite utility che vengono messe a disposizione su richiesta dal servizio di supporto tecnico Doctor Web. Purtroppo, il grande numero di trojan-cryptolocker che spunta ogni giorno non permette di creare utility per tutti i cryptolocker. Se i vostri file sono stati criptati da un trojan ancora sconosciuto, potete ordinare il servizio di decifrazione. Il servizio è gratis per i proprietari delle licenze commerciali valide Dr.Web Security Space, Dr.Web Enterprise Security Suite (Protezione completa) e per gli abbonati al servizio "Antivirus Dr.Web" (il piano tariffario Dr.Web Premium) – se queste condizioni sono soddisfatte al momento del verificarsi dell'incidente informatico.

Se avete bisogno del servizio di decifrazione, [inviateci](#) per l'analisi almeno tre-cinque file criptati di vario tipo. Inoltre, le informazioni aggiuntive possono aiutare la decifrazione – una descrizione del processo di infezione, l'email di riscatto ecc. Se sapete dopo l'esecuzione di quale file i malintenzionati hanno potuto criptare i vostri dati, è preferibile allegare anche questo file alla richiesta.

**Attenzione!** Prima di eseguire le utility, create copie dei file criptati.

## 4.2. Dove potrebbero esserci i file dei programmi cryptolocker

Se avete trovato un file sospetto di cui l'avvio aveva potuto portare all'infezione del computer e alla cifratura dei file – inviate il file sospetto per l'analisi. I file potrebbero esserci nei seguenti percorsi:

APPDATA	SO Windows NT/2000/XP: Disco:\Documents and Settings\%UserName%\Application Data\ %USERPROFILE%\Local Settings\Application Data SO Windows Vista/7/8: Disco:\Users\%UserName%\AppData\Roaming\ %USERPROFILE%\AppData\Local
TEMP (directory temporanea)	%TEMP%\*.tmp %TEMP%\*.tmp\ %TEMP%\* %WINDIR%\Temp
Directory temporanea di Internet Explorer	SO Windows NT/2000/XP: %USERPROFILE%\Local Settings\ Temporary Internet Files\ SO Windows Vista/7/8: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\ ..\temporary internet files\content.ie5\ ..\temporary internet files\content.ie5\*\
Desktop	%UserProfile%\Desktop\
Cestino	Disco:\Recycler\ Disco:\\$Recycle.Bin\ Disco:\\$Recycle.Bin \s-1-5-21-????????-????????-????????-1000 (? -- 0-9)
Directory di sistema di Windows	%WinDir% %SystemRoot%\system32
Directory dei documenti dell'utente	%USERPROFILE%\Documenti\ %USERPROFILE%\Documenti\Downloads
Directory per il download dei file nel web browser	%USERPROFILE%\Downloads
Directory di esecuzione automatica	%USERPROFILE%\Menu Start\Programmi\Esecuzione automatica

**Attenzione!** I file dei Trojan.Encoder potrebbero esserci non soltanto nei percorsi sopracitati.

## 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](http://www.drweb.com) | [www.free.drweb.com](http://www.free.drweb.com) | [www.av-desk.com](http://www.av-desk.com) | [www.drweb-curent.com](http://www.drweb-curent.com)



© Doctor Web,  
2003 – 2017



Unitevi a noi sui social network

