Dr.WEB®
dal 1992

Proteggi ciò che crei

Trojan — encoder
Minaccia No 1.

I trojan-encoder sono una delle più gravi minacce di oggi. I programmi malevoli della famiglia **Trojan.Encoder** criptano file di utente sui PC e sui dispositivi mobili dopodiché richiedono alla vittima di pagare per la decifratura.

I primi trojan della famiglia Trojan.Encoder comparsero negli **anni 2006–2007**.

A partire da gennaio 2009, il numero di versioni è aumentato circa del **1900%!**

Attualmente il **Trojan.Encoder** ha **diverse migliaia di varianti**.

Cosa si perde

Oggi i malfattori richiedono di pagare fino a 1500 bitcoin per la decifratura di file.
1 bitcoin = 272 euro o 330 dollari
La somma di riscatto può raggiungere **49500 dollari**.

Anche se pagherete il riscatto a un malintenzionato, egli non vi garantirà il recupero delle informazioni.

Ci sono casi assurdi, per esempio quando, nonostante il riscatto pagato, i criminali non hanno potuto decifrare i file che aveva cifrato il Trojan.Encoder (Cryptolocker) **creato da loro stessi** e hanno consigliato all'utente vittima di chiedere l'aiuto... al servizio di supporto tecnico Doctor Web!

Come i trojan-encoder si infiltrano nel computer

In oltre il 90% dei casi, gli utenti **avviano** (attivano) gli encoder sul computer con le proprie mani. E se è una versione sconosciuta dal database dei virus, la distruzione dei file è inevitabile.

Alcune versioni di encoder non vengono riconosciute da nessun antivirus.

La causa è che i malintenzionati creando trojan-encoder li testano contro il rilevamento da parte delle versioni attuali degli strumenti antivirus. Pertanto, se viene utilizzato un mero antivirus che non include protezione preventiva, parental control e gli altri strumenti che possono limitare la possibilità di penetrazione e di esecuzione di programmi malevoli ancora sconosciuti dal database dei virus, l'utente corre un rischio maggiore di prendersi un trojan-encoder sul computer, da cui nessun antivirus potrà proteggerlo.

3d street Yamskogo polya 2-12A, Moscow, Russia, 125040

Phone: +7 495 789–45–87
Fax: +7 495 789–45–97

www.drweb.com
www.drweb-curenet.com
www.av-desk.com
freedrweb.com

Dr.WEB®
dal 1992

Come aiuta Dr.Web

1. Agite in modo proattivo – utilizzate un programma antivirus che includa le tecnologie di protezione preventiva. Esse consentono di riconoscere gli encoder sulla base degli algoritmi di comportamento simili nelle loro versioni.
   - Protezione preventiva Dr.Web: http://products.drweb.com/technologies/preventive_protection.
2. Per proteggere le vostre informazioni dall'eventuale perdita causata dalle azioni dei trojan-encoder, utilizzate il componente "Prevenzione della perdita di dati" che fa parte di Dr.Web Security Space (versioni 9 e 10). A differenza dei soliti programmi di backup, Dr.Web utilizza uno storage di backup che è **protetto** dall'accesso non autorizzato da parte dei malintenzionati. Nel caso un trojan riuscirà comunque a cifrare i vostri file (non più di 10), sarete in grado di recuperarli in modo autonomo senza dover contattare il servizio di supporto tecnico Doctor Web.
   - Video su protezione di dati da perdita: http://support.drweb.ru/video/security_space.
3. Nel caso il vostro PC è stato infettato da una variante di trojan sconosciuta da Dr.Web, rivolgetevi per l'aiuto nella decifratura al supporto tecnico Doctor Web e **non eseguite alcun'azione con il computer compromesso**.
   - Regole di condotta in caso di incidenti informatici provocati da virus: http://legal.drweb.com/encoder.
   - Perizia di incidenti informatici provocati da virus: http://antifraud.drweb.com/expertise.

   Per gli utenti commerciali dei prodotti Dr.Web, la decifratura da parte dei nostri specialisti è gratuita.
   - Richiesta per la decifratura gratuita: https://support.drweb.com/new/free_unlocker/for_decode/?lng=it.

Prospettive della decifratura

I trojan della famiglia Trojan.Encoder utilizzano diverse **decine di vari algoritmi di cifratura** di file.

Secondo le statistiche di Doctor Web, la decifratura dei file corrotti da un trojan è possibile soltanto nel 10% dei casi.

Questo significa che è persa per sempre la maggior parte dei dati degli utenti che trascurano le necessarie misure di protezione.

Da metà aprile 2013 a marzo 2015, il laboratorio di virus Doctor Web ha ricevuto oltre **8500 richieste per la decifratura** di file criptati da trojan-encoder.

Ogni giorno il laboratorio di virus Doctor Web riceve in media 40 richieste per la decifratura.

Alcune versioni di trojan **possono essere decifrate soltanto dagli specialisti Doctor Web** – gli utenti lo testimoniano sui forum.

A partire da maggio 2014 gli specialisti Doctor Web hanno condotto un'indagine scientifica per creare gli algoritmi di decifratura per affrontare il **Trojan.Encoder.398. Oggi lo sviluppatore degli antivirus Doctor Web è l'unica società** i cui specialisti **con la probabilità del 90%** possono ripristinare completamente i dati criptati da questo trojan.

Per maggiori informazioni su encoder: http://antifraud.drweb.com/encryption_trojs/

Doctor Web
Doctor Web è un'azienda russa, produttrice degli antivirus Dr.Web sviluppati fin dal 1992.
Russia, 125040, Mosca, la 3° via Yamskogo polya, 2-12A
Tel.: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97
www.drweb.com | www.drweb-curenet.com | www.av-desk.com | freedrweb.com