Dr.WEB®
since 1992

Defend what you create

トロイの木馬エンコーダ
脅威ランキング上位

現在、トロイの木馬エンコーダは最も深刻な脅威の一つです。Trojan.Encoderファミリーに属するマルウェアはコンピュータ及びモバイルデバイス上のユーザーファイルを暗号化し、被害者から復号化するための身代金を要求しています。

Trojan.Encoderファミリー最初の亜種は2006-2007年に発見されました。

2009年１月以降、Trojan.Encorderの驚異的な増加率は1900%!!

現時点で数千種の亜種が存在するTrojan.Encoderは、ユーザーにとって最も危険な脅威の一つであるといえます。

ユーザーにとっての被害について

現在、ファイルを復号化するために要求される身代金は1500ビットコインになっています（1ビットコイン＝272 ユーロ 又は 330 ドル）。

49500ドルの身代金というケースさえあります。

しかし、犯罪者に身代金を支払っても、データが復元される確実性が全くありません。

被害者からの報告によると、身代金を払った後、犯罪者は自己作成のTrojan.Encoderに暗号化されたファイルの復号化に失敗し、複合化できなくなったケースも発生しています。

トロイの木馬エンコーダがシステム上に侵入する経路とは？

ユーザー自身の不注意でコンピュータ上にトロイの木馬を持ち込んで起動させてしまうというケースが90%におよびます。もし、ウイルスデータベースにはない未知の亜種であれば、ファイルが破損される可能性が非常に高いです。

アンチウイルスが検知できないトロイ木馬エンコーダの亜種が存在します。

トロイの木馬を作成するときに、ウイルス作成者は最新アンチウイルスソフトウェアに検出されないようにテストを行っています。上記のことからすると、予防的保護機能、ペアレンタルコントロール、及びウイルスデータベースにはない未知のマルウェア進入を防ぐ他の機能を備えていないアンチウイルスを使うと、コンピュータはトロイの木馬に感染してしまうリスクが非常に高くなります。

Dr.Webが役に立つ理由は？

1. 前もって予防対策を施すために、予防的保護機能を搭載するアンチウイルスソフトウェアの利用が望ましいです。予防的保護機能は類似するパターンでトロイの木馬を検出することが可能です。
   - Dr.Web Preventive Protection（予防的保護機能）:
     http://products.drweb.ru/technologies/preventive_protection/

株式会社Doctor Web Pacific〒210-0005
神奈川県川崎市川崎区東田町1-2
NKF川崎ビル 2F
TEL 044-201-7711
FAX 044-201-7712
www.drweb.co.jp
www.av-desk.com
www.freedrweb.com

Dr.WEB®
since 1992

2. トロイの木馬侵入によるデータ損失を防ぐためにDr.Web Security Space (バージョン9 及び10)に含まれるデータ損失保護機能を利用してください。普通のバックアッププログラムと違って、Dr.Webは不正アクセスから保護されるファイルコピーの保存場所を用いています。万一、ファイルがトロイの木馬に暗号化されたら、ユーザー自身は独自で復元できるため、Doctor　Webテクニカルサポートにお問い合わせる必要はありません（暗号化されたファイル数が10個以下の場合）。

   ■ "データ損失防止機能に関する動画(英語)：http://support.drweb.ru/video/security_space/

3. コンピュータがDr.Webデータベースに追加されていない未知のトロイの木馬の亜種に感染した場合、**コンピュータに対して一切の対策を取らずに**、復号化を行うためにDoctor Webテクニカルサポートにお問い合わせください。

   ■ コンピュータがウイルスに感染した場合どうすれば？ http://legal.drweb.ru/encoder/

   Dr.Web有償版を利用するユーザーに対して弊社スタッフは復号化サービスを無料で提供いたします。

   ■ 無料復号化サービスのお問い合わせ：https://support.drweb.com/new/free_unlocker/for_decode/?lng=jp

ファイル復号化の成功率について

Trojan.Encoderファミリに属するトロイの木馬はそれぞれ異なる数十種類の暗号化ルーチンを使用しています。

Doctor Web 統計データによると、トロイの木馬に破損されたファイルを復号化できる成功率は10%に過ぎません。

この統計を見ると、セキュリティ対策を怠ったユーザーにとって、殆どのデータを復元するのが不可能であることが明らかになります。

2013年4月中旬から2015年3月までには、トロイの木馬エンコーダによって暗号化されたファイルの復号化について、Doctor　Webウイルスラボへのお問い合わせが8500件を超えました。

毎日、Doctor　Webウイルスラボ宛に送信されるファイル復号化についてのお問い合わせは、およそ40件になっています。

フォーラムの投稿者によると、トロイの木馬亜種の一部についてはDoctor　Webスタッフのみ復号化することが可能なものがあります。

2014年5月以降、Doctor　WebではTrojan.Encoder.398の暗号解読ルーチンの作成を目的として徹底的な研究が行われました。現時点においてDr.Webは、暗号化されたデータを**90%**の確率で復元できる唯一のアンチウイルスメーカーです。これを話題にしたニュースが2014年11月にリリースされました。

トロイの木馬エンコーダに関する詳しい情報はこちら: http://antifraud.drweb.com/encryption_trojs/

Doctor Webは、ロシアに本社を置く、『Dr.Webアンチウイルスソフトウェア』のデベロッパーです。その製品の開発は1992年に始まりました。Doctor Webは、あらゆるビジネスにとって重要かつ不可欠な要素―情報セキュリティ―を満たすためのソフトウェアの、ロシア市場におけるキープレーヤーです。また、独自のマルウェア検出及び修復テクノロジーを有する、世界でも数少ないアンチウイルスベンダーの1つでもあります。そのアンチウイルス保護システムによって、カスタマーの情報システムを、未知のものを含むあらゆる脅威から保護します。Doctor Webは、アンチウイルスをサービスとして提供した最初の会社であり、現在においても、ロシア市場におけるインターネットサービスプロバイダ（ISP）に 対するインターネットセキュリティサービスの第一人者として不動の地位を保っています。数々の賞を受賞し、ロシア連邦による認定を受けた証明書を保有する Doctor Webの世界中に広がるユーザーが、有能なロシアのプログラマーチームによって生み出される製品の品質の高さを明確に物語っています。

株式会社Doctor Web Pacific〒210-0005
神奈川県川崎市川崎区東田町1-2
NKF川崎ビル 2F

TEL 044-201-7711
FAX 044-201-7712