Dr.WEB®
с 1992 года

Защити созданное

Троянцы-шифровальщики

Угроза № 1

Троянцы-шифровальщики — одна из самых актуальных угроз на сегодняшний день. Вредоносные программы семейства **Trojan.Encoder** шифруют на ПК и мобильных устройствах пользовательские файлы, после чего требуют у жертвы оплатить их расшифровку.

Первые троянцы-шифровальщики семейства **Trojan.Encoder** появились в **2006–2007 годах**.

С января 2009 года число их разновидностей увеличилось примерно на **1 900%!**

В настоящее время **Trojan.Encoder** имеет **несколько тысяч модификаций**.

Что вы теряете

Сегодня вымогатели требуют за расшифровку файлов до 1 500 биткоинов.

1 биткоин = 272 евро или 330 долларов.

Сумма выкупа может достигать **49 500 долларов**.

Даже если вы заплатите выкуп злоумышленнику, никакой гарантии восстановления информации он вам не даст.

Доходит до курьезов – зафиксирован случай, когда, несмотря на заплаченный выкуп, преступники не смогли расшифровать файлы, зашифрованные созданным ими **Trojan.Encoder**, и отправили пострадавшего пользователя за помощью... в службу технической поддержки компании «Доктор Веб»!

Как троянцы-шифровальщики проникают на компьютер

Более чем в 90% случаев пользователи запускают (активируют) на компьютере шифровальщиков собственными руками. И если это не известная вирусной базе модификация — уничтожение файлов неизбежно.

Некоторые модификации шифровальщиков не распознаются ни одним антивирусом.

Происходит это потому, что в процессе создания злоумышленниками троянцев-шифровальщиков производится их тестирование на необнаружение актуальными версиями антивирусных средств. Таким образом, используя только антивирус, в составе которого нет превентивной защиты, родительского контроля, а также иных средств ограничения возможности проникновения и запуска еще неизвестных вирусной базе вредоносных программ, пользователь подвергается повышенной опасности заражения троянцем-шифровальщиком, от которой не спасет ни один антивирус.

ООО «Доктор Веб»

125040, Россия, Москва,
3-я ул. Ямского поля,
вл. 2, корп. 12а

Телефон: +7 495 789–45–87
(многоканальный)
Факс: +7 495 789–45–97

антивирус.рф
www.drweb.ru
www.av-desk.com
www.freedrweb.com

Dr.WEB®
с 1992 года

Чем поможет Dr.Web

1. Действуйте на опережение – используйте антивирусную программу, в состав которой входят технологии превентивной защиты. Они позволяют распознать шифровальщиков по схожим между их модификациями алгоритмам поведения.
   - Превентивная защита Dr.Web: http://products.drweb.ru/technologies/preventive_protection.
2. Для предотвращения потери данных в результате действия троянцев-шифровальщиков используйте компонент «Защита от потери данных», входящий в Dr.Web Security Space (версии 9 и 10). В отличие от обычных программ резервного копирования, Dr.Web использует **защищенное** от несанкционированного доступа злоумышленников хранилище для копий файлов. И если троянец все-таки зашифрует ваши файлы (не более 10), вы сможете восстановить их самостоятельно, без обращения в службу технической поддержки «Доктор Веб».
   - Видео о защите от потери данных: http://support.drweb.ru/video/security_space.
3. В случае если ваш ПК оказался инфицирован неизвестной Dr.Web модификацией троянца, обратитесь за помощью в расшифровке в службу технической поддержки «Доктор Веб», не предпринимая никаких действий с зараженным компьютером.
   - Правила поведения в условиях вирусозависимого компьютерного инцидента http://legal.drweb.ru/encoder.
   - Экспертиза вирусозависимых компьютерных инцидентов: http://antifraud.drweb.ru/expertise.

   Для коммерческих пользователей продуктов Dr.Web расшифровка силами наших специалистов – бесплатна.
   - Запрос на бесплатную расшифровку: https://support.drweb.ru/new/free_unlocker/for_decode/?lng=ru.

Перспективы расшифровки

Троянцы семейства **Trojan.Encoder** используют **несколько десятков различных алгоритмов шифрования** пользовательских файлов.

По статистике компании «Доктор Веб», расшифровка поврежденных троянцем файлов возможна только в 10% случаев.

А это значит, что для пользователей, пренебрегавших нужными мерами защиты, большинство их данных потеряны безвозвратно.

С середины апреля 2013 года по март 2015 года в антивирусную лабораторию компании «Доктор Веб» поступило более **8 500 заявок на расшифровку** файлов, пострадавших от действий троянцев-энкодеров.

Ежесуточно в среднем 40 заявок на расшифровку поступают сотрудникам антивирусной лаборатории «Доктор Веб».

Некоторые модификации троянцев **могут расшифровать только специалисты компании «Доктор Веб»** – об этом свидетельствуют пользователи на форумах.

Начиная с мая 2014 года специалисты компании «Доктор Веб» проводили серьезную научно-исследовательскую работу по созданию алгоритмов расшифровки **Trojan.Encoder.398. На сегодняшний день разработчик антивирусов Dr.Web является единственной компанией**, специалисты которой с вероятностью в 90% могут полностью восстановить зашифрованные этим троянцем данные.

Подробнее о шифровальщиках: http://antifraud.drweb.com/encryption_trojs.

ООО «Доктор Веб»

«Доктор Веб» – российский разработчик средств информационной безопасности. Антивирусные продукты Dr.Web разрабатываются с 1992 года.
125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Телефон: +7 (495) 789–45–87 (многоканальный), факс: +7 (495) 789–45–97

антивирус.рф | www.drweb.ru | www.av-desk.com | www.freedrweb.com