Осовский И.А, softmasterhl.awardspace.info
«специалист по внедрению ПСПО в системе образования» 2011г.,
физик, математик, программист, эксперт по компьютерам и свободному ПО.

Незащищённость Операционной Системы «Окна» (Windows) от вредоносных шифраторов пользовательской информации.

«оценка переводов средств в платёжной системе Bitcoin от заражённых пользователей шифровальщиком CryptoLocker за период с 15.10.2013 по 18.12.2013 - около $27 млн.»…
«в Австралии, по официальным данным, с августа по декабрь 2014 года произошло около 16 тыс. онлайн-вымогательства, при этом общая сумма выкупа - около $7 млн.»
https://ru.wikipedia.org/wiki/Ransomware.

Наверно, излишне напоминать, что всё это происходило в широко распространённой ОС «Окна»: лицензионной, обновлённой, защищённой «защитником» и брандмауером, насилуемой разными лицензионными и обновлёнными — работающими антивирусными программами или без всего этого.
Ведь сами по себе шифровальщики являются лишь инструментом, а не вредоносными программами (и, само собой, даже не вирусами). Более того, считается, что шифровальщик начал действовать с согласия пользователя (санкционированно), как и большинство «закрытых» программ, в том числе, и сама ОС«Окна», используя «современную» (фактически — обманную, мошенническую) практику получения выражения согласия на неизвестные (недокументированные) для пользователя действия ПО — путём нажатия на кнопочку мышкой или клавиатурой… Однако, этот инструмент может быть использован, в том числе, и для незаконного последующего вымогательства.

Шифровальщик XTBL — это вредоносная программа, которая при своей активизации шифрует пользовательские файлы (например: документы, изображения, видео, …), меняет расширение их на .xtbl *«Ваши файлы были зашифрованы. Чтобы расшифровать их, Вам необходимо отправить код на электронный адрес … Далее вы получите все необходимые инструкции. Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.»* Это пример сообщения, о том, что можно попрощаться со всеми собственными пользовательскими данными или восстановить их, купив программу и ключ, необходимые для расшифровки. XTBL использует качественный, современный, стойкий алгоритм шифрования, что практически исключает возможность подбора ключа для расшифровки файлов. XTBL может распространяется при любом внесении информации в компьютер, как червь, вирус, троян.. — несанкционированно, или, например, через «просматриваемые» сайты, или электронную почту, в которой, используя вводящие в заблуждения заголовки и содержание писем, пытаются обманом заставить пользователя открыть вложенный в письмо документ, а в результате открытия прикреплённого файла будет запуск шифровальщика и внедрение его в ОС.

В защищённых ОС, например, Линукс, Мак, Юникс … — внедрение чего-либо в ОС несанкционированно или в результате действий пользователя, не являющимся администратором ОС, — невозможно. Поэтому, в частности, в них нет вирусов и т.п. ***Удобные для пользователя, качественные и современные, лицензионные и свободные*** **дистрибутивы с ОС Линукс — распространяется бесплатно, например, российский — АльтЛинукс**.