Крипто вирус шифровальщик, как избежать потерю данных, памятка для пользователей

В нашу компанию поступает множество обращений от пользователей о тех фактах, что им были присланы письма от людей, которых они хорошо знают, письма от клиентов или поставщиков, письма из банков, налоговых, судебных приставов и тому подобное, либо письма из неизвестных источников. И в этих письмах было либо вложение, которое являлось вирусом или вредоносным файлом, либо ссылка на вирусный сайт.

Хотим обратить ваше внимание на так называемый ”вирус-шифровальщик” или ”крипто-вирус”. Сам шифровальщик по сути не является вирусом, так что антивирусы идентифицировать его не могут. Как правило пользователи получают его по электронной почте во вложении и запускают самостоятельно.

Крипто вирус или шифровальщик делает зашифрованными любые файлы, хранящиеся на компьютере пользователя и на сетевых ресурсах. Целью вируса могут оказаться как личные файлы пользователей, как правило это файлы word, excel, пдф файлы, картинки, базы данных 1с, так и целые образы дисков, и резервные копии важной информации.

Самостоятельно восстановить зашифрованные файлы не представляется возможным. Вредоносный шифровальщик подвергает изменениям отдельный фрагмент файла. Затем происходит генерация уникального ключа, а потом ключ отправляется злоумышленникам.

Акцентируем внимание, что пользователь **самостоятельно запускает крипто-вирус шифровальщик**, открыв вложение в электронной почте. После чего запускается скрытый процесс, который шифрует файлы. Пользователь узнает о наличии вируса достаточно поздно, после того как перестают открываться файлы, то есть когда файлы уже зашифрованы.

Вредоносный код создает в папках текстовый документ, в котором говорится о возможности обратной дешифровки инфицированных файлов за отдельную плату. Если пользователь не изъявляет желания заплатить злоумышленникам за дешифрацию, то уникальный ключ удаляется, а зашифрованные файлы остаются недоступными навсегда. Эксперты «Лаборатории Касперского» отмечают, что зараженные файлы на данный момент не поддаются расшифровке.

Наша компания дает ряд рекомендаций как избежать заражения крипто вирусом:

1. Рассматривайте все деловые и личные письма, как потенциально опасные. Если возникают сомнения, удаляйте.

2. Поле «От кого» ничего не значит. Если у вашего знакомого вирус, то этот вирус может отправлять свои копии по все адресам, имеющимся в адресной книге.

3. Внимательно смотрите типы файлов во вложении, самые распространенные файлы пользователей: word - **.doc**, **.docx**; excel - **.xls**, **.xlsx**; пдф файлы -**.pdf**; картинки, фотографии - **.jpeg**, **.jpg**. **Им доверять можно**. Архивы имеют тип **.rar** и **.zip**. Так же внимательно смотрите типы файлов в архивах.

4. Если Вы все-таки открыли вложение, и ничего визуально не произошло, выключите компьютер и обратитесь в службу технической поддержки.

5. Будьте осторожны с письмами без текстового содержания, имеющими только ссылку или приложение во вложении.

6. Не нажимаете на ссылки или вложение, если они не ожидались вами от этого отправителя.

7. Если не уверены, то позвоните отправителю.

8. Храните информацию на сервере.