УДК 004.491.22 **Технические науки**

Бондаренко Е.С., *студентка 5 курса электротехнического факультета, Пермский национальный исследовательский политехнический университет*

ЭВОЛЮЦИЯ ВИРУСОВ-ШИФРОВАЛЬЩИКОВ

Аннотация. В статье рассматривается механизм работы вируса-шифровальщика. Также рассматривается принцип работы самого первого вируса-шифровальщика, а так же самого последнего на данный момент.

Ключевые слова: вирус-шифровальщик, вирус, пользователь, файл, электронный.

Abstract. This article describes principle of operation of cipher-virus. Also it describes the work of the first cipher-virus and the latest one presently existed.

Keywords: cipher-virus, virus, user, file, electronic.

Про существование вирусов-шифровальщиков известно уже давно и сейчас ими уже никого не удивишь. Они, по своей природе, являются подтипом так называемого вируса троянца, который под видом какого-либо файла проникает на компьютер. Однако, с каждым годом данный тип вируса становится все изощреннее и по-прежнему представляют угрозу для пользователей, а особенно, для сотрудников больших корпораций.

Под шифровальщиками (криптолокерами) подразумевается целое семейство вирусов, которые шифруют и блокируют доступ к файлам пользователя. Активно тема с данными вирусами поднялась год назад (лето 2014 года), хотя они существовали значительно раньше [1].

Как же вирус-шифровальщик может попасть на компьютер? Обычно это происходит так: на адрес электронной почты пользователя приходит письмо с каким либо вложением, чаще всего это картинка формата .jpg. В большинстве случаев целью вирусов-щифровальщиков оказываются большие корпорации. Один из возможных случаев: сотруднику компании на электронную почту приходит

подставное письмо, например, от недовольного клиента. Текст в письме направлен на то, чтобы вызвать желание у пользователя скачать присылаемый файл.

Вирус отправляет запрос на сервер злоумышленника. Происходит генерация уникального ключа, с помощью которого все файлы на компьютере жертвы шифруются. Ключ отсылается на сервер и хранится там. Вирус показывает пользователю окошко (либо меняет рабочий стол) с предупреждением и требованием выкупа. За расшифровку файлов потребуют определенное количество биткоинов (криптовалюта, использующаяся в интернете). При этом зашифрованные файлы невозможно открыть, сохранить, отредактировать, поскольку они наглухо зашифрованы стойким алгоритмом.

При этом есть некоторые нюансы. Некоторые шифровальщики вообще выбрасывают ключ, а потому, заплатив выкуп, пользователь все равно не расшифрует свои фото, видео и другие файлы.

Рассмотрим, что собой представлял первый вирус-шифровальщик. Во время его появления никто не думал, как можно вылечить или расшифровать файлы после воздействия исполняемого кода, который был заключен во вложении электронной почты. Первый вирус-шифровальщик имел название «I Love You». Пользователь, который ничего не подозревал, просто открывал вложение в письме, пришедшем по электронной почте и в результате получал полностью невоспроизводимые файлы мультимедиа (видео, графику и аудио). Такие действия выглядели более деструктивными, однако денег за расшифровку данных в то время никто не требовал [2].

Современные вирусы-шифровальщики стали намного изощреннее. Самый последний на данный момент вирус-шифровальщик, появившийся в июле 2016 года, имеет название «Satana» («Сатана»). Данный вирус способен зашифровать самые разнообразные файлы, а именно: с расширениями .bak, .doc, .jpg, .jpe, .txt, .tex, .dbf, .db, .xls, .cry, .xml, .vsd, .pdf, .csv, .bmp, .tif, .1cd, .tax, .gif, .gbr, .png, .mdb, .mdf, .sdf, .dwg, .dxf, .dgn, .stl, .gho, .v2i, .3ds, .ma, .ppt, .acc, .vpd, .odt, .ods, .rar, .zip, .7z, .cpp, .pas, .asm [3]. Однако, помимо шифрования, «Сатана» подменяет главную загрузочную запись Windows (Master Boot Record, MBR), отрезая жертве доступ к

операционной системе. Опытный эксперт, возможно, сможет восстановить работу операционной системы, однако расшифровать файлы не получится.

Подводя итог, важно отметить, что избежать воздействия вируса-шифровальщика вполне реально. Чтобы защититься, необходимо соблюдать следующие рекомендации:

1. *Обязательно установить антивирусную программу*. Так как исходный код более старых троянцев-шифровальщиков давно раскрыт, он содержится в базе даже бесплатных антивирусных программ типа Avast или Avira, и они могут защитить компьютер в 80% случаев.

2. *Обновлять браузер, использовать самую последнюю версию*. Вирусы часто используют уязвимости в браузере для заражения вашего компьютера. Обновления часто исправляют ошибки предыдущей версии браузера.

3. *Не запускать подозрительные файлы.* В 90% случаев шифровальщики отправляются жертвам в виде спама по электронной почте. Поэтому не открывайте письма от незнакомых адресатов и с подозрительным содержанием.

4. *Регулярно сохранять важную информацию (backup)*. Желательно периодически делать резервную копию ваших файлов и хранить ее, например, на переносном жестком диске.

Библиографический список

1. Официальный сайт организации Центр продающих текстов Text-info – [Электронный ресурс]. – URL: http://text-info.com/blog/virusy-shifrovalshhiki-ugroza-dlya-biznesa (дата обращения 21.08.2016).

2. Информационный портал Компьютерология – [Электронный ресурс]. – URL: http://computerologia.ru/13319-2/ (дата обращения 21.08.2016).

3. Информационный портал АО «Лаборатория Касперского» – [Электронный ресурс]. – URL: https://blog.kaspersky.ru/satana-ransomware/12442/ (дата обращения 20.08.2016).