FOREIGN EXPERIENCE OF STATE SUPPORT OF SMALL AND MEDIUM-SIZED BUSINESSES AND THE POSSIBILITY OF ITS USEING IN RUSSIA

Makuhina M.N., Averchenkova E.E.

Keywords: *credit market, industrial diversification, import substitution, innovative system.*

The article is dedicated to the foreign experience of state support of small and medium-sized businesses and the possibility of its use in Russia. Particular attention is paid to the lending market, stimulate the development of the state program of industrial diversification and import substitution. It was determined the improving direction of Russian innovation system.

УДК 004.056.57

ВИРУС VAULT

Малькова А.А., студентка 4 курса экономического факультета
Научный руководитель – Голубев С.В.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновская ГСХА

Ключевые слова: *спам, вирус, фишинговые письма, Locker, шифрование.*

В статье рассмотрены вирусы группы Locker и методы борьбы с ними.

В настоящее время распространяется множество вымогательских программ, например, хорошо известные Cryptolocker, CTB locker, Cryptobot, Cryptographic Locker и т.п. Все они используют одинаковую технику распространения, используемую множеством других вирусов, таких как ложные антишпионские программы, троянские программы и др.

Прежде всего, необходимо запомнить следующее: такое ПО активно продвигается при помощи спама. Спам – это надоедливые сообщения электронной почты, сопровождаемые зараженными прикрепленными файлами или вредоносными ссылками. Стремясь вынудить пользователей щелкнуть по таким ссылкам или скачать вредоносные прикрепления, сообщения уведомляют об интригующих вещах, таких

как недостающие платежи, предупреждения от правительственных органов и подобные выдумки, которые обычно не оставляют людей равнодушными.

Locker virus (также может быть обнаружен как Locker v1.7, Locker V2.16, Locker v2.60, Locker v3.5.3, Locker v.3.49 и Locker V5.52) – это по-настоящему опасная киберугроза, действующая в соответствии со своим наименованием. Как только указанное приложение проникает в целевой компьютер, оно выискивает в системе определенные файлы и «закрывает» доступ к ним. Вдобавок, если попытаться открыть любой из таких файлов, можно увидеть сообщение, предлагающее сделать платеж в обмен на ключ расшифровки. Обычно это нужно для разблокирования нужных Вам файлов и восстановления доступа к ним. Прежде, чем потребовать выкуп, Locker перешифровывает все самые частоиспользуемые файлы:

.doc, .docm, .docx, ., .jpg, . odt, . ppt, . psd, . ptx, . raw.

Данная киберугроза легко может привести Вас к потере всех фотографий, музыкальных файлов, файлов с результатами Вашей творческой деятельности, а также других документов.

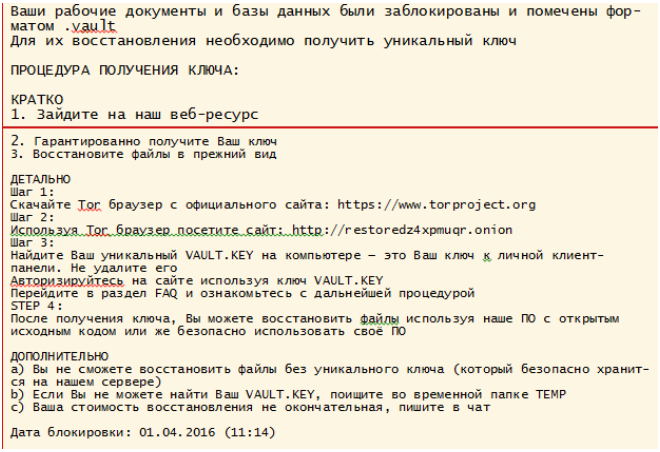
Прежде всего, нужно удалить Locker virus из системы до того, как он сможет перешифровать слишком большое количество файлов. Вдобавок поискать копии заблокированных файлов. Если Вы не делали резервного копирования, можно попытаться воспользоваться следующими средствами: R-Studio, Photorec, кроме того следует попробовать Kaspesky Ransomware Decryptor. Если даже указанные программы не смогли помочь, это значит, что зашифрованные файлы, к сожалению, утрачены навсегда.

Для удаления Locker virus рекомендуют программу SpyHunter, а также STOPzilla, Malwarebytes Anti Malware.

Модифицированный вирус из семейства FileCoder и вымогателя Win32/Virlock – это вирус-вымогатель, который размножается через почту в виде вложения архива. Основной способ распространения вымогателя CTB-Locker – это фишинговые письма по электронной почте. Современными антивирусы, к примеру, ESET ловит его как Win32/TrojanDownloader.Elenoocka.A. Файл является загрузчиком на компьютер жертвы вируса FileCoder (CTB-Locker), который обнаруживается как Win32/FileCoder.DA. После загрузки локера файлы на диске зашифровываются. Шифровальщик CTB-locker аналогичен известному вирусу CryptoLocker, но отличается алгоритмами шифрования. Шифрование проходит тихо и без симптомов, пока по окончанию, скрипт не подменит заставку на рабочем столе на bmp картинку.

Регулярное обновление антивирусных баз, является главной мерой для предотвращения заражения. Если произошло заражения и вымогания денег – нельзя платить мошенникам, хотя бы потому, что Ваши данные никто Вам не вернет.

Если у вас внезапно открывается текстовый файл в блокноте следующего содержания, значит, вы столкнулись с вирусом шифровальщика vault:



Появление такого сообщения уже означает, что Vault вирус заразил ваш компьютер и начал шифрование файлов. В этот момент необходимо сразу же выключить компьютер, отключить его от сети и вынуть все сменные носители.

К стандартному имени файла прибавляется новое расширение .vault. Простое переименовывание файла обратно тут не помогает. Получается, что исходный файл не удаляется, а перезаписывается зашифрованным документом. После этого его невозможно восстановить стандартными средствами по восстановлению удаленных файлов.

После обнаружения вируса шифровальщика первым делом необходимо от него избавиться, проведя лечение компьютера. Лучше всего загрузиться с какого-нибудь загрузочного диска и вручную очистить систему. После удаления надо почистить автозагрузку, чтобы не было ссылок на удаленные файлы и ошибок при запуске.

Если у вас включена защита системы, то вы можете воспользоваться инструментом восстановления предыдущих версий файлов и папок.

Стандартные рекомендации, которые актуальны для любых вирусов в интернете:

Не запускайте незнакомые приложения, ни в почте, ни скачанные из интернета. Старайтесь вообще из интернета ничего не качать и не запускать. Попросите лучше компетентного знакомого вам что-то найти в интернете.

Всегда имейте резервную копию важных данных. Причем хранить ее нужно отключенной от компьютера или сети. Храните отдельную флешку или внешний жесткий диск для архивных копий. Подключайте их раз в неделю к компьютеру, копируйте файлы, отключайте и больше не пользуйтесь. Для повседневных нужд приобретайте отдельные устройства. Лучше купить дополнительную флешку, чем потерять важные данные.

Повысьте меру своего понимания происходящих в компьютере процессах. Никакой антивирус и специалист не сможет защитить ваши данные, если вы сами не научитесь это делать. Уделите время, почитайте тематические статьи на тему информационной безопасности, сходите на соответствующие курсы, повысьте свою компьютерную грамотность. Это в современной жизни обязательно пригодится.

Библиографический список:

1. Денисов, Т.В. Антивирусная защита / Т.В. Денисов // Мой Компьютер. – 2014. – № 4. – С. 28 – 32.

2. Мостовой, Д.Ю. Современные технологии борьбы с вирусами / Д.Ю. Мостовой // Мир ПК. – 2013. – № 8. – С. 43 – 47.

3. Файтс, Ф. Компьютерный вирус: проблемы и прогноз / Ф. Файтс, П. Джонстон, М. Кратц. – М.: Мир. – 2013. – 53 с.

VIRUS VAULT

Malkova A.A., Golubev S.V.

Key words: *spam, virus, phishing emails, Locker, encryption.*

The article deals with viruses Group Locker and methods to combat them.

УДК 338.242

МЕХАНИЗМ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ СЕЛЬСКОХОЗЯЙСТВЕННЫХ ПРЕДПРИЯТИЙ В УЛЬЯНОВСКОЙ ОБЛАСТИ

Малькова А.А., студентка 4 курса экономического факультета
Научный руководитель – Нейф Н.М.,
кандидат экономических наук, доцент