НАША ГАЗЕТА
nashagazeta.ch
Опубликовано на Швейцария: новости на русском языке (https://nashagazeta.ch)

В Швейцарии действует новый вирус-вымогатель | En Suisse, un nouveau rançongiciel

Auteur: Лейла Бабаева, Женева/Берн , 12.08.2014.

Текст на мониторе сообщает о том, сколько времени отпущено на оплату ключа расшифровки, и о том, что по истечении срока требуемая сумма удвоится (tdg.ch)
Швейцарцы становятся жертвами компьютерного вируса, шифрующего файлы, за расшифровку которых нужно заплатить.
|
De plus en plus de Suisses sont victimes d’un nouveau virus qui chiffre les fichiers éléctroniques dont le déchiffrage doit être payé.
En Suisse, un nouveau rançongiciel

SynoLocker TM – такое нестрашное имя носит, в общем-то, мирный вирус. Он не

стирает информацию, не выдает бесполезные рекламные сообщения, а просто… шифрует файлы 2048-битным кодом, который сегодня считается не поддающимся взлому. Чтобы расшифровать файлы, достаточно ввести специальный ключ, который можно купить у создателей вируса. Где же их искать, спросит читатель? С этим как раз проблем нет: у авторов есть сайт, на котором можно пообщаться с ними в чате. Они вежливо ответят на все относящиеся к делу вопросы, так что у обратившегося к ним – клиента? пострадавшего? – не останется сомнений в порядке оплаты.

При этом вирус страшен лишь тем, кто использует сетевые хранилища известной тайваньской корпорации Synology Inc., и особенно тем, кто давно купил свое устройство и не обновил старую версию установленной на нем управляющей системы DiskStation Manager до самой последней (так как старые версии содержат некоторые ошибки, исправленные в более поздних версиях). Если представить, что SynoLocker внедрился в системное хранилище консалтинговой фирмы, которая хранит там ценнейшие документы, то можно понять чувства бизнесменов, у которых застопорится работа до того момента, как они избавятся от новой электронной напасти.

В интервью газете Tribune de Genève программист Робер Ипполит, который работает в этой сфере уже тридцать лет, признался, что ему пришлось заплатить от имени одного из своих клиентов, чтобы получить ключ расшифровки.

По информации женевской полиции, в неделю вирус поражает устройства 5-10 пользователей, а из тридцати клиентов Робера в сети хакеров попались двое. Программист был вынужден заплатить на этой неделе требуемую пиратами сумму в ночь со вторника на среду, так как один из пострадавших хотел немедленного решения проблемы.

Робер рассказал о пережитых перипетиях: «Первая трудность состояла в том, что пираты требовали оплату в электронной валюте bitcoin (биткоин), а ее быстро не достанешь: нужно открывать счет, переводить на него деньги… Чтобы сэкономить время, я отправился к биткоин-банкомату в Паки». На первый взгляд, злоумышленники хотели получить немного – всего 0,6 биткоина. Но если знать, что эта сумма соответствует приблизительно 650 франкам (курс переменчив в зависимости от страны, в которой совершается операция), то мысль о благородстве вымогателей растает сама собой.

После оплаты компьютерщик ввел полученный ключ, но система клиента отреагировала на вирус (еще до введения ключа) неожиданным образом, и расшифрованные файлы, которые сохранили свои прежние имена, стало невозможно использовать. По этой причине пришлось переустанавливать систему, а после заново установить вирус, чтобы еще раз проделать операцию расшифровки.

Благодаря такому приключению Робер узнал, как можно «собственными руками» установить вирус в компьютер. «На сайте хакеров есть вкладка «поддержка», где можно пообщаться с авторами в чате». Написав туда, он получил очень вежливый ответ: «Уважаемый посетитель, мы приняли к сведению вашу проблему…», а через час ему прислали описание необходимых действий.

Интересно, что при наличии резервной копии на внешнем жестком диске или сервере можно было не платить пиратам ни сантима (ни биткоина, в данном случае), а просто взять нужные данные из безопасного места. Робер советует клиентам покупать хотя

бы внешние жесткие диски, но, «как только речь заходит о приобретении дополнительного оборудования, всем начинает казаться, что им пытаются продать бесполезные продукты или услуги. Только те, кто пережил вирусную атаку, думают иначе…»

Что же до Synology, то ее продажи поначалу снизились из-за программы-вымогателя, но «потом ситуация нормализовалась». На сайте французского отделения Synology упоминается описанный нами вирус и даются ссылки как для скачивания последней версии системы DiskStation Manager, так и для получения технической помощи в случае заражения вирусом.

Поддержка пришла и со стороны швейцарских властей: в четверг на сайте Конфедерации появилось сообщение с рекомендациями по борьбе с SynoLocker и ссылкой на бесплатный онлайн-сервис, который позволяет справиться с подобным вирусом – Cryptolocker.

программисты в швейцарии
Статьи по теме
Кибершпионы «Красного октября» проникли в посольства в Швейцарии
Бум киберпреступности в Швейцарии

Source URL:
http://www.nashagazeta.ch/news/la-vie-en-suisse/v-shveycarii-deystvuet-novyy-virus-vymogatel