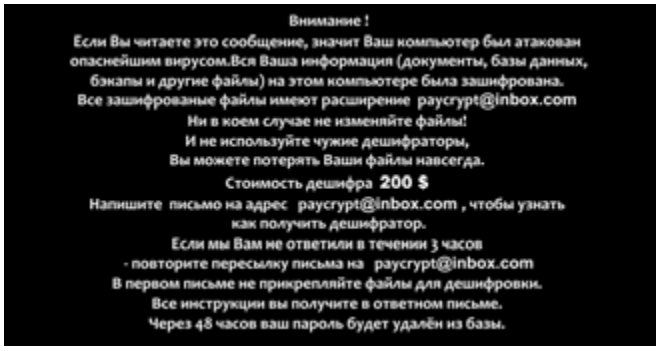
Визитка

ВЛАДИМИР МАРТЬЯНОВ,
инженер – вирусный аналитик, компания "Доктор Веб"

Если к вам пришел...

Предположим, вы (или сотрудник вашей компании) увидели на экране требование выкупа за возврат в целости и сохранности данных, зашифрованных троянцем-шифровальщиком (энкодером). Что делать?



Главная задача – сохранить как можно больше файлов незашифрованными.

Если вы заметили, что файлы начали шифроваться только что или совсем недавно – выдергивайте провод питания из зараженного компьютера!

Да, совет вызывает обоснованные опасения по поводу потери данных на диске. Но вы и так их теряете каждую секунду раздумий – троянец, вполне возможно, все еще продолжает шифровать ваши файлы. Ни один энкодер не способен зашифровать все данные мгновенно, поэтому до окончания шифрования какая-то их часть остается нетронутой. И чем больше времени прошло с начала шифрования, тем меньше нетронутых данных остается. Раз наша задача сохранить как можно большее их количество, нужно прекратить работу энкодера. Можно, в принципе, начать анализировать список процессов, искать, где в них троянец, пытаться его завершить… Но выдернутый шнур питания – это гораздо быстрее! Штатное завершение работы операционной системы не только занимает некоторое время. Троянец вполне может ему препятствовать или даже имитировать выключение устройства с целью продолжения работы.

Естественно, дамп оперативной памяти, снятый в момент работы троянца, может очень сильно помочь в целях расшифровки, но простой пользователь наверняка не знает как его сделать, и на поиски способов или действующей в компании инструкции уйдет много драгоценного времени.

Естественно, есть риск - вероятность повреждения файловой системы и невозможность дальнейшего снятия дампа ОЗУ. Поврежденная файловая система для неподготовленного человека – проблема посерьезнее, чем энкодер. После энкодера остаются хотя бы файлы, повреждение же таблицы разделов приведет к невозможности загрузки ОС. С другой стороны, грамотный специалист по восстановлению данных ту же таблицу разделов починит без особых проблем, а энкодер до многих файлов может просто не успеть добраться.

И еще один плюс подобного подхода. Все, наверно, смотрели детективы и видели, как происходит идеальный обыск. Место преступления должно быть зафиксировано в состоянии, максимально близком к моменту совершения преступления. Однако завершение работы операционной системы вполне может изменить ее состояние.

Вторая задача – сохранение «места происшествия» для дальнейшего изучения.

Почему это так важно? Любая работа по расшифровке файлов начинается с того, что вирусные аналитики пытаются понять, что же именно произошло, получить полную картину произошедшего.

Внимание! В идеале для анализа желательно получить все файлы, которые запускались в процессе шифрования. Их анализ позволяет понять, как происходило шифрование, оставлял ли троян артефакты, которые позволят упростить расшифровку. Возможно, анализ запускавшихся файлов поможет и с анализом причин заражения.

Идеальный способ законсервировать практически все что нужно – опять-таки выключить питание и не загружать ОС, в которой был запущен энкодер. Для доступа к данным с диска (а такой доступ точно потребуется) можно использовать LiveCD/LiveUSB – например Dr.Web LiveDisk. Можно также подключить диск к не пораженному ПК, но так есть риск запуска энкодера в новой системе или же изменения файлов на пораженных дисках. Поэтому лучше LiveCD/LiveUSB.

Внимание! Описанный выше вариант действий неприемлем, если вы собираетесь провести полноценное расследование инцидента. Чтобы «место преступления» было принято

в качестве доказательства или улики, необходима сохранность его состояния на момент инцидента. Однако любой запуск с LiveCD/LiveUSB (если, естественно, это не специальный LiveCD/LiveUSB, используемый для целей расследования) может изменить временные метки файлов – и этот факт позволит адвокату отвести ваши доказательства. То же самое произойдет и если вы подключили диск к иному компьютеру.

На этом этапе мы имеем, в идеале, компьютер, который был обесточен сразу после обнаружения шифрования и ни разу с этого момента не включался. На практике такого почти не бывает: я не могу вспомнить ни одного такого случая из более чем девяти тысяч. Скорее всего, в вашем случае шифрование уже завершилось, а выключить машину надолго не выйдет по тем или иным причинам. И тут важно понимать, как нужно (а точнее, как не нужно) работать с такой «недоконсервированной» системой, принимая во внимание задачи «максимального сохранения».

Первое правило: не паниковать.

Еще раз убедитесь, что шифрование новых файлов не происходит, в противном случае обесточьте машину. Необдуманные и поспешные действия после окончания шифрования могут привести (и не раз приводили!) к большим проблемам, нежели само шифрование. На данный момент все самое плохое уже произошло и нужно спокойно решать проблему.

Внимание! Запуск антивирусного сканера (в том числе с LiveCD/LiveUSB) после обнаружения шифровальщика, вполне возможно, уничтожит следы заражения, что также снизит возможность поиска решения проблемы.

Второе правило: ничего не чистить, не удалять, систему не переустанавливать.

Для расшифровки наибольшее значение может иметь неприметный файлик на 40 байт во временном каталоге или непонятный ярлык на рабочем столе. Вы наверняка не знаете, будут ли они важны для расшифровки или нет, поэтому лучше не трогайте ничего. Чистка реестра – вообще сомнительная процедура, а некоторые энкодеры оставляют там важные для расшифровки следы работы. Антивирусы, конечно, могут найти тело троянца-энкодера. И даже могут его удалить раз и навсегда, но что тогда останется для анализа? Как мы поймем, как и чем шифровались файлы? Поэтому лучше оставьте зверька на диске. Еще один важный момент: я не знаю ни одного средства для чистки системы, которое бы принимало в расчет возможность работы энкодера и сохраняло бы все следы его работы. И, скорее всего, такие средства не появятся. Переустановка системы точно уничтожит все следы троянца, кроме зашифрованных файлов.

Третье правило: оставьте расшифровку профессионалам.

Если у вас за плечами пара лет написания программ, вы действительно понимаете что такое RC4, AES, RSA и в чем между ними различие, знаете, что такое Hiew и что означает 0xDEADC0DE – можете попробовать. Остальным не советую. Допустим, вы нашли какую-то чудо-методику расшифровки файлов и у вас даже получилось расшифровать один файл. Это не гарантирует, что методика сработает на всех ваших файлах. Более того, это не гарантирует, что по этой методике вы файлы не испортите еще сильнее. Даже в нашей работе бывают неприятные моменты, когда в коде расшифровки обнаруживаются серьезные ошибки, но в тысячах случаев до этого момента код работал как надо.

Внимание! Помните, что время – это деньги. Известен случай шифрования даже главного сервера банка – после обнаружения факта инцидента у вас будет на счету каждая минута. Срочный поиск всего необходимого уже после обнаружения того же шифровальщика – плохая практика. ДО этого момента у вас (и у дежурной смены) должны быть все необходимые контакты.

Четвертое правило: для расшифровки нужны данные.

Внимание! И снова: время – это деньги. Как ни странно, пострадавшие от действия шифровальщиков пишут куда угодно – на самые разные форумы. Я, например, видел запрос на Япе. Но даже если сразу идет обращение в трекер антивирусной компании, как правило, сотрудникам техподдержки сначала приходится выяснять ситуацию.

Говорят, продвинутые астрологи лечат болезни по одной фотографии. К сожалению, вирусные аналитики пока так не умеют. Поэтому огромная просьба: если вы хотите победить злоумышленников – давайте нам максимум информации.

Прикрепите к комментарию в запросе несколько (трипять. Не менее!) зашифрованных файлов (по возможности, разных типов и размеров: doc (в первую очередь), pdf, jpg, zip и т.п.), если есть возможность – сам вредоносный файл, а также требования злоумышленников о перечислении денежных средств. Опишите, если известно как происходил процесс заражения (укажите сайт, с которого был загружен троян или приложите письмо, в результате получения которого все и произошло). Пересылаемое письмо должно содержать служебные заголовки, простая пересылка недопустима. Крайне желательно пересылать письмо в формате EML.

Внимание! Всё пересылаемое обязательно помещать в архив с паролем!

Теперь, когда понятно, что делать и чего не делать, можно приступать к расшифровке. В теории расшифровка возможна почти всегда. Это если знать все нужные для нее данные или же обладать неограниченным количеством денег, времени и процессорных ядер. На практике что-то можно будет расшифровать почти сразу. Что-то будет ждать своей очереди пару месяцев или даже лет. За какие-то случаи можно даже и не браться: суперкомпьютер даром на 5 лет в аренду никто не даст. Плохо еще и то, что кажущийся простым случай при детальном рассмотрении оказывается крайне сложным. К кому обращаться – вам решать. Можете обратиться к нам, можете к злоумышленникам, требующим выкуп, а можете – к безвестному соседу, который говорит, что все вернет как было за 5 минут. У нас есть многолетний опыт в расшифровке данных, наша компания имеет софт для расшифровки файлов после более чем тысячи различных вариантов энкодеров и мы создаем его для новых версий шифровальщиков.

Пятое правило: пострадали – примите меры!

Как ни странно, нередки ситуации, когда вслед за первым случаем заражения идут последующие. При этом вполне возможно, если в первом случае расшифровка была успешной, то в остальных так уже не повезет.

Поэтому: итогом обработки инцидента должен стать анализ причин заражения и усовершенствование системы защиты.

В любом случае, успехов в восстановлении данных и как можно реже сталкиваться с энкодерами!

Источник полезных сведений: http://legal.drweb.ru/encoder. ADV