Dr.WEB®
с 1992 года

Троянцы-шифровальщики

Эпидемия с 2006 года

Dr.WEB®
с 1992 года

Содержание

Что такое и зачем

Сейчас, когда эпидемия троянцев-шифровальщиков (Trojan.Encoder; в просторечии — энкодер, шифровальщик) длится уже несколько лет и, к сожалению, не думает идти на спад, о вредоносных программах этого семейства наслышаны многие. В том числе те, кто далек от компьютерной тематики вообще и от вопросов информационной безопасности в частности. Некоторые и вовсе столкнулись с шифровальщиками на собственном опыте. И речь идет не только и не столько о троянце WannaCry, наделавшем много шума по всему миру в мае 2017 года, сколько о тысячах других троянцев, портящих данные и нервы миллионам людей.

Первый вирусный инцидент с троянцами семейства Trojan.Encoder был зафиксирован в мае 2005 года. Но простой алгоритм шифрования не сделал его особо эффективным — поврежденные троянцем файлы без особого труда лечились антивирусной программой. Не вызвал он особого ажиотажа и в среде злоумышленников — до лета 2007 года в вирусной базе Dr.Web было менее 10 записей для энкодеров. И все они также не требовали к себе какого-то «особого» отношения — зашифрованные файлы восстанавливались непосредственно антивирусом, без привлечения дополнительных утилит.

- 2005 год — первый инцидент
- 2007 год — в базе Dr.Web только 10 записей о шифровальщиках
- 2017 год — глобальная эпидемия WannaCry (Trojan.Encoder.11432)

Вплоть до 2009 года появление различных вариаций было, скорее, «пробой пера» злоумышленников, постоянно находившихся в поиске новых методов атак на ПК и сети. В самом деле, создать серьезный шифровальщик, результаты деятельности которого не будут дешифроваться «на лету» или за очень короткий срок, — задача нетривиальная. А для вирусописателей-одиночек, на которых до недавнего времени держался мир вредоносного ПО, — просто непосильная. Ведь троянец-шифровальщик, как и следует из названия, кодирует файлы, а значит, именно навыки криптографии нужны его создателю в первую очередь.

Также стоит отметить ключевое отличие троянцев от компьютерных вирусов. Первые — самостоятельные приложения, а не «паразиты», цепляющиеся к файлам. Это определяет и ключевой момент в поведении антивируса и пользователя в отношении троянца. В то время как от вируса зараженный файл можно избавить, получив «чистую» версию оригинала, троянца вылечить невозможно, ибо он сам по себе является вредоносным файлом. Даже если это легитимное приложение с «теневым» функционалом, оно все равно цельное, устранить его негативный эффект можно только полным удалением.

Выглядит сообщение шифровальщика примерно так

Клин клином

Возможно, мы бы стали свидетелями бурного роста числа энкодеров еще в 2010–2011 годах, если бы не набравшие тогда огромную популярность троянцы семейства Trojan.WinLock.

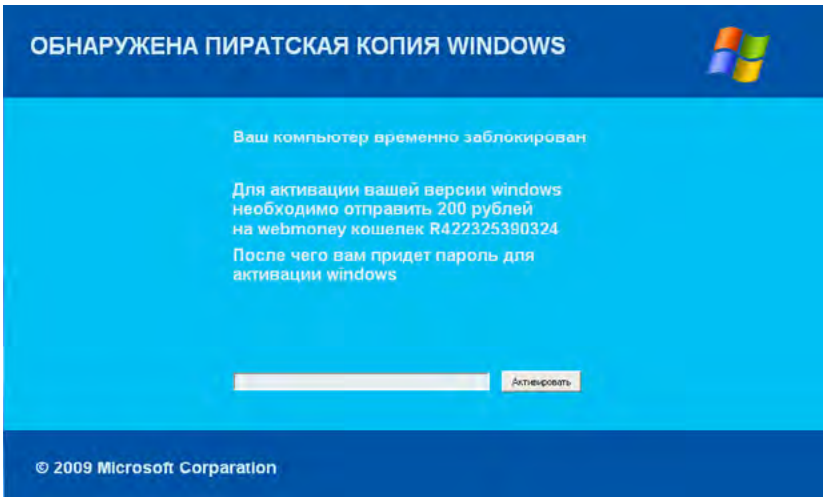
Хоть они и были просты в обнаружении и лечении, а справиться с ними даже безо всякого антивируса мог любой квалифицированный специалист или админ, это не спасло мир от эпидемии.

Сервис компании «Доктор Веб» для разблокировки Windows самим пользователем

https://www.drweb.com/xperf/unlocker

И в первую очередь она была связана с простотой самих «локеров», которые можно было писать «на коленке» хоть по пачке в неделю (существовали даже специальные «генераторы» этих троянцев), а значит, и с обилием жертв, так или иначе сталкивающихся с блокировкой Windows, — у себя, близких или на работе.

Можно предположить, что именно этот «вал» блокировщиков Windows и отсрочил развитие энкодеров как более сложной технологии, прибыль от использования которой на тот момент еще не была оценена.



Типичный WinLock

Стенка на стенку

Но, разумеется, такая «благодатная» для злоумышленников технология не могла остаться невостребованной на рынке кибермошенничества. Совершенствовались антивирусные системы, развивались и злоумышленники, объединяясь в преступные сообщества, привлекая на свою сторону все больше квалифицированных специалистов по криптографии, социальной инженерии и прочим направлениям, без которых сами по себе шифровальщики не могли представлять серьезную угрозу.

Итак, давайте посмотрим: сколько нужно злоумышленников, чтобы с нуля создать и распространить «эффективного» шифровальщика?

Первое, что необходимо сделать, — написать троянца. Во-первых, для этого потребуется специ-

алист по криптографии, который воплотит в коде определенный алгоритм шифрования. Во-вторых, если криптограф не силен в стелс-технологиях, нужен еще один программист, который будет обеспечивать скрытность действий энкодера в системе. Ему же стоит позаботиться о том, чтобы троянец не обнаруживался известными антивирусами. Иногда для этого даже нанимают тестировщика (уже третий член команды). Если планируется использование уязвимостей или прочие сложные сетевые «фокусы», то не обойтись еще и без специалиста по сетевым технологиям.

Итак, троянца написали и протестировали на антивирусах, с этим порядок. Теперь его надо распространить — ведь он не вирус, и сам размножаться не умеет. Тут потребуется еще больше народу. Во-первых, специалист по социальной инженерии, который придумает содержание спам-писем и сформулирует задание на разработку фишинговых сайтов. Это необходимо для того, чтобы максимальное число пользователей перешло по ссылке в письме, сохранило и запустило вложение или «купилось» на фишинговый сайт. Во-вторых, веб-дизайнер, который разработает упомянутый сайт. В-третьих, спамер, в идеале — с обширными базами для рассылки, лучше всего — четко таргетированными (база компаний, база физлиц в определенном регионе и т. д.). В-четвертых, специалист по «сокрытию улик», чья основная задача состоит в сохранении анонимности и скрытности действий всех участников преступного сообщества. И сюда же условно можно причислить «вольных художников» из мира киберкриминала — различных исследователей уязвимостей, которые ищут «дыры» в ОС и приложениях, после чего продают эту информацию разработчикам вредоносного ПО.

Конечно, зачастую услуги каждого из этих «специалистов» могут быть просто оплачены отдельно — например, куплена краденая база данных адресов и заказана спам-рассылка по ней, а один программист может применять знания из нескольких нужных областей. Кроме того, можно «расковырять» уже существующего троянца и, модифицировав его, распространить как нового. Для совсем ленивых есть вариант покупки на черном рынке готовой к распространению версии шифровальщика, которую достаточно настроить под свои реквизиты и выпустить в сеть, а то и вовсе купить доступ к «вредоносному облаку» с настроенной админ-панелью по принципу SAAS. Вариантов много, но, как показывает практика, самые удачные для злоумышленников атаки проводились именно с помощью новых уникальных троянцев с продуманной стратегией распространения.
А значит — это был результат работы целой группы квалифицированных специалистов, направивших свои знания отнюдь не на благое дело.

Кто же противостоит этой армии? Разумеется, в первую очередь это специалисты антивирусных компаний: вирусные аналитики, специалисты по криптографии (которые заняты тем, что взламывают шифры ребят из стана злоумышленников), эксперты по защите информации, борьбе со спамом и многие другие. Ведь если задача злоумышленников — создать один или несколько вредоносных файлов, то цель разработчиков антивирусного продукта — максимально защитить каждого пользователя от любых киберугроз. От домашнего пользователя с ПК или смартфоном до крупного корпоративного клиента с тысячей физических серверов самого разного функционала — всему должна быть обеспечена безопасность на высшем уровне. И чтобы защитить весь этот спектр устройств, сети, трафик, рабочие станции, почтовые серверы, шлюзы, нужна масса специалистов высочайшего класса. Именно такие люди и работают в компании «Доктор Веб», что дает нам возможность достойно отвечать на возникающие угрозы для пользователей.

У нас эпидемия!

Злоумышленники достаточно долго не могли «распробовать» шифровальщиков как инструмент вымогательства денег у домашних и корпоративных пользователей, но когда вошли во вкус, процесс пошел живее. С 2012 года число выявляемых шифровальщиков начало довольно быстро расти. Одновременно с этим стали совершенствоваться и методы использования различных алгоритмов шифрования.

Как говорилось выше, для работы с первыми шифровальщиками не требовались дополнительные инструменты, но для борьбы с образцами 2012 года такой номер уже не проходил. Наиболее популярные энкодеры того времени — Trojan.Encoder.94/102 и их модификации. В первом случае данные шифровались относительно простым симметричным алгоритмом, а вот 102-й не кодировал, а, скорее, ломал данные, отчего полноценная расшифровка оказывалась невозможна. Но некоторые типы файлов удавалось восстановить с помощью созданной специалистами компании «Доктор Веб» утилиты.

В том же году энкодеры были переведены в отдельное направление исследований, начался активный сбор вредоносных образцов и ключей к ним. Тогда же компания «Доктор Веб» начала первой в мире предоставлять услуги по восстановлению зашифрованной информации. Любой пострадавший от действия энкодеров мог обратиться в службу технической поддержки «Доктор Веб» и бесплатно получить помощь в восстановлении своих данных. При этом обратившийся возвращал себе ценную информацию, если это было возможно, а специалисты компании получали бесценный и эксклюзивный опыт по работе с новейшими модификациями и новыми представителями «шифровального семейства».

Но если в 2012 году связанные с шифровальщиками инциденты были просто «одной из угроз», то уже в 2013 году стало ясно, что «за шифровальщиками будущее» — столь быстрым стал рост числа обращений и количества новых модификаций.

С 2015 года порядка 50% (!!!)

запросов в службу технической поддержки «Доктор Веб» это просьбы о расшифровке.

2016 год — 42 276 обращений

8 месяцев 2017 — 19 698 обращений

Речь идет не о половине вирусных инцидентов, а о половине ВСЕХ обращений, включая вопросы по настройке антивируса, приобретению и т. д.

Почтовые ящики, дружественные зомби и задние двери

Троянцы (а большинство шифровальщиков относятся именно к этому типу вредоносных программ) отличаются от других типов вредоносных программ тем, что они не могут активизироваться сами, их кто-то должен загрузить и запустить — сам пользователь, кликнув по ссылке в почтовом сообщении или скачав и запустив «очень нужную» программу; злоумышленник, проникший на компьютер с помощью подбора пароля; иная вредоносная программа (например, типа Trojan.Downloader).

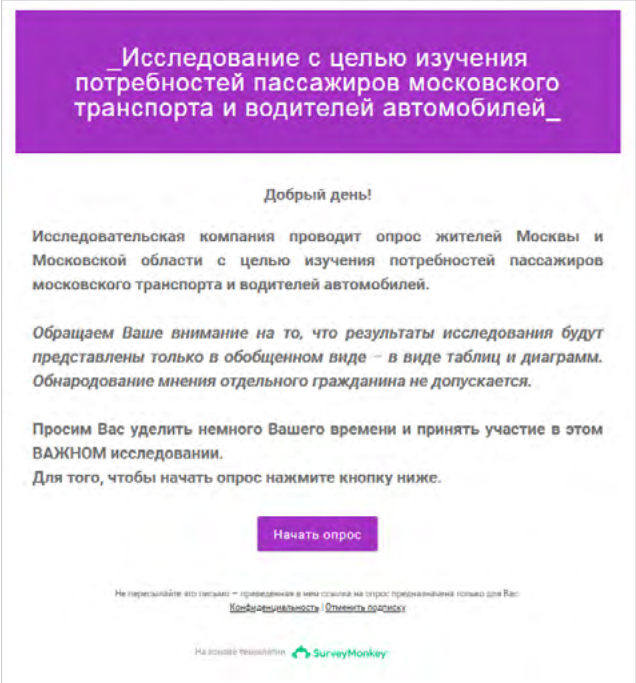
В 90% (!!!) случаев заражения сами пользователи активировали троянца у себя на ПК.

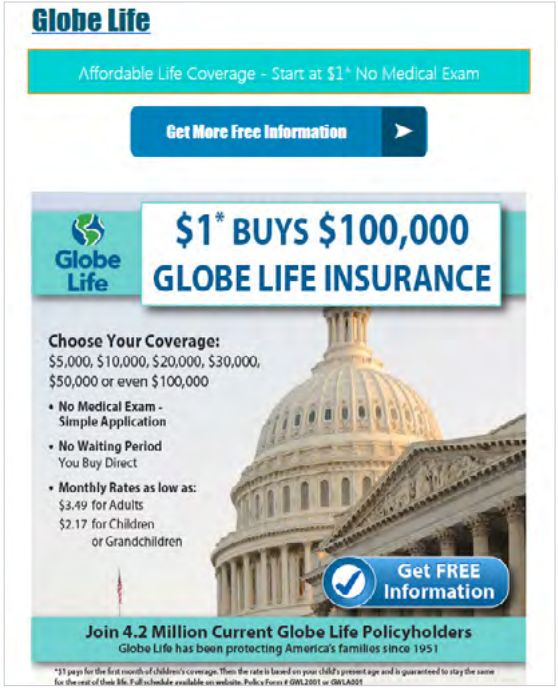
Все остальное — это более-менее резонансные эпидемии, организованные гибридными троянцами, в состав которых входили сетевые черви и прочие дополнительные компоненты, позволяющие организовать автоматическое распространение и запуск шифровальщика.

Говорить о том, что не стоит запускать подозрительные файлы и «бродить» по злачным сайтам, можно долго, да и сказано все это уже много раз и на разные лады. Поэтому лучше отдельно напомним о том:

Как именно троянец может попасть к вам на ПК и почему у вас может возникнуть желание запустить его

Почта. При отсутствии эффективного спам-фильтра в вашу почту будет сыпаться немыслимое количество самых разнообразных спамовых писем. Да, большая часть из них будет просто неуместной и навязчивой рекламой, но некоторые могут оказаться весьма «интересными». Сообщения о сборах на лечение больных детей, к которым приложены «подтверждающие медицинские документы», уведомления из налоговой инспекции с требованиями оплатить налог, прочитать приложенную повестку в суд или срочно оплатить приложенный счет за услуги связи — самые частые уловки злоумышленников. Что интересно, зачастую в поле «От» у этих писем стоят реальные адреса налоговой инспекции или иной известной организации — причем с указанием действующих сотрудников, возможно, известных получателю. Изначальный «кредит доверия» этим компаниям вкупе с низкой осведомленностью подавляющего большинства офисных сотрудников о киберугрозах делает такие атаки весьма эффективными — не каждый знает, что содержимое поля «От» ничего не значит и там можно указать произвольный текст.





Приложенные к таким письмам «документы» и оказываются этими самыми троянцами, которых пользователь запускает при открытии архивов. Важно, что хотя для человека такие «письма счастья» выглядят весьма серьезно, спам-фильтр вряд ли пропустит их, а почтовый антивирус сможет обезвредить известные ему угрозы, тем самым избавив пользователя от риска попасться на удочку злоумышленников.

1. **Вредоносные сайты.** Тут есть два варианта. В первом случае пользователь, скачивая приложения или другие файлы с фишинговых, взломанных или просто никем не контролируемых ресурсов (файлообменники, торренты и т. д.), сам запускает их, даже не подозревая, что вместе с полезным материалом получил вредоносный «довесок».
   Второй вариант развития событий еще хуже: достаточно бывает просто зайти на зараженный сайт, чтобы запустившийся скрипт загрузил на ПК троянца и активизировал его.
   К счастью, это возможно только при совершенно «небезопасных» настройках браузера и операционной системы. К несчастью, именно такие настройки и имеет большинство пользователей...
2. **Сменные носители информации.** Это основной путь заражения компьютеров, либо вообще не имеющих сетевых подключений, либо являющихся частью небольших локальных сетей без выхода в Интернет.
   Если сменный носитель, будь то флешка или съемный жесткий диск, заражен, а на компьютере не отключена функция автозапуска и нет антивирусной программы, то велик риск, что для активации троянца будет достаточно просто вставить устройство в USB-разъем.

Эти три пути являются основными и составляют те самые 90% «собственноручных» заражений. Остальные 10% приходятся на уже упомянутые эпидемии, а также различные диверсии и саботаж, удаленную установку и запуск троянцев.

Регулярно обновляемый и правильно настроенный антивирус может перекрыть большую часть этих каналов распространения шифровальщиков.

«Энигма» отдыхает

Во времена Второй мировой войны неким эталоном криптографии считалась немецкая шифровальная машина «Энигма», на долгие годы ставшая нарицательным именованием для мощного кодирования.

Но технологии не стоят на месте, и нынешние алгоритмы шифрования — куда более сложные, чем раньше. Их достаточно много, но в энкодерах чаще всего применяется только ключевое шифрование симметричного и несимметричного типов. Первые имеют битность 1024 или 2048 бит, вторые — 128 или 256 бит. Под «битностью» мы понимаем количество вариантов по формуле 2^*кол-во бит*, которым может быть зашифрована информация.

Наиболее распространены варианты с ассиметричным 256-битным шифрованием, ибо они являются самыми устойчивыми к взлому (чтобы «в лоб» подобрать такой ключ даже на самом современном компьютере, потребуется в разы больше лет, чем существует наша вселенная).

Словом, есть много полезных в плане информационной безопасности алгоритмов защиты данных (для чего изначально шифрование и разрабатывалось), но как топором можно рубить не только дрова, но и соседей, так и технологии шифрования не остались в стороне от внимания киберпреступников.

Кодируем и взламываем

С учетом сверхвысокой сложности взлома высокобитных шифров ситуация складывается так, что практически всегда появление возможности расшифровки данных связано либо с успешным получением хотя бы одного ключа, либо с криворукостью разработчиков троянца.

В первом случае, хоть злоумышленники и предлагают выкупать ключи, зачастую все необходимое уже содержится в самом шифровальщике. Главное, чтобы с ним поработал квалифицированный специалист по дешифровке. Причем важно не только извлечь этот ключ, чтобы расшифровать данные на конкретном зашифрованном ПК, нужно еще понять его структуру и на ее основе написать специальную утилиту — генератор ключей дешифрования, который сможет подобрать нужный ключ для любого компьютера, пострадавшего от данного троянца.

Когда же речь идет о некорректной работе самого троянца, то здесь варианты могут разниться — от неправильного использования алгоритма шифрования, что в итоге может привести к длине шифра 64 бита, а то и меньше, до полного пропуска шифрования — тогда файл всего лишь меняет расширение.

Используя обе перечисленные возможности, специалисты компании «Доктор Веб» успешно помогают пользователям с восстановлением зашифрованных данных. У нас в распоряжении есть множество утилит, предназначенных для устранения последствий действий большинства троянцев.

Кстати, есть же еще один алгоритм шифровки: «клешнями». Это когда криво сделанный энкодер вместо шифрования файлов просто безвозвратно разрушает их структуру.

И ты, Android!

Говоря о шифровальщиках, мы обычно подразумеваем троянцев, «орудующих» на компьютерах, будь то обычный ПК или ноутбук. Но когда все поголовно ходят со смартфонами, было бы странно ожидать, что рано или поздно эпидемия троянцев не коснется и мобильных устройств.

Разумеется, как большинство ПК используют в качестве операционной системы Windows, которая и является основной мишенью злоумышленников, так и преобладание на рынке мобильных ОС пользователей Android сделало их излюбленными жертвами вымогателей.

Первыйтроянец-шифровальщик для Android появился еще в 2014 году и назывался SimpleLocker (дословно «простой блокировщик»).

На поверку он и в самом деле оказался простым, и файлы легко поддавались дешифровке — после его обнаружения специалисты компании «Доктор Веб» оперативно выпустили бесплатную утилиту, которая восстанавливала большую часть зашифрованных файлов. Не все, к сожалению, — злоумышленники напортачили даже в простой блокировке, и некоторые файлы портились.

В дальнейшем ситуация хоть и ухудшилась, но не так критично, как в случае с ПК. Почти все мобильные энкодеры, разработанные после SimpleLocker, были не троянцами-шифровальщиками, а именно троянцами-блокировщиками (эдакий мобильный аналог WinLock) — они блокировали экран устройства и выдавали сообщение о том, что все данные зашифрованы
и для их восстановления нужно заплатить выкуп. При этом непосредственно шифрования файлов не происходило, и проблему решало устранение блокировки экрана.

Отсутствие активного развития «мобильных» шифровальщиков связано с тремя ключевыми факторами.

1. Объем критически важных данных на смартфонах обычно крайне мал, чтобы их ценность была сопоставима с суммой выкупа или со стоимостью самого устройства — проще полностью «зачистить» аппарат и начать работать с ним «с нуля». В то же время цена данных на ПК может в сотни, а порой и в тысячи раз превышать стоимость «железа».
2. Шифровальщики — одни из самых сложных в реализации троянцев. И, учитывая предыдущий пункт, просто нет смысла тратить на них время и силы, когда можно ограничиться блокировкой экрана и «страшной надписью» про шифрование.
3. Архитектура Andorid'а построена таким образом, что зашифровать файлы пользователя там значительно сложнее, чем в Windows – это связано с бОльшими программными ограничениями.

Впрочем, недавно все же нашлись еще одни желающие поэкспериментировать – в середине октября 2017 года появился второй действующий Android-шифровальщик.

Dr.Web Security Space для Android защищает от шифровальщиков для мобильных устройств.

Главное, чтобы он был установлен и запущен на мобильном устройстве, а также мог регулярно получать обновления.

По пути Колумба

Если посмотреть на карту вспышек эпидемий того или иного шифровальщика, то чаще всего можно обнаружить, что происходят они не по всему миру, а на территории одного или нескольких государств, почти не задевая пользователей из других регионов. С чем связана такая избирательность?

Как правило, точную географическую направленность атаки троянцев имеют по одной из следующих причин.

1. Злоумышленники хотят нанести вред инфраструктуре предприятий или государственных структур определенной страны (например, NonPetya целенаправленно вредил пользователям бухгалтерской программы, использующейся преимущественно в Украине).
2. Создатели троянца сами проживают на территории, подвергающейся атаке, что облегчает им получение средств от своих сограждан. Они знают, каким софтом те пользуются, на каком языке говорят, на какие новости наиболее активно отреагируют, необдуманно перейдя по ссылке из письма или скачав приложенный архив.
3. Создатели троянца живут в соседнем с жертвами государстве – «за руку схватят» с меньшей вероятностью, а получить деньги с соседей – не так и сложно.
4. Атакующие стремятся кого-либо скомпрометировать. В этом случае злоумышленники будут маскироваться таким образом, чтобы под подозрение попали их «коллеги» из другой страны или региона. Многочисленные истории о «русских хакерах» — хороший тому пример.

Но, как и любая эпидемия, держаться в строгих рамках распространение троянцев не может. Интернет границ не имеет, «дыры» в нем общие, люди между собой общаются, письмами-файлами обмениваются. Как следствие — вирусные инциденты могут произойти в любой точке мира, потому что троянец «уплывает не туда», подобно спутавшему континенты мореплавателю. И даже самая целенаправленная атака лишь на 70–80% поразит запланированный регион или страну, в то время как все остальные случаи, возможно даже массовые, придутся на совершенно другие территории и пользователей. И зачастую жертвам из таких «нецелевых» регионов приходится хуже всего, ибо даже при желании заплатить выкуп они зачастую не могут этого сделать.

Когда Доу Джонс и Сонька Золотая Ручка заодно

Казалось бы, как может быть связан финансовый рынок и мир киберпреступлений, в частности — злоумышленники, промышляющие разработкой и распространением энкодеров? Один пытается наполнить деньгами свои карманы, вторые — поглубже залезть в карманы первых, ничего общего!

Но зависимость, к сожалению, присутствует. За 2017 год произошел резкий рост стоимости криптовалют, параллельно с ним начался «бум» майнинга, а криптовалюты стали одной из популярных «кухонных тем» даже для тех, кто от них далек. Многие увидели в криптовалютах шанс быстрого обогащения, и, разумеется, это привлекло на криптобиржи множество новых игроков со всего мира.

Но причем здесь кибермошенники? Если прочитать новости о самых известных шифровальщиках или просто немного изучить самих троянцев, станет понятно — выкуп почти всегда требуется в криптовалюте! И если запрошенные условные 5 биткойнов в начале 2017 года стоили бы жертве порядка 5000 долларов США, то в конце 2019 года подобный же запрос означал бы потерю почти 37 000 долларов!

С 2017 года вымогатели почти всегда требуют выкуп в криптовалютах.

Получается, что с ростом курсов криптовалют пропорционально растут и суммы выкупа. Конечно, «просадка» курсов будет означать и падение стоимости дешифровки, но, по прогнозам большинства аналитиков, криптовалюты и дальше будут в цене, а значит, о «дешевой» расшифровке лучше забыть сразу.

Шифровальщики «честные» и не очень, или Немного о крабах в мире разработки софта

Все шифровальщики требуют от своих жертв деньги, но зачастую ~~они делают это без уважения~~ возникает ситуация, при которой заплативший выкуп человек или компания либо не получают обещанный ключ расшифровки вообще, либо присланный ключ никак не помогает в расшифровке. Этот вариант — самый неприятный, но, увы, вполне вероятный. Также существует его «зеркальная», то есть весьма удачная версия, которая, хоть и встречается крайне редко, зато оборачивается куда меньшими проблемами.

Начнем с плохого. Файлы зашифрованы троянцем, условия выкупа известны. В панике заплатив злоумышленникам (этого делать не надо, но зачастую жертва в состоянии аффекта совершает ошибочные действия), пользователь получил ключ расшифровки. Если преступники наделены хотя бы толикой совести и действительно разбираются в криптографии, то с помощью ключа человек сможет восстановить свои данные. А уж сколько это будет стоить — зависит от троянца, точнее — от аппетитов его создателей.

Увы, после выплаты денег есть риск либо не получить ключ вообще (без комментариев), либо присланный ключ сможет расшифровать только часть файлов, либо вообще не осилит дешифровку.

Доходит до курьезов

Зафиксирован случай, когда, несмотря на заплаченный выкуп, преступники не смогли расшифровать файлы, зашифрованные созданным ими Trojan.Encoder, и отправили пострадавшего пользователя за помощью... в службу технической поддержки компании «Доктор Веб»!

Почему это происходит?

Обычный обман, то есть когда ключ вам просто не прислали, мы в расчет не берем. Неработоспособность же присланного ключа может объясняться различными факторами, но основных причины две.

1. Троянец имеет два алгоритма шифрования — демонстрационный и полноценный. Расшифровка данных, зашифрованных по первому методу, возможна с применением «демонстрационного» ключа, который жертве могут предоставить бесплатно. По сути, это лишь попытка показать, что «у всех все дешифруется», а если остальные файлы (после выкупа «полного» ключа) не восстановились — вы сами виноваты и что-то сделали не так. На самом же деле прочая информация шифровалась совсем по другим, более сложным алгоритмам.
2. Троянец делали злоумышленники, которые не дружат ни с головой, ни с руками. Как результат — в ходе шифрования он делает ошибки, а сгенерированный ключ не учитывает их наличия и оказывается бесполезным.

Среди прочих же проявлений «клешнерукости» создателей троянцев можно упомянуть ошибки в требованиях выкупа (биткойн-кошелек указан неверно), ошибки при выдаче ключей (у автора может быть несколько троянцев, имеющих разные ключи) и выполнении шифрования (файлы не зашифровались, а побились, превратившись в бесполезный мусор).

И немного о хорошем. Почти всегда это следствие уже упомянутой глупости, но в данном случае это играет на руку жертве — алгоритм шифрования может дать сбой и либо значительно упростить шифрование, либо просто поменять расширение файлов, никак не модифицировав их изнутри.

Побольше бы таких «шифровальщиков»!

Стоит отметить, что ввиду чрезвычайной стойкости большинства алгоритмов шифрования, особенно ассиметричных, именно «дыры» в самих энкодерах и позволяют заниматься расшифровкой в тех случаях, когда ключей дешифрования еще нет. В основном «полезные» ошибки троянцев бывают двух видов.

1. «Кривое» использование алгоритмов шифрования или банальные ошибки и опечатки в коде сильно упрощают его, позволяя просто подобрать ключ дешифровки.
2. Троянец оставляет копии незашифрованных файлов, например, просто удаляя их. При этом средство восстановления данных может решить проблему без утилиты дешифровки.

Но рассчитывать на удачу однозначно не стоит.

Франкенштейн лезет в сеть

Как уже говорилось выше, сами по себе энкодеры не были бы так страшны, если бы злоумышленники, распространяющие их, не использовали всю «обойму» доступных им инструментов. И, как показывает практика, наибольшего «успеха» добились авторы тех энкодеров, которые использовали их в составе комплексных атак. То есть наиболее типовые алгоритмы заражения, с точки зрения пользователей — «открыл письмо и запустил вложение» или «скачал файл, запустил, а там троянец», — в этом случае неактуальны.

Когда атака проводится с помощью комбинации нескольких вредоносных программ, функционирующих как целая система, для пользователя процесс будет напоминать ситуацию «Я ничего не трогал, оно само!». Вот основные примеры, показывающие, как такая комбинация может превратиться в страшную силу для кибератаки.

1. Средство удаленного администрирования + энкодер — злоумышленник сам запускает шифровальщика на ПК жертвы или на всех ПК сети, до которых смог дотянуться.
2. Сетевой червь + энкодер — кошмар для сетей, в которые попал червь.
3. Дроппер + энокдер — аналог предыдущего варианта.
4. Загрузчик + энкодер — сначала жертва устанавливает приложение, к которому «прицеплен» троянец семейства.Downloader, а тот уже загружает с сервера энкодер и запускает его.

К счастью, первые три случая из-за сложности своей реализации куда менее распространены, чем стандартная рассылка энкодеров или их загрузчиков через почту или вредоносные сайты, но и их сбрасывать со счетов тоже нельзя. Особенно в свете того, что именно эти «вредоносные франкенштейны» повинны в наиболее громких эпидемиях.

Насчет комбинации шифровальщика с загрузчиком — ситуация более интересная. С одной стороны, этот метод распространен достаточно широко, с другой — атаку этого типа антивирусу предотвратить гораздо легче, так как действия загрузчиков более стандартны, а значит, отлавливаются эвристическим анализатором. Получается, что при успешно отбитой атаке на защищаемый ПК в файлах отчета (логах) антивируса будут наблюдаться строки вида: «... Trojan.DownLoader.**** ...», а до загрузки на ПК шифровальщиков дело уже не дойдет. Хотя справедливости ради стоит отметить, что загрузчик может «тащить» на компьютер что угодно, не обязательно шифровальщика, но в последнее время чаще всего акцент делается именно на них.

She makes me cry!

Гибридный WannaCry, наделавший много шума по всему миру и принесший убытков более чем на 4 млрд долларов США, был помесью сетевого червя, использующего уязвимость в протоколе SMB в Windows, и троянца, который, собственно, шифровал файлы на зараженном ПК.

Распространение WannaCry было лавинообразным и началось 12 мая 2017 года, уже к вечеру того же дня превратившись в эпидемию мирового масштаба.

От WannaCry пострадали более 500 000 компьютеров по всему миру.

Но самое интересное во всей этой истории — не то, что троянец распространился по сети и вызвал массовое заражение. Примечательны здесь действия, а вернее, бездействие его жертв. Разберем чуть подробнее весь механизм атаки.

1. Червь попадал на ПК через Интернет, используя известную на тот момент уязвимость в Windows. Поскольку «дыра» была известна давно, то на компьютеры, получающие автоматическое обновление ОС, WannaCry просто не имел доступа. Это — первая ошибка его жертв.
2. Запустившись в системе, он вел себя достаточно нагло, даже не пытаясь скрыть свое присутствие. Подобная активность может быть подозрительной ИСКЛЮЧИТЕЛЬНО для антивируса, поэтому пользователи, обходящиеся без него, были лишены шанса обнаружить угрозу.

   Что примечательно, несмотря на такое «хамское» поведение вредоносной программы, ни одно антивирусное приложение, кроме Dr.Web, даже не попыталось его остановить!

   Пользователи Dr.Web не пострадали от эпидемии WannaCry

   Новость

   Пользователи других антивирусов оказались беззащитны перед атакой, если шифровальщик уже попал на компьютер. А эвристический анализатор Dr.Web успевал «придушить гада».
3. Когда значительная часть данных уже была зашифрована, выдавалось сообщение с требованием выкупа. Тут уже поздно было что-либо делать.

Стоит отметить, что этот троянец (сам шифровальщик, а не его сопутствующие компоненты) был достаточно простым, отчего эпидемия и была остановлена весьма быстро. Оказалось, что в самом его теле был зашит алгоритм, полностью деактивирующий червя при успешном обращении к некоему интернет-ресурсу. Как только этот ресурс был зарегистрирован одним из исследователей-вирусологов и смог давать червям «положительный» ответ на сетевой запрос, распространение WannaCry мгновенно остановилось.

А теперь давайте проведем небольшую работу над ошибками.

1. Нужно использовать и регулярно обновлять только поддерживаемую разработчиком версию ОС. Так, хотя Microsoft и выпустила экстренное обновление безопасности для уже неподдерживаемой Windows XP, многим хватило времени, чтобы заразиться.
2. Автоматическое обновление должно быть включено! Ни один ПК, где ОС регулярно обновлялась, от атаки не пострадал.
3. На компьютере должен быть установлен антивирус, который необходимо регулярно обновлять! Да, вероятность того, что антивирус спасет компьютер, — не 100%, но без него вы полностью беззащитны даже перед самым старым и простым шифровальщиком или вирусом.

Не будь как не-Петя!

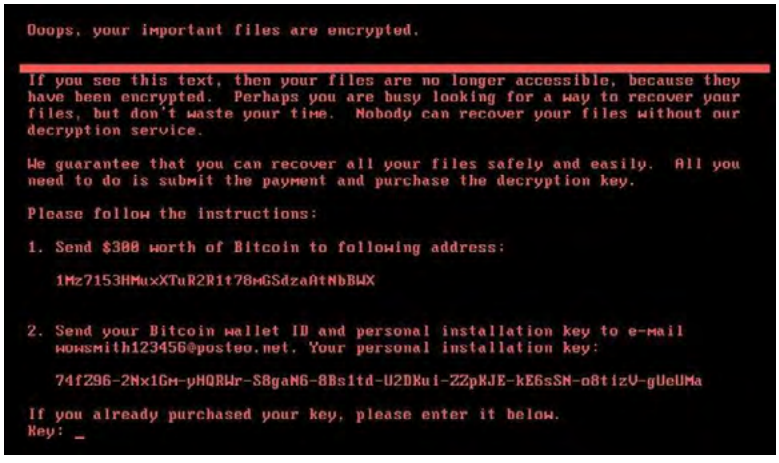
Еще один известный псевдошифровальщик, блеснувший летом 2017 года, — сетевой червь со встроенным троянцем NotPetya (почти полная переработка не слишком «удачного» для злоумышленников троянца Petya, появившегося весной 2016 года).

Подобно WannaCry, он использовал уязвимости в ПО, но не в операционной системе, а в бухгалтерской программе M.E.Dock.

Также NotPetya отличился более узкой направленностью — основной удар троянца пришелся на государственные структуры и промышленные предприятия Украины, использующие указанное выше приложение. Хотя позже он был замечен и в других странах, но там ущерб от него оказался значительно меньше.

Кроме того, хотя троянец и воспринимается большинством как типичный шифровальщик, он им не является. Да, в выдаваемом сообщении говорится, что файлы зашифрованы и нужно заплатить выкуп, но на деле проку от выплаты не будет — NotPetya не шифрует файлы, вместо этого он целенаправленно их портит, делая восстановление (именно восстановление, а не расшифровку) совершенно невозможным.

То есть на деле этот псевдошифровальщик оказывается близким родственником различных вирусов-вандалов, основная задача которых — безвозвратно уничтожать ценные для жертвы данные. Соответственно, можно предположить, что цель этого троянца была не только и не столько в обогащении его авторов, сколько в нанесении массового вреда предприятиям и государственным структурам.



Немного унылой статистики

За прошедшее с начала активного развития шифровальщиков время в компании «Доктор Веб» было собрано огромное количество статистической информации по типам энкодеров, количеству обращений и возможностям расшифровки. Ниже приведены некоторые, на наш взгляд, самые интересные статистические данные.

- В настоящее время существует несколько тысяч модификаций шифровальщиков, хотя количество принципиально различных троянцев куда меньше и не дотягивает даже до сотни.
- Каждый день специалисты антивирусной лаборатории «Доктор Веб» вносят в вирусную базу больше десятка новых модификаций шифровальщиков. Всего же объем обращений пользователей по проблемам, связанными с энкодерами, с 2014 года более-менее стабилен и составляет примерно половину от всех запросов в службу поддержки «Доктор Веб».
- Несмотря на свою «эпидемичность» и широкую известность, троянцы-шифровальщики не входят в первую десятку наиболее часто встречающихся угроз. Да что там! Они и в первой сотне-то в хвосте плетутся. Увы, это говорит лишь об их относительной малочисленности, ибо по суммам причиненного ущерба они лидируют. В самом деле, если вредоносная программа устанавливает лишнюю панель в браузер, делает компьютер частью бот-сети для майнинга, занимается рассылкой спама или чем-то подобным — это плохо, неприятно, это может скомпрометировать вас. Но не лишит всего и сразу, в отличие от троянца-шифровальщика.

Для каждого конкретного энкодера есть своя вероятность расшифровки.

Чтобы подобрать ключи для расшифровки файлов, зашифрованных троянцем Trojan.Encoder.741, методом простого перебора, потребуется

10790283805422499354415233560 1 год

Некоторые, например Trojan.Matsnu1, допускают полное восстановление всех данных, Trojan.Encoder.2667 — чуть больше чем в половине случаев, а после Trojan.Encoder.858 исправить уже ничего нельзя. Причем для разных модификаций одного и того же троянца шанс расшифровки может отличаться на 30–40%.

- Немного сухих цифр об обращениях в службу технической поддержки «Доктор Веб» за 9 месяцев 2017 года. Всего — 15 598 прямых обращений.

Наиболее часто детектируемые шифровальщики (III-IV кв. 2019 года)

Trojan.Encoder.11432

Trojan.Encoder.24384

Trojan.Encoder.858

Trojan.Encoder.3953

Trojan.Encoder.29417

Шифровальщики, заразившие максимальное количество устройств (III-IV кв. 2019 года)

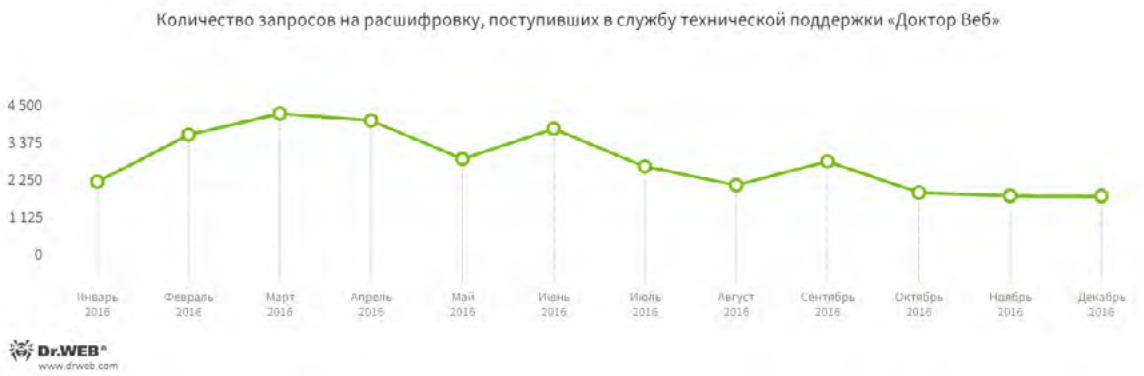
Trojan.Encoder.11432

Trojan.Encoder.24384

Trojan.Encoder.858

Trojan.Encoder.4691

Trojan.Encoder.28718



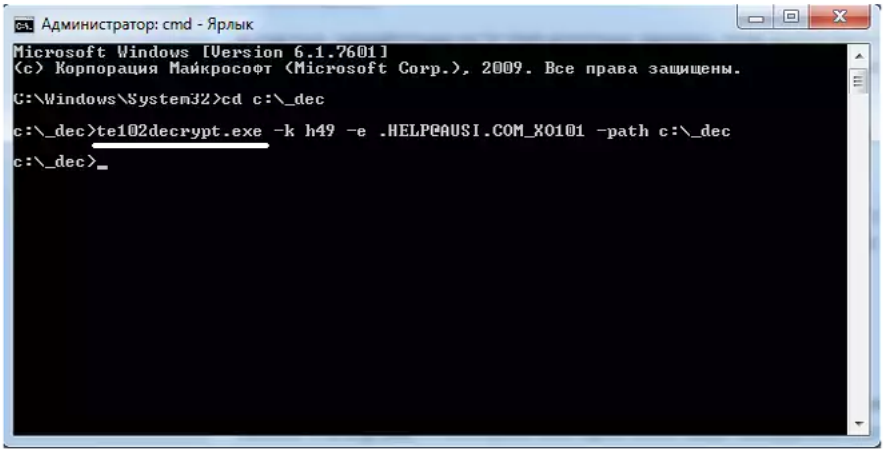
Посмотреть инфографику по теме можно тут: https://antifraud.drweb.ru/encryption_trojs?lng=ru.

Вампиры и комары

Если на вас нападет вампир и всласть пообедает, то, скорее всего, вы останетесь в живых (чисто физически выпить более двух литров крови разом проблематично — она питательная). И конечно, первое, что вам захочется, — это получить переливание. Но что если вместо врача с капельницей на вас налетит стая голодных комаров? Неприятно. А ведь зачастую вы сами зовете их!

Это небольшое лирическое отступление — всего лишь попытка показать, как ведет себя типичная жертва троянцев-вымогателей. «Словив» шифровальщика и обнаружив, что данные действительно зашифрованы, а сумма выкупа неадекватно велика, человек, как правило, устремляется в Интернет с типовым запросом «как расшифровать файлы». Получив в ответ кучу ссылок, он видит среди них множество предложений по расшифровке данных. Разумеется, небесплатных.

Коротко о вирусе: троянцы семейства **Trojan.Encoder** представляют собой вредоносные программы (скрипты), шифрующие файлы на диске компьютера и требующие деньги за их расшифровку (дешифратор). Зашифрованными могут оказаться файлы *.mp3, *.doc, *.docx, *.pdf, *.jpg, *.rar *.1CD и так далее.
Со всем семейством этого вируса познакомиться лично не удалось, но, как показывает практика, метод заражения, лечения и расшифровки у всех примерно похожи:
1. жертва заражается через спам-письмо с вложением (маскируя: Повестка в суд, налоговые органы или счет)
2. вирус распознается и удаляется (уже) почти любым антивирусом со свежими базами,
3. файлы расшифровываются путем подбора паролей-ключей к используемым видам шифрования.
Например, в Trojan.Encoder.225 используется шифрование RC4 (модифицированный) + DES, а в Trojan.Encoder.263 — Blowfish в CTR-режиме. Эти вирусы на данный момент расшифровываются на 99% исходя из личной практики.
Просто позвоните по бесплатному тел. [redacted], и мы поможем с пострадавшим компьютером.



Внимание на скриншот! Ребята не «палятся» :)

В такой момент пострадавший, уже потерявший свои данные, теряет еще и деньги, платя мошенникам, которые буквально паразитируют на других мошенниках — авторах троянца. Самые разные сервисы в Интернете предлагают полную расшифровку всех файлов после действий любых троянцев. Уже сама эта «панацея» должна бы насторожить, но в панике или просто под действием стресса людям свойственно хвататься за любую возможность, какой бы призрачной она ни выглядела.

Что же на самом деле стоит за подобными объявлениями о дешифровке? Вариантов несколько.

1. Откровенное мошенничество — передав деньги за «услугу расшифровки», пользователь получает совершенно «левую» утилиту, попутно с напоминанием о том, что расшифровка не гарантирована. Это пишется и на сайте, но где-нибудь в незаметном месте и мельчайшим шрифтом.
2. «Перепродажа» ключей дешифрования, добытых в Интернете различными путями. Известно множество случаев, когда подобным образом продавались утилиты компании «Доктор Веб» (как на примере с картинки выше).
3. «Представительство» вирусописателей в Интернете — когда работники подобных сервисов действуют совместно с разработчиками вирусов, таким образом «помогая» тем, у кого не хватает денег на выкуп. Пожалуй, это наиболее распространенный вариант, «спасибо» TORу и i2p.

Правильным же в случае заражения ПК троянцем-шифровальщиком может быть только одно действие — обращение в службу технической поддержки компании «Доктор Веб» и строгое следование всем полученным инструкциям.

Что можем мы?

«В любви, как на войне, все средства хороши». Старая поговорка в полной мере касается и противостояния антивирусных вендоров, в том числе и компании «Доктор Веб», и киберпреступного сообщества.

Понятно, что основа «армии» защитников — это специалисты по вирусному анализу, а когда речь идет о троянцах — еще и по расшифровке. Именно они разрабатывают алгоритмы дешифровки, разбирают новые способы защиты софта и оборудования, ищут более совершенные методы противодействия вирусам и прочим типам атак.

Но ведь чтобы проанализировать вирус, попытаться разобраться в коде троянца или исследовать какую бы то ни было вредоносную программу, их надо получить. Методы, которыми мы достаем образцы для исследований, — весьма разнообразны. Это и «взлом» вирусов и троянцев, которые попадают к нам от уже пострадавших пользователей (самый плохой вариант), и поиск в Интернете последних вредоносных «новинок» и уже «слитых» выкупленных ключей, а то и вовсе «ловля на живца». Так называется расстановка по сети компьютеров-ловушек. Это обычные компьютеры, имеющие доступ в Интернет и лишенные какой бы то ни было защиты, то есть являющиеся идеальными мишенями для атаки. Иногда для увеличения «улова» с такого компьютера специально бродят по «злачным местам» Всемирной паутины, а заодно в больших количествах закачивают спам, полученный с таких же почтовых ящиков-ловушек. Этот метод весьма эффективен, особенно в плане превентивного противодействия новейшим угрозам.

Далее, попав в антивирусную лабораторию, вредоносное приложение тщательно анализируется, декомпилируется и исследуется. Изучаются его строение, алгоритмы работы (шифрования, если речь об энкодере), а также «поведение в дикой природе» — то есть эмулируется атака на условный компьютер. Подобный тщательный разбор позволяет найти слабые места энкодера и использовать их ему же во вред — восстанавливать зашифрованные им файлы, адаптировать антивирус таким образом, чтобы он обнаруживал и устранял эту угрозу еще до момента ее активации в системе.

Когда троянец проанализирован, запись о нем вносится в вирусные базы, после чего опасности для пользователей он уже не представляет — он будет остановлен и уничтожен автоматически.

Что можете вы?

Для минимизации вероятности заражения вашего ПК троянцем-шифровальщиком вам стоит предпринять несколько основных действий, которые хоть и не сделают компьютер на 100% неуязвимым, но снизят риск заражения до околонулевых величин. Соблюдая эти несложные правила, вы сильно облегчите жизнь себе, попутно донельзя усложнив ее киберзлоумышленникам.

Первое, что нужно сделать – отладить механизм резервного копирования. Использование защищенных хранилищ для важных данных, размещение дополнительных копий на сменных носителях – гарантия того, что даже в самом неблагоприятном случае ваша информация не пропадет безвозвратно. Когда вопрос резервирования будет решен, можно переходить к настройкам.

Настройка Windows

1. Нужно использовать только поддерживаемые производителем версии ОС. В противном случае многие «дыры», на которые уже махнули рукой разработчики, могут быть использованы злоумышленниками.
2. Автоматическое обновление системы должно быть включено. Обновления безопасности — это первое, о чем заботятся разработчики и за чем наиболее пристально следят злоумышленники.
3. Обычная работа на ПК должна вестись под учетной записью с ограниченными правами. В противном случае запустившийся троянец получит права администратора и широкое «поле деятельности».
4. Учетная запись «Гость» должна быть отключена, поскольку потенциально может использоваться для удаленного запуска вредоносного ПО.
5. Отображение расширений файлов должно быть включено — это убережет в ситуации, когда вам «подсунули» исполняемый файл (*.exe или *.bat) или архив под видом картинки или медиафайла.
6. Функция автозапуска для сменных носителей должна быть отключена. Этим вы отсечете вариант автоматической активации троянца с зараженной флешки или съемного диска.
7. Оповещения системы (UAC-уведомления) должны быть включены. Так вы обеспечите себе стабильное информирование обо всех происходящих в системе важных событиях.

Общие рекомендации

1. Не открывайте вложения из писем, если не полностью уверены, что отправитель — именно тот, за кого себя выдает, а вложение — необходимые и известные вам файлы.
2. Регулярно проводите архивацию данных на сменные носители или на другой ПК. Так вы не только защитите их от порчи или потери в результате форс-мажора, но и сможете восстановить после действий шифровальщика.
3. Используйте только легальное лицензионное программное обеспечение, полученное из официальных источников. Это гарантия того, что вы не получите «в нагрузку» к ломаному софту троянцев и прочий мусор.
4. Все используемые программы должны обновляться по мере необходимости. Как и ОС, они могут иметь уязвимости, которые их авторы устраняют по мере обнаружения, выпуская новые версии или патчи к уже существующим.

Настройка Dr.Web

1. На компьютере должна быть установлена актуальная версия антивируса, а все его компоненты должны быть активны. Без этого говорить о какой бы то ни было защите не имеет смысла.
2. В настоящее время просто антивируса уже недостаточно — рекомендуется использовать комплексное решение безопасности, например Dr.Web Security Space (для домашних ПК) или Dr. Web Enterprise Security Suite (для компаний).
3. На доступ к настройкам Dr.Web должен быть установлен пароль, отличный от пароля учетной записи.
4. Автоматическое обновление должно быть включено.
5. Функция использования облака Dr.Web Cloud должна быть активна.
6. Проверка зашифрованного интернет-трафика должна быть включена.
7. Уровень превентивной защиты недопустимо опускать ниже «Оптимального». При повышенной вероятности инфицирования или в период эпидемии его можно повышать до «Среднего» или даже «Параноидального» — это усложнит работу с ПК, но практически полностью исключит риск активации троянца.
8. Используйте функцию «Защита от потери данных».
9. Настройте доступ к отдельным файлам и папкам на ПК с помощью Офисного/Родительского контроля.
10. Настройте брандмауэр для максимально эффективной фильтрации трафика и сетевой активности приложений.
11. Функцию «Исключение из проверки» для путей, сайтов или приложений лучше не использовать, в противном случае именно через них может быть совершена атака.

Интерактивный проект	Учебный курс
«Настрой-ка Dr.Web от шифроальщиков»	DWCERT-070-6 Защита рабочих станций и файловых серверов Windows от действий программ-шифровальщиков

К сожалению, некоторые пользователи пренебрегают многими, а иногда и вообще всеми перечисленными правилами, ссылаясь на то, что это «замедляет и усложняет работу». Отчасти это действительно так, но если сравнивать эти недостатки с полной потерей данных — то выбор в пользу безопасности кажется вполне очевидным.

Я в беде!

Но допустим, что худшее случилось, все меры не помогли, и в один прекрасный момент вы обнаружили, что ваши файлы зашифрованы, а на экране красуется надпись с требованием выкупа. Что делать?

Для начала нужно вспомнить, что, кроме списка необходимых действий, есть и более важный перечень — того, что делать нельзя ни в коем случае.

Недопустимыми являются следующие действия.

1. Проверка и лечение компьютера с помощью антивируса или утилиты Dr.Web CureIt! (или аналогичной).
2. Переустановка Windows.
3. Перемещение или удаление любых (в том числе незашифрованных) файлов на компьютере.
4. Использование компьютера для каких бы то ни было задач.
5. Если на компьютере (в корне диска C:\ или папке профиля пользователя) появились файлы с названиями crypted, pass или другими подобными, их ни в коем случае нельзя перемещать или удалять!
6. Очистка истории браузера.
7. Смена расширения зашифрованных файлов.
8. Запуск каких-либо утилит дешифровки без консультации со специалистами.

Одним словом, до обращения в техническую поддержу «Доктор Веб» лучше не делать вообще ничего, чем ошибочными шагами усложнить дальнейшую расшифровку или сделать ее невозможной.

Список же «рекомендованных» действий тоже относительно мал, ибо основная работа ляжет на плечи специалистов по расшифровке.

1. Обесточьте ПК, выдернув вилку из розетки или воспользовавшись кнопкой On/Off на блоке питания. Обратите внимание, что речь идет не о кнопке включения компьютера, расположенной на лицевой стороне системного блока, а именно о тумблере блока питания (расположен позади).
2. Обратитесь в службу технической поддержки компании «Доктор Веб» , использовав другой компьютер. Эта услуга бесплатна для пользователей коммерческих лицензий Dr.Web при условии соблюдения этих условий на момент заражения.

К запросу в службу поддержки нужно приложить несколько образцов зашифрованных файлов, но если у вас нет уверенности, как лучше действовать, — лучше задать этот вопрос инженеру поддержки и далее следовать его рекомендациям. Меньше дров наломаете.

Также постарайтесь максимально подробно вспомнить обстоятельства заражения: это касается и полученных вами по электронной почте подозрительных писем, и скачанных из Интернета программ, и сайтов, которые вы посещали. Эти данные также приложите к запросу.

Если у вас сохранилось письмо с вложением, после открытия которого файлы на компьютере оказались зашифрованными, не удаляйте его: это письмо должно помочь специалистам определить версию троянца, проникшего на ваш компьютер.

Продукты Dr.Web позволяют автоматически собрать необходимую для анализа ситуации информацию. Для этого, щелкнув по значку антивируса в системном трее, выберите пункт «Инструменты» и в появившемся окне выберите «Отчет для технической поддержки». Делать это нужно, предварительно получив от специалиста «добро» на включение зараженной машины и выполнение на ней необходимых действий.

Полезные ссылки

- Заказать расшифровку
- О Dr.Web Rescue Pack

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

Тел.: +7 (495) 789–45–87 (многоканальный)

Факс: +7 (495) 789–45–97

антивирус.рф | www.drweb.ru | estore.drweb.ru | curenet.drweb.ru | www.av-desk.com | free.drweb.ru