CIS / № 2 (29) / 2024 / www.cis.ru

«Если на стене висит ружьё, оно обязательно выстрелит»,

или всё, что вам необходимо знать о шифровальщике MS BitLocker

Степень эффективности нанесения ущерба у механизма BitLocker намного выше, чем у любого вируса-шифровальщика. Принципы его работы не соответствуют высоким требованиям, предъявляемым к защите крупных ИТ-инфраструктур. Однако модель распространения BitLocker помогла «заразить» подавляющее большинство российских компаний. Нет нужды навязывать его пользователям и службе безопасности: они сами охотно устанавливают его в больших количествах.

Почему обеспечение перехода с MS BitLocker крайне важно расскажем в статье.

Microsoft BitLocker – историческая справка по продукту

Windows изначально позиционировалась вендором Microsoft как удобная домашняя операционная система, ориентированная на B2C-рынок. В самом начале становления ОС Windows такая стратегия оказалась невероятно результативной. В те времена вопросы защиты информации не были приоритетными, дело ограничивалось предотвращением офлайн атак: кто-то из числа сотрудников офиса или сотрудник службы технического обслуживания мог забрать любые данные из корпоративного компьютера, используя загрузочную флеш-карту со своей ОС и набором утилит для поиска паролей. Единственным условием осуществления атаки было наличие физического доступа к компьютеру.

В середине 2000-х годов начался выпуск версий ОС Windows, нацеленных на B2B-рынок. Соприкосновение с бизнес-средой начало трансформировать операционную систему. В ответ на потребности корпоративных клиентов в дополнительной защите информации в Windows Vista впервые был анонсирован BitLocker.

BitLocker представляет собой функцию полнодискового шифрования, выделенную компанией Microsoft в отдельный программный продукт. При разработке этого продукта производитель преследовал цель сохранить простоту работы с операционной системой, потому что далеко не каждый пользователь обладает высокой экспертизой в области безопасности данных. Как итог – BitLocker остался непрофессиональным облегчённым инструментом шифрования. Однако область кибератак с того времени претерпела существенные изменения и вышла далеко за пределы известных тогда угроз.

Порочная практика использования недоверенных средств защиты

Сегодня прослеживается пугающая по масштабам тенденция. Многие российские компании начинали пользоваться BitLocker ещё на заре его появления. Поскольку это средство защиты не требует приложения особых усилий (нет сложных настроек и многоэтапных сценариев ввода в эксплуатацию, не нужно обучать администраторов безопасности, даже оплаты за использование продукта не требуется), Bitlocker незаметно врос в корпоративную среду и прижился на рабочих станциях как простейший механизм шифрования информации. В целом ряде компаний его применение стало своеобразным стандартом.

Однако есть ряд обстоятельств, которые заставляют задуматься о целесообразности его использования:

BitLocker не является основным компонентом ОС, ресурсы в его развитие выделяются по остаточному принципу. Вследствие чего продукт изобилует уязвимостями различного уровня критичности.

Неоднозначное поведение Microsoft в вопросах реализации алгоритмов шифрования (добавление или исключение ряда криптографических опций из продукта без уведомления клиентов), породившее недоверие как к вендору, так и к продукту.

Архитектура безопасности и логика, заложенная в BitLocker, не рассчитана на распространение в больших и сложно устроенных ИТ-инфраструктурах. Это самая глубинная проблема, которая на сегодняшний день не имеет решения.

Уход Microsoft с отечественного рынка и отказ от своих обязательств окончательно раскрыл масштаб проблемы. Сотни тысяч рабочих станций у нас в стране зашифрованы сегодня продуктом, производитель которого осуществляет открытые враждебные действия по отношению к нашему государству.

Почему BitLocker не подходит для защиты организаций

Устойчивость криптографических алгоритмов, применяемых в BitLocker, вызывает одобрение экспертного сообщества и даёт основание полагать, что для доступа злоумышленников к зашифрованной им информации понадобятся большие вычислительные ресурсы, т. е. информация зашифрована надёжно. Но при этом ключевая схема, методы защиты и хранения ключей шифрования, схема хранения и передачи паролей восстановления крайне уязвимы к компрометации. И злоумышленники эти слабости активно эксплуатируют. Именно поэтому применять BitLocker допустимо лишь на автономных домашних компьютерах, но никак не в корпоративной среде. При наличии большого количества компьютеров крупная компания просто не может обойтись без использования централизованного управления программой BitLocker и хранения её ключей шифрования в ИТ-инфраструктуре или облаке. И это делает общую защищённость данных крайне низкой, а возможность компрометации – крайне высокой.

Наиболее критичные проблемы безопасности BitLocker

На общем фоне выделяются несколько наиболее критичных проблем.

Ложная функция расшифрования данных

В ряде конфигураций поведение BitLocker крайне подозрительное. Внимательный пользователь заметит, что процесс зашифровывания занимает у BitLocker некоторое время. А вот «расшифровывание» почему-то производится мгновенно. Хотя выполнение этих операции по времени должно быть примерно одинаковым. К сожалению, чудес не бывает. Моментальная расшифровка говорит о присутствии остаточной ключевой информации (например, ключей шифрования) и кратно повышает вероятность доступа к ней. Такая псевдорасшифровка случается не регулярно и зависит от версии и типа ОС Windows,

Смотрите видео о проблеме BitLocker

ряда установленных обновлений, версии самого BitLocker и режима подключения рабочей станции к корпоративному каталогу Microsoft Active Directory. Если в компании хотя бы на 100-200 рабочих станциях применяется этот механизм шифрования, отследить, где и когда произойдёт ложное расшифрование невозможно. Чем это опасно? Полученные ключи можно, например, использовать для компрометации резервных копий, которые ранее делались на этой рабочей станции. Мало того, если в будущем администратор примет решение о возврате BitLocker, то применяться будут именно эти «старые» ключи шифрования, которые реально не были удалены при прошлом расшифровывании. С моей точки зрения, это «зияющая дыра в безопасности», которая сводит на нет все преимущества шифрования.

Небезопасные обновления

Здесь проблемой является не сам продукт, а нюансы его архитектуры внутри ОС и особенности применения ключевой схемы. При выполнении ряда обновлений возникает ситуация, когда требуется промежуточная перезагрузка со специального мини-образа операционной системы. Так как системный раздел при этом зашифрован, то ключ шифрования этого раздела условно должен быть доступен на этапе перезагрузки компьютера.

Чтобы процесс обновления и перезагрузки не слишком тревожил пользователя и не загружал ИТ-администратора лишними задачами, компания Microsoft решила временно помещать ключ шифрования в открытом виде в контейнер протектора без установленного пароля. Это означает, что в момент процедуры обновления злоумышленник может легко получить доступ к самому охраняемому элементу – к ключу шифрования. Это не потребует применения сложного инструментария и глубоких знаний криптоанализа. Всё делается штатными средствами или простыми коммерчески доступными утилитами по извлечению ключей.

Хранение ключей восстановления

При включении шифрования в Windows BitLocker предлагает сохранить ключи восстановления доступа в ряде внутренних служб, среди которых будет MS Active Directory и пространство учётной записи MS Azure.

В обоих случаях передача и хранение ключа будет осуществляться в открытом виде. Это означает, что все без исключения сотрудники ИТ-отдела компании, использующей BitLocker, будут иметь доступ к хранилищу этих ключей.

Вероятность, что уволенный ИТ-администратор заберёт с собой флеш-карту с полным набором ключей шифрования, можно попробовать оценить самостоятельно. Но, с нашей точки зрения, она выше 70% – это прямая угроза безопасности рабочих станций и всей организации.

То самое ружьё

Информационная безопасность требует однозначности и полного доверия к средству защиты. Многие годы крупные организации в нашей стране практиковали шифрование рабочих станций средством BitLocker. Теперь его применение ставится под сомнение, оно окончательно перестало быть доверенным. Высокая политизированность производителя этого средства и острая внешнеполитическая повестка повышают вероятность враждебного поведения вендора по отношению к отечественным организациям. На простом техническом языке это звучит так: BitLocker намного «эффективнее» вируса шифровальщика – будущие жертвы сами охотно устанавливают и используют его в больших количествах. Шифрование в Windows устроено так, что небольшое и неотслеживаемое обновление операционной системы может превратить в «кирпич» сотни тысяч отечественных рабочих станций мгновенно. Расшифровать такие машины за биткойны, как это делается в случае с вирусом-шифровальщиком, не получится.

Как решить проблему BitLocker

Все эти обстоятельства не возникли сегодня и не являются тайной. Сообщество российских ИБ-экспертов активно обсуждает эти вопросы и вырабатывает пути перехода на альтернативные решения.

Отделы безопасности крупных компаний так же осознают возникшие риски и делают практические шаги по их устранению. Каждый ищет свой способ решения проблемы. Кто-то находится в поиске бесплатного аналога (что само по себе утопия), кто-то занял выжидательную позицию и пытается спрогнозировать действия Microsoft, кто-то вступает на сложную тропу поиска замещающих средств защиты.

Какими свойствами должна обладать альтернатива BitLocker

В самую первую очередь, альтернативное средство защиты должно быть разработано ответственным производителем с положительной репутацией на рынке. Естественно, и само техническое решение должно быть полностью российским. Важно, чтобы разработчик корректно организовал жизненный цикл разработки продукта, в том числе согласно принятому в России «Стандарту разработки безопасного ПО». Обязательная составляющая – отсутствие сторонних библиотек и программных компонентов от «недоверенных» производителей, полноценная служба поддержки в РФ и наличие сертификатов, подтверждающих успешное прохождение испытаний на соответствие требованиям к средствам защиты у ключевых регуляторов.

Всем этим требованиям в полной мере отвечает продукт компании Аладдин – Secret Disk. Secret Disk это система защиты информации на рабочих станциях и серверах с помощью шифрования.