Описание уязвимостей MS Bitlocker

Информационный бюллетень

Программа шифрования информации на дисках компьютеров MS Bitlocker получила широкую популярность за счет своей простоты и бесплатного распространения. Дистрибутив программы поставляется в составе ОС Windows, в следствии чего Bitlocker необоснованно считается встроенным средством защиты Windows. Однако, данное средство защиты является самостоятельным программным продуктом, обладающим огромным количеством проблем безопасности.

Экспертное сообщество регулярно обращает внимание пользователей MS Windows на проблемность использования Bitlocker и большие риски компрометации информации при использовании данного средства защиты. Так как технической информации и публикаций в изданиях великое множество, ориентироваться в острой проблеме достаточно сложно, поэтому в данном документе представлена проанализированная и обработанная информация об уязвимостях Bitlocker.

Небезопасная передача ключей шифрования

Передача ключей между модулем TPM и центральным процессором в открытом виде. Метод предполагает, что у злоумышленника есть физический доступ к ноутбуку или ПК, который он собирается взломать. А также предполагается, что на компьютере используется внешний доверенный платформенный модуль (TPM). В некоторых современных компьютерах модуль TPM интегрируется непосредственно в ЦП и данный метод взлома работать не будет, но при использовании внешних модулей TPM (большинства современных ноутбуков) передача ключа, необходимого для получения данных, происходит при запуске ноутбука через шину LPC от модуля TPM к ЦП.

Ссылка на видео

Bitlocker не защищает ключи шифрования при такой передаче ключа. Это дает возможность перехватить ключ и тем самым обойти механизмы безопасности. Для реализации этой уязвимости хватит использования простой модели Raspberry Pi Pico, которую необходимо подключить напрямую к шине LPC ноутбука. Как только ноутбук начнет загрузку, эта дешевая плата считает необработанные данные, которые содержат ключ шифрования.
Далее злоумышленнику остается только создать свой "собственный" внешний модуль TPM, используя относительно простые средства. Защитный механизм Bitlocker можно быстро и легко обойти при определенных условиях.
Важно - этот метод не работает в конфигурациях, где TPM интегрирован непосредственно в процессор, поскольку в таких случаях ""подслушать"" канал передачи информации не представляется возможным. Стоимость технической организации такой атаки не превышает 150$"

Система защиты информации Cryptallit LSM, то же задействует модуль TPM для формирования ключа шифрования и проверки целостности загрузчика ОС Windows, при этом программа формирует защищенный канал передачи ключей с использованием протокола RSA.

Фейковое расшифрование данных

Если при первой активации BitLocker приходится долго ждать выполнения процесса полнодискового шифрования (FDE), который может занять несколько часов, ведь даже прочитать все блоки терабайт данных на HDD быстрее не удается, то по множественным наблюдениям экспертов отключение BitLocker (расшифрование данных) происходит практически мгновенно. Чудес не бывает - процесс расшифрования данных занимает сопоставимое с зашифрованием время. Дело в том, что при отключении BitLocker не выполняет расшифровку данных. Все секторы так и останутся зашифрованными ключом FVEK (ключ шифрования данных). Просто доступ к этому ключу больше никак не будет ограничиваться. Все проверки отключатся, а VMK (контейнер ключа шифрования данных) останется записанным среди метаданных диска в открытом виде. При каждом включении компьютера загрузчик ОС будет считывать VMK (уже без проверки TPM, запроса ключа на флешке или пароля), автоматически расшифровывать им FVEK, а затем и все файлы по мере обращения к ним. Для пользователя все будет выглядеть как полное отсутствие шифрования, но самые внимательные могут заметить незначительное снижение быстродействия дисковой подсистемы.
Злоумышленнику нужно только получить физический доступ к компьютеру, чтоб довольно просто скопировать незащищенные ключи шифрования. Далее их можно использовать, например, для доступа к резервным копиям дисков, в которых хранится ценная информация.
Что удивительно - если активировать защиту Bitlocker повторно, то будут использованы те же ключи шифрования и протекторы доступа к информации. То есть после повторного зашифрования Bitlocker старые ключи шифрования не будут считаются скомпрометированными.

Ссылка на статью

Cryptallit LSM обеспечивает выполнение реального расшифрования данных. Время работы функции, при этом, сопоставимо с временем зашифрования. При завершении расшифрования все ключи и ключевые контейнеры будут отмечены, как скомпрометированные и безопасно удалены с компьютера. Старые ключи останутся лишь в защищенной базе данных системы.

Потеря данных при повреждении защищенного диска

Риск полной потери защищенных данных Bilocker при повреждении секторов диска. Повреждение хотя бы нескольких секторов данных, на зашифрованном с помощью Bitlocker диске, может привести к безвозвратной потере данных всего диска. Если так называемые «bad blocks» придутся на crypto-storage (криптохранилище), область служебных данных Bitlocker будет недоступна, а ключевая схема этого средства шифрования будет нарушена. Доступ к данным будет невозможен в следствии потери ключа в криптохранилище. Восстановлению доступа не поможет даже наличие аварийного ключа (Recovery key), так как схема аварийного восстановления доступа так-же зависит от целостности криптохранилища.

Ссылка на видео

При подготовке системного диска к защите Cryptallit LSM создает сразу две служебные области, в которые помещается криптохранилище. Эти области находятся в разных секторах диска, что исключает их потерю при повреждении даже значительной части диска. Помимо этого, ввод в эксплуатацию предусматривает обязательную передачу копии служебной области в базу данных на сервере управления. Передаваемые данные надежно защищены при передаче и хранении. Ключевая схема Cryptalit LSM позволяет восстановить доступ к данным даже при значительном повреждении диска.

Компрометация данных при обновлениях ОС Windows

Как и в большинстве проблем безопасности Bitlocker, данная уязвимость связана с защитой ключей шифрования и специфичностью обновления ОС Windows. При применении некоторых типов обновлений операционная система требует промежуточной перезагрузки со специально подготовленного образа. Загрузка с дополнительного образа нужна, потому что системный раздел зашифрован и ключ шифрования диска C: не доступен подпрограмме обновления.
Для упрощения процедуры и облегчения жизни администратора системы ключ шифрования помещается во временную область диска в открытом виде. Если быть точнее в специальную область помещается открытый (без пароля) протектор с ключом шифрования. Злоумышленник может легко получить доступ к данному протектору и, следовательно, к ключу шифрования. Все действия исключают применения сложных инструментов и наличия высокой квалификации злоумышленника. Доступ к незащищенному протектору осуществляется штатными средствами ОС Windows.

Ссылка на статью

Программа Cryptallit LSM рассчитана на выполнение самых сложных обновлений ОС Windows (обновления безопасности или обновления стека драйверов), требующих перезагрузки компьютера. В подобных сценариях контейнер с ключом шифрования сохраняется в специальной области диска и требует аутентификации администратора по паролю для обеспечения доступа к зашифрованному содержимому диска. Защищенность протектора с ключом шифрования не уступает уровню защищенности самих данных на системном диске

Депонирование ключей восстановления в незащищенном виде

Ссылка на статью

По мнению большинства экспертов, проблема незащищенного хранения ключей шифрования является самой критичной уязвимостью Bitlocker. При первичной настройке параметров безопасности программа предложит сохранить ключи восстановления доступа в ряде внутренних ресурсов. Крайне сомнительным, в данном случае, является выбор места хранения каталог MS AD или облачный сервис MS Azure. При выборе этих мест хранения для ключей восстановления возникает ряд высоковероятных рисков:
• Ключи восстановления передаются по сети в открытом виде
• Хранение ключей восстановления в AD осуществляется в открытом виде
• При использовании MS Azure доступ к незащищенным ключам восстановления доступа имеет технический персонал этого облачного сервиса
• Дополнительных инструментов контроля доступа к ключам восстановления не предусмотрено
Все это говорит о том, что при создании Bitlocker угроза внутреннего привилегированного нарушителя (например ИТ-администратора) не рассматривалась в принципе

В основу создания Cryptallit LSM закладывалась полноценная модель разграничения полномочий, поэтому процедура ввода в эксплуатацию и настройки параметров безопасности строго разграничивает действия ИТ-администратора и специалиста по безопасности. При этом ключи восстановления доступа хранятся только в защищенных контейнерах и передаются в БД сервера управления Cryptallit в защищенном виде

Дистанционная блокировка рабочих станций

Служба доставки обновлений ОС Windows разработана так, что владелец компьютера не может контролировать скачивание и применением некоторых пакетов обновлений. Даже в случае оптимизации доставки больших пакетов в службе обновлений MS Windows их применение\выполнение весьма ограниченно, при этом анализ содержания обновлений очень трудоемкая задача. Все это приводит к тому, что крупным организациям достаточно сложно анализировать содержание бесконечных пакетов обновлений. Если с одним из обновлений поступят технические инструкции на уничтожение небольшой служебной области Bitlocker на диске защищенного компьютера, то доступ ко всему зашифрованному содержимому будет потерян.

На фоне всего этого, компания Microsoft уже не раз демонстрировала враждебность к своим российским клиентам, открыто поддерживая конфликтную санкционную политику. Это порождает высоковероятный риск силового воздействия со стороны Microsoft и массового блокирования защищенных рабочих станций организации, использующей Bitlocker.

Простота применения инструментария

На ИТ-рынке представлено достаточно большое количество программ, обеспечивающих обход защитных механизмов или получение ключа шифрования\восстановления доступа Bitlocker. Среди них есть платные и бесплатные программы. Как правило набор инструментов рассчитан на широкий спектр потребителей и не требует глубоких знаний основ криптографии.

Для примера, сценарий доступа к защищенным данным по VMK (или volume master key). В ключевой схеме Bitlocker VMK это ключ, с помощью которого шифруется и дешифруется главный ключ шифрования. Процедура получения или восстановления VMK довольно простая. Надо просто запустить специальную программу Forensic Disk Decryptor (EFDD) выпускаемую компанией Элкомсофт. С ее помощью VMK ключ изымается из дампа памяти, файла гибернации или депонированного дубликата за несколько мгновений

Ссылки по теме

1. BitCracker OpenCL-версии
2. Bitlocker Device Unlocker
3. DisLocker
4. Elcomsoft Forensic Disk Decryptor
5. Экспертная статья
6. Экспертная статья
7. Экспертная статья
8. Экспертная статья