Вас взломали? Проверьте!

В наше время одной из наиболее распространённых проблем является компрометация паролей пользователей. Причин этого очень много. К наиболее распространённым, на мой взгляд, относятся:

- Использование простых паролей
- Использование одного и того же пароля на различных интернет-ресурсах
- Использование бесплатных Wi-Fi

На самом деле, причин намного больше, но результат один и тот же. Как быть? Что можно этому противопоставить?

На мой взгляд, помочь в решении этой проблемы может следующее:

- Использование менеджеров паролей (при этом вам не нужно помнить все пароли, достаточно не забывать мастер-пароль, который, естественно, должен быть сложным)
- Использование различных сервисов для проверки утечки паролей, связанных с вашей учётной записью, с целью своевременной смены пароля
- Использование многофакторной аутентификации

Мало того, стоит учесть, что основной источник утёкших паролей – это взлом форумов через различные уязвимости. Увы, форумы взламывают, извлекают оттуда хеши паролей и затем ломают их с помощью hashcat.

Hashcat

Hashcat – это, по словам создателей, самый быстрый в мире инструмент для восстановления паролей.

Стоит учесть, что это кроссплатформенное программное обеспечение, которое работает как под Windows так и под Linux. Для работы нжны драйвера. Вместе с тем она полностью бесплатна и имеет открытый исходный код.

Официальный сайт: hashcat.net/hashcat

Одновременно использует как ресурсы видеокарты, так и центрального процессора, поддерживает огромное количество алгоритмов, в том числе умеет восстанавливать пароли Wi-Fi. Взлом осуществляется как по словарю и маске, так и с помощью brute force.

Поддерживает работу с такими алгоритмами хэширования: md5, md5crypt, sha1, sha2, sha256, md4, mysql, sha512, wpa, wpa2, grub2, android, sha256crypt, drupal7, scrypt, django и другими.

Драйверы для hashcat

Необходимы следующие драйвера для видеокарт:

- Видеокарты AMD на Windows требуют «AMD Radeon Software Crimson Edition» (15.12 или более поздняя версия)
- Intel CPUs требует «OpenCL Runtime for Intel Core and Intel Xeon Processors» (16.1.1 или более поздняя версия)
- Intel GPUs на Windows требует «OpenCL Driver for Intel Iris and Intel HD Graphics»
- Видеокарты NVIDIA требуют «NVIDIA Driver» (367. x или более поздняя версия)

На данный момент hashcat доступен для macOS, Windows и Linux с GPU, CPU и общей поддержкой OpenCL, что позволяет использовать FPGA и другие ускорительные карты.

Принцип работы

Принцип работы всех программ, позволяющих взламывать пароли, практически одинаковый. Утилиты различаются разве что скоростью перебора паролей, в них могут быть реализованы и разные алгоритмы атак. Основная идея состоит в том, чтобы по заранее заданному подмножеству букв/слов (так называемый словарь) осуществлять быстрый перебор комбинаций. От каждой комбинации вычисляется хеш и сравнивается с оригинальным. В случае совпадения пароль считается взломанным. В случае с Hashcat подбор рекомендуется производить на GPU, так как графический процессор способен перебирать комбинации значительно быстрее.

Типы атак

Hashcat предполагает использование различных типов атак для достижения эффективного покрытия всевозможных хешей:

- Атака «грубой силой» (Brute-force attack)
- Атака по маске (Mask attack)
  - Считается самой эффективной на данный момент. Идея состоит в том, чтобы с помощью частотного словаря (наиболее употребляемые пароли) построить маску и тем самым сократить количество комбинаций
  - Например, достаточно стандартной являются комбинации с заглавной первой буквой и цифрами на конце (Julia1983). В случае обычного перебора это заняло бы чуть более чем 4 года на обычной для современного GPU скорости (100 Мега-хешей в секунду)
  - Используя стандартную для многих людей маску (заглавная буква в начале и год в конце), подобный пароль можно было бы подобрать. Это заняло бы около 40 минут на той же скорости GPU
- Атака перебором всех комбинаций в словаре (Combinator attack)
- Простой перебор по словарю (Dictionary attack)
- Атака по следу (Fingerprint attack)
- Гибридная атака (Hybrid attack)
- Атака перемешиванием (Permutation attack)
- Атака на основе правила (Rule-based attack)
- Атака поиском по таблице (Table-lookup attack), только на CPU
- Атака перебором по заглавным и прописным буквам (Toggle-Case attack)

Традиционная атака «Грубой силой» считается устаревшей, поэтому команда Hashcat рекомендует использовать атаку по маске в качестве полной замены.

Стоит признать, что пароли, увы, могут быть какими угодно стойкими. Но потом они утекают не от пользователей.

Именно об этом я и хотел бы поговорить в этой статье.

Сервисы проверки утечек

Рассмотрим несколько возможностей проверки, не числится ли ваш пароль в списке утечек.

Сервис haveibeenpwned.com

Данный сервис предназначен для того, чтобы пользователи могли проверить свой адрес e-mail на утечку паролей.

Он содержит данные 124684519 учётных записей. Следует учесть, что вы можете заказать уведомление, если ваш e-mail появится в базах данного сервиса.

На вкладке haveibeenpwned.com/Passwords вы можете проверить свой пароль на утечку. База данных Pwned Passwords – это 555278657 реальных паролей, ранее обнаруженных при взломе данных. Они доступны для поиска в Интернете, а также

могут быть загружены для использования в других онлайн-системах.

Сервис Pwned Passwords был создан в августе 2017 года после того, как NIST выпустил руководство, в котором, в частности, рекомендуется проверять предоставленные пользователем пароли на наличие существующих нарушений данных. Обоснование этого совета и предложений о том, как приложения могут использовать эти данные, подробно описано в блоге под названием Introducing 306 Million Freely Downloadable Pwned Passwords.

В феврале 2018 года была выпущена вторая версия сервиса, содержащая более чем полмиллиарда паролей, при этом каждый из которых также подсчитывал, сколько раз они употреблялись. Выпуск третьей версии в июле 2018 года представил ещё 16 миллионов паролей, четвёртая версия вышла в январе 2019 года. Наряду с утечкой данных «Сбор №1» общее количество паролей превысило 551 млн. Наконец, пятая версия вышла в июле 2019 года с ещё 30 миллионами паролей. Итого общее количество записей составило почти 555 миллионов.

Сервис от Google

Сегодня вы можете проверить, не оказались ли пароли, которые сохранены в вашем аккаунте Google, в руках злоумышленников. Для этого достаточно зайти в диспетчер паролей – он сопоставит ваши данные с базой всех крупных утечек.

Информацию об утечках Google собирает сама. В основном данные поступают из открытых источников, но иногда компания находит украденные пароли на просторах «тёмного интернета».

Если Google обнаружит, что какие-то ваши пароли ранее попали в открытый доступ, то предложит их сменить. Также сервис сообщит, если вы используете один и тот же пароль на большом количестве сайтов. Диспетчер предупредит и о слишком слабых паролях, которые легко угадать.

Удобно? Безусловно! Безопасно? Не думаю.

Как это работает?

Конечно, вы знаете, что у Google довольно давно есть менеджер паролей, который синхронизируется между Chrome и Android. В этот менеджер компания добавляет функцию «проверки пароля», которая проанализирует ваши логины, чтобы убедиться, что они не были частью серьёзного нарушения безопасности, ведь на сегодня подобных утечек очень и очень много.

Ранее проверка пароля уже была доступна в качестве расширения, но сейчас Google встраивает её прямо в элементы управления учётной записью Google. Проверить ваши пароли вы можете на сайте passwords.google.com, который является ярлыком URL для менеджера паролей Google.

Ваши учётные данные сравниваются с миллионами миллионов скомпрометированных учётных записей, которые были частью серьёзных нарушений. Google говорит, что он также в некоторой степени контролирует «тёмную сеть» для сбора паролей, но большая часть базы данных, с которой сравнивается проверка паролей, происходит от сканирования открытой сети.

Стоит понимать, что у Google это ни в коем случае не единственный сервис, который делает подобные проверки. В эпоху постоянных утечек и нарушений безопасности в крупных компаниях, затронувших десятки, а может, и сотни миллионов клиентов, таким полезным ресурсом оказался haveibeenpwned.com.

Если ваш пароль скомпрометирован или оказался слишком простым, Google предложит изменить соответствующий пароль. То же самое касается, если Google видит, что вы повторно используете пароли, что является неверной практикой, ведь все сервисы должны иметь уникальный логин-пароль. И, конечно же, Google также будет уведомлять вас об учётных записях с использованием слабых паролей, которые легко угадываются. При этом нужно учесть, что пароли хешировались и шифровались перед отправкой в Google.

Поскольку проверка пароля основывается на отправке вашей конфиденциальной информации в Google, компания стремится подчеркнуть, что данные зашифрованы и даже она не может просмотреть их. Пароли в базе данных хранятся в хешированном и зашифрованном виде, и любое предупреждение о ваших данных полностью локально для конкретного компьютера.

Марк Ришер, директор Google по безопасности учётных записей, обратил внимание на то, что потребителей всё чаще просят хранить свои пароли в нескольких местах одновременно. У Apple есть iCloud Keychain, у Google – менеджер паролей. А кроме того, есть другие сторонние менеджеры паролей. Что делать? Выбрать менеджер и придерживаться его в дальнейшем? Или попытаться синхронизировать несколько менеджеров паролей? Вероятность несоответствия или наличия старого неправильного пароля в одном из этих мест довольно высока. На самом деле, нет достойного ответа на этот вопрос.

Согласно опросу Harris Poll, посвящённому проверке привычек пользователей в использовании паролей в США, результаты весьма тревожны. Слишком многие всё ещё включают в пароли предметы, которые незнакомец может легко узнать, например: день рождения, имя питомца и т.д. И мало кто говорит о преимуществах дополнительных мер безопасности, таких как двухфакторная аутентификация (её используют только 37% респондентов) и менеджеров паролей (15%).

66% опрошенных заявили, что используют один и тот же пароль для нескольких учётных записей в Интернете.

Повторное использование пароля – это главная привычка, которую Google пытается сломать, потому что использование одного и того же пароля для нескольких служб может поставить вас в опасное положение, если хотя бы один из сервисов будет скомпрометирован. Если вы не поклонник цифровых менеджеров паролей, то просто запишите их в записную книжку где-нибудь дома. Даже это более удачный вариант, поскольку не будете повторять один и тот же пароль.

Почему я не буду использовать этот сервис

Прежде всего, потому что это привязывает к браузеру от Google, а меня это не устраивает. Увы, но использовать Google Chrome в корпоративной среде, с моей точки зрения, дурная затея. Почему?

Как я думаю, данный сервис в первую очередь предназначен для персональных пользователей. И тут есть ряд вопросов.

Вместе с тем стоит отметить, что для использования Google Chrome в корпоративной среде существует особая версия – cloud.google.com/chrome-enterprise/browser/download/. Она содержит и групповые политики, и средства централизованного обновления.

Вы доверяете компании Google? Я с большим трудом. Вспомним: «Пароли хранятся в шифрованном виде». А теперь вопрос: где хранится мастер-пароль? У вас? Не думаю. Скорее всего, он хранится у специалистов Google. В любом случае достоверной информации об этом нет.

А как быть, если вы используете не только браузер Google Chrome? Например, вы используете дома Chrome, а планшет – от Apple, впрочем, как и iPhone. Тогда вам придётся устанавливать браузер от Google на все устройства.

Что посоветую я? Использовать сторонние менеджеры паролей. Благо их много. Но я бы все равно рекомендовал использовать платные версии.

Впрочем, естественно, выбирать вам.

Чуть не забыл: если вы станете запоминать пароли в Google, то потребуется уделить внимание следующему:

- Защите ПК (смартфона). Ведь любой, получивший доступ к нему, автоматически получает доступ ко всем вашим паролям
- Кроме того, стоит внедрить многофакторную аутентификацию для вашего аккаунта Google
- Помнить, что несмотря на двухфакторную аутентификацию, любой, получивший доступ к вашему ПК (смартфону), даже если вы вышли из учётной записи Google, будет нуждаться только в вашем пароле, второй фактор ему не потребуется

Firefox Monitor

Данный сервис monitor.firefox.com позволяет узнать, были ли вы частью утечки данных в Интернете. На этой же странице вы можете подписаться на мониторинг утечек с помощью аккаунта Firefox. Вы сможете отслеживать несколько адресов электронной почты.

Выводы

Проблемой в случае использования любых интернет-сервисов проверки электронных адресов на утечку в том, что вы сами пересылаете свой реальный электронный адрес. А в случае компрометации любого из этих сервисов, вы рискуете стать целью атаки направленного фишинга. Поэтому рассмотрим использование подобного сервиса в менеджере паролей на примере Kaspersky Password Manager.

Get Hacked?

Вы можете уточнить, не взломан ли ваш пароль с помощью сервиса Get Hacked? от компании Lancelot Software. Загрузить данное ПО вы можете бесплатно из Microsoft Store.

Описание

Данное приложение обнаружит, если какой-либо из ваших адресов электронной почты будет обнаружен в базах взломанных учётных записей, и немедленно сообщит вам об этом. Вооружившись этой информацией, вы можете немедленно изменить свой пароль.

Функции:

- **Простота в использовании:** всё, что нужно сделать, это ввести имя пользователя или адрес электронной почты, который вы хотите отслеживать
- **Hands-off:** фоновый мониторинг всех ваших предметов. Вы получите уведомление, если обнаружится что-то новое
- **Безопасно:** в приложении используется обширная база данных о нарушениях, созданная доверенной компанией Troy Hunt
- **Постоянно обновляется:** база данных hasibeenpwned часто обнаруживает обновления, у вас всегда будут свежие данные для сравнения
- **Конфиденциальность:** это приложение никогда не сообщит ваш адрес электронной почты или имя пользователя, оно использует его только для проверки haveibeenpwned API (который сам использует безопасный протокол HTTPS)

Kaspersky Password Manager

Проверка паролей

Ваши учётные записи подвергаются большому риску, если у них одинаковые или слабые пароли (например, qwerty или 12345), а также, если эти пароли основаны на информации, которую легко угадать или получить (например, имена родственников или даты рождения).

С Kaspersky Password Manager можно быстро проверить, насколько сложные пароли вы используете и повторяется ли один пароль в нескольких учётных записях.

Когда вы вводите пароль в онлайн-форму для регистрации или его изменения, расширение Kaspersky Password Manager отображает рекомендации, как создать сложный пароль, на основании информации о сложности вводимого вами пароля.

Проверка на скомпрометированность

Для дополнительной безопасности Kaspersky Password Manager может проверить, были ли ваши пароли взломаны или подверглись утечке с онлайн ресурсов.

Программа использует алгоритм криптографического хеширования (SHA-256) для безопасной проверки паролей на скомпрометированность. Программа высчитывает по SHA-256 контрольную сумму для каждого пароля в вашем хранилище и сравнивает их с контрольными суммами по SHA-256 в базе скомпрометированных паролей. Если контрольные суммы совпадают, программа предупреждает, что пароль является скомпрометированным и его лучше сменить.

По умолчанию проверка паролей на скомпрометированность включена.

Следует учесть, что Kaspersky Password Manager проверяет на скомпрометированность только активные записи с паролями.

Проверка на утечку с помощью канала Telegram

В данном случае мы сможем не только узнать, встречается ли наш адрес электронной почты в списке утечек, но и проверить телефон. Для этого потребуется телеграм-канал t.me/LeakCheck

Далее всё просто. Вы вводите искомый адрес электронной почты или требуемый номер телефона и получаете результат: в базах утечек он или нет. И если в базе, то сколько раз он встречается.

Однако куда большей проблемой являются корпоративные пароли. В следующем разделе мы рассмотрим обеспечение парольной защиты Azure AD для Windows Server Active Directory.

Защита паролем Azure AD для Windows Server Active Directory

Защита паролем Azure AD – это функция, которая улучшает политику паролей в организации. Локальное развёртывание защиты паролем использует как глобальные, так и пользовательские списки запрещённых паролей, которые хранятся в Azure AD. При этом выполняются те же

проверки локально, что и Azure AD для облачных изменений. Эти проверки выполняются во время смены пароля и сценариев сброса пароля.

Защита паролем Azure AD разработана с учётом следующих принципов:

- Контроллеры домена никогда не должны общаться напрямую с Интернетом
- Новые сетевые порты на контроллерах домена не открываются
- Изменения схемы Active Directory не требуются. Программное обеспечение использует существующий **контейнер** Active Directory и объекты схемы **serviceConnectionPoint**
- Отсутствуют требования по минимальным функциональным уровням леса и домена
- Программное обеспечение не создаёт и не требует учётных записей в доменах Active Directory, которые оно защищает
- Пользовательские текстовые пароли никогда не покидают контроллер домена: ни во время операций проверки пароля, ни в любое другое время
- Программное обеспечение не зависит от других функций Azure AD; например, синхронизация хэша пароля Azure AD не связана и не требуется для работы защиты паролем Azure AD

Инкрементное развёртывание

Защита паролем Azure AD поддерживает поэтапное развёртывание на контроллерах домена в домене Active Directory, но важно понимать, что это на самом деле означает.

Программное обеспечение агента DC для защиты паролем Azure AD может проверять пароли только в том случае, если оно установлено на контроллере домена, и только для изменений паролей, отправляемых на него. Невозможно контролировать, какие контроллеры домена выбираются клиентскими компьютерами Windows для обработки изменений пароля пользователя. Для обеспечения согласованного поведения и обеспечения безопасности универсальной защиты паролем программное обеспечение агента DC должно быть установлено на всех контроллерах домена в домене.

Многие организации захотят провести тщательное тестирование защиты паролем Azure AD на подмножестве своих контроллеров домена перед полным развёртыванием. Защита паролем Azure AD поддерживает частичное развёртывание, то есть программное обеспечение агента DC на данном контроллере домена будет активно проверять пароли, даже если на других контроллерах домена нет установленного программного обеспечения агента DC. Частичное развёртывание этого типа НЕ является безопасным и НЕ рекомендуется, кроме как для целей тестирования.

Архитектурная схема

Прежде чем развёртывать защиту паролем Azure AD в локальной среде Active Directory, важно понять основные концепции дизайна и функций. Следующая диаграмма показывает, как компоненты защиты паролем работают вместе (рис. 1):

- Служба прокси защиты паролем Azure AD работает на любом присоединённом к домену компьютере в текущем лесу Active Directory. Его основная цель – пересылать запросы на загрузку политики паролей с контроллеров домена в Azure AD. Затем он возвращает ответы из Azure AD на контроллер домена.
- DLL-библиотека фильтра паролей агента DC получает запросы на подтверждение пароля пользователя от операционной системы. Он перенаправляет их в службу агента DC, которая работает локально на контроллере домена.
- Служба DC Agent для защиты паролем получает запросы на проверку пароля от DLL фильтра паролей агента DC. Он обрабатывает их, используя текущую (локально доступную) политику паролей, и возвращает результат: *успешно* или *неудачно*.

Как работает защита паролем

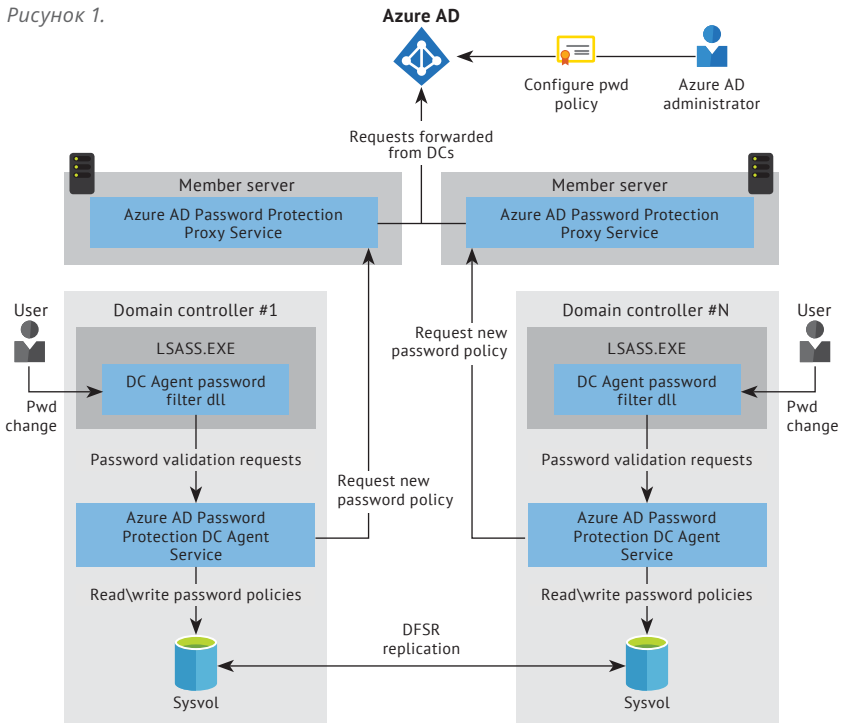
Каждый экземпляр службы прокси-сервера защиты паролей Azure AD объявляет себя на контроллерах домена в лесу, создавая объект **ServiceConnectionPoint** в Active Directory.

Каждая служба агента DC для защиты паролем также создаёт объект **ServiceConnectionPoint** в Active Directory. Этот объект используется в основном для отчётов и диагностики.

Служба агента DC отвечает за инициирование загрузки новой политики паролей из Azure AD. Первым шагом является поиск прокси-службы Azure AD Password Protection, запрашивая у леса объекты proxy **ServiceConnectionPoint**. При обнаружении доступной прокси-службы агент DC отправляет запрос на загрузку политики паролей в прокси-службу. Прокси-служба в свою очередь отправляет запрос в Azure AD. Затем прокси-служба возвращает ответ службе DC Agent.

После того как служба агента DC получает новую политику паролей от Azure AD, она сохраняет её в отдельной папке в корне *общей* папки *sysvol* своего домена. Служба агента DC также отслеживает эту папку в случае репликации новых политик из других служб агента DC в домене.

Рисунок 1.



Служба агента DC всегда запрашивает новую политику при запуске службы. После запуска службы агента DC он ежечасно проверяет возраст текущей локальной политики. Если политика старше одного часа, агент DC запрашивает новую политику у Azure AD через службу прокси, как описано ранее. Если текущая политика не старше одного часа, агент DC продолжает использовать эту политику.

Всякий раз, когда загружается политика паролей защиты паролем Azure AD, она специфична для клиента. Другими словами, политики паролей всегда являются комбинацией глобального списка запрещённых паролей Microsoft и пользовательского списка запрещённых паролей.

Агент DC связывается со службой прокси через RPC по TCP. Прокси-служба прослушивает эти вызовы на динамическом или статическом порте RPC в зависимости от конфигурации.

Агент DC никогда не прослушивает доступный по сети порт.

Прокси-сервис никогда не вызывает сервис DC Agent.

Служба прокси не имеет состояния. Он никогда не кэширует политики или любое другое состояние, загруженное из Azure.

Служба DC Agent всегда использует самую последнюю локально доступную политику паролей для оценки пароля пользователя. Если на локальном DC нет политики паролей, он принимается автоматически. Когда это происходит, регистрируется сообщение о событии, чтобы предупредить администратора.

Защита паролем Azure AD не является механизмом приложения политики в реальном времени. Может быть задержка между тем, когда изменение конфигурации политики паролей производится в Azure AD, и когда это изменение достигает и применяется на всех контроллерах домена.

Защита паролем Azure AD действует как дополнение к существующим политикам паролей Active Directory, а не как замена. Это включает в себя любые другие сторонние библиотеки фильтров паролей, которые могут быть установлены. Active Directory всегда требует, чтобы все компоненты проверки пароля были согласованы, прежде чем принимать пароль.

Два необходимых установщика агента для защиты паролем Azure AD доступны в Центре загрузки Microsoft.

Устраните «плохие» пароли в вашей организации

Лидеры отрасли советуют вам не использовать один и тот же пароль в нескольких местах, чтобы сделать его стойким и не делать простым, например «Password123». Как организации могут гарантировать, что их пользователи следуют рекомендациям передового опыта? Как они могут убедиться, что пользователи не используют слабые пароли?

Первым шагом к созданию более надёжных паролей является предоставление рекомендаций вашим пользователям.

Важно иметь хорошее руководство, но даже при этом мы знаем, что многие пользователи всё равно будут выбирать слабые пароли. Azure AD Password Protection защищает вашу организацию, обнаруживая и блокируя известные слабые пароли и их варианты.

Глобальный список запрещённых паролей

Группа Azure AD Identity Protection постоянно анализирует данные телеметрии безопасности Azure AD, выискивая часто используемые слабые или скомпрометированные пароли. Содержимое глобального списка запрещённых паролей не основано на каком-либо внешнем источнике данных. Этот глобальный список полностью образован на текущих результатах телеметрии и анализа безопасности Azure AD.

Всякий раз, когда новый пароль изменяется или сбрасывается для любого пользователя в любом клиенте Azure AD, текущая версия глобального списка запрещённых паролей используется в качестве ключевого ввода при проверке надёжности пароля. Следует учесть, что киберпреступники также используют подобные стратегии в своих атаках. Поэтому Microsoft не публикует содержимое этого списка.

Пользовательский список забаненных паролей

Некоторые организации могут захотеть ещё больше повысить безопасность, добавив свои собственные настройки поверх глобального списка запрещённых паролей в том, что Microsoft называет настраиваемым списком запрещённых паролей. Microsoft рекомендует, чтобы термины, добавленные в этот список, были в основном сфокусированы на специфических для организации условиях, таких как:

- Торговые марки
- Названия продуктов
- Местоположение (например, штаб-квартира компании)
- Специфичные для компании внутренние условия
- Сокращения, имеющие конкретное фирменное значение

После добавления терминов в пользовательский список запрещённых паролей при проверке они будут объединены с условиями в глобальном списке таких паролей.

Атака паролем и сторонние скомпрометированные списки паролей

Одним из ключевых преимуществ защиты паролем Azure AD является защита от атак с использованием паролей. В большинстве случаев атаки с разбивкой паролей не осуществляются на какую-либо отдельную учётную запись более чем несколько раз, так как такое поведение значительно увеличивает вероятность обнаружения. Поэтому большинство атак с применением паролей основывается на том, что для каждой из учётных записей на предприятии предоставляется только небольшое количество известных слабых паролей. Этот метод позволяет злоумышленнику быстро найти учётную запись со слабым паролем, избегая при этом обнаружения.

Защита паролем Azure AD разработана для эффективной блокировки всех известных слабых паролей, которые, вероятно, будут использоваться при атаках с использованием паролей на основе реальных данных телеметрии безопасности, как это видно из Azure AD. Microsoft знает о сторонних веб-сайтах, которые перечисляют миллионы паролей, которые были скомпрометированы в результате ранее известных нарушений безопасности. Обычно сторонние продукты для проверки паролей основаны на сравнении методом «грубой силы» с этими миллионами паролей. Microsoft считает, что такие методы не лучший способ улучшить общую надёжность пароля, учитывая типичные стратегии, используемые злоумышленниками с распылением паролей.

Владимир Безмалый
Microsoft Security Trusted Advisor
Консультант ООН по вопросам информационной безопасности