Лаборатория Касперского провела анализ стойкости пользовательских паролей.

Вычислительные мощности компьютеров достигли уровня, при котором пароли, считавшиеся надежными несколько лет назад, могут быть взломаны в 2024 году за считанные секунды. Современные графические процессоры, такие как RTX 4090, способны подбирать восьмизначные пароли, состоящие из латинских букв одного регистра и цифр (это 36 различных символов, доступных для комбинации), всего за 17 секунд.

Исследование , проведенное Лабораторией Касперского, показало, что 59% паролей можно взломать менее чем за час.

Хранение паролей

Сервисы для аутентификации пользователей хранят пары «логин-пароль» в виде хэшей, чтобы в случае утечки злоумышленники не могли ими воспользоваться. Перед хэшированием к паролю добавляется соль, чтобы исключить возможность подбора пароля по существующим радужным таблицам. Несмотря на необратимость хэшей, злоумышленники могут попытаться подобрать пароли, используя утекшую базу данных. В сети доступны инструменты для подбора паролей, такие как hashcat .

Методология исследования

Исследование проводилось на основе 193 миллионов паролей, обнаруженных в свободном доступе на различных даркнет-ресурсах. Лаборатория Касперского не собирает и не хранит пароли пользователей. Время подбора пароля для его хэша оценивалось с использованием как полного перебора (брутфорс), так и различных продвинутых алгоритмов (перебор, основанный на словаре и/или распространенных комбинациях символов).

Брутфорс

Метод полного перебора остается одним из самых простых: машина перебирает все возможные варианты пароля, пока один из них не окажется верным. Однако этот способ не учитывает словарные пароли и менее эффективен для длинных паролей.

Для наглядности пароли из выборки были разделены на схемы по типам символов:

Время подбора пароля методом полного перебора зависит от его длины и количества типов символов. Результаты в таблице рассчитаны для видеокарты RTX 4090 и

алгоритма хэширования MD5 с солью. Скорость подбора при такой конфигурации составляет 164 миллиарда хэшей в секунду. Данные в таблице округлены.

Самый популярный тип паролей (28%) включает в себя строчные и заглавные буквы, спецсимволы и цифры. Большинство таких паролей в исследуемой выборке брутфорсом подобрать сложно. Около 5% можно подобрать за день, а для подбора 85% паролей этого типа понадобится более года. Время подбора зависит от длины: пароль из девяти символов можно подобрать за год, из десяти — более чем за год.

Наименее стойкие для атаки брутфорсом пароли состоят только из букв, только из цифр или только из спецсимволов. Большинство из них подбирается менее чем за день. Длина стойкого пароля, состоящего только из букв, начинается с 11 символов. Стойких паролей из цифр в выборке не было.

Умный перебор

Брутфорс не является оптимальным алгоритмом подбора паролей. Часто пользователи используют определенные комбинации символов: слова, имена, даты, последовательности (12345 или qwerty). Умные алгоритмы учитывают эти особенности и ускоряют процесс подбора. Среди таких алгоритмов:

Для каждого пароля было рассчитано значение best — лучшее время подбора среди всех использованных алгоритмов. Это гипотетический идеальный случай. Для его реализации необходимо угадать подходящий алгоритм или одновременно запустить каждый из описанных алгоритмов на отдельной видеокарте.

Ниже приводятся результаты оценки стойкости паролей описанными алгоритмами на видеокарте RTX 4090 для MD5 с солью.

Использование наиболее эффективного алгоритма позволяет взломать 45% паролей за одну минуту, 59% — за один час, а 73% — менее чем за месяц. Только для 23% паролей взлом займет более года.

Исследователи отмечают, что подбор всех паролей из базы займет практически столько же времени, сколько и взлом одного пароля. При переборе атакующий проверяет наличие в базе хэша, полученного на текущей итерации. Если хэш имеется в базе, конкретный пароль помечается как взломанный, и алгоритм продолжает подбирать другие пароли.

Словарные слова

Чтобы проанализировать, какие схемы паролей наиболее устойчивы ко взломам, было рассчитано значение best для расширенного набора критериев. Для этого был составлен словарь часто встречающихся комбинаций символов длиной от четырех символов, дополнив ими указанные выше схемы паролей.

Большинство паролей (57%) содержат слово из словаря, что существенно снижает их стойкость. На взлом половины из них потребуется меньше минуты, 67% можно подобрать менее чем за час, и только 12% являются стойкими — на их подбор уйдет более года. Даже если в таком пароле используется весь набор рекомендуемых символов — буквы в разных регистрах, цифры и спецсимволы — лишь в 20% случаев он будет стойким

Среди популярных словарных последовательностей: имена (ahmed, nguyen, kumar), популярные слова (forever, love, google), стандартные пароли (password, qwerty12345).

Для защиты своих аккаунтов рекомендуется использовать случайные, программно-сгенерированные пароли или мнемонические фразы вместо осмысленных словосочетаний. Также важно проверять устойчивость паролей к взлому, избегать повторного использования одних и тех же паролей в разных сервисах и следить за утечками данных.