

Утечка 16 миллиардов паролей Apple, Facebook, Google и других - Действуй сейчас

Автор: Дэйви Уиндер. Старший автор, писатель, хакер и аналитик по кибербезопасности.

Дэйви Уиндер - ветеран.



Подписывайтесь на автора.

Опубликовано 19 июня 2025 г., 07: 45 EDT



Поделиться



Сохранить



Комментарий 0



Произошла крупнейшая утечка паролей в истории.
Getty

Обновление от 19 июня 2025 г.: Эта статья, первоначально опубликованная 18 июня, дополнена комментариями основателей Keeper Security относительно утечки 16 миллиардов паролей и других учетных данных для входа в систему среди основных поставщиков технологий.

Если вы подумали, что мой отчет от 23 мая, подтверждающий утечку регистрационных данных на удивительную сумму **184 миллиона скомпрометированных учетных данных**, был пугающим, я надеюсь, что теперь вы сели. Исследователи только что подтвердили то, что, безусловно, также является крупнейшей утечкой данных за всю историю, когда были раскрыты почти невероятные 16 миллиардов учетных данных для входа, включая пароли. В рамках продолжающегося расследования, которое началось в начале года, исследователи предположили, что массовая утечка паролей - дело рук нескольких **инфостилеров**. Вот что вам нужно знать и делать.





Автор: Дэйви Уиндер

Это КОЗЕЛ отпущения, когда дело доходит до утечки паролей?

Компрометация пароля - это не шутка; это приводит к компрометации учетной записи, а это приводит к, ну, компрометации почти всего, что вам дорого в этом технологически ориентированном мире, в котором мы живем. Вот почему Google призывает миллиарды пользователей [заменить свои пароли](#) на более безопасные ключи доступа. Вот почему ФБР предупреждает людей [не нажимать](#) о ссылках в SMS-сообщениях. Вот почему украденные пароли выставлены на продажу, [их миллионы](#), в темной паутине любому, у кого для покупки требуется совсем немного наличных. И именно поэтому это последнее откровение, честно говоря, так чертовски волнует всех.

По словам Вилиуса Петкаускаса из Cybernews, чьи исследователи расследуют утечку с начала года, "было обнаружено 30 открытых наборов данных, содержащих от десятков миллионов до более 3,5 миллиардов записей каждый". В общей сложности, Петкаускас [подтвердил](#), количество скомпрометированных записей сейчас достигло 16 миллиардов. Давайте немного поразмыслим над этим. Эти коллекции учетных данных для входа, эти базы данных, набитые скомпрометированными паролями, представляют собой то, что считается крупнейшей подобной утечкой в истории.

ПОДРОБНЕЕ ДЛЯ ВАС



Утечка объемом 16 миллиардов, размещенная в ряде сверхмассивных наборов данных, включает миллиарды учетных данных для входа в систему из социальных сетей, VPN, порталов разработчиков и учетных записей пользователей всех основных поставщиков.

Примечательно, что мне сказали, что ни об одном из этих наборов данных ранее не сообщалось как об утечке, это все новые данные. Ну, почти никаких: база данных паролей из 184 миллионов, о которой я упоминал в начале статьи, является единственным исключением.

"Это не просто утечка - это план массового использования", - заявили исследователи. И они правы. Эти учетные данные являются отправной точкой для фишинговых атак и захвата аккаунта. "Это не просто старые бреши, которые перерабатываются, - предупредили они, - это свежие разведданные, которые можно использовать в качестве оружия".

Подсказка: Получите самые важные новости недели об искусственном интеллекте, касающиеся самых шумных компаний и самых смелых прорывов, в своем почтовом ящике.

☐ Получайте последние новости о специальных предложениях, обновлениях продуктов и предложениях по контенту от Forbes и его партнеров.

Эл. адрес

Регистрация

Регистрируясь, вы соглашаетесь с нашими [Условия обслуживания](#), и вы признаете нашу [Положение о конфиденциальности](#). Forbes защищен reCAPTCHA, а Google [Политика конфиденциальности](#) и [Условия обслуживания](#) применяются.

Большая часть этой информации была структурирована в формате URL-адреса, за которым следовали данные для входа в систему и пароль. Исследователи заявили, что содержащаяся информация открывает двери "практически для любого онлайн-сервиса, который только можно себе представить, от Apple, Facebook и Google до GitHub, Telegram и различных правительственных служб".

F

Article by Thomas Coughlin, Contributor

Published Jun 18, 2025

Pure Introduces Products That Manage Data For A Post AI Training World

Читать дальше

00:22

03:12

FORBES

Предупреждение Google Chrome - пользователи Windows, Android, Mac И Linux действуют сейчас

Автор: Дэйви Уиндер



Надежное управление паролями имеет важное значение в свете крупных утечек, таких как эта

Не все базы паролей являются результатом взлома и вредоносного ПО infostealer, как, например, в случае с 16-миллиардным мегадампом, представленным здесь. Даррен Гуччионе, генеральный директор и соучредитель Keeper Security, платформы управления привилегированным доступом, сказал мне, что утечка паролей GOAT была подходящим напоминанием о том, "насколько легко получить конфиденциальные данные [непреднамеренно разоблаченный в Интернете](#)." И Гуччоне, конечно, не ошибается, на самом деле это далеко не так. Это может быть лишь верхушкой самого большого айсберга безопасности, который вот-вот обрушится на онлайн-мир. Я имею в виду, только представьте, сколько открытых учетных данных, включая пароли, хранятся там, в облаке, или, точнее, в неправильно настроенных облачных средах, ожидая, пока кто-нибудь найдет их. Если нам повезет, этот кто-то будет исследователем безопасности, который ответственно раскроет информацию о воздействии владельцу или хостингу; если нет, то это будет злоумышленник. На кого бы вы поставили свои деньги ?

"Тот факт, что учетные данные, о которых идет речь, имеют высокую ценность для широко используемых сервисов, влечет за собой далеко идущие последствия", - сказал Гуччионе. Именно поэтому для потребителей как никогда важно инвестировать в решения для управления паролями и инструменты мониторинга dark web. Последнее может помочь, предупреждая пользователей о том, что их пароли были раскрыты в Интернете, и, надеюсь, позволяя им предпринять прямые действия и обновить логины своих учетных записей, если пароль повторно использовался в разных сервисах.

≡

Forbes

Организации, однако, также не избегают необходимости инвестиций. Им следует подумать о внедрении

Подписка

Вход

моделей безопасности с нулевым доверием, которые обеспечивают контроль привилегированного доступа, чтобы "ограничить риск, гарантируя, что доступ к конфиденциальным системам всегда проходит проверку подлинности, авторизуется и регистрируется", - заключил Гуччионе, "независимо от того, где хранятся данные".

FORBES

Атака Windows XFiles - ваши пароли в опасности

Автор: Дэйви Уиндер

Кибербезопасность - это общая ответственность - не делитесь своими паролями

В конечном счете, это подтверждает тот факт, что кибербезопасность - это не просто техническая задача, но и общая ответственность. "Организации должны вносить свой вклад в защиту пользователей, - сказал Джаввад Малик, ведущий специалист по повышению осведомленности в области безопасности KnowBe4. - и люди должны сохранять бдительность и помнить о любых попытках кражи учетных данных для входа. Выбирайте надежные и уникальные пароли и внедряйте многофакторную аутентификацию везде, где это возможно ".

К этому я бы добавил: измените пароли своих учетных записей, используйте менеджер паролей и переключайтесь на ключи доступа везде, где это возможно. Настало время отнестись к этому серьезно, не ждите, пока ваши пароли появятся в этих наборах данных о текущих утечках - позаботьтесь о своей безопасности паролей прямо сейчас.

FORBES

Подтверждена атака с использованием пароля учетной записи Microsoft -
Действуй сейчас

Автор: Дэйви Уиндер



Редакционные стандарты	Перепечатка и разрешения
------------------------	--------------------------



Найти Дэйви Уиндера на [LinkedIn](#) и [x](#). Навестить Дэйви [Веб-сайт](#). Просмотр [дополнительная работа](#).

Подписаться на автора

Присоединяйтесь к беседе

Комментариев 0

Одно сообщество. Много голосов. Создайте бесплатную учетную запись, чтобы делиться своими мыслями. Прочитайте рекомендации нашего сообщества [здесь](#).

Просмотреть все комментарии (0)

Forbes

© 2025 Forbes Media LLC. Все права защищены.

AdChoices Положение о конфиденциальности Не продавайте и не распространяйте Мою Личную информацию

Ограничьте использование моей конфиденциальной личной информации Настройки конфиденциальности Цифровые условия продажи Условия обслуживания Связаться с нами

Отправьте нам отзыв Сообщите о проблеме с безопасностью Вакансии в Forbes Перепечатки & Разрешения Forbes Press Комната Реклама