



DISTILLERY

КОД ИБ — РОСТОВ-НА-ДОНУ 2021

Сергей Сторчак

- специалист по информационной безопасности
- 10+ лет в ИБ



ser-storchak.blogspot.com



ser-storchak@mail.ru



sergey.storchak@distillery.com



[@ser_storchak](https://twitter.com/ser_storchak)

Презентация отражает личную точку зрения автора,
а не его работодателя.

Have I Been Pwned (HIBP)

';--have i been pwned?

Check if your email or phone is in a data breach

|email or phone (international format)

pwned?

*<https://haveibeenpwned.com/>

Have I Been Pwned (HIBP)

';--have i been pwned?

Check if your email or phone is in a data breach

Oh no — pwned!

Pwned in 3 [data breaches](#) and found no pastes ([subscribe](#) to search sensitive breaches)

*Проверка
емайлов*

Уведомления для личных аккаунтов

Notify me

Subscribe to breach notifications

Get notified when future pwnage occurs and your account is compromised.

Я не робот



reCAPTCHA

[Конфиденциальность](#) - [Условия использования](#)

notify me of pwnage

Уведомления для корпоративных аккаунтов

Domain search

Search for pwned accounts across an entire domain and receive future notifications

Domain search allows you to find all email addresses on a particular domain that have been caught up in any of the data breaches currently in the system. You can also receive notifications if they appear in future breaches by providing a notification email. Before you can perform a domain search, you need to verify that you control the domain you're searching. **If you cannot verify that you control the domain, you will not be able to search for breached email addresses on it.**

Domain name

Would you like to be notified of any future breaches of accounts on this domain? After the verification process is complete, you'll receive a summary email regarding impacted accounts if anything on this domain shows up again in the future. **You will only be notified of breaches after you successfully complete the domain verification process.**

Subscribe me



Notification email

Уведомления для корпоративных аккаунтов

Email	Breach
[REDACTED]@distillery.com	Adapt, Apollo, Data Enrichment Exposure From PDL Customer
[REDACTED]@distillery.com	Apollo
[REDACTED]@distillery.com	Apollo, Data Enrichment Exposure From PDL Customer
[REDACTED]@distillery.com	Adapt
[REDACTED]@distillery.com	Apollo, Data Enrichment Exposure From PDL Customer
[REDACTED]@distillery.com	Data Enrichment Exposure From PDL Customer
[REDACTED]@distillery.com	Apollo
[REDACTED]@distillery.com	Apollo
[REDACTED]@distillery.com	Apollo, Data Enrichment Exposure From PDL Customer
[REDACTED]@distillery.com	Apollo
[REDACTED]@distillery.com	Apollo, Cit0day, Covve, Data Enrichment Exposure From PDL Customer
[REDACTED]@distillery.com	Apollo
[REDACTED]@distillery.com	Apollo, Data Enrichment Exposure From PDL Customer

Подписка на корпоративные уведомления

APOLLO

Apollo

In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.

Breach date: 23 July 2018

Date added to HIBP: 5 October 2018

Compromised accounts: 125,929,660

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles

[Permalink](#)

*<https://haveibeenpwned.com/PwnedWebsites>

Алгоритм работы с отчетом

- удалить несуществующие почтовые адреса
- удалить записи о базах утечек, где не были скомпрометированы пароли
- выполнить почтовую рассылку для скомпрометированных пользователей
- настроить на почтовом сервере/шлюзе блокировку
@mail.haveibeenpwned.com, чтобы можно было самостоятельно удалить email с базы HIBP
- удалить email с "Have I Been Pwned" (<https://haveibeenpwned.com/OptOut>)

*Проверка
паролей*

Проверка паролей

Pwned Passwords

Pwned Passwords are 613,584,246 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)



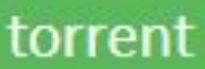
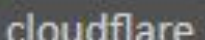




pwned?

Oh no — pwned!

This password has been seen 24 230 577 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

Проверка паролей

	Format	File	Date	Size	SHA-1 hash of 7-Zip file
 	SHA-1	Version 7 (ordered by prevalence)	19 November 2020	12.50GB	5c779a65d89b80a86349a805894f89fd510f8d18
 	SHA-1	Version 7 (ordered by hash)	19 November 2020	10.9GB	dba43bd82997d5cef156219cb0d295e1ab948727
 	NTLM	Version 7 (ordered by prevalence)	19 November 2020	10.0GB	0599805fdc50b3cd32a01be82a1cabfa86d28b36
 	NTLM	Version 7 (ordered by hash)	19 November 2020	8.5GB	7b79e9c32b2cd43362ea119886b56f37e124b195

Проверка паролей

Title	User Name	Password	URL	Creation Time	Last Modification ...	Expiry Time	Have I been pwned?
Main							
dropbox						Never expires	Pwned (password coun...
inoreader.com						Never expires	Pwned (password coun...
hackyou.ctf.su						Never expires	Pwned (password coun...
bankir						Never expires	Pwned (password coun...
Nexpose						Never expires	Pwned (password coun...
facebook						Never expires	Pwned (password coun...
Работа							
SEPM						Never expires	Pwned (password coun...
Nessus						Never expires	Pwned (password coun...
Nexpose						Never expires	Pwned (password coun...
Firefox Work						Never expires	Pwned (password coun...
Mozilla						Never expires	Pwned (password coun...
Общие							
inj3ct0r						Never expires	Pwned (password coun...
Google						Never expires	Pwned (password coun...
inoreader.com						Never expires	Pwned (password coun...
loomportal						Never expires	Pwned (password coun...
moodle						Never expires	Pwned (password coun...
open-class.ru						Never expires	Pwned (password coun...
live.com						Never expires	Pwned (password coun...

HIBP Offline Check Options

Manage plugin settings.

Actions

Check All Passwords Clear Status

Options

Check mode: Offline Online Bloom Filter

Pwned passwords file:

Bloom filter:

Column name: (Enable new column in: View - Configure Columns...)

Secure text:

Insecure text:

Excluded text:

Automatically check new or updated entries

Include breach count details for insecure passwords

Exclude Recycle Bin entries from Find results

Exclude expired entries from Find results

Display warning message after editing insecure passwords:

WARNING - INSECURE PASSWORD

This password is insecure and publicly known

Рекомендации для Microsoft 365

Требования к окончанию срока действия паролей

Требования сменить пароль приносят больше вреда, чем пользы, так как из-за них пользователи выбирают предсказуемые пароли, состоящие из последовательных слов и чисел, которые близко связаны друг с другом. В таких случаях следующий пароль можно легко угадать на основе предыдущего.

Требования к окончанию срока действия паролей не сдерживают атаки, так как злоумышленники почти всегда используют учетные данные сразу после их взлома. Дополнительные сведения см. в статье [Пора отказаться от обязательной смены паролей](#) ↗.

*<https://docs.microsoft.com/ru-ru/microsoft-365/admin/misc/password-policy-recommendations>

Рекомендации

- настроить срок действия пароля через групповые политики (6 месяцев и более)
- включить многофакторную аутентификацию
- запретить использовать корпоративную почту для регистрации на веб-сервисах, не связанных с производственной необходимостью
- принудительно сменить пароль в веб-сервисе/AD, если аккаунт присутствует в свежей базе утечек
- повышать осведомленность пользователей в сфере ИБ и проводить учебные фишинговые рассылки

Дополнительные ресурсы

- <http://spbsecurity.blogspot.com/2018/08/HIBP.html>
- <https://www.troyhunt.com/pwned-passwords-now-as-ntlm-hashes/>
- <https://snusbase.com/>
- <https://leakedsource.ru/>

Вопросы



Спасибо!

Сергей Сторчак



ser-storchak.blogspot.com



ser-storchak@mail.ru



sergey.storchak@distillery.com



[@ser_storchak](https://twitter.com/ser_storchak)