Report for: david@roblox.com

As of 2025-08-13T23:50:22.312Z

Minified and concise search report.

Module Responses:

TRELLO

Picture Url
Profile Url

Registered: true
Id: 509bf771d7cd02e149007dbc
Name: David Baszucki
Username: davidbaszucki
Last Seen: 2016-08-23T00:08:23.124000+00:00
Member Type: normal

REPLIT

Registered: true

ADOBE

Registered: true
Status: active
Type: individual

AUTODESK

Registered: true

XVIDEOS

Registered: true

NOTION

Registered: true
Id: d75bed35-2ad4-4caf-8543-ab1d5108bff4
Version: 1
Role: reader

DEVIANTART

Registered: true

GRAVATAR

Picture Url
Profile Url

Registered: true
Id: a4f798c3c5edb75f66f8529cc225540ffd051e0f9f3b6471015098e40b944f28
Name: reesemcblox
Username: reesemcblox

WIX

Registered: true

TWITTER

Registered: true

DISQUS

Registered: true

4SHARED

Registered: true

TYPING

Registered: true
Id: 164991716
Username: buliderman.
Login Type: username

APPLE

Registered: true
Email Hint: d *** @gmail.com
Phone Hint: (***) ***-**42

HIBP

Picture Url

Registered: true
Breach: true
Name: Adobe
Website: adobe.com
Bio: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Creation Date: 2013-10-04T00:00:00
Logo: https://logos.haveibeenpwned.com/Adobe.png
Website: adobe.com
Description: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.
Title: Adobe
Modified Date: 2022-05-15T23:52:49Z
Breach Count: 152445165

HIBP

Picture Url

Registered: true
Breach: true
Name: PHP Freaks
Website: phpfreaks.com
Bio: In October 2015, the PHP discussion board PHP Freaks was hacked and 173k user accounts were publicly leaked. The breach included multiple personal data attributes as well as salted and hashed passwords.
Creation Date: 2015-10-27T00:00:00
Logo: https://logos.haveibeenpwned.com/PHPFreaks.png
Website: phpfreaks.com
Description: In October 2015, the PHP discussion board PHP Freaks was hacked and 173k user accounts were publicly leaked. The breach included multiple personal data attributes as well as salted and hashed passwords.
Title: PHP Freaks
Modified Date: 2015-10-30T14:19:52Z
Breach Count: 173891

HIBP

Picture Url

Registered: true
Breach: true
Name: LinkedIn

Website: linkedin.com
Bio: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.
Creation Date: 2012-05-05T00:00:00
Logo: https://logos.haveibeenpwned.com/LinkedIn.png
Website: linkedin.com
Description: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.
Title: LinkedIn
Modified Date: 2016-05-21T21:35:40Z
Breach Count: 164611595

HIBP

Picture Url

Registered: true
Breach: true
Name: Dropbox
Website: dropbox.com
Bio: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).
Creation Date: 2012-07-01T00:00:00
Logo: https://logos.haveibeenpwned.com/Dropbox.png
Website: dropbox.com
Description: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).
Title: Dropbox

Modified Date: 2016-08-31T00:19:19Z
Breach Count: 68648009

HIBP

Picture Url

Registered: true
Breach: true
Name: B2B USA Businesses
Bio: In mid-2017, a spam list of over 105 million individuals in corporate America was discovered online. Referred to as "B2B USA Businesses", the list categorised email addresses by employer, providing information on individuals' job titles plus their work phone numbers and physical addresses. Read more about spam lists in HIBP.
Creation Date: 2017-07-18T00:00:00
Logo: https://logos.haveibeenpwned.com/Email.png
Description: In mid-2017, a spam list of over 105 million individuals in corporate America was discovered online. Referred to as "B2B USA Businesses", the list categorised email addresses by employer, providing information on individuals' job titles plus their work phone numbers and physical addresses. Read more about spam lists in HIBP.
Title: B2B USA Businesses
Modified Date: 2017-07-18T07:38:04Z
Breach Count: 105059554

HIBP

Picture Url

Registered: true
Breach: true
Name: Onliner Spambot
Bio: In August 2017, a spambot by the name of <a href="https://benkowlab.blogspot.com.au/2017/08/from-onliner-spambot-to-millions-of.html" target="_blank" rel="noopener">Onliner Spambot was identified by security researcher Benkow mo□ u□ qa/>. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.
Creation Date: 2017-08-28T00:00:00
Logo: https://logos.haveibeenpwned.com/Email.png

Description: In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow mo u qa. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.
Title: Onliner Spambot
Modified Date: 2017-08-29T19:25:56Z
Breach Count: 711477622

HIBP

Picture Url

Registered: true
Breach: true
Name: Bitly
Website: bitly.com
Bio: In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.
Creation Date: 2014-05-08T00:00:00
Logo: https://logos.haveibeenpwned.com/Bitly.png
Website: bitly.com
Description: In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.
Title: Bitly
Modified Date: 2017-10-06T08:05:10Z
Breach Count: 9313136

HIBP

Picture Url

Registered: true
Breach: true
Name: Exactis

Website: exactis.com
Bio: In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.
Creation Date: 2018-06-01T00:00:00
Logo: https://logos.haveibeenpwned.com/Exactis.png
Website: exactis.com
Description: In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.
Title: Exactis
Modified Date: 2018-07-25T20:00:44Z
Breach Count: 131577763

HIBP

Picture Url

Registered: true
Breach: true
Name: Apollo
Website: apollo.io
Bio: 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.
Creation Date: 2018-07-23T00:00:00

Logo: https://logos.haveibeenpwned.com/Apollo.png
Website: apollo.io
Description: 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.
Title: Apollo
Modified Date: 2018-10-23T04:01:48Z
Breach Count: 125929660

HIBP

Picture Url

Registered: true
Breach: true
Name: AerServ
Website: aerserv.com
Bio: In April 2018, the ad management platform known as AerServ suffered a data breach. Acquired by InMobi earlier in the year, the AerServ breach impacted over 66k unique email addresses and also included contact information and passwords stored as salted SHA-512 hashes. The data was publicly posted to Twitter later in 2018 after which InMobi was notified and advised they were aware of the incident.
Creation Date: 2018-04-01T00:00:00
Logo: https://logos.haveibeenpwned.com/AerServ.png
Website: aerserv.com
Description: In April 2018, the ad management platform known as AerServ suffered a data breach. Acquired by InMobi earlier in the year, the AerServ breach impacted over 66k unique email addresses and also included contact information and passwords stored as salted SHA-512 hashes. The data was publicly posted to Twitter later in 2018 after which InMobi was notified and advised they were aware of the incident.
Title: AerServ
Modified Date: 2018-12-06T02:58:12Z
Breach Count: 66308

HIBP

Picture Url

Registered: true
Breach: true
Name: You've Been Scraped
Bio: In October and November 2018, security researcher Bob Diachenko identified several unprotected MongoDB instances believed to be hosted by a data aggregator. Containing a total of over 66M records, the owner of the data couldn't be identified but it is believed to have been scraped from LinkedIn hence the title "You've Been Scraped". The exposed records included names, both work and personal email addresses, job titles and links to the individuals' LinkedIn profiles.
Creation Date: 2018-10-05T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In October and November 2018, security researcher Bob Diachenko identified several unprotected MongoDB instances believed to be hosted by a data aggregator. Containing a total of over 66M records, the owner of the data couldn't be identified but it is believed to have been scraped from LinkedIn hence the title "You've Been Scraped". The exposed records included names, both work and personal email addresses, job titles and links to the individuals' LinkedIn profiles.
Title: You've Been Scraped
Modified Date: 2018-12-06T19:11:27Z
Breach Count: 66147869

HIBP

Picture Url

Registered: true
Breach: true
Name: Verifications.io
Website: verifications.io
Bio: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.
Creation Date: 2019-02-25T00:00:00
Logo: https://logos.haveibeenpwned.com/VerificationsIO.png

Website: verifications.io
Description: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.
Title: Verifications.io
Modified Date: 2019-03-09T20:49:51Z
Breach Count: 763117241

HIBP

Picture Url

Registered: true
Breach: true
Name: Everybody Edits
Website: everybodyedits.com
Bio: In March 2019, the multiplayer platform game Everybody Edits suffered a data breach. The incident exposed 871k unique email addresses alongside usernames and IP addresses. The data was subsequently distributed online across a collection of files.
Creation Date: 2019-03-23T00:00:00
Logo: https://logos.haveibeenpwned.com/EverybodyEdits.png
Website: everybodyedits.com
Description: In March 2019, the multiplayer platform game Everybody Edits suffered a data breach. The incident exposed 871k unique email addresses alongside usernames and IP addresses. The data was subsequently distributed online across a collection of files.
Title: Everybody Edits
Modified Date: 2019-04-03T10:55:58Z
Breach Count: 871190

HIBP

Picture Url

Registered: true
Breach: true
Name: Evite
Website: evite.com
Bio: In April 2019, the social planning website for managing online invitations Evite identified a data breach of their systems. Upon investigation, they found unauthorised access to a database archive dating back to 2013. The exposed data included a total of 101 million unique email addresses, most belonging to recipients of invitations. Members of the service also had names, phone numbers, physical addresses, dates of birth, genders and passwords stored in plain text exposed.
Creation Date: 2013-08-11T00:00:00
Logo: https://logos.haveibeenpwned.com/Evite.png
Website: evite.com
Description: In April 2019, the social planning website for managing online invitations Evite identified a data breach of their systems. Upon investigation, they found unauthorised access to a database archive dating back to 2013. The exposed data included a total of 101 million unique email addresses, most belonging to recipients of invitations. Members of the service also had names, phone numbers, physical addresses, dates of birth, genders and passwords stored in plain text exposed.
Title: Evite
Modified Date: 2019-07-14T14:51:51Z
Breach Count: 100985047

HIBP

Picture Url

Registered: true
Breach: true
Name: Canva
Website: canva.com
Bio: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins.
Creation Date: 2019-05-24T00:00:00
Logo: https://logos.haveibeenpwned.com/Canva.png
Website: canva.com
Description: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins.
Title: Canva
Modified Date: 2019-08-09T14:24:01Z

Breach Count: 137272116

HIBP

Picture Url

Registered: true
Breach: true
Name: Data Enrichment Exposure From PDL Customer
Bio: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.
Creation Date: 2019-10-16T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.
Title: Data Enrichment Exposure From PDL Customer
Modified Date: 2019-11-22T20:13:04Z
Breach Count: 622161052

HIBP

Picture Url

Registered: true
Breach: true
Name: Covve
Website: covve.com
Bio: In February 2020, a massive trove of personal information referred to as "db8151dd" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. Later identified as originating from the Covve contacts app, the exposed data included extensive personal information and interactions between Covve users and their contacts. The data was provided to HIBP by dehashed.com.

Creation Date: 2020-02-20T00:00:00
Logo: https://logos.haveibeenpwned.com/Covve.png
Website: covve.com
Description: In February 2020, a massive trove of personal information referred to as "db8151dd" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. Later identified as originating from the Covve contacts app, the exposed data included extensive personal information and interactions between Covve users and their contacts. The data was provided to HIBP by dehashed.com.
Title: Covve
Modified Date: 2020-05-19T20:25:18Z
Breach Count: 22802117

HIBP

Picture Url

Registered: true
Breach: true
Name: NetGalley
Website: netgalley.com
Bio: In December 2020, the book promotion site NetGalley suffered a data breach. The incident exposed 1.4 million unique email addresses alongside names, usernames, physical and IP addresses, phone numbers, dates of birth and passwords stored as salted SHA-1 hashes.
Creation Date: 2020-12-21T00:00:00
Logo: https://logos.haveibeenpwned.com/NetGalley.png
Website: netgalley.com
Description: In December 2020, the book promotion site NetGalley suffered a data breach. The incident exposed 1.4 million unique email addresses alongside names, usernames, physical and IP addresses, phone numbers, dates of birth and passwords stored as salted SHA-1 hashes.
Title: NetGalley
Modified Date: 2021-11-25T22:08:12Z
Breach Count: 1436435

HIBP

Picture Url

Registered: true
Breach: true

Name: LinkedIn Scraped Data (2021)
Website: linkedin.com
Bio: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.
Creation Date: 2021-04-08T00:00:00
Logo: https://logos.haveibeenpwned.com/LinkedIn.png
Website: linkedin.com
Description: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.
Title: LinkedIn Scraped Data (2021)
Modified Date: 2023-11-07T06:51:33Z
Breach Count: 125698496

HIBP

Picture Url

Registered: true
Breach: true
Name: Gravatar
Website: gravatar.com
Bio: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.
Creation Date: 2020-10-03T00:00:00
Logo: https://logos.haveibeenpwned.com/Gravatar.png

Website: gravatar.com
Description: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.
Title: Gravatar
Modified Date: 2021-12-08T01:47:02Z
Breach Count: 113990759

HIBP

Picture Url

Registered: true
Breach: true
Name: Twitter (200M)
Website: twitter.com
Bio: In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.
Creation Date: 2021-01-01T00:00:00
Logo: https://logos.haveibeenpwned.com/Twitter.png
Website: twitter.com
Description: In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.
Title: Twitter (200M)
Modified Date: 2023-01-05T20:49:16Z
Breach Count: 211524284

HIBP

Picture Url

Registered: true
Breach: true
Name: Roblox
Website: roblox.com
Bio: In August 2016, Roblox disclosed a data breach that affected over 50k users. The security incident impacted email and IP addresses, usernames, purchases and Robux balances which were left exposed on a test server.
Creation Date: 2016-07-31T00:00:00
Logo: https://logos.haveibeenpwned.com/Roblox.png
Website: roblox.com
Description: In August 2016, Roblox disclosed a data breach that affected over 50k users. The security incident impacted email and IP addresses, usernames, purchases and Robux balances which were left exposed on a test server.
Title: Roblox
Modified Date: 2023-07-23T04:01:44Z
Breach Count: 52458

HIBP

Picture Url

Registered: true
Breach: true
Name: LinkedIn Scraped and Faked Data (2023)
Website: linkedin.com
Bio: In November 2023, a post to a popular hacking forum alleged that millions of LinkedIn records had been scraped and leaked. On investigation, the data turned out to be a combination of legitimate data scraped from LinkedIn and email addresses constructed from impacted individuals' names.
Creation Date: 2023-11-04T00:00:00
Logo: https://logos.haveibeenpwned.com/LinkedIn.png
Website: linkedin.com
Description: In November 2023, a post to a popular hacking forum alleged that millions of LinkedIn records had been scraped and leaked. On investigation, the data turned out to be a combination of legitimate data scraped from LinkedIn and email addresses constructed from impacted individuals' names.
Title: LinkedIn Scraped and Faked Data (2023)
Modified Date: 2024-06-04T19:46:37Z
Breach Count: 19788753

HIBP

Picture Url

Registered: true
Breach: true
Name: Trello
Website: trello.com
Bio: In January 2024, data was scraped from Trello and posted for sale on a popular hacking forum. Containing over 15M email addresses, names and usernames, the data was obtained by enumerating a publicly accessible resource using email addresses from previous breach corpuses. Trello advised that no unauthorised access had occurred.
Creation Date: 2024-01-16T00:00:00
Logo: https://logos.haveibeenpwned.com/Trello.png
Website: trello.com
Description: In January 2024, data was scraped from Trello and posted for sale on a popular hacking forum. Containing over 15M email addresses, names and usernames, the data was obtained by enumerating a publicly accessible resource using email addresses from previous breach corpuses. Trello advised that no unauthorised access had occurred.
Title: Trello
Modified Date: 2024-01-22T19:41:05Z
Breach Count: 15111945

HIBP

Picture Url

Registered: true
Breach: true
Name: Operation Endgame
Bio: In May 2024, a coalition of international law enforcement agencies took down a series of botnets in a campaign they coined "Operation Endgame". Data seized in the operation included impacted email addresses and passwords which were provided to HIBP to help victims learn of their exposure.
Creation Date: 2024-05-30T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In May 2024, a coalition of international law enforcement agencies took down a series of botnets in a campaign they coined "Operation Endgame". Data seized in the operation included impacted email addresses and passwords which were provided to HIBP to help victims learn of their exposure.
Title: Operation Endgame

Modified Date: 2025-05-23T20:39:21Z
Breach Count: 16466858

HIBP

Picture Url

Registered: true
Breach: true
Name: DemandScience by Pure Incubation
Website: demandscience.com
Bio: In early 2024, a large corpus of data from DemandScience (a company owned by Pure Incubation), appeared for sale on a popular hacking forum. Later attributed to a leak from a decommissioned legacy system, the breach contained extensive data that was largely business contact information aggregated from public sources. Specifically, the data included 122M unique corporate email addresses, physical addresses, phone numbers, employers and job titles. It also included names and for many individuals, a link to their LinkedIn profile.
Creation Date: 2024-02-28T00:00:00
Logo: https://logos.haveibeenpwned.com/DemandScience.png
Website: demandscience.com
Description: In early 2024, a large corpus of data from DemandScience (a company owned by Pure Incubation), appeared for sale on a popular hacking forum. Later attributed to a leak from a decommissioned legacy system, the breach contained extensive data that was largely business contact information aggregated from public sources. Specifically, the data included 122M unique corporate email addresses, physical addresses, phone numbers, employers and job titles. It also included names and for many individuals, a link to their LinkedIn profile.
Title: DemandScience by Pure Incubation
Modified Date: 2024-11-13T10:00:34Z
Breach Count: 121796165

HIBP

Picture Url

Registered: true
Breach: true
Name: Stealer Logs, Jan 2025
Bio: In January 2025, stealer logs with 71M email addresses were added to HIBP. Consisting of email address, password and the website the credentials were entered against, this breach marks the launch of a new HIBP feature enabling the retrieval of the specific websites the logs were collected against. The incident also resulted in 106M more

passwords being added to the Pwned Passwords service.
Creation Date: 2025-01-13T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In January 2025, stealer logs with 71M email addresses were added to HIBP. Consisting of email address, password and the website the credentials were entered against, this breach marks the launch of a new HIBP feature enabling the retrieval of the specific websites the logs were collected against. The incident also resulted in 106M more passwords being added to the Pwned Passwords service.
Title: Stealer Logs, Jan 2025
Modified Date: 2025-01-15T00:04:36Z
Breach Count: 71039833

HIBP

Picture Url

Registered: true
Breach: true
Name: ALIEN TXTBASE Stealer Logs
Bio: In February 2025, 23 billion rows of stealer logs were obtained from a Telegram channel known as ALIEN TXTBASE. The data contained 284M unique email addresses alongside the websites they were entered into and the passwords used. This data is now searchable in HIBP by both email domain and the domain of the target website.
Creation Date: 2025-02-15T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In February 2025, 23 billion rows of stealer logs were obtained from a Telegram channel known as ALIEN TXTBASE. The data contained 284M unique email addresses alongside the websites they were entered into and the passwords used. This data is now searchable in HIBP by both email domain and the domain of the target website.
Title: ALIEN TXTBASE Stealer Logs
Modified Date: 2025-02-25T19:25:18Z
Breach Count: 284132969

HIBP

Picture Url

Registered: true
Breach: true
Name: Data Troll Stealer Logs

Bio: In June 2025, headlines erupted over a "16 billion password" breach. In reality, the dataset was a compilation of publicly accessible stealer logs, mostly repurposed from older leaks, with only a small portion of genuinely new material. HIBP received 2.7B rows containing 109M unique email addresses, which was subsequently added to the service under the name "Data Troll". The websites the stealer logs were captured against are searchable via the HIBP dashboard.
Creation Date: 2025-06-20T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In June 2025, headlines erupted over a "16 billion password" breach. In reality, the dataset was a compilation of publicly accessible stealer logs, mostly repurposed from older leaks, with only a small portion of genuinely new material. HIBP received 2.7B rows containing 109M unique email addresses, which was subsequently added to the service under the name "Data Troll". The websites the stealer logs were captured against are searchable via the HIBP dashboard.
Title: Data Troll Stealer Logs
Modified Date: 2025-08-13T19:48:00Z
Breach Count: 109532219

EVENTBRITE

Registered: true
Id: 1438354492
Verified: true

BITMOJI

Registered: true

FACEBOOK

Registered: true
Email Hint: d*****@r*******.com, d*****@b*******.com

SAMSUNG

Registered: true

EA

Registered: true

MAPS

Profile Url

Registered: true

GOOGLE

Picture Url

Registered: true
Id: 117568937777121061361
Last Seen: 2025-08-01T02:26:44

PANDORA

Picture Url
Profile Url

Registered: true
Username: david34233
Followers: 0
Following: 0
Likes: 20
Stations: 25
