Report for: jfizzleproductions@yahoo.com

As of 2024-08-10T16:13:55.640Z

Minified and concise search report.

Module Responses:

FACEBOOK

Registered: true

HIBP

Picture Url

Registered: true
Breach: true
Name: Anti Public Combo List
Bio: In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.
Creation Date: 2016-12-16T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.
Title: Anti Public Combo List
Breach Count: 457962538

HIBP

Picture Url

Registered: true
Breach: true
Name: Collection #1
Bio: In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.
Creation Date: 2019-01-07T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.
Title: Collection #1
Breach Count: 772904991

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://haveibeenpwned.com/Content/Images/PwnedLogos/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
Breach Count: 622161052

HIBP

Picture Url

Registered: true
Breach: true
Name: Last.fm
Website: last.fm
Bio: In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. Whilst Last.fm knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.
Creation Date: 2012-03-22T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Lastfm.png
Website: last.fm
Description: In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. Whilst Last.fm knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.
Title: Last.fm
Breach Count: 37217682

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://haveibeenpwned.com/Content/Images/PwnedLogos/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

Breach Count: 711477622

HIBP

Picture Url

Registered: true

Breach: true

Name: ReverbNation

Website: reverbnation.com

Bio: In January 2014, the online service for assisting musicians to build their careers ReverbNation suffered a data breach which wasn't identified until September the following year. The breach contained over 7 million accounts with unique email addresses and salted SHA1 passwords.

Creation Date: 2014-01-01T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Reverb-Nation.png

Website: reverbnation.com

Description: In January 2014, the online service for assisting musicians to build their careers ReverbNation suffered a data breach which wasn't identified until September the following year. The breach contained over 7 million accounts with unique email addresses and salted SHA1 passwords.

Title: ReverbNation

Breach Count: 7040725

HIBP

Picture Url

Registered: true
Breach: true
Name: River City Media Spam List
Website: rivercitymediaonline.com
Bio: In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.
Creation Date: 2017-01-01T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Email.png
Website: rivercitymediaonline.com
Description: In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.
Title: River City Media Spam List
Breach Count: 393430309

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://haveibeenpwned.com/Content/Images/PwnedLogos/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
Breach Count: 763117241

WIX

Registered: true

CYBERBACKGROUNDCHECKS

Registered: true
Name: Jeffery Wayne Mcbride JR
Age: 37
Location: 100 Anabel Ave, Saint Louis, MO, 63135, US
Email: nmcbride@aol.com, mahanbrooke@yahoo.com, jefferymcbride87@gmail.com, jfizzleproductions@netzero.net, mcbridejeffery@gmail.com, lsmithnsg@msn.com, lauracarlson@live.com, jfizzleproductions@yahoo.com, tru_2_da_game87@yahoo.com, anthony77525@yahoo.com, ghetto_mix_boy@yahoo.com, ghettomixboy@yahoo.com, plumer_99@yahoo.com, ajfizzleproductionsz34@yahoo.com, lmcmaster406@comcast.net, mc406@wmconnect.com, j_fizzle_4shizzle@earthlink.net, jream@bellatlantic.net, nmcbride68@aol.com, jeffery.mcbride@iwon.com, anita.mcbride@bellsouth.net
Phone: (573) 221-2678, (573) 221-1688, (573) 406-1573, (415) 846-8800, (440) 570-8284, (573) 719-3335, (314) 521-2225, (573) 221-5781, (573) 822-3096, (816) 853-5496, (573) 221-7000, (573) 221-8929, (573) 795-4249
Other Names: Jeffery W Mcbride JR, Jeffery Wayne Mcbride, Jeffery W Mcbride, Jeffery Mcbride, Jeffery M Mcbride, Jeffery Mcbride JR, Jefferyw Mcbride JR, Jeffery Mcbrde, Jeffrey W Mcbride, Jeffrey Mcbride, Jeff W Mcbride, Jaffery Mcbride, Jefferyw Mcbride, Jeffery Wayne, Jeffrey Mcbride JR, Jeff Mcbride, Jefferey Mcbride, Jeffery Undefined Mcbride JR, Jeffery Mcbrode, Jeffrey Mc Bride, Jeff Mc Bride, Jeff Mc
Results Page: https://www.cyberbackgroundchecks.com/detail/jeffery-wayne-mcbride/pidnazpgallmzqapgagxypm