

OSINT Industries

Report for: **sarahwilkes25@yahoo.com**

As of **2024-08-22T20:00:02.979Z**

[Map](#) • [Modules](#) • [Timeline](#)

Module Responses

GOOGLE

Registered : true

Id : 100482049158763793470

Last Seen : 2023-03-27T14:23:54



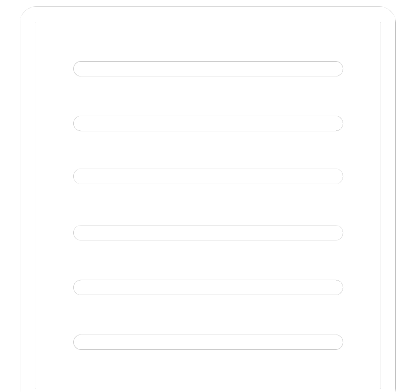
HIBP

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 <https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned> Password reuse, credential stuffing and another billion records in Have I Been Pwned.

Creation Date : 2016-12-16T00:00:00

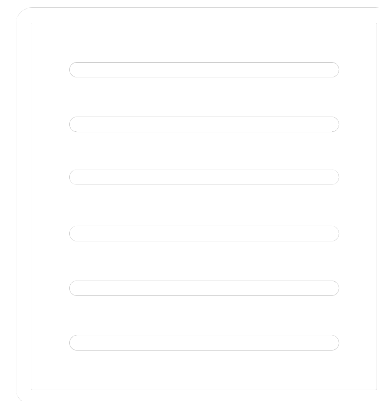
Registered : true

Breach : true

Name : Data Enrichment Exposure From PDL Customer

Bio : In October 2019, <https://www.troyhunt.com/data-enrichment-people-data-labs-and-another-622m-email-addresses> 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



Registered : true

Breach : true

Name : MySpace

Website : myspace.com

Bio : In approximately 2008, <http://motherboard.vice.com/read/427-million-myspace-passwords-emails-data-breach> MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but <https://www.troyhunt.com/dating-the-ginormous-myspace-breach> analysis of the data suggests it was 8 years before being made public.

Creation Date : 2008-07-01T00:00:00



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](https://web.archive.org/web/20170426084052/https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire). 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



Registered : true

Breach : true

Name : Verifications.io

Website : verifications.io

Bio : In February 2019, the email address validation service [verifications.io](https://securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service) suffered a data breach. Discovered by [Bob Diachenko](https://twitter.com/mayhemdayone) and [Vinny Troia](https://twitter.com/vinnytroia), 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](https://web.archive.org/web/20190227230352/https://verifications.io/).

Creation Date : 2019-02-25T00:00:00



MYSFACE

Registered : true

FANPOP

Registered : true

CYBERBACKGROUNDCHECKS

Registered : true

Name : Sarah D Smith

Location : 649 Larch Way, San Francisco, CA, 94115, US

Email : sarah-d-smith@live.com, sarahmechell09@gmail.com, sarahwilkes25@yahoo.com, allenbo03@yahoo.com, sarahsmith25@yahoo.com

Phone : (415) 902-9304, (386) 684-9424, (415) 574-1036, (386) 684-9590, (904) 328-0702, (415) 684-8297

MAPS

Registered : true

Profile Url : <https://www.google.com/maps/contrib/100482049158763793470/reviews>

Timeline

Content: Breached on Anti Public Combo List

Date/Year: 2016-12-16T00:00:00

Content: Breached on Data Enrichment Exposure From PDL Customer

Date/Year: 2019-10-16T00:00:00

Content: Breached on MySpace

Date/Year: 2008-07-01T00:00:00

Content: Breached on River City Media Spam List

Date/Year: 2017-01-01T00:00:00

Content: Breached on Verifications.io

Date/Year: 2019-02-25T00:00:00

Content: Last Active (Google)

Date/Year: 2023-03-27T14:23:54

osint.industries