

OSINT Industries

Report for: **lauren.blasch@gmail.com**

As of **2025-03-13T21:32:25.837Z**

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

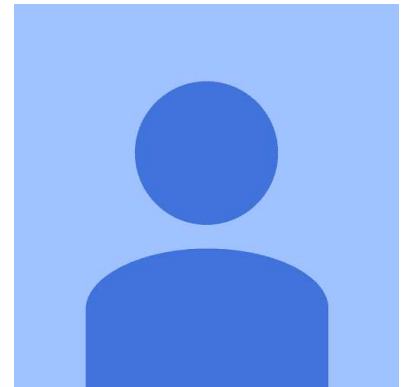
Module Responses

GOOGLE

Registered : true

Id : 113936306169434750902

Last Seen : 2023-09-03T06:33:10



HIBP

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

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



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



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

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. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Creation Date : 2013-08-11T00:00:00



Registered : true

Breach : true

Name : Data Enrichment Exposure From PDL Customer

Bio : In October 2019, <a

href="https://www.troyhunt.com/data-enrichment-people-data-labs-and-another-622m-email-addresses"

target="_blank" rel="noopener">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 : Neiman Marcus

Website : neimanmarcus.com

Bio : In May 2024, the American luxury retailer Neiman Marcus suffered a data breach <a

href="https://www.bleepingcomputer.com/news/security/neiman-marcus-data-breach-31-million-email-addresses-found-exposed/"

target="_blank" rel="noopener">which was later posted to a

popular hacking forum. The data included 31M unique email

addresses, names, phone numbers, dates of birth, physical

addresses and partial credit card data (note: this is insufficient to

make purchases). The breach was traced back to a series of

attacks against the Snowflake cloud service which impacted 165

organisations worldwide.

Creation Date : 2024-04-14T00:00:00

Registered : true

Breach : true

Name : National Public Data

Bio : In April 2024, a large trove of data made headlines as having exposed "3 billion people" due to a breach of the National Public Data background check service. The initial corpus of data released in the breach contained billions of rows of personal information, including US social security numbers. Further partial data sets were later released including extensive personal information and 134M unique email addresses, although the origin and accuracy of the data remains in question. This breach has been flagged as "unverified" and a full description of the incident is in the link above.

Creation Date : 2024-04-09T00:00:00

MAPS

Registered : true

Profile Url : https://www.google.com/maps/contrib/113936306169434750902/reviews

Timeline

Content: Breached on Adobe

Date/Year: 2013-10-04T00:00:00

Content: Breached on LinkedIn

Date/Year: 2012-05-05T00:00:00

Content: Breached on Dropbox

Date/Year: 2012-07-01T00:00:00

Content: Breached on You've Been Scraped

Date/Year: 2018-10-05T00:00:00

Content: Breached on Evite

Date/Year: 2013-08-11T00:00:00

Content: Breached on Data Enrichment Exposure From PDL Customer

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

Content: Breached on Neiman Marcus

Date/Year: 2024-04-14T00:00:00

Content: Breached on National Public Data

Date/Year: 2024-04-09T00:00:00

Content: Last Active (Google)

Date/Year: 2023-09-03T06:33:10

osint.industries