OSINT Industries

Report for: sarahluv1978@hotmail.com
As of 2024-08-22T18:26:30.267Z

Module Responses

NIKERUNCLUB

Registered : true
Id : b6f39898-b945-4bbe-a767-bee8d7cbb232
First Name : Sarah
Last Name : Troland
Username : SarahT833131052
Profile Url : http://my.nike.com/SarahT833131052
Private : false

MYFITNESSPAL

Registered : true

HIBP

Registered : true
Breach : true
Name : CoinTracker
Website : cointracker.io

Bio : In December 2022, the Crypto & NFT taxes service CoinTracker reported a data breach that impacted over 1.5M of their customers. The company later attributed the breach to a compromise SendGrid in an attack that targeted multiple customers of the email provider. The breach exposed email addresses and partially redacted phone numbers, with CoinTracker advising that the later did not originate from their service.
Creation Date : 2022-12-01T00:00:00

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.
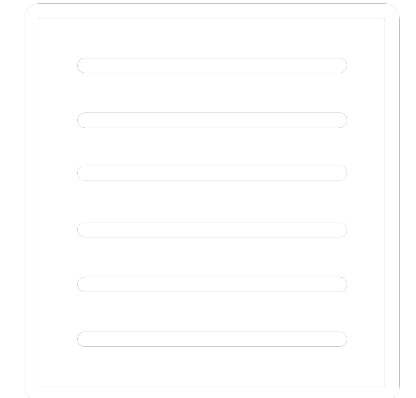**Creation Date** : 2019-10-16T00:00:00

Registered : true
Breach : true
Name : Modern Business Solutions
Website : modbsolutions.com
Bio : In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique

email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently attributed to "Modern Business Solutions", a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.

Creation Date : 2016-10-08T00:00:00

Registered : true

Breach : true

Name : MyFitnessPal

Website : myfitnesspal.com

Bio : In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Creation Date : 2018-02-01T00:00:00

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

Registered : true

Breach : true

Name : Not Acxiom

Bio : In 2020, a corpus of data containing almost a quarter of a billion records spanning over 400 different fields was misattributed to database marketing company Acxiom and subsequently circulated within the hacking community. On review, Acxiom concluded that "the claims are indeed false and that the data, which has been readily available across multiple environments, does not come from Acxiom and is in no way the subject of an Acxiom breach". The data contained almost 52M unique email addresses.
Creation Date : 2020-06-21T00:00:00
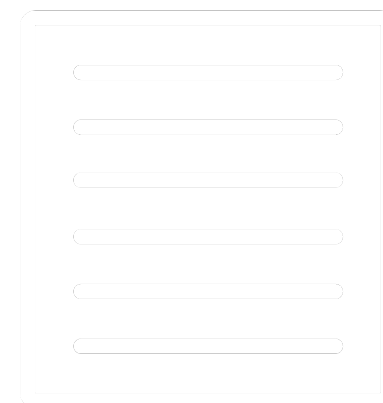
Registered : true

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. 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 : The Post Millennial

Website : thepostmillennial.com

Bio : In May 2024, the conservative news website The Post Millennial suffered a data breach. The breach resulted in the defacement of the website and links posted to 3 different corpuses of data including hundreds of writers and editors (IP, physical address and email exposed), tens of thousands of subscribers to the site (name, email, username, phone and plain text password exposed), and tens of millions of email addresses from thousands of mailing lists alleged to have been used by The Post Millennial (this has not been independently verified). The mailing lists appear to be sourced from various campaigns not necessarily run by The Post Millennial and contain a variety of different personal attributes including name, phone and physical address (depending on the campaign). The data was subsequently posted to a popular hacking forum and extensively torrented.

Creation Date : 2024-05-02T00:00:00

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

Registered : true

Breach : true

Name : Zynga

Website : zynga.com

Bio : In September 2019, game developer Zynga (the creator of Words with Friends) suffered a data breach. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.

Creation Date : 2019-09-01T00:00:00

NEXTDOOR

Registered : true

SPOTIFY

Registered : true

TALENT

Registered : true

CYBERBACKGROUNDCHECKS

Registered : true

Name : Sarah M Brunson

Age : 49

Location : 125 Eastwood Dr, Greenville, OH, 45331, US

Email : sarahmbrunson@yahoo.com, sarahluv1978@hotmail.com, diamond321@hotmail.com, derrick.patterson96@yahoo.com, go.fumc@voyager.net

Phone : (937) 459-5035, (937) 569-1688, (937) 548-4385, (313) 530-7658, (937) 547-9604, (832) 526-8630, (313) 299-0868, (219) 981-2232, (937) 548-9105

DISNEYSTORE

Registered : true

WIX

Registered : true

ESPN

Registered : true

PANDORA

Registered : true
Username : sarahluv1978
Profile Url : https://pandora.com/content/mobile/profile.vm?webname=sarahluv1978
Followers : 0
Following : 0

ZILLOW

Registered : true

MICROSOFT

Registered : true
Id : DBC6E8B0950DF655
Name : Sarah Troland
Location : US
Last Seen : 2024-08-15T07:49:23.343000+00:00
Creation Date : 2011-08-14T18:30:53.670000+00:00

PINTEREST

Registered : true

Timeline

Content: Breached on CoinTracker

Date/Year: 2022-12-01T00:00:00

Content: Breached on Data Enrichment Exposure From PDL Customer

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

Content: Breached on Modern Business Solutions

Date/Year: 2016-10-08T00:00:00

Content: Breached on MyFitnessPal

Date/Year: 2018-02-01T00:00:00

Content: Breached on National Public Data

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

Content: Breached on Not Acxiom

Date/Year: 2020-06-21T00:00:00

Content: Breached on River City Media Spam List

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

Content: Breached on The Post Millennial

Date/Year: 2024-05-02T00:00:00

Content: Breached on Verifications.io

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

Content: Breached on Zynga

Date/Year: 2019-09-01T00:00:00

Content: Last Active (Microsoft)

Date/Year: 2024-08-15T07:49:23.343000+00:00

Content: Created Account (Microsoft)

Date/Year: 2011-08-14T18:30:53.670000+00:00