OSINT Industries

Report for: bettyrushing68@yahoo.com

As of 2024-07-17T12:19:54.056Z

Map • Modules • Timeline

Map Outline

Module Responses

HIBP

Registered : true
Breach : true
Name : Advance Auto Parts
Website : advanceautoparts.com
Bio : In June 2024, Advance Auto Parts confirmed they had suffered a data breach which was posted for sale to a popular hacking forum. Linked to unauthorised access to Snowflake cloud services, the breach exposed a large number of records related to both customers and employees. In total, 79M unique email addresses were included in the breach, alongside names, phone numbers, addresses and further data attributes related to company employees.
Creation Date : 2024-06-05T00:00:00

Registered : true
Breach : true
Name : AT&T
Bio : In March 2024, tens of millions of records allegedly breached from AT&T were posted to a popular hacking forum. Dating back to August 2021, the data was originally posted for sale before later being freely released. At the time, AT&T maintained that there had not been a breach of their systems and that the data originated from elsewhere. 12 days later, AT&T acknowledged that data fields specific to them were in the breach and that it was not yet known whether the breach occurred at their end or that of a vendor. AT&T also proceeded to reset customer account passcodes, an indicator that there was sufficient belief passcodes had been compromised. The incident exposed names, email and physical addresses, dates of birth, phone numbers and US social security numbers.
Creation Date : 2021-08-20T00:00:00

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 : Home Chef
Website : homechef.com
Bio : In early 2020, the food delivery service Home Chef suffered a data breach which was subsequently sold online. The breach exposed the personal information of almost 9 million customers including names, IP addresses, post codes, the last 4 digits of credit card numbers and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.
Creation Date : 2020-02-10T00:00:00

Registered : true
Breach : true
Name : Mindjolt
Website : mindjolt.com
Bio : In March 2019, the online gaming website MindJolt suffered a data breach that exposed 28M unique email addresses. Also impacted were names and dates of birth, but no passwords. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date : 2019-03-18T00:00:00

Registered : true
Breach : true
Name : River City Media Spam List
Website : rivercitymediaonline.com
Bio : In January 2017, <a href="https://web.archive.org/web/20170426084052/https://mackeeper.com/blog/post/339-

spammergate-the-fall-of-an-empire" target="_blank" rel="noopener">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 : Special K Data Feed Spam List
Website : data4marketers.com
Bio : In mid to late 2015, a spam list known as the Special K Data Feed was discovered containing almost 31M identities. The data includes personal attributes such as names, physical and IP addresses, genders, birth dates and phone numbers. Read more about spam lists in HIBP.
Creation Date : 2015-10-07T00:00:00

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

DISQUS
Registered : true

DISNEYSTORE
Registered : true

ESPN
Registered : true

SMULE
Registered : true
Id : 211232602
Username : Rellabella
Profile Url : https://www.smule.com/Rellabella
Verified : false

PINTEREST
Registered : true

SPOTIFY
Registered : true

INSTACART
Registered : true

PANDORA

Registered : true
Username : bettyrushing68
Profile Url : https://pandora.com/content/mobile/profile.vm?webname=bettyrushing68
Followers : 0
Following : 0

MICROSOFT

Registered : true
Id : 11FF17F4ECFE29D0
Name : bettyrushing68@yahoo.com
Location : US
Last Seen : 2024-07-04T03:25:56.490000+00:00
Creation Date : 2017-08-31T20:51:13.150000+00:00

CYBERBACKGROUNDCHECKS

Registered : true
Name : Clarence Michael Rushing JR
Age : 69
Location : 2515 Highway 59 W, Covington, TN, 38019, US
Email : bettyrushing68@yahoo.com, djacka@bellsouth.net, rush12@bigriver.net, brushing@xipline.com
Phone : (901) 603-4188, (901) 296-5077, (901) 835-5623, (901) 872-2431, (901) 872-0772, (901) 872-4740, (901) 872-6095, (510) 236-2641, (901) 292-1850, (901) 873-1102, 872-4740

Timeline

Content: Breached on Advance Auto Parts
Date/Year: 2024-06-05T00:00:00

Content: Breached on AT&T
Date/Year: 2021-08-20T00:00:00

Content: Breached on Data Enrichment Exposure From PDL Customer
Date/Year: 2019-10-16T00:00:00

Content: Breached on Home Chef
Date/Year: 2020-02-10T00:00:00

Content: Breached on Mindjolt
Date/Year: 2019-03-18T00:00:00

Content: Breached on River City Media Spam List
Date/Year: 2017-01-01T00:00:00

Content: Breached on Special K Data Feed Spam List
Date/Year: 2015-10-07T00:00:00

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: Last Seen (Microsoft)
Date/Year: 2024-07-04T03:25:56.490000+00:00

Content: Created (Microsoft)
Date/Year: 2017-08-31T20:51:13.150000+00:00