OSINT Industries

Report for: glites07@yahoo.com
As of 2024-08-22T18:08:53.012Z

Map • Modules • Timeline

Module Responses

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 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 : 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

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 : Exactis
Website : exactis.com
Bio : In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis'

service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.
Creation Date : 2018-06-01T00:00:00

Registered : true
Breach : true
Name : Exploit.In
Bio : In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 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 : 2016-10-13T00:00:00

Registered : true
Breach : true
Name : Lead Hunter
Bio : In March 2020, a massive trove of personal information referred to as "Lead Hunter" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. The data contained 69 million unique email addresses across 110 million rows of data accompanied by additional personal information including names, phone numbers, genders and physical addresses. At the time of publishing, the breach could not be attributed to those responsible for obtaining and exposing it. The data was provided to HIBP by dehashed.com.
Creation Date : 2020-03-04T00:00:00

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 : MySpace
Website : myspace.com
Bio : In approximately 2008, 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 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 : 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 SOCRadar
Bio : In August 2024, over 332M rows of email addresses were posted to a popular hacking forum. The post alleged the addresses were scraped from cybersecurity firm SOCRadar, however an investigation on their behalf concluded that "the actor merely utilised functionalities inherent in the platform's standard offerings, designed to gather information from publicly available sources". There is no suggestion the incident compromised SOCRadar's security or posed any risk to their customers. In total, the data set contained 282M unique addresses of valid email address format.
Creation Date : 2024-08-03T00:00:00

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

MYSPACE

Registered : true

CYBERBACKGROUNDCHECKS

Registered : true
Name : Teresa Lee Bartlett
Age : 72
Location : 7812 Harlan Dr, White City, OR, 97503, US
Email : tlabartlett@yahoo.com, evansdm56@gmail.com, tlabartlett@aol.com, mbrook52544@aol.com, missashley18@hotmail.com, gunnarbartlett@gmail.com, lbartlett1@sbcglobal.net, glites07@yahoo.com, blackman785@gmail.com, blklstd1984@aol.com, naomi.bartlett@aol.com, tlabartlett@q.com
Phone : (319) 551-6805, (319) 363-9813, (319) 365-1964, (319) 551-7590, (319) 826-3543, (319) 202-6393, (319) 202-5424, (319) 551-6804

DISNEYSTORE

Registered : true

ESPN

Registered : true

Timeline

Content: Breached on Anti Public Combo List
Date/Year: 2016-12-16T00:00:00

Content: Breached on Collection #1
Date/Year: 2019-01-07T00:00:00

Content: Breached on Evite
Date/Year: 2013-08-11T00:00:00

Content: Breached on Exactis
Date/Year: 2018-06-01T00:00:00

Content: Breached on Exploit.In
Date/Year: 2016-10-13T00:00:00

Content: Breached on Lead Hunter
Date/Year: 2020-03-04T00:00:00

Content: Breached on Modern Business Solutions
Date/Year: 2016-10-08T00:00:00

Content: Breached on MySpace
Date/Year: 2008-07-01T00:00:00

Content: Breached on National Public Data
Date/Year: 2024-04-09T00:00:00

Content: Breached on Not SOCRadar
Date/Year: 2024-08-03T00:00:00

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