OSINT Industries

Report for: sarah-d-smith@live.com

As of 2024-08-22T19:35:45.433Z

Map • Modules • Timeline

Module Responses

GOOGLE

Registered : true
Id : 109866251541569410341
Last Seen : 2023-09-06T02:40:30

PICSART

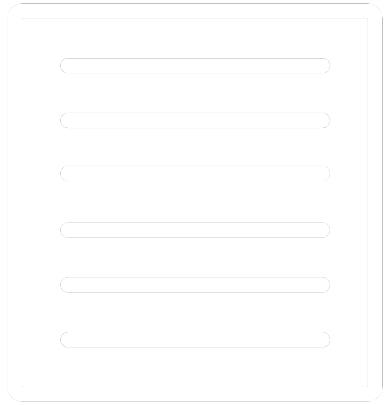
Registered : true
Id : 54612775
Name : Sarah Smith
Username : player_5814391
Profile Url : https://picsart.com/u/player_5814391
Followers : 0
Following : 0

LINKEDIN

Registered : true

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

cafemom

Name : CafeMom
Website : cafemom.com
Bio : In 2014, the social network for mothers CafeMom suffered a data breach. The data surfaced alongside a number of other historical breaches including Kickstarter, Bitly and Disqus and contained 2.6 million email addresses and plain text passwords.
Creation Date : 2014-04-10T00:00:00

Registered : true
Breach : true
Name : Coupon Mom / Armor Games
Bio : In 2014, a file allegedly containing data hacked from Coupon Mom was created and included 11 million email addresses and plain text passwords. On further investigation, the file was also found to contain data indicating it had been sourced from Armor Games. Subsequent verification with HIBP subscribers confirmed the passwords had previously been used and many subscribers had used either Coupon Mom or Armor Games in the past. On disclosure to both organisations, each found that the data did not represent their entire customer base and possibly includes records from other sources with common subscribers. The breach has subsequently been flagged as "unverified" as the source cannot be emphatically proven. In July 2020, the data was also found to contain BeerAdvocate accounts sourced from a previously unknown breach.
Creation Date : 2014-02-08T00:00:00

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 : Explore Talent (August 2024)
Website : exploretalent.com
Bio : In August 2024, a slew of security vulnerabilities were identified with a conglomerate of online services which included the talent network Explore Talent. A vulnerable API exposed the personal records of 11.4M users of the service of which 8.9M unique email addresses were provided to HIBP. This incident is separate to the Explore Talent breach which occurred in 2022 and was loaded into HIBP in July 2024.
Creation Date : 2024-08-15T00:00:00

Registered : true
Breach : true
Name : Gravatar
Website : gravatar.com
Bio : In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.
Creation Date : 2020-10-03T00:00:00

Registered : true
Breach : true
Name : Instant Checkmate
Website : instantcheckmate.com
Bio : In 2019, the public records search service Instant Checkmate suffered a data breach that later came to light in early 2023. The data included almost 12M unique customer email addresses, names, phone numbers and passwords stored as scrypt hashes.
Creation Date : 2019-04-12T00:00:00

Registered : true
Breach : true
Name : Mindjolt
Website : mindjolt.com
Bio : In March 2019, the online gaming website <a href="https://www.zdnet.com/article/a-hacker-has-

dumped-nearly-one-billion-user-records-over-the-past-two-months/" target="_blank" rel="noopener">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 : 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 <a href="https://www.troyhunt.com/dating-the-ginormous-myspace-breach" target="_blank"

rel="noopener">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 : Netlog
Website : netlog.com
Bio : In July 2018, the Belgian social networking site Netlog identified a data breach of their systems dating back to November 2012 (PDF). Although the service was discontinued in 2015, the data breach still impacted 49 million subscribers for whom email addresses and plain text passwords were exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date : 2012-11-01T00:00:00

Registered : true
Breach : true
Name : Onliner Spambot
Bio : In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moɈuƎq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.
Creation Date : 2017-08-28T00:00:00

Registered : true

Breach : true
Name : piZap
Website : pizap.com
Bio : In approximately December 2017, the online photo editing site piZap suffered a data breach. The data was later placed up for sale on a dark web marketplace along with a collection of other data breaches in February 2019. A total of 42 million unique email addresses were included in the breach alongside names, genders and links to Facebook profiles when the social media platform was used to authenticate to piZap. When accounts were created directly on piZap without using Facebook for authentication, passwords stored as SHA-1 hashes were also exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date : 2017-12-07T00:00:00

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 : Verifications.io
Website : verifications.io
Bio : In February 2019, the email address validation service <a href="https://securitydiscovery.com/800-

million-emails-leaked-online-by-email-verification-service" target="_blank" rel="noopener">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

NAPSTER

Registered : true profile
Id : B379A37F391DC7BAE040960A3903544D
Username : Colossal26828
Followers : 0
Following : 0
Private : false

MYSPACE

Registered : true

TWITTER

Registered : true

SAMSUNG

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

MICROSOFT

Registered : true
Id : 9FBC97D981D5CD30
Name : sarah smith
Location : US
Last Seen : 2019-04-25T23:12:14.017000+00:00
Creation Date : 2009-11-30T00:08:40.357000+00:00

MAPS

Registered : true
Profile Url : https://www.google.com/maps/contrib/109866251541569410341/reviews

YELP

Registered : true
Id : 0cKe6gJKPjU-_gbePoMDZQ
Name : sarah s.
First Name : sarah
Gender : f
Location : San Francisco, CA
Profile Url : https://www.yelp.com/user_details?userid=0cKe6gJKPjU-_gbePoMDZQ&utm_source=ishare
Followers : 0
Following : 0
Creation Date : 2010-10-22T05:58:28

Timeline

Content: Breached 4 times in 2019. (HaveIBeenPwnd!)
Date/Year: 2019

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

Content: Breached on CafeMom
Date/Year: 2014-04-10T00:00:00

Content: Breached on Coupon Mom / Armor Games
Date/Year: 2014-02-08T00:00:00

Content: Breached on Explore Talent (August 2024)
Date/Year: 2024-08-15T00:00:00

Content: Breached on Gravatar
Date/Year: 2020-10-03T00:00:00

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 Netlog
Date/Year: 2012-11-01T00:00:00

Content: Breached on Onliner Spambot
Date/Year: 2017-08-28T00:00:00

Content: Breached on piZap

Date/Year: 2017-12-07T00:00:00

Content: Breached on River City Media Spam List

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

Content: Last Active (Microsoft)

Date/Year: 2019-04-25T23:12:14.017000+00:00

Content: Created Account (Microsoft)

Date/Year: 2009-11-30T00:08:40.357000+00:00

Content: Last Active (Google)

Date/Year: 2023-09-06T02:40:30

Content: Created Account (Yelp)

Date/Year: 2010-10-22T05:58:28