Report for: info@ilovemysupertv.com

As of 2024-07-26T03:21:24.864Z

Minified and concise search report.

Module Responses:

HIBP

Picture Url

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
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: 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.
Title: Anti Public Combo List
Breach Count: 457962538

HIBP

Picture Url

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
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: 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.
Title: Data Enrichment Exposure From PDL Customer
Breach Count: 622161052

HIBP

Picture Url

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
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/LinkedIn.png
Website: linkedin.com
Description: 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.
Title: LinkedIn
Breach Count: 164611595

HIBP

Picture Url

Registered: true
Breach: true
Name: LinkedIn Scraped Data (2021)
Website: linkedin.com
Bio: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.
Creation Date: 2021-04-08T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/LinkedIn.png
Website: linkedin.com
Description: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.
Title: LinkedIn Scraped Data (2021)
Breach Count: 125698496

HIBP

Picture Url

Registered: true
Breach: true
Name: Trik Spam Botnet
Bio: In June 2018, the command and control server of a malicious botnet known as the "Trik Spam Botnet" was misconfigured such that it exposed the email addresses of more than 43 million people. The researchers who discovered the exposed Russian server believe the list of addresses was used to distribute various malware strains via malspam campaigns (emails designed to deliver

malware).
Creation Date: 2018-06-12T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Email.png
Description: In June 2018, the command and control server of a malicious botnet known as the "Trik Spam Botnet" was misconfigured such that it exposed the email addresses of more than 43 million people. The researchers who discovered the exposed Russian server believe the list of addresses was used to distribute various malware strains via malspam campaigns (emails designed to deliver malware).
Title: Trik Spam Botnet
Breach Count: 43432346

HIBP

Picture Url

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
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: 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.
Title: You've Been Scraped
Breach Count: 66147869

LINKEDIN

Registered: true
