OSINT Industries

Report for: **sathia.musso@gmail.com**

As of **2024-04-03T03:31:37.425Z**

Map • Modules • Timeline

Map Outline

Module Responses

GOOGLE

Registered: true
Id: 105120671917295944275
Name: S “ツ” F
First Name: S
Last Name: F
Last Seen: 2024-04-02T09:35:03

YOUTUBE

Registered: true
Id: UCPbG2Cs9ww2Oj9wh3bYor1g
Name: Sat_
Profile Url: https://www.youtube.com/channel/UCPbG2Cs9ww2Oj9wh3bYor1g
Creation Date: 2014-01-01T00:00:00

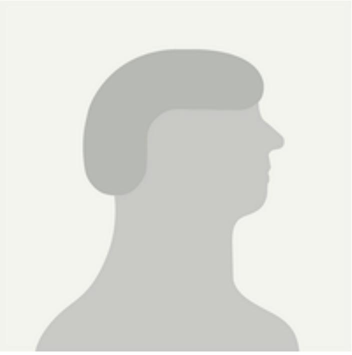
SKYPE

Registered: true
Id: sathia.musso
Location: Italy
Username: sathia.musso

CHESS

Registered: true
Id: 3978649
Location: Italy
Username: sathio
Profile Url: https://www.chess.com/member/sathio
Email Hint: s**********o@g***l.com
Last Seen: 2010-09-14T21:26:16
Creation Date: 2010-09-14T21:26:15

ETSY



Registered: true
Name: sathia

GRAVATAR

Registered: true
Id: sathio
Name: sathio
Username: sathio
Profile Url: https://gravatar.com/sathio
Banner Url: https://2.gravatar.com/avatar/3678e4fddd885112cd01763e2afcf8ee

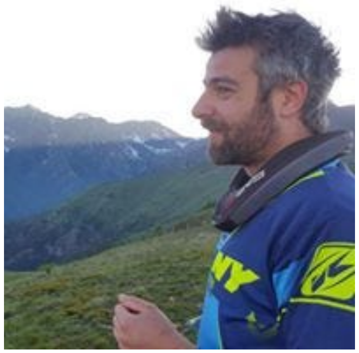
GITHUB

Registered: true
Id: 1990816

Name: Sathia
Username: sathio
Profile Url: https://github.com/sathio
Followers: 6
Following: 4
Last Seen: 2024-01-22T11:09:59+00:00
Creation Date: 2012-07-17T10:57:59+00:00

MEDIUM

Registered: true
Id: e75f11d8cdc
Name: Sat
Username: sathio
Profile Url: https://medium.com/@sathio
Followers: 31
Following: 43
Premium: false

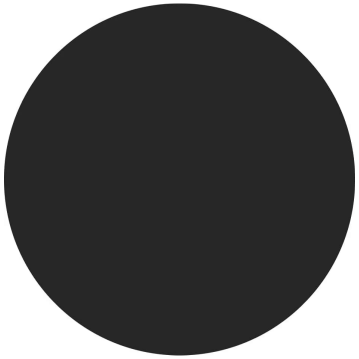


DROPBOX

Registered: true
Id: dbid:AABmIlDYpDCoyhhgsdc2OQiSauGgV9pj5UI
Name: sathio musso
First Name: sathio
Last Name: musso
Email: sathia.musso@gmail.com
Verified: true

AIRBNB

Registered: true
Id: 103328292
First Name: Sathia
Profile Url: https://www.airbnb.com/users/show/103328292
Verified: false
Creation Date: 2016-11-11T15:24:39+00:00



FITBIT

Registered: true
Id: 8N6TZG

Name: sathia m.
Profile Url: https://static0.fitbit.com/images/profile/defaultProfile_150.png

INSTAGRAM

Registered: true

APPLE

Registered: true
Phone Hint: ??? ??? ??85

MAPS

Registered: true
Profile Url: https://www.google.com/maps/contrib/105120671917295944275/reviews
Private: false

CRYPTOINTEL

Registered: true

Website: https://www.binance.com

MICROSOFT

Registered: true

Id: B7AA3EA05A0BD7E6

Name: sathia.musso sathia.musso

Location: IT

Last Seen: 2024-03-31T18:45:24.110000+00:00

Creation Date: 2022-03-18T20:47:58.567000+00:00

EMAILCHECKER

Registered: true

Website: firefox.com

Registered: true

Website: komoot.com

Registered: true
Website: imgur.com

Registered: true
Website: envato.com

Registered: true
Website: tumblr.com

Registered: true
Website: spotify.com

Registered: true
Website: zoho.com

Registered: true
Website: vimeo.com

Registered: true
Website: lastpass.com

Registered: true
Website: pinterest.com

Registered: true
Website: soundcloud.com

Registered: true

Website: giphy.com

Registered: true
Website: adobe.com

HIBP

Registered: true
Breach: true
Name: 2,844 Separate Data Breaches
Bio: In February 2018, a massive collection of almost 3,000 alleged data breaches was found online. Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single "unverified" data breach.
Creation Date: 2018-02-19T00:00:00

Registered: true
Breach: true
Name: Apollo
Website: apollo.io
Bio: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed

data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.
Creation Date: 2018-07-23T00:00:00

Registered: true
Breach: true
Name: Cit0day
Website: cit0day.in
Bio: In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.
Creation Date: 2020-11-04T00:00:00

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: 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: Deezer
Website: deezer.com
Bio: In late 2022, the music streaming service Deezer disclosed a data breach that impacted over 240M customers. The breach dated back to a mid-2019 backup exposed by a 3rd party partner which was subsequently sold and then broadly redistributed on a popular hacking forum. Impacted data included 229M unique email addresses, IP addresses, names, usernames, genders, DoBs and the geographic location of the customer.
Creation Date: 2019-04-22T00:00:00

Registered: true
Breach: true
Name: Dropbox
Website: dropbox.com
Bio: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Creation Date: 2012-07-01T00:00:00

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: 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: imgur
Website: imgur.com

Bio: In September 2013, the online image sharing community imgur suffered a data breach. A selection of the data containing 1.7 million email addresses and passwords surfaced more than 4 years later in November 2017. Although imgur stored passwords as SHA-256 hashes, the data in the breach contained plain text passwords suggesting that many of the original hashes had been cracked. imgur advises that they rolled over to bcrypt hashes in 2016.
Creation Date: 2013-09-01T00:00:00

Registered: true
Breach: true
Name: Kayo.moe Credential Stuffing List
Bio: In September 2018, a collection of almost 42 million email address and plain text password pairs was uploaded to the anonymous file sharing service kayo.moe. The operator of the service contacted HIBP to report the data which, upon further investigation, turned out to be a large credential stuffing list. For more information, read about The 42M Record kayo.moe Credential Stuffing Data.
Creation Date: 2018-09-11T00:00:00

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

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

Registered: true
Breach: true
Name: Naz.API
Bio: In September 2023, over 100GB of stealer logs and credential stuffing lists titled "Naz.API" was posted to a popular hacking forum. The incident contained a combination of email address and plain text password pairs alongside the service they were entered into, and standalone credential pairs obtained from unnamed sources. In total, the corpus of data included 71M unique email addresses and 100M unique passwords.
Creation Date: 2023-09-20T00:00:00

Registered: true
Breach: true
Name: Open Subtitles
Website: opensubtitles.org
Bio: In August 2021, the subtitling website Open Subtitles suffered a data breach and subsequent ransom demand. The breach exposed almost 7M subscribers' personal data including email and IP addresses, usernames, the country of the user and passwords stored as unsalted MD5 hashes.
Creation Date: 2021-08-01T00:00:00

Registered: true
Breach: true
Name: Trello
Website: trello.com
Bio: In January 2024, data was scraped from Trello and posted for sale on a popular hacking forum. Containing over 15M email addresses, names and usernames, the data was obtained by enumerating a publicly accessible resource using email addresses from previous breach corpuses. Trello advised that no unauthorised access had occurred.
Creation Date: 2024-01-16T00:00:00

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: 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

Timeline

Content: Last Seen (google)
Start: 2024-04-02T09:35:03

Content: Last Seen (microsoft)
Start: 2024-03-31T18:45:24.110000+00:00

Content: Last Seen (github)
Start: 2024-01-22T11:09:59+00:00

Content: Breached on Trello (HaveIBeenPwnd!)
Start: 2024-01-16T00:00:00
End: null

Content: Breached on Naz.API (HaveIBeenPwnd!)

Start: 2023-09-20T00:00:00
End: null

Content: Reviewed Fiscella Vincenzo (Google Maps)
Start: 2023-09-14T10:24:37
End: null

Content: Reviewed L'Osteria del Tarassaco (Google Maps)
Start: 2022-08-25T09:27:05
End: null

Content: Reviewed Ristorante Montepratello (Google Maps)
Start: 2022-08-22T11:47:45
End: null

Content: Reviewed Falegnameria Mirarchi Vincenzo (Google Maps)
Start: 2022-05-02T07:53:48
End: null

Content: Created Account (microsoft)
Start: 2022-03-18T20:47:58.567000+00:00

Content: Reviewed MOTORDON SRL (Google Maps)
Start: 2021-10-15T08:53:53
End: null

Content: Reviewed Pasticceria Uva (Google Maps)
Start: 2021-09-17T16:00:08
End: null

Content: Breached on Open Subtitles (HaveIBeenPwnd!)
Start: 2021-08-01T00:00:00
End: null

Content: Breached on LinkedIn Scraped Data (2021) (HaveIBeenPwnd!)
Start: 2021-04-08T00:00:00
End: null

Content: Breached on Cit0day (HaveIBeenPwnd!)
Start: 2020-11-04T00:00:00
End: null

Content: Breached on Gravatar (HaveIBeenPwnd!)
Start: 2020-10-03T00:00:00
End: null

Content: Reviewed Spreafico Cicli (Google Maps)
Start: 2020-09-10T07:19:37
End: null

Content: Reviewed Francesconi Planet Car Service (Google Maps)
Start: 2019-07-30T08:37:23
End: null

Content: Breached 4 times in 2019. (HaveIBeenPwnd!)
Start: Tue Jan 01 2019 00:00:00 GMT-0300 (Uruguay Standard Time)

Content: Breached 4 times in 2018. (HaveIBeenPwnd!)

Start: Mon Jan 01 2018 00:00:00 GMT-0300 (Uruguay Standard Time)

Content: Reviewed DAM Hairdressers Domenico Anna Martina (Google Maps)
Start: 2017-06-13T15:00:39
End: null

Content: Created Account (airbnb)
Start: 2016-11-11T15:24:39+00:00

Content: Breached on Exploit.In (HaveIBeenPwnd!)
Start: 2016-10-13T00:00:00
End: null

Content: Created Account (youtube)
Start: 2014-01-01T00:00:00

Content: Breached on imgur (HaveIBeenPwnd!)
Start: 2013-09-01T00:00:00
End: null

Content: Created Account (github)
Start: 2012-07-17T10:57:59+00:00

Content: Breached on Dropbox (HaveIBeenPwnd!)
Start: 2012-07-01T00:00:00
End: null

Content: Breached on LinkedIn (HaveIBeenPwnd!)
Start: 2012-05-05T00:00:00

End: null

Content: Last Seen (chess)
Start: 2010-09-14T21:26:16

Content: Created Account (chess)
Start: 2010-09-14T21:26:15

Map Outline

Module Responses

GOOGLE

Registered: true

Id: 105120671917295944275

Name: S “ツ” F

First Name: S

Last Name: F

Last Seen: 2024-04-02T09:35:03

YOUTUBE

Registered: true

Id: UCPbG2Cs9ww2Oj9wh3bYor1g

Name: Sat_

Profile Url: https://www.youtube.com/channel/UCPbG2Cs9ww2Oj9wh3bYor1g

Creation Date: 2014-01-01T00:00:00

SKYPE

Registered: true
Id: sathia.musso
Location: Italy
Username: sathia.musso

CHESS

Registered: true
Id: 3978649
Location: Italy
Username: sathio
Profile Url: https://www.chess.com/member/sathio
Email Hint: s**********o@g***l.com
Last Seen: 2010-09-14T21:26:16
Creation Date: 2010-09-14T21:26:15

ETSY

Registered: true
Name: sathia

GRAVATAR

Registered: true
Id: sathio
Name: sathio
Username: sathio
Profile Url: https://gravatar.com/sathio
Banner Url: https://2.gravatar.com/avatar/3678e4fddd885112cd01763e2afcf8ee

GITHUB

Registered: true
Id: 1990816

Name: Sathia
Username: sathio
Profile Url: https://github.com/sathio
Followers: 6
Following: 4
Last Seen: 2024-01-22T11:09:59+00:00
Creation Date: 2012-07-17T10:57:59+00:00

MEDIUM

Registered: true
Id: e75f11d8cdc
Name: Sat
Username: sathio
Profile Url: https://medium.com/@sathio
Followers: 31
Following: 43
Premium: false

DROPBOX

Registered: true
Id: dbid:AABmIlDYpDCoyhhgsdc2OQiSauGgV9pj5UI
Name: sathio musso
First Name: sathio
Last Name: musso
Email: sathia.musso@gmail.com
Verified: true

AIRBNB

Registered: true
Id: 103328292
First Name: Sathia
Profile Url: https://www.airbnb.com/users/show/103328292
Verified: false
Creation Date: 2016-11-11T15:24:39+00:00

FITBIT

Registered: true
Id: 8N6TZG

Name: sathia m.

Profile Url: https://static0.fitbit.com/images/profile/defaultProfile_150.png

INSTAGRAM

Registered: true

APPLE

Registered: true

Phone Hint: ??? ??? ??85

MAPS

Registered: true

Profile Url: https://www.google.com/maps/contrib/105120671917295944275/reviews

Private: false

CRYPTOINTEL

Registered: true
Website: https://www.binance.com

MICROSOFT

Registered: true
Id: B7AA3EA05A0BD7E6
Name: sathia.musso sathia.musso
Location: IT
Last Seen: 2024-03-31T18:45:24.110000+00:00
Creation Date: 2022-03-18T20:47:58.567000+00:00

EMAILCHECKER

Registered: true
Website: firefox.com

Registered: true
Website: komoot.com

Registered: true
Website: imgur.com

Registered: true
Website: envato.com

Registered: true
Website: tumblr.com

Registered: true
Website: spotify.com

Registered: true
Website: zoho.com

Registered: true
Website: vimeo.com

Registered: true
Website: lastpass.com

Registered: true
Website: pinterest.com

Registered: true
Website: soundcloud.com

Registered: true

Website: giphy.com

Registered: true
Website: adobe.com

HIBP

Registered: true
Breach: true
Name: 2,844 Separate Data Breaches
Bio: In February 2018, a massive collection of almost 3,000 alleged data breaches was found online. Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single "unverified" data breach.
Creation Date: 2018-02-19T00:00:00

Registered: true
Breach: true
Name: Apollo
Website: apollo.io
Bio: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed

data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.
Creation Date: 2018-07-23T00:00:00

Registered: true
Breach: true
Name: Cit0day
Website: cit0day.in
Bio: In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.
Creation Date: 2020-11-04T00:00:00

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: 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: Deezer
Website: deezer.com
Bio: In late 2022, the music streaming service Deezer disclosed a data breach that impacted over 240M customers. The breach dated back to a mid-2019 backup exposed by a 3rd party partner which was subsequently sold and then broadly redistributed on a popular hacking forum. Impacted data included 229M unique email addresses, IP addresses, names, usernames, genders, DoBs and the geographic location of the customer.
Creation Date: 2019-04-22T00:00:00

Registered: true
Breach: true
Name: Dropbox
Website: dropbox.com
Bio: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Creation Date: 2012-07-01T00:00:00

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: 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: imgur
Website: imgur.com

Bio: In September 2013, the online image sharing community imgur suffered a data breach. A selection of the data containing 1.7 million email addresses and passwords surfaced more than 4 years later in November 2017. Although imgur stored passwords as SHA-256 hashes, the data in the breach contained plain text passwords suggesting that many of the original hashes had been cracked. imgur advises that they rolled over to bcrypt hashes in 2016.
Creation Date: 2013-09-01T00:00:00

Registered: true
Breach: true
Name: Kayo.moe Credential Stuffing List
Bio: In September 2018, a collection of almost 42 million email address and plain text password pairs was uploaded to the anonymous file sharing service kayo.moe. The operator of the service contacted HIBP to report the data which, upon further investigation, turned out to be a large credential stuffing list. For more information, read about The 42M Record kayo.moe Credential Stuffing Data.
Creation Date: 2018-09-11T00:00:00

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

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

Registered: true
Breach: true
Name: Naz.API
Bio: In September 2023, over 100GB of stealer logs and credential stuffing lists titled "Naz.API" was posted to a popular hacking forum. The incident contained a combination of email address and plain text password pairs alongside the service they were entered into, and standalone credential pairs obtained from unnamed sources. In total, the corpus of data included 71M unique email addresses and 100M unique passwords.
Creation Date: 2023-09-20T00:00:00

Registered: true
Breach: true
Name: Open Subtitles
Website: opensubtitles.org
Bio: In August 2021, the subtitling website Open Subtitles suffered a data breach and subsequent ransom demand. The breach exposed almost 7M subscribers' personal data including email and IP addresses, usernames, the country of the user and passwords stored as unsalted MD5 hashes.
Creation Date: 2021-08-01T00:00:00

Registered: true
Breach: true
Name: Trello
Website: trello.com
Bio: In January 2024, data was scraped from Trello and posted for sale on a popular hacking forum. Containing over 15M email addresses, names and usernames, the data was obtained by enumerating a publicly accessible resource using email addresses from previous breach corpuses. Trello advised that no unauthorised access had occurred.
Creation Date: 2024-01-16T00:00:00

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: 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

Timeline

Content: Last Seen (google)
Start: 2024-04-02T09:35:03

Content: Last Seen (microsoft)
Start: 2024-03-31T18:45:24.110000+00:00

Content: Last Seen (github)
Start: 2024-01-22T11:09:59+00:00

Content: Breached on Trello (HaveIBeenPwnd!)
Start: 2024-01-16T00:00:00
End: null

Content: Breached on Naz.API (HaveIBeenPwnd!)

Start: 2023-09-20T00:00:00
End: null

Content: Reviewed Fiscella Vincenzo (Google Maps)
Start: 2023-09-14T10:24:37
End: null

Content: Reviewed L'Osteria del Tarassaco (Google Maps)
Start: 2022-08-25T09:27:05
End: null

Content: Reviewed Ristorante Montepratello (Google Maps)
Start: 2022-08-22T11:47:45
End: null

Content: Reviewed Falegnameria Mirarchi Vincenzo (Google Maps)
Start: 2022-05-02T07:53:48
End: null

Content: Created Account (microsoft)
Start: 2022-03-18T20:47:58.567000+00:00

Content: Reviewed MOTORDON SRL (Google Maps)
Start: 2021-10-15T08:53:53
End: null

Content: Reviewed Pasticceria Uva (Google Maps)
Start: 2021-09-17T16:00:08
End: null

Content: Breached on Open Subtitles (HaveIBeenPwnd!)
Start: 2021-08-01T00:00:00
End: null

Content: Breached on LinkedIn Scraped Data (2021) (HaveIBeenPwnd!)
Start: 2021-04-08T00:00:00
End: null

Content: Breached on Cit0day (HaveIBeenPwnd!)
Start: 2020-11-04T00:00:00
End: null

Content: Breached on Gravatar (HaveIBeenPwnd!)
Start: 2020-10-03T00:00:00
End: null

Content: Reviewed Spreafico Cicli (Google Maps)
Start: 2020-09-10T07:19:37
End: null

Content: Reviewed Francesconi Planet Car Service (Google Maps)
Start: 2019-07-30T08:37:23
End: null

Content: Breached 4 times in 2019. (HaveIBeenPwnd!)
Start: Tue Jan 01 2019 00:00:00 GMT-0300 (Uruguay Standard Time)

Content: Breached 4 times in 2018. (HaveIBeenPwnd!)

Start: Mon Jan 01 2018 00:00:00 GMT-0300 (Uruguay Standard Time)

Content: Reviewed DAM Hairdressers Domenico Anna Martina (Google Maps)
Start: 2017-06-13T15:00:39
End: null

Content: Created Account (airbnb)
Start: 2016-11-11T15:24:39+00:00

Content: Breached on Exploit.In (HaveIBeenPwnd!)
Start: 2016-10-13T00:00:00
End: null

Content: Created Account (youtube)
Start: 2014-01-01T00:00:00

Content: Breached on imgur (HaveIBeenPwnd!)
Start: 2013-09-01T00:00:00
End: null

Content: Created Account (github)
Start: 2012-07-17T10:57:59+00:00

Content: Breached on Dropbox (HaveIBeenPwnd!)
Start: 2012-07-01T00:00:00
End: null

Content: Breached on LinkedIn (HaveIBeenPwnd!)
Start: 2012-05-05T00:00:00

End: null

Content: Last Seen (chess)
Start: 2010-09-14T21:26:16

Content: Created Account (chess)
Start: 2010-09-14T21:26:15

osint.industries