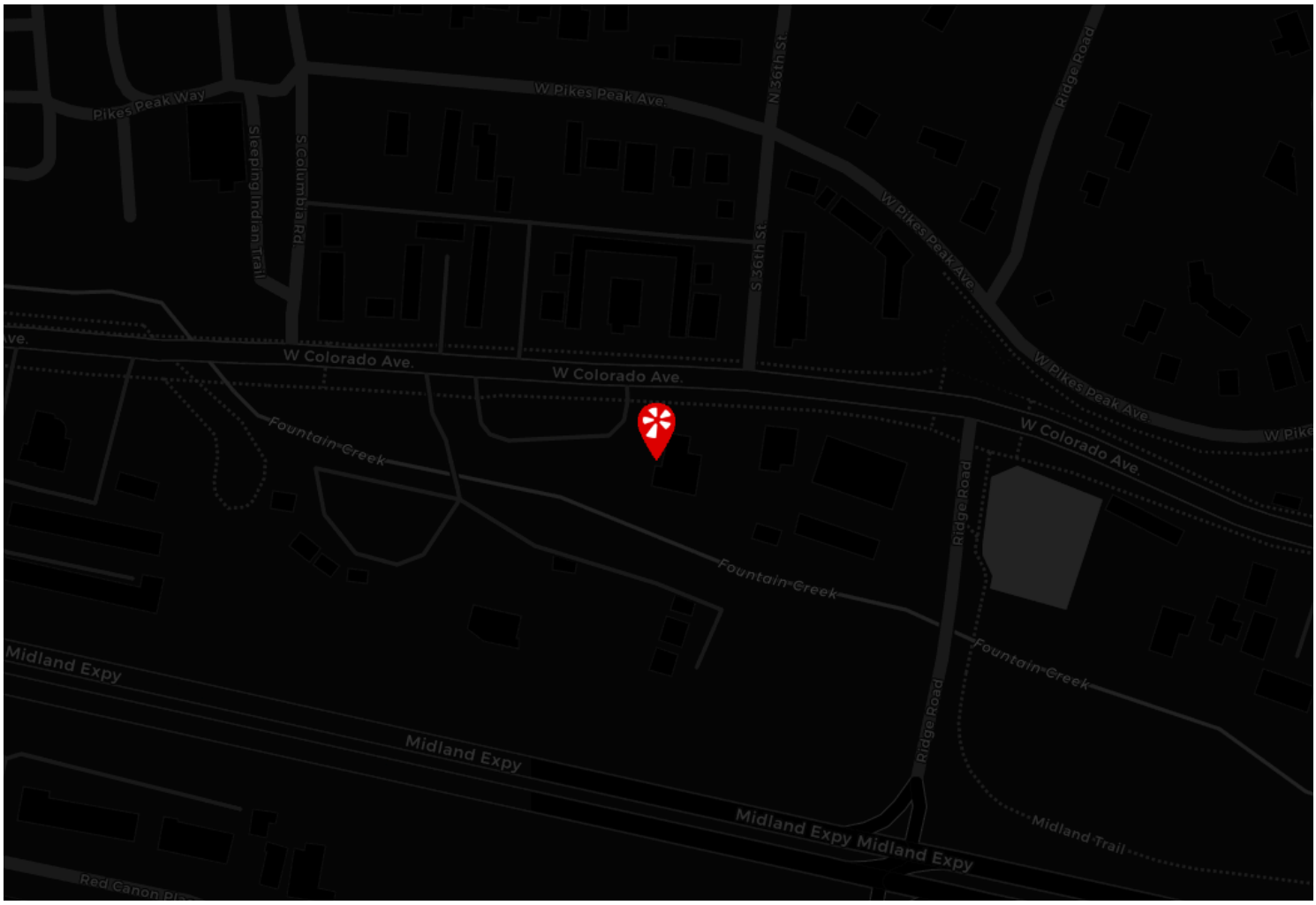
OSINT Industries

Report for: **hmsih@yahoo.com**

As of **2024-04-21T08:53:20.967Z**

Map • Modules • Timeline

Map Outline



Module Responses

GOOGLE

Registered: true
Id: 114156180893589396037

ETSY

Registered: true
Name: melinda

FOURSQUARE

Registered: true
Id: 981183
First Name: Melinda
Last Name: Sih
Gender: female
Location: US
Username: melindas4438457
Profile Url: https://foursquare.com/melindas4438457
Private: false

AIRBNB

Registered: true
Id: 69066357
First Name: Melinda
Profile Url: https://www.airbnb.com/users/show/69066357
Verified: false
Creation Date: 2016-04-26T19:40:01+00:00

FACEBOOK

Registered: true

NIKERUNCLUB

Registered: true
Id: d6cdf964-483c-4692-9b93-692fb41a1310
First Name: melinda
Last Name: sih
Username: melindas216793914
Profile Url: http://my.nike.com/melindas216793914
Private: false

FITBIT

Registered: true
Id: 286MQN
Name: hmsih
Profile Url: https://static0.fitbit.com/images/profile/defaultProfile_150.png

MYFITNESSPAL

Registered: true
Id: 7825804539915185124
Location: US
Creation Date: 2016-05-15T13:22:13.039000+00:00

INSTAGRAM

Registered: true

ASKFM

Registered: true
Name: mmcs
Language: en
Username: mmcs1989
Profile Url: https://ask.fm/mmcs1989
Verified: false

APPLE

Registered: true

MICROSOFT

Registered: true
Id: FEA69C11D7BDBEC0
Name: hmsih@yahoo.com
Location: US
Last Seen: 2024-01-13T07:05:21.120000+00:00
Creation Date: 2016-08-20T21:48:16.780000+00:00

YELP

Registered: true
Id: i84Ci79wGy7YbEMIaoyfgQ
Name: Melinda S.
First Name: Melinda
Gender: f
Location: Prairie Village, KS
Profile Url: https://www.yelp.com/user_details?userid=i84Ci79wGy7YbEMIaoyfgQ&utm_source=ishare
Followers: 0
Following: 0
Creation Date: 2016-06-12T01:01:38

EMAILCHECKER

Registered: true
Website: nextdoor.com

Registered: true
Website: bitmoji.com

Registered: true
Website: pinterest.com

Registered: true
Website: realtor.com

Registered: true
Website: change.org

Registered: true
Website: remind.com

Registered: true
Website: caringbridge.org

Registered: true
Website: uber.com

HIBP

Registered: true
Breach: true
Name: 8tracks
Website: 8tracks.com
Bio: In June 2017, the online playlists service known as 8Tracks suffered a data breach which impacted 18 million accounts. In their disclosure, 8Tracks advised that "the vector for the attack was an employee's GitHub account, which was not secured using two-factor authentication". Salted SHA-1 password hashes for users who *didn't* sign up with either Google or Facebook authentication were also included. The data was provided to HIBP by whitehat security researcher and data analyst Adam Davies and contained almost 8 million unique email addresses. The complete set of 18M records was later provided by JimScott.Sec@protonmail.com and updated in HIBP accordingly.
Creation Date: 2017-06-27T00:00:00

Registered: true
Breach: true
Name: Animoto
Website: animoto.com
Bio: In July 2018, the cloud-based video making service Animoto suffered a data breach. The breach exposed 22 million unique email addresses alongside names, dates of birth, country of origin and salted password hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date: 2018-07-10T00:00:00

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: 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: B2B USA Businesses
Bio: In mid-2017, a spam list of over 105 million individuals in corporate America was discovered online. Referred to as "B2B USA Businesses", the list categorised email addresses by employer, providing information on individuals' job titles plus their work phone numbers and physical addresses. Read more about spam lists in HIBP.
Creation Date: 2017-07-18T00:00:00

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 & Leads
Website: datanleads.com
Bio: In November 2018, security researcher Bob Diachenko identified an unprotected database believed to be hosted by a data aggregator. Upon further investigation, the data was linked to marketing company Data & Leads. The exposed Elasticsearch instance contained over 44M unique email addresses along with

names, IP and physical addresses, phone numbers and employment information. No response was received from Data & Leads when contacted by Bob and their site subsequently went offline.
Creation Date: 2018-11-14T00:00:00

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: 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: HauteLook
Website: hautelook.com
Bio: In mid-2018, the fashion shopping site HauteLook was among a raft of sites that were breached and their data then sold in early-2019. The data included over 28 million unique email addresses alongside names, genders, dates of birth and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.
Creation Date: 2018-08-07T00:00:00

Registered: true
Breach: true
Name: Luxottica
Website: luxottica.com
Bio: In March 2021, the world's largest eyewear company Luxoticca suffered a data breach via one of their partners that exposed the personal information of more than 70M people. The data was subsequently sold via a popular hacking forum in late 2022 and included email and physical addresses, names, genders, dates of birth and phone numbers. In a statement from Luxottica, they advised they were aware of the incident and are currently "considering other notification obligations".
Creation Date: 2021-03-16T00:00:00

Registered: true
Breach: true
Name: MyFitnessPal
Website: myfitnesspal.com
Bio: In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".
Creation Date: 2018-02-01T00:00:00

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: Poshmark
Website: poshmark.com
Bio: In mid-2018, social commerce marketplace Poshmark suffered a data breach that exposed 36M user accounts. The compromised data included email addresses, names, usernames, genders, locations and passwords stored as bcrypt hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date: 2018-05-16T00:00:00

Registered: true
Breach: true
Name: SHEIN
Website: shein.com
Bio: In June 2018, online fashion retailer SHEIN suffered a data breach. The company discovered the breach 2 months later in August then disclosed the incident another month after that. A total of 39 million

unique email addresses were found in the breach alongside MD5 password hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date: 2018-06-01T00:00:00

Registered: true
Breach: true
Name: Straffic
Website: straffic.io
Bio: In February 2020, Israeli marketing company Straffic exposed a database with 140GB of personal data. The publicly accessible Elasticsearch database contained over 300M rows with 49M unique email addresses. Exposed data also included names, phone numbers, physical addresses and genders. In their breach disclosure message, Straffic stated that "it is impossible to create a totally immune system, and these things can occur".
Creation Date: 2020-02-14T00:00:00

Registered: true
Breach: true
Name: Ticketfly
Website: ticketfly.com
Bio: In May 2018, the website for the ticket distribution service Ticketfly was defaced by an attacker and was subsequently taken offline. The attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a reply and subsequently posted the breached data online to a publicly accessible location. The data included over 26 million unique email addresses along with names, physical addresses and phone numbers. Whilst there were no passwords in the publicly leaked data, Ticketfly later issued an incident update and stated that "It is possible, however, that hashed values of password credentials could have been accessed".
Creation Date: 2018-05-31T00:00:00

Registered: true
Breach: true
Name: Twitter (200M)
Website: twitter.com
Bio: In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.
Creation Date: 2021-01-01T00:00:00

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: Wanelo
Website: wanelo.com
Bio: In approximately December 2018, the digital mall Wanelo 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 April 2019. A total of 23 million unique email addresses were included in the breach alongside passwords stored as either MD5 or bcrypt hashes. After the initial HIBP load, further data containing names, shipping addresses and IP addresses were also provided to HIBP, albeit without direct association to the email addresses and passwords. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date: 2018-12-13T00:00:00

Timeline

Content: Last Seen (microsoft)
Start: 2024-01-13T07:05:21.120000+00:00

Content: Breached on AT&T (HaveIBeenPwnd!)
Start: 2021-08-20T00:00:00
End: null

Content: Breached on Luxottica (HaveIBeenPwnd!)
Start: 2021-03-16T00:00:00
End: null

Content: Breached on Twitter (200M) (HaveIBeenPwnd!)
Start: 2021-01-01T00:00:00
End: null

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

Content: Breached on Straffic (HaveIBeenPwnd!)
Start: 2020-02-14T00:00:00
End: null

Content: Breached on Data Enrichment Exposure From PDL Customer (HaveIBeenPwnd!)

Start: 2019-10-16T00:00:00
End: null

Content: Breached on Verifications.io (HaveIBeenPwnd!)
Start: 2019-02-25T00:00:00
End: null

Content: Breached on Collection #1 (HaveIBeenPwnd!)
Start: 2019-01-07T00:00:00
End: null

Content: Breached 8 times in 2018. (HaveIBeenPwnd!)
Start: Mon Jan 01 2018 00:00:00 GMT+0900 (Japan Standard Time)

Content: Breached on Onliner Spambot (HaveIBeenPwnd!)
Start: 2017-08-28T00:00:00
End: null

Content: Breached on B2B USA Businesses (HaveIBeenPwnd!)
Start: 2017-07-18T00:00:00
End: null

Content: Breached on 8tracks (HaveIBeenPwnd!)
Start: 2017-06-27T00:00:00
End: null

Content: Breached on Anti Public Combo List (HaveIBeenPwnd!)
Start: 2016-12-16T00:00:00
End: null

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

Content: Created Account (microsoft)
Start: 2016-08-20T21:48:16.780000+00:00

Content: Reviewed Amanda's Fonda. (Yelp)
Start: 2016-06-12T01:01:46
End: null

Content: Created Account (yelp)
Start: 2016-06-12T01:01:38

Content: Created Account (myfitnesspal)
Start: 2016-05-15T13:22:13.039000+00:00

Content: Created Account (airbnb)
Start: 2016-04-26T19:40:01+00:00

Map Outline

Module Responses

GOOGLE

Registered: true
Id: 114156180893589396037

ETSY

Registered: true
Name: melinda

FOURSQUARE

Registered: true
Id: 981183
First Name: Melinda
Last Name: Sih
Gender: female
Location: US
Username: melindas4438457
Profile Url: https://foursquare.com/melindas4438457
Private: false

AIRBNB

Registered: true
Id: 69066357
First Name: Melinda
Profile Url: https://www.airbnb.com/users/show/69066357
Verified: false
Creation Date: 2016-04-26T19:40:01+00:00

FACEBOOK

Registered: true

NIKERUNCLUB

Registered: true
Id: d6cdf964-483c-4692-9b93-692fb41a1310

First Name: melinda
Last Name: sih
Username: melindas216793914
Profile Url: http://my.nike.com/melindas216793914
Private: false

FITBIT

Registered: true
Id: 286MQN
Name: hmsih
Profile Url: https://static0.fitbit.com/images/profile/defaultProfile_150.png

MYFITNESSPAL

Registered: true
Id: 7825804539915185124
Location: US
Creation Date: 2016-05-15T13:22:13.039000+00:00

INSTAGRAM

Registered: true

ASKFM

Registered: true
Name: mmcs
Language: en
Username: mmcs1989
Profile Url: https://ask.fm/mmcs1989
Verified: false

APPLE

Registered: true

MICROSOFT

Registered: true
Id: FEA69C11D7BDBEC0
Name: hmsih@yahoo.com
Location: US
Last Seen: 2024-01-13T07:05:21.120000+00:00
Creation Date: 2016-08-20T21:48:16.780000+00:00

YELP

Registered: true
Id: i84Ci79wGy7YbEMIaoyfgQ
Name: Melinda S.
First Name: Melinda
Gender: f
Location: Prairie Village, KS
Profile Url: https://www.yelp.com/user_details?userid=i84Ci79wGy7YbEMIaoyfgQ&utm_source=ishare
Followers: 0
Following: 0
Creation Date: 2016-06-12T01:01:38

EMAILCHECKER

Registered: true
Website: nextdoor.com

Registered: true
Website: bitmoji.com

Registered: true
Website: pinterest.com

Registered: true
Website: realtor.com

Registered: true
Website: change.org

Registered: true

Website: remind.com

Registered: true
Website: caringbridge.org

Registered: true
Website: uber.com

HIBP

Registered: true
Breach: true
Name: 8tracks
Website: 8tracks.com
Bio: In June 2017, the online playlists service known as 8Tracks suffered a data breach which impacted 18 million accounts. In their disclosure, 8Tracks advised that "the vector for the attack was an employee's GitHub account, which was not secured using two-factor authentication". Salted SHA-1 password hashes for users who *didn't* sign up with either Google or Facebook authentication were also included. The data was provided to HIBP by whitehat security researcher and data analyst Adam Davies and contained almost 8 million unique email addresses. The complete set of 18M records was later provided by JimScott.Sec@protonmail.com and updated in HIBP accordingly.
Creation Date: 2017-06-27T00:00:00

Registered: true
Breach: true
Name: Animoto
Website: animoto.com
Bio: In July 2018, the cloud-based video making service Animoto suffered a data breach. The breach exposed 22 million unique email addresses alongside names, dates of birth, country of origin and salted password hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date: 2018-07-10T00:00:00

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: 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: B2B USA Businesses
Bio: In mid-2017, a spam list of over 105 million individuals in corporate America was discovered online. Referred to as "B2B USA Businesses", the list categorised email addresses by employer, providing information on individuals' job titles plus their work phone numbers and physical addresses. Read more about spam lists in HIBP.
Creation Date: 2017-07-18T00:00:00

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 & Leads
Website: datanleads.com
Bio: In November 2018, security researcher Bob Diachenko identified an unprotected database believed to be hosted by a data aggregator. Upon further investigation, the data was linked to marketing company Data & Leads. The exposed Elasticsearch instance contained over 44M unique email addresses along with names, IP and physical addresses, phone numbers and employment information. No response was received from Data & Leads when contacted by Bob and their site subsequently went offline.
Creation Date: 2018-11-14T00:00:00

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: 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: HauteLook
Website: hautelook.com
Bio: In mid-2018, the fashion shopping site HauteLook was among a raft of sites that were breached and their data then sold in early-2019. The data included over 28 million unique email addresses alongside names, genders, dates of birth and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.
Creation Date: 2018-08-07T00:00:00

Registered: true
Breach: true
Name: Luxottica
Website: luxottica.com
Bio: In March 2021, the world's largest eyewear company Luxoticca suffered a data breach via one of their partners that exposed the personal information of more than 70M people. The data was subsequently sold via a popular hacking forum in late 2022 and included email and physical addresses, names, genders, dates of birth and phone numbers. In a statement from Luxottica, they advised they were aware of the incident and are currently "considering other notification obligations".
Creation Date: 2021-03-16T00:00:00

Registered: true
Breach: true
Name: MyFitnessPal
Website: myfitnesspal.com
Bio: In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as

SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".
Creation Date: 2018-02-01T00:00:00

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: Poshmark
Website: poshmark.com
Bio: In mid-2018, social commerce marketplace Poshmark suffered a data breach that exposed 36M user accounts. The compromised data included email addresses, names, usernames, genders, locations and passwords stored as bcrypt hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date: 2018-05-16T00:00:00

Registered: true
Breach: true
Name: SHEIN
Website: shein.com
Bio: In June 2018, online fashion retailer SHEIN suffered a data breach. The company discovered the breach 2 months later in August then disclosed the incident another month after that. A total of 39 million unique email addresses were found in the breach alongside MD5 password hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date: 2018-06-01T00:00:00

Registered: true
Breach: true
Name: Straffic
Website: straffic.io
Bio: In February 2020, Israeli marketing company Straffic exposed a database with 140GB of personal data. The publicly accessible Elasticsearch database contained over 300M rows with 49M unique email addresses. Exposed data also included names, phone numbers, physical addresses and genders. In their breach disclosure message, Straffic stated that "it is impossible to create a totally immune system, and these things can occur".
Creation Date: 2020-02-14T00:00:00

Registered: true

Breach: true
Name: Ticketfly
Website: ticketfly.com
Bio: In May 2018, the website for the ticket distribution service Ticketfly was defaced by an attacker and was subsequently taken offline. The attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a reply and subsequently posted the breached data online to a publicly accessible location. The data included over 26 million unique email addresses along with names, physical addresses and phone numbers. Whilst there were no passwords in the publicly leaked data, Ticketfly later issued an incident update and stated that "It is possible, however, that hashed values of password credentials could have been accessed".
Creation Date: 2018-05-31T00:00:00

Registered: true
Breach: true
Name: Twitter (200M)
Website: twitter.com
Bio: In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.
Creation Date: 2021-01-01T00:00:00

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: Wanelo
Website: wanelo.com
Bio: In approximately December 2018, the digital mall Wanelo 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 April 2019. A total of 23 million unique email addresses were included in the breach alongside passwords stored as either MD5 or bcrypt hashes. After the initial HIBP load, further data containing names, shipping addresses and IP addresses were also provided to HIBP, albeit without direct association to the email addresses and passwords. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date: 2018-12-13T00:00:00

Timeline

Content: Last Seen (microsoft)
Start: 2024-01-13T07:05:21.120000+00:00

Content: Breached on AT&T (HaveIBeenPwnd!)
Start: 2021-08-20T00:00:00
End: null

Content: Breached on Luxottica (HaveIBeenPwnd!)
Start: 2021-03-16T00:00:00
End: null

Content: Breached on Twitter (200M) (HaveIBeenPwnd!)
Start: 2021-01-01T00:00:00
End: null

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

Content: Breached on Straffic (HaveIBeenPwnd!)
Start: 2020-02-14T00:00:00
End: null

Content: Breached on Data Enrichment Exposure From PDL Customer (HaveIBeenPwnd!)
Start: 2019-10-16T00:00:00
End: null

Content: Breached on Verifications.io (HaveIBeenPwnd!)
Start: 2019-02-25T00:00:00
End: null

Content: Breached on Collection #1 (HaveIBeenPwnd!)
Start: 2019-01-07T00:00:00
End: null

Content: Breached 8 times in 2018. (HaveIBeenPwnd!)
Start: Mon Jan 01 2018 00:00:00 GMT+0900 (Japan Standard Time)

Content: Breached on Onliner Spambot (HaveIBeenPwnd!)
Start: 2017-08-28T00:00:00
End: null

Content: Breached on B2B USA Businesses (HaveIBeenPwnd!)
Start: 2017-07-18T00:00:00
End: null

Content: Breached on 8tracks (HaveIBeenPwnd!)
Start: 2017-06-27T00:00:00

End: null

Content: Breached on Anti Public Combo List (HaveIBeenPwnd!)
Start: 2016-12-16T00:00:00
End: null

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

Content: Created Account (microsoft)
Start: 2016-08-20T21:48:16.780000+00:00

Content: Reviewed Amanda's Fonda. (Yelp)
Start: 2016-06-12T01:01:46
End: null

Content: Created Account (yelp)
Start: 2016-06-12T01:01:38

Content: Created Account (myfitnesspal)
Start: 2016-05-15T13:22:13.039000+00:00

Content: Created Account (airbnb)
Start: 2016-04-26T19:40:01+00:00