Report for: minerbubs1234@gmail.com

As of 2024-11-24T00:55:34.765Z

Minified and concise search report.

Module Responses:

SPOTIFY

Registered: true

GRAVATAR

Picture Url
Profile Url
Banner Url

Registered: true
Id: minerbubs1234
Name: vu5
Username: minerbubs1234

ADOBE

Registered: true
Status: active
Type: individual

GIPHY

INSTAGRAM

REPLIT

KHANACADEMY

Picture Url
Profile Url

Registered: true
Id: kaid_383520251376558996219868
Name: minerbubs1234
Username: minerbubs1234
Points: 0

ACTIVISION

CALLOFDUTY

WORDPRESS

DISQUS

HIBP

Picture Url

Registered: true

Breach: true

Name: DLH.net

Website: dlh.net

Bio: In July 2016, the gaming news site <a href="http://www.zdnet.com/article/millions-of-steam-game-keys-stolen-after-site-hack/" target="_blank" rel="noopener">DLH.net suffered a data breach</a> which exposed 3.3M subscriber identities. Along with the keys used to redeem and activate games on the Steam platform, the breach also resulted in the exposure of email addresses, birth dates and salted MD5 password hashes. The data was donated to Have I Been Pwned by data breach monitoring service <a href="https://vigilante.pw/" target="_blank" rel="noopener">Vigilante.pw</a>.

Creation Date: 2016-07-31T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/DLH.png

Website: dlh.net

Description: In July 2016, the gaming news site <a href="http://www.zdnet.com/article/millions-of-steam-game-keys-stolen-after-site-hack/" target="_blank" rel="noopener">DLH.net suffered a data breach</a> which exposed 3.3M subscriber identities. Along with the keys used to redeem and activate games on the Steam platform, the breach also resulted in the exposure of email addresses, birth dates and salted MD5 password hashes. The data was donated to Have I Been Pwned by data breach monitoring service <a href="https://vigilante.pw/" target="_blank" rel="noopener">Vigilante.pw</a>.

Title: DLH.net

Breach Count: 3264710

HIBP

Picture Url

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 <em>billion</em> 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 <a href="https://www.troyhunt.com/the-773-million-record-collection-1-data-reach" target="_blank" rel="noopener">The 773 Million Record "Collection #1" Data Breach</a>.

Creation Date: 2019-01-07T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png

Description: 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 <em>billion</em> 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 <a href="https://www.troyhunt.com/the-773-million-record-collection-1-data-reach" target="_blank" rel="noopener">The 773 Million Record "Collection #1" Data Breach</a>.
Title: Collection #1
Breach Count: 772904991

HIBP

Picture Url

Registered: true
Breach: true
Name: Club Penguin Rewritten (January 2018)
Website: cprewritten.net
Bio: In January 2018, the children's gaming site <a href="https://community.cprewritten.net/" target="_blank" rel="noopener">Club Penguin Rewritten</a> (CPRewritten) suffered a data breach (note: CPRewritten is an independent recreation of Disney's Club Penguin game). The incident exposed almost 1.7 million unique email addresses alongside IP addresses, usernames and passwords stored as bcrypt hashes. When contacted, CPRewritten advised they were aware of the breach and had &quot;contacted affected users&quot;.
Creation Date: 2018-01-21T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/ClubPenguinRewritten.png
Website: cprewritten.net
Description: In January 2018, the children's gaming site <a href="https://community.cprewritten.net/" target="_blank" rel="noopener">Club Penguin Rewritten</a> (CPRewritten) suffered a data breach (note: CPRewritten is an independent recreation of Disney's Club Penguin game). The incident exposed almost 1.7 million unique email addresses alongside IP addresses, usernames and passwords stored as bcrypt hashes. When contacted, CPRewritten advised they were aware of the breach and had &quot;contacted affected users&quot;.
Title: Club Penguin Rewritten (January 2018)
Breach Count: 1688176

HIBP

Picture Url

Registered: true
Breach: true
Name: Club Penguin Rewritten (July 2019)
Website: cprewritten.net
Bio: In July 2019, the children's gaming site <a href="https://community.cprewritten.net/" target="_blank" rel="noopener">Club Penguin Rewritten</a> (CPRewritten) suffered a data breach (note: CPRewritten is an independent recreation of Disney's Club Penguin game). In addition to an earlier data breach that impacted 1.7 million accounts, the subsequent breach exposed 4 million unique email addresses alongside IP addresses, usernames and passwords stored as bcrypt hashes.

Creation Date: 2019-07-27T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/ClubPenguinRewritten.png

Website: cprewritten.net

Description: In July 2019, the children's gaming site <a href="https://community.cprewritten.net/" target="_blank" rel="noopener">Club Penguin Rewritten</a> (CPRewritten) suffered a data breach (note: CPRewritten is an independent recreation of Disney's Club Penguin game). In addition to an earlier data breach that impacted 1.7 million accounts, the subsequent breach exposed 4 million unique email addresses alongside IP addresses, usernames and passwords stored as bcrypt hashes.

Title: Club Penguin Rewritten (July 2019)

Breach Count: 4007909

HIBP

Picture Url

Registered: true

Breach: true

Name: Canva

Website: canva.com

Bio: In May 2019, the graphic design tool website <a href="https://support.canva.com/contact/customer-support/may-24-security-incident-faqs/" target="_blank" rel="noopener">Canva suffered a data breach</a> that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Creation Date: 2019-05-24T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Canva.png

Website: canva.com

Description: In May 2019, the graphic design tool website <a href="https://support.canva.com/contact/customer-support/may-24-security-incident-faqs/" target="_blank" rel="noopener">Canva suffered a data breach</a> that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Title: Canva

Breach Count: 137272116

HIBP

Picture Url

Registered: true

Breach: true

Name: Cracked.to

Website: cracked.to

Bio: In July 2019, the hacking website <a href="https://cracked.to" target="_blank" rel="noopener">Cracked.to</a> suffered a data breach. There were 749k unique email addresses spread across 321k forum users and other tables in the database. A rival hacking website claimed responsibility for breaching the MyBB based forum which disclosed email and IP addresses, usernames, private messages and passwords stored as bcrypt hashes.

Creation Date: 2019-07-21T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/CrackedTO.png

Website: cracked.to

Description: In July 2019, the hacking website <a href="https://cracked.to" target="_blank" rel="noopener">Cracked.to</a> suffered a data breach. There were 749k unique email addresses spread across 321k forum users and other tables in the database. A rival hacking website claimed responsibility for breaching the MyBB based forum which disclosed email and IP addresses, usernames, private messages and passwords stored as bcrypt hashes.

Title: Cracked.to

Breach Count: 749161

HIBP

Picture Url

Registered: true

Breach: true

Name: Void.to

Website: void.to

Bio: In June 2019, the hacking website <a href="https://void.to/" target="_blank" rel="noopener">Void.to</a> suffered a data breach. There were 95k unique email addresses spread across 86k forum users and other tables in the database. A rival hacking website claimed responsibility for breaching the MyBB based forum which disclosed email and IP addresses, usernames, private messages and passwords stored as either salted MD5 or bcrypt hashes.

Creation Date: 2019-06-13T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/VoidTO.png

Website: void.to

Description: In June 2019, the hacking website <a href="https://void.to/" target="_blank" rel="noopener">Void.to</a> suffered a data breach. There were 95k unique email addresses spread across 86k forum users and other tables in the database. A rival hacking website claimed responsibility for breaching the MyBB based forum which disclosed email and IP addresses, usernames, private messages and passwords stored as either salted MD5 or bcrypt hashes.

Title: Void.to

Breach Count: 95431

HIBP

Picture Url

Registered: true

Breach: true

Name: Minehut

Website: minehut.com

Bio: In May 2019, the Minecraft server website <a href="https://minehut.com/" target="_blank" rel="noopener">Minehut</a> suffered a data breach. The company advised a database backup had been obtained after which they subsequently notified all impacted users. 397k email addresses from the incident were provided to HIBP. A data set with both email addresses and bcrypt password hashes was also later provided to HIBP.

Creation Date: 2019-05-17T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Minehut.png

Website: minehut.com

Description: In May 2019, the Minecraft server website <a href="https://minehut.com/" target="_blank" rel="noopener">Minehut</a> suffered a data breach. The company advised a database backup had been obtained after which they subsequently notified all impacted users. 397k email addresses from the incident were provided to HIBP. A data set with both email addresses and bcrypt password hashes was also later provided to HIBP.

Title: Minehut

Breach Count: 396533

HIBP

Picture Url

Registered: true

Breach: true

Name: Wishbone (2020)

Website: wishbone.io

Bio: In January 2020, the mobile app to &quot;compare anything&quot; <a href="https://www.infosecurity-magazine.com/news/wishbone-breach-40-million-records/" target="_blank" rel="noopener">Wishbone suffered another data breach</a> which followed their breach from 2016. An extensive amount of personal information including almost 10M unique email addresses alongside names, phone numbers geographic locations and other personal attributes were leaked online and extensively redistributed. Passwords stored as unsalted MD5 hashes were also included in the breach. The data was provided to HIBP by a source who requested it be attributed to &quot;All3in&quot;.

Creation Date: 2020-01-27T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Wishbone.png

Website: wishbone.io

Description: In January 2020, the mobile app to &quot;compare anything&quot; <a href="https://www.infosecurity-magazine.com/news/wishbone-breach-40-million-records/" target="_blank" rel="noopener">Wishbone suffered another data breach</a> which followed their breach from 2016. An extensive amount of personal information including almost 10M unique email addresses alongside names, phone numbers geographic locations and other personal attributes were leaked online and extensively redistributed. Passwords stored as unsalted MD5 hashes were also included in the breach. The data was provided to HIBP by a source who requested it be attributed to &quot;All3in&quot;.

Title: Wishbone (2020)

Breach Count: 9705172

HIBP

Picture Url

Registered: true
Breach: true
Name: ZAP-Hosting
Website: zap-hosting.com
Bio: In November 2021, web host <a href="https://twitter.com/zaphosting/status/1503346593591873543" target="_blank" rel="noopener">ZAP-Hosting suffered a data breach</a> that exposed over 60GB of data containing 746k unique email addresses. The breach also contained support chat logs, IP addresses, names, purchases, physical addresses and phone numbers.
Creation Date: 2021-11-22T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/ZAPHosting.png
Website: zap-hosting.com
Description: In November 2021, web host <a href="https://twitter.com/zaphosting/status/1503346593591873543" target="_blank" rel="noopener">ZAP-Hosting suffered a data breach</a> that exposed over 60GB of data containing 746k unique email addresses. The breach also contained support chat logs, IP addresses, names, purchases, physical addresses and phone numbers.
Title: ZAP-Hosting
Breach Count: 746682

HIBP

Picture Url

Registered: true
Breach: true
Name: Aimware
Website: aimware.net
Bio: In mid-2019, the video game cheats website &quot;Aimware&quot; suffered a data breach that exposed hundreds of thousands of subscribers' personal information. Data included email and IP addresses, usernames, forum posts, private messages, website activity and passwords stored as salted MD5 hashes. The data was provided to HIBP by a source who requested it be attributed to &quot;clerk/anthrax/soontoberichh&quot;.
Creation Date: 2019-04-28T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Aimware.png
Website: aimware.net
Description: In mid-2019, the video game cheats website &quot;Aimware&quot; suffered a data breach that exposed hundreds of thousands of subscribers' personal information. Data included email and IP addresses, usernames, forum posts, private messages, website activity and

passwords stored as salted MD5 hashes. The data was provided to HIBP by a source who requested it be attributed to &quot;clerk/anthrax/soontoberichh&quot;.

Title: Aimware

Breach Count: 305470

HIBP

Picture Url

Registered: true

Breach: true

Name: Paragon Cheats

Website: paragoncheats.com

Bio: In May 2021, the Grand Theft Auto Online cheats website <a href="https://screenrant.com/gta-online-cheater-mod-shut-down/" target="_blank" rel="noopener">Paragon Cheats suffered a data breach that lead to the shutdown of the service</a>. The breach exposed 188k customer records including usernames, email and IP addresses. The data was provided to HIBP by a source who requested it be attributed to &quot;VRAirhead and xFueY&quot;.

Creation Date: 2021-05-22T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/ParagonCheats.png

Website: paragoncheats.com

Description: In May 2021, the Grand Theft Auto Online cheats website <a href="https://screenrant.com/gta-online-cheater-mod-shut-down/" target="_blank" rel="noopener">Paragon Cheats suffered a data breach that lead to the shutdown of the service</a>. The breach exposed 188k customer records including usernames, email and IP addresses. The data was provided to HIBP by a source who requested it be attributed to &quot;VRAirhead and xFueY&quot;.

Title: Paragon Cheats

Breach Count: 188089

HIBP

Picture Url

Registered: true

Breach: true

Name: OGUsers (2021 breach)

Website: ogusers.com

Bio: In April 2021, the account hijacking and SIM swapping forum <a href="https://www.bleepingcomputer.com/news/security/fourth-times-a-charm-ogusers-hacking-forum-hacked-again/" target="_blank" rel="noopener">OGusers suffered a data breach</a>, the fourth since December 2018. The breach was subsequently sold on a rival hacking forum and contained usernames, email and IP addresses and passwords stored as either salted MD5 or argon2 hashes. A total of 348k unique email addresses appeared in the breach.

Creation Date: 2021-04-11T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/OGUsers.png

Website: ogusers.com
Description: In April 2021, the account hijacking and SIM swapping forum <a href="https://www.bleepingcomputer.com/news/security/fourth-times-a-charm-ogusers-hacking-forum-hacked-again/" target="_blank" rel="noopener">OGusers suffered a data breach</a>, the fourth since December 2018. The breach was subsequently sold on a rival hacking forum and contained usernames, email and IP addresses and passwords stored as either salted MD5 or argon2 hashes. A total of 348k unique email addresses appeared in the breach.
Title: OGUsers (2021 breach)
Breach Count: 348302

HIBP

Picture Url

Registered: true
Breach: true
Name: Twitter
Website: twitter.com
Bio: In January 2022, <a href="https://www.bleepingcomputer.com/news/security/hacker-selling-twitter-account-data-of-54-million-users-for-30k/" target="_blank" rel="noopener">a vulnerability in Twitter's platform allowed an attacker to build a database of the email addresses and phone numbers of millions of users of the social platform</a>. In a disclosure notice later shared in August 2022, <a href="https://privacy.twitter.com/en/blog/2022/an-issue-affecting-some-anonymous-accounts" target="_blank" rel="noopener">Twitter advised that the vulnerability was related to a bug introduced in June 2021</a> and that they are directly notifying impacted customers. The impacted data included either email address or phone number alongside other public information including the username, display name, bio, location and profile photo. The data included 6.7M unique email addresses across both active and suspended accounts, the latter appearing in a separate list of 1.4M addresses.
Creation Date: 2022-01-01T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Twitter.png
Website: twitter.com
Description: In January 2022, <a href="https://www.bleepingcomputer.com/news/security/hacker-selling-twitter-account-data-of-54-million-users-for-30k/" target="_blank" rel="noopener">a vulnerability in Twitter's platform allowed an attacker to build a database of the email addresses and phone numbers of millions of users of the social platform</a>. In a disclosure notice later shared in August 2022, <a href="https://privacy.twitter.com/en/blog/2022/an-issue-affecting-some-anonymous-accounts" target="_blank" rel="noopener">Twitter advised that the vulnerability was related to a bug introduced in June 2021</a> and that they are directly notifying impacted customers. The impacted data included either email address or phone number alongside other public information including the username, display name, bio, location and profile photo. The data included 6.7M unique email addresses across both active and suspended accounts, the latter appearing in a separate list of 1.4M addresses.
Title: Twitter
Breach Count: 6682453

HIBP

Picture Url

Registered: true

Breach: true

Name: Twitter (200M)

Website: twitter.com

Bio: In early 2023, <a href="https://www.bleepingcomputer.com/news/security/200-million-twitter-users-email-addresses-allegedly-leaked-online/" target="_blank" rel="noopener">over 200M records scraped from Twitter appeared on a popular hacking forum</a>. 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

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Twitter.png

Website: twitter.com

Description: In early 2023, <a href="https://www.bleepingcomputer.com/news/security/200-million-twitter-users-email-addresses-allegedly-leaked-online/" target="_blank" rel="noopener">over 200M records scraped from Twitter appeared on a popular hacking forum</a>. 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.

Title: Twitter (200M)

Breach Count: 211524284

HIBP

Picture Url

Registered: true

Breach: true

Name: OGUsers (2022 breach)

Website: ogusers.com

Bio: In July 2022, the account hijacking and SIM swapping forum OGusers suffered a data breach, the fifth since December 2018. The breach contained usernames, email and IP addresses and passwords stored as argon2 hashes. A total of 529k unique email addresses appeared in the breach.

Creation Date: 2022-07-13T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/OGUsers.png

Website: ogusers.com

Description: In July 2022, the account hijacking and SIM swapping forum OGusers suffered a data breach, the fifth since December 2018. The breach contained usernames, email and IP addresses and passwords stored as argon2 hashes. A total of 529k unique email addresses appeared in the breach.

Title: OGUsers (2022 breach)

Breach Count: 529020

HIBP

Picture Url

Registered: true
Breach: true
Name: RaidForums
Website: raidforums.com
Bio: In May 2023, <a href="https://www.bleepingcomputer.com/news/security/new-hacking-forum-leaks-data-of-478-000-raidforums-members/" target="_blank" rel="noopener">478k user records from the now defunct hacking forum known as &quot;RaidForums&quot; was posted to another hacking forum</a>. The data dated back to September 2020 and included email addresses, usernames, dates of birth, IP addresses and passwords stored as Argon2 hashes. The data was provided to HIBP by a source who requested it be attributed to &quot;white_peacock@riseup.net&quot;.
Creation Date: 2020-09-24T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/RaidForums.png
Website: raidforums.com
Description: In May 2023, <a href="https://www.bleepingcomputer.com/news/security/new-hacking-forum-leaks-data-of-478-000-raidforums-members/" target="_blank" rel="noopener">478k user records from the now defunct hacking forum known as &quot;RaidForums&quot; was posted to another hacking forum</a>. The data dated back to September 2020 and included email addresses, usernames, dates of birth, IP addresses and passwords stored as Argon2 hashes. The data was provided to HIBP by a source who requested it be attributed to &quot;white_peacock@riseup.net&quot;.
Title: RaidForums
Breach Count: 478604

KAHOOT

PINTEREST

AUTODESK

WIX

NZXT

DISNEY

MEDAL

Registered: true

DIGITALOCEAN

NVIDIA

FACEBOOK

Registered: true

APPLE

Registered: true
Phone Hint: (***) ***-**95

ESPN

PLAYGAMES

Picture Url
Banner Url

Registered: true
Id: g13888417261573788852
Name: SolemnTree90554
Username: SolemnTree90554
Bio: Strategist
Last Seen: 2017-08-12T02:00:21
Banner Url Landscape: https://lh3.googleusercontent.com/
AogCtkMsMmscGAqvG5xC5h5Oy0XwlL9nIE9fq8HR2rXlRl5cInsZxnhrkqH0zlPE0AmGoe_x0WzzSck5Tb0

GRAMMARLY

TWITTER

Registered: true
Phone Hint: *** 95

MAPS

Profile Url

Registered: true

STEAM

Registered: true

GOOGLE

Picture Url

Registered: true
Id: 101992846262551936045
Last Seen: 2023-09-01T21:08:04

DROPBOX

Picture Url

Registered: true
Id: dbid:AABw7gkkn-KDPVBQjysDBcai4hVObSP1gfk
Name: v Pulse
First Name: v Pulse
Verified: true

MICROSOFT

Registered: true
Id: A88B953070CDDF27
Name: minerbubs1234@gmail.com
Location: US
Phone Hint: ********95
Last Seen: 2024-11-21T21:12:01.060000+00:00
Creation Date: 2024-07-03T03:24:46.950000+00:00

EA
