Your Security Rabbits report for February 27, 2022

Source: Have I been pwned?

Have I been pwnd

GiveSendGo(givesendgo.com)
In February 2022, the Christian fundraising service GiveSendGo suffered a data breach which exposed the personal data of 90k donors to the Canadian "Freedom Convoy" protest against vaccine mandates. The breach exposed names, email addresses, post codes, donation amount and comments left at the time of donation.

Count: 89966 | Created: 2022-02-07 | Updated: 2022-02-15

BTC-Alpha(btc-alpha.com)
In November 2021, the crypto exchange platform BTC-Alpha suffered a ransomware attack data breach after which customer data was publicly dumped. The impacted data included 362k email and IP addresses, usernames and passwords stored as PBKDF2 hashes. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 362426 | Created: 2021-11-02 | Updated: 2022-01-27

Upstox(upstox.com)
In April 2021, Indian brokerage firm Upstox suffered a data breach. The incident exposed extensive personal information on over 100k customers including names, genders, dates of birth, physical addresses, banking information and passwords stored as bcrypt hashes. Extensive "know your customer" information was also exposed including scans of bank statements, cheques and identity documents complete with Aadhaar numbers. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 111002 | Created: 2021-04-08 | Updated: 2022-01-19

Carding Mafia (December 2021)(cardmafia.cc)
In December 2021, the Carding Mafia forum suffered a data breach that exposed over 300k members' email addresses. Dedicated to the theft and trading of stolen credit cards, the forum breach also exposed usernames, IP addresses and passwords stored as salted MD5 hashes. This breach came only 9 months after another breach of the forum in March 2021.

Count: 303877 | Created: 2021-12-28 | Updated: 2022-01-16

Carding Mafia (March 2021)(cardmafia.cc)
In March 2021, the Carding Mafia forum suffered a data breach that exposed almost 300k members' email addresses. Dedicated to the theft and trading of stolen credit cards, the forum breach also exposed usernames, IP addresses and passwords stored as salted MD5 hashes.

Count: 297744 | Created: 2021-03-18 | Updated: 2022-01-15

RedDoorz(reddoorz.com)
In September 2020, the hotel management & booking platform RedDoorz suffered a data breach that exposed over 5.8M user accounts. The breached data included names, email addresses, phone numbers, genders, dates of birth and passwords stored as bcrypt hashes. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 5890277 | Created: 2020-09-04 | Updated: 2022-01-28

ShockGore(shockgore.com)
In August 2020, the website for sharing graphic videos and images of gore and animal cruelty suffered a data breach. The breach exposed 74k unique email addresses alongside usernames, IP addresses, genders and unsalted SHA-1 password hashes. Private messages were also exposed, many containing requests for material of a depraved nature. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 73944 | Created: 2020-08-11 | Updated: 2022-01-20

Open Subtitles(opensubtitles.org)
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.

Count: 6783158 | Created: 2021-08-01 | Updated: 2022-01-19

Aditya Birla Fashion and Retail(abfrl.com)
In December 2021, Indian retailer Aditya Birla Fashion and Retail Ltd was breached and ransomed. The ransom demand was allegedly rejected and data containing 5.4M unique email addresses was subsequently dumped publicly on a popular hacking forum the next month. The data contained extensive personal customer information including names, phone numbers, physical addresses, DoBs, order histories and passwords stored as MD5 hashes. Employee data was also dumped publicly and included salary grades, marital statuses and religions. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 5470063 | Created: 2021-12-01 | Updated: 2022-01-15

Guns.com(guns.com)
In January 2021, the firearms website guns.com suffered a data breach. The breach exposed 376k unique email addresses along with names, phone numbers, physical addresses, gun purchases, partial credit card data, dates of birth and passwords stored as bcrypt hashes.

Count: 375928 | Created: 2021-01-12 | Updated: 2022-01-13

Doxbin(doxbin.com)
In January 2022, the "doxing" website designed to disclose the personal information of targeted individuals ("doxes") Doxbin suffered a data breach. The breach was subsequently leaked online and included over 370k unique email addresses across user accounts and doxes. User accounts also included usernames, password hashes and browser user agents. The personal information disclosed in the doxes was often extensive including names, physical addresses, phone numbers and more.

Count: 370794 | Created: 2022-01-05 | Updated: 2022-01-09

Emotet()
In January 2021, the FBI in partnership with the Dutch NHTCU, German BKA and other international law enforcement agencies brought down the world's most dangerous malware: Emotet. The agencies obtained data collected by the malware and provided impacted email addresses to HIBP so that impacted individuals and domain owners could assess their exposure. Read more about the takedown and recommended actions.

Count: 4324770 | Created: 2021-01-27 | Updated: 2022-01-05

RedLine Stealer()
In December 2021, logs from the RedLine Stealer malware were left publicly exposed and were then obtained by security researcher Bob Diachenko. The data included 441 thousand unique email addresses, usernames and plain text passwords.

Count: 441657 | Created: 2021-12-05 | Updated: 2022-01-05

DatPiff(datpiff.com)
In late 2021, email address and plain text password pairs from the rap mixtape website DatPiff appeared for sale on a popular hacking forum. The data allegedly dated back to an earlier breach and in total, contained almost 7.5M email addresses and cracked password pairs. The original data source allegedly contained usernames, security questions and answers and passwords stored as MD5 hashes with a static salt.

Count: 7476940 | Created: 2021-08-25 | Updated: 2022-01-04

Gravatar(gravatar.com)
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.

Count: 113990759 | Created: 2020-10-03 | Updated: 2021-12-08

PeoplesEnergy(peoplesenergy.co.uk)
In December 2020, the UK power company People's Energy suffered a data breach. The breach exposed almost 7GB of files containing 359k unique email addresses along with names, phones numbers, physical addresses and dates of birth. The incident also included People's Energy staff email addresses and bcrypt password hashes (no customer passwords were exposed). The data was provided to HIBP by a source who requested it be attributed to pom@pompur.in.

Count: 358822 | Created: 2020-12-16 | Updated: 2021-11-25

FlexBooker(flexbooker.com)
In December 2021, the online booking service FlexBooker suffered a data breach that exposed 3.7 million accounts. The data included email addresses, names, phone numbers and for a small number of accounts, password hashes and partial credit card data. FlexBooker has identified the breach as originating from a compromised account within their AWS infrastructure. The data was found being actively traded on a popular hacking forum and was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 3756794 | Created: 2021-12-23 | Updated: 2022-01-06

Nameless Malware()
In January 2021, NordLocker provided HIBP 1.1 million email addresses collected by nameless malware. The malware campaign ran between 2018 and 2020 and infected 3.25 million computers, stealing files, credentials and taking screenshots and photos using the computer's webcam. Read more in NordLocker's writeup about the Nameless malware that stole 1.2 TB of private data.

Count: 1121484 | Created: 2020-01-01 | Updated: 2022-01-05

Trik Spam Botnet()
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).

Count: 43432346 | Created: 2018-06-12 | Updated: 2022-01-05

Protemps(protemps.com.sg)
In October 2021, the Singaporean recruitment website Protemps suffered a data breach that exposed almost 50,000 unique email addresses. The impacted data includes names, email and physical addresses, phone numbers, passport numbers and passwords stored as unsalted MD5 hashes, among troves of other jobseeker data. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 49591 | Created: 2021-10-04 | Updated: 2021-12-20

NetGalley(netgalley.com)
In December 2020, the book promotion site NetGalley suffered a data breach. The incident exposed 1.4 million unique email addresses alongside names, usernames, physical and IP addresses, phone numbers, dates of birth and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by a source who requested it be attributed to pom@pompur.in.

Count: 1436435 | Created: 2020-12-21 | Updated: 2021-11-25

WiziShop(wizishop.fr)
In July 2020, the French e-commerce platform WiziShop suffered a data breach. The breach exposed 18GB worth of data including names, phone numbers, dates of birth, physical and IP addresses, SHA-1 password hashes and almost 3 million unique email addresses. The data was provided to HIBP by a source who requested it be attributed to "pom@pompur.in".

Count: 2856769 | Created: 2020-07-14 | Updated: 2021-11-25

IDC Games(idcgames.com)
In March 2021, 4 million records sourced from IDC Games were shared on a public hacking forum. The data included usernames, email addresses and passwords stored as salted MD5 hashes.

Count: 3966871 | Created: 2021-03-15 | Updated: 2021-11-17

ActMobile(actmobile.com)
In October 2021, security researcher Bob Diachenko discovered an exposed database he attributed to ActMobile, the operators of Dash VPN and FreeVPN. The exposed data included 1.6 million unique email addresses along with IP addresses and password hashes, all of which were subsequently leaked on a popular hacking forum. Although usage of the service was verified by HIBP subscribers, ActMobile denied the data was sourced from them and the breach has subsequently been flagged as "unverified".

Count: 1583193 | Created: 2021-10-08 | Updated: 2021-11-09

CoinMarketCap(coinmarketcap.com)
During October 2021, 3.1 million email addresses with accounts on the cryptocurrency market capitalisation website CoinMarketCap were discovered being traded on hacking forums. Whilst the email addresses were found to correlate with CoinMarketCap accounts, it's unclear precisely how they were obtained. CoinMarketCap has provided the following statement on the data: "CoinMarketCap has become aware that batches of data have shown up online purporting to be a list of user accounts. While the data lists we have seen are only email addresses (no passwords), we have found a correlation with our subscriber base. We have not found any evidence of a data leak from our own servers xe2x80x94 we are actively investigating this issue and will update our subscribers as soon as we have any new information."

Count: 3117548 | Created: 2021-10-12 | Updated: 2021-10-22

Playbook(playbook.vc)
In September 2021, a publicly accessible PostgresSQL database belonging to the Playbook service was identified. Run by VC firm Plug and Play Ventures, the database had been exposed since October 2020 and contained more than 50 thousand unique email addresses along with names, phone numbers, job titles and passwords stored as PBKDF2 hashes. It took more than 2 weeks after being notified of the exposed data to properly secure it. It's unknown whether Plug and Play Ventures notified impacted individuals as they ceased responding to queries from the press.

Count: 50538 | Created: 2020-10-19 | Updated: 2021-10-11

Republican Party of Texas(texasgop.org)
In September 2021, the Republican Party of Texas was hacked by a group claiming to be "Anonymous" in retaliation for the state's controversial abortion ban. The September defacement was followed by a leak of data and documents which included material from the hosting provider Epik. Impacted data included over 72 thousand unique email addresses across various tables, some also including names, geographic location data, IP addresses and browser user agents.

Count: 72596 | Created: 2021-09-11 | Updated: 2021-10-06

Ajarn(ajarn.com)
In September 2021, the Thai-based English language teaching website Ajarn discovered they'd been the victim of a data breach dating back to December 2018. The breach was self-submitted to HIBP and included 266k email addresses, names, genders, phone numbers and other personal information. Hashed

Ducks Unlimited(ducks.org)
In mid-2021, Risk Based Security reported on a database sourced from Ducks Unlimited being traded online. The data dated back to January 2021 and contained 1.3M unique email addresses across both a membership list and a list of website users. Impacted data included names, phones numbers, physical addresses, dates of birth and passwords stored as unsalted MD5 hashes.

Count: 1324364 | Created: 2021-01-29 | Updated: 2021-11-16

CyberServe(cyberserve.co.il)
In October 2021, the Israeli hosting provider CyberServe was breached and ransomed before having a substantial amount of their customer data leaked publicly by a group known as "Black Shadow". Amongst the data was the LGBTQ dating site Atraf and the Machon Mor medical institute. Due to multiple different sites being compromised, the impacted data is broad and ranges from relationship information to medical data to email addresses and passwords stored in plain text. The data was made available to HIBP with support from May Brooks-Kempler, founder of the Think Safe Cyber community in Israel.

Count: 1107034 | Created: 2021-10-29 | Updated: 2021-11-04

Thingiverse(thingiverse.com)
In October 2021, a database backup taken from the 3D model sharing service Thingiverse began extensively circulating within the hacking community. Dating back to October 2020, the 36GB file contained 228 thousand unique email addresses, mostly alongside comments left on 3D models. The data also included usernames, IP addresses, full names and passwords stored as either unsalted SHA-1 or bcrypt hashes. In some cases, physical addresses was also exposed. Thingiverse's owner, MakerBot, is aware of the incident but at the time of writing, is yet to issue a disclosure statement. The data was provided to HIBP by dehashed.com.

Count: 228102 | Created: 2020-10-13 | Updated: 2021-10-14

Fantasy Football Hub(fantasyfootballhub.co.uk)
In October 2021, the fantasy premier league (soccer) website Fantasy Football Hub suffered a data breach that exposed 66 thousand unique email addresses. The data included names, usernames, IP addresses, transactions and passwords stored as WordPress MD5 hashes.

Count: 66479 | Created: 2021-10-02 | Updated: 2021-10-07

LinkedIn Scraped Data(linkedin.com)
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.

Count: 125698496 | Created: 2021-04-08 | Updated: 2021-10-02

Epik(epik.com)
In September 2021, the domain registrar and web host Epik suffered a significant data breach, allegedly in retaliation for hosting alt-right websites. The breach exposed a huge volume of data not just of Epik customers, but also scraped WHOIS records belonging to individuals and organisations who were not Epik customers. The data included over 15 million unique email addresses (including anonymised versions for domain privacy), names, phone numbers,

passwords were also impacted in the breach.

Count: 266399 | Created: 2018-12-13 | Updated: 2021-09-26

IndiaMART(indiamart.com)
In August 2021, 38 million records from Indian e-commerce company IndiaMART were found being traded on a popular hacking forum. Dated several months earlier, the data included over 20 million unique email addresses alongside names, phone numbers and physical addresses. It's unclear whether IndiaMART intentionally exposed the data attributes as part of the intended design of the platform or whether the data was obtained by exploiting a vulnerability in the service.

Count: 20154583 | Created: 2021-05-23 | Updated: 2021-08-27

Imavex(imavex.com)
In August 2021, the website development company Imavex suffered a data breach that exposed 878 thousand unique email addresses. The data included user records containing names, usernames and password material with some records also containing genders and partial credit card data, including the last 4 digits of the card and expiry date. Hundreds of thousands of form submissions and orders via Imavex customers were also exposed and contained further personal information of submitters and the contents of the form.

Count: 878209 | Created: 2021-08-20 | Updated: 2021-08-26

SubaGames(subagames.com)
In November 2016, the game developer Suba Games suffered a data breach which led to the exposure of 6.1M unique email addresses. Impacted data also included usernames and passwords, most of which appeared circulating in the breached file in plain text after being cracked from salted MD5 hashes. The data was provided to HIBP by dehashed.com.

Count: 6137666 | Created: 2016-11-01 | Updated: 2021-08-25

OrderSnapp(ordersnapp.com)
In June 2020, the restaurant solutions provider OrderSnapp suffered a data breach which exposed 1.3M unique email addresses. Impacted data also included names, phone numbers, dates of birth and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 1304447 | Created: 2020-06-29 | Updated: 2021-08-08

Audi(audiusa.com)
In August 2019, Audi USA suffered a data breach after a vendor left data unsecured and exposed on the internet. The data contained 2.7M unique email addresses along with names, phone numbers, physical addresses and vehicle information including VIN. In a disclosure statement from Audi, they also advised some customers had driver's licenses, dates of birth, social security numbers and other personal information exposed.

Count: 2743539 | Created: 2019-08-14 | Updated: 2021-07-23

Guntrader(guntrader.uk)
In July 2021, the United Kingdom based website Guntrader suffered a data breach that exposed 112k unique email addresses. Extensive personal information was also exposed including names, phone numbers, geolocation data, IP addresses and various physical address attributes (cities for all users, complete addresses for some). Passwords stored as bcrypt hashes were also exposed.

Count: 112031 | Created: 2021-07-17 | Updated: 2021-07-21

physical addresses, purchases and passwords stored in various formats.

Count: 15003961 | Created: 2021-09-13 | Updated: 2021-09-19

Vastaamo(vastaamo.fi)
In October 2020, the Finnish psychotherapy service Vastaamo was the subject of a ransomware attack targeting first the company itself, followed by their patients directly. The original security incident dates back to a period between late 2018 and early 2019 and exposed data including 30k unique email addresses, names, social security numbers and notes on individuals' psychotherapy sessions. This breach has been flagged as "sensitive" and is only searchable by owners of the email addresses and domains exposed in the incident.

Count: 30433 | Created: 2019-03-31 | Updated: 2021-08-27

Eatigo(eatigo.com)
In October 2018, the restaurant reservation service Eatigo suffered a data breach that exposed 2.8 million accounts. The data included email addresses, names, phone numbers, social media profiles, genders and passwords stored as unsalted MD5 hashes.

Count: 2789609 | Created: 2018-10-16 | Updated: 2021-08-25

Patreon(patreon.com)
In October 2015, the crowdfunding site Patreon was hacked and over 16GB of data was released publicly. The dump included almost 14GB of database records with more than 2.3M unique email addresses, millions of personal messages and passwords stored as bcrypt hashes.

Count: 2330382 | Created: 2015-10-01 | Updated: 2021-08-10

MMG Fusion(mmgfusion.com)
In December 2020, the dental practice management service MMG Fusion was the victim of a data breach which exposed 2.6M unique email addresses. The data also included patient appointments, names, phone numbers, dates of birth, genders and physical addresses. A small number of records also included passwords stored as bcrypt hashes.

Count: 2660295 | Created: 2020-12-20 | Updated: 2021-08-07

Ticketfly(ticketfly.com)
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".

Count: 26151608 | Created: 2018-05-31 | Updated: 2021-07-23

ShortEdition(short-edition.com)
In June 2021, the French publishing house of short literature Short xc3x89dition suffered a data breach that exposed 505k records. Impacted data included email and physical addresses, names, usernames, phone numbers, dates of birth, genders and passwords stored as either salted SHA-1 or salted SHA-512 hashes. Short xc3x89dition self-submitted the impacted data to HIBP.

Count: 505466 | Created: 2021-06-26 | Updated: 2021-07-19

Raychat(raychat.ir)
In January 2021, the now defunct Iranian social media platform Raychat suffered a data breach that exposed 939 thousand unique email addresses. The data included names, IP addresses, browser user agent strings and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 938981 | Created: 2021-01-31 | Updated: 2021-07-04

Teespring(teespring.com)
In April 2020, the custom printed apparel website Teespring suffered a data breach that exposed 8.2 million customer records. The data included email addresses, names, geographic locations and social media IDs.

Count: 8234193 | Created: 2020-04-01 | Updated: 2021-06-25

DominosIndia(dominos.co.in)
In April 2021, 13TB of compromised Domino's India appeared for sale on a hacking forum after which the company acknowledged a major data breach they dated back to March. The compromised data included 22.5 million unique email addresses, names, phone numbers, order histories and physical addresses.

Count: 22527655 | Created: 2021-03-24 | Updated: 2021-06-20

JD(jd.com)
In 2013 (exact date unknown), the Chinese e-commerce service JD suffered a data breach that exposed 13GB of data containing 77 million unique email addresses. The data also included usernames, phone numbers and passwords stored as SHA-1 hashes. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 77449341 | Created: 2013-01-01 | Updated: 2021-06-02

MobiFriends(mobifriends.com)
In January 2020, the Barcelona-based dating app MobiFriends suffered a data breach that exposed 3.5 million unique email addresses. The data also included usernames, genders, dates of birth and MD5 password hashes. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 3512952 | Created: 2020-01-06 | Updated: 2021-05-23

Yam(yam.com)
In June 2013, the Taiwanese website Yam.com suffered a data breach which was shared to a popular hacking forum in 2021. The data included 13 million unique email addresses alongside names, usernames, phone numbers, physical addresses, dates of birth and unsalted MD5 password hashes.

Count: 13258797 | Created: 2013-06-02 | Updated: 2021-05-22

IIMJobs(iimjobs.com)
In December 2018, the Indian job portal IIMJobs suffered a data breach that exposed 4.1 million unique email addresses. The data also included names, phone numbers, geographic locations, dates of birth, job titles, job applications and cover letters plus passwords stored as unsalted MD5 hashes. The data was provided to HIBP by dehashed.com.

Count: 4216063 | Created: 2018-12-31 | Updated: 2021-05-21

DriveSure(drivesure.com)
In December 2020, the car dealership service

University of California(universityofcalifornia.edu)
In December 2020, the University of California suffered a data breach due to vulnerability in in a third-party provider, Accellion. The breach exposed extensive personal data on both students and staff including 547 thousand unique email addresses, names, dates of birth, genders, social security numbers, ethnicities and other academic related data attributes. Further analysis is available in Exploring the Impact of the UC Data Breach. The data was provided to HIBP courtesy of Cyril Gorlla.

Count: 547422 | Created: 2020-12-24 | Updated: 2021-07-04

yotepresto.com(yotepresto.com)
In June 2020, the Mexican lending platform yotepresto.com suffered a data breach. Over 1.4 million customers were impacted by the breach which disclosed email and IP addresses, usernames and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 1444629 | Created: 2020-06-22 | Updated: 2021-06-25

Fotolog(fotolog.com)
In December 2018, the photo sharing social network Fotolog suffered a data breach that exposed 16.7 million unique email addresses. The data also included usernames and unsalted SHA-256 password hashes. The site was dissolved the following year and repurposed as a news website based in Brcko, Bosnia and Herzegovina.

Count: 16717854 | Created: 2018-12-01 | Updated: 2021-06-15

Livpure(livpure.com)
In August 2020, the Indian retailer Livpure suffered a data breach which exposed over 1 million customer purchases with 270 thousand unique email addresses. The data also included names, phone numbers, physical addresses and details of purchased items. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 269552 | Created: 2020-08-29 | Updated: 2021-05-23

Moneycontrol(moneycontrol.com)
In April 2021, hackers posted data for sale originating from the online Indian financial platform, Moneycontrol. The data included 763 thousand unique email addresses (allegedly a subset of a larger 40 million account breach), alongside geographic locations, phone numbers, genders, dates of birth and plain text passwords. The date of the original breach is unclear, although the breached data indicates the file was created in September 2017 and Moneycontrol has stated that the breach is "an old data set".

Count: 762874 | Created: 2017-09-07 | Updated: 2021-05-22

Daily Quiz(dailyquiz.me)
In January 2021, the quiz website Daily Quiz suffered a data breach that exposed over 8 million unique email addresses. The data also included usernames, IP addresses and passwords stored in plain text.

Count: 8032404 | Created: 2021-01-13 | Updated: 2021-05-21

WedMeGood(wedmegood.com)
In January 2021, the Indian wedding planning platform WedMeGood suffered a data breach that exposed 1.3 million customers. The breach exposed 41.5GB of data including email and physical addresses, names, genders, phone numbers and password hashes. The data was provided to HIBP by dehashed.com.

Count: 1306723 | Created: 2021-01-06 | Updated: 2021-05-13

provider DriveSure suffered a data breach. The incident resulted in 26GB of data being downloaded and later shared on a hacking forum. Impacted personal information included 3.6 million unique email addresses, names, phone numbers and physical addresses. Vehicle data was also exposed and included makes, models, VIN numbers and odometer readings. A small number of passwords stored as bcrypt hashes were also included in the data set.

Count: 3675099 | Created: 2020-12-19 | Updated: 2021-05-10

ParkMobile(parkmobile.io)
In March 2021, the mobile parking app service ParkMobile suffered a data breach which exposed 21 million customers' personal data. The impacted data included email addresses, names, phone numbers, vehicle licence plates and passwords stored as bcrypt hashes. The following month, the data appeared on a public hacking forum where it was extensively redistributed.

Count: 20949825 | Created: 2021-03-21 | Updated: 2021-04-30

Jefit(jefit.com)
In August 2020, the workout tracking app Jefit suffered a data breach. The data was subsequently sold within the hacking community and included over 9 million email and IP addresses, usernames and passwords stored as either vBulletin or argon2 hashes. Several million cracked passwords later appeared in broad circulation.

Count: 9052457 | Created: 2020-08-11 | Updated: 2021-04-27

MangaDex(mangadex.org)
In March 2021, the manga fan site MangaDex suffered a data breach that resulted in the exposure of almost 3 million subscribers. The data included email and IP addresses, usernames and passwords stored as bcrypt hashes. The data was subsequently circulated within hacking groups.

Count: 2987329 | Created: 2021-03-22 | Updated: 2021-04-25

ClearVoice Surveys(clearvoicesurveys.com)
In April 2021, the market research surveys company ClearVoice Surveys had a publicly facing database backup from 2015 taken and redistributed on a popular hacking forum. The data included 15M unique email addresses across more than 17M rows of data that also included names, physical and IP addresses, genders, dates of birth and plain text passwords. ClearVoice Surveys advised they were aware of the breach and confirmed its authenticity.

Count: 15074786 | Created: 2015-08-23 | Updated: 2021-04-23

Unverified Data Source(astoriacompany.com)
In January 2021, over 11M unique email addresses were discovered by Night Lion Security alongside an extensive amount of personal information including names, physical and IP addresses, phone numbers and dates of birth. Some records also contained social security numbers, driver's license details, personal financial information and health-related data, depending on where the information was sourced from. Initially attributed to Astoria Company, they subsequently investigated the incident and confirmed the data did not originate from their services.

Count: 11498146 | Created: 2021-01-26 | Updated: 2021-04-12

Facebook(facebook.com)
In April 2021, a large data set of over 500

WeLeakInfo(weleakinfo.com)
In March 2021, the Stripe account of the now-defunct WeLeakInfo service was taken over by "pompompurin" after acquiring an expired domain name with an email address used to manage the account. Access to Stripe then exposed almost 12k unique email addresses from customers who'd made credit card payments in order to obtain breached data hosted by WeLeakInfo. The data was subsequently leaked publicly and also included names, payment histories, IP addresses, billing addresses, partial credit card data and the organisation making the purchase.

Count: 11788 | Created: 2021-03-08 | Updated: 2021-05-03

Descomplica(descomplica.com.br)
In March 2021, the Brazilian EdTech company Descomplica suffered a data breach which was subsequently posted to a popular hacking forum. The data included almost 5 million email addresses, names, the first 6 and last 4 digits and the expiry date of credit cards, purchase histories and password hashes.

Count: 4845378 | Created: 2021-03-14 | Updated: 2021-04-28

bigbasket(bigbasket.com)
In October 2020, the Indian grocery platform bigbasket suffered a data breach that exposed over 20 million customer records. The data was originally sold before being leaked publicly in April the following year and included email, IP and physical addresses, names, phones numbers, dates of birth passwords stored as Django(SHA-1) hashes.

Count: 24500011 | Created: 2020-10-14 | Updated: 2021-04-26

ShopBack(shopback.com)
In September 2020, the cashback reward program ShopBack suffered a data breach. The incident exposed over 20 million unique email addresses along with names, phone numbers, country of residence and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.

Count: 20529819 | Created: 2020-09-17 | Updated: 2021-04-25

PhoneHouse(phonehouse.es)
In April 2021, the Spanish retailer Phone House allegedly suffered a ransomware attack that also exposed significant volumes of customer data. Attributed to the Babuk ransomware, a collection of data alleged to be a subset of a larger corpus was posted to a dark web site and contained 5.2M email addresses along with names, nationalities, genders, dates of birth, phone numbers and physical addresses. Phone House has been threatened with further releases if a ransom is not paid.

Count: 5223350 | Created: 2021-04-08 | Updated: 2021-04-22

Armor Games(armorgames.com)
In January 2019, the game portal website Armor Games suffered a data breach. A total of 10.6 million email addresses were impacted by the breach which also exposed usernames, IP addresses, birthdays of administrator accounts and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 10604307 | Created: 2019-01-01 | Updated: 2021-04-07

million Facebook users was made freely available for download. Encompassing approximately 20% of Facebook's subscribers, the data was allegedly obtained by exploiting a vulnerability Facebook advises they rectified in August 2019. The primary value of the data is the association of phone numbers to identities; whilst each record included phone, only 2.5 million contained an email address. Most records contained names and genders with many also including dates of birth, location, relationship status and employer.

Count: 509458528 | Created: 2019-08-01 | Updated: 2021-04-06

Travel Oklahoma(travelok.com)
In December 2020, the Oklahoma state Tourism and Recreation Department suffered a data breach. The incident exposed 637k email addresses across a variety of tables including age ranges against brochure orders and dates of birth against contest entries. Genders, names and physical addresses were also exposed. The data was provided to HIBP by a source who requested it be attributed to "badhou3a".

Count: 637279 | Created: 2020-12-17 | Updated: 2021-03-10

Oxfam(oxfam.org.au)
In January 2021, Oxfam Australia was the victim of a data breach which exposed 1.8M unique email addresses of supporters of the charity. The data was put up for sale on a popular hacking forum and also included names, phone numbers, addresses, genders and dates of birth. A small number of people also had partial credit card data exposed (the first 6 and last 3 digits of the card, plus card type and expiry) and in some cases the bank name, account number and BSB were also exposed. The data was subsequently made freely available on the hacking forum later the following month.

Count: 1834006 | Created: 2021-01-20 | Updated: 2021-03-02

SuperVPN & GeckoVPN()
In February 2021, a series of "free" VPN services were breached including SuperVPN and GeckoVPN, exposing over 20M records. The data appeared together in a single file with a small number of records also included from FlashVPN, suggesting that all three brands may share the same platform. Impacted data also included email addresses, the country logged in from and the date and time each login occurred alongside device information including the make and model, IMSI number and serial number. The data was provided to HIBP by a source who requested it be attributed to redredred@riseup.net.

Count: 20339937 | Created: 2021-02-25 | Updated: 2021-02-28

NurseryCam(nurserycam.co.uk)
In February 2021, a series of egregiously bad security flaws were identified in the NurseryCam system designed for parents to remotely monitor their children whilst attending nursery. The flaws led to the exposure of over 10k parent records before the service was shut down. The email addresses alone were provided to Have I Been Pwned to ensure parents were properly notified of the incident.

Count: 10585 | Created: 2021-02-12 | Updated: 2021-02-23

CityBee(citybee.lt)
In February 2021, the Lithuanian car-sharing service CityBee announced they'd suffered a data breach that exposed 110k customers' personal information. The breach exposed names, email addresses, government issued IDs and passwords stored as unsalted SHA-1 hashes.

Liker(liker.com)
In March 2021, the self-proclaimed "kinder, smarter social network" Liker suffered a data breach, allegedly in retaliation for the Gab data breach and scraping of data from Parler. The site remained offline after the breach which exposed 465k email addresses in addition to names, dates of birth, education levels, private messages, security questions and answers in plain text, passwords stored as bcrypt hashes and other personal data attributes. Liker did not respond when contacted about the breach.

Count: 465141 | Created: 2021-03-08 | Updated: 2021-03-24

Gab(gab.com)
In February 2021, the alt-tech social network service Gab suffered a data breach. The incident exposed almost 70GB of data including 4M user accounts, a small number of private chat logs and a list of public groups and public posts made to the service. Only a small number of accounts included email addresses and / or passwords stored as bcrypt hashes with a total of 66.5k unique email addresses being exposed across the corpus of data.

Count: 66521 | Created: 2021-02-26 | Updated: 2021-03-03

Ticketcounter(ticketcounter.nl)
In August 2020, the Dutch ticketing service Ticketcounter inadvertently published a database backup to a publicly accessible location where it was then found and downloaded in February 2021. The data contained 1.9M unique email addresses which were offered for sale on a hacking forum alongside names, physical and IP addresses, genders, dates of birth, payment histories and in some cases, bank account numbers. Ticketcounter was later held to ransom with the threat of the breached being released publicly. The data was provided to HIBP by a source who requested it be attributed to redredred@riseup.net.

Count: 1921722 | Created: 2021-02-22 | Updated: 2021-03-01

Filmai.in(filmai.in)
In approximately 2019 or 2020, the Lithuanian movie streaming service Filmai.in suffered a data breach exposing 645k email addresses, usernames and plain text passwords.

Count: 645786 | Created: 2020-01-01 | Updated: 2021-02-23

Ge.tt(ge.tt)
In May 2017, the file sharing platform Ge.tt suffered a data breach. The data was subsequently put up for sale on a dark web marketplace in February 2019 alongside a raft of other breaches. The Ge.tt breach included names, social media profile identifiers, SHA256 password hashes and almost 2.5M unique email addresses. The data was provided to HIBP by a source who requested it be attributed to BreachDirectory.

Count: 2481121 | Created: 2017-05-04 | Updated: 2021-02-22

StoryBird(storybird.com)
In August 2015, the storytelling service StoryBird suffered a data breach exposing 4 million records with 1 million unique email addresses. Impacted data also included names, usernames and passwords stored as PBKDF2 hashes. The data was provided to HIBP by dehashed.com.

Count: 1047200 | Created: 2015-08-07 | Updated: 2021-02-02

Count: 110156 | Created: 2021-02-05 | Updated: 2021-02-17

Pixlr(pixlr.com)
In October 2020, the online photo editing application Pixlr suffered a data breach exposing 1.9 million subscribers. Impacted data included names, email addresses, social media profiles, the country signed up from and passwords stored as SHA-512 hashes. The data was provided to HIBP by dehashed.com.

Count: 1906808 | Created: 2020-10-07 | Updated: 2021-02-01

MeetMindful(meetmindful.com)
In early 2020, the online dating service MeetMindful suffered a data breach that exposed 1.4 million unique customer email addresses. Included in the data was an extensive array of personal information used to find romantic matches including physical attributes, use of alcohol, drugs and cigarettes, marital statuses, birthdates, genders and the gender being sought. Additional personal information such as names, geographical locations and IP addresses were also exposed, along with passwords stored as bcrypt hashes.

Count: 1422717 | Created: 2020-01-26 | Updated: 2021-01-31

Romwe(romwe.com)
In mid-2018, the Hong Kong-based retailer Romwe suffered a data breach which exposed almost 20 million customers. The data was subsequently sold online and includes names, phone numbers, email and IP addresses, customer geographic locations and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.

Count: 19531820 | Created: 2018-06-01 | Updated: 2021-01-18

GeniusU(geniusu.com)
In November 2020, a collection of data breaches were made public including the "Entrepreneur Success Platform", GeniusU. Dating back to the previous month, the data included 1.3M names, email and IP addresses, genders, links to social media profiles and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 1301460 | Created: 2020-10-02 | Updated: 2021-01-10

Ledger(ledger.com)
In June 2020, the hardware crypto wallet manufacturer Ledger suffered a data breach that exposed over 1 million email addresses. The data was initially sold before being dumped publicly in December 2020 and included names, physical addresses and phone numbers. The data was provided to HIBP by Alon Gal, CTO of cybercrime intelligence firm Hudson Rock.

Count: 1075241 | Created: 2020-06-25 | Updated: 2020-12-20

Pluto TV(pluto.tv)
In October 2018, the internet television service Pluto TV suffered a data breach which was then shared extensively in hacking communities. Pluto TV "decided not to proactively inform users of the breach" which contained 3.2M unique email and IP addresses, names, usernames, genders, dates of birth and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 3225080 | Created: 2018-10-12 | Updated: 2020-12-05

Cit0day(cit0day.in)
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

Bonobos(bonobos.com)
In August 2020, the clothing store Bonobos suffered a data breach that exposed almost 70GB of data containing 2.8 million unique email addresses. The breach also exposed names, physical and IP addresses, phone numbers, order histories and passwords stored as salted SHA-512 hashes, including historical passwords. The breach also exposed partial credit card data including card type, the name on the card, expiry date and the last 4 digits of the card. The data was provided to HIBP by dehashed.com.

Count: 2811929 | Created: 2020-08-14 | Updated: 2021-01-31

Nitro(gonitro.com)
In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.

Count: 77159696 | Created: 2020-09-28 | Updated: 2021-01-19

Jobandtalent(jobandtalent.com)
In approximately February 2018, the employment website Jobandtalent suffered a data breach which then appeared for sale alongside other breaches a year later. The incident impacted 11 million subscribers and exposed their names, email and IP addresses and passwords stored as salted SHA-1 hashes.

Count: 10981207 | Created: 2018-02-01 | Updated: 2021-01-17

Glofox(glofox.com)
In March 2020, the Irish gym management software company Glofox suffered a data breach which exposed 2.3M membership records. The data included email addresses, names, phone numbers, genders, dates of birth and passwords stored as unsalted MD5 hashes.

Count: 2330735 | Created: 2020-03-27 | Updated: 2021-01-10

Peatix(peatix.com)
In January 2019, the event organising platform Peatix suffered a data breach. The incident exposed 4.2M email addresses, names and salted password hashes. The data was provided to HIBP by dehashed.com.

Count: 4227907 | Created: 2019-01-20 | Updated: 2020-12-06

Experian (2015)(experian.com)
In September 2015, the US based credit bureau and consumer data broker Experian suffered a data breach that impacted 15 million customers who had applied for financing from T-Mobile. An alleged data breach was subsequently circulated containing personal information including names, physical and email addresses, birth dates and various other personal attributes. Multiple Have I Been Pwned subscribers verified portions of the data as being accurate, but the actual source of it was inconclusive therefor this breach has been flagged as "unverified".

Count: 7196890 | Created: 2015-09-16 | Updated: 2020-11-22

123RF(123rf.com)

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.

Count: 226883414 | Created: 2020-11-04 | Updated: 2020-11-19

Home Chef(homechef.com)
In early 2020, the food delivery service Home Chef suffered a data breach which was subsequently sold online. The breach exposed the personal information of almost 9 million customers including names, IP addresses, post codes, the last 4 digits of credit card numbers and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 8815692 | Created: 2020-02-10 | Updated: 2020-11-13

Lazada RedMart(redmart.lazada.sg)
In October 2020, news broke of Lazada RedMart data breach containing records as recent as July 2020 and being sold via an online marketplace. In all, the data contained 1.1 million customer email addresses alongside names, phone numbers, physical addresses, partial credit card numbers and passwords stored as SHA-1 hashes.

Count: 1107789 | Created: 2020-07-30 | Updated: 2020-11-10

James(jamesdelivery.com.br)
In June 2020, 14 previously undisclosed data breaches appeared for sale including the Brazilian delivery service, "James". The breach occurred in March 2020 and exposed 1.5M unique email addresses, customer locations expressed in longitude and latitude and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 1541284 | Created: 2020-03-25 | Updated: 2020-11-05

Promofarma(promofarma.com)
In August 2019, a data breach from the Spanish online pharmacy Promofarma appeared for sale on a dark web marketplace. The breach exposed over 2.7M records and contained almost 1.3M unique customer email addresses. The data also included customer names and was provided to HIBP by dehashed.com.

Count: 1277761 | Created: 2019-08-03 | Updated: 2020-11-03

StarTribune(startribune.com)
In October 2019, the Minnesota-based news service StarTribune suffered a data breach which was subsequently sold on the dark web. The breach exposed over 2 million unique email addresses alongside names, usernames, physical addresses, dates of birth, genders and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 2192857 | Created: 2019-10-10 | Updated: 2020-10-31

Chowbus(chowbus.com)
In October 2020, the Asian food delivery app Chowbus suffered a data breach which led to over 800,000 records being emailed to customers. The email contained a link to a CSV file with customer data including physical addresses, names, phone numbers and over 444,000 unique email addresses.

Count: 444224 | Created: 2020-10-05 | Updated: 2020-10-06

LiveAuctioneers(liveauctioneers.com)
In June 2020, the online antiques marketplace

In March 2020, the stock photo site 123RF suffered a data breach which impacted over 8 million subscribers and was subsequently sold online. The breach included email, IP and physical addresses, names, phone numbers and passwords stored as MD5 hashes. The data was provided to HIBP by dehashed.com.

Count: 8661578 | Created: 2020-03-22 | Updated: 2020-11-15

Animal Jam(animaljam.com)
In October 2020, the online game for kids Animal Jam suffered a data breach which was subsequently shared through online hacking communities the following month. The data contained 46 million user accounts with over 7 million unique email addresses. Impacted data also included usernames, IP addresses and for some records, dates of birth (sometimes in partial form), physical addresses, parent names and passwords stored as PBKDF2 hashes.

Count: 7104998 | Created: 2020-10-12 | Updated: 2020-11-12

Mashable(mashable.com)
In approximately mid-2020, Mashable suffered a data breach that subsequently turned up publicly in November 2020. The data included 1.4 million unique email addresses along with names, genders, expired auth tokens, physical locations, links to social media profiles and days and months of birth. The data was provided to HIBP by dehashed.com.

Count: 1414677 | Created: 2020-06-01 | Updated: 2020-11-10

Wongnai(wongnai.com)
In October 2020, 17 previously undisclosed data breaches appeared for sale including the Thai restaurant, hotel and attraction finding service, Wongnai. The breach exposed almost 4M unique customer records from some time during 2020 along with names, phone numbers, links to social media profiles and passwords stored as MD5 hashes. The data was self-submitted to HIBP by Wongnai.

Count: 3924454 | Created: 2020-10-28 | Updated: 2020-11-05

Minted(minted.com)
In May 2020, the online marketplace for independent artists Minted suffered a data breach that exposed 4.4M unique customer records subsequently sold on a dark web marketplace. Exposed data also included names, physical addresses, phone numbers and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 4418182 | Created: 2020-05-06 | Updated: 2020-11-03

Reincubate(reincubate.com)
In October 2020, the app data company Reincubate suffered a data breach which exposed a backup from November 2017 (the newest record in the data appeared several months earlier). The data included over 616k unique email addresses, names and passwords stored as PBKDF2 hashes.

Count: 616146 | Created: 2017-05-11 | Updated: 2020-10-29

Experian (South Africa)()
In August 2020, Experian South Africa suffered a data breach which exposed the personal information of tens of millions of individuals. Only 1.3M of the records contained email addresses, whilst most contained government issued identity numbers, names, addresses, occupations and employers, amongst other person information.

Count: 1284637 | Created: 2020-08-19 | Updated: 2020-09-02

LiveAuctioneers suffered a data breach which was subsequently sold online then extensively redistributed in the hacking community. The data contained 3.4 million records including names, email and IP addresses, physical addresses, phones numbers and passwords stored as unsalted MD5 hashes. The data was provided to HIBP by breachbase.pw.

Count: 3385862 | Created: 2020-06-19 | Updated: 2020-08-22

Utah Gun Exchange(utahgunexchange.com)
In July 2020, the Utah Gun Exchange website suffered a data breach which included several other associated websites. In total, 235k unique email addresses were exposed before being traded online alongside names, usernames, genders, IP addresses and password hashes. The data was provided to HIBP by breachbase.pw.

Count: 235233 | Created: 2020-07-17 | Updated: 2020-08-19

Catho(catho.com.br)
In approximately March 2020, the Brazilian recruitment website Catho was compromised and subsequently appeared alongside 20 other breached websites listed for sale on a dark web marketplace. The breach included almost 11 million records with 1.2 million unique email addresses. Names, usernames and plain text passwords were also exposed. The data was provided to HIBP by breachbase.pw.

Count: 1173012 | Created: 2020-03-01 | Updated: 2020-08-18

Army Force Online(armyforceonline.com)
In May 2016, the online gaming site Army Force Online suffered a data breach that exposed 1.5M accounts. The breached data was found being regularly traded online and included usernames, email and IP addresses and MD5 passwords.

Count: 1531235 | Created: 2016-05-18 | Updated: 2020-08-07

JoomlArt(joomlart.com)
In January 2018, the Joomla template website JoomlArt inadvertently exposed more than 22k unique customer records in a Jira ticket. The exposed data was from iJoomla and JomSocial, both services that JoomlArt acquired the previous year. The data included usernames, email addresses, purchases and passwords stored as MD5 hashes. When contacted, JoomlArt advised they were aware of the incident and had previously notified impacted parties.

Count: 22477 | Created: 2018-01-30 | Updated: 2020-08-07

Muslim Match(muslimmatch.com)
In June 2016, the Muslim Match dating website had 150k email addresses exposed. The data included private chats and messages between relationship seekers and numerous other personal attributes including passwords hashed with MD5.

Count: 149830 | Created: 2016-06-24 | Updated: 2020-08-07

ProctorU(proctoru.com)
In June 2020, the online exam service ProctorU suffered a data breach which was subsequently shared extensively across online hacking communities. The breach contained 444k user records including names, email and physical addresses, phones numbers and passwords stored as bcrypt hashes. The data was provided to HIBP by breachbase.pw.

Count: 444453 | Created: 2020-06-26 | Updated: 2020-08-06

Unico Campania(unicocampania.it)
In August 2020, the Neapolitan public transport website Unico Campania was hacked and the data extensively circulated. The breach contained 166k user records with email addresses and plain text passwords.

Count: 166031 | Created: 2020-08-19 | Updated: 2020-08-19

Sonicbids(sonicbids.com)
In December 2019, the booking website Sonicbids suffered a data breach which they attributed to "a data privacy event involving our third-party cloud hosting services". The breach contained 752k user records including names and usernames, email addresses and passwords stored as PBKDF2 hashes. The data was provided to HIBP by breachbase.pw.

Count: 751700 | Created: 2019-12-30 | Updated: 2020-08-18

Android Forums(androidforums.com)
In October 2011, the Android Forums website was hacked and 745k user accounts were subsequently leaked publicly. The compromised data included email addresses, user birth dates and passwords stored as a salted MD5 hash.

Count: 745355 | Created: 2011-10-30 | Updated: 2020-08-07

HTH Studios(hthstudios.com)
In August 2018, the adult furry interactive game creator HTH Studios suffered a data breach impacting multiple repositories of customer data. Several months later, the data surfaced on a popular hacking forum and included 411k unique email addresses along with physical and IP addresses, names, orders, salted SHA-1 and salted MD5 hashes. HTH Studios is aware of the incident.

Count: 411755 | Created: 2018-08-24 | Updated: 2020-08-07

Kreditplus(kreditplus.com)
In June 2020, the Indonesian credit service Kreditplus suffered a data breach which exposed 896k records containing 769k unique email addresses. The breach exposed extensive personal information including names, family makeup, information on spouses, income and expenses, religions and employment information. The data was provided to HIBP by breachbase.pw.

Count: 768890 | Created: 2020-06-23 | Updated: 2020-08-07

Zoosk (2020)(zoosk.com)
In January 2020, the online dating service Zoosk suffered a data breach which was subsequently shared extensively across online hacking communities. The breach contained 24 million unique email addresses alongside extensive personal information including genders, sexualities, dates of birth, physical attributes such as height and weight, religions, ethnicities and political views. The breach also allegedly exposed MD5 password hashes, although the data circulating in hacking circles had this field nulled out. The breach was provided to HIBP by breachbase.pw.

Count: 23927853 | Created: 2020-01-12 | Updated: 2020-08-07

Zoosk (2011)(zoosk.com)
In approximately 2011, an alleged breach of the dating website Zoosk began circulating. Comprised of almost 53 million records, the data contained email addresses and plain text passwords. However, during extensive verification in May 2016 no evidence could be found that the data was indeed sourced from the dating service. This breach has consequently been flagged as fabricated; it's highly unlikely the data was sourced from Zoosk.

Count: 52578183 | Created: 2011-01-01 | Updated: 2020-08-06

TrueFire(truefire.com)
In February 2020, the guitar tuition website TrueFire suffered a data breach which impacted 600k members. The breach exposed extensive personal information including names, email and physical addresses, account balances and unsalted MD5 password hashes. The data was provided to HIBP by dehashed.com.

Count: 599667 | Created: 2020-02-21 | Updated: 2020-08-02

Havenly(havenly.com)
In June 2020, the interior design website Havenly suffered a data breach which impacted almost 1.4 million members of the service. The exposed data included email addresses, names, phone numbers, geographic locations and passwords stored as SHA-1 hashes, all of which was subsequently shared extensively throughout online hacking communities. The data was provided to HIBP by dehashed.com.

Count: 1369180 | Created: 2020-06-25 | Updated: 2020-08-01

Swvl(swvl.com)
In June 2020, the Egyptian bus operator Swvl suffered a data breach which impacted over 4 million members of the service. The exposed data included names, email addresses, phone numbers, profile photos, partial credit card data (type and last 4 digits) and passwords stored as bcrypt hashes, all of which was subsequently shared extensively throughout online hacking communities. The data was provided to HIBP by breachbase.pw.

Count: 4195918 | Created: 2020-06-23 | Updated: 2020-07-31

Appen(appen.com)
In June 2020, the AI training data company Appen suffered a data breach exposing the details of almost 5.9 million users which were subsequently sold online. Included in the breach were names, email addresses and passwords stored as bcrypt hashes. Some records also contained phone numbers, employers and IP addresses. The data was provided to HIBP by dehashed.com.

Count: 5888405 | Created: 2020-06-22 | Updated: 2020-07-30

Dunzo(dunzo.com)
In approximately June 2019, the Indian delivery service Dunzo suffered a data breach. Exposing 3.5 million unique email addresses, the Dunzo breach also included names, phone numbers and IP addresses which were all broadly distributed online via a hacking forum. The data was provided to HIBP by dehashed.com.

Count: 3465259 | Created: 2020-06-19 | Updated: 2020-07-29

Dave(dave.com)
In June 2020, the digital banking app Dave suffered a data breach which exposed 7.5 million rows of data and subsequently appeared for public download on a hacking forum. The breach exposed extensive personal information including almost 3 million unique email addresses alongside names, dates of birth, encrypted social security numbers and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 2964182 | Created: 2020-06-28 | Updated: 2020-07-27

Promo(promo.com)
In July 2020, the self-proclaimed "World's #1 Marketing Video Maker" Promo suffered a data breach which was then shared extensively on a hacking forum. The incident exposed 22 million records containing almost 15 million unique email addresses alongside IP addresses,

DecoratingTheHouse(ggumim.co.kr)
In March 2020, the Korean interior decoration website ???? (Decorating the House) suffered a data breach which impacted almost 1.3 million members. Served via the URL ggumim.co.kr, the exposed data included email addresses, names, usernames and phone numbers, all of which was subsequently shared extensively throughout online hacking communities. The data was provided to HIBP by breachbase.pw.

Count: 1298651 | Created: 2020-03-27 | Updated: 2020-08-02

Vakinha(vakinha.com.br)
In June 2020, the Brazilian fund raising service Vakinha suffered a data breach which impacted almost 4.8 million members. The exposed data included email addresses, names, phone numbers, geographic locations and passwords stored as bcrypt hashes, all of which was subsequently shared extensively throughout online hacking communities. The data was provided to HIBP by dehashed.com.

Count: 4775203 | Created: 2020-06-22 | Updated: 2020-08-01

Scentbird(scentbird.com)
In June 2020, the online fragrance service Scentbird suffered a data breach that exposed the personal information of over 5.8 million customers. Personal information including names, email addresses, genders, dates of birth, passwords stored as bcrypt hashes and indicators of password strength were all exposed. The data was provided to HIBP by breachbase.pw.

Count: 5814988 | Created: 2020-06-22 | Updated: 2020-07-30

Chatbooks(chatbooks.com)
In March 2020, the photo print service Chatbooks suffered a data breach which was subsequently put up for sale on a dark web marketplace. The breach contained 15 million user records with 2.5 million unique email addresses alongside names, phone numbers, social media profiles and salted SHA-512 password hashes. The data was provided to HIBP by dehashed.com.

Count: 2520441 | Created: 2020-03-26 | Updated: 2020-07-29

Drizly(drizly.com)
In approximately July 2020, the US-based online alcohol delivery service Drizly suffered a data breach. The data was sold online before being extensively redistributed and contained 2.5 million unique email addresses alongside names, physical and IP addresses, phone numbers, dates of birth and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 2479044 | Created: 2020-07-02 | Updated: 2020-07-28

Hurb(hurb.com)
In approximately March 2019, the online Brazilian travel agency Hurb (formerly Hotel Urbano) suffered a data breach. The data subsequently appeared online for download the following year and included over 20 million customer records with email and IP addresses, names, dates of birth, phone numbers and passwords stored as unsalted MD5 hashes. The data was provided to HIBP by dehashed.com.

Count: 20727771 | Created: 2019-03-14 | Updated: 2020-07-27

Coupon Mom / Armor Games()
In 2014, a file allegedly containing data hacked from Coupon Mom was created and included 11 million email addresses and plain text passwords. On further investigation, the file was also found to contain data indicating it had been sourced from Armor Games. Subsequent verification with HIBP subscribers confirmed the passwords had previously been used and many subscribers had used either Coupon Mom or Armor Games in the past. On disclosure to both

genders, names and salted SHA-256 password hashes. The data was provided to HIBP by dehashed.com.

Count: 14610585 | Created: 2020-06-22 | Updated: 2020-07-26

Wattpad(wattpad.com)
In June 2020, the user-generated stories website Wattpad suffered a huge data breach that exposed almost 270 million records. The data was initially sold then published on a public hacking forum where it was broadly shared. The incident exposed extensive personal information including names and usernames, email and IP addresses, genders, birth dates and passwords stored as bcrypt hashes.

Count: 268765495 | Created: 2020-06-29 | Updated: 2020-07-19

Quidd(quidd.co)
In 2019, online marketplace for trading stickers, cards, toys, and other collectibles Quidd suffered a data breach. The breach exposed almost 4 million users' email addresses, usernames and passwords stored as bcrypt hashes. The data was subsequently sold then redistributed extensively via hacking forums.

Count: 3805863 | Created: 2019-07-01 | Updated: 2020-06-24

Mathway(mathway.com)
In January 2020, the math solving website Mathway suffered a data breach that exposed over 25M records. The data was subsequently sold on a dark web marketplace and included names, Google and Facebook IDs, email addresses and salted password hashes.

Count: 25692862 | Created: 2020-01-13 | Updated: 2020-06-05

Lead Hunter()
In March 2020, a massive trove of personal information referred to as "Lead Hunter" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. The data contained 69 million unique email addresses across 110 million rows of data accompanied by additional personal information including names, phone numbers, genders and physical addresses. At the time of publishing, the breach could not be attributed to those responsible for obtaining and exposing it. The data was provided to HIBP by dehashed.com.

Count: 68693853 | Created: 2020-03-04 | Updated: 2020-06-03

Wishbone (2020)(wishbone.io)
In January 2020, the mobile app to "compare anything" Wishbone suffered another data breach 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 "All3in".

Count: 9705172 | Created: 2020-01-27 | Updated: 2020-05-28

PetFlow(petflow.com)
In December 2017, the pet care delivery service PetFlow suffered a data breach which consequently appeared for sale on a dark web marketplace. Almost 1M accounts were impacted and exposed email addresses and passwords stored as unsalted MD5 hashes. The data was provided to HIBP by a source who requested it be attributed to "nano@databases.pw".

organisations, each found that the data did not represent their entire customer base and possibly includes records from other sources with common subscribers. The breach has subsequently been flagged as "unverified" as the source cannot be emphatically proven. In July 2020, the data was also found to contain BeerAdvocate accounts sourced from a previously unknown breach.

Count: 11010525 | Created: 2014-02-08 | Updated: 2020-07-21

Tokopedia(tokopedia.com)
In April 2020, Indonesia's largest online store Tokopedia suffered a data breach. The incident resulted in 15M rows of data being posted to a popular hacking forum. An additional 76M rows were later provided to HIBP in July 2020. In total, the data included over 71M unique email addresses alongside names, genders, birth dates and passwords stored as SHA2-384 hashes.

Count: 71443698 | Created: 2020-04-17 | Updated: 2020-07-17

Foodora(foodora.com)
In April 2016, the online food delivery service Foodora suffered a data breach which was then extensively redistributed online. The breach included the personal information of hundreds of thousands of customers from multiple countries including their names, delivery addresses, phone numbers and passwords stored as either a salted MD5 or a bcrypt hash.

Count: 582578 | Created: 2016-04-22 | Updated: 2020-06-16

Zoomcar(zoomcar.com)
In July 2018, the Indian self-drive car rental company Zoomcar suffered a data breach which was subsequently sold on a dark web marketplace in 2020. The breach exposed over 3.5M records including names, email and IP addresses, phone numbers and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 3589795 | Created: 2018-07-01 | Updated: 2020-06-05

Wishbone (2016)(wishbone.io)
In August 2016, the mobile app to "compare anything" known as Wishbone suffered a data breach. The data contained 9.4 million records with 2.2 million unique email addresses and was allegedly a subset of the complete data set. The exposed data included genders, birthdates, email addresses and phone numbers for an audience predominantly composed of teenagers and young adults.

Count: 2247314 | Created: 2016-08-07 | Updated: 2020-05-28

LiveJournal(livejournal.com)
In mid-2019, news broke of an alleged LiveJournal data breach. This followed multiple reports of credential abuse against Dreamwidth beginning in 2018, a fork of LiveJournal with a significant crossover in user base. The breach allegedly dates back to 2017 and contains 26M unique usernames and email addresses (both of which have been confirmed to exist on LiveJournal) alongside plain text passwords. An archive of the data was subsequently shared on a popular hacking forum in May 2020 and redistributed broadly. The data was provided to HIBP by a source who requested it be attributed to "nano@databases.pw".

Count: 26372781 | Created: 2017-01-01 | Updated: 2020-05-26

Artsy(artsy.net)
In April 2018, the online arts database Artsy suffered a data breach which consequently appeared for sale on a dark web marketplace. Over 1M accounts were impacted and included IP and email addresses, names and passwords stored as salted SHA-512 hashes. The data was provided to HIBP by a source who requested it be attributed to "nano@databases.pw".

Count: 990919 | Created: 2017-12-09 | Updated: 2020-05-26

Lifebear(lifebear.com)
In early 2019, the Japanese schedule app Lifebear appeared for sale on a dark web marketplace amongst a raft of other hacked websites. The breach exposed almost 3.7M unique email addresses, usernames and passwords stored as salted MD5 hashes. The data was provided to HIBP by a source who requested it be attributed to "nano@databases.pw".

Count: 3670561 | Created: 2019-02-28 | Updated: 2020-05-25

Nulled.ch(nulled.ch)
In May 2020, the hacking forum Nulled.ch was breached and the data published to a rival hacking forum. Over 43k records were compromised and included IP and email addresses, usernames and passwords stored as salted MD5 hashes alongside the private message history of the website's admin. The data was provided to HIBP by a source who requested it be attributed to "Split10".

Count: 43491 | Created: 2020-05-20 | Updated: 2020-05-24

Ulmon(ulmon.com)
In January 2020, the travel app creator Ulmon suffered a data breach. The service had almost 1.3M records with 777k unique email addresses, names, passwords stored as bcrypt hashes and in some cases, social media profile IDs, telephone numbers and bios. The data was subsequently posted to a popular hacking forum.

Count: 777769 | Created: 2020-01-26 | Updated: 2020-05-08

TaiLieu(tailieu.vn)
In November 2019, the Vietnamese education website TaiLieu allegedly suffered a data breach exposing 7.3M customer records. Impacted data included names and usernames, email addresses, dates of birth, genders and passwords stored as unsalted MD5 hashes. The data was provided to HIBP by dehashed.com after being shared on a popular hacking forum. TaiLieu did not respond when contacted about the incident.

Count: 7327477 | Created: 2019-11-24 | Updated: 2020-05-03

Aptoide(aptoide.com)
In April 2020, the independent Android app store Aptoide suffered a data breach. The incident resulted in the exposure of 20M customer records which were subsequently shared online via a popular hacking forum. Impacted data included email and IP addresses, names, IP addresses and passwords stored as SHA-1 hashes without a salt.

Count: 20012235 | Created: 2020-04-13 | Updated: 2020-04-19

OGUsers (2019 breach)(ogusers.com)
In May 2019, the account hijacking and SIM swapping forum OGusers suffered a data breach. The breach exposed a database backup from December 2018 which was published on a rival hacking forum. There were 161k unique email addresses spread across 113k forum users and other tables in the database. The exposed data also included usernames, IP addresses, private messages and passwords stored as salted MD5 hashes.

Count: 161143 | Created: 2018-12-26 | Updated: 2020-04-04

Dueling Network(duelingnetwork.com)
In March 2017, the Flash game based on the

Count: 1079970 | Created: 2018-04-01 | Updated: 2020-05-25

Nulled.cr(nulled.cr)
In May 2016, the cracking community forum known as Nulled.cr was hacked and 599k user accounts were leaked publicly. The compromised data included email and IP addresses, weak salted MD5 password hashes and hundreds of thousands of private messages between members.

Count: 599080 | Created: 2016-05-06 | Updated: 2020-05-24

Covve(covve.com)
In February 2020, a massive trove of personal information referred to as "db8151dd" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. Later identified as originating from the Covve contacts app, the exposed data included extensive personal information and interactions between Covve users and their contacts. The data was provided to HIBP by dehashed.com.

Count: 22802117 | Created: 2020-02-20 | Updated: 2020-05-19

Elanic(elanic.in)
In January 2020, the Indian fashion marketplace Elanic had 2.8M records with 2.3M unique email addresses posted publicly to a popular hacking forum. Elanic confirmed that they had "verified the data and it was pulled from one of our test servers where this data was exposed publicly" and that the data was "old" (the hacking forum reported it as being from 2016-2018). When asked about disclosure to impacted customers, Elanic advised that they had "decided to not have as such any communication and public disclosure".

Count: 2325283 | Created: 2018-01-01 | Updated: 2020-05-04

Vianet(vianet.com.np)
In April 2020, the Nepalese internet service provider Vianet suffered a data breach. The attack on the ISP led to the exposure of 177k customer records including 94k unique email addresses. Also exposed were names, phone numbers and physical addresses.

Count: 94353 | Created: 2020-04-08 | Updated: 2020-04-22

HTC Mania(htcmania.com)
In January 2020, the Spanish mobile phone forum HTC Mania suffered a data breach of the vBulletin based site. The incident exposed 1.5M member email addresses, usernames, IP addresses, dates of birth and salted MD5 password hashes and password histories. Data from the breach was subsequently redistributed on popular hacking websites.

Count: 1488089 | Created: 2020-01-04 | Updated: 2020-04-06

OGUsers (2020 breach)(ogusers.com)
In April 2020, the account hijacking and SIM swapping forum OGUsers suffered their second data breach in less than a year. As with the previous breach, the exposed data included email and IP addresses, usernames, private messages and passwords stored as salted MD5 hashes. A total of 263k email addresses across user accounts and other tables were posted to a rival hacking forum.

Count: 263189 | Created: 2020-04-02 | Updated: 2020-04-04

PropTiger(proptiger.com)

Yu-Gi-Oh trading card game Dueling Network suffered a data breach. The site itself was taken offline in 2016 due to a cease-and-desist order but the forum remained online for another year. The data breach exposed usernames, IP and email addresses and passwords stored as MD5 hashes. The data was provided to HIBP by a source who requested it be attributed to "burger vault".

Count: 6486626 | Created: 2017-03-29 | Updated: 2020-03-31

Tamodo(tamodo.com)
In February 2020, the affiliate marketing network Tamodo suffered a data breach which was subsequently shared on a popular hacking forum. The incident exposed almost 500k accounts including names, email addresses, dates of birth and passwords stored as bcrypt hashes. Tamodo failed to respond to multiple attempts to report the breach via published communication channels.

Count: 494945 | Created: 2020-02-28 | Updated: 2020-03-24

AnimeGame(animegame.me)
In February 2020, the gaming website AnimeGame suffered a data breach. The incident affected 1.4M subscribers and exposed email addresses, usernames and passwords stored as salted MD5 hashes. The data was subsequently shared on a popular hacking forum and was provided to HIBP by dehashed.com.

Count: 1431378 | Created: 2020-02-27 | Updated: 2020-03-09

Slickwraps(slickwraps.com)
In February 2020, the online store for consumer electronics wraps Slickwraps suffered a data breach. The incident resulted in the exposure of 858k unique email addresses across customer records and newsletter subscribers. Additional impacted data included names, physical addresses, phone numbers and purchase histories.

Count: 857611 | Created: 2020-02-16 | Updated: 2020-02-22

Adult FriendFinder (2015) (adultfriendfinder.com)
In May 2015, the adult hookup site Adult FriendFinder was hacked and nearly 4 million records dumped publicly. The data dump included extremely sensitive personal information about individuals and their relationship statuses and sexual preferences combined with personally identifiable information.

Count: 3867997 | Created: 2015-05-21 | Updated: 2020-02-07

DailyObjects(dailyobjects.com)
In approximately January 2018, a collection of more than 464k customer records from the Indian online retailer DailyObjects were leaked online. The data included names, physical and email addresses, phone numbers and "pincodes" stored in plain text. After multiple attempts to contact them, DailyObjects responded and received a copy of the data for verification, however failed to respond to multiple contact attempts following that.

Count: 464260 | Created: 2018-01-01 | Updated: 2020-01-28

europa.jobs(europa.jobs)
In August 2019, the now defunct European jobs website europa.jobs (Google cache link) suffered a data breach. The incident exposed 226k unique email addresses alongside extensive personal information including names, dates of birth, job applications and passwords. The data was subsequently redistributed on a popular hacking forum.

In January 2018, the Indian property website PropTiger suffered a data breach which resulted in a 3.46GB database file being exposed and subsequently shared extensively on a popular hacking forum 2 years later. The exposed data contained both user records and login histories with over 2M unique customer email addresses. Exposed data also included additional personal attributes such as names, dates of birth, genders, IP addresses and passwords stored as MD5 hashes. PropTiger advised they believe the usability of the data is "limited" due to how certain data attributes were generated and stored. The data was provided to HIBP by dehashed.com.

Count: 2156921 | Created: 2018-01-30 | Updated: 2020-03-24

The Halloween Spot(thehalloweenspot.com)
In September 2019, the Halloween costume store The Halloween Spot suffered a data breach. Originally misattributed to fancy dress store Smiffys, the breach contained 13GB of data with over 10k unique email addresses alongside names, physical and IP addresses, phone numbers and order histories. The Halloween Spot advised customers the breach was traced back to "an old shipping information database".

Count: 10653 | Created: 2019-09-27 | Updated: 2020-03-16

Straffic(straffic.io)
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".

Count: 48580249 | Created: 2020-02-14 | Updated: 2020-02-27

MGM Resorts(mgmresorts.com)
In July 2019, MGM Resorts discovered a data breach of one of their cloud services. The breach included 10.6M guest records with 3.1M unique email addresses stemming back to 2017. The exposed data included email and physical addresses, names, phone numbers and dates of birth and was subsequently shared on a popular hacking forum in February 2020 where it was extensively redistributed. The data was provided to HIBP by Under The Breach.

Count: 3081321 | Created: 2019-07-25 | Updated: 2020-02-20

Adult FriendFinder (2016)(adultfriendfinder.com)
In October 2016, the adult entertainment company Friend Finder Networks suffered a massive data breach. The incident impacted multiple separate online assets owned by the company, the largest of which was the Adult FriendFinder website alleged to be "the world's largest sex & swinger community". Exposed data included usernames, passwords stored as SHA-1 hashes and 170 million unique email addresses. This incident is separate to the 2015 data breach Adult FriendFinder also suffered. The data was provided to HIBP by dehashed.com.

Count: 169746810 | Created: 2016-10-16 | Updated: 2020-02-07

Tout(tout.com)
In approximately September 2014, the now defunct social networking service Tout suffered a data breach. The breach subsequently appeared years later and included 653k unique email addresses, names, IP addresses, the location of the user, their bio and passwords stored as bcrypt hashes. The data was provided to HIBP by a source who requested it to be attributed to "nmapthis@protonmail.com".

Count: 652683 | Created: 2014-09-11 | Updated: 2020-01-25

Planet Calypso(planetcalypsoforum.com)
In approximately July 2019, the forums for the Planet Calypso game suffered a data breach. The breach of the vBulletin based forum exposed email and IP addresses, usernames and passwords stored as salted MD5 hashes.

Count: 62261 | Created: 2019-07-01 | Updated: 2020-01-12

Count: 226095 | Created: 2019-08-11 | Updated: 2020-01-15

BtoBet(btobet.com)
In December 2019, a large collection of data from Nigerian gambling company Surebet247 was sent to HIBP. Alongside the Surebet247, database backups from gambling sites BetAlfa, BetWay, BongoBongo and TopBet was also included. Further investigation implicated betting platform provider BtoBet as being the common source of the data. Impacted data included user records and extensive information on gambling histories.

Count: 444241 | Created: 2019-12-26 | Updated: 2020-01-11

Zynga(zynga.com)
In September 2019, game developer Zynga (the creator of Words with Friends) suffered a data breach. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.

Count: 172869660 | Created: 2019-09-01 | Updated: 2020-01-11

Universarium(universarium.org)
In approximately November 2019, the Russian "Remote preparatory faculty for IT specialties" Universarium suffered a data breach. The incident exposed 565k email addresses and passwords in plain text. Universarium did not respond to multiple attempts to make contact over a period of many weeks. The data was provided to HIBP by dehashed.com.

Count: 564962 | Created: 2019-11-01 | Updated: 2020-01-03

GateHub(gatehub.net)
In October 2019, 1.4M accounts from the cryptocurrency wallet service GateHub were posted to a popular hacking forum. GateHub had previously acknowledged a data breach in June, albeit with a smaller number of impacted accounts. Data from the breach included email addresses, mnemonic phrases, encrypted master keys, encrypted recovery keys and passwords stored as bcrypt hashes.

Count: 1408078 | Created: 2019-06-04 | Updated: 2019-12-24

Data Enrichment Exposure From PDL Customer()
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.

Count: 622161052 | Created: 2019-10-16 | Updated: 2019-11-22

GPS Underground(gpsunderground.com)
In early 2017, GPS Underground was amongst a collection of compromised vBulletin websites that were found being sold online. The breach dated back to mid-2016 and included 670k records with usernames, email and IP addresses, dates of birth and salted MD5 password hashes.

Count: 669584 | Created: 2016-07-01 | Updated: 2019-11-19

ToonDoo(toondoo.com)
In August 2019, the comic strip creation website ToonDoo suffered a data breach. The

Go Games(gogames.me)
In approximately October 2015, the manga website Go Games suffered a data breach. The exposed data included 3.4M customer records including email and IP addresses, usernames and passwords stored as salted MD5 hashes. Go Games did not respond when contacted about the incident. The data was provided to HIBP by dehashed.com.

Count: 3430083 | Created: 2015-10-24 | Updated: 2020-01-11

Indian Railways(indianrails.in)
In November 2019, the website for Indian Rail left more than 2M records exposed on an unprotected Firebase database instance. The exposed data included 583k unique email addresses alongside usernames and passwords stored in plain text.

Count: 583377 | Created: 2019-10-28 | Updated: 2020-01-10

Factual(factual.com)
In March 2017, a file containing 8M rows of data allegedly sourced from data aggregator Factual was compiled and later exchanged on the premise it was a "breach". The data contained 2.5M unique email addresses alongside business names, addresses and phone numbers. After consultation with Factual, they advised the data was "publicly available information about businesses and other points of interest that Factual makes available on its website and to customers".

Count: 2461696 | Created: 2017-03-22 | Updated: 2019-12-24

AgusiQ-Torrents.pl(agusiq-torrents.pl)
In September 2019, Polish torrent site AgusiQ-Torrents.pl suffered a data breach. The incident exposed 90k member records including email and IP addresses, usernames and passwords stored as MD5 hashes.

Count: 90478 | Created: 2019-09-24 | Updated: 2019-12-04

EpicBot(epicbot.com)
In September 2019, the RuneScape bot provider EpicBot suffered a data breach that impacted 817k subscribers. Data from the breach was subsequently shared on a popular hacking forum and included usernames, email and IP addresses and passwords stored as either salted MD5 or bcrypt hashes. EpicBot did not respond when contacted about the incident.

Count: 816662 | Created: 2019-09-01 | Updated: 2019-11-19

Minehut(minehut.com)
In May 2019, the Minecraft server website Minehut 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.

Count: 396533 | Created: 2019-05-17 | Updated: 2019-11-17

Vedantu(vedantu.com)

data was subsequently redistributed on a popular hacking forum in November where the personal information of over 6M subscribers was shared. Impacted data included email and IP addresses, usernames, genders, the location of the individual and salted password hashes.

Count: 6002694 | Created: 2019-08-21 | Updated: 2019-11-11

Hookers.nl(hookers.nl)
In October 2019, the Dutch prostitution forum Hookers.nl suffered a data breach which exposed the personal information of sex workers and their customers. The IP and email addresses, usernames and either bcrypt or salted MD5 password hashes of 291k members were accessed via an unpatched vulnerability in the vBulletin forum software.

Count: 290955 | Created: 2019-10-10 | Updated: 2019-10-23

Sephora(sephora.com.au)
In approximately January 2017, the beauty store Sephora suffered a data breach. Impacting customers in South East Asia, Australia and New Zealand, 780k unique email addresses were included in the breach alongside names, genders, dates of birth, ethnicities and other personal information. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 780073 | Created: 2017-01-09 | Updated: 2019-10-06

Wanelo(wanelo.com)
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".

Count: 23165793 | Created: 2018-12-13 | Updated: 2019-10-01

KiwiFarms(kiwifarms.net)
In September 2019, the forum for discussing "lolcows" (people who can be milked for laughs) Kiwi Farms suffered a data breach. The disclosure notice advised that email and IP addresses, dates of birth and content created by members were all exposed in the incident.

Count: 4606 | Created: 2019-09-10 | Updated: 2019-09-17

Poshmark(poshmark.com)
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".

Count: 36395491 | Created: 2018-05-16 | Updated: 2019-09-02

Mastercard Priceless Specials(specials.mastercard.de)
In August 2019, the German Mastercard bonus program "Priceless Specials" suffered a data breach. Personal data on almost 90k program members was subsequently extensively circulated online and included names, email and IP addresses, phone numbers and partial credit card data. Following the incident, the

In mid-2019, the Indian interactive online tutoring platform Vedantu suffered a data breach which exposed the personal data of 687k users. The JSON formatted database dump exposed extensive personal information including email and IP address, names, phone numbers, genders and passwords stored as bcrypt hashes. When contacted about the incident, Vedantu advised that they were aware of the breach and were in the process of informing their customers.

Count: 686899 | Created: 2019-07-08 | Updated: 2019-11-01

Zooville(zooville.org)
In September 2019, the zoophilia and bestiality forum Zooville suffered a data breach. The usernames and email addresses of 71k members were accessed via an unpatched vulnerability in the vBulletin forum software then subsequently distributed online. A second data set was later provided to HIBP which contained a complete vBulletin database dump including IP addresses, dates of birth and passwords stored as bcrypt hashes. The site administrator advised that following the breach, all data had been deleted from the forum and a new one had been stood up on the XenForo platform. The data was provided to HIBP by a source who requested it be attributed to "burger vault".

Count: 71407 | Created: 2019-09-27 | Updated: 2019-10-20

StreetEasy(streeteasy.com)
In approximately June 2016, the real estate website StreetEasy suffered a data breach. In total, 988k unique email addresses were included in the breach alongside names, usernames and SHA-1 hashes of passwords, all of which appeared for sale on a dark web marketplace in February 2019. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 988230 | Created: 2016-06-28 | Updated: 2019-10-06

Lumin PDF(luminpdf.com)
In April 2019, the PDF management service Lumin PDF suffered a data breach. The breach wasn't publicly disclosed until September when 15.5M records of user data appeared for download on a popular hacking forum. The data had been left publicly exposed in a MongoDB instance after which Lumin PDF was allegedly been "contacted multiple times, but ignored all the queries". The exposed data included names, email addresses, genders, spoken language and either a bcrypt password hash or Google auth token. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 15453048 | Created: 2019-04-01 | Updated: 2019-09-18

Void.to(void.to)
In June 2019, the hacking website Void.to 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.

Count: 95431 | Created: 2019-06-13 | Updated: 2019-09-11

XKCD(xkcd.com)
In July 2019, the forum for webcomic XKCD suffered a data breach that impacted 562k subscribers. The breached phpBB forum leaked usernames, email and IP addresses and passwords stored in MD5 phpBB3 format. The data was provided to HIBP by white hat security researcher and data analyst Adam Davies.

Count: 561991 | Created: 2019-07-01 | Updated: 2019-09-01

Coinmama(coinmama.com)
In August 2017, the crypto coin brokerage service Coinmama suffered a data breach that impacted 479k subscribers. The breach was discovered in February 2019 with exposed data including email addresses, usernames and passwords stored as MD5 WordPress hashes. The data was provided to HIBP by white hat security researcher and data analyst Adam Davies.

program was subsequently suspended.

Count: 89388 | Created: 2019-08-20 | Updated: 2019-09-01

8tracks(8tracks.com)
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 employeexe2x80x99s 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.

Count: 17979961 | Created: 2017-06-27 | Updated: 2019-08-25

Cracked.to(cracked.to)
In July 2019, the hacking website Cracked.to 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.

Count: 749161 | Created: 2019-07-21 | Updated: 2019-08-12

Canva(canva.com)
In May 2019, the graphic design tool website Canva suffered a data breach 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".

Count: 137272116 | Created: 2019-05-24 | Updated: 2019-08-09

Club Penguin Rewritten (January 2018) (cprewritten.net)
In January 2018, the children's gaming site Club Penguin Rewritten (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 "contacted affected users".

Count: 1688176 | Created: 2018-01-21 | Updated: 2019-07-30

Anime-Planet(anime-planet.com)
In approximately 2016, the anime website Anime-Planet suffered a data breach that impacted 369k subscribers. The exposed data included usernames, IP and email addresses, dates of birth and passwords stored as unsalted MD5 hashes and for newer accounts, bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 368507 | Created: 2016-01-01 | Updated: 2019-07-28

EpicNPC(epicnpc.com)
In January 2016, the hacked account reseller EpicNPC suffered a data breach that impacted 409k subscribers. The impacted data included usernames, IP and email addresses and passwords stored as salted MD5 hashes. The data was provided to HIBP by dehashed.com.

Count: 478824 | Created: 2017-08-03 | Updated: 2019-08-30

Chegg(chegg.com)
In April 2018, the textbook rental service Chegg suffered a data breach that impacted 40 million subscribers. The exposed data included email addresses, usernames, names and passwords stored as unsalted MD5 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 39721127 | Created: 2018-04-28 | Updated: 2019-08-16

StockX(stockx.com)
In July 2019, the fashion and sneaker trading platform StockX suffered a data breach which was subsequently sold via a dark webmarketplace. The exposed data included 6.8 million unique email addresses, names, physical addresses, purchases and passwords stored as salted MD5 hashes. The data was provided to HIBP by dehashed.com.

Count: 6840339 | Created: 2019-07-26 | Updated: 2019-08-11

CafePress(cafepress.com)
In February 2019, the custom merchandise retailer CafePress suffered a data breach. The exposed data included 23 million unique email addresses with some records also containing names, physical addresses, phone numbers and passwords stored as SHA-1 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 23205290 | Created: 2019-02-20 | Updated: 2019-08-05

Club Penguin Rewritten (July 2019)(cprewritten.net)
In July 2019, the children's gaming site Club Penguin Rewritten (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.

Count: 4007909 | Created: 2019-07-27 | Updated: 2019-07-30

Clash of Kings(f.elex.com)
In July 2016, the forum for the game "Clash of Kings" suffered a data breach that impacted 1.6 million subscribers. The impacted data included usernames, IP and email addresses and passwords stored as MD5 hashes. The data was provided to HIBP by dehashed.com.

Count: 1604957 | Created: 2016-07-14 | Updated: 2019-07-27

Rbx.Rocks(rbx.rocks)
In August 2018, the Roblox trading site Rbx.Rocks suffered a data breach. Almost 25k records were sent to HIBP in November and included names, email addresses and passwords stored as bcrypt hashes. In July 2019, a further 125k records emerged bringing the total size of the incident to 150k. The website has since gone offline with a message stating that "Rbx.Rocks v2.0 is currently under construction".

Count: 408795 | Created: 2016-01-02 | Updated: 2019-07-27

Snail(snail.com)
In March 2015, the gaming website Snail suffered a data breach that impacted 1.4 million subscribers. The impacted data included usernames, IP and email addresses and passwords stored as unsalted MD5 hashes. The data was provided to HIBP by dehashed.com.

Count: 1410899 | Created: 2015-03-14 | Updated: 2019-07-27

Xiaomi(xiaomi.cn)
In August 2012, the Xiaomi user forum website suffered a data breach. In all, 7 million email addresses appeared in the breach although a significant portion of them were numeric aliases on the bbs_ml_as_uid.xiaomi.com domain. Usernames, IP addresses and passwords stored as salted MD5 hashes were also exposed. The data was provided with support from dehashed.com. Read more about Chinese data breaches in Have I Been Pwned.

Count: 7088010 | Created: 2012-08-01 | Updated: 2019-07-21

Flash Flash Revolution (2019 breach)(flashflashrevolution.com)
In July 2019, the music-based rhythm game Flash Flash Revolution suffered a data breach. The 2019 breach imapcted almost 1.9 million members and is *in addition to* the 2016 data breach of the same service. Email and IP addesses, usernames, dates of birth and salted MD5 hashes were all exposed in the breach. The data was provided with support from dehashed.com.

Count: 1858124 | Created: 2019-07-16 | Updated: 2019-07-21

Artvalue(artvalue.com)
In June 2019, the France-based art valuation website Artvalue.com left their 158k member subscriber base publicly exposed in a text file on their website. The exposed data included names, usernames, email addresses and passwords stored as MD5 hashes. The site operator did not respond when contacted about the incident, although the exposed file was subsequently removed.

Count: 157692 | Created: 2019-06-19 | Updated: 2019-07-19

Roll20(roll20.net)
In December 2018, the tabletop role-playing games website Roll20 suffered a data breach. Almost 4 million customers were impacted by the breach and had email and IP addresses, names, bcrypt hashes of passwords and the last 4 digits of credit cards exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 3994436 | Created: 2018-12-26 | Updated: 2019-07-19

Animoto(animoto.com)
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".

Count: 22437749 | Created: 2018-07-10 | Updated: 2019-07-18

BlackSpigotMC(blackspigot.com)
In July 2019, the hacking website BlackSpigotMC suffered a data breach. The XenForo forum based site was allegedly compromised by a rival hacking website and

Count: 149958 | Created: 2018-08-06 | Updated: 2019-07-27

Stronghold Kingdoms(strongholdkingdoms.com)
In July 2018, the massive multiplayer online game Stronghold Kingdoms suffered a data breach. Almost 5.2 million accounts were impacted by the incident which exposed emails addresses, usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 5187305 | Created: 2018-07-04 | Updated: 2019-07-21

Flash Flash Revolution (2016 breach)(flashflashrevolution.com)
In February 2016, the music-based rhythm game known as Flash Flash Revolution was hacked and 1.8M accounts were exposed. Along with email and IP addresses, the vBulletin forum also exposed salted MD5 password hashes.

Count: 1771845 | Created: 2016-02-01 | Updated: 2019-07-21

GameSalad(gamesalad.com)
In February 2019, the education and game creation website Game Salad suffered a data breach. The incident impacted 1.5M accounts and exposed email addresses, usernames, IP addresses and passwords stored as SHA-256 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 1506242 | Created: 2019-02-24 | Updated: 2019-07-21

EatStreet(eatstreet.com)
In May 2019, the online food ordering service EatStreet suffered a data breach affecting 6.4 million customers. An extensive amount of personal data was obtained including names, phone numbers, addresses, partial credit card data 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".

Count: 6353564 | Created: 2019-05-03 | Updated: 2019-07-19

YouNow(younow.com)
In February 2019, data from the live broadcasting service YouNow appeared for sale on a dark web marketplace. Whilst it's not clear what date the actual breach occurred on, the impacted data included 18M unique email addresses, IP addresses, names, usernames and links to social media profiles. As authentication is performed via social providers, no passwords were exposed in the breach. Many records didn't have associated email addresses thus the unique number is lower than the reported total number of accounts. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 18241518 | Created: 2019-02-15 | Updated: 2019-07-18

Bulgarian National Revenue Agency(nap.bg)
In July 2019, a massive data breach of the Bulgarian National Revenue Agency began circulating with data on 5 million people. Allegedly obtained in June, the data was broadly shared online and included taxation information alongside names, phone numbers, physical addresses and 471 thousand unique email addresses. The breach is said to have affected "nearly all adults in Bulgaria".

Count: 471167 | Created: 2019-07-15 | Updated: 2019-07-18

SHEIN(shein.com)
In June 2018, online fashion retailer SHEIN suffered a data breach. The

resulted in 8.5GB of data being leaked including the database and website itself. The exposed data included 140k unique email addresses, usernames, IP addresses, genders, geographic locations and passwords stored as bcrypt hashes.

Count: 140029 | Created: 2019-07-14 | Updated: 2019-07-17

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

Count: 41817893 | Created: 2017-12-07 | Updated: 2019-07-16

Evite(evite.com)
In April 2019, the social planning website for managing online invitations Evite identified a data breach of their systems. Upon investigation, they found unauthorised access to a database archive dating back to 2013. The exposed data included a total of 101 million unique email addresses, most belonging to recipients of invitations. Members of the service also had names, phone numbers, physical addresses, dates of birth, genders and passwords stored in plain text exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 100985047 | Created: 2013-08-11 | Updated: 2019-07-14

Zhenai.com(zhenai.com)
In December 2011, the Chinese dating site known as Zhenai.com suffered a data breach that impacted 5 million subscribers. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and plain text passwords. Read more about Chinese data breaches in Have I Been Pwned.

Count: 5024908 | Created: 2011-12-21 | Updated: 2019-07-11

Social Engineered(socialengineered.net)
In June 2019, the "Art of Human Hacking" site Social Engineered suffered a data breach. The breach of the MyBB forum was published on a rival hacking forum and included 89k unique email addresses spread across 55k forum users and other tables in the database. The exposed data also included usernames, IP addresses, private messages and passwords stored as salted MD5 hashes.

Count: 89392 | Created: 2019-06-13 | Updated: 2019-06-25

Emuparadise(emuparadise.me)
In April 2018, the self-proclaimed "biggest retro gaming website on earth", Emuparadise, suffered a data breach. The compromised vBulletin forum exposed 1.1 million email addresses, IP address, usernames and passwords stored as salted MD5 hashes. The data was provided to HIBP by dehashed.com.

Count: 1131229 | Created: 2018-04-01 | Updated: 2019-06-15

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".

Count: 39086762 | Created: 2018-06-01 | Updated: 2019-07-17

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

Count: 49038354 | Created: 2012-11-01 | Updated: 2019-07-15

MindJolt(mindjolt.com)
In March 2019, the online gaming website MindJolt suffered a data breach that exposed 28M unique email addresses. Also impacted were names and dates of birth, but no passwords. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Count: 28364826 | Created: 2019-03-18 | Updated: 2019-07-13

WienerBuchereien()
In June 2019, the library of Vienna (Wiener Bxc3xbcchereien) suffered a data breach. The compromised data included 224k unique email addresses, names, physical addresses, phone numbers and dates of birth. The breached data was subsequently posted to Twitter by the alleged perpetrator of the breach.

Count: 224119 | Created: 2019-06-10 | Updated: 2019-06-28

D3Scene(d3scene.com)
In January 2016, the gaming website D3Scene, suffered a data breach. The compromised vBulletin forum exposed 569k million email addresses, IP address, usernames and passwords stored as salted MD5 hashes. The data was provided to HIBP by dehashed.com.

Count: 568827 | Created: 2016-01-01 | Updated: 2019-06-15

Ordine Avvocati di Roma(ordineavvocatiroma.it)
In May 2019, the Lawyers Order of Rome suffered a data breach by a group claiming to be Anonymous Italy. Data on tens of thousands of Roman lawyers was taken from the breached system and redistributed online. The data included contact information, email addresses and email messages themselves encompassing tens of thousands of unique email addresses. A total of 42k unique addresses appeared in the breach.

Count: 41960 | Created: 2019-05-07 | Updated: 2019-05-26

Manga Traders(mangatraders.com)
In June 2014, the Manga trading website Mangatraders.com had the usernames and passwords of over 900k users leaked on the internet (approximately 855k of the emails were unique). The passwords were weakly hashed with a single iteration of MD5 leaving them vulnerable to being easily cracked.

Count: 855249 | Created: 2014-06-09 | Updated: 2019-05-13

Appartoo(appartoo.com)
In March 2017, the French Flatsharing site known as Appartoo suffered a data breach. The incident exposed an extensive amount of personal information on almost 50k members including email addresses, genders, ages, private messages sent between users of the service and passwords stored as SHA-256 hashes. Appartoo advised that all subscribers were notified of the incident in early 2017.

Count: 49681 | Created: 2017-03-25 | Updated: 2019-05-02

Bukalapak(bukalapak.com)
In March 2019, the Indonesian e-commerce website Bukalapak discovered a data breach of the organisation's backups dating back to October 2017. The incident exposed approximately 13 million unique email addresses alongside IP addresses, names and passwords stored as bcrypt and salted SHA-512 hashes. The data was provided to HIBP by a source who requested it to be attributed to "Maxime Thalet".

Count: 13369666 | Created: 2017-10-23 | Updated: 2019-04-18

Knuddels(knuddels.de)
In September 2018, the German social media website Knuddels suffered a data breach. The incident exposed 808k unique email addresses alongside usernames, real names, the city of the person and their password in plain text. Knuddels was subsequently fined xe2x82xac20k for the breach.

Count: 808330 | Created: 2018-09-05 | Updated: 2019-04-08

Everybody Edits(everybodyedits.com)
In March 2019, the multiplayer platform game Everybody Edits suffered a data breach. The incident exposed 871k unique email addresses alongside usernames and IP addresses. The data was subsequently distributed online across a collection of files.

Count: 871190 | Created: 2019-03-23 | Updated: 2019-04-03

Whitepages(whitepages.com)
In mid-2016, the telephone and address directory service Whitepages was among a raft of sites that were breached and their data then sold in early-2019. The data included over 11 million unique email addresses alongside names and passwords stored as either a SHA-1 or bcrypt hash. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Count: 11657763 | Created: 2016-06-27 | Updated: 2019-03-27

Bookmate(bookmate.com)
In mid-2018, the social ebook subscription service Bookmate was among a raft of sites that were breached and their data then sold in early-2019. The data included almost 4 million unique email addresses alongside names, genders, dates of birth and passwords stored as salted SHA-512 hashes. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Count: 3830916 | Created: 2018-07-08 | Updated: 2019-03-22

Vodafone(vodafone.is)
In November 2013, Vodafone in Iceland suffered an attack attributed to the Turkish hacker collective "Maxn3y". The data was consequently publicly exposed and included user names, email addresses, social security numbers, SMS message, server logs and passwords from a variety of different internal sources.

Count: 56021 | Created: 2013-11-30 | Updated: 2019-05-13

Morele.net(morele.net)
In October 2018, the Polish e-commerce website Morele.net suffered a data breach. The incident exposed almost 2.5 million unique email addresses alongside phone numbers, names and passwords stored as md5crypt hashes.

Count: 2467304 | Created: 2018-10-10 | Updated: 2019-04-20

DataCamp(datacamp.com)
In December 2018, the data science website DataCamp suffered a data breach of records dating back to January 2017. The incident exposed 760k unique email and IP addresses along with names and passwords stored as bcrypt hashes. 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".

Count: 760561 | Created: 2017-01-30 | Updated: 2019-04-09

Demon Forums(demonforums.net)
In February 2019, the hacking forum Demon Forums suffered a data breach. The compromise of the vBulletin forum exposed 52k unique email addresses alongside usernames and passwords stored as salted MD5 hashes.

Count: 52623 | Created: 2019-02-20 | Updated: 2019-04-04

Intelimost(intelimost.com)
In March 2019, a spam operation known as "Intelimost" sent millions of emails appearing to come from people the recipients knew. Security researcher Bob Diachenko found over 3 million unique email addresses in an exposed Elasticsearch database, alongside plain text passwords used to access the victim's mailbox and customise the spam.

Count: 3073409 | Created: 2019-03-10 | Updated: 2019-04-02

500px(500px.com)
In mid-2018, the online photography community 500px suffered a data breach. The incident exposed almost 15 million unique email addresses alongside names, usernames, genders, dates of birth and either an MD5 or bcrypt password hash. 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".

Count: 14867999 | Created: 2018-07-05 | Updated: 2019-03-25

8fit(8fit.com)
In July 2018, the health and fitness service 8fit suffered a data breach. The data subsequently appeared for sale on a dark web marketplace in February 2019 and included over 15M unique email addresses alongside names, genders, IP addresses and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Count: 15025407 | Created: 2018-07-01 | Updated: 2019-03-21

HauteLook(hautelook.com)
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.

Count: 28510459 | Created: 2018-08-07 | Updated: 2019-03-21

Houzz(houzz.com)
In mid-2018, the housing design website Houzz suffered a data breach. The company learned of the incident later that year then disclosed it to impacted members in February 2019. Almost 49 million unique email addresses were in the breach alongside names, IP addresses, geographic locations and either salted hashes of passwords or links to social media profiles used to authenticate to the service. The data was provided to HIBP by dehashed.com.

Count: 48881308 | Created: 2018-05-23 | Updated: 2019-03-12

Verifications.io(verifications.io)
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.

Count: 763117241 | Created: 2019-02-25 | Updated: 2019-03-09

MyFitnessPal(myfitnesspal.com)
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".

Count: 143606147 | Created: 2018-02-01 | Updated: 2019-02-21

EyeEm(eyeem.com)
In February 2018, photography website EyeEm suffered a data breach. The breach was identified among a collection of other large incidents and exposed almost 20M unique email addresses, names, usernames, bios and password hashes. The data was provided to HIBP by a source who asked for it to be attributed to "Kuroi'sh or Gabriel Kimiaie-Asadi Bildstein".

Count: 19611022 | Created: 2018-02-28 | Updated: 2019-02-16

Collection #1()
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

ixigo(ixigo.com)
In January 2019, the travel and hotel booking site ixigo suffered a data breach. The data appeared for sale on a dark web marketplace the following month and included over 17M unique email addresses alongside names, genders, phone numbers, connections to Facebook profiles and passwords stored as MD5 hashes. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Count: 17204697 | Created: 2019-01-03 | Updated: 2019-03-17

ShareThis(sharethis.com)
In July 2018, the social bookmarking and sharing service ShareThis suffered a data breach. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and password hashes. 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 dehashed.com.

Count: 40960499 | Created: 2018-07-09 | Updated: 2019-03-12

Dubsmash(dubsmash.com)
In December 2018, the video messaging service Dubsmash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. 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".

Count: 161749950 | Created: 2018-12-01 | Updated: 2019-02-25

MyHeritage(myheritage.com)
In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 password hashes. 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 be attributed to "BenjaminBlue@exploit.im".

Count: 91991358 | Created: 2017-10-26 | Updated: 2019-02-20

devkitPro(devkitpro.org)
In February 2019, the devkitPro forum suffered a data breach. The phpBB based forum had 1,508 unique email addresses exposed in the breach alongside forum posts, private messages and passwords stored as weak salted hashes. The data breach was self-submitted to HIBP by the forum operator.

Count: 1508 | Created: 2019-02-03 | Updated: 2019-02-11

FaceUP(faceup.dk)
In 2013, the Danish social media site FaceUP suffered a data breach. The incident exposed 87k unique email addresses alongside genders, dates of birth, names, phone numbers and passwords stored as unsalted MD5 hashes. When notified of the incident, FaceUP advised they had identified a SQL injection vulnerability at the time and forced password resets on impacted customers.

Count: 87633 | Created: 2013-01-01 | Updated: 2019-01-13

Breach.

Count: 772904991 | Created: 2019-01-07 | Updated: 2019-01-16

Dangdang(dangdang.com)
In 2011, the Chinese e-commerce site Dangdang suffered a data breach. The incident exposed over 4.8 million unique email addresses which were subsequently traded online over the ensuing years.

Count: 4848734 | Created: 2011-06-01 | Updated: 2019-01-10

BannerBit(bannerbit.com)
In approximately December 2018, the online ad platform BannerBit suffered a data breach. Containing 213k unique email addresses and plain text passwords, the data was provided to HIBP by a third party. Multiple attempts were made to contact BannerBit, but no response was received.

Count: 213415 | Created: 2018-12-29 | Updated: 2019-01-08

BlankMediaGames(blankmediagames.com)
In December 2018, the Town of Salem website produced by BlankMediaGames suffered a data breach. Reported to HIBP by DeHashed, the data contained 7.6M unique user email addresses alongside usernames, IP addresses, purchase histories and passwords stored as phpass hashes. DeHashed made multiple attempts to contact BlankMediaGames over various channels and many days but had yet to receive a response at the time of publishing.

Count: 7633234 | Created: 2018-12-28 | Updated: 2019-01-02

GoldSilver(goldsilver.com)
In October 2018, the bullion education and dealer services site GoldSilver suffered a data breach that exposed 243k unique email addresses spanning customers and mailing list subscribers. An extensive amount of personal information on customers was obtained including names, addresses, phone numbers, purchases and passwords and answers to security questions stored as MD5 hashes. In a small number of cases, passport, social security numbers and partial credit card data was also exposed. The data breach and source code belonging to GoldSilver was publicly posted on a dark web service where it remained months later. When notified about the incident, GoldSilver advised that "all affected customers have been directly notified".

Count: 242715 | Created: 2018-10-21 | Updated: 2018-12-27

Mappery(mappery.com)
In December 2018, the mapping website Mappery suffered a data breach that exposed over 205k unique email addresses. The incident also exposed usernames, the geographic location of the user and passwords stored as unsalted SHA-1 hashes. No response was received from Mappery when contacted about the incident.

Count: 205242 | Created: 2018-12-11 | Updated: 2018-12-18

Bombuj.eu(bombuj.eu)
In December 2018, the Slovak website for watching movies online for free Bombuj.eu suffered a data breach. The incident exposed over 575k unique email addresses and passwords stored as unsalted MD5 hashes. No response was received from Bombuj.eu when contacted about the incident.

Count: 575437 | Created: 2018-12-07 | Updated: 2018-12-10

Hub4Tech(hub4tech.com)
On an unknown date in approximately 2017, the Indian training and assessment service known as Hub4Tech suffered a data breach via a SQL injection attack. The incident exposed almost 37k unique email addresses and passwords stored as unsalted MD5 hashes. No response was received from Hub4Tech when contacted about the incident.

Count: 36916 | Created: 2017-01-01 | Updated: 2018-12-09

AerServ(aerserv.com)
In April 2018, the ad management platform known as AerServ suffered a data breach. Acquired by InMobi earlier in the year, the AerServ breach impacted over 66k unique email addresses and also included contact information and passwords stored as salted SHA-512 hashes. The data was publicly posted to Twitter later in 2018 after which InMobi was notified and advised they were aware of the incident.

Count: 66308 | Created: 2018-04-01 | Updated: 2018-12-06

YouveBeenScraped()
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.

Count: 66147869 | Created: 2018-10-05 | Updated: 2018-12-06

ForumCommunity(forumcommunity.net)
In approximately mid-2016, the Italian-based service for creating forums known as ForumCommunity suffered a data breach. The incident impacted over 776k unique email addresses along with usernames and unsalted MD5 password hashes. No response was received from ForumCommunity when contacted.

Count: 776648 | Created: 2016-06-01 | Updated: 2018-12-05

Technic(technicpack.net)
In November 2018, the Minecraft modpack platform known as Technic suffered a data breach. Technic promptly disclosed the breach and advised that the impacted data included over 265k unique users' email and IP addresses, chat logs, private messages and passwords stored as bcrypt hashes with a work factor of 13. Technic self-submitted the breach to HIBP.

Count: 265410 | Created: 2018-11-30 | Updated: 2018-12-04

Data & Leads(datanleads.com)
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.

Count: 44320330 | Created: 2018-11-14 | Updated: 2018-11-28

Adapt(adapt.io)
In November 2018, security researcher Bob Diachenko identified an unprotected database hosted by data aggregator "Adapt". A provider of "Fresh Quality Contacts", the service

Elasticsearch Instance of Sales Leads on AWS()
In October 2018, security researcher Bob Diachenko identified multiple exposed databases with hundreds of millions of records. One of those datasets

exposed over 9.3M unique records of individuals and employer information including their names, employers, job titles, contact information and data relating to the employer including organisation description, size and revenue. No response was received from Adapt when contacted.

Count: 9363740 | Created: 2018-11-05 | Updated: 2018-11-22

KnownCircle(knowncircle.com)
In approximately April 2016, the "marketing automation for agents and professional service providers" company KnownCircle had a large volume of data obtained by an external party. The data belonging to the now defunct service appeared in JSON format and contained gigabytes of data related to the real estate and insurance sectors. The personal data in the breach appears to have primarily been used for marketing purposes, including logs of emails sent and tracking of gift cards. A small number of passwords for KnownCircle staff were also present and were stored as bcrypt hashes.

Count: 1957600 | Created: 2016-04-12 | Updated: 2018-11-17

WPSandbox(wpsandbox.io)
In November 2018, the WordPress sandboxing service that allows people to create temporary websites WP Sandbox discovered their service was being used to host a phishing site attempting to collect Microsoft OneDrive accounts. After identifying the malicious site, WP Sandbox took it offline, contacted the 858 people who provided information to it then self-submitted their addresses to HIBP. The phishing page requested both email addresses and passwords.

Count: 858 | Created: 2018-11-04 | Updated: 2018-11-06

Baby Names(babynames.com)
In approximately 2008, the site to help parents name their children known as Baby Names suffered a data breach. The incident exposed 846k email addresses and passwords stored as salted MD5 hashes. When contacted in October 2018, Baby Names advised that "the breach happened at least ten years ago" and that members were notified at the time.

Count: 846742 | Created: 2008-10-24 | Updated: 2018-10-24

Wife Lovers(wifelovers.com)
In October 2018, the site dedicated to posting naked photos and other erotica of wives Wife Lovers suffered a data breach. The underlying database supported a total of 8 different adult websites and contained over 1.2M unique email addresses. Wife Lovers acknowledged the breach which impacted names, usernames, email and IP addresses and passwords hashed using the weak DEScrypt algorithm. The breach has been marked as "sensitive" due to the nature of the site.

Count: 1274051 | Created: 2018-10-07 | Updated: 2018-10-23

Digimon(digimon.co.in)
In September 2016, over 16GB of logs from a service indicated to be digimon.co.in were obtained, most likely from an unprotected Mongo DB instance. The service ceased running shortly afterwards and no information remains about the precise nature of it. Based on enquiries made via Twitter, it appears to have been a mail service possibly based on PowerMTA and used for delivering spam. The logs contained information including 7.7M unique email recipients (names and addresses), mail server IP addresses, email subjects and tracking information including mail opens and clicks.

Count: | Created: 2016- | Updated: 2018-

was an Elasticsearch instance on AWS containing sales lead data and 5.8M unique email addresses. The data contained information relating to individuals and the companies they worked for including their names, email addresses and company name and contact information. Despite best efforts, it was not possible to identify the owner of the data hence this breach as been titled "Elasticsearch Sales Leads".

Count: 5788169 | Created: 2018-10-29 | Updated: 2018-11-18

SIAE(siae.it)
In November 2018, the Societxc3xa0 Italiana degli Autori ed Editori (Italian Society of Authors and Publishers, or SIAE) was hacked, defaced and almost 4GB of data leaked publicly via Twitter. The data included over 14k registered users' names, email addresses and passwords.

Count: 14609 | Created: 2018-11-03 | Updated: 2018-11-07

Mac Forums(mac-forums.com)
In July 2016, the self-proclaimed "Ultimate Source For Your Mac" website Mac Forums suffered a data breach. The vBulletin-based system exposed over 326k usernames, email and IP addresses, dates of birth and passwords stored as salted MD5 hashes. The data was later discovered being traded on a popular hacking forum. Mac Forums did not respond when contacted about the incident via their contact us form.

Count: 326714 | Created: 2016-07-03 | Updated: 2018-10-29

Apollo(apollo.io)
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.

Count: 125929660 | Created: 2018-07-23 | Updated: 2018-10-23

Facepunch(facepunch.com)
In June 2016, the game development studio Facepunch suffered a data breach that exposed 343k users. The breached data included usernames, email and IP addresses, dates of birth and salted MD5 password hashes. Facepunch advised they were aware of the incident and had notified people at the time. The data was provided to HIBP by whitehat security researcher and data analyst Adam Davies.

Count: 342913 | Created: 2016-06-03 | Updated: 2018-10-17

SaverSpy()
In September 2018, security researcher Bob Diachenko discovered a massive collection of personal details exposed in an unprotected Mongo DB instance. The data appears to have been used in marketing campaigns (possibly for spam purposes) but had little identifying data about it other than a description of "Yahoo_090618_ SaverSpy". The data set provided to HIBP had almost 2.5M unique email addresses (all of which were from Yahoo!) alongside names, genders and physical addresses.

Count: 2457420 | Created: 2018-09-18 | Updated: 2018-09-25

7687679	09-05	09-28

Real Estate Mogul(realestatemogul.com)
In September 2016, the real estate investment site Real Estate Mogul had a Mongo DB instance compromised and 5GB of data downloaded by an unauthorised party. The data contained real estate listings including addresses and the names, phone numbers and 308k unique email addresses of the sellers. Real Estate Mogul was advised of the incident in September 2018 and stated that they "found no instance of user account credentials like usernames and passwords nor billing information within this file".

Count: 307768 | Created: 2016-09-06 | Updated: 2018-09-24

NemoWeb(nemoweb.net)
In September 2016, almost 21GB of data from the French website used for "standardised and decentralized means of exchange for publishing newsgroup articles" NemoWeb was leaked from what appears to have been an unprotected Mongo DB. The data consisted of a large volume of emails sent to the service and included almost 3.5M unique addresses, albeit many of them auto-generated. Multiple attempts were made to contact the operators of NemoWeb but no response was received.

Count: 3472916 | Created: 2016-09-04 | Updated: 2018-09-24

Russian America(russianamerica.com)
In approximately 2017, the website for Russian speakers in America known as Russian America suffered a data breach. The incident exposed 183k unique records including names, email addresses, phone numbers and passwords stored in both plain text and as MD5 hashes. Russian America was contacted about the breach but did not respond.

Count: 182717 | Created: 2017-01-01 | Updated: 2018-09-13

NapsGear(napsgear.org)
In October 2015, the anabolic steroids retailer NapsGear suffered a data breach. An extensive amount of personal information on 287k customers was exposed including email addresses, names, addresses, phone numbers, purchase histories and salted MD5 password hashes.

Count: 287071 | Created: 2015-10-21 | Updated: 2018-09-10

SvenskaMagic(svenskamagic.com)
Sometime in 2015, the Swedish magic website SvenskaMagic suffered a data breach that exposed over 30k records. The compromised data included usernames, email addresses and MD5 password hashes. The data was self-submitted to HIBP by SvenskaMagic.

Count: 30327 | Created: 2015-07-01 | Updated: 2018-08-30

SpyFone(spyfone.com)
In August 2018, the spyware company SpyFone left terabytes of data publicly exposed. Collected surreptitiously whilst the targets were using their devices, the data included photos, audio recordings, text messages and browsing history which were then exposed via a number of misconfigurations within SpyFone's systems. The data belonged the thousands of SpyFone customers and included 44k unique email addresses, many likely belonging to people the targeted phones had contact with.

Count: 44109 | Created: 2018-08-16 | Updated: 2018-08-24

Lanwar(lanwar.com)
In July 2018, staff of the Lanwar gaming site discovered a data breach they believe dates

Mortal Online(mortalonline.com)
In June 2018, the massively multiplayer online role-playing game (MMORPG) Mortal Online suffered a data breach. A file containing 570k email addresses and cracked passwords was subsequently distributed online. A larger more complete file containing 607k email addresses with original unsalted MD5 password hashes along with names, usernames and physical addresses was later provided and the original breach in HIBP was updated accordingly. The data was provided to HIBP by whitehat security researcher and data analyst Adam Davies.

Count: 606637 | Created: 2018-06-17 | Updated: 2018-09-24

Kayo.moe Credential Stuffing List()
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.

Count: 41826763 | Created: 2018-09-11 | Updated: 2018-09-13

FreshMenu(freshmenu.com)
In July 2016, the India-based food delivery service FreshMenu suffered a data breach. The incident exposed the personal data of over 110k customers and included their names, email addresses, phone numbers, home addresses and order histories. When advised of the incident, FreshMenu acknowledged being already aware of the breach but stated they had decided not to notify impacted customers.

Count: 110355 | Created: 2016-07-01 | Updated: 2018-09-10

Warmane(warmane.com)
In approximately December 2016, the online service for World of Warcraft private servers Warmane suffered a data breach. The incident exposed over 1.1M accounts including usernames, email addresses, dates of birth and salted MD5 password hashes. The data was subsequently extensively circulated online and was later provided to HIBP by whitehat security researcher and data analyst Adam Davies.

Count: 1116256 | Created: 2016-12-01 | Updated: 2018-09-08

Atlas Quantum(atlasquantum.com)
In August 2018, the cryptocurrency investment platform Atlas Quantum suffered a data breach. The breach leaked the personal data of 261k investors on the platform including their names, phone numbers, email addresses and account balances.

Count: 261463 | Created: 2018-08-25 | Updated: 2018-08-28

MyFHA(myfha.net)
In approximately February 2015, the home financing website MyFHA suffered a data breach which disclosed the personal information of nearly 1 million people. The data included extensive personal information relating to home financing including personal contact info, credit statuses, household incomes, loan amounts and notes on personal circumstances, often referring to legal issues, divorces and health conditions. Multiple parties contacted HIBP with the data after which MyFHA was alerted in mid-July and acknowledged the legitimacy of the breach then took the site offline.

Count: 972629 | Created: 2015-02-18 | Updated: 2018-08-09

back to sometime over the previous several months. The data contained 45k names, email addresses, usernames and plain text passwords. A Lanwar staff member self-submitted the breach to HIBP and has also contacted the relevant authorities about the incident after identifying a phishing attempt to extort Bitcoin from a user.

Count: 45120 | Created: 2018-07-28 | Updated: 2018-08-08

Fashion Nexus(fashionnexus.co.uk)
In July 2018, UK-based ecommerce company Fashion Nexus suffered a data breach which exposed 1.4 million records. Multiple websites developed by sister company White Room Solutions were impacted in the breach amongst which were sites including Jaded London and AX Paris. The various sites exposed in the incident included a range of different data types including names, phone numbers, addresses and passwords stored as a mix of salted MD5 and SHA-1 as well as unsalted MD5 passwords. When asked by reporter Graham Cluley if a public statement on the incident was available, a one-word response of "No" was received.

Count: 1279263 | Created: 2018-07-09 | Updated: 2018-07-31

SweClockers.com(sweclockers.com)
In early 2015, the Swedish tech news site SweClockers was hacked and 255k accounts were exposed. The attack led to the exposure of usernames, email addresses and salted hashes of passwords stored with a combination of MD5 and SHA512.

Count: 254867 | Created: 2015-04-01 | Updated: 2018-07-27

Funny Games(funny-games.biz)
In April 2018, the online entertainment site Funny Games suffered a data breach that disclosed 764k records including usernames, email and IP addresses and salted MD5 password hashes. The incident was disclosed to Funny Games in July who acknowledged the breach and identified it had been caused by legacy code no longer in use. The record count in the breach constitute approximately half of the user base.

Count: 764357 | Created: 2018-04-28 | Updated: 2018-07-24

LightsHope(lightshope.org)
In June 2018, the World of Warcraft service Light's Hope suffered a data breach which they subsequently self-submitted to HIBP. Over 30K unique users were impacted and their exposed data included email addresses, dates of birth, private messages and passwords stored as bcrypt hashes.

Count: 30484 | Created: 2018-06-25 | Updated: 2018-07-04

Gaadi(gaadi.com)
In May 2015, the Indian motoring website known as Gaadi had 4.3 million records exposed in a data breach. The data contained usernames, email and IP addresses, genders, the city of users as well as passwords stored in both plain text and as MD5 hashes. The site was previously reported as compromised on the Vigilante.pw breached database directory.

Count: 4261179 | Created: 2015-05-14 | Updated: 2018-07-01

Creative(creative.com)
In May 2018, the forum for Singaporean hardware company Creative Technology suffered a data breach which resulted in the disclosure of 483k unique email addresses. Running on an old version of vBulletin, the

Adult-FanFiction.Org(adult-fanfiction.org)
In May 2018, the website for sharing adult-orientated works of fiction known as Adult-FanFiction.Org had 186k records exposed in a data breach. The data contained names, email addresses, dates of birth and passwords stored as *both* MD5 hashes and plain text. AFF did not respond when contacted about the breach and the site was previously reported as compromised on the Vigilante.pw breached database directory.

Count: 186082 | Created: 2018-05-30 | Updated: 2018-08-06

League of Legends(leagueoflegends.com)
In June 2012, the multiplayer online game League of Legends suffered a data breach. At the time, the service had more than 32 million registered accounts and the breach affected various personal data attributes including "encrypted" passwords. In 2018, a 339k record subset of the data emerged with email addresses, usernames and plain text passwords, likely cracked from the original cryptographically protected ones.

Count: 339487 | Created: 2012-06-11 | Updated: 2018-07-28

Exactis(exactis.com)
In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.

Count: 131577763 | Created: 2018-06-01 | Updated: 2018-07-25

Pemiblanc(pemiblanc.com)
In April 2018, a credential stuffing list containing 111 million email addresses and passwords known as Pemiblanc was discovered on a French server. The list contained email addresses and passwords collated from different data breaches and used to mount account takeover attacks against other services. Read more about the incident.

Count: 110964206 | Created: 2018-04-02 | Updated: 2018-07-09

Yatra(yatra.com)
In September 2013, the Indian bookings website known as Yatra had 5 million records exposed in a data breach. The data contained email and physical addresses, dates of birth and phone numbers along with both PINs and passwords stored in plain text. The site was previously reported as compromised on the Vigilante.pw breached database directory.

Count: 5033997 | Created: 2013-09-01 | Updated: 2018-07-04

Estonian Citizens (via Estonian Cybercrime Bureau)()
In June 2018, the Cybercrime Bureau of the Estonian Central Criminal Police contacted HIBP and asked for assistance in making a data set of 655k email addresses searchable. The Estonian police suspected the email addresses and passwords they obtained were being used to access mailboxes, cryptocurrency exchanges, cloud service accounts and other similar online assets. They've requested that individuals who find themselves in the data set ***and also identify that cryptocurrency has been stolen*** contact them at cybercrime@politsei.ee.

Count: 655161 | Created: 2018-06-07 | Updated: 2018-06-11

Linux Forums(linuxforums.org)
In May 2018, the Linux Forums website suffered a data breach which resulted in the disclosure of 276k unique email addresses. Running on an old version of vBulletin, the breach also disclosed usernames, IP addresses and salted MD5

breach also disclosed usernames, IP addresses and salted MD5 password hashes. After being notified of the incident, Creative permanently shut down the forum.

Count: 483015 | Created: 2018-05-01 | Updated: 2018-06-07

ViewFines(viewfines.co.za)
In May 2018, the South African website for viewing traffic fines online known as ViewFines suffered a data breach. Over 934k records containing 778k unique email addresses were exposed and included names, phone numbers, government issued IDs and passwords stored in plain text.

Count: 777649 | Created: 2018-05-07 | Updated: 2018-05-24

TGBUS(tgbus.com)
In approximately 2017, it's alleged that the Chinese gaming site known as TGBUS suffered a data breach that impacted over 10 million unique subscribers. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains usernames, email addresses and salted MD5 password hashes and was provided with support from dehashed.com. Read more about Chinese data breaches in Have I Been Pwned.

Count: 10371766 | Created: 2017-09-01 | Updated: 2018-04-28

17173(17173.com)
In late 2011, a series of data breaches in China affected up to 100 million users, including 7.5 million from the gaming site known as 17173. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains usernames, email addresses and salted MD5 password hashes and was provided with support from dehashed.com. Read more about Chinese data breaches in Have I Been Pwned.

Count: 7485802 | Created: 2011-12-28 | Updated: 2018-04-28

CashCrate(cashcrate.com)
In June 2017, news broke that CashCrate had suffered a data breach exposing 6.8 million records. The breach of the cash-for-surveys site dated back to November 2016 and exposed names, physical addresses, email addresses and passwords stored in plain text for older accounts along with weak MD5 hashes for newer ones.

Count: 6844490 | Created: 2016-11-17 | Updated: 2018-04-20

Smogon(smogon.com)
In April 2018, the Pokxc3xa9mon website known as Smogon announced they'd suffered a data breach. The breach dated back to September 2017 and affected their XenForo based forum. The exposed data included usernames, email addresses, genders and both bcrypt and MD5 password hashes.

Count: 386489 | Created: 2017-09-10 | Updated: 2018-04-11

Bestialitysextaboo(bestialitysextaboo.com)
In March 2018, the animal bestiality website known as Bestialitysextaboo was hacked. A collection of various sites running on the same service were also compromised and details of the hack (including links to the data) were posted on a popular forum. In all, more than 3.2k unique email addresses were included alongside usernames, IP addresses, dates of birth, genders and bcrypt hashes of passwords.

Count: 3204 | Created: 2018-03-19 | Updated: 2018-03-29

password hashes. Linux Forums did not respond to multiple attempts to contact them about the breach.

Count: 275785 | Created: 2018-05-01 | Updated: 2018-06-07

YouPorn(youporn.com)
In February 2012, the adult website YouPorn had over 1.3M user accounts exposed in a data breach. The publicly released data included both email addresses and plain text passwords.

Count: 1327567 | Created: 2012-02-21 | Updated: 2018-05-20

VNG(zing.vn)
In April 2018, news broke of a massive data breach impacting the Vietnamese company known as VNG after data was discovered being traded on a popular hacking forum where it was extensively redistributed. The breach dated back to an incident in May of 2015 and included of over 163 million customers. The data in the breach contained a wide range of personal attributes including usernames, birth dates, genders and home addresses along with unsalted MD5 hashes and 25 million unique email addresses. The data was provided to HIBP by dehashed.com.

Count: 24853850 | Created: 2015-05-19 | Updated: 2018-04-28

ILikeCheats(ilikecheats.net)
In October 2014, the game cheats website known as ILikeCheats suffered a data breach that exposed 189k accounts. The vBulletin based forum leaked usernames, IP and email addresses and weak MD5 hashes of passwords. The data was provided with support from dehashed.com.

Count: 188847 | Created: 2014-10-18 | Updated: 2018-04-22

Taringa(taringa.net)
In September 2017, news broke that Taringa had suffered a data breach exposing 28 million records. Known as "The Latin American Reddit", Taringa's breach disclosure notice indicated the incident dated back to August that year. The exposed data included usernames, email addresses and weak MD5 hashes of passwords.

Count: 27971100 | Created: 2017-08-01 | Updated: 2018-04-19

HiAPK(hiapk.com)
In approximately 2014, it's alleged that the Chinese Android store known as HIAPK suffered a data breach that impacted 13.8 million unique subscribers. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains usernames, email addresses and salted MD5 password hashes and was provided to HIBP by white hat security researcher and data analyst Adam Davies. Read more about Chinese data breaches in Have I Been Pwned.

Count: 13873674 | Created: 2014-01-01 | Updated: 2018-04-01

MDPI(mdpi.com)
In August 2016, the Swiss scholarly open access publisher known as MDPI had 17.5GB of data obtained from an unprotected Mongo DB instance. The data contained email exchanges between MDPI and their authors and reviewers which included 845k unique email addresses. MDPI have confirmed that the system has since been protected and that no data of a sensitive nature was impacted. As such, they concluded that notification to their subscribers was not necessary due to the fact that all their authors and reviewers are available online on their website.

Count: 845012 | Created: 2016-08-30 | Updated: 2018-03-25

Florida Virtual School(flvs.net)
In March 2018, the Florida Virtual School (FLVS) posted a data breach notification to their website. The school had identified a data breach which had occurred sometime between 6 May 2016 and 12 Feb 2018 and an XML file containing 368k student records was subsequently found circulating. Each record contained student name, date of birth, password, grade, email *and* parent email resulting in a total of 543k unique email addresses. Due to the prevalence of email addresses belonging to individuals who are still legally children, the data breach has been flagged as "sensitive".

Count: 542902 | Created: 2018-02-12 | Updated: 2018-03-18

MangaFox.me(mangafox.me)
In approximately July 2016, the manga website known as mangafox.me suffered a data breach. The vBulletin based forum exposed 1.3 million accounts including usernames, email and IP addresses, dates of birth and salted MD5 password hashes.

Count: 1311610 | Created: 2016-06-01 | Updated: 2018-03-17

xHamster(xhamster.com)
In November 2016, news broke that hackers were trading hundreds of thousands of xHamster porn account details. In total, the data contained almost 380k unique user records including email addresses, usernames and unsalted MD5 password hashes.

Count: 377377 | Created: 2016-11-28 | Updated: 2018-03-08

2,844 Separate Data Breaches()
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.

Count: 80115532 | Created: 2018-02-19 | Updated: 2018-02-26

Underworld Empire(underworldempireforums.com)
In April 2017, the vBulletin forum for the Underworld Empire game suffered a data breach that exposed 429k accounts. The data was then posted to a hacking forum in mid-February 2018 where it was made available to download. The source data contained IP and email addresses, usernames and salted MD5 hashes.

Count: 428779 | Created: 2017-04-25 | Updated: 2018-02-19

Guns and Robots(play-gar.com)
In approximately April 2016, the gaming website Guns and Robots suffered a data breach resulting in the exposure of 143k unique records. The data contained email and IP addresses, usernames and SHA-1 password hashes. The site was previously reported as compromised on the Vigilante.pw breached database directory.

Count: 143569 | Created: 2016-04-01 | Updated: 2018-02-14

Autocentrum.pl(autocentrum.pl)
In February 2018, data belonging to the Polish motoring website autocentrum.pl was found online. The data contained 144k email addresses and plain text passwords.

Count: 143717 | Created: 2018-02-04 | Updated: 2018-02-09

TheTVDB.com(thetvdb.com)
In November 2017, the open television database known as TheTVDB.com suffered a data breach. The breached data was posted to a hacking forum and included 182k records with usernames, email addresses and MySQL password hashes.

Count: 181871 | Created: 2017-11-21 | Updated: 2018-01-29

The Fly on the Wall(theflyonthewall.com)
In December 2017, the stock market news website The Fly on the Wall suffered a data breach. The data in the breach included 84k unique email addresses as well as purchase histories and credit card data. Numerous attempts were made to contact The Fly on the Wall about the incident, however no responses were received.

Count: 84011 | Created: 2017-12-31 | Updated: 2018-01-15

Lyrics Mania(lyricsmania.com)
In December 2017, the song lyrics website known as Lyrics Mania suffered a data breach. The data in the breach included 109k usernames, email addresses and plain text passwords. Numerous attempts were made to contact Lyrics Mania about the incident, however no responses were received.

Count: 109202 | Created: 2017-12-21 | Updated: 2018-01-15

Open CS:GO(opencsgo.com)
In December 2017, the website for purchasing Counter-Strike skins known as Open CS:GO (Counter-Strike: Global Offensive) suffered a data breach (address since redirects to dropgun.com). The 10GB file contained an extensive amount of personal information including email and IP addresses, phone numbers, physical addresses and purchase histories. Numerous attempts were made to contact Open CS:GO about the incident, however no responses were received.

Count: 512311 | Created: 2017-11-28 | Updated: 2018-01-15

mail.ru Dump(mail.ru)
In September 2014, several large dumps of user accounts appeared on the Russian Bitcoin Security Forum including one with nearly 5M email addresses and passwords, predominantly on the mail.ru domain. Whilst unlikely to be the result of a direct attack against mail.ru, the credentials were confirmed by many as legitimate for other services they had subscribed to. Further data allegedly valid for mail.ru and containing email addresses and plain text passwords was added in January 2018 bringing to total to more than 16M records. The incident was also then flagged as "unverified", a concept that was introduced after the initial data load in 2014.

Count: 16630988 | Created: 2014-09-10 | Updated: 2018-01-09

2fast4u(2fast4u.be)
In December 2017, the Belgian motorcycle forum 2fast4u discovered a data breach of their system. The breach of the vBulletin message board impacted over 17k individual users and exposed email addresses, usersnames and salted MD5 passwords.

HoundDawgs(hounddawgs.org)
In December 2017, the Danish torrent tracker known as HoundDawgs suffered a data breach. More than 55GB of data was dumped publicly and whilst there was initially contention as to the severity of the incident, the data did indeed contain more than 45k unique email addresses complete extensive logs of torrenting activity, IP addresses and SHA1 passwords.

Count: 17706 Created: 2017-12-20 Updated: 2018-01-07

Ancestry(ancestry.com)
In November 2015, an Ancestry service known as RootsWeb suffered a data breach. The breach was not discovered until late 2017 when a file containing almost 300k email addresses and plain text passwords was identified.

Count: 297806 Created: 2015-11-07 Updated: 2017-12-24

CrackingForum(crackingforum.com)
In approximately mid-2016, the cracking community forum known as CrackingForum suffered a data breach. The vBulletin based forum exposed 660k email and IP addresses, usernames and salted MD5 hashes.

Count: 660305 Created: 2016-07-01 Updated: 2017-12-10

Netshoes(netshoes.com.br)
In December 2017, the online Brazilian retailer known as Netshoes had half a million records allegedly hacked from their system posted publicly. The company was contacted by local Brazilian media outlet Tecmundo and subsequently advised that no indications have been identified of an invasion of the company's systems. However, Netshoes' own systems successfully confirm the presence of matching identifiers and email addresses from the data set, indicating a high likelihood that the data originated from them.

Count: 499836 Created: 2017-12-07 Updated: 2017-12-10

imgur(imgur.com)
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.

Count: 1749806 Created: 2013-09-01 Updated: 2017-11-25

V-Tight Gel(vtightgel.com)
In approximately February 2016, data surfaced which was allegedly obtained from V-Tight Gel (vaginal tightening gel). Whilst the data set was titled V-Tight, within there were 50 other (predominantly wellness-related) domain names, most owned by the same entity. Multiple HIBP subscribers confirmed that although they couldn't recall providing data specifically to V-Tight, their personal information including name, phone and physical address was accurate. V-Tight Gel did not reply to multiple requests for comment.

Count: 2013164 Created: 2016-02-13 Updated: 2017-11-17

CafeMom(cafemom.com)
In 2014, the social network for mothers CafeMom suffered a data breach. The data surfaced alongside a number of other historical breaches including Kickstarter, Bitly and Disqus and contained 2.6 million email addresses and plain text passwords.

Count: 2628148 Created: 2014-04-10 Updated: 2017-11-09

JobStreet(jobstreet.com)
In October 2017, the Malaysian website lowyat.net ran a story on a massive set of

Count: 45701 Created: 2017-12-30 Updated: 2018-01-03

000webhost(000webhost.com)
In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.

Count: 14936670 Created: 2015-03-01 Updated: 2017-12-10

dvd-shop.ch(dvd-shop.ch)
In December 2017, the online Swiss DVD store known as dvd-shop.ch suffered a data breach. The incident led to the exposure of 68k email addresses and plain text passwords. The site has since been updated to indicate that it is currently closed.

Count: 67973 Created: 2017-12-05 Updated: 2017-12-10

ai.type(aitype.com)
In December 2017, the virtual keyboard application ai.type was found to have left a huge amount of data publicly facing in an unsecured MongoDB instance. Discovered by researchers at The Kromtech Security Center, the 577GB data set included extensive personal information including over 20 million unique email addresses, social media profiles and address book contacts. The email addresses alone were provided to HIBP to enable impacted users to assess their exposure.

Count: 20580060 Created: 2017-12-05 Updated: 2017-12-08

Bolt(bolt.cd)
In approximately March 2017, the file sharing website Bolt suffered a data breach resulting in the exposure of 995k unique user records. The data was sourced from their vBulletin forum and contained email and IP addresses, usernames and salted MD5 password hashes. The site was previously reported as compromised on the Vigilante.pw breached database directory.

Count: 995274 Created: 2017-03-01 Updated: 2017-11-24

PoliceOne(policeone.com)
In February 2017, the law enforcement website PoliceOne confirmed they'd suffered a data breach. The breach contained over 700k accounts which appeared for sale by a data broker and included email and IP addresses, usernames and salted MD5 password hashes. The file the data was contained in indicated the original breach dated back to July 2014.

Count: 709926 Created: 2014-07-01 Updated: 2017-11-15

RankWatch(rankwatch.com)
In approximately November 2016, the search engine optimisation management company RankWatch exposed a Mongo DB with no password publicly whereupon their data was exfiltrated and posted to an online forum. The data contained 7.4 million unique email addresses along with names, employers, phone numbers and job titles in a table called "us_emails". When contacted and advised of the incident, RankWatch would not reveal the purpose of the data, where it had been acquired from and whether the data owners had consented to its collection. The forum which originally posted the data explained it as being "in the same vein as the modbsolutions leak", a large list of corporate data allegedly used for spam purposes.

Count: 7445067 Created: 2016-11-19 Updated: 2017-11-03

breached data affecting millions of Malaysians after someone posted it for sale on their forums. The data spanned multiple separate breaches including the JobStreet jobs website which contained almost 4 million unique email addresses. The dates in the breach indicate the incident occurred in March 2012. The data later appeared freely downloadable on a Tor hidden service and contained extensive information on job seekers including names, genders, birth dates, phone numbers, physical addresses and passwords.

Count: 3883455 | Created: 2012-03-07 | Updated: 2017-10-30

Master Deeds()
In March 2017, a 27GB database backup file named "Master Deeds" was sent to HIBP by a supporter of the project. Upon detailed analysis later that year, the file was found to contain the personal data of tens of millions of living and deceased South African residents. The data included extensive personal attributes such as names, addresses, ethnicities, genders, birth dates, government issued personal identification numbers and 2.2 million email addresses. At the time of publishing, it's alleged the data was sourced from Dracore Data Sciences (Dracore is yet to publicly confirm or deny the data was sourced from their systems). On 18 October 2017, the file was found to have been published to a publicly accessible web server where it was located at the root of an IP address with directory listing enabled. The file was dated 8 April 2015.

Count: 2257930 | Created: 2017-03-14 | Updated: 2017-10-18

diet.com(diet.com)
In August 2014, the diet and nutrition website diet.com suffered a data breach resulting in the exposure of 1.4 million unique user records dating back as far as 2004. The data contained email and IP addresses, usernames, plain text passwords and dietary information about the site members including eating habits, BMI and birth date. The site was previously reported as compromised on the Vigilante.pw breached database directory.

Count: 1383759 | Created: 2014-08-10 | Updated: 2017-10-13

AbuseWith.Us(abusewith.us)
In 2016, the site dedicated to helping people hack email and online gaming accounts known as Abusewith.us suffered multiple data breaches. The site allegedly had an administrator in common with the nefarious LeakedSource site, both of which have since been shut down. The exposed data included more than 1.3 million unique email addresses, often accompanied by usernames, IP addresses and plain text or hashed passwords retrieved from various sources and intended to be used to compromise the victims' accounts.

Count: 1372550 | Created: 2016-07-01 | Updated: 2017-10-09

Disqus(disqus.com)
In October 2017, the blog commenting service Disqus announced they'd suffered a data breach. The breach dated back to July 2012 but wasn't identified until years later when the data finally surfaced. The breach contained over 17.5 million unique email addresses and usernames. Users who created logins on Disqus had salted SHA1 hashes of passwords whilst users who logged in via social providers only had references to those accounts.

Count: 17551044 | Created: 2012-07-01 | Updated: 2017-10-06

ReverbNation(reverbnation.com)
In January 2014, the online service for assisting musicians to build their careers ReverbNation suffered a data breach which wasn't identified until September the following

Shotbow(shotbow.net)
In May 2016, the multiplayer server for Minecraft service Shotbow announced they'd suffered a data breach. The incident resulted in the exposure of over 1 million unique email addresses, usernames and salted SHA-256 password hashes.

Count: 1052753 | Created: 2016-05-09 | Updated: 2017-10-29

We Heart It(weheartit.com)
In November 2013, the image-based social network We Heart It suffered a data breach. The incident wasn't discovered until October 2017 when 8.6 million user records were sent to HIBP. The data contained user names, email addresses and password hashes, 80% of which were salted SHA-256 with the remainder being MD5 with no salt.

Count: 8600635 | Created: 2013-11-03 | Updated: 2017-10-14

Victory Phones(victoryphones.com)
In January 2017, the automated telephony services company Victory Phones left a Mongo DB database publicly facing without a password. Subsequently, 213GB of data was downloaded by an unauthorised party including names, addresses, phone numbers and over 166k unique email addresses.

Count: 166046 | Created: 2017-01-01 | Updated: 2017-10-11

Bitly(bitly.com)
In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.

Count: 9313136 | Created: 2014-05-08 | Updated: 2017-10-06

Kickstarter(kickstarter.com)
In February 2014, the crowdfunding platform Kickstarter announced they'd suffered a data breach. The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.

Count: 5176463 | Created: 2014-02-16 | Updated: 2017-10-06

Staminus(staminus.net)
In March 2016, the DDoS protection service Staminus was "massively hacked" resulting in an outage of more than 20 hours and the disclosure of customer credentials (with unsalted MD5 hashes), support tickets, credit card numbers

year. The breach contained over 7 million accounts with unique email addresses and salted SHA1 passwords.

Count: 7040725 | Created: 2014-01-01 | Updated: 2017-10-05

AKP Emails(akparti.org.tr)
In July 2016, a hacker known as Phineas Fisher hacked Turkey's ruling party (Justice and Development Party or "AKP") and gained access to 300k emails. The full contents of the emails were subsequently published by WikiLeaks and made searchable. HIBP identified over 917k unique email address patterns in the data set, including message IDs and a number of other non-user addresses.

Count: 917461 | Created: 2016-07-19 | Updated: 2017-10-01

MALL.cz(mall.cz)
In July 2017, the Czech Republic e-commerce site MALL.cz suffered a data breach after which 735k unique accounts including email addresses, names, phone numbers and passwords were later posted online. Whilst passwords were stored as hashes, a number of different algorithms of varying strength were used over time. All passwords included in the publicly distributed data were in plain text and were likely just those that had been successfully cracked (members with strong passwords don't appear to be included). According to MALL.cz, the breach only impacted accounts created before 2015.

Count: 735405 | Created: 2017-07-27 | Updated: 2017-09-04

Onliner Spambot()
In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moxcax9euxc6x8eq. 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.

Count: 711477622 | Created: 2017-08-28 | Updated: 2017-08-29

Bin Weevils(binweevils.com)
In September 2014, the online game Bin Weevils suffered a data breach. Whilst originally stating that only usernames and passwords had been exposed, a subsequent story on DataBreaches.net indicated that a more extensive set of personal attributes were impacted (comments there also suggest the data may have come from a later breach). Data matching that pattern was later provided to Have I Been Pwned by @akshayindia6 and included almost 1.3m unique email addresses, genders, ages and plain text passwords.

Count: 1287073 | Created: 2014-09-01 | Updated: 2017-08-18

MCBans(mcbans.com)
In October 2016, the Minecraft banning service known as MCBans suffered a data breach resulting in the exposure of 120k unique user records. The data contained email and IP addresses, usernames and password hashes of unknown format. The site was previously reported as compromised on the Vigilante.pw breached database directory.

Count: 119948 | Created: 2016-10-27 | Updated: 2017-07-23

Evermotion(evermotion.org)
In May 2015, the Polish 3D modelling website known as Evermotion suffered a data breach resulting in the exposure of 435k unique user

and other sensitive data. 27k unique email addresses were found in the data which was subsequently released to the public. Staminus is no longer in operation.

Count: 26815 | Created: 2016-03-11 | Updated: 2017-10-05

7k7k(7k7k.com)
In approximately 2011, it's alleged that the Chinese gaming site known as 7k7k suffered a data breach that impacted 9.1 million subscribers. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains usernames, email addresses and plain text passwords. Read more about Chinese data breaches in Have I Been Pwned.

Count: 9121434 | Created: 2011-01-01 | Updated: 2017-09-26

Zomato(zomato.com)
In May 2017, the restaurant guide website Zomato was hacked resulting in the exposure of almost 17 million accounts. The data was consequently redistributed online and contains email addresses, usernames and salted MD5 hashes of passwords (the password hash was not present on all accounts). This data was provided to HIBP by whitehat security researcher and data analyst Adam Davies.

Count: 16472873 | Created: 2017-05-17 | Updated: 2017-09-04

Biohack.me(biohack.me)
In December 2016, the forum for the biohacking website Biohack.me suffered a data breach that exposed 3.4k accounts. The data included usernames, email addresses and hashed passwords along with the private messages of forum members. The data was self-submitted to HIBP by the Biohack.me operators.

Count: 3402 | Created: 2016-12-02 | Updated: 2017-08-23

Dailymotion(dailymotion.com)
In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords.

Count: 85176234 | Created: 2016-10-20 | Updated: 2017-08-07

B2B USA Businesses()
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.

Count: 105059554 | Created: 2017-07-18 | Updated: 2017-07-18

Powerbot(powerbot.org)
In approximately September 2014, the RuneScape bot website Powerbot

records. The data was sourced from a vBulletin forum and contained email addresses, usernames, dates of birth and salted MD5 hashes of passwords. The site was previously reported as compromised on the Vigilante.pw breached database directory.

Count: 435510 | Created: 2015-05-07 | Updated: 2017-07-02

Programming Forums(programmingforums.org)
In approximately late 2015, the programming forum at programmingforums.org suffered a data breach resulting in the exposure of 707k unique user records. The data contained email and IP addresses, usernames and salted MD5 hashes of passwords. The site was previously reported as compromised on the Vigilante.pw breached database directory.

Count: 707432 | Created: 2015-12-01 | Updated: 2017-07-01

Coachella(coachella.com)
In February 2017, hundreds of thousands of records from the Coachella music festival were discovered being sold online. Allegedly taken from a combination of the main Coachella website and their vBulletin-based message board, the data included almost 600k usernames, IP and email addresses and salted hashes of passwords (MD5 in the case of the message board).

Count: 599802 | Created: 2017-02-22 | Updated: 2017-06-27

Data Enrichment Records()
In December 2016, more than 200 million "data enrichment profiles" were found for sale on the darknet. The seller claimed the data was sourced from Experian and whilst that claim was rejected by the company, the data itself was found to be legitimate suggesting it may have been sourced from other legitimate locations. In total, there were more than 8 million unique email addresses in the data which also contained a raft of other personal attributes including credit ratings, home ownership status, family structure and other fields described in the story linked to above. The email addresses alone were provided to HIBP.

Count: 8176132 | Created: 2016-12-23 | Updated: 2017-06-08

Edmodo(edmodo.com)
In May 2017, the education platform Edmodo was hacked resulting in the exposure of 77 million records comprised of over 43 million unique customer email addresses. The data was consequently published to a popular hacking forum and made freely available. The records in the breach included usernames, email addresses and bcrypt hashes of passwords.

Count: 43423561 | Created: 2017-05-11 | Updated: 2017-06-01

Bell (2017 breach)(bell.ca)
In May 2017, the Bell telecommunications company in Canada suffered a data breach resulting in the exposure of millions of customer records. The data was consequently leaked online with a message from the attacker stating that they were "releasing a significant portion of Bell.ca's data due to the fact that they have failed to cooperate with us" and included a threat to leak more. The impacted data included over 2 million unique email addresses and 153k survey results dating back to 2011 and 2012. There were also 162 Bell employee records with more comprehensive personal data including names, phone numbers and plain text "passcodes". Bell suffered another breach in 2014 which exposed 40k records.

Count: 2231256 | Created: 2017-05-15 | Updated: 2017-05-16

suffered a data breach resulting in the exposure of over half a million unique user records. The data contained email and IP addresses, usernames and salted MD5 hashes of passwords. The site was previously reported as compromised on the Vigilante.pw breached database directory.

Count: 503501 | Created: 2014-09-01 | Updated: 2017-07-01

XPG(xpgamesaves.com)
In approximately early 2016, the gaming website Xpgamesaves (XPG) suffered a data breach resulting in the exposure of 890k unique user records. The data contained email and IP addresses, usernames and salted MD5 hashes of passwords. The site was previously reported as compromised on the Vigilante.pw breached database directory. This data was provided by security researcher and data analyst, Adam Davies.

Count: 890341 | Created: 2016-01-01 | Updated: 2017-07-01

Exposed VINs()
In June 2017, an unsecured database with more than 10 million VINs (vehicle identification numbers) was discovered by researchers. Believed to be sourced from US car dealerships, the data included a raft of personal information and vehicle data along with 397k unique email addresses.

Count: 396650 | Created: 2017-06-05 | Updated: 2017-06-09

Abandonia(abandonia.com)
In November 2015, the gaming website dedicated to classic DOS games Abandonia suffered a data breach resulting in the exposure of 776k unique user records. The data contained email and IP addresses, usernames and salted MD5 hashes of passwords.

Count: 776125 | Created: 2015-11-01 | Updated: 2017-06-05

DaFont(dafont.com)
In May 2017, font sharing site DaFont suffered a data breach resulting in the exposure of 637k records. Allegedly due to a SQL injection vulnerability exploited by multiple parties, the exposed data included usernames, email addresses and passwords stored as MD5 without a salt.

Count: 637340 | Created: 2017-05-16 | Updated: 2017-05-18

Exploit.In()
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.

Count: 593427119 | Created: 2016-10-13 | Updated: 2017-05-06

Anti Public Combo List()
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.

Count: 457962538 | Created: 2016-12-16 | Updated: 2017-05-04

R2 (2017 forum breach)(r2games.com)
In early 2017, the forum for the gaming website R2 Games was hacked. R2 had previously appeared on HIBP in 2015 after a prior incident. This one exposed over 1 million unique user accounts and corresponding MD5 password hashes with no salt.

Count: 1023466 | Created: 2017-01-01 | Updated: 2017-04-25

Youku(youku.com)
In late 2016, the online Chinese video service Youku suffered a data breach. The incident exposed 92 million unique user accounts and corresponding MD5 password hashes. The data was contributed to Have I Been Pwned courtesy of rip@creep.im.

Count: 91890110 | Created: 2016-12-01 | Updated: 2017-04-15

Bitcoin Talk(bitcointalk.org)
In May 2015, the Bitcoin forum Bitcoin Talk was hacked and over 500k unique email addresses were exposed. The attack led to the exposure of a raft of personal data including usernames, email and IP addresses, genders, birth dates, security questions and MD5 hashes of their answers plus hashes of the passwords themselves.

Count: 501407 | Created: 2015-05-22 | Updated: 2017-03-27

HLTV(hltv.org)
In June 2016, the "home of competitive Counter Strike" website HLTV was hacked and 611k accounts were exposed. The attack led to the exposure of names, usernames, email addresses and bcrypt hashes of passwords.

Count: 611070 | Created: 2016-06-19 | Updated: 2017-03-22

CrimeAgency vBulletin Hacks()
In January 2016, a large number of unpatched vBulletin forums were compromised by an actor known as "CrimeAgency". A total of 140 forums had data including usernames, email addresses and passwords (predominantly stored as salted MD5 hashes), extracted and then distributed. Refer to the complete list of the forums for further information on which sites were impacted.

Count: 942044 | Created: 2017-01-19 | Updated: 2017-03-21

NetProspex(netprospex.com)
In 2016, a list of over 33 million individuals in corporate America sourced from Dun & Bradstreet's NetProspex service was leaked online. D&B believe the targeted marketing data was lost by a customer who purchased it from them. It contained extensive personal and corporate information including names, email addresses, job titles and general information about the employer.

Count: | Created: 2016- | Updated: 2017-

Retina-X(retinax.com)
In February 2017, the mobile device monitoring software developer Retina-X was hacked and customer data downloaded before being wiped from their servers. The incident was covered in the Motherboard article titled Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones. The service, used to monitor mobile devices, had 71k email addresses and MD5 hashes with no salt exposed. Retina-X disclosed the incident in a blog post on April 27, 2017.

Count: 71153 | Created: 2017-02-23 | Updated: 2017-04-30

FashionFantasyGame(fashionfantasygame.com)
In late 2016, the fashion gaming website Fashion Fantasy Game suffered a data breach. The incident exposed 2.3 million unique user accounts and corresponding MD5 password hashes with no salt. The data was contributed to Have I Been Pwned courtesy of rip@creep.im.

Count: 2357872 | Created: 2016-12-01 | Updated: 2017-04-20

Health Now Networks(healthnow.co)
In March 2017, the telemarketing service Health Now Networks left a database containing hundreds of thousands of medical records exposed. There were over 900,000 records in total containing significant volumes of personal information including names, dates of birth, various medical conditions and operator notes on the individuals' health. The data included over 320k unique email addresses.

Count: 321920 | Created: 2017-03-25 | Updated: 2017-04-07

Evony(evony.com)
In June 2016, the online multiplayer game Evony was hacked and over 29 million unique accounts were exposed. The attack led to the exposure of usernames, email and IP addresses and MD5 hashes of passwords (without salt).

Count: 29396116 | Created: 2016-06-01 | Updated: 2017-03-25

Torrent Invites(torrent-invites.com)
In December 2013, the torrent site Torrent Invites was hacked and over 352k accounts were exposed. The vBulletin forum contained usernames, email and IP addresses, birth dates and salted MD5 hashes of passwords.

Count: 352120 | Created: 2013-12-12 | Updated: 2017-03-22

Soundwave(soundwave.com)
In approximately mid 2015, the music tracking app Soundwave suffered a data breach. The breach stemmed from an incident whereby "production data had been used to populate the test database" and was then inadvertently exposed in a MongoDB. The data contained 130k records and included email addresses, dates of birth, genders and MD5 hashes of passwords without a salt.

Count: 130705 | Created: 2015-07-16 | Updated: 2017-03-17

Ster-Kinekor(sterkinekor.co.za)
In 2016, the South African cinema company Ster-Kinekor had a security flaw which leaked a large amount of customer data via an enumeration vulnerability in the API of their old website. Whilst more than 6 million accounts were leaked by the flaw, the exposed data only contained 1.6 million unique email addresses. The data also included extensive personal information such as names, addresses, birthdates, genders and plain text passwords.

Count: 1619544 | Created: 2017-03-09 | Updated: 2017-03-13

33698126	09-01	03-15

BTC-E(btc-e.com)
In October 2014, the Bitcoin exchange BTC-E was hacked and 568k accounts were exposed. The data included email and IP addresses, wallet balances and hashed passwords.

Count:	Created:	Updated:
568340	2014-10-01	2017-03-12

Little Monsters(littlemonsters.com)
In approximately January 2017, the Lady Gaga fan site known as "Little Monsters" suffered a data breach that impacted 1 million accounts. The data contained usernames, email addresses, dates of birth and bcrypt hashes of passwords.

Count:	Created:	Updated:
995698	2017-01-01	2017-03-07

Funimation(funimation.com)
In July 2016, the anime site Funimation suffered a data breach that impacted 2.5 million accounts. The data contained usernames, email addresses, dates of birth and salted SHA1 hashes of passwords.

Count:	Created:	Updated:
2491103	2016-07-01	2017-02-20

Justdate.com(justdate.com)
An alleged breach of the dating website Justdate.com began circulating in approximately September 2016. Comprised of over 24 million records, the data contained various personal attributes such as email addresses, dates of birth and physical locations. However, upon verification with HIBP subscribers, only a fraction of the data was found to be accurate and no account owners recalled using the Justdate.com service. This breach has consequently been flagged as fabricated; it's highly unlikely the data was sourced from Justdate.com.

Count:	Created:	Updated:
24451312	2016-09-29	2017-02-07

HongFire(hongfire.com)
In March 2015, the anime and manga forum HongFire suffered a data breach. The hack of their vBulletin forum led to the exposure of 1 million accounts along with email and IP addresses, usernames, dates of birth and salted MD5 passwords.

Count:	Created:	Updated:
999991	2015-03-01	2017-02-05

PSP ISO(pspiso.com)
In approximately September 2015, the PlayStation PSP forum known as PSP ISO was hacked and almost 1.3 million accounts were exposed. Along with email and IP addresses, the vBulletin forum also exposed salted MD5 password hashes.

Count:	Created:	Updated:
1274070	2015-09-25	2017-01-29

Non Nude Girls(nonnudegirls.org)
In May 2013, the non-consensual voyeurism site "Non Nude Girls" suffered a data breach. The hack of the vBulletin forum led to the exposure of over 75k accounts along with email and IP addresses, names and plain text passwords.

Count:	Created:	Updated:
75383	2013-05-21	2017-01-25

The Candid Board(thecandidboard.com)
In September 2015, the non-consensual voyeurism site "The Candid Board" suffered a data breach. The hack of the vBulletin forum led to the exposure of over 178k accounts along with email and IP addresses, dates of

River City Media Spam List(rivercitymediaonline.com)
In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

Count:	Created:	Updated:
393430309	2017-01-01	2017-03-08

CloudPets(cloudpets.com)
In January, the maker of teddy bears that record children's voices and sends them to family and friends via the internet CloudPets left their database publicly exposed and it was subsequently downloaded by external parties (the data was also subject to 3 different ransom demands). 583k records were provided to HIBP via a data trader and included email addresses and bcrypt hashes, but the full extent of user data exposed by the system was over 821k records and also included children's names and references to portrait photos and voice recordings.

Count:	Created:	Updated:
583503	2017-01-01	2017-02-27

Elance(elance.com)
Sometime in 2009, staffing platform Elance suffered a data breach that impacted 1.3 million accounts. Appearing online 8 years later, the data contained usernames, email addresses, phone numbers and SHA1 hashes of passwords, amongst other personal data.

Count:	Created:	Updated:
1291178	2009-01-01	2017-02-18

Freedom Hosting II(fhostingesps6bly.onion)
In January 2017, the free hidden service host Freedom Hosting II suffered a data breach. The attack allegedly took down 20% of dark web sites running behind Tor hidden services with the attacker claiming that of the 10,613 impacted sites, more than 50% of the content was child pornography. The hack led to the exposure of MySQL databases for the sites which included a vast amount of information on the hidden services Freedom Hosting II was managing. The impacted data classes far exceeds those listed for the breach and differ between the thousands of impacted sites.

Count:	Created:	Updated:
380830	2017-01-31	2017-02-05

CD Projekt RED(cdprojektred.com)
In March 2016, Polish game developer CD Projekt RED suffered a data breach. The hack of their forum led to the exposure of almost 1.9 million accounts along with usernames, email addresses and salted SHA1 passwords.

Count:	Created:	Updated:
1871373	2016-03-01	2017-01-31

Xbox 360 ISO(xbox360iso.com)
In approximately September 2015, the XBOX 360 forum known as XBOX360 ISO was hacked and 1.2 million accounts were exposed. Along with email and IP addresses, the vBulletin forum also exposed salted MD5 password hashes.

Count:	Created:	Updated:
1296959	2015-09-25	2017-01-29

MrExcel(mrexcel.com)
In December 2016, the forum for the Microsoft Excel tips and solutions site Mr Excel suffered a data breach. The hack of the vBulletin forum led to the exposure of over 366k accounts along with email and IP addresses, dates of birth and salted passwords hashed with MD5. The owner of the MrExcel forum subsequently self-submitted the data to HIBP.

Count:	Created:	Updated:
366140	2016-12-05	2017-01-22

Eroticy(eroticy.com)
In mid-2016, it's alleged that the adult website known as Eroticy was hacked. Almost 1.4 million unique accounts were found circulating in late 2016 which contained a raft of personal information ranging from email addresses to phone numbers to plain text passwords. Whilst many HIBP subscribers confirmed their data was legitimate, the actual source of the breach remains

birth and salted passwords hashed with MD5.

Count: 178201 | Created: 2015-09-03 | Updated: 2017-01-22

QIP(qip.ru)
In mid-2011, the Russian instant messaging service known as QIP (Quiet Internet Pager) suffered a data breach. The attack resulted in the disclosure of over 26 million unique accounts including email addresses and passwords with the data eventually appearing in public years later.

Count: 26183992 | Created: 2011-06-01 | Updated: 2017-01-08

Cross Fire(cfire.mail.ru)
In August 2016, the Russian gaming forum known as Cross Fire (or cfire.mail.ru) was hacked along with a number of other forums on the Russian mail provider, mail.ru. The vBulletin forum contained 12.8 million accounts including usernames, email addresses and passwords stored as salted MD5 hashes.

Count: 12865609 | Created: 2016-08-08 | Updated: 2016-12-28

Parapa(parapa.mail.ru)
In August 2016, the Russian gaming site known as xd0x9fxd0xb0xd1x80xd0xb0 xd0x9fxd0xb0 (or parapa.mail.ru) was hacked along with a number of other forums on the Russian mail provider, mail.ru. The vBulletin forum contained 4.9 million accounts including usernames, email addresses and passwords stored as salted MD5 hashes.

Count: 4946850 | Created: 2016-08-08 | Updated: 2016-12-28

Kimsufi(kimsufi.com)
In mid-2015, the forum for the providers of affordable dedicated servers known as Kimsufi suffered a data breach. The vBulletin forum contained over half a million accounts including usernames, email and IP addresses and passwords stored as salted MD5 hashes.

Count: 504565 | Created: 2015-05-01 | Updated: 2016-12-27

uuu9(uuu9.com)
In September 2016, data was allegedly obtained from the Chinese website known as uuu9.com and contained 7.5M accounts. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and user names. Read more about Chinese data breaches in Have I Been Pwned.

Count: 7485802 | Created: 2016-09-06 | Updated: 2016-12-27

PayAsUGym(payasugym.com)
In December 2016, an attacker breached PayAsUGym's website exposing over 400k customers' personal data. The data was consequently leaked publicly and broadly distributed via Twitter. The leaked data contained personal information including email addresses and passwords hashed using MD5 without a salt.

Count: 400260 | Created: 2016-12-15 | Updated: 2016-12-17

SC Daily Phone Spam List(data4marketers.com)
In early 2015, a spam list known as SC Daily Phone emerged containing almost 33M identities. The data includes personal attributes such as names, physical and IP addresses, genders, birth dates and phone numbers. Read more about spam lists in HIBP.

inconclusive. A detailed account of the data has been published in the hope of identifying the origin of the breach.

Count: 1370175 | Created: 2015-06-01 | Updated: 2017-01-10

PokemonNegro(pokemonnegro.com)
In approximately October 2016, the Spanish Pokxc3xa9mon site Pokxc3xa9mon Negro suffered a data breach. The attack resulted in the disclosure of 830k accounts including email and IP addresses along with plain text passwords. Pokxc3xa9mon Negro did not respond when contacted about the breach.

Count: 830155 | Created: 2016-10-01 | Updated: 2017-01-03

DaniWeb(daniweb.com)
In late 2015, the technology and social site DaniWeb suffered a data breach. The attack resulted in the disclosure of 1.1 million accounts including email and IP addresses which were also accompanied by salted MD5 hashes of passwords. However, DaniWeb have advised that "the breached password hashes and salts are incorrect" and that they have since switched to new infrastructure and software.

Count: 1131636 | Created: 2015-12-01 | Updated: 2016-12-28

Bot of Legends(botoflegends.com)
In November 2014, the forum for Bot of Legends suffered a data breach. The IP.Board forum contained 238k accounts including usernames, email and IP addresses and passwords stored as salted MD5 hashes.

Count: 238373 | Created: 2014-11-13 | Updated: 2016-12-27

OVH(ovh.com)
In mid-2015, the forum for the hosting provider known as OVH suffered a data breach. The vBulletin forum contained 453k accounts including usernames, email and IP addresses and passwords stored as salted MD5 hashes.

Count: 452899 | Created: 2015-05-01 | Updated: 2016-12-27

Ethereum(ethereum.org)
In December 2016, the forum for the public blockchain-based distributed computing platform Ethereum suffered a data breach. The database contained over 16k unique email addresses along with IP addresses, private forum messages and (mostly) bcrypt hashed passwords. Ethereum elected to self-submit the data to HIBP, providing the service with a list of email addresses impacted by the incident.

Count: 16431 | Created: 2016-12-16 | Updated: 2016-12-20

QuinStreet(quinstreet.com)
In approximately late 2015, the maker of "performance marketing products" QuinStreet had a number of their online assets compromised. The attack impacted 28 separate sites, predominantly technology forums such as flashkit.com, codeguru.com and webdeveloper.com (view a full list of sites). QuinStreet advised that impacted users have been notified and passwords reset. The data contained details on over 4.9 million people and included email addresses, dates of birth and salted MD5 hashes.

Count: 4907802 | Created: 2015-12-14 | Updated: 2016-12-17

Special K Data Feed Spam List(data4marketers.com)
In mid to late 2015, a spam list known as the Special K Data Feed was discovered containing almost 31M identities. The data includes personal attributes such as names, physical and IP addresses, genders, birth dates and phone numbers. Read more about spam lists in HIBP.

Count: 30741620 | Created: 2015-10-07 | Updated: 2016-11-24

Count: 32939105 | Created: 2015-04-14 | Updated: 2016-11-24

GeekedIn(geekedin.net)
In August 2016, the technology recruitment site GeekedIn left a MongoDB database exposed and over 8M records were extracted by an unknown third party. The breached data was originally scraped from GitHub in violation of their terms of use and contained information exposed in public profiles, including over 1 million members' email addresses. Full details on the incident (including how impacted members can see their leaked data) are covered in the blog post on 8 million GitHub profiles were leaked from GeekedIn's MongoDB - here's how to see yours.

Count: 1073164 | Created: 2016-08-15 | Updated: 2016-11-17

CheapAssGamer.com(cheapassgamer.com)
In approximately mid-2015, the forum for CheapAssGamer.com suffered a data breach. The database from the IP.Board based forum contained 445k accounts including usernames, email and IP addresses and salted MD5 password hashes.

Count: 444767 | Created: 2015-07-01 | Updated: 2016-11-08

Aipai.com(aipai.com)
In September 2016, data allegedly obtained from the Chinese gaming website known as Aipai.com and containing 6.5M accounts was leaked online. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and MD5 password hashes. Read more about Chinese data breaches in Have I Been Pwned.

Count: 6496778 | Created: 2016-09-27 | Updated: 2016-11-07

Duowan.com(duowan.com)
In approximately 2011, data was allegedly obtained from the Chinese gaming website known as Duowan.com and contained 2.6M accounts. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses, user names and plain text passwords. Read more about Chinese data breaches in Have I Been Pwned.

Count: 2639894 | Created: 2011-01-01 | Updated: 2016-11-07

Heroes of Gaia(heroesofgaia.com)
In early 2013, the online fantasy multiplayer game Heroes of Gaia suffered a data breach. The newest records in the data set indicate a breach date of 4 January 2013 and include usernames, IP and email addresses but no passwords.

Count: 179967 | Created: 2013-01-04 | Updated: 2016-11-07

War Inc.(thewarinc.com)
In mid-2012, the real-time strategy game War Inc. suffered a data breach. The attack resulted in the exposure of over 1 million accounts including usernames, email addresses and salted MD5 hashes of passwords.

Count: 1020136 | Created: 2012-07-04 | Updated: 2016-11-07

Rambler(rambler.ru)
In late 2016, a data dump of almost 100M accounts from Rambler, sometimes referred to as "The Russian Yahoo", was discovered being traded online. The data set provided to Have I Been Pwned included 91M unique usernames

Dodonew.com(dodonew.com)
In late 2011, data was allegedly obtained from the Chinese website known as Dodonew.com and contained 8.7M accounts. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and user names. Read more about Chinese data breaches in Have I Been Pwned.

Count: 8718404 | Created: 2011-12-01 | Updated: 2016-11-10

Lookbook(lookbook.nu)
In August 2012, the fashion site Lookbook suffered a data breach. The data later appeared listed for sale in June 2016 and included 1.1 million usernames, email and IP addresses, birth dates and plain text passwords.

Count: 1074948 | Created: 2012-08-24 | Updated: 2016-11-08

Civil Online(co188.com)
In mid-2011, data was allegedly obtained from the Chinese engineering website known as Civil Online and contained 7.8M accounts. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email and IP addresses, user names and MD5 password hashes. Read more about Chinese data breaches in Have I Been Pwned.

Count: 7830195 | Created: 2011-07-10 | Updated: 2016-11-07

Epic Games(epicgames.com)
In August 2016, the Epic Games forum suffered a data breach, allegedly due to a SQL injection vulnerability in vBulletin. The attack resulted in the exposure of 252k accounts including usernames, email addresses and salted MD5 hashes of passwords.

Count: 251661 | Created: 2016-08-11 | Updated: 2016-11-07

Unreal Engine(unrealengine.com)
In August 2016, the Unreal Engine Forum suffered a data breach, allegedly due to a SQL injection vulnerability in vBulletin. The attack resulted in the exposure of 530k accounts including usernames, email addresses and salted MD5 hashes of passwords.

Count: 530147 | Created: 2016-08-11 | Updated: 2016-11-07

uTorrent(utorrent.com)
In early 2016, the forum for the uTorrent BitTorrent client suffered a data breach which came to light later in the year. The database from the IP.Board based forum contained 395k accounts including usernames, email addresses and MD5 password hashes without a salt.

Count: 395044 | Created: 2016-01-14 | Updated: 2016-11-05

Modern Business Solutions(modbsolutions.com)
In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The

(which also form part of Rambler email addresses) and plain text passwords. According to Rambler, the data dates back to March 2014.

Count: 91436280 | Created: 2014-03-01 | Updated: 2016-11-01

GFAN(gfan.com)
In October 2016, data surfaced that was allegedly obtained from the Chinese website known as GFAN and contained 22.5M accounts. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email and IP addresses, user names and salted and hashed passwords. Read more about Chinese data breaches in Have I Been Pwned.

Count: 22526334 | Created: 2016-10-10 | Updated: 2016-10-10

126(126.com)
In approximately 2012, it's alleged that the Chinese email service known as 126 suffered a data breach that impacted 6.4 million subscribers. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and plain text passwords. Read more about Chinese data breaches in Have I Been Pwned.

Count: 6414191 | Created: 2012-01-01 | Updated: 2016-10-08

Aternos(aternos.org)
In December 2015, the service for creating and running free Minecraft servers known as Aternos suffered a data breach that impacted 1.4 million subscribers. The data included usernames, email and IP addresses and hashed passwords.

Count: 1436486 | Created: 2015-12-06 | Updated: 2016-10-01

i-Dressup(i-dressup.com)
In June 2016, the teen social site known as i-Dressup was hacked and over 2 million user accounts were exposed. At the time the hack was reported, the i-Dressup operators were not contactable and the underlying SQL injection flaw remained open, allegedly exposing a total of 5.5 million accounts. The breach included email addresses and passwords stored in plain text.

Count: 2191565 | Created: 2016-07-15 | Updated: 2016-09-26

GameTuts(game-tuts.com)
Likely in early 2015, the video game website GameTuts suffered a data breach and over 2 million user accounts were exposed. The site later shut down in July 2016 but was identified as having been hosted on a vBulletin forum. The exposed data included usernames, email and IP addresses and salted MD5 hashes.

Count: 2064274 | Created: 2015-03-01 | Updated: 2016-09-23

MoDaCo(modaco.com)
In approximately January 2016, the UK based Android community known as MoDaCo suffered a data breach which exposed 880k subscriber identities. The data included email and IP addresses, usernames and passwords stored as salted MD5 hashes.

Count: 879703 | Created: 2016-01-01 | Updated: 2016-09-20

Regpack(bluesnap.com)
In July 2016, a tweet was posted with a link to

data was subsequently attributed to "Modern Business Solutions", a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.

Count: 58843488 | Created: 2016-10-08 | Updated: 2016-10-12

NetEase(163.com)
In October 2015, the Chinese site known as NetEase (located at 163.com) was reported as having suffered a data breach that impacted hundreds of millions of subscribers. Whilst there is evidence that the data itself is legitimate (multiple HIBP subscribers confirmed a password they use is in the data), due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and plain text passwords. Read more about Chinese data breaches in Have I Been Pwned.

Count: 234842089 | Created: 2015-10-19 | Updated: 2016-10-09

Taobao(taobao.com)
In approximately 2012, it's alleged that the Chinese shopping site known as Taobao suffered a data breach that impacted over 21 million subscribers. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and plain text passwords. Read more about Chinese data breaches in Have I Been Pwned.

Count: 21149008 | Created: 2012-01-01 | Updated: 2016-10-08

Leet(leet.cc)
In August 2016, the service for creating and running Pocket Minecraft edition servers known as Leet was reported as having suffered a data breach that impacted 6 million subscribers. The incident reported by Softpedia had allegedly taken place earlier in the year, although the data set sent to HIBP was dated as recently as early September but contained only 2 million subscribers. The data included usernames, email and IP addresses and SHA512 hashes. A further 3 million accounts were obtained and added to HIBP several days after the initial data was loaded bringing the total to over 5 million.

Count: 5081689 | Created: 2016-09-10 | Updated: 2016-09-30

gPotato(gpotato.com)
In July 2007, the multiplayer game portal known as gPotato (link to archive of the site at that time) suffered a data breach and over 2 million user accounts were exposed. The site later merged into the Webzen portal where the original accounts still exist today. The exposed data included usernames, email and IP addresses, MD5 hashes and personal attributes such as gender, birth date, physical address and security questions and answers stored in plain text.

Count: 2136520 | Created: 2007-07-12 | Updated: 2016-09-24

Last.fm(last.fm)
In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. Whilst Last.fm knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.

Count: 37217682 | Created: 2012-03-22 | Updated: 2016-09-20

eThekwini Municipality(eservices.durban.gov.za)
In September 2016, the new eThekwini eServices website in South Africa was launched with a number of security holes that lead to the leak of over 98k residents' personal information and utility bills across 82k unique email addresses. Emails were sent prior to launch containing passwords in plain text and the site allowed anyone to download utility bills without sufficient authentication. Various methods of customer data enumeration was possible and phishing attacks began appearing the day after launch.

Count: 81830 | Created: 2016-09-07 | Updated: 2016-09-15

an alleged data breach of BlueSnap, a global payment gateway and merchant account provider. The data contained 324k payment records across 105k unique email addresses and included personal attributes such as name, home address and phone number. The data was verified with multiple Have I Been Pwned subscribers who confirmed it also contained valid transactions, partial credit card numbers, expiry dates and CVVs. A downstream consumer of BlueSnap services known as Regpack was subsequently identified as the source of the data after they identified human error had left the transactions exposed on a publicly facing server. A full investigation of the data and statement by Regpack is detailed in the post titled Someone just lost 324k payment records, complete with CVVs.

Count: 104977 | Created: 2016-05-20 | Updated: 2016-09-13

Pokebip(pokebip.com)
In July 2015, the French Pokxc3xa9mon site Pokxc3xa9bip suffered a data breach which exposed 657k subscriber identities. The data included email and IP addresses, usernames and passwords stored as unsalted MD5 hashes.

Count: 657001 | Created: 2015-07-28 | Updated: 2016-09-09

Onverse(onverse.com)
In January 2016, the online virtual world known as Onverse was hacked and 800k accounts were exposed. Along with email and IP addresses, the site also exposed salted MD5 password hashes.

Count: 800157 | Created: 2016-01-01 | Updated: 2016-09-06

WIIU ISO(wiiuiso.com)
In September 2015, the Nintendo Wii U forum known as WIIU ISO was hacked and 458k accounts were exposed. Along with email and IP addresses, the vBulletin forum also exposed salted MD5 password hashes.

Count: 458155 | Created: 2015-09-25 | Updated: 2016-09-06

Dropbox(dropbox.com)
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).

Count: 68648009 | Created: 2012-07-01 | Updated: 2016-08-31

Nihonomaru(nihonomaru.net)
In late 2015, the anime community known as Nihonomaru had their vBulletin forum hacked and 1.7 million accounts exposed. The compromised data included email and IP addresses, usernames and salted hashes of passwords.

Count: 1697282 | Created: 2015-12-01 | Updated: 2016-08-30

GTAGaming(gtagaming.com)
In August 2016, the Grand Theft Auto forum GTAGaming was hacked and nearly 200k user accounts were leaked. The vBulletin based forum included usernames, email addresses and password hashes.

Count: 197184 | Created: 2016-08-01 | Updated: 2016-08-23

xat(xat.com)
In November 2015, the online chatroom known as "xat" was hacked and 6 million user

ClixSense(clixsense.com)
In September 2016, the paid-to-click site ClixSense suffered a data breach which exposed 2.4 million subscriber identities. The breached data was then posted online by the attackers who claimed it was a subset of a larger data breach totalling 6.6 million records. The leaked data was extensive and included names, physical, email and IP addresses, genders and birth dates, account balances and passwords stored as plain text.

Count: 2424784 | Created: 2016-09-04 | Updated: 2016-09-11

DLH.net(dlh.net)
In July 2016, the gaming news site DLH.net suffered a data breach 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 Vigilante.pw.

Count: 3264710 | Created: 2016-07-31 | Updated: 2016-09-07

ServerPact(serverpact.com)
In mid-2015, the Dutch Minecraft site ServerPact was hacked and 73k accounts were exposed. Along with birth dates, email and IP addresses, the site also exposed SHA1 password hashes with the username as the salt.

Count: 73587 | Created: 2016-01-01 | Updated: 2016-09-06

Brazzers(brazzers.com)
In April 2013, the adult website known as Brazzers was hacked and 790k accounts were exposed publicly. Each record included a username, email address and password stored in plain text. The breach was brought to light by the Vigilante.pw data breach reporting site in September 2016.

Count: 790724 | Created: 2013-04-01 | Updated: 2016-09-05

InterPals(interpals.net)
In late 2015, the online penpal site InterPals had their website hacked and 3.4 million accounts exposed. The compromised data included email addresses, geographical locations, birthdates and salted hashes of passwords.

Count: 3439414 | Created: 2015-11-04 | Updated: 2016-08-30

Minecraft World Map(minecraftworldmap.com)
In approximately January 2016, the Minecraft World Map site designed for sharing maps created for the game was hacked and over 71k user accounts were exposed. The data included usernames, email and IP addresses along with salted and hashed passwords.

Count: 71081 | Created: 2016-01-15 | Updated: 2016-08-29

Teracod(teracod.org)
In May 2015, almost 100k user records were extracted from the Hungarian torrent site known as Teracod. The data was later discovered being torrented itself and included email addresses, passwords, private messages between members and the peering history of IP addresses using the service.

Count: 97151 | Created: 2016-05-28 | Updated: 2016-08-22

Warframe(warframe.com)
In November 2014, the online game Warframe was hacked and 819k unique email addresses were exposed. Allegedly due to a SQL injection flaw in Drupal,

accounts were exposed. Used as a chat engine on websites, the leaked data included usernames, email and IP addresses along with hashed passwords.

Count: 5968783 | Created: 2015-11-04 | Updated: 2016-08-05

Trillian(trillian.im)
In December 2015, the instant messaging application Trillian suffered a data breach. The breach became known in July 2016 and exposed various personal data attributes including names, email addresses and passwords stored as salted MD5 hashes.

Count: 3827238 | Created: 2015-12-27 | Updated: 2016-07-15

Neopets(neopets.com)
In May 2016, a set of breached data originating from the virtual pet website "Neopets" was found being traded online. Allegedly hacked "several years earlier", the data contains sensitive personal information including birthdates, genders and names as well as almost 27 million unique email addresses. Passwords were stored in plain text and IP addresses were also present in the breach.

Count: 26892897 | Created: 2013-05-05 | Updated: 2016-07-07

iMesh(imesh.com)
In September 2013, the media and file sharing client known as iMesh was hacked and approximately 50M accounts were exposed. The data was later put up for sale on a dark market website in mid-2016 and included email and IP addresses, usernames and salted MD5 hashes.

Count: 49467477 | Created: 2013-09-22 | Updated: 2016-07-02

WHMCS(whmcs.com)
In May 2012, the web hosting, billing and automation company WHMCS suffered a data breach that exposed 134k email addresses. The breach included extensive information about customers and payment histories including partial credit card numbers.

Count: 134047 | Created: 2012-05-21 | Updated: 2016-06-28

VK(vk.com)
In approximately 2012, the Russian social media site known as VK was hacked and almost 100 million accounts were exposed. The data emerged in June 2016 where it was being sold via a dark market website and included names, phone numbers email addresses and plain text passwords.

Count: 93338602 | Created: 2012-01-01 | Updated: 2016-06-09

MySpace(myspace.com)
In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.

Count: 359420698 | Created: 2008-07-01 | Updated: 2016-05-31

Fling(fling.com)
In 2011, the self-proclaimed "World's Best Adult Social Network" website known as Fling was hacked and more than 40 million accounts obtained by the attacker. The breached data included highly sensitive personal attributes such as sexual orientation and sexual interests as well as email addresses and passwords

the attack exposed usernames, email addresses and data in a "pass" column which adheres to the salted SHA12 password hashing pattern used by Drupal 7. Digital Extremes (the developers of Warframe), asserts the salted hashes are of "alias names" rather than passwords.

Count: 819478 | Created: 2014-11-24 | Updated: 2016-07-21

17(17app.co)
In April 2016, customer data obtained from the streaming app known as "17" appeared listed for sale on a Tor hidden service marketplace. The data contained over 4 million unique email addresses along with IP addresses, usernames and passwords stored as unsalted MD5 hashes.

Count: 4009640 | Created: 2016-04-19 | Updated: 2016-07-08

Badoo(badoo.com)
In June 2016, a data breach allegedly originating from the social website Badoo was found to be circulating amongst traders. Likely obtained several years earlier, the data contained 112 million unique email addresses with personal data including names, birthdates and passwords stored as MD5 hashes. Whilst there are many indicators suggesting Badoo did indeed suffer a data breach, the legitimacy of the data could not be emphatically proven so this breach has been categorised as "unverified".

Count: 112005531 | Created: 2013-06-01 | Updated: 2016-07-06

Tianya(tianya.cn)
In December 2011, China's largest online forum known as Tianya was hacked and tens of millions of accounts were obtained by the attacker. The leaked data included names, usernames and email addresses.

Count: 29020808 | Created: 2011-12-26 | Updated: 2016-06-30

Uiggy(uiggy.com)
In June 2016, the Facebook application known as Uiggy was hacked and 4.3M accounts were exposed, 2.7M of which had email addresses against them. The leaked accounts also exposed names, genders and the Facebook ID of the owners.

Count: 2682650 | Created: 2016-06-01 | Updated: 2016-06-27

BitTorrent(bittorrent.com)
In January 2016, the forum for the popular torrent software BitTorrent was hacked. The IP.Board based forum stored passwords as weak SHA1 salted hashes and the breached data also included usernames, email and IP addresses.

Count: 34235 | Created: 2016-01-01 | Updated: 2016-06-08

tumblr(tumblr.com)
In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

Count: 65469298 | Created: 2013-02-28 | Updated: 2016-05-29

Fur Affinity(furaffinity.net)
In May 2016, the Fur Affinity website for people with an interest in anthropomorphic animal characters (also known as "furries") was hacked. The attack exposed 1.2M email addresses (many accounts had a different "first" and "last" email against them) and hashed passwords.

stored in plain text.

Count: 40767652 | Created: 2011-03-10 | Updated: 2016-05-28

LinkedIn(linkedin.com)
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.

Count: 164611595 | Created: 2012-05-05 | Updated: 2016-05-21

Qatar National Bank(qnb.com)
In July 2015, the Qatar National Bank suffered a data breach which exposed 15k documents totalling 1.4GB and detailing more than 100k accounts with passwords and PINs. The incident was made public some 9 months later in April 2016 when the documents appeared publicly on a file sharing site. Analysis of the breached data suggests the attack began by exploiting a SQL injection flaw in the bank's website.

Count: 88678 | Created: 2015-07-01 | Updated: 2016-05-01

Lifeboat(lbsg.net)
In January 2016, the Minecraft community known as Lifeboat was hacked and more than 7 million accounts leaked. Lifeboat knew of the incident for three months before the breach was made public but elected not to advise customers. The leaked data included usernames, email addresses and passwords stored as straight MD5 hashes.

Count: 7089395 | Created: 2016-01-01 | Updated: 2016-04-25

TruckersMP(truckersmp.com)
In February 2016, the online trucking simulator mod TruckersMP suffered a data breach which exposed 84k user accounts. In a first for "Have I Been Pwned", the breached data was self-submitted directly by the organisation that was breached itself.

Count: 83957 | Created: 2016-02-25 | Updated: 2016-04-24

Mate1.com(mate1.com)
In February 2016, the dating site mate1.com suffered a huge data breach resulting in the disclosure of over 27 million subscribers' information. The data included deeply personal information about their private lives including drug and alcohol habits, incomes levels and sexual fetishes as well as passwords stored in plain text.

Count: 27393015 | Created: 2016-02-29 | Updated: 2016-04-14

Avast(avast.com)
In May 2014, the Avast anti-virus forum was hacked and 423k member records were exposed. The Simple Machines Based forum included usernames, emails and password hashes.

Count: 422959 | Created: 2014-05-26 | Updated: 2016-03-12

Lord of the Rings Online(lotro.com)
In August 2013, the interactive video game Lord of the Rings Online suffered a data breach that exposed over 1.1M players' accounts. The data was being actively traded on underground forums and included email addresses, birth dates and password hashes.

Count: 1141278 | Created: 2013-08-01 | Updated: 2016-03-12

Count: 1270564 | Created: 2016-05-17 | Updated: 2016-05-27

Rosebutt Board(rosebuttboard.com)
Some time prior to May 2016, the forum known as "Rosebutt Board" was hacked and 107k accounts were exposed. The self-described "top one board for anal fisting, prolapse, huge insertions and rosebutt fans" had email and IP addresses, usernames and weakly stored salted MD5 password hashes hacked from the IP.Board based forum.

Count: 107303 | Created: 2016-05-09 | Updated: 2016-05-10

Beautiful People(beautifulpeople.com)
In November 2015, the dating website Beautiful People was hacked and over 1.1M accounts were leaked. The data was being traded in underground circles and included a huge amount of personal information related to dating.

Count: 1100089 | Created: 2015-11-11 | Updated: 2016-04-25

Naughty America(naughtyamerica.com)
In March 2016, the adult website Naughty America was hacked and the data consequently sold online. The breach included data from numerous systems with various personal identity attributes, the largest of which had passwords stored as easily crackable MD5 hashes. There were 1.4 million unique email addresses in the breach.

Count: 1398630 | Created: 2016-03-14 | Updated: 2016-04-24

COMELEC (Philippines Voters)(comelec.gov.ph)
In March 2016, the Philippines Commission of Elections website (COMELEC) was attacked and defaced, allegedly by Anonymous Philippines. Shortly after, data on 55 million Filipino voters was leaked publicly and included sensitive information such as genders, marital statuses, height and weight and biometric fingerprint data. The breach only included 228k email addresses.

Count: 228605 | Created: 2016-03-27 | Updated: 2016-04-14

The Fappening(thefappening.so)
In December 2015, the forum for discussing naked celebrity photos known as "The Fappening" (named after the iCloud leaks of 2014) was compromised and 179k accounts were leaked. Exposed member data included usernames, email addresses and salted hashes of passwords.

Count: 179030 | Created: 2015-12-01 | Updated: 2016-04-13

Dungeons & Dragons Online(ddo.com)
In April 2013, the interactive video game Dungeons & Dragons Online suffered a data breach that exposed almost 1.6M players' accounts. The data was being actively traded on underground forums and included email addresses, birth dates and password hashes.

Count: 1580933 | Created: 2013-04-02 | Updated: 2016-03-12

Malwarebytes(malwarebytes.org)
In November 2014, the Malwarebytes forum was hacked and 111k member records were exposed. The IP.Board forum included email and IP addresses, birth dates and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

Count: 111623 | Created: 2014-11-15 | Updated: 2016-03-09

Minefield(minefield.fr)
In June 2015, the French Minecraft server known as Minefield was hacked and 188k member records were exposed. The IP.Board forum included email and IP addresses, birth dates and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

Count: 188343 | Created: 2015-06-28 | Updated: 2016-03-09

Team SoloMid(solomid.net)
In December 2014, the electronic sports organisation known as Team SoloMid was hacked and 442k members accounts were leaked. The accounts included email and IP addresses, usernames and salted hashes of passwords.

Count: 442166 | Created: 2014-12-22 | Updated: 2016-03-09

WildStar(wildstar-online.com)
In July 2015, the IP.Board forum for the gaming website WildStar suffered a data breach that exposed over 738k forum members' accounts. The data was being actively traded on underground forums and included email addresses, birth dates and passwords.

Count: 738556 | Created: 2015-07-11 | Updated: 2016-03-06

KM.RU(km.ru)
In February 2016, the Russian portal and email service KM.RU was the target of an attack which was consequently detailed on Reddit. Allegedly protesting "the foreign policy of Russia in regards to Ukraine", KM.RU was one of several Russian sites in the breach and impacted almost 1.5M accounts including sensitive personal information.

Count: 1476783 | Created: 2016-02-29 | Updated: 2016-03-03

Nival(nival.com)
In February 2016, the Russian gaming company Nival was the target of an attack which was consequently detailed on Reddit. Allegedly protesting "the foreign policy of Russia in regards to Ukraine", Nival was one of several Russian sites in the breach and impacted over 1.5M accounts including sensitive personal information.

Count: 1535473 | Created: 2016-02-29 | Updated: 2016-03-03

SkTorrent(sktorrent.eu)
In February 2016, the Slovak torrent tracking site SkTorrent was hacked and over 117k records leaked online. The data dump included usernames, email addresses and passwords stored in plain text.

Count: 117070 | Created: 2016-02-19 | Updated: 2016-02-23

R2Games(r2games.com)
In late 2015, the gaming website R2Games was hacked and more than 2.1M personal records disclosed. The vBulletin forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked. A further 11M accounts were added to "Have I Been Pwned" in March 2016 and another 9M in July 2016 bringing the total to over 22M.

Count: 22281337 | Created: 2015-11-01 | Updated: 2016-02-09

Comcast(comcast.net)
In November 2015, the US internet and cable TV provider Comcast suffered a data breach

Seedpeer(seedpeer.eu)
In July 2015, the torrent site Seedpeer was hacked and 282k member records were exposed. The data included usernames, email addresses and passwords stored as weak MD5 hashes.

Count: 281924 | Created: 2015-07-12 | Updated: 2016-03-09

Sumo Torrent(sumotorrent.sx)
In June 2014, the torrent site Sumo Torrent was hacked and 285k member records were exposed. The data included IP addresses, email addresses and passwords stored as weak MD5 hashes.

Count: 285191 | Created: 2014-06-21 | Updated: 2016-03-09

Acne.org(acne.org)
In November 2014, the acne website acne.org suffered a data breach that exposed over 430k forum members' accounts. The data was being actively traded on underground forums and included email addresses, birth dates and passwords.

Count: 432943 | Created: 2014-11-25 | Updated: 2016-03-06

MajorGeeks(majorgeeks.com)
In November 2015, almost 270k accounts from the MajorGeeks support forum were breached. The accounts were being actively sold and traded online and included email addresses, salted password hashes and IP addresses.

Count: 269548 | Created: 2015-11-15 | Updated: 2016-03-03

iPmart(ipmart-forum.com)
During 2015, the iPmart forum (now known as Mobi NUKE) was hacked and over 2 million forum members' details were exposed. The vBulletin forum included IP addresses, birth dates and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked. A further 368k accounts were added to "Have I Been Pwned" in March 2016 bringing the total to over 2.4M.

Count: 2460787 | Created: 2015-07-01 | Updated: 2016-02-23

Linux Mint(linuxmint.com)
In February 2016, the website for the Linux distro known as Linux Mint was hacked and the ISO infected with a backdoor. The site also ran a phpBB forum which was subsequently put up for sale complete with almost 145k email addresses, passwords and other personal subscriber information.

Count: 144989 | Created: 2016-02-21 | Updated: 2016-02-22

Plex(plex.tv)
In July 2015, the discussion forum for Plex media centre was hacked and over 327k accounts exposed. The IP.Board forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

Count: 327314 | Created: 2015-07-02 | Updated: 2016-02-08

PS3Hax(ps3hax.net)

that exposed 590k customer email addresses and plain text passwords. A further 27k accounts appeared with home addresses with the entire data set being sold on underground forums.

Count: 616882 | Created: 2015-11-08 | Updated: 2016-02-08

PSX-Scene(psx-scene.com)
In approximately February 2015, the Sony Playstation forum known as PSX-Scene was hacked and more than 340k accounts were exposed. The vBulletin forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

Count: 341118 | Created: 2015-02-01 | Updated: 2016-02-07

OwnedCore(OwnedCore.com)
In approximately August 2013, the World of Warcraft exploits forum known as OwnedCore was hacked and more than 880k accounts were exposed. The vBulletin forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

Count: 880331 | Created: 2013-08-01 | Updated: 2016-02-06

Heroes of Newerth(heroesofnewerth.com)
In December 2012, the multiplayer online battle arena game known as Heroes of Newerth was hacked and over 8 million accounts extracted from the system. The compromised data included usernames, email addresses and passwords.

Count: 8089103 | Created: 2012-12-17 | Updated: 2016-01-24

Gamigo(gamigo.com)
In March 2012, the German online game publisher Gamigo was hacked and more than 8 million accounts publicly leaked. The breach included email addresses and passwords stored as weak MD5 hashes with no salt.

Count: 8243604 | Created: 2012-03-01 | Updated: 2016-01-18

Money Bookers(moneybookers.com)
Sometime in 2009, the e-wallet service known as Money Bookers suffered a data breach which exposed almost 4.5M customers. Now called Skrill, the breach was not discovered until October 2015 and included names, email addresses, home addresses and IP addresses.

Count: 4483605 | Created: 2009-01-01 | Updated: 2015-11-30

VTech(vtechda.com)
In November 2015, hackers extracted more than 4.8 million parents' and 227k children's accounts from VTech's Learning Lodge website. The Hong Kong company produces learning products for children including software sold via the compromised website. The data breach exposed extensive personal details including home addresses, security questions and answers and passwords stored as weak MD5 hashes. Furthermore, children's details including names, ages, genders and associations to their parents' records were also exposed.

Count: 4833678 | Created: 2015-11-13 | Updated: 2015-11-25

Black Hat World(blackhatworld.com)
In June 2014, the search engine optimisation forum Black Hat World had three quarters of a million accounts breached from their system. The breach included various personally identifiable attributes which were publicly released in a MySQL database script.

In approximately July 2015, the Sony Playstation hacks and mods forum known as PS3Hax was hacked and more than 447k accounts were exposed. The vBulletin forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

Count: 447410 | Created: 2015-07-01 | Updated: 2016-02-07

Xbox-Scene(xboxscene.com)
In approximately February 2015, the Xbox forum known as Xbox-Scene was hacked and more than 432k accounts were exposed. The IP.Board forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

Count: 432552 | Created: 2015-02-01 | Updated: 2016-02-07

Gamerzplanet(gamerzplanet.net)
In approximately October 2015, the online gaming forum known as Gamerzplanet was hacked and more than 1.2M accounts were exposed. The vBulletin forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

Count: 1217166 | Created: 2015-10-23 | Updated: 2016-02-05

vBulletin(vbulletin.com)
In November 2015, the forum software maker vBulletin suffered a serious data breach. The attack lead to the release of both forum user and customer accounts totalling almost 519k records. The breach included email addresses, birth dates, security questions and answers for customers and salted hashes of passwords for both sources.

Count: 518966 | Created: 2015-11-03 | Updated: 2016-01-24

Nexus Mods(nexusmods.com)
In December 2015, the game modding site Nexus Mods released a statement notifying users that they had been hacked. They subsequently dated the hack as having occurred in July 2013 although there is evidence to suggest the data was being traded months in advance of that. The breach contained usernames, email addresses and passwords stored as a salted hashes.

Count: 5915013 | Created: 2013-07-22 | Updated: 2016-01-17

Neteller(neteller.com)
In May 2010, the e-wallet service known as Neteller suffered a data breach which exposed over 3.6M customers. The breach was not discovered until October 2015 and included names, email addresses, home addresses and account balances.

Count: 3619948 | Created: 2010-05-17 | Updated: 2015-11-30

Foxy Bingo(foxybingo.com)
In April 2007, the online gambling site Foxy Bingo was hacked and 252,000 accounts were obtained by the hackers. The breached records were subsequently sold and traded and included personal information data such as plain text passwords, birth dates and home addresses.

Count: 252216 | Created: 2008-04-04 | Updated: 2015-11-22

Final Fantasy Shrine(ffshrine.org)
In September 2015, the Final Fantasy discussion forum known as FFShrine was breached and the data dumped publicly. Approximately 620k records were released containing email addresses, IP addresses and salted hashes of passwords.

Count: 777387 | Created: 2014-06-23 | Updated: 2015-11-03

Mac-Torrents(mac-torrents.com)
In October 2015, the torrent site Mac-Torrents was hacked and almost 94k usernames, email addresses and passwords were leaked. The passwords were hashed with MD5 and no salt.

Count: 93992 | Created: 2015-10-31 | Updated: 2015-10-31

MPGH(mpgh.net)
In October 2015, the multiplayer game hacking website MPGH was hacked and 3.1 million user accounts disclosed. The vBulletin forum breach contained usernames, email addresses, IP addresses and salted hashes of passwords.

Count: 3122898 | Created: 2015-10-22 | Updated: 2015-10-26

MyVidster(myvidster.com)
In August 2015, the social video sharing and bookmarking site MyVidster was hacked and nearly 20,000 accounts were dumped online. The dump included usernames, email addresses and hashed passwords.

Count: 19863 | Created: 2015-08-15 | Updated: 2015-10-10

XSplit(xsplit.com)
In November 2013, the makers of gaming live streaming and recording software XSplit was compromised in an online attack. The data breach leaked almost 3M names, email addresses, usernames and hashed passwords.

Count: 2983472 | Created: 2013-11-07 | Updated: 2015-08-08

Hemmakvall(hemmakvall.se)
In July 2015, the Swedish video store chain Hemmakvxc3xa4ll was hacked and nearly 50k records dumped publicly. The disclosed data included various attributes of their customers including email and physical addresses, names and phone numbers. Passwords were also leaked, stored with a weak MD5 hashing algorithm.

Count: 47297 | Created: 2015-07-08 | Updated: 2015-07-09

Minecraft Pocket Edition Forum(minecraftpeforum.net)
In May 2015, the Minecraft Pocket Edition forum was hacked and over 16k accounts were dumped public. Allegedly hacked by @rmsg0d, the forum data included numerous personal pieces of data for each user. The forum has subsequently been decommissioned.

Count: 16034 | Created: 2015-05-24 | Updated: 2015-06-30

mSpy(mspy.com)
In May 2015, the "monitoring" software known as mSpy suffered a major data breach. The software (allegedly often used to spy on unsuspecting victims), stored extensive personal information within their online service which after being breached, was made freely available on the internet.

Count: 699793 | Created: 2015-05-14 | Updated: 2015-05-28

Telecom Regulatory Authority of India(trai.gov.in)
In April 2015, the Telecom Regulatory Authority of India (TRAI) published tens of thousand of emails sent by Indian citizens supporting net neutrality as part of the SaveTheInternet campaign. The published data included lists of emails including the sender's name and email address as well as the contents

Count: 620677 | Created: 2015-09-18 | Updated: 2015-10-31

PHP Freaks(phpfreaks.com)
In October 2015, the PHP discussion board PHP Freaks was hacked and 173k user accounts were publicly leaked. The breach included multiple personal data attributes as well as salted and hashed passwords.

Count: 173891 | Created: 2015-10-27 | Updated: 2015-10-30

Paddy Power(paddypower.com)
In October 2010, the Irish bookmaker Paddy Power suffered a data breach that exposed 750,000 customer records with nearly 600,000 unique email addresses. The breach was not disclosed until July 2014 and contained extensive personal information including names, addresses, phone numbers and plain text security questions and answers.

Count: 590954 | Created: 2010-10-25 | Updated: 2015-10-11

Ashley Madison(ashleymadison.com)
In July 2015, the infidelity website Ashley Madison suffered a serious data breach. The attackers threatened Ashley Madison with the full disclosure of the breach unless the service was shut down. One month later, the database was dumped including more than 30M unique email addresses. This breach has been classed as "sensitive" and is not publicly searchable, although individuals may discover if they've been impacted by registering for notifications. Read about this approach in detail.

Count: 30811934 | Created: 2015-07-19 | Updated: 2015-08-18

Hacking Team(hackingteam.com)
In July 2015, the Italian security firm Hacking Team suffered a major data breach that resulted in over 400GB of their data being posted online via a torrent. The data searchable on "Have I Been Pwned?" is from 189GB worth of PST mail folders in the dump. The contents of the PST files is searchable on Wikileaks.

Count: 32310 | Created: 2015-07-06 | Updated: 2015-07-12

myRepoSpace(myrepospace.com)
In July 2015, the Cydia repository known as myRepoSpace was hacked and user data leaked publicly. Cydia is designed to facilitate the installation of apps on jailbroken iOS devices. The repository service was allegedly hacked by @its_not_herpes and 0x8badfl00d in retaliation for the service refusing to remove pirated tweaks.

Count: 252751 | Created: 2015-07-06 | Updated: 2015-07-08

NextGenUpdate(nextgenupdate.com)
Early in 2014, the video game website NextGenUpdate reportedly suffered a data breach that disclosed almost 1.2 million accounts. Amongst the data breach was usernames, email addresses, IP addresses and salted and hashed passwords.

Count: 1194597 | Created: 2014-04-22 | Updated: 2015-06-05

SprashivaiRu(sprashivai.ru)
In May 2015, xd0xa1xd0xbfxd1x80xd0xb0xd1x88xd0xb8xd0xb2xd0xb0xd0xb9.xd1x80xd1x83 (a the Russian website for anonymous reviews) was reported to have had 6.7 million user details exposed by a hacker known as "w0rm". Intended to be a site for expressing anonymous opinions, the leaked data included email addresses, birth dates and other personally identifiable data about almost 3.5 million unique email addresses found in the leak.

Count: 3474763 | Created: 2015-05-11 | Updated: 2015-05-12

StarNet(starnet.md)
In February 2015, the Moldavian ISP "StarNet" had it's database published online. The dump included nearly 140k email addresses, many with personal details including contact information, usage patterns of the ISP and even passport numbers.

of the email as well, often with signatures including other personal data.

Count: 107776 | Created: 2015-04-27 | Updated: 2015-04-27

Quantum Booter(quantumbooter.net)
In March 2014, the booter service Quantum Booter (also referred to as Quantum Stresser) suffered a breach which lead to the disclosure of their internal database. The leaked data included private discussions relating to malicious activity Quantum Booter users were performing against online adversaries, including the IP addresses of those using the service to mount DDoS attacks.

Count: 48592 | Created: 2014-03-18 | Updated: 2015-04-04

Flashback(flashback.se)
In February 2015, the Swedish forum known as Flashback had sensitive internal data on 40k members published via the tabloid newspaper Aftonbladet. The data was allegedly sold to them via Researchgruppen (The Research Group) who have a history of exposing otherwise anonymous users, primarily those who they believe participate in "troll like" behaviour. The compromised data includes social security numbers, home and email addresses.

Count: 40256 | Created: 2015-02-11 | Updated: 2015-02-12

Lizard Squad(lizardstresser.su)
In January 2015, the hacker collective known as "Lizard Squad" created a DDoS service by the name of "Lizard Stresser" which could be procured to mount attacks against online targets. Shortly thereafter, the service suffered a data breach which resulted in the public disclosure of over 13k user accounts including passwords stored in plain text.

Count: 13451 | Created: 2015-01-16 | Updated: 2015-01-18

AhaShare.com(ahashare.com)
In May 2013, the torrent site AhaShare.com suffered a breach which resulted in more than 180k user accounts being published publicly. The breach included a raft of personal information on registered users plus despite assertions of not distributing personally identifiable information, the site also leaked the IP addresses used by the registered identities.

Count: 180468 | Created: 2013-05-30 | Updated: 2014-11-06

Bitcoin Security Forum Gmail Dump(forum.btcsec.com)
In September 2014, a large dump of nearly 5M usernames and passwords was posted to a Russian Bitcoin forum. Whilst commonly reported as 5M "Gmail passwords", the dump also contained 123k yandex.ru addresses. Whilst the origin of the breach remains unclear, the breached credentials were confirmed by multiple source as correct, albeit a number of years old.

Count: 4789599 | Created: 2014-01-09 | Updated: 2014-09-10

Insanelyi(insanelyi.com)
In July 2014, the iOS forum Insanelyi was hacked by an attacker known as Kim Jong-Cracks. A popular source of information for users of jailbroken iOS devices running Cydia, the Insanelyi breach disclosed over 104k users' emails addresses, user names and weakly hashed passwords (salted MD5).

Count: 104097 | Created: 2014-07-22 | Updated: 2014-07-22

Count: 139395 | Created: 2015-02-26 | Updated: 2015-04-11

ThisHabbo Forum(thishabboforum.com)
In 2014, the ThisHabbo forum (a fan site for Habbo.com, a Finnish social networking site) appeared among a list of compromised sites which has subsequently been removed from the internet. Whilst the actual date of the exploit is not clear, the breached data includes usernames, email addresses, IP addresses and salted hashes of passwords. A further 584k records were added from a more comprehensive breach file provided in October 2016.

Count: 612414 | Created: 2014-01-01 | Updated: 2015-03-28

Crack Community(crackcommunity.com)
In late 2013, the Crack Community forum specialising in cracks for games was compromised and over 19k accounts published online. Built on the MyBB forum platform, the compromised data included email addresses, IP addresses and salted MD5 passwords.

Count: 19210 | Created: 2013-09-09 | Updated: 2015-02-03

Dominos(pizza.dominos.be)
In June 2014, Domino's Pizza in France and Belgium was hacked by a group going by the name "Rex Mundi" and their customer data held to ransom. Domino's refused to pay the ransom and six months later, the attackers released the data along with troves of other hacked accounts. Amongst the customer data was passwords stored with a weak MD5 hashing algorithm and no salt.

Count: 648231 | Created: 2014-06-13 | Updated: 2015-01-04

Yandex Dump(forum.btcsec.com)
In September 2014, news broke of a massive leak of accounts from Yandex, the Russian search engine giants who also provides email services. The purported million "breached" accounts were disclosed at the same time as nearly 5M mail.ru accounts with both companies claiming the credentials were acquired via phishing scams rather than being obtained as a result of direct attacks against their services.

Count: 1186564 | Created: 2014-09-07 | Updated: 2014-09-12

PokemonCreed(pokemoncreed.net)
In August 2014, the Pokxc3xa9mon RPG website Pokxc3xa9mon Creed was hacked after a dispute with rival site, Pokxc3xa9mon Dusk. In a post on Facebook, "Cruz Dusk" announced the hack then pasted the dumped MySQL database on pkmndusk.in. The breached data included over 116k usernames, email addresses and plain text passwords.

Count: 116465 | Created: 2014-08-08 | Updated: 2014-08-10

Astropid(astropid.com)
In December 2013, the vBulletin forum for the social engineering site known as "AstroPID" was breached and leaked publicly. The site provided tips on fraudulently obtaining goods and services, often by providing a legitimate "PID" or Product Information Description. The breach resulted in nearly 6k user accounts and over 220k private messages between forum members being exposed.

Count: 5788 | Created: 2013-12-19 | Updated: 2014-07-06

Lounge Board(loungeboard.net)
At some point in 2013, 45k accounts were breached from the Lounge Board "General Discussion Forum" and then dumped publicly. Lounge Board was a MyBB forum launched in 2012 and discontinued in mid 2013 (the last activity in the logs was from August 2013).

Count: 45018 | Created: 2013-08-01 | Updated: 2014-07-06

Verified(verified.cm)
In January 2014, one of the largest communities of Eastern Europe cybercriminals known as "Verified" was hacked. The breach exposed nearly 17k users of the vBulletin forum including their personal messages and other potentially personally identifiable information.

Count: 16919 | Created: 2014-01-10 | Updated: 2014-07-06

Win7Vista Forum(win7vista.com)
In September 2013, the Win7Vista Windows forum (since renamed to the "Beyond Windows 9" forum) was hacked and later had its internal database dumped. The dump included over 200k membersxe2x80x99 personal information and other internal data extracted from the forum.

Count: 202683 | Created: 2013-09-03 | Updated: 2014-06-01

Cannabis.com(cannabis.com)
In February 2014, the vBulletin forum for the Marijuana site cannabis.com was breached and leaked publicly. Whilst there has been no public attribution of the breach, the leaked data included over 227k accounts and nearly 10k private messages between users of the forum.

Count: 227746 | Created: 2014-02-05 | Updated: 2014-06-01

Business Acumen Magazine(businessacumen.biz)
In April 2014, the Australian "Business Acumen Magazine" website was hacked by an attacker known as 1337MiR. The breach resulted in over 26,000 accounts being exposed including usernames, email addresses and password stored with a weak cryptographic hashing algorithm (MD5 with no salt).

Count: 26596 | Created: 2014-04-25 | Updated: 2014-05-11

hackforums.net(hackforums.net)
In June 2011, the hacktivist group known as "LulzSec" leaked one final large data breach they titled "50 days of lulz". The compromised data came from sources such as AT&T, Battlefield Heroes and the hackforums.net website. The leaked Hack Forums data included credentials and personal information of nearly 200,000 registered forum users.

Count: 191540 | Created: 2011-06-25 | Updated: 2014-05-11

Fridae(fridae.asia)
In May 2014, over 25,000 user accounts were breached from the Asian lesbian, gay, bisexual and transgender website known as "Fridae". The attack which was announced on Twitter appears to have been orchestrated by Deletesec who claim that "Digital weapons shall annihilate all secrecy within governments and corporations". The exposed data included password stored in plain text.

Count: 35368 | Created: 2014-05-02 | Updated: 2014-05-06

BigMoneyJobs(bigmoneyjobs.com)
In April 2014, the job site bigmoneyjobs.com was hacked by an attacker known as "ProbablyOnion". The attack resulted in the exposure of over 36,000 user accounts including email addresses, usernames and passwords which were stored in plain text. The attack was allegedly mounted by exploiting a SQL injection vulnerability.

Count: 36789 | Created: 2014-04-03 | Updated: 2014-04-08

Boxee(forums.boxee.com)
In March 2014, the home theatre PC software maker Boxee had their forums compromised in an attack. The attackers obtained the entire vBulletin MySQL database and promptly posted it for download on the Boxee forum itself. The data included 160k users, password histories, private messages and a variety of other data exposed across nearly 200 publicly exposed tables.

Count: 158093 | Created: 2014-03-29 | Updated: 2014-03-30

hemmelig.com(hemmelig.com)
In December 2011, Norway's largest online sex shop hemmelig.com was hacked by a collective calling themselves "Team Appunity". The attack exposed over 28,000 usernames and email addresses along with nicknames, gender, year of birth and unsalted MD5 password hashes.

Count: 28641 | Created: 2011-12-21 | Updated: 2014-03-25

UN Internet Governance Forum(intgovforum.org)
In February 2014, the Internet Governance Forum (formed by the United Nations for policy dialogue on issues of internet governance) was attacked by hacker collective known as Deletesec. Although tasked with "ensuring the security and stability of the Internet", the IGFxe2x80x99s website was still breached and resulted in the leak of 3,200 email addresses, names, usernames and cryptographically stored passwords.

Count: 3200 | Created: 2014-02-20 | Updated: 2014-02-23

Muslim Directory(muslimdirectory.co.uk)
In February 2014, the UK guide to services and business known as the Muslim Directory was attacked by the hacker known as @th3inf1d3l. The data was consequently dumped publicly and included the web accounts of tens of thousands of users which contained data including their names, home address, age group, email, website activity and password in plain text.

Count: 37784 | Created: 2014-02-17 | Updated: 2014-02-23

Spirol(spirol.com)
In February 2014, Connecticut based Spirol Fastening Solutions suffered a data breach that exposed over 70,000 customer records. The attack was allegedly mounted by exploiting a SQL injection vulnerability which yielded data from Spirolxe2x80x99s CRM system ranging from customersxe2x80x99 names, companies, contact information and over 55,000 unique email addresses.

Forbes(forbes.com)
In February 2014, the Forbes website succumbed to an attack that leaked over 1 million user accounts. The attack was attributed to the Syrian Electronic Army, allegedly as retribution for a perceived "Hate of Syria". The attack not only leaked user credentials, but also resulted in the posting of fake news stories to forbes.com.

Count: 1057819 | Created: 2014-02-15 | Updated: 2014-02-15

Count: 55622 | Created: 2014-02-22 | Updated: 2014-02-22

Tesco(tesco.com)
In February 2014, over 2,000 Tesco accounts with usernames, passwords and loyalty card balances appeared on Pastebin. Whilst the source of the breach is not clear, many confirmed the credentials were valid for Tesco and indeed they have a history of poor online security.

Count: 2239 | Created: 2014-02-12 | Updated: 2014-02-13

Bell (2014 breach)(bell.ca)
In February 2014, Bell Canada suffered a data breach via the hacker collective known as NullCrew. The breach included data from multiple locations within Bell and exposed email addresses, usernames, user preferences and a number of unencrypted passwords and credit card data from 40,000 records containing just over 20,000 unique email addresses and usernames.

Count: 20902 | Created: 2014-02-01 | Updated: 2014-02-01

Snapchat(snapchat.com)
In January 2014 just one week after Gibson Security detailed vulnerabilities in the service, Snapchat had 4.6 million usernames and phone number exposed. The attack involved brute force enumeration of a large number of phone numbers against the Snapchat API in what appears to be a response to Snapchat's assertion that such an attack was "theoretical". Consequently, the breach enabled individual usernames (which are often used across other services) to be resolved to phone numbers which users usually wish to keep private.

Count: 4609615 | Created: 2014-01-01 | Updated: 2014-01-02

Adobe(adobe.com)
In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Count: 152445165 | Created: 2013-10-04 | Updated: 2013-12-04

Sony(sony.com)
In 2011, Sony suffered breach after breach after breach — it was a *very* bad year for them. The breaches spanned various areas of the business ranging from the PlayStation network all the way through to the motion picture arm, Sony Pictures. A SQL Injection vulnerability in sonypictures.com lead to tens of thousands of accounts across multiple systems being exposed complete with plain text passwords.

Count: 37103 | Created: 2011-06-02 | Updated: 2013-12-04

Yahoo(yahoo.com)
In July 2012, Yahoo! had their online publishing service "Voices" compromised via a SQL injection attack. The breach resulted in the disclosure of nearly half a million usernames and passwords stored in plain text. The breach showed that of the compromised accounts, a staggering 59% of people who also had accounts in the Sony breach reused their passwords across both services.

Count: 453427 | Created: 2012-07-11 | Updated: 2013-12-04

WPT Amateur Poker League(wptapl.com)
In January 2014, the World Poker Tour (WPT) Amateur Poker League website was hacked by the Twitter user @smitt3nz. The attack resulted in the public disclosure of 175,000 accounts including 148,000 email addresses. The plain text password for each account was also included in the breach.

Count: 148366 | Created: 2014-01-04 | Updated: 2014-02-01

Battlefield Heroes(battlefieldheroes.com)
In June 2011 as part of a final breached data dump, the hacker collective "LulzSec" obtained and released over half a million usernames and passwords from the game Battlefield Heroes. The passwords were stored as MD5 hashes with no salt and many were easily converted back to their plain text versions.

Count: 530270 | Created: 2011-06-26 | Updated: 2014-01-23

Pixel Federation(pixelfederation.com)
In December 2013, a breach of the web-based game community based in Slovakia exposed over 38,000 accounts which were promptly posted online. The breach included email addresses and unsalted MD5 hashed passwords, many of which were easily converted back to plain text.

Count: 38108 | Created: 2013-12-04 | Updated: 2013-12-06

Gawker(gawker.com)
In December 2010, Gawker was attacked by the hacker collective "Gnosis" in retaliation for what was reported to be a feud between Gawker and 4Chan. Information about Gawkers 1.3M users was published along with the data from Gawker's other web presences including Gizmodo and Lifehacker. Due to the prevalence of password reuse, many victims of the breach then had their Twitter accounts compromised to send Acai berry spam.

Count: 1247574 | Created: 2010-12-11 | Updated: 2013-12-04

Stratfor(stratfor.com)
In December 2011, "Anonymous" attacked the global intelligence company known as "Stratfor" and consequently disclosed a veritable treasure trove of data including hundreds of gigabytes of email and tens of thousands of credit card details which were promptly used by the attackers to make charitable donations (among other uses). The breach also included 860,000 user accounts complete with email address, time zone, some internal system data and MD5 hashed passwords with no salt.

Count: 859777 | Created: 2011-12-24 | Updated: 2013-12-04

Hot topics

The war on information

Russia ran a massive DDOS attack against Ukrainian government websites the day before the military action. Russia has at least 3 departments within the GRU, Russia's intelligence service, specialized in cyberattacks. What are the risks for the rest of the world?
- Russia cyber-attacking directly.
- 20% of the US Fortune 500 companies use Ukrainian contractors, services or products. If compromised, this could be used to access many customer systems.

The Anonymous group anounced that is was "officially in cyber war against the Russian government". Since Thursday, they:
- Took down several Russian government websites.
- Leaked the database of Russian Ministry of Defense website.
- Intercepted military communications.
- Hacked Russian state TV channels to broadcast information regarding Ukraine. You can watch an impressive demo on Twitter: https://twitter.com/YourAnonOne/status/1497682868985905154

--
JL Dupont

Source: SpamHaus

Top phishing countries

#1 United States	#2 Hong Kong
#3 Germany	#4 Canada
#5 Russia	#6 Japan
#7 Singapore	#8 Netherlands
#9 Bulgaria	#10 France