



















































































































Pwned websites











































Breached websites that have been loaded into this service










































Here's an overview of the various breaches that have been consolidated into this site. Each of these has been dumped publicly and is readily available via various sites on the web. This information is also [available via an RSS feed \(https://feeds.feedburner.com/HaveIBeenPwnedLatestBreaches\)](https://feeds.feedburner.com/HaveIBeenPwnedLatestBreaches).



















	593,427,119	Exploit.In accounts ⓘ
	457,962,538	Anti Public Combo List accounts ⓘ
	393,430,309	River City Media Spam List accounts 
	359,420,698	MySpace accounts
	234,842,089	NetEase accounts ⓘ
	164,611,595	LinkedIn accounts
	152,445,165	Adobe accounts
	112,005,531	Badoo accounts  ⓘ
	93,338,602	VK accounts
	91,890,110	Youku accounts
	91,436,280	Rambler accounts
	68,648,009	Dropbox accounts
	65,469,298	tumblr accounts
	58,843,488	Modern Business Solutions accounts
	52,578,183	Zoosk accounts  
	49,467,477	iMesh accounts
	40,767,652	Fling accounts 
	37,217,682	Last.fm accounts
	33,698,126	NetProspex accounts 
	32,939,105	SC Daily Phone Spam List accounts 
	30,811,934	Ashley Madison accounts 
	30,741,620	Special K Data Feed Spam List accounts 
	29,396,116	Evony accounts
	29,020,808	Tianya accounts
	27,393,015	Mate1.com accounts 
	26,892,897	Neopets accounts
	26,183,992	QIP accounts
	24,451,312	Justdate.com accounts  
	22,526,334	GFAN accounts ⓘ
	22,281,337	R2Games accounts
	21,149,008	Taobao accounts ⓘ
	13,545,468	000webhost accounts
	12,865,609	Cross Fire accounts

	8,718,404 Dodonew.com accounts ?
	8,243,604 Gamigo accounts
	8,089,103 Heroes of Newerth accounts
	7,830,195 Civil Online accounts ?
	7,485,802 uuu9 accounts ?
	7,196,890 Experian accounts ?
	7,089,395 Lifeboat accounts
	6,496,778 Aipai.com accounts ?
	6,414,191 126 accounts ?
	5,968,783 xat accounts
	5,915,013 Nexus Mods accounts
	5,081,689 Leet accounts
	4,946,850 Папа Па accounts
	4,907,802 QuinStreet accounts
	4,833,678 VTech accounts
	4,821,262 mail.ru Dump accounts
	4,789,599 Bitcoin Security Forum
	Gmail Dump accounts
	4,609,615 Snapchat accounts
	4,483,605 Money Bookers accounts
	4,009,640 17 accounts
	3,867,997 Adult Friend Finder accounts
	3,827,238 Trillian accounts
	3,619,948 Neteller accounts
	3,474,763 Спрашивай.ру accounts
	3,439,414 InterPals accounts
	3,264,710 DLH.net accounts
	3,122,898 MPGH accounts
	2,983,472 XSplit accounts
	2,682,650 Uiggy accounts
	2,639,894 Duowan.com accounts ?
	2,491,103 Funimation accounts
	2,460,787 iPmart accounts
	2,424,784 ClixSense accounts
	2,357,872 FashionFantasyGame accounts
	2,330,382 Patreon accounts
	2,247,314 Wishbone accounts
	2,231,256 Bell (2017 breach) accounts
	2,191,565 i-Dressup accounts
	2,136,520 gPotato accounts
	2,064,274 GameTuts accounts
	1,871,373 CD Projekt RED accounts
	1,771,845 Flash Flash Revolution accounts

	1,697,282 Nihonomaru accounts
	1,619,544 Ster-Kinekor accounts
	1,580,933 Dungeons & Dragons Online accounts
	1,535,473 Nival accounts
	1,531,235 Army Force Online accounts
	1,476,783 KM.RU accounts
	1,436,486 Aternos accounts
	1,398,630 Naughty America accounts
	1,370,175 Eroticy accounts  
	1,327,567 YouPorn accounts 
	1,296,959 Xbox 360 ISO accounts
	1,291,178 Elance accounts
	1,274,070 PSP ISO accounts
	1,270,564 Fur Affinity accounts 
	1,247,574 Gawker accounts
	1,217,166 Gamerzplanet accounts
	1,194,597 NextGenUpdate accounts
	1,186,564 Yandex Dump accounts
	1,141,278 Lord of the Rings Online accounts
	1,131,636 DaniWeb accounts
	1,100,089 Beautiful People accounts 
	1,074,948 Lookbook accounts
	1,073,164 GeekedIn accounts
	1,057,819 Forbes accounts
	1,023,466 R2 (2017 forum breach) accounts
	1,020,136 War Inc. accounts
	999,991 HongFire accounts 
	995,698 Little Monsters accounts
	942,044 CrimeAgency vBulletin Hacks accounts 
	880,331 OwnedCore accounts
	879,703 MoDaCo accounts
	859,777 Stratfor accounts
	855,249 Manga Traders accounts
	830,155 Pokémon Negro accounts
	819,478 Warframe accounts
	800,157 Onverse accounts
	790,724 Brazzers accounts 
	777,387 Black Hat World accounts
	745,355 Android Forums accounts
	738,556 WildStar accounts
	488,782 mSpyn accounts


	Have I been pwned? Pwned websites
	577,173 Pokébip accounts
	657,001 Pokébip accounts
	648,231 Domino's accounts
	637,340 DaFont accounts
	620,677 Final Fantasy Shrine accounts
	616,882 Comcast accounts
	612,414 ThisHabbo Forum accounts
	611,070 HLTV accounts
	599,080 Nulled accounts
	590,954 Paddy Power accounts
	583,503 CloudPets accounts
	568,340 BTC-E accounts
	530,270 Battlefield Heroes accounts
	530,147 Unreal Engine accounts
	518,966 vBulletin accounts
	504,565 Kimsufi accounts
	501,407 Bitcoin Talk accounts
	458,155 WiiU ISO accounts
	453,427 Yahoo accounts
	452,899 OVH accounts
	447,410 PS3Hax accounts
	444,767 CheapAssGamer.com accounts
	442,166 Team SoloMid accounts
	432,943 Acne.org accounts
	432,552 Xbox-Scene accounts
	422,959 Avast accounts
	400,260 PayAsUGym accounts
	395,044 uTorrent accounts
	380,830 Freedom Hosting II accounts
	366,140 MrExcel accounts
	352,120 Torrent Invites accounts
	341,118 PSX-Scene accounts
	327,314 Plex accounts
	321,920 Health Now Networks accounts
	285,191 Sumo Torrent accounts
	281,924 Seedpeer accounts
	269,548 MajorGeeks accounts
	254,867 SweClockers.com accounts
	252,751 myRepoSpace accounts
	252,216 Foxy Bingo accounts
	251,661 Epic Games accounts
	238,373 Bot of Legends accounts

	228,605 COMELEC (Philippines Voters) accounts
	227,746 Cannabis.com accounts
	202,683 Win7Vista Forum accounts
	197,184 GTAGaming accounts
	191,540 hackforums.net accounts
	188,343 Minefield accounts
	180,468 AhaShare.com accounts
	179,967 Heroes of Gaia accounts
	179,030 The Fappening accounts 
	178,201 The Candid Board accounts 
	173,891 PHP Freaks accounts
	158,093 Boxee accounts
	149,830 Muslim Match accounts 
	148,366 WPT Amateur Poker League accounts
	144,989 Linux Mint accounts
	139,395 StarNet accounts
	134,047 WHMCS accounts
	130,705 Soundwave accounts
	117,070 SkTorrent accounts
	116,465 Pokémon Creed accounts
	111,623 Malwarebytes accounts
	107,776 Telecom Regulatory Authority of India accounts
	107,303 Rosebutt Board accounts 
	104,977 Regpack accounts
	104,097 Insanelyi accounts
	97,151 Teracod accounts
	93,992 Mac-Torrents accounts
	88,678 Qatar National Bank accounts
	83,957 TruckersMP accounts
	81,830 eThekweni Municipality accounts
	75,383 Non Nude Girls accounts 
	73,587 ServerPact accounts
	71,153 Retina-X accounts
	71,081 Minecraft World Map accounts
	56,021 Vodafone accounts
	55,622 Spirol accounts
	48,592 Quantum Booter accounts
	47,297 Hemmakväll accounts
	45,018 Lounge Board accounts

	Have I been pwned? Pwned websites
	40,256 Flashback accounts
	38,108 Pixel Federation accounts
	37,784 Muslim Directory accounts
	37,103 Sony accounts
	36,789 BigMoneyJobs accounts
	35,368 Fridae accounts 
	34,235 BitTorrent accounts
	32,310 Hacking Team accounts
	28,641 hemmelig.com accounts
	26,596 Business Acumen Magazine accounts
	20,902 Bell (2014 breach) accounts
	19,863 MyVidster accounts
	19,210 Crack Community accounts
	16,919 Verified accounts
	16,431 Ethereum accounts
	16,034 Minecraft Pocket Edition Forum accounts
	13,451 Lizard Squad accounts
	5,788 Astropid accounts
	3,200 UN Internet Governance Forum accounts
	2,239 Tesco accounts

 Sensitive breach (/FAQs#SensitiveBreach), not publicly searchable

 Retired breach (/FAQs#RetiredBreach), removed from system

 Unverified breach (/FAQs#UnverifiedBreach), may be sourced from elsewhere

 Fabricated breach (/FAQs#FabricatedBreach), likely not legitimate

 Spam List (/FAQs#SpamList), used for spam marketing



000webhost

In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach (<http://www.troyhunt.com/2015/10/breaches-traders-plain-text-passwords.html>) that exposed over 13 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.

Compromised data: Email addresses, IP addresses, Names, Passwords

126

126

In approximately 2012, it's alleged that the Chinese email service known as 126 (<http://126.com>) 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. (<https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/>)

Compromised data: Email addresses, Passwords

17

In April 2016, customer data obtained from the streaming app known as "17" appeared listed for sale on a Tor hidden service marketplace (<https://motherboard.vice.com/read/another-day-another-hack-millions-of-user-accounts-for-streaming-app-17>). The data contained over 4 million unique email addresses along with IP addresses, usernames and passwords stored as unsalted MD5 hashes.

Compromised data: Device information, Email addresses, IP addresses, Passwords, Usernames



Acne.org

In November 2014, the acne website [acne.org](http://www.acne.org/) (<http://www.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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames



Adobe

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 (<http://stricture-group.com/files/adobe-top100.txt>). The unencrypted hints also disclosed much about the passwords (<http://www.troyhunt.com/2013/11/adobe-credentials-and-serious.html>) adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Adult Friend Finder

Adult Friend Finder

In May 2015, the adult hookup site Adult Friend Finder was hacked (<http://www.bbc.com/news/business-32839196>) 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.

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Races, Relationship statuses, Sexual orientations, Spoken languages, Usernames

AhaShare.com

AhaShare.com

In May 2013, the torrent site [AhaShare.com](http://www.ahashare.com) (<http://www.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.

Compromised data: Email addresses, Genders, Geographic locations, IP addresses, Passwords, Usernames, Website activity, Years of birth



Aipai.com ?

In September 2016, data allegedly obtained from the Chinese gaming website known as [Aipai.com](http://aipai.com) (<http://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.](https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/) (<https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/>)

Compromised data: Email addresses, Passwords

ANDROIDFORUMS

Android Forums

In October 2011, the Android Forums website was [hacked](http://www.pcworld.com/article/259201/online_android_forum_hacked_user_data_accessed.html) (http://www.pcworld.com/article/259201/online_android_forum_hacked_user_data_accessed.html) 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.

Compromised data: Dates of birth, Email addresses, Homepage URLs, Instant messenger identities, IP addresses, Passwords

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](https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned) (<https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned>).

Compromised data: Email addresses, Passwords

ARMY FORCE ONLINE

Army Force Online

In May 2016, the the online gaming site [Army Force Online](http://armyforceonline.com) (<http://armyforceonline.com>) 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.

Compromised data: Avatars, Email addresses, Geographic locations, IP addresses, Names, Passwords, Usernames, Website activity

Ashley Madison ?

In July 2015, the infidelity website Ashley Madison suffered a serious data breach (<http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/>). 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](https://haveibeenpwned.com/NotifyMe) (<https://haveibeenpwned.com/NotifyMe>). [Read about this approach in detail](http://www.troyhunt.com/2015/07/heres-how-im-going-to-handle-ashley.html) (<http://www.troyhunt.com/2015/07/heres-how-im-going-to-handle-ashley.html>).

Compromised data: Dates of birth, Email addresses, Ethnicities, Genders, Names, Passwords, Payment histories, Phone numbers, Physical addresses, Security questions and answers, Sexual orientations, Usernames, Website activity



Astropid

In December 2013, the vBulletin forum for the social engineering site known as "AstroPID" was breached and leaked publicly (<https://www.sinister.ly/Thread-40-Compromised-databases>). 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.

Compromised data: Email addresses, Instant messenger identities, IP addresses, Names, Passwords, Private messages, Usernames, Website activity



Aternos

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 (<https://twitter.com/AternosStatus/status/696121828360716288>). The data included usernames, email and IP addresses and hashed passwords.

Compromised data: Email addresses, IP addresses, Passwords, Usernames, Website activity



Avast

In May 2014, the Avast anti-virus forum was hacked (<https://www.grahamcluley.com/2014/05/avast-forum-hacked/>) and 423k member records were exposed. The Simple Machines Based forum included usernames, emails and password hashes.

Compromised data: Email addresses, Passwords, Usernames



Badoo

In June 2016, a data breach allegedly originating from the social website Badoo was found to be circulating amongst traders (<https://motherboard.vice.com/read/another-day-another-hack-user-accounts-of-dating-site-badoo>). 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 (<https://www.troyhunt.com/introducing-unverified-breaches-to-have-i-been-pwned>) so this breach has been categorised as "unverified".

Compromised data: Dates of birth, Email addresses, Genders, Names, Passwords, Usernames



Battlefield Heroes

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 (<https://www.rockpapershotgun.com/2011/06/26/lulzsec-over-release-battlefield-heroes-data>). The passwords were stored as MD5 hashes with no salt and many were easily converted back to their plain text versions.

Compromised data: Passwords, Usernames



Beautiful People

In November 2015, the dating website [Beautiful People](http://www.forbes.com/sites/thomasbrewster/2016/04/25/beautiful-people-hack-sexual-preference-location-addresses/#26a2cdf7559f) was hacked (<http://www.forbes.com/sites/thomasbrewster/2016/04/25/beautiful-people-hack-sexual-preference-location-addresses/#26a2cdf7559f>) 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.

Compromised data: Beauty ratings, Car ownership statuses, Dates of birth, Drinking habits, Education levels, Email addresses, Genders, Geographic locations, Home ownership statuses, Income levels, IP addresses, Job titles, Names, Passwords, Personal descriptions, Personal interests, Physical attributes, Sexual orientations, Smoking habits, Website activity



Bell (2014 breach)

In February 2014, Bell Canada suffered a data breach via the hacker collective known as NullCrew (http://news.softpedia.com/news/Hackers-Claim-to-Have-Breached-Bell-Canada-s-Systems-422952.shtml?utm_medium=twitter&utm_source=FredToadster). 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.

Compromised data: Credit cards, Genders, Passwords, Usernames



Bell (2017 breach)

In May 2017, the Bell telecommunications company in Canada suffered a data breach (<http://www.cbc.ca/beta/news/technology/bell-data-breach-customer-names-phone-numbers-emails-leak-1.4116608>) 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.

Compromised data: Email addresses, Geographic locations, IP addresses, Job titles, Names, Passwords, Phone numbers, Spoken languages, Survey results, Usernames



BigMoneyJobs

In April 2014, the job site [bigmoneyjobs.com](http://www.bigmoneyjobs.com) (<http://www.bigmoneyjobs.com>) was hacked by an attacker known as "ProbablyOnion" (<https://twitter.com/ProbablyOnion2/status/451477310319779841>). The attack resulted in the exposure of over 36,000 user accounts (http://news.softpedia.com/news/BigMoneyJobs-Hacked-Details-of-36-000-Users-Leaked-Online-436250.shtml?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=information_security) including email addresses, usernames and passwords which were stored in plain text. The attack was allegedly mounted by exploiting a SQL injection vulnerability.

Compromised data: Career levels, Education levels, Email addresses, Names, Passwords, Phone numbers, Physical addresses, Salutations, User website URLs, Website activity



Bitcoin Security Forum Gmail Dump

In September 2014, a large dump of nearly 5M usernames and passwords was posted to a Russian Bitcoin forum (<https://forum.btcsec.com/index.php?topic/9426-gmail-meniai-parol/>). 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 sources as correct (https://web.archive.org/web/20140910190920/http://www.reddit.com/r/netsec/comments/2fz13q/5_millions_of_gmail_passwords_leaked_rus_most/) albeit a number of years old.

Compromised data: Email addresses, Passwords

Bitcoin Talk

In May 2015, the Bitcoin forum Bitcoin Talk was hacked (<https://www.cryptocoinsnews.com/bitcoin-exchange-btc-e-bitcointalk-forum-breaches-details-revealed/>) 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.

Compromised data: Dates of birth, Email addresses, Genders, IP addresses, Passwords, Security questions and answers, Usernames, Website activity



BitTorrent

In January 2016, the forum for the popular torrent software BitTorrent was hacked (<https://motherboard.vice.com/read/another-day-another-hack-user-accounts-for-bittorrents-forum-hacking>). The IP.Board based forum stored passwords as weak SHA1 salted hashes and the breached data also included usernames, email and IP addresses.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Black Hat World

In June 2014, the search engine optimisation forum Black Hat World (<http://www.blackhatworld.com>) 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.

Compromised data: Dates of birth, Email addresses, Instant messenger identities, IP addresses, Passwords, Usernames, Website activity



Bot of Legends

In November 2014, the forum for Bot of Legends (<http://botoflegends.com>) suffered a data breach. The IP.Board forum contained 238k accounts including usernames, email and IP addresses and passwords stored as salted MD5 hashes.

Compromised data: Email addresses, IP addresses, Passwords, Usernames, Website activity



Boxee

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.

Compromised data: Dates of birth, Email addresses, Geographic locations, Historical passwords, Instant messenger identities, IP addresses, Passwords, Private messages, User website URLs, Usernames



Brazzers

In April 2013, the adult website known as Brazzers was hacked (<https://motherboard.vice.com/read/nearly-800000-brazzers-porn-site-accounts-exposed-in-forum-hack>) 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 (<https://vigilante.pw>) data breach reporting site in September 2016.

Compromised data: Email addresses, Passwords, Usernames



BTC-E

In October 2014, the Bitcoin exchange BTC-E was hacked (<https://www.databreaches.net/bitcoin-exchange-btc-e-and-bitcointalk-forum-breaches/>) and 568k accounts were exposed. The data included email and IP addresses, wallet balances and hashed passwords.

Compromised data: Account balances, Email addresses, IP addresses, Passwords, Usernames, Website activity

B U S I N E S S

M A G A Z I N E

Business Acumen Magazine

In April 2014, the Australian "Business Acumen Magazine" website was hacked by an attacker known as 1337MiR (<http://1337mir.com/cracked/2014/04/businessacumen-biz-hacked-26000-user-password-leaked/>). 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).

Compromised data: Email addresses, Names, Passwords, Usernames, Website activity



Cannabis.com

In February 2014, the vBulletin forum for the Marijuana site cannabis.com was breached and leaked publicly (<https://www.google.com/search?q=%22cannabisforum.tar%22>). 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.

Compromised data: Dates of birth, Email addresses, Geographic locations, Historical passwords, Instant messenger identities, IP addresses, Passwords, Private messages, Usernames, Website activity



CD Projekt RED

In March 2016, Polish game developer CD Projekt RED suffered a data breach (<http://forums.cdprojektred.com/forum/en/the-witcher-series/news-aa/7248610-important-potential-unauthorized-access-to-the-forums%E2%80%99-data>). The hack of their forum led to the exposure of almost 1.9 million accounts along with usernames, email addresses and salted SHA1 passwords.

Compromised data: Email addresses, Passwords, Usernames

cheapassgamer

CheapAssGamer.com

In approximately mid-2015, the forum for CheapAssGamer.com (<https://www.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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Civil Online ?

In mid-2011, data was allegedly obtained from the Chinese engineering website known as Civil Online (<http://www.co188.com/>) 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.](https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/) (<https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/>)

Compromised data: Email addresses, IP addresses, Passwords, Usernames, Website activity



ClixSense

In September 2016, the paid-to-click site ClixSense suffered a data breach (<http://cybercashworldwide.com/clixsense-has-been-hacked>) 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.

Compromised data: Account balances, Dates of birth, Email addresses, Genders, IP addresses, Names, Passwords, Payment histories, Payment methods, Physical addresses, Usernames, Website activity



CloudPets

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 (<https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages>) (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.

Compromised data: Email addresses, Family members' names, Passwords



Comcast

In November 2015, the US internet and cable TV provider Comcast suffered a data breach that exposed 590k customer email addresses and plain text passwords (<http://www.ibtimes.co.uk/comcast-data-breach-590000-customer-passwords-go-sale-dark-web-1528026>). A further 27k accounts appeared with home addresses with the entire data set being sold on underground forums.

Compromised data: Email addresses, Passwords, Physical addresses



COMELEC (Philippines Voters)

In March 2016, the Philippines Commission of Elections website (<http://www.comelec.gov.ph/>) (COMELEC) was attacked and defaced (<http://www.rappler.com/nation/politics/elections/2016/127256-comelec-website-hacked-anonymous-philippines>), allegedly by Anonymous Philippines. Shortly after, data on 55 million Filipino voters was leaked publicly (http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/) and included sensitive information such as genders, marital statuses, height and weight and biometric fingerprint data. The breach only included 228k email addresses.

Compromised data: Biometric data, Dates of birth, Email addresses, Family members' names, Genders, Job titles, Marital statuses, Names, Passport numbers, Phone numbers, Physical addresses, Physical attributes



Crack Community

In late 2013, the Crack Community (<http://crackcommunity.com>) 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames, Website activity

vBulletin

CrimeAgency vBulletin Hacks 🔥

In January 2016, a large number of unpatched vBulletin forums were compromised by an actor known as "CrimeAgency" (<http://news.softpedia.com/news/vbulletin-hack-exposes-820-000-accounts-from-126-forums-513416.shtml>). 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 (<https://troyhunt.com/i-just-added-another-140-data-breaches-to-have-i-been-pwned>) for further information on which sites were impacted.

Compromised data: Email addresses, Passwords, Usernames



Cross Fire

In August 2016, the Russian gaming forum known as Cross Fire (or cfire.mail.ru) was hacked (<http://www.zdnet.com/article/over-25-million-accounts-stolen-after-mail-ru-forums-raided-by-hackers/>) 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.

Compromised data: Email addresses, Passwords, Usernames



DaFont

In May 2017, font sharing site DaFont suffered a data breach (<http://www.zdnet.com/article/font-sharing-site-dafont-hacked-thousands-of-accounts-stolen/>) 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.

Compromised data: Email addresses, Passwords, Usernames

DaniWeb

In late 2015, the technology and social site DaniWeb (<https://www.daniweb.com>) 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.

Compromised data: Email addresses, IP addresses, Passwords



DLH.net

In July 2016, the gaming news site [DLH.net](http://www.zdnet.com/article/millions-of-steam-game-keys-stolen-after-site-hack/) suffered a data breach (<http://www.zdnet.com/article/millions-of-steam-game-keys-stolen-after-site-hack/>) 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](https://vigilante.pw/) (<https://vigilante.pw/>).

Compromised data: Dates of birth, Email addresses, Names, Passwords, Usernames, Website activity



Dodone.com ?

In late 2011, data was allegedly obtained from the Chinese website known as [Dodone.com](http://dodone.com) (<http://dodone.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 flag ged as "unverified". The data in the breach contains email addresses and user names. [Read more about Chinese data breaches in Have I been pwned.](https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/) (<https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/>)

Compromised data: Email addresses, Usernames



Domino's

In June 2014, [Domino's Pizza](http://www.welivesecurity.com/2014/06/16/dominos-pizza-hacked/) in France and Belgium was hacked (<http://www.welivesecurity.com/2014/06/16/dominos-pizza-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](http://cyberintelligence.in/rex-mundi-hackers-leaked-data-dominos-accord-easypay/) (<http://cyberintelligence.in/rex-mundi-hackers-leaked-data-dominos-accord-easypay/>) along with troves of other hacked accounts. Amongst the customer data was passwords stored with a weak MD5 hashing algorithm and no salt.

Compromised data: Email addresses, Names, Passwords, Phone numbers, Physical addresses



Dropbox

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](https://motherboard.vice.com/read/dropbox-forces-password-resets-after-user-credentials-exposed) for customers they believed may be at risk (<https://motherboard.vice.com/read/dropbox-forces-password-resets-after-user-credentials-exposed>). A large volume of data totalling over 68 million records [was subsequently traded online](https://motherboard.vice.com/read/hackers-stole-over-60-million-dropbox-accounts) (<https://motherboard.vice.com/read/hackers-stole-over-60-million-dropbox-accounts>) and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcr ypt).

Compromised data: Email addresses, Passwords



Dungeons & Dragons Online

In April 2013, the interactive video game [Dungeons & Dragons Online](https://www.ddo.com) (<https://www.ddo.com>) 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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity



Duowan.com ?

In approximately 2011, data was allegedly obtained from the Chinese gaming website known as [Duowan.com](http://www.duowan.com) (<http://www.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.](https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/) (<https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/>)

Compromised data: Email addresses, Passwords, Usernames

Elance

Elance

Sometime in 2009, staffing platform [Elance](http://www.ibtimes.co.uk/elance-data-breach-hacker-leaks-1-3-million-accounts-staffing-platform-1605368) suffered a data breach that impacted 1.3 million accounts (<http://www.ibtimes.co.uk/elance-data-breach-hacker-leaks-1-3-million-accounts-staffing-platform-1605368>). Appearing online 8 years later, the data contained usernames, email addresses, phone numbers and SHA1 hashes of passwords, amongst other personal data.

Compromised data: Email addresses, Employers, Geographic locations, Passwords, Phone numbers, Usernames



Epic Games

In August 2016, the Epic Games forum suffered a data breach (<http://www.zdnet.com/article/epic-games-unreal-engine-forums-hacked-in-latest-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.

Compromised data: Email addresses, Passwords, Usernames

Eroticy

Eroticy ?

In mid-2016, it's alleged that the adult website known as [Eroticy](http://eroticity.com) (<http://eroticity.com>) 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 inconclusive. [A detailed account of the data has been published](https://www.troyhunt.com/a-data-breach-investigation-blow-by-blow) (<https://www.troyhunt.com/a-data-breach-investigation-blow-by-blow>) in the hope of identifying the origin of the breach.

Compromised data: Email addresses, IP addresses, Names, Passwords, Payment histories, Phone numbers, Physical addresses, Usernames, Website activity



eThekweni Municipality

In September 2016, the new eThekweni eServices website (<http://eservices.durban.gov.za>) 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 (<http://mybroadband.co.za/news/security/179064-e-thekweni-municipality-leaking-private-details-of-over-300000-residents.html>) 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.

Compromised data: Dates of birth, Deceased date, Email addresses, Genders, Government issued IDs, Names, Passport numbers, Passwords, Phone numbers, Physical addresses, Utility bills



Ethereum

In December 2016, the forum for the public blockchain-based distributed computing platform [Ethereum](https://blog.ethereum.org/2016/12/19/security-alert-12192016-ethereum-org-forums-database-compromised/) suffered a data breach (<https://blog.ethereum.org/2016/12/19/security-alert-12192016-ethereum-org-forums-database-compromised/>). The database contained over 16k unique email addresses along with IP addresses, private forum messages and (mostly) bcrypt hashed passwords. [Ethereum](https://www.troyhunt.com/the-ethereum-forum-was-hacked-and-theyve-voluntarily-submitted-the-data-to-have-i-been-pwned/) elected to self-submit the data to HIBP (https://www.troyhunt.com/the-ethereum-forum-was-hacked-and-theyve-voluntarily-submitted-the-data-to-have-i-been-pwned), providing the service with a list of email addresses impacted by the incident.

Compromised data: Email addresses, IP addresses, Passwords, Private messages, Usernames, Website activity



Evony

In June 2016, the online multiplayer game [Evony](http://securityaffairs.co/wordpress/52260/data-breach/evony-data-breach.html) was hacked (<http://securityaffairs.co/wordpress/52260/data-breach/evony-data-breach.html>) 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).

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Experian ?

In September 2015, the US based credit bureau and consumer data broker [Experian](http://krebsonsecurity.com/2015/10/experian-breach-affects-15-million-consumers/) suffered a data breach (<http://krebsonsecurity.com/2015/10/experian-breach-affects-15-million-consumers/>) 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 therefore this breach has been flagged as "unverified".

Compromised data: Credit status information, Dates of birth, Email addresses, Ethnicities, Family structure, Genders, Home ownership statuses, Income levels, IP addresses, Names, Phone numbers, Physical addresses, Purchasing habits

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](https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned/) (https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned).

Compromised data: Email addresses, Passwords



FashionFantasyGame

In late 2016, the fashion gaming website [Fashion Fantasy Game](http://www.zdnet.com/article/amid-data-breach-responsibility-thrown-to-the-wind/) suffered a data breach (<http://www.zdnet.com/article/amid-data-breach-responsibility-thrown-to-the-wind/>). 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.

Compromised data: Email addresses, Passwords



Final Fantasy Shrine

In September 2015, the Final Fantasy discussion forum known as FFShrine (<http://ffshrine.org>) was breached and the data dumped publicly. Approximately 620k records were released containing email addresses, IP addresses and salted hashes of passwords.

Compromised data: Email addresses, Passwords, Usernames, Website activity

Flash Flash Revolution

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

Compromised data: Email addresses, Passwords, Usernames

Flashback

In February 2015, the Swedish forum known as Flashback (<http://www.flashback.se/>) had sensitive internal data on 40k members published via the tabloid newspaper Aftonbladet (<http://www.aftonbladet.se/>). The data was allegedly sold to them via Researchgruppen (<http://swedishsurveyor.com/2015/02/11/the-inquisition/>) (The Research Group) who have a history of exposing otherwise anonymous users (<https://www.technologyreview.com/photoessay/533426/the-troll-hunters/>), primarily those who they believe participate in "troll like" behaviour. The compromised data includes social security numbers, home and email addresses.

Compromised data: Email addresses, Government issued IDs, Physical addresses

Fling

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 (<https://motherboard.vice.com/read/another-day-another-hack-passwords-and-sexual-desires-for-dating-site-fling>). The breached data included highly sensitive personal attributes such as sexual orientation and sexual interests as well as email addresses and passwords stored in plain text.

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Passwords, Phone numbers, Sexual fetishes, Sexual orientations, Usernames, Website activity

Forbes

In February 2014, the Forbes website succumbed to an attack that leaked over 1 million user accounts (http://news.cnet.com/8301-1009_3-57618945-83/syrian-electronic-army-hacks-forbes-steals-user-data). 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.

Compromised data: Email addresses, Passwords, User website URLs, Usernames



Foxy Bingo

In April 2007, the online gambling site Foxy Bingo (<https://www.foxybingo.com>) was hacked and 252,000 accounts were obtained by the hackers. The breached records were subsequently sold and traded (<http://www.itpro.co.uk/637279/gambler-busted-flogging-stolen-data-to-gaming-firms>) and included personal information data such as plain text passwords, birth dates and home addresses.

Compromised data: Account balances, Browser user agent details, Dates of birth, Email addresses, Genders, Names, Passwords, Phone numbers, Physical addresses, Usernames, Website activity

Freedom Hosting II 🔒

In January 2017, the free hidden service host Freedom Hosting II suffered a data breach (<http://www.theverge.com/2017/2/3/14497992/freedom-hosting-ii-hacked-anonymous-dark-web-tor>). 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.

Compromised data: Email addresses, Passwords, Usernames



Fridae 🔒

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 (<https://twitter.com/Survela/status/463327706361659392>) appears to have been orchestrated by Deletesecc (<http://pastebin.com/ipFKjv6z>) who claim that "Digital weapons shall annihilate all secrecy within governments and corporations". The exposed data included password stored in plain text.

Compromised data: Email addresses, Passwords, Usernames, Website activity



Funimation

In July 2016, the anime site Funimation (<https://www.funimation.com/>) 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.

Compromised data: Dates of birth, Email addresses, Passwords, Usernames



Fur Affinity 🔒

In May 2016, the Fur Affinity website for people with an interest in anthropomorphic animal characters (also known as "furries") was hacked (<https://motherboard.vice.com/read/another-day-another-hack-furry-site-hacked-content-deleted>). The attack exposed 1.2M email addresses (many accounts had a different "first" and "last" email against them) and hashed passwords.

Compromised data: Email addresses, Passwords, Usernames



Gamerzplanet

In approximately October 2015, the online gaming forum known as Gamerzplanet (<http://gamerzplanet.net>) 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



GameTuts

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 (<https://twitter.com/TeamModio/status/756705841168916486>) but was identified as having been hosted on a vBulletin forum. The exposed data included usernames, email and IP addresses and salted MD5 hashes.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Gamigo

In March 2012, the German online game publisher Gamigo was hacked (<http://www.zdnet.com/article/8-24-million-gamigo-passwords-leaked-after-hack/>) and more than 8 million accounts publicly leaked. The breach included email addresses and passwords stored as weak MD5 hashes with no salt.

Compromised data: Email addresses, Passwords



Gawker

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 Gawker's 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 (<http://www.troyhunt.com/2011/01/why-your-apps-security-design-could.html>).

Compromised data: Email addresses, Passwords, Usernames



GeekedIn

In August 2016, the technology recruitment site GeekedIn (<http://geekedin.net>) 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](https://www.troyhunt.com/8-million-github-profiles-were-leaked-from-geekedins-mongodb-heres-how-to-see-yours) (<https://www.troyhunt.com/8-million-github-profiles-were-leaked-from-geekedins-mongodb-heres-how-to-see-yours>).

Compromised data: Email addresses, Geographic locations, Names, Professional skills, Usernames, Years of professional experience



GFAN ?

In October 2016, data surfaced that was allegedly obtained from the Chinese website known as [GFAN \(http://www.gfan.com\)](http://www.gfan.com) 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 salt ed and hashed passwords. [Read more about Chinese data breaches in Have I been pwned. \(https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/\)](https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/)

Compromised data: Email addresses, IP addresses, Passwords, Usernames



gPotato

In July 2007, the multiplayer game portal known as [gPotato \(https://web.archive.org/web/20070710161412/http://gpotato.com/\)](https://web.archive.org/web/20070710161412/http://gpotato.com/) (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 \(http://www.webzen.com/\)](http://www.webzen.com/) 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.

Compromised data: Dates of birth, Email addresses, Genders, IP addresses, Names, Passwords, Physical addresses, Security questions and answers, Usernames, Website activity



GTAGaming

In August 2016, the Grand Theft Auto forum [GTAGaming](https://motherboard.vice.com/read/grand-theft-auto-fan-site-hacked) was hacked and nearly 200k user accounts were leaked (<https://motherboard.vice.com/read/grand-theft-auto-fan-site-hacked>). The vBulletin based forum included usernames, email addresses and password hashes.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity

Hack Forums

hackforums.net

In June 2011, the hacktivist group known as "LulzSec" leaked one final large data breach they titled "50 days of lulz" (<http://www.forbes.com/sites/andygreenberg/2011/06/25/lulzsec-says-goodbye-dumping-nato-att-gamer-data/>). The compromised data came from sources such as AT&T, Battlefield Heroes and the [hackforums.net website \(http://hackforums.net\)](http://hackforums.net). The leaked Hack Forums data included credentials and personal information of nearly 200,000 registered forum users.

Compromised data: Dates of birth, Email addresses, Instant messenger identities, IP addresses, Passwords, Social connections, Spoken languages, Time zones, User website URLs, Usernames, Website activity

Hacking Team

In July 2015, the Italian security firm [Hacking Team \(http://hackingteam.com\)](http://hackingteam.com) suffered a major data breach that resulted in over 400GB of their data being posted online via a torrent (<http://www.techtimes.com/articles/68204/20150711/hacking-team-hacked-400gb-data-dump-state-surveillance-exposes-dirty.htm>). 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 (<https://wikileaks.org/hackingteam/emails>).

Compromised data: Email addresses, Email messages



Health Now Networks

In March 2017, the telemarketing service Health Now Networks left a database containing hundreds of thousands of medical records exposed (<https://www.databreaches.net/leak-of-diabetic-patients-data-highlights-risks-of-giving-info-to-telemarketers/>). 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.

Compromised data: Dates of birth, Email addresses, Genders, Health insurance information, IP addresses, Names, Personal health data, Phone numbers, Physical addresses, Security questions and answers, Social connections



Hemmakväll

In July 2015, the Swedish video store chain Hemmakväll (<http://www.hemmakvall.se/>) was hacked (<http://www.dn.se/ekonomi/hemmakvall-hackat-50000-kunders-uppgifter-pa-vift/>) 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.

Compromised data: Email addresses, Names, Passwords, Phone numbers, Physical addresses



hemmelig.com

In December 2011, Norway's largest online sex shop hemmelig.com was hacked by a collective calling themselves "Team Appunity" (<http://www.dazzlepod.com/hemmelig/?page=93>). The attack exposed over 28,000 usernames and email addresses along with nicknames, gender, year of birth and unsalted MD5 password hashes.

Compromised data: Email addresses, Genders, Nicknames, Passwords, Usernames, Years of birth



Heroes of Gaia

In early 2013, the online fantasy multiplayer game Heroes of Gaia (<http://hog.playsnail.com>) 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.

Compromised data: Browser user agent details, Email addresses, IP addresses, Usernames, Website activity



Heroes of Newerth

In December 2012, the multiplayer online battle arena game known as Heroes of Newerth (<http://www.heroesofnewerth.com/>) was hacked (https://www.reddit.com/r/HeroesofNewerth/comments/14zj2p/i_am_the_guy_who_hacked_hon/) and over 8 million accounts extracted from the system. The compromised data included usernames, email addresses and passwords.

Compromised data: Email addresses, Passwords, Usernames



HLTV

In June 2016, the "home of competitive Counter Strike" website HLTV was hacked (<http://www.hltv.org/news/18087-security-breach>) and 611k accounts were exposed. The attack led to the exposure of names, usernames, email addresses and bcrypt hashes of passwords.

Compromised data: Email addresses, Names, Passwords, Usernames, Website activity



HongFire

In March 2015, the anime and manga forum HongFire (<http://www.hongfire.com>) 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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames



i-Dressup

In June 2016, the teen social site known as i-Dressup was hacked (<http://arstechnica.com/security/2016/09/social-hangout-site-for-teens-leaks-millions-of-plaintext-passwords/>) 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.

Compromised data: Email addresses, Passwords



iMesh

In September 2013, the media and file sharing client known as iMesh was hacked and approximately 50M accounts were exposed (<http://www.ibtimes.co.uk/imesh-hack-more-51-million-user-records-former-filesharing-site-sale-dark-web-1565185>). 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames

insanelyi

Insanelyi

In July 2014, the iOS forum Insanelyi (<http://insanelyi.com>) was hacked by an attacker known as Kim Jong-Cracks (http://securityaffairs.co/wordpress/26835/hacking/hacked-bigboss-cydia.html?utm_content=bufferc7e16). A popular source of information for users of jailbroken iOS devices running Cydia, the Insanelyi breach disclosed over 104k users' email addresses, user names and weakly hashed passwords (salted MD5).

Compromised data: Email addresses, Passwords, Usernames, Website activity



InterPals

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.

Compromised data: Dates of birth, Email addresses, Geographic locations, Names, Passwords, Usernames



iPmart

During 2015, the [iPmart forum \(http://ipmart-forum.com\)](http://ipmart-forum.com) (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.

Compromised data: Dates of birth, Email addresses, Passwords, Usernames

Justdate.com

An alleged breach of the dating website [Justdate.com \(http://www.justdate.com/\)](http://www.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 \(https://www.troyhunt.com/introducing-fabricated-data-breaches-to-have-i-been-pwned\)](https://www.troyhunt.com/introducing-fabricated-data-breaches-to-have-i-been-pwned); it's highly unlikely the data was sourced from Justdate.com.

Compromised data: Dates of birth, Email addresses, Geographic locations, Names

KimSufi

KimSufi

In mid-2015, the forum for the providers of affordable dedicated servers known as [Kimsufi \(https://www.kimsufi.com\)](https://www.kimsufi.com) 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



KM.RU

In February 2016, the Russian portal and email service [KM.RU \(http://km.ru\)](http://km.ru) was the target of an attack which was consequently detailed on [Reddit \(https://www.reddit.com/r/pwned/comments/47u1bf/operation_wrath_of_anakin_evolved\)](https://www.reddit.com/r/pwned/comments/47u1bf/operation_wrath_of_anakin_evolved). 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.

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, Recovery email addresses, Security questions and answers, Usernames

last.fm

Last.fm

In March 2012, the music website [Last.fm](https://techcrunch.com/2016/09/01/43-million-passwords-hacked-in-last-fm-breach/) was hacked (<https://techcrunch.com/2016/09/01/43-million-passwords-hacked-in-last-fm-breach/>) and 43 million user accounts were exposed. Whilst [Last.fm](http://www.last.fm/passwordsecurity) knew of an incident back in 2012 (<http://www.last.fm/passwordsecurity>), 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.

Compromised data: Email addresses, Passwords, Usernames, Website activity

Leet

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 (<http://news.softpedia.com/news/data-for-6-million-minecraft-gamers-stolen-from-leet-cc-servers-507445.shtml>). 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames, Website activity

lifeboat

Lifeboat

In January 2016, the Minecraft community known as Lifeboat was hacked and more than 7 million accounts leaked (<https://motherboard.vice.com/read/another-day-another-hack-7-million-emails-and-hashed-passwords-for-minecraft>). 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.

Compromised data: Email addresses, Passwords, Usernames

LinkedIn

In May 2016, LinkedIn had 164 million email addresses and passwords exposed (<https://www.troyhunt.com/observations-and-thoughts-on-the-linkedin-data-breach>). 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.

Compromised data: Email addresses, Passwords



Linux Mint

In February 2016, the website for the Linux distro known as Linux Mint was hacked and the ISO infected with a backdoor (<https://thehackernews.com/2016/02/linux-mint-hack.html>). 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.

Compromised data: Avatars, Dates of birth, Email addresses, Geographic locations, IP addresses, Passwords, Time zones, Website activity

Little Monsters

In approximately January 2017, the Lady Gaga fan site known as "Little Monsters" suffered a data breach that impacted 1 million accounts (<https://www.heise.de/security/meldung/Little-Monsters-Nutzerdaten-aus-Lady-Gagas-Social-Network-sollen-geleakt-sein-3646447.html>). The data contained usernames, email addresses, dates of birth and bcrypt hashes of passwords.

Compromised data: Dates of birth, Email addresses, Passwords, Usernames



Lizard Squad

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 (<https://krebsonsecurity.com/2015/01/another-lizard-arrested-lizard-lair-hacked/>) which resulted in the public disclosure of over 13k user accounts including passwords stored in plain text.

Compromised data: Email addresses, Passwords, Usernames

Lookbook

Lookbook

In August 2012, the fashion site Lookbook suffered a data breach (<https://www.hackread.com/hacker-selling-million-lookbook-accounts/>). The data later appeared listed for sale in June 2016 and included 1.1 million usernames, email addresses, birth dates and plain text passwords.

Compromised data: Dates of birth, Email addresses, IP addresses, Names, Passwords, Usernames, Website activity



Lord of the Rings Online

In August 2013, the interactive video game Lord of the Rings Online (<https://www.lotro.com>) 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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity

Lounge Board

Lounge Board

At some point in 2013, 45k accounts were breached from the Lounge Board "General Discussion Forum" and then dumped publicly (<http://leak.sx/thread-186921>). Lounge Board was a MyBB forum launched in 2012 and discontinued in mid 2013 (the last activity in the logs was from August 2013).

Compromised data: Email addresses, IP addresses, Names, Passwords, Private messages, Usernames, Website activity

MAC TORRENTS

Mac-Torrents

In October 2015, the torrent site Mac-Torrents (<http://www.mac-torrents.com>) was hacked and almost 94k usernames, email addresses and passwords were leaked. The passwords were hashed with MD5 and no salt.

Compromised data: Email addresses, Passwords, Usernames

@ .RU

mail.ru Dump

In September 2014, several large dumps of user accounts appeared on the Russian Bitcoin Security Forum (<https://forum.btcsec.com/>) 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 (<https://globalvoicesonline.org/2014/09/10/russia-email-yandex-mailru-passwords-hacking/>), the credentials were confirmed by many as legitimate for other services they had subscribed to.

Compromised data: Email addresses, Passwords



MajorGeeks

In November 2015, almost 270k accounts from the MajorGeeks (<http://www.majorgeeks.com>) support forum were breached. The accounts were being actively sold and traded online and included email addresses, salted password hashes and IP addresses.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Malwarebytes

In November 2014, the [Malwarebytes forum](http://www.scmagazine.com/malwarebytes-forum-hacked/article/385187/) was hacked (<http://www.scmagazine.com/malwarebytes-forum-hacked/article/385187/>) 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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity



Manga Traders

In June 2014, the Manga trading website [Mangatraders.com](http://www.mangatraders.com) (<http://www.mangatraders.com>) had the usernames and passwords of over 900k users leaked on the internet (<https://boards.4chan.org/a/thread/108603065/mangatraders-has-been-hacked-emails-and-passwords>) (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.

Compromised data: Email addresses, Passwords

Mate1.com

In February 2016, the dating site [mate1.com](https://motherboard.vice.com/read/hacker-claims-to-have-sold-27m-dating-site-passwords-mate1-com-hell-forum) suffered a huge data breach (<https://motherboard.vice.com/read/hacker-claims-to-have-sold-27m-dating-site-passwords-mate1-com-hell-forum>) 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.

Compromised data: Astrological signs, Dates of birth, Drinking habits, Drug habits, Education levels, Email addresses, Ethnicities, Fitness levels, Genders, Geographic locations, Income levels, Job titles, Names, Parenting plans, Passwords, Personal descriptions, Physical attributes, Political views, Relationship statuses, Religions, Sexual fetishes, Travel habits, Usernames, Website activity, Work habits



Minecraft Pocket Edition Forum

In May 2015, the [Minecraft Pocket Edition forum](http://www.databreaches.net/minecraft-pocket-edition-forum-hacked-dumped/) was hacked (<http://www.databreaches.net/minecraft-pocket-edition-forum-hacked-dumped/>) and over 16k accounts were dumped public. Allegedly hacked by [@rmsg0d](https://twitter.com/rmsg0d) (<https://twitter.com/rmsg0d>), the forum data included numerous personal pieces of data for each user. The forum has subsequently been decommissioned.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Minecraft World Map

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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Minefield

In June 2015, the French Minecraft server known as Minefield (<https://www.minefield.fr>) 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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity

MoDaCo

In approximately January 2016, the UK based Android community known as MoDaCo (<http://www.modaco.com>) suffered a data breach which exposed 880k subscriber identities. The data included email and IP addresses, usernames and passwords stored as salted MD5 hashes.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Modern Business Solutions

In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (<https://twitter.com/0x2Taylor/status/784544208879292417>) (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 data was subsequently attributed to "Modern Business Solutions" (<http://news.softpedia.com/news/hacker-steals-58-million-user-records-from-data-storage-provider-509190.shtml>), 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.

Compromised data: Dates of birth, Email addresses, Genders, IP addresses, Job titles, Names, Phone numbers, Physical addresses



Money Bookers

Sometime in 2009, the e-wallet service known as Money Bookers suffered a data breach which exposed almost 4.5M customers (<http://www.forbes.com/sites/thomasbrewster/2015/11/30/paysafe-optimal-neteller-moneybookers-gambling-cyberattacks-data-breach/>). Now called Skrill, the breach was not discovered until October 2015 and included names, email addresses, home addresses and IP addresses.

Compromised data: Dates of birth, Email addresses, IP addresses, Names, Phone numbers, Physical addresses

MPGH

MPGH

In October 2015, the multiplayer game hacking website MPGH was hacked (<http://www.mpggh.net>) and 3.1 million user accounts disclosed. The vBulletin forum breach contained usernames, email addresses, IP addresses and salted hashes of passwords.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



MrExcel

In December 2016, the forum for the Microsoft Excel tips and solutions site [Mr Excel](http://www.mrexcel.com/details-of-data-breach-at-mrexcel-com/) suffered a data breach (<http://www.mrexcel.com/details-of-data-breach-at-mrexcel-com/>). 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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Social connections, Usernames, Website activity



mSpy

In May 2015, the "monitoring" software known as [mSpy](http://www.mspy.com) (<http://www.mspy.com>) suffered a major data breach (<http://krebsonsecurity.com/2015/05/mobile-spy-software-maker-mspy-hacked-customer-data-leaked/#more-30913>). 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.

Compromised data: Device usage tracking data

Muslim

Muslim Directory

In February 2014, the UK guide to services and business known as the Muslim Directory was attacked by the hacker known as @th3inf1d3l (<http://www.cyberwarnews.info/2014/02/17/muslim-directory-hacked-38903-user-credentials-leaked/>). 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.

Compromised data: Age groups, Email addresses, Employers, Names, Passwords, Phone numbers, Physical addresses, Website activity



Muslim Match

In June 2016, the Muslim Match dating website had 150k email addresses exposed (<https://motherboard.vice.com/read/hacked-private-messages-from-dating-site-muslim-match>). The data included private chats and messages between relationship seekers and numerous other personal attributes including passwords hashed with MD5.

Compromised data: Chat logs, Email addresses, Geographic locations, IP addresses, Passwords, Private messages, User statuses, Usernames



myRepoSpace

In July 2015, the Cydia repository known as [myRepoSpace](https://myrepospace.com/) (<https://myrepospace.com/>) was hacked and user data leaked publicly (https://www.reddit.com/r/jailbreak/comments/3c9qr1/discussion_myrepospace_user_data_leaked/). Cydia is designed to facilitate the installation of apps on jailbroken iOS devices. The repository service was allegedly hacked by @its_not_herpes (https://twitter.com/its_not_herpes) and 0x8badf00d (<https://twitter.com/0x8badf00d>) in retaliation for the service refusing to remove pirated tweaks.

Compromised data: Email addresses, IP addresses, Passwords, Usernames

MySpace

In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts (<https://motherboard.vice.com/read/427-million-myspace-passwords-emails-data-breach>). 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 \(https://www.troyhunt.com/dating-the-ginormous-myspace-breach/\)](https://www.troyhunt.com/dating-the-ginormous-myspace-breach/).

Compromised data: Email addresses, Passwords, Usernames



MyVidster

In August 2015, the social video sharing and bookmarking site [MyVidster](https://www.reddit.com/r/pwned/comments/3h4tud/myvidstercom_hacked_1_million_member_database/) was hacked (https://www.reddit.com/r/pwned/comments/3h4tud/myvidstercom_hacked_1_million_member_database/) and nearly 20,000 accounts were dumped online. The dump included usernames, email addresses and hashed passwords.

Compromised data: Email addresses, Passwords, Usernames



Naughty America

In March 2016, the adult website [Naughty America](http://www.forbes.com/sites/thomasbrewster/2016/04/14/naughty-america-fappening-hacked-porn-sites/) was hacked and the data consequently sold online (<http://www.forbes.com/sites/thomasbrewster/2016/04/14/naughty-america-fappening-hacked-porn-sites/>). 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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity



Neopets

In May 2016, a set of breached data originating from the virtual pet website "Neopets" was found being traded online (<https://motherboard.vice.com/read/neopets-hack-another-day-another-hack-tens-of-millions-of-neopets-accounts>). 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.

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Names, Passwords, Usernames



NetEase

In October 2015, the Chinese site known as [NetEase \(http://www.163.com\)](http://www.163.com) (located at [163.com \(http://www.163.com\)](http://www.163.com)) was reported as having suffered a data breach that impacted hundreds of millions of subscribers (<http://news.mydrivers.com/1/452/452173.htm>). 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. \(https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/\)](https://www.troyhunt.com/handling-chinese-data-breaches-in-have-i-been-pwned/)

Compromised data: Email addresses, Passwords



Neteller

In May 2010, the e-wallet service known as [Neteller](http://www.forbes.com/sites/thomasbrewster/2015/11/30/paysafe-optimal-neteller-moneybookers-gambling-cyberattacks-data-breach/) suffered a data breach which exposed over 3.6M customers (<http://www.forbes.com/sites/thomasbrewster/2015/11/30/paysafe-optimal-neteller-moneybookers-gambling-cyberattacks-data-breach/>). The breach was not discovered until October 2015 and included names, email addresses, home addresses and account balances.

Compromised data: Account balances, Dates of birth, Email addresses, Genders, IP addresses, Names, Phone numbers, Physical addresses, Security questions and answers, Website activity

NETPROSPEX

NetProspex

In 2016, a list of over 33 million individuals in corporate America sourced from Dun & Bradstreet's NetProspex service was leaked online (<https://www.troyhunt.com/weve-lost-control-of-our-personal-data-including-33m-netprospex-records>). 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.

Compromised data: Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses



NextGenUpdate

Early in 2014, the video game website NextGenUpdate (<http://www.nextgenupdate.com>) reportedly suffered a data breach (<https://leakforums.org/thread-265363>) that disclosed almost 1.2 million accounts. Amongst the data breach was usernames, email addresses, IP addresses and salted and hashed passwords.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Nexus Mods

In December 2015, the game modding site Nexus Mods released a statement notifying users that they had been hacked (<http://www.nexusmods.com/games/news/12670/>). 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.

Compromised data: Email addresses, Passwords, Usernames



Nihonomaru

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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames

Nival

In February 2016, the Russian gaming company Nival (<http://nival.com>) was the target of an attack which was consequently detailed on Reddit (https://www.reddit.com/r/pwned/comments/47u1bf/operation_wrath_of_anakin_evolved). 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.

Compromised data: Avatars, Dates of birth, Email addresses, Genders, Names, Spoken languages, Usernames, Website activity



Non Nude Girls 🔒

In May 2013, the non-consensual voyeurism site "Non Nude Girls" suffered a data breach (<http://www.ibtimes.co.uk/upskirt-porn-website-hit-massive-data-leak-exposing-nearly-180000-voyeurs-1602756>). 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.

Compromised data: Email addresses, IP addresses, Names, Passwords, Usernames, Website activity



Nulled

In May 2016, the cracking community forum known as Nulled (<http://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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Private messages, Usernames, Website activity



Onverse

In January 2016, the online virtual world known as Onverse (<http://www.onverse.com>) was hacked and 800k accounts were exposed. Along with email and IP addresses, the site also exposed salted MD5 password hashes.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



OVH

In mid-2015, the forum for the hosting provider known as OVH (<https://www.ovh.com>) suffered a data breach. The vBulletin forum contained 453k accounts including usernames, email and IP addresses and passwords stored as salted MD5 hashes.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



OwnedCore

In approximately August 2013, the World of Warcraft exploits forum known as OwnedCore (<http://www.ownedcore.com>) 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Paddy Power

In October 2010, the Irish bookmaker Paddy Power suffered a data breach (<http://www.telegraph.co.uk/technology/internet-security/11005558/Irish-government-disappointed-over-Paddy-Power-hack.html>) 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.

Compromised data: Account balances, Dates of birth, Email addresses, IP addresses, Names, Phone numbers, Physical addresses, Security questions and answers, Usernames, Website activity



Patreon

In October 2015, the crowdfunding site Patreon was hacked (<http://www.zdnet.com/article/patreon-hacked-anonymous-patrons-exposed/>) and over 16GB of data was released publicly. The dump included almost 14GB of database records with more than 2.3M unique email addresses and millions of personal messages.

Compromised data: Email addresses, Payment histories, Physical addresses, Private messages, Website activity



PayAsUGym

In December 2016, an attacker breached PayAsUGym's website (https://twitter.com/real_1x0123/status/809443917984911364) 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.

Compromised data: Browser user agent details, Email addresses, IP addresses, Names, Partial credit card data, Passwords, Phone numbers, Website activity



PHP Freaks

In October 2015, the PHP discussion board PHP Freaks was hacked (<http://forums.phpfreaks.com/topic/298874-alert-the-phpfreaks-forum-members-data-appears-to-have-been-stolen>) and 173k user accounts were publicly leaked. The breach included multiple personal data attributes as well as salted and hashed passwords.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity



Pixel Federation

In December 2013, a breach of the web-based game community based in Slovakia (<http://www.cyberwarnews.info/2013/12/04/pixel-federation-hacked-38000-user-credentials-leaked>) 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.

Compromised data: Email addresses, Passwords



Plex

In July 2015, the discussion forum for Plex media centre was hacked and over 327k accounts exposed (<https://blog.plex.tv/2015/07/02/security-notice-forum-user-password-resets>). The IP.Board forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

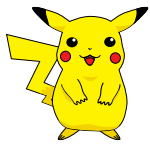
Compromised data: Email addresses, IP addresses, Passwords, Usernames



Pokébip

In July 2015, the French Pokémon site Pokébip suffered a data breach (https://www.pokebip.com/news3382__message_de_securite_de_l_equipe_pokebip_.html) which exposed 657k subscriber identities. The data included email and IP addresses, usernames and passwords stored as unsalted MD5 hashes.

Compromised data: Email addresses, IP addresses, Passwords, Time zones, Usernames, Website activity



Pokémon Creed

In August 2014, the Pokémon RPG website Pokémon Creed (<http://pokemoncreed.net>) was hacked after a dispute with rival site, Pokémon Dusk (<http://pkmndusk.in>). In a post on Facebook (<https://www.facebook.com/ramandeep.s.dehal/posts/749666358442465>), "Cruz Dusk" announced the hack then pasted the dumped MySQL database on pkmndusk.in (<http://pkmndusk.in>). The breached data included over 116k usernames, email addresses and plain text passwords.

Compromised data: Email addresses, Genders, IP addresses, Passwords, Usernames, Website activity



Pokémon Negro

In approximately October 2016, the Spanish Pokémon site Pokémon Negro (<http://pokemonnegro.com>) suffered a data breach. The attack resulted in the disclosure of 830k accounts including email and IP addresses along with plain text passwords. Pokémon Negro did not respond when contacted about the breach.

Compromised data: Email addresses, IP addresses, Passwords



PS3Hax

In approximately July 2015, the Sony Playstation hacks and mods forum known as PS3Hax (<http://www.ps3hax.net>) 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



PSP ISO

In approximately September 2015, the PlayStation PSP forum known as PSP ISO (<http://www.pspiso.com>) 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



PSX-Scene

In approximately February 2015, the Sony Playstation forum known as PSX-Scene (<http://psx-scene.com>) 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Qatar National Bank

In July 2015, the Qatar National Bank suffered a data breach (http://www.theregister.co.uk/2016/04/25/breaking_qatar_bank_hack/) 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 (<http://blog.trendmicro.co.uk/qatar-bank-breach-lifts-the-veil-on-targeted-attack-strategies/#more-520>) in the bank's website.

Compromised data: Bank account numbers, Banking PINs, Customer feedback, Dates of birth, Financial transactions, Genders, Geographic locations, Government issued IDs, IP addresses, Marital statuses, Names, Passwords, Phone numbers, Physical addresses, Security questions and answers, Spoken languages



QIP

In mid-2011, the Russian instant messaging service known as QIP (Quiet Internet Pager) suffered a data breach (<http://securityaffairs.co/wordpress/51118/data-breach/qip-data-breach.html>). 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.

Compromised data: Email addresses, Passwords, Usernames, Website activity



Quantum Booter

In March 2014, the booter service (http://www.webopedia.com/TERM/B/booter_services.html) Quantum Booter (also referred to as Quantum Stresser) suffered a breach which led 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.

Compromised data: Email addresses, IP addresses, Passwords, Private messages, Usernames, Website activity



QuinStreet

In approximately late 2015, the maker of "performance marketing products" QuinStreet (<http://quinstreet.com/>) had a number of their online assets compromised. The attack impacted 28 separate sites, predominantly technology forums such as flashkit.com (<http://quinstreet.com/>), codeguru.com (<http://quinstreet.com/>) and webdeveloper.com (<http://quinstreet.com/>) (view a full list of sites (<http://pastebin.com/raw/6p50GgCV>)). 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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity

R2 (2017 forum breach)

In early 2017, the forum for the gaming website R2 Games was hacked (<http://www.csoonline.com/article/3192246/security/r2games-compromised-again-over-one-million-accounts-exposed.html>). 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.

Compromised data: Email addresses, Passwords, Usernames, Website activity

R2Games

In late 2015, the gaming website R2Games (<https://www.r2games.com>) 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames

Рамблер/

Rambler

In late 2016, a data dump of almost 100M accounts from Rambler, sometimes referred to as "The Russian Yahoo", was discovered being traded online (<http://www.zdnet.com/article/russian-portal-email-provider-rambler-hacked-98-million-accounts-leaked/>). The data set provided to Have I been pwned included 91M unique usernames (which also form part of Rambler email addresses) and plain text passwords. According to Rambler, the data dates back to March 2014.

Compromised data: Email addresses, Passwords, Usernames



Regpack

In July 2016, a tweet was posted with a link to an alleged data breach of BlueSnap, a global payment gateway and merchant account provider (<http://bluesnap.com>). 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 (<http://www.regpacks.com/>) 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 (<https://www.troyhunt.com/someone-just-lost-324k-payment-records-complete-with-cvvs/>).

Compromised data: Browser user agent details, Credit card CVV, Email addresses, IP addresses, Names, Partial credit card data, Phone numbers, Physical addresses, Purchases

Retina-X

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 (https://motherboard.vice.com/en_us/article/inside-stalkerware-surveillance-market-flexispy-retina-x). 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 (<http://www.phonesheriff.com/blog/retina-x-studios-server-breached-by-hackers/>) on April 27, 2017.

Compromised data: Email addresses, Passwords



River City Media Spam List

In January 2017, a massive trove of data from River City Media was found exposed online (<https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire>). 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.

Compromised data: Email addresses, IP addresses, Names, Physical addresses

Rosebutt Board

Some time prior to May 2016, the forum known as "Rosebutt Board" was hacked (<https://motherboard.vice.com/read/rosebuttboard-ip-board>) 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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames



SC Daily Phone Spam List

In early 2015, a spam list known as SC Daily Phone (<http://www.data4marketers.com/2015APRspecials.html>) 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. \(<https://www.troyhunt.com/have-i-been-pwned-and-spam-lists-of-personal-information>\)](https://www.troyhunt.com/have-i-been-pwned-and-spam-lists-of-personal-information)

Compromised data: Dates of birth, Email addresses, Genders, IP addresses, Names, Physical addresses



Seedpeer

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.

Compromised data: Email addresses, Passwords, Usernames



ServerPact

In mid-2015, the Dutch Minecraft site ServerPact was hacked (<https://twitter.com/serverpact/status/772534083788365829>) 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.

Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames

SkTorrent

In February 2016, the Slovak torrent tracking site SkTorrent was hacked and over 117k records leaked online (<http://tech.sme.sk/c/20099331/hackeri-ukradli-na-slovensku-118-tisic-identit.html>). The data dump included usernames, email addresses and passwords stored in plain text.

Compromised data: Email addresses, Passwords, Usernames



Snapchat

In January 2014 just one week after Gibson Security detailed vulnerabilities in the service (<http://gibsonsec.org/snapchat/fulldisclosure/>), Snapchat had 4.6 million usernames and phone numbers exposed. The attack involved brute force enumeration of a large number of phone numbers (<http://www.troyhunt.com/2014/01/searching-snapchat-data-breach-with.html>) 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.

Compromised data: Geographic locations, Phone numbers, Usernames

Sony

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](http://www.sonypictures.com) (<http://www.sonypictures.com>) led to tens of thousands of accounts across multiple systems being exposed (<http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html>) complete with plain text passwords.

Compromised data: Dates of birth, Email addresses, Genders, Names, Passwords, Phone numbers, Physical addresses, Usernames



Soundwave

In approximately mid 2015, the music tracking app Soundwave suffered a data breach (<http://www.soundwave.com/help/>). 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.

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, Names, Passwords, Social connections



Special K Data Feed Spam List

In mid to late 2015, a spam list known as the Special K Data Feed (http://www.data4marketers.com/d4m_SpecialKfeed2015.html) 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. (<https://www.troyhunt.com/have-i-been-pwned-and-spam-lists-of-personal-information>)

Compromised data: Dates of birth, Email addresses, Genders, IP addresses, Names, Physical addresses



Spirol

In February 2014, Connecticut based Spirol Fastening Solutions suffered a data breach that exposed over 70,000 customer records (<http://news.softpedia.com/news/Details-of-70-000-Users-Leaked-by-Hackers-From-Systems-of-SPIROL-International-428669.shtml>). The attack was allegedly mounted by exploiting a SQL injection vulnerability which yielded data from Spirol's CRM system ranging from customers' names, companies, contact information and over 55,000 unique email addresses.

Compromised data: Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses



StarNet

In February 2015, the Moldavian ISP "StarNet" had its database published online (<http://www.moldova.org/the-database-of-an-internet-provider-from-moldova-was-stolen-and-published/>). The dump included nearly 140k email addresses, many with personal details including contact information, usage patterns of the ISP and even passport numbers.

Compromised data: Customer interactions, Dates of birth, Email addresses, Genders, IP addresses, MAC addresses, Names, Passport numbers, Passwords, Phone numbers



Ster-Kinekor

In 2016, the South African cinema company Ster-Kinekor had a security flaw (<http://blog.roguecode.co.za/sterkinekor-vulnerability-download-millions-accounts>) 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.

Compromised data: Dates of birth, Email addresses, Genders, Names, Passwords, Phone numbers, Physical addresses, Spoken languages



Stratfor

In December 2011, "Anonymous" attacked the global intelligence company known as "Stratfor" (<http://www.troyhunt.com/2011/12/5-website-security-lessons-courtesy-of.html>) 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.

Compromised data: Credit cards, Email addresses, Names, Passwords, Phone numbers, Physical addresses, Usernames



Sumo Torrent

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.

Compromised data: Email addresses, IP addresses, Passwords, Usernames, Website activity
