JOE BLACK SECURITY

BLACK IS THE NEW RED

JBS LeakDB Report

Example.com

EXAMPLE

A GREAT COMPANY

https://Joe.Black - info@joe.black

Joe Black Security (JBS) Legal Disclaimer

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. JBS reserves the right to modify the contents of this document at any time without prior notice.

All data obtained by JBS pertaining to entities or individuals not associated or connected to JBS in any way, was discovered on the public internet, and as such, is considered public domain. JBS takes every measure to maintain strict security controls over all data in its possession and will never disclose sensitive information to any 3rd party without the written consent of the data's original owner.

Although JBS uses reasonable efforts to include accurate and up-to-date information herein, JBS makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. JBS disclaims all warranties of any kind, express or implied. Neither JBS nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

This document contains data that should be considered highly sensitive and confidential information and should be treated by representatives of the organization accordingly.

Contents

JBS LeakDB

About JBS LeakDB

LeakDB came about as a RedTeam tool for an easy way to break into customer networks. The insight its data provides has proven to be invaluable time and time again and that the employee truly is the weakest link.
The average online user has between 20-25 accounts. With so many accounts to keep track of, poor password habits and password re-use becomes a serious issue. Knowing when an employee's company credentials are leaked from 3rd party sites could mean the difference between a timely but inconvenient password reset for an employee and an unauthorized breach of an organization's networks.
With countless sites being breached everyday and having their databases leaked to the the dark-web or even directly to the Clearnet, It's trivial for even an average user with basic skills to locate and download copies of this data. Which means it's more important than ever to know exactly where and what your employees are doing with their company emails. Catching an employee's credentials in the wild before they are used by malicious attackers could save your organization a lot of time and money.

Why should LeakDB matter to you?

Why does any of this matter to an organization? What does database leaks from 3rd party sites have anything to do with your average organization? The answer can be broken down into four parts:

Unauthorized Authenticated Access / Password Re-use

- While an unauthenticated attacker can usually be discovered attempting to gain access to an organization's networks, its significantly more difficult to differentiate between an authenticated user and a cautious unauthorized authenticated attacker after access was obtained with valid credentials.
- Every day there is numerous databases being leaked online from major and minor organizations all over the world. Some are large enough to make it into the news, some are too small, but many simply go unnoticed.
- 'Credential Stuffing' or an automated injection of breached username/password pairs in order to fraudulently gain access to user accounts, is a relatively new style of attack due to the massive influx of recently leaked data.
- Attackers scour the internet and the darkweb for these golden gems. You can be assured that every email that is associated with your organization is being tested against any of your login forms exposed to the internet.
- The only way to prevent an attacker from gaining unauthorized authenticated access to your networks is to know about the leaked credentials before an attacker has a chance to use them.

Predicting Password Patterns and habits

- Many times the credentials leaked online that are associated with an employee emails, are not valid for logging into corporate networks.
- While this might prevent Credential Stuffing, a dedicated attacker can still learn a lot from leaked credentials.
- Such as if a user has a habit to add a single digit or increment a digit to a common password for different services.
- This is known as Predicting Password Patterns, and can be just as disastrous if this is a habit of an employee and can lead to unauthorized authenticated access.

Learning User Habits and Misuse

- A less well known but still relevant threat to an organization is what other services an employee is using their company email for.
- Some services such as LinkedIn are generally acceptable but these carry their own risks. Such as an attacker taking over an account of a third party site and using it to abuse the trust that account carries.
- Additionally, employees sometimes feel they can use company emails on any service they like, even on more questionable services such as dating or pornographic sites. This should never be the case.
- Company emails are just that, company emails, and should only ever be used for company related correspondence.

Mass Phishing Campaigns

- A final risk to all organizations, big and small, is mass phishing campaigns.
- With the influx of gigantic compilation lists containing millions or even billions of emails like Exploit.IN and BreachComp, even if leaked passwords are not valid, an attacker now has a wealth of information to perform phishing campaigns against numerous corporate emails.

Next Steps

- Using proprietary tools, JBS can test leaked credentials against externally facing network resources. If valid credentials are discovered, you will be alerted immediately and JBS will assist with a remediation plan.
- Obtaining the fill list of leaked credentials to test against your own internal authentication systems.
- Signup for JBS's LeakDB Alert Service and be alerted whenever new credentials for your organization is discovered.
- Contact us at info@joe.black for more information.

Password Analytics Summary

Password Analytics Introduction

E-mail address from the domain Example.com appear in 129 database leak(s).

Text based passwords continue to be the primary means of user authentication used by information systems worldwide. This is due to the simplicity and low cost implementation of this authentication mechanism. Where this type of authentication becomes an issue is when a user is introduced. The effort of remembering and using a complex password for a service a user might use multiple times a day, tends to influence those users into picking a simpler password and re-using passwords across multiple sites. This has the effect of introducing weak passwords into potentially critical systems such as an organization's networks.

Additionally, hacker and cyber criminal groups greatly benefit from studying passwords from leaked databases in order to understand an organization's employee habits in choosing passwords. This significantly increases their chances of finding a current valid password.

Analyzing this type of data can also help organizations understand their employee's password habits and assist them when choosing password complexity rules as well as training employees on secure password practices.
The following is a simple analysis on cleartext passwords found associated with the Example.com domain.

Search Summary	Domain	Total email count	Cleartext passwords*	Hashed passwords*	Found in
	Example.com	319,640	186,159	177,620	129 databases

* Cleartext passwords and Hashed Passwords are based on counts of data points found within leaked databases. In some cases both clear and hashed passwords were found in a single database while in other cases, neither was found.

Password Analysis

Password Length Analysis

Password Length	Percent	Total
7	21.09 %	39884
8	19.76 %	37369
6	17.62 %	33314
9	13.97 %	26413
10	11.12 %	21036

Password Length Analysis

Password lengths are a quick indicator into the level of security employees use in their everyday online activities. While this is not a direct indication into the lengths of cleartext passwords used in a corporate environment, as many users tend to use 'throw away' passwords for many online accounts, it provides an attacker a general overview of the lengths they will likely come up against.

This analysis was performed on the cleartext passwords found in multiple leaks and shows the top 5 password lengths that are commonly used on 3rd party sites.

Frequency Analysis

Frequency Analysis

How often certain passwords show up in leaked accounts associated with an organization is another indicator into the habits of users. Because these passwords are leaked from 3rd party sites, frequently used words provide attackers not only evidence that the data belongs to a certain organization, but also information that will assist them in cracking additional hashes found in other leaks by reusing common words.
This analysis was performed using the keyword of the organizations name.

Frequency Analysis	Count
91***61	11269
12**56	3161
123***789	2010
12*45	973
9-1***961	933

Advanced (Hashcat) Mask Analysis

Advanced Mask	Percent	Total
?d?d?d?d?d?d?d	8.98 %	16989
?d?d?d?d?d?d	6.8 %	12854
?l?l?l?l?l?l?l?l	4.86 %	9185
?l?l?l?l?l?l	4.33 %	8180
?d?d?d?d?d?d?d?d	4.14 %	7831

Advanced (Hashcat) Mask Analysis

A mask analysis takes cleartext passwords and applies a set value for each character's character set. This mask significantly reduces the time needed for hash cracking as its no longer necessary to brute-force the entire character set but instead only focus on a pre-determined mask of characters.

Mask values:

l: lower alpha
u: capfirst alpha
d: digit
s: special
a: all

Simple Mask Analysis

Simple Mask Analysis

Simple mask analysis is a lot like Advanced Masks but focuses just on the character sets used.
This analysis more clearly defines the distribution of characters used in password leaks.

Simple Mask	Percent	Total
lower_alpha_num	39.76 %	75200
numeric	27.92 %	52800
lower_alpha	20.34 %	38464
lower_alpha_special	2.71 %	5116
lower_alpha_special_num	2.49 %	4705

Additional Findings:

Other Findings	Count
Total count of leaked passwords:	186159
Passwords under 9 characters long	41355
Organization's name was found	1357 times
Top 60 common passwords found	9724 times
Keyboard Walking was found	20 times
Common dates found in passwords	16 times

Additional Findings

• Total count of leaked passwords is the count of all cleartext passwords found in public leaks

• Passwords under 9 characters is the count of all cleartext passwords that don't meet a 10 character length minimum

• The times the organization's name was found in any part of the cleartext password

• A count of how many times cleartext passwords match the to 60 most common passwords

• Keyboard walking is a form of quick key presses across a keyboard in a predictable or simple pattern

• A count of any dates that were found in the cleartext passwords

Leaked Database Summary

Sample Data:

Below is a redacted and truncated sample of lines from the list of leaked credentials
* Passwords are redacted for security reasons
* The final CSV will contain additional unredacted information

Leak	Date	Email	Clear Pass	Hashed Pass
Cheat-maste...	unkn	la*******01@example.com	da***23	--
Comp	2019	so************17@example.com	9-1***961	--
Comp	2019	br*****98@example.com	2s***ke	--
Comp	2019	v**a@example.com	ht**tp	--
Comp	2019	g-***or@example.com	ca****e1	--
Comp	2019	ll******as@example.com	pe***z.	--
Comp	2019	me**********le@example.com	ha***h1	--
Comp	2019	so*************27@example.com	91***61	--
NetEase	2015	m**f@example.com	135*****411	--
000Webhost.com	2015	no*******ll@example.com	ay****$$	--
Badoo.com	2013	ha*****1s@example.com	11**11	a3f0047610c05096f39c4bd1bdf4e...
Fling.com	2011	pr*******************me@example.com	lun****714	ff4ccf7b3954de148b3d2e7b374e1...
Zoosk	2011	pa***********ha@example.com	an**it	ea7f09aceac5db41e510cbb4e144a...
MySpace	2008	gu*******14@example.com	gu**14	873581A1CBDF4C8CAE46C2A582C05...
iMesh.com	2013	as**as@example.com	as**as	--

JBS LeakDB Search Results:

JBS LeakDB has 129 databases in which an email with the domain Example.com was found.
The following list provides details about each database leak:

Legend:

- **Year leaked:** When the website was hacked or when the data was leaked to the internet
- **Email count:** A count of emails associated with the above domain included in each leak
- **Verified?:** If the data was verified by the company whos data was leaked or by 3rd party researchers
- **Sensitive?:** If the data came from a sensitive source such as a dating or pornographic website
- **Details:** Specific details about the breach and what data was leaked.
- **Data exposed:** Indicates that fields data was included in the leaked database
- **--:** Indicates no data for that field was included the leaked database

ARMOR GAMES	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://armorgames.com/	2019	24	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	Data exposed	Data exposed	--	--	--	Data exposed

In January 2019, the game portal website website Armor Games suffered a data breach. A total of 10.6 million email addresses were impacted by the breach which also exposed usernames, IP addresses, birthdays of administrator accounts and passwords stored as salted SHA-1 hashes.

CLASSIC CK KOREA 대한민국 클래식음악 No,1	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.classickorea.co.kr/	2019	1	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker’s Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	Comp	2019	110,269	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This is a compliation of numerous untitled email:password leaks including giant lists like Colletion #1-#5, Breach Comp, Exploit.In, Anti Public, etc... Note: This list does not include data from many of the most popular free email services. If your org uses a free email service, contact us for a more detailed search.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.flashflashrevolution.com/	2019	37	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.luminpdf.com/	2019	14	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In April 2019, the PDF management service Lumin PDF suffered a data breach. The breach wasn't publicly disclosed until September when 15.5M records of user data appeared for download on a popular hacking forum. The data had been left publicly exposed in a MongoDB instance after which Lumin PDF was allegedly been "contacted multiple times, but ignored all the queries". The exposed data included names, email addresses, genders, spoken language and either a bcrypt password hash or Google auth token.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://stockx.com/	2019	6	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	--	Data exposed	--	--	--	--

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://animoto.com/	2018	1,476	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	Data exposed	--	--	--	--

In July 2018, the cloud-based video making service Animoto suffered a data breach. The breach exposed 22 million unique email addresses alongside names, dates of birth, country of origin and salted password hashes.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.blankmediagames.com/	2018	221	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In December 2018, the Town of Salem website produced by BlankMediaGames suffered a data breach. The data contained 7.6M unique user email addresses alongside usernames, IP addresses, purchase histories and passwords stored as phpass hashes.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.cashcrate.com/	2018	277	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	--	Data exposed	--	--	--	Data exposed

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

Chegg	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.chegg.com/	2018	373	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	--	--	--	--	--	--

In April 2018, the textbook rental service Chegg suffered a data breach that impacted 40 million subscribers. The exposed data included email addresses, usernames, names and passwords stored as unsalted MD5 hashes.

DESURA	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.desura.com/	2018	306	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In late 2011, a series of data breaches in China affected up to 100 million users, including the social site known as Desura. 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 cleartext passwords

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://dubsmash.com/	2018	5,325	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	--	Data exposed	--	--	--	--

In December 2018, the video messaging service Dubsmash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly.

HAUTELOOK	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.hautelook.com/	2018	209	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In mid-2018, the fashion shopping site HauteLook was among a raft of sites that were breached and their data then sold in early-2019. The data included over 28 million unique email addresses alongside names, genders, dates of birth and passwords stored as bcrypt hashes.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.morele.net/	2018	4	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	--	--	Data exposed	--	--	--

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.myfitnesspal.com/	2018	765	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly.

SHEIN	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.shein.com	2018	421	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In June 2018, online fashion retailer SHEIN suffered a data breach. The company discovered the breach 2 months later in August then disclosed the incident another month after that. A total of 39 million unique email addresses were found in the breach alongside MD5 password hashes.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://news.zing.vn/	2018	236	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	Data exposed	Data exposed	--	--	Data exposed

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.51cto.com/	2017	7	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In 2013, 51cto, a Chinese social media site was hacked and over 2 million accounts were leaked to the internet.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://8tracks.com/	2017	100	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In June 2017, the online playlists service known as 8Tracks suffered a data breach which impacted 18 million accounts. In their disclosure, 8Tracks advised that "the vector for the attack was an employee's GitHub account, which was not secured using two-factor authentication". Salted SHA-1 password hashes for users who didn't sign up with either Google or Facebook authentication were also included.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.binweevils.com/	2017	4	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	--	--	--	--	Data exposed

In September 2014, the online game Bin Weevils suffered a data breach. net indicated that a more extensive set of personal attributes were impacted (comments there also suggest the data may have come from a later breach). Data matching that pattern was later provided to Have I been pwned by @akshayindia6 and included almost 1.3m unique email addresses, genders, ages and plain text passwords.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.edmodo.com/	2017	1,464	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	Email2Name	2017	82	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
--	Data exposed	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.fotoboom.com/	2017	29	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In early 2018, a large dataset consisting of over 1400 individual databases was found online. This leak contained a file named www.fotoboom.com.txt consisting of email addresses and a combination of hashed and plaintext passwords. While the validity of this breach cannot be confirmed, many of the accounts had not been seen in previous data breaches.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.futureshop.co.uk/	2017	3	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.icross.co.kr/	2017	1	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In early 2018, a large dataset consisting of over 1400 individual databases was found online. This leak contained a file named lifetip.icross.co.kr.txt consisting of email addresses and a combination of hashed and plaintext passwords. While the validity of this breach cannot be confirmed, many of the accounts had not been seen in previous data breaches.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	Japan Combo	2017	284	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.jobstreet.com/	2017	10	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	Data exposed	Data exposed	--	Data exposed	Data exposed

In October 2017, the Malaysian website lowyat.net ran a story on a massive set of breached data affecting millions of Malaysians after someone posted it for sale on their forums. The data spanned multiple separate breaches including the JobStreet jobs website which contained almost 4 million unique email addresses. The dates in the breach indicate the incident occurred in March 2012. The data later appeared freely downloadable on a Tor hidden service and contained extensive information on job seekers includ

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.magazinedee.com/	2017	6	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	RiverCity	2017	69	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
--	Data exposed	--	Data exposed	--	--	--	Data exposed

In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.taringa.net	2017	14	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

zomato	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.zomato.com/	2017	260	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In May 2017, the restaurant guide website Zomato was hacked resulting in the exposure of almost 17 million accounts. The data was consequently redistributed online and contains email addresses, usernames and salted MD5 hashes of passwords (the password hash was not present on all accounts).

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://17.media	2016	34	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In April 2016, customer data obtained from the streaming app known as "17" appeared listed for sale on a Tor hidden service marketplace. The data contained over 4 million unique email addresses along with IP addresses, usernames and passwords stored as unsalted MD5 hashes.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://en.cdprojektred.com/	2016	19	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In March 2016, Polish game developer CD Projekt RED suffered a data breach. The hack of their forum led to the exposure of almost 1.9 million accounts along with usernames, email addresses and salted SHA1 passwords.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://cfire.mail.ru/	2016	214	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In August 2016, the Russian gaming forum known as Cross Fire (or cfire.mail.ru) was hacked along with a number of other forums on the Russian mail provider, mail.ru. The vBulletin forum contained 12.8 million accounts including usernames, email addresses and passwords stored as salted MD5 hashes.

ClixSense	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.clixsense.com/	2016	1	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	Data exposed	--	--	--	Data exposed

In September 2016, the paid-to-click site ClixSense suffered a data breach which exposed 2.4 million subscriber identities. The breached data was then posted online by the attackers who claimed it was a subset of a larger data breach totalling 6.6 million records. The leaked data was extensive and included names, physical, email and IP addresses, genders and birth dates, account balances and passwords stored as plain text.

dailymotion	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.dailymotion.com/	2016	85,367	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

DUNGEONS & DRAGONS ONLINE	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://ddo.com/	2016	4	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	Data exposed	--	--	--	--	Data exposed

In April 2013, the interactive video game Dungeons &amp; Dragons Online suffered a data breach that exposed almost 1.6M players' accounts. The data was being actively traded on underground forums and included email addresses, birth dates and password hashes.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.dfb.de/	2016	27	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.dlh.net/	2016	11	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	--	--	--	--	--

In July 2016, the gaming news site DLH.net suffered a data breach which exposed 3.3M subscriber identities. Along with the keys used to redeem and activate games on the Steam platform, the breach also resulted in the exposure of email addresses, birth dates and salted MD5 password hashes. The data was donated to Have I been pwned by data breach monitoring service Vigilante.pw.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.dropbox.com/	2016	1,833	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://elobuddy.net/	2016	2	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.evony.com/	2016	2,632	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.fashionfantasygame.com/	2016	133	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://game-tuts.com/	2016	45	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

Likely in early 2015, the video game website GameTuts suffered a data breach and over 2 million user accounts were exposed. The site later shut down in July 2016 but was identified as having been hosted on a vBulletin forum. The exposed data included usernames, email and IP addresses and salted MD5 hashes.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://forum.gamevn.com/	2016	3	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

gamigo	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://en.gamigo.com/	2016	67	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In March 2012, the German online game publisher Gamigo was hacked and more than 8 million accounts publicly leaked. The breach included email addresses and passwords stored as weak MD5 hashes with no salt.

机锋 GFAN.COM	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.gfan.com/	2016	111	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In October 2016, data surfaced that was allegedly obtained from the Chinese website known as GFAN and contained 22.5M accounts.

iDressup	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.i-dressup.com/	2016	326	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In June 2016, the teen social site known as i-Dressup was hacked and over 2 million user accounts were exposed. At the time the hack was reported, the i-Dressup operators were not contactable and the underlying SQL injection flaw remained open, allegedly exposing a total of 5.5 million accounts. The breach included email addresses and passwords stored in plain text.

lifeboat	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://forums.lbsg.net/	2016	1,319	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In January 2016, the Minecraft community known as Lifeboat was hacked and more than 7 million accounts leaked. Lifeboat knew of the incident for three months before the breach was made public but elected not to advise customers. The leaked data included usernames, email addresses and passwords stored as straight MD5 hashes.

LEET	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://leet.cc/	2016	571	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In August 2016, the service for creating and running Pocket Minecraft edition servers known as Leet was reported as having suffered a data breach that impacted 6 million subscribers. The incident reported by Softpedia had allegedly taken place earlier in the year contained only 2 million subscribers. The data included usernames, email and IP addresses and SHA512 hashes.

mangafox	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.mangafox.me/	2016	16	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	Data exposed	--	--	--	--	Data exposed

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

mate1	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.mate1.com/	2016	2,915	YES	YES

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	--	--	--	--	--

In February 2016, the dating site mate1.com suffered a huge data breach resulting in the disclosure of over 27 million subscribers' information. The data included deeply personal information about their private lives including drug and alcohol habits, incomes levels and sexual fetishes as well as passwords stored in plain text.

Modern Business Solutions	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://modbsolutions.com	2016	133	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
--	Data exposed	Data exposed	Data exposed	--	--	--	Data exposed

In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently attributed to "Modern Business Solutions", a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be

拇指玩	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.muzhiwan.com/	2016	227	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

NULLED	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.nulled.to/	2016	10	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	Data exposed	--	--	--	--	Data exposed

In May 2016, the cracking community forum known as Nulled 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.

Shadi.com dreams into reality	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.shadi.com/	2016	70	YES	YES

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	Data exposed	Data exposed	--	--	--

In 2016 Shadi.com's Database was breached containing 2 million of their users information containing private information about their sexual lives or fantasies along with their addresses, names and email/passwords.

SUBAGAMES	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://subagames.com/	2016	127	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In September 2016, SubaGames.com was hacked and 3,494,889 Users' account data was breached. The passwords in this database are in salted(hex) vB hashes.

YOUKU	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.youku.com/	2016	728	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.000webhost.com/	2015	209	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	--	--	--	--	--	Data exposed

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.ashleymadison.com/	2015	1,428	YES	YES

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	Data exposed	Data exposed	--	--	--

In July 2015, the infidelity website Ashley Madison suffered a serious data breach. The attackers threatened Ashley Madison with the full disclosure of the breach unless the service was shut down. One month later, the database was dumped including more than 30M unique email addresses. This breach has been classed as "sensitive" and is not publicly searchable, although individuals may discover if they've been impacted by registering for notifications. Read about this approach in detail.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
Bitcoin Forum	https://bitcointalk.org/	2015	9	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	Data exposed	--	--	--	--	Data exposed

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://butterflylabs.com	2015	2	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
<DANIWEB>	https://www.daniweb.com/	2015	27	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In late 2015, the technology and social site DaniWeb suffered a data breach. The attack resulted in the disclosure of 1.1 million accounts including email and IP addresses which were also accompanied by salted MD5 hashes of passwords. However, DaniWeb have advised that "the breached password hashes and salts are incorrect" and that they have since switched to new infrastructure and software.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
gaadi	https://www.gaadi.com/	2015	96	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	--	--	Data exposed	--	--	Data exposed

In May 2015, the Indian motoring website known as Gaadi had 4.3 million records exposed in a data breach. The data contained usernames, email and IP addresses, genders, the city of users as well as passwords stored in both plain text and as MD5 hashes.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
GAMERZ PLANET	http://www.gamerzplanet.net	2015	6	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In approximately October 2015, the online gaming forum known as Gamerzplanet was hacked and more than 1.2M accounts were exposed. The vBulletin forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked.

GROUPON	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.groupon.co.id/	2015	4	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

interpals	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.interpals.net/	2015	5,615	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	--	--	--	--	--

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.

MPGH	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.mpgh.net/	2015	62	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In October 2015, the multiplayer game hacking website MPGH was hacked and 3.1 million user accounts disclosed. The vBulletin forum breach contained usernames, email addresses, IP addresses and salted hashes of passwords.

網易 NETEASE www.163.com	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.163.com/	2015	1,511	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In October 2015, the Chinese site known as NetEase (located at 163.com) was reported as having suffered a data breach that impacted hundreds of millions of subscribers. The data in the breach contains email addresses and plain text passwords.

N 炎丸	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.nihonomaru.net/	2015	34	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

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.

2	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.r2games.com/	2015	425	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In late 2015, the gaming website R2Games was hacked and more than 2.1M personal records disclosed. The vBulletin forum included IP addresses and passwords stored as salted hashes using a weak implementation enabling many to be rapidly cracked. A further 11M accounts were added to "Have I been pwned" in March 2016 and another 9M in July 2016 bringing the total to over 22M.

xat	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.xat.com/	2015	765	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In November 2015, the online chatroom known as "xat" was hacked and 6 million user accounts were exposed. Used as a chat engine on websites, the leaked data included usernames, email and IP addresses along with hashed passwords.

bitly	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://bitly.com/	2014	85	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

Cannabis.com	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://boards.cannabis.com/	2014	18	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	Data exposed	--	--	--	--	Data exposed

In February 2014, the vBulletin forum for the Marijuana site cannabis.com was breached and leaked publicly.

CouponMom ARMOR GAMES	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.couponmom.com/	2014	258	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In 2014, a file allegedly containing data hacked from Coupon Mom was created and included 11 million email addresses and plain text passwords. On further investigation, the file was also found to contain data indicating it had been sourced from Armor Games.

diet.com	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.diet.com/	2014	36	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	--	--	--	--	Data exposed

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

Forbes	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.forbes.com/	2014	1	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In February 2014, the Forbes website succumbed to an attack that leaked over 1 million user accounts. The attack was attributed to the Syrian Electronic Army, allegedly as retribution for a perceived "Hate of Syria". The attack not only leaked user credentials, but also resulted in the posting of fake news stories to forbes.com.

HABBO	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://habbo.st/	2014	9	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker’s Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

安卓网	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.hiapk.com/	2014	114	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In approximately 2014, it's alleged that the Chinese Android store known as HIAPK suffered a data breach that impacted 13.8 million unique subscribers. The data in the breach contains usernames, email addresses and salted MD5 password hashes

KICKSTARTER	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.kickstarter.com/	2014	1	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

клерк	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.klerk.ru/	2014	2	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

TGBUS.com	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.tgbus.com/	2014	227	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In approximately 2017, it's alleged that the Chinese gaming site known as TGBUS suffered a data breach that impacted over 10 million unique subscribers.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.adobe.com/	2013	4,306	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

AhaShare.com	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.ahashare.com	2013	1	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	Data exposed	--	--	--	--	Data exposed

In May 2013, the torrent site AhaShare.com suffered a breach which resulted in more than 180k user accounts being published publicly. The breach included a raft of personal information on registered users plus despite assertions of not distributing personally identifiable information, the site also leaked the IP addresses used by the registered identities.

badoo	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://badoo.com/	2013	13,944	NO	YES

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	--	--	--	--	--

In June 2016, a data breach allegedly originating from the social website Badoo was found to be circulating amongst traders. Likely obtained several years earlier, the data contained 112 million unique email addresses with personal data including names, birthdates and passwords stored as MD5 hashes.

iMesh	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://imesh.com	2013	13,383	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In September 2013, the media and file sharing client known as iMesh was hacked and approximately 50M accounts were exposed. The data was later put up for sale on a dark market website in mid-2016 and included email and IP addresses, usernames and salted MD5 hashes.

neopets	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.neopets.com/	2013	2,032	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	Data exposed	--	--	--	--	Data exposed

In May 2016, a set of breached data originating from the virtual pet website "Neopets" was found being traded online. Allegedly hacked "several years earlier", the data contains sensitive personal information including birthdates, genders and names as well as almost 27 million unique email addresses. Passwords were stored in plain text and IP addresses were also present in the breach.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.nexusmods.com/	2013	14	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

In December 2015, the game modding site Nexus Mods released a statement notifying users that they had been hacked. They subsequently dated the hack as having occurred in July 2013 although there is evidence to suggest the data was being traded months in advance of that. The breach contained usernames, email addresses and passwords stored as a salted hashes.

tumblr.	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.tumblr.com/	2013	787	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://vk.com/	2013	3,701	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	--	--	Data exposed	--	--	--

In approximately 2012, the Russian social media site known as VK was hacked and almost 100 million accounts were exposed. The data emerged in June 2016 where it was being sold via a dark market website and included names, phone numbers email addresses and plain text passwords.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://weheartit.com/	2013	215	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In November 2013, the image-based social network We Heart It suffered a data breach. The data contained user names, email addresses and password hashes, 80% of which were salted SHA-256 with the remainder being MD5 with no salt.

212300.com	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.212300.com/	2012	7	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	Data exposed

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

DISQUS	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://disqus.com/	2012	12,882	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

last.fm	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.last.fm/	2012	455	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. fm knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.

in	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.linkedin.com/	2012	806	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

人人网	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://renren.com/	2012	81	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In December 2011 a database breach affecting renren.com leaked 4.7 million user records including email addresses and plaintext passwords.

淘宝网 Taobao.com	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.taobao.com/	2012	211	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In approximately 2012, it's alleged that the Chinese shopping site known as Taobao suffered a data breach that impacted over 21 million subscribers. The data in the breach contains email addresses and plain text passwords.

17173	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.17173.com/	2011	320	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In late 2011, a series of data breaches in China affected up to 100 million users, including 7.5 million from the gaming site known as 17173.

52PK.com 游戏网	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.52pk.com/	2011	211	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In late 2011, a series of data breaches in China affected up to 100 million users, including the social site known as 52pk. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains usernames, email addresses and cleartext passwords

7K7K	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.7k7k.com/	2011	89	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In approximately 2011, it's alleged that the Chinese gaming site known as 7k7k suffered a data breach that impacted 9.1 million subscribers. The data in the breach contains usernames, email addresses and plain text passwords.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.aipai.com/	2011	47	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In September 2016, data allegedly obtained from the Chinese gaming website known as Aipai.com and containing 6.5M accounts was leaked online. The data in the breach contains email addresses and MD5 password hashes.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://androidforums.com/	2011	2	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	Data exposed	--	--	--	--	Data exposed

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

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.csdn.net/	2011	10	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

One of the biggest programming communities in China, leaked 6M user data. A text file with 6M CSDN user info: user name, password, emails, all in clear text, was found on the internet.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://dodonew.com/	2011	591	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
--	--	--	--	--	--	--	--

In late 2011, data was allegedly obtained from the Chinese website known as Dodonew.com and contained 8.7M accounts. The data in the breach contains email addresses and user names.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.fling.com/	2011	3,058	YES	YES

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	Data exposed	--	Data exposed	--	--	Data exposed

In 2011, the self-proclaimed "World's Best Adult Social Network" website known as Fling was hacked and more than 40 million accounts obtained by the attacker. The breached data included highly sensitive personal attributes such as sexual orientation and sexual interests as well as email addresses and passwords stored in plain text.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://houdao.com/	2011	97	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.mop.com/	2011	62	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In late 2011, a series of data breaches in China affected up to 100 million users, including the social site known as Mop. 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 cleartext passwords

Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
https://www.pconline.com.cn/	2011	102	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker’s Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
https://www.stratfor.com/	2011	40	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	--	Data exposed	Data exposed	Data exposed	--	--

In December 2011, "Anonymous" attacked the global intelligence company known as "Stratfor" and consequently disclosed a veritable treasure trove of data including hundreds of gigabytes of email and tens of thousands of credit card details which were promptly used by the attackers to make charitable donations (among other uses). The breach also included 860,000 user accounts complete with email address, time zone, some internal system data and MD5 hashed passwords with no salt.

Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
http://www.tianya.cn/	2011	426	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
--	Data exposed	--	--	--	--	--	--

In December 2011, China's largest online forum known as Tianya was hacked and tens of millions of accounts were obtained by the attacker. The leaked data included names, usernames and email addresses.

Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
http://www.uuu9.com/	2011	515	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In September 2016, data was allegedly obtained from the Chinese website known as uuu9.com and contained 7.5M accounts. The data in the breach contains email addresses and user names.

Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
https://www.weibo.com/	2011	75	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In late 2011, a series of data breaches in China affected up to 100 million users, including the social site known as Weibo. 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 cleartext passwords

Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
https://www.zoosk.com/	2011	2,716	NO	YES

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

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

Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
http://www.hacker.co.kr/	2010	2	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In early 2010, the popular computer hardware market Hacker.co.kr was breached. Its not known who was the responsible party that leaked the stolen database. Due to its age and the fact that the site no longer exists, its not possible to verify the data.

moneybookers.com	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://moneybookers.com	2009	35	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
--	Data exposed	Data exposed	Data exposed	Data exposed	--	--	Data exposed

Sometime in 2009, the e-wallet service known as Money Bookers suffered a data breach which exposed almost 4.5M customers. Now called Skrill, the breach was not discovered until October 2015 and included names, email addresses, home addresses and IP addresses.

myspace	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://myspace.com/	2008	26,198	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.gpotato.com/	2007	79	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	Data exposed	Data exposed	--	--	--	Data exposed

In July 2007, the multiplayer game portal known as gPotato (link to archive of the site at that time) suffered a data breach and over 2 million user accounts were exposed. The site later merged into the Webzen portal where the original accounts still exist today. The exposed data included usernames, email and IP addresses, MD5 hashes and personal attributes such as gender, birth date, physical address and security questions and answers stored in plain text.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.2games.com/	unkn	191	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker’s Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

百合网 baihe.com	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.baihe.com/	unkn	454	NO	YES

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	Data exposed	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker’s Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

bizbilla Enabling Business	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.bizbilla.com/	unkn	1	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In 2017, a leak from Bizbilla.com surfaced on the clear net. Originally with passwords in MD5 format, they were quickly cracked, and a plaintext version began circling.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://cheat-master.net	unkn	79	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker’s Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

EURONICS Ti ascolta. Davvero.	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.euronics.it/	unkn	1	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

In early 2018, a large dataset consisting of over 1400 individual databases was found online. This leak contained a file named lavoraconnoi.euronics.it.txt consisting of email addresses and a combination of hashed and plaintext passwords. While the validity of this breach cannot be confirmed, many of the accounts had not been seen in previous data breaches.

FOREX INVESTOR	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://forex-investor.net/	unkn	2	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

GigaSize	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.gigasize.com/	unkn	64	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

SPARK MINDA ASHOK MINDA GROUP	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://www.mindacorporation.com/	unkn	4	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

MMGP MONEY MAKER GROUP	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://mmgp.ru/	unkn	1	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

Turn Page Your Digital Publishing Solution	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	http://pubpit.com/	unkn	5	YES	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

小说阅读网	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://www.readnovel.com/	unkn	981	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker's Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

	Leaked Website / Service	Year leaked	Email count	Verified?	Sensitive?
	https://twitter.com/	unkn	171	NO	NO

Password	First/last name	Date of birth	Address	Phone number	Credit card	SSN	IP Address
Data exposed	--	--	--	--	--	--	--

This database leak was found being spread on a clearnet 'Hacker’s Forum'. Very little is known about this hack and as such is considered unverified. More information will be added about this leak as it comes available.

Contact us at info@joe.black for more information