
CONFIDENTIAL EXPOSURE REPORT

Breach & credential exposure assessment

Prepared for

example.com

DATE

12 Oct 2026

REPORT ID

8799a434

SEVERITY

CRITICAL

DATASETS

9

PREPARED BY

Leaked.Domains

Executive summary

823,015

EXPOSED RECORDS

72,417

ACTIVE COMPROMISE

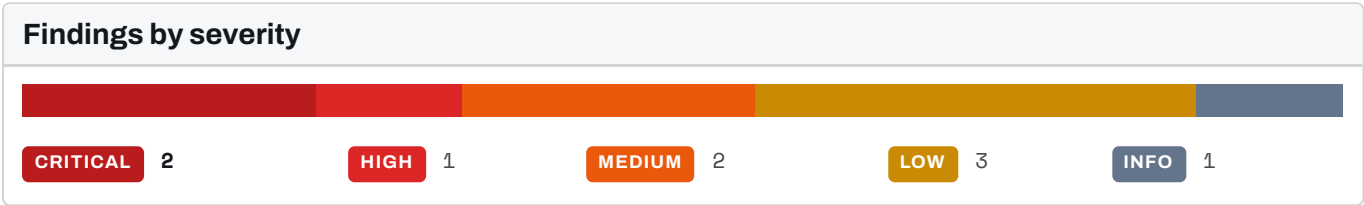
290

DISTINCT BREACHES

9

DATASETS AFFECTED

Searching example.com across every dataset returned **823,015 records** spanning **290 distinct breaches**. Of these, **72,417 came from infostealer logs**: credentials taken from infected machines rather than from a breached website. That is evidence of a live compromise and is where remediation should start.



Exposure at a glance				
DATASET	CLASSIFICATION	SEVERITY	RECORDS	BREACHES
Infostealer credentials	Active compromise	CRITICAL	50,168	1
Combolist credentials (ULP)	Active compromise	CRITICAL	22,249	1
Leaked credentials	Historical exposure	HIGH	408,797	246
LinkedIn profiles	Historical exposure	MEDIUM	398	3
Personal records	Historical exposure	MEDIUM	257,019	34
TLS certificates	Attack surface	LOW	326	1
DNS records	Attack surface	LOW	76,624	2
Subdomains	Attack surface	LOW	260	-
Domain registration	Attack surface	INFO	7,174	2
Facebook profiles	NO EXPOSURE FOUND		0	-

A dataset listed as “no exposure found” was searched and returned nothing. It is reported rather than omitted, because knowing a dataset is clean is itself a result.

Findings, impact and recommended action

Ordered by severity. Each finding states what was found, why it matters, and the action it calls for.

Infostealer credentials

CRITICAL 50,168

These credentials were taken from infected machines, not from a breached website. The password was saved in a browser on a host someone controls, so treat the host as compromised and the credential as known-good to an attacker.

Unique email addresses	With a cleartext password	Named breaches
12,058	49,030	1

Action: Reset these credentials, revoke their sessions, and get the affected hosts reimaged. Session cookies stolen alongside them defeat a password reset on its own.

Combolist credentials (ULP)

CRITICAL 22,249

These credentials come from combolists (URL, login and password lines compiled from infostealer logs). The login and password were valid for the site shown at some point, but the list does not say which machine they came from.

Unique email addresses	With a cleartext password	Named breaches
7,307	22,249	1

Action: Reset these credentials, revoke their sessions, and check those accounts for sign-ins you do not recognise. Treat reused passwords as exposed everywhere they are used.

Leaked credentials

HIGH 408,797

Email addresses and passwords for this domain are in circulation. Any that are still valid, or reused on corporate systems, allow direct account takeover.

Unique email addresses	With a cleartext password	Named breaches
272,427	227,523	246

Action: Force a reset for every address listed and block reuse of the exposed passwords.

LinkedIn profiles

MEDIUM 398

Names, roles and locations tied to corporate addresses let an attacker pick a plausible sender and a plausible target for business email compromise.

Unique email addresses	Named breaches
356	3

Action: Treat the named staff as elevated phishing risk and verify payment or access changes out of band.

Personal records

MEDIUM 257,019

Personal detail attached to corporate addresses is the raw material for targeted phishing and for answering account recovery questions.

Unique email addresses	Named breaches
213,117	34

Action: Fold these addresses into phishing awareness training and stop using knowledge-based answers for account recovery.

TLS certificates

LOW 326

Certificate transparency is public and permanent. Every hostname ever certified is listed here, which routinely surfaces internal and staging names the owner believed were private.

Named breaches

1

Action: Review the hostnames for names that were never meant to be public, and watch for certificates issued for your domain by anyone else.

DNS records

LOW 76,624

Resolved records map the externally reachable estate, including hosting providers and netblocks an attacker can enumerate.

Named breaches

2

Action: Remove records pointing at decommissioned hosts; a dangling record invites subdomain takeover.

Subdomains

LOW 260

Each name is a reachable entry point. Forgotten staging and administrative hosts are the ones that go unpatched.

Action: Confirm every name is intended to be public and retire the ones that are not.

Domain registration

INFO 7,174

Registration contacts are a named route to the people who can transfer the domain.

Unique registrant addresses

652

Named breaches

2

Action: Use registrar privacy and a role address, and enable transfer lock.

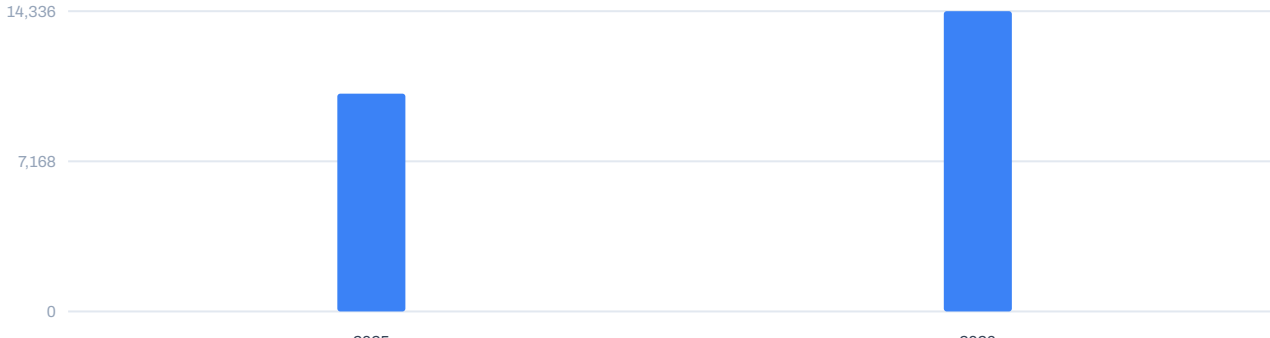
Findings by dataset

In the order requested. Each panel says whether it is evidence of active compromise, historical exposure, or attack surface.

Infostealer credentials

CRITICALACTIVE COMPROMISE50,168

Records by year



Year	Records
2025	7,168
2026	14,336

How the passwords were stored

No password

50,168100.0%



Sample records

15 of 50,168 records. Passwords and phone numbers are masked; the full values are in the CSV export.

EMAIL ADDRESS	PASSWORD	SITE	STEALER
isabela.costa@example.com	*****	https://mail.example.com	chrome default (133.0.6943.142)
mathieu.bernard@example.com	*****	https://mail.example.com	chrome default (133.0.6943.142)
kadmin/admin@example.com	*****	http://n001.hdfs.example.com:8080	google chrome default
jakub.nowak@example.com	*****	http://mail.example.com	chrome default (133.0.6943.142)
kamil.nowak@example.com	*****	https://mail.example.com	chrome default (133.0.6943.142)
carlos.gomez@example.com	*****	https://mail.example.com	chrome default (133.0.6943.142)
admin@example.com	*****	https://suseai.example.com	mozilla firefox
aleksandra.kowalska@example.com	*****	https://example.com	chrome default (133.0.6943.142)
alejandrof@example.com	*****	https://mail.example.com	chrome default (133.0.6943.142)

EMAIL ADDRESS	PASSWORD	SITE	STEALER
marie.dupont@example.com		https://mail.example.com	chrome default (133.0.6943.142)
jakub.nowak@example.com		https://mail.example.com	chrome default (133.0.6943.142)
lucas.silva@example.com		https://mail.example.com	chrome default (133.0.6943.142)
hiroko.saito@example.com		https://example.com	chrome default (133.0.6943.142)
admin@example.com		https://suseai.example.com	mozilla firefox
johndoe@example.com		https://www.example.com	chrome default (133.0.6943.142)

Breaches contributing to this dataset

BREACH	DATE	STORED AS	RECORDS	FLAGS
Info Stealer Logs (legacy)	2019-2025	None	50,168	VERIFIED SENSITIVE

Combolist credentials (ULP)

CRITICALACTIVE COMPROMISE22,249

Records by year

Year	Records
2025	22,249

How the passwords were stored

No password

22,249100.0%

Category	Count	Percentage
No password	22,249	100.0%

Sample records

15 of 22,249 records. Passwords and phone numbers are masked; the full values are in the CSV export.

EMAIL ADDRESS	PASSWORD	SITE
nitin@example.com		http://example.com/campanha floorestquickstep/register.php
sarah.gelade@example.com		https://.example.com
-		http://gateway.example.com/loginpages/login.shtml

EMAIL ADDRESS	PASSWORD	SITE
-		http://gkbhjp.example.com/loginpages/login.shtml
-		http://gateway.example.com/loginpages/login.shtml
-		https://gateway.example.com/loginpages/login.shtml
-		http://gateway.example.com/login.shtml
-		https://gateway.example.com/loginpages/login.shtml
-		http://gateway.example.com/loginpages/login.shtml
-		https://gateway.example.com/loginpages/login.shtml
-		http://gateway.example.com/loginpages/login.shtml
v852avithas.es		http://gateway.example.com/loginpages/login.shtml
-		http://gateway.example.com/loginpages/userlogin.shtml
-		http://apps.example.com
-		http://gateway.example.com/loginpages/login.shtml

Breaches contributing to this dataset

BREACH	DATE	STORED AS	RECORDS	FLAGS
ULP Combolists	2019-2025	None	22,249	VERIFIED SENSITIVE

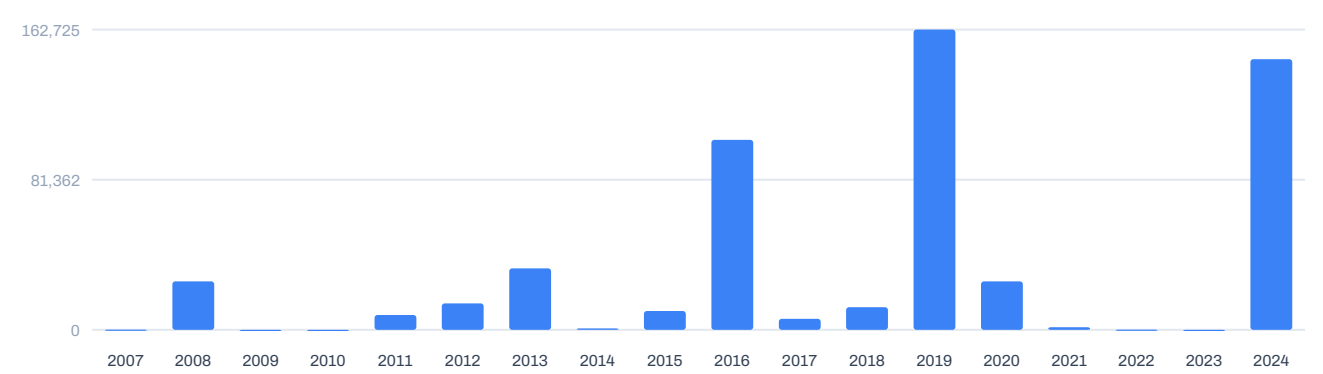
Leaked credentials

HIGH

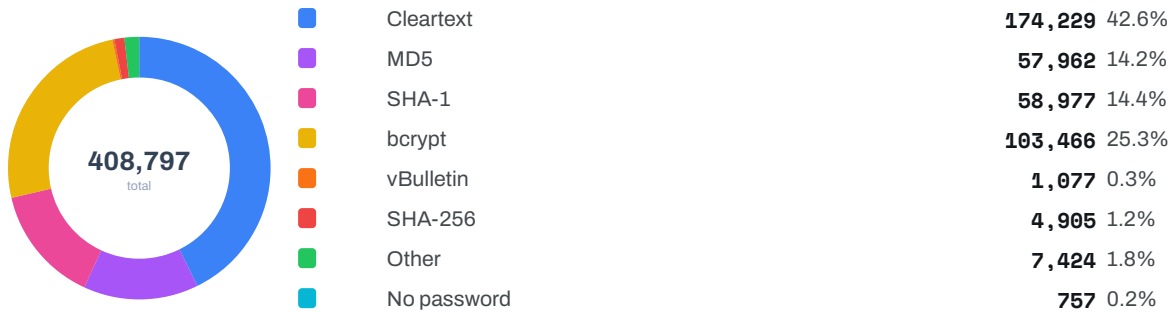
HISTORICAL EXPOSURE

408,797

Records by year



How the passwords were stored



64 of these breaches stored passwords in cleartext, so those credentials need no cracking at all.

Sample records

15 of 408,797 records. Passwords and phone numbers are masked; the full values are in the CSV export.

EMAIL ADDRESS	USERNAME	PASSWORD	BREACH
rahavendra2015@example.com	rahavendra2015		CompDB
rahbarnikky@example.com	rahbarnikky		CompDB
ruby_z_satur@example.com	ruby_z_satur	-	CompDB
rsb92402@example.com	rsb92402	-	CompDB
rrusta@example.com	rrusta		CompDB
root@example.com	root		CompDB
rheegan@example.com	rheegan		CompDB
rishata@example.com	rishat	-	CompDB
rejkfewahgfe@example.com	rejkfewahgfe		CompDB
roffk@example.com	roffk		CompDB
rahbar1994example@example.com	rahbar1994example		CompDB
r3play@example.com	r3play	-	CompDB
raymondpwood@example.com	raymondpwood	-	CompDB
rded4ws@example.com	rded4ws		CompDB
ranavaya_dinesh@example.com	ranavaya_dinesh		CompDB

Breaches contributing to this dataset

BREACH	DATE	STORED AS	RECORDS	FLAGS
CompDB	2019-2024	Cleartext	143,070	
DailyMotion.com	2016	Bcrypt	77,251	VERIFIED
MySpace.com	2008	SHA1	26,286	VERIFIED
Zynga.com	2019	MD5	15,635	VERIFIED
AdultFriendFinder.com	2016	SHA1	14,335	VERIFIED SENSITIVE
Badoo.com	2013	MD5	13,784	SENSITIVE
Disqus.com	2012	SHA1	12,816	VERIFIED
Minted.com	2020	BCrypt	10,193	VERIFIED

BREACH	DATE	STORED AS	RECORDS	FLAGS
Wattpad.com	2020	Bcrypt	8,199	VERIFIED
iMesh.com	2013	MD5	7,630	VERIFIED
InterPals.net	2015	MD5	5,615	VERIFIED
Dubsmash.com	2018	SHA256/Cleartext	4,807	VERIFIED
Adobe.com	2013	3DES	4,307	VERIFIED
VK.com	2013	Cleartext	3,679	VERIFIED
Myheritage.com	2017	Cleartext	3,205	
1win	2024	Sha256	3,111	VERIFIED
Fling.com	2011	Cleartext	3,058	VERIFIED SENSITIVE
Mate1.com	2016	Cleartext	2,914	VERIFIED SENSITIVE
Showing the 18 largest of 246 breaches. The full list is in the appendix.				

LinkedIn profiles

MEDIUM

HISTORICAL EXPOSURE

398

Records by year

Year	Records
2018	136
2019	136
2021	136

Sample records

15 of 398 records.

EMAIL ADDRESS	FIRST NAME	LAST NAME	LOCATION	BREACH
rtg6wy8wly@example.com	PSEUDO	FAKERSON	los angeles, california, united states	PDL (People Data Labs)
rayt86@gmail.com, blah@example.com, tray@cactusgroup.com	TREVOR	RAY	mountain view, california, united states	PDL (People Data Labs)
kevinfray@example.com	KEVIN	RAY	lakeland, florida, united states	PDL (People Data Labs)
belma-demirci@example.com	BELMA	DEMIRCI	-	LinkedIn Scrape
parentoo@example.com	SVENJA	KOTESKO	berlin, berlin, germany	PDL (People Data Labs)
mexico@example.com	PO	PO	-	Apollo v5 (Personal)

EMAIL ADDRESS	FIRST NAME	LAST NAME	LOCATION	BREACH
muti_muti@example.com	KERIM	SARI	turkey	PDL (People Data Labs)
meg_galicia@example.com, grace.esmilla@philips.com	GRACE	ESMILLA	taiwan	PDL (People Data Labs)
daky_good@example.com	JESUS	BONILLA	-	LinkedIn Scrape
daky_good@example.com	JESUS	BONILLA	oaxaca, mexico	PDL (People Data Labs)
germanlarrainm@gmail.com, glarrain@example.com, german.larrain@larrainvial.com	GERMÁN	LARRAÍN	-	LinkedIn Scrape
e.g.tana08241@example.com	POP	PORPAISAL	tailândia, para, brazil	PDL (People Data Labs)
ksjdkajdkajdkasjd@example.com	JOHN	DOE	-	Apollo v5 (Personal)
kemo_a.n@example.com	KEMO	AMR	saudi arabia	PDL (People Data Labs)
kickervsalpine@example.com	JAMES	BARTOLO	malta	PDL (People Data Labs)
Breaches contributing to this dataset				
BREACH	DATE	STORED AS	RECORDS	FLAGS
Apollo v5 (Personal)	2018	None	136	
LinkedIn Scrape	2021	None	132	
PDL (People Data Labs)	2019	None	130	

Personal records

MEDIUMHISTORICAL EXPOSURE257,019

Records by year

Year	Records
2015	0
2016	0
2017	0
2018	0
2019	249,180
2020	0
2021	0
2022	0
2023	0
2024	0
2025	0

Sample records

15 of 257,019 records.

EMAIL ADDRESS	USERNAME	BREACH
cowgirlsaddleup1@aol.com, random_7999654569@example.com	cowgirlsaddleup1, random_7999654569	USA 280m Homeowners

EMAIL ADDRESS	USERNAME	BREACH
cathyconlon@example.com	cathyconlon	Verifications.io
carlosparkman@example.com	carlosparkman	Verifications.io
constancesklein@example.com	constancesklein	Verifications.io
cd@example.com	cd	Verifications.io
canyete-navarro@example.com	canyete-navarro	Verifications.io
chivugomez@example.com	chivugomez	Verifications.io
customer@example.com	customer	Verifications.io
cleyton_silva@example.com	cleyton_silva	Verifications.io
csadvorb3ly@example.com	csadvorb3ly	Verifications.io
claricethivierge@example.com	claricethivierge	Verifications.io
chrisghunt@example.com	chrisghunt	Verifications.io
colleencgorham@example.com	colleencgorham	Verifications.io
clint@example.com	clint	Verifications.io
ccc-mlc-tac@example.com	ccc-mlc-tac	Verifications.io

Breaches contributing to this dataset				
BREACH	DATE	STORED AS	RECORDS	FLAGS
ApexSMS (MobileDrip)	2019	None	235,449	
Verifications.io	2019	None	13,291	VERIFIED
Twitter2025	2025	None	3,135	VERIFIED
Airtel (India)	2024	None	949	
Vodafone (India)	2024	None	703	
Idea Cellular (India)	2024	None	549	
Luxottica.com	2021-03-16	None	481	VERIFIED
Reliance_Jio (India)	2017	None	404	
VBT.ru	2024	MD5	390	
AT&T	2024	None	188	VERIFIED
Tata_Docomo (India)	2024	None	186	
USA 280m Homeowners	2019	None	178	VERIFIED
VietnamAirlines	2025	None	177	VERIFIED
US 185M Cell Phones 2019	2019	None	150	VERIFIED
BSNL_Mobile (India)	2024	None	147	
ModernBusinessSolutions	2016	None	133	VERIFIED
China People Data	unknown	None	86	SENSITIVE
Email2Name	2017	None	82	

Showing the 18 largest of 34 breaches. The full list is in the appendix.

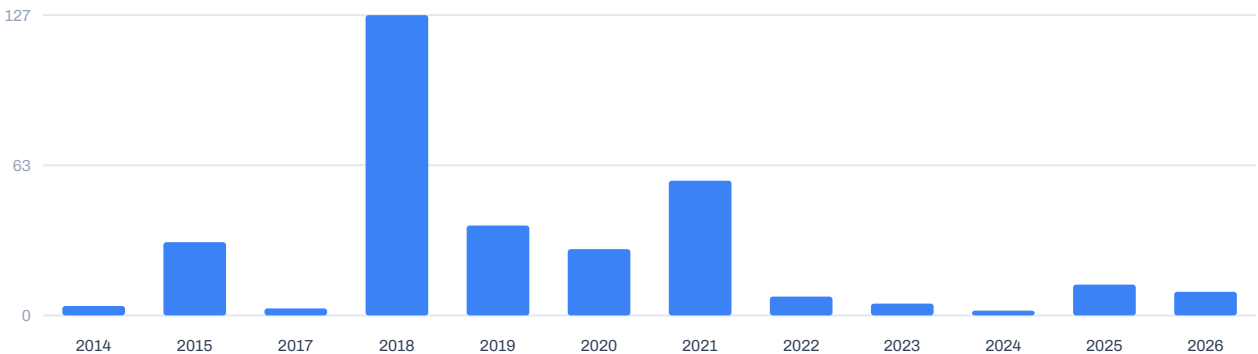
TLS certificates

LOW

ATTACK SURFACE

326

Records by year



Sample records

15 of 326 records.

ORGANISATION	COVERS	VALID FROM	EXPIRES
GMO GlobalSign K.K.	example.com	2017-11-13T07:16:44	2018-11-14T07:16:44
GMO GlobalSign K.K.	example.com	2017-12-14T09:11:12	2018-11-03T05:44:04
GMO GlobalSign K.K.	example.com	2017-11-02T05:44:04	2018-11-03T05:44:04
Internet Corporation for Assigned Names and Numbers	www.example.org, example.com, example.edu, example.net (+4 more)	2018-11-28T00:00:00	2020-12-02T12:00:00
Example	test29310038.example.com	2018-06-07T08:34:26	2020-06-30T14:59:59
,Example	test29310029.example.com, www.test29310029.example.com	2018-06-07T08:53:22	2020-06-30T14:59:59
Example	test29310003.example.com	2018-06-07T08:32:14	2020-06-30T14:59:59
Example	test29310027.example.com	2018-06-07T08:33:45	2020-06-30T14:59:59
Example	test29310040.example.com, www.test29310040.example.com	2018-06-07T08:54:07	2020-06-30T14:59:59
Ceska posta	www.example.com	2018-04-27T07:47:12	2020-05-16T07:47:12
,Example	test29310006.example.com	2018-06-07T08:32:25	2020-06-30T14:59:59
Ceska posta	www.example.com	2018-05-02T07:32:03	2020-05-21T07:32:03
Example	test29310022.example.com	2018-06-07T08:33:27	2020-06-30T14:59:59
,Example	test29310032.example.com	2018-06-07T08:34:03	2020-06-30T14:59:59
Example	test29310009.example.com	2018-06-07T08:32:36	2020-06-30T14:59:59

Breaches contributing to this dataset

BREACH	DATE	STORED AS	RECORDS	FLAGS
Certificates	2022	None	326	VERIFIED

DNS records

LOW

ATTACK SURFACE

76,624

No year trend available: timestamp indexed as text, not a date.

Sample records

15 of 76,624 records.

HOST	TYPE	RESOLVES TO	NETWORK
www.example.com	aaaa	2606:2800:220:1:248:1893:25c8:1946	EDGECAST
thisisan.example.com	ptr	161.167.229.200	WAL-MART4
do1.example.com	ptr	165.227.187.232	DIGITALOCEAN-ASN
sub-09.example.com	ptr	165.227.139.66	DIGITALOCEAN-ASN
ucp-manager-0.example.com	ptr	165.227.182.71	DIGITALOCEAN-ASN
ucp-node-0.example.com	ptr	165.227.188.165	DIGITALOCEAN-ASN
zuhoerer.example.com	ptr	46.148.26.228	Infium, UAB
eenvobilling.example.com	ptr	46.148.26.44	Infium, UAB
lwrighty91.example.com	ptr	46.148.26.91	Infium, UAB
kostia20072007.example.com	ptr	46.17.104.101	First Server Limited
viktor167801.example.com	ptr	46.17.104.15	First Server Limited
mark1.malmberg.example.com	ptr	46.17.104.165	First Server Limited
fasdwt285183.example.com	ptr	46.17.105.107	First Server Limited
tempbelmail.example.com	ptr	46.17.105.115	First Server Limited
bobgrudin.example.com	ptr	46.17.105.155	First Server Limited

Breaches contributing to this dataset

BREACH	DATE	STORED AS	RECORDS	FLAGS
1f6132c5ae0c (not catalogued)	-	-	76,622	
1ffe024393ca (not catalogued)	-	-	2	

Subdomains

LOW

ATTACK SURFACE

260

No year trend available: no date field.

Sample records

15 of 260 records.

SUBDOMAIN	LABEL
kzumberg18031.example.com	kzumberg18031
achrafnawras.example.com	achrafnawras
adm.example.com	adm
blackforest5.example.com	blackforest5
cr3w.nnov.example.com	cr3w.nnov
oleg.derimedved.example.com	oleg.derimedved
red1m1t.example.com	red1m1t
example4241.example.com	example4241

SUBDOMAIN	LABEL
deltel.example.com	deltel
p2pygtyb4f.example.com	p2pygtyb4f
seregavsv.example.com	seregavsv
timushev.r87.example.com	timushev.r87
x82.sultanov.example.com	x82.sultanov
nimab007.example.com	nimab007
nickyaristov2.example.com	nickyaristov2

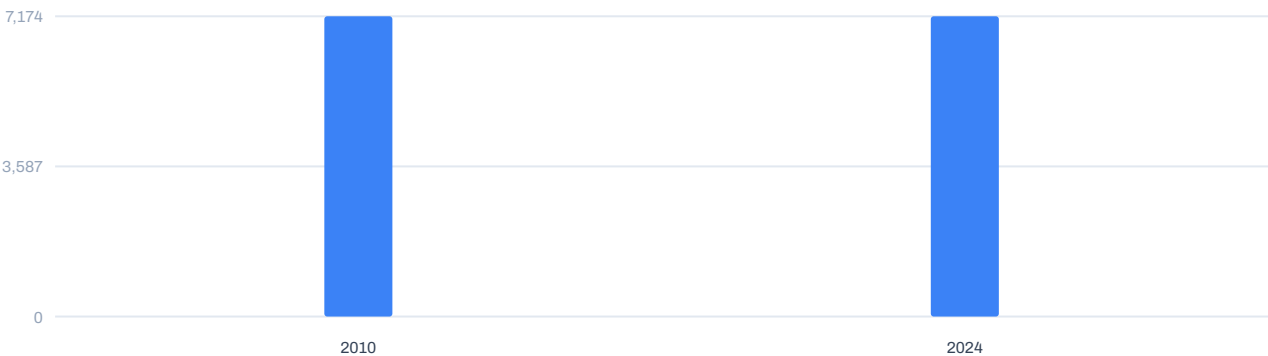
Domain registration

INFO

ATTACK SURFACE

7,174

Records by year



Sample records

15 of 7,174 records.

DOMAIN	REGISTRANT EMAIL	COUNTRY	NAMESERVERS
hpicheck.mobi	privatedomain@example.com	UNITED KINGDOM	NS67.1AND1.CO.UK, NS68.1AND1.CO.UK
hgdev-484.com	test.user@example.com	US	NS1.HOSTGATOR.COM, NS2.HOSTGATOR.COM
hgdev-226.com	test.user@example.com	US	NS1.HOSTGATOR.COM, NS2.HOSTGATOR.COM
girlpowerzone.com	invalid@example.com, tech@moniker.com	United States	NS1.MONIKERDNS.NET, NS2.MONIKERDNS.NET (+2 more)
gfgfhfghgfhfghg.com	dns@surf-town.net, dfsfhghghgh44@example.co m	Denmark	NS1.REGISTRANT- VERIFICATION.COM, NS2.REGISTRANT- VERIFICATION.COM
hgfhghgfhghfg.com	dns@surf-town.net, dfsfhghghgh44@example.co m	Denmark	NS1.REGISTRANT- VERIFICATION.COM, NS2.REGISTRANT- VERIFICATION.COM
goindnfkdfdfdnfdkdkdffjfdjf dfdf.com	dns@surf-town.net, sampletetetgdfg@example .com	India	NS1.REGISTRANT- VERIFICATION.COM, NS2.REGISTRANT- VERIFICATION.COM
gmoqr.com	invalid@example.com, tech@moniker.com	United States	NS1.MONIKERDNS.NET, NS2.MONIKERDNS.NET (+2 more)

DOMAIN	REGISTRANT EMAIL	COUNTRY	NAMESERVERS	
hghfsdhghfggsdhsdgsd44ddd.com	hsdhhhjghjg@example.com, dns@surf-town.net	Denmark	NS1.REGISTRANT-VERIFICATION.COM, NS2.REGISTRANT-VERIFICATION.COM	
gregdfgfdgfdgdfg.com	ppppp@example.com	SINGAPORE	NS1.REGISTRANT-VERIFICATION.COM, NS2.REGISTRANT-VERIFICATION.COM	
gpsten.net	josephmhurta@example.com	UNITED STATES	-	
inviq.net	invalid@example.com	UNITED STATES	NS2.MONIKERDNS.NET, NS3.MONIKERDNS.NET (+1 more)	
gharyb.com	customer@example.com	NETHERLANDS	NS1.YOURSRS.COM, NS2.YOURSRS.COM	
garywingking.com	johnsmith@example.com	UNITED STATES	-	
houseofdarcia.com	reynolds@example.com	SWITZERLAND	-	
Breaches contributing to this dataset				
BREACH	DATE	STORED AS	RECORDS	FLAGS
Whois Source 1	2010-2024	None	6,947	
Whois Source 3	2010-2024	None	227	

Infostealer credentials: password analysis

Measured over a random sample of **5,000** recovered passwords from 50,168 records. Rates generalise to the whole set; the counts are the sample's own.

What the passwords look like

Passwords over 9 characters

1,121

22.4% of sample

Contains the organisation name

6

0.1% of sample

Among the 60 most common passwords

120

2.4% of sample

Contains keyboard walking

155

3.1% of sample

Contains a month, day or year

236

4.7% of sample

Length distribution

4 chars

41.1% (2,055)

8 chars

18.5% (927)

6 chars

5.7% (284)

10 chars

5.4% (271)

9 chars

4.9% (247)

Character sets

lower_alpha_num

51.1% (2,554)

numeric

15.9% (793)

lower_alpha

13.3% (663)

mixed_alpha_num

5.0% (250)

all

4.4% (222)

Most common structures

Hashcat mask notation

?d?d?d?d

6.1% (305)

?1?1?1?1

3.5% (176)

?d?d?d?d?d?d?d?d

2.7% (133)

?d?1?d?d

2.7% (133)

?1?1?1?d

2.4% (122)

?l lowercase, ?u uppercase, ?d digit, ?s symbol. A structure shared by many passwords is a structure an attacker can target directly.

Combolist credentials (ULP): password analysis

Measured over a random sample of **5,000** recovered passwords from 22,249 records. Rates generalise to the whole set; the counts are the sample's own.

What the passwords look like

Passwords over 9 characters

1,749

35.0% of sample

Contains the organisation name

40

0.8% of sample

Among the 60 most common passwords

391

7.8% of sample

Contains keyboard walking

312

6.2% of sample

Contains a month, day or year

231

4.6% of sample

Length distribution

4 chars

29.9% (1,481)

8 chars

18.0% (891)

10 chars

8.3% (410)

6 chars

7.4% (368)

9 chars

6.8% (336)

Character sets

lower_alpha_num

41.3% (2,046)

numeric

15.8% (782)

lower_alpha

14.2% (706)

mixed_alpha_num

8.3% (410)

all

8.2% (404)

Most common structures

Hashcat mask notation

?d?d?d?d

5.3% (263)

?d?d?d?d?d?d

4.1% (204)

?1?1?1?1

3.3% (165)

?1?1?1?1?1?1?1?1

2.9% (144)

?1?1?1?1?1

2.2% (109)

?l lowercase, ?u uppercase, ?d digit, ?s symbol. A structure shared by many passwords is a structure an attacker can target directly.

Leaked credentials: password analysis

Measured over a random sample of **5,000** recovered passwords from 408,797 records. Rates generalise to the whole set; the counts are the sample's own.

What the passwords look like		
Passwords over 9 characters	2,175	43.5% of sample
Contains the organisation name	79	1.6% of sample
Among the 60 most common passwords	364	7.3% of sample
Contains keyboard walking	464	9.3% of sample
Contains a month, day or year	119	2.4% of sample

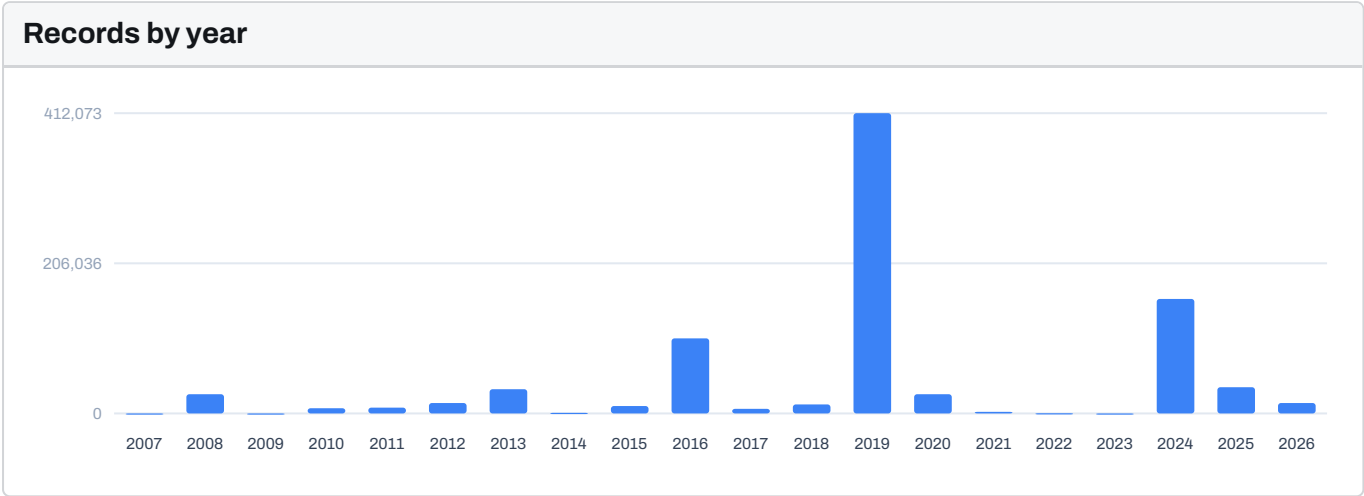
Length distribution		
8 chars		22.4% (1,079)
6 chars		17.9% (864)
9 chars		13.6% (656)
7 chars		13.4% (643)
10 chars		13.3% (639)

Character sets		
lower_alpha_num		40.1% (1,931)
numeric		23.9% (1,150)
lower_alpha		18.9% (912)
mixed_alpha_num		4.0% (193)
lower_alpha_special_num		3.6% (174)

Most common structures		Hashcat mask notation
?d?d?d?d?d?d		7.8% (376)
?1?1?1?1?1?1?1?1		5.3% (256)
?d?d?d?d?d?d?d?d?d		5.1% (245)
?1?1?1?1?1?1		3.8% (185)
?d?d?d?d?d?d?d?d?d?d		3.0% (143)
?l lowercase, ?u uppercase, ?d digit, ?s symbol. A structure shared by many passwords is a structure an attacker can target directly.		

Exposure over time

When the data behind these findings was disclosed or captured, across every dataset that carries a date.



YEAR	RECORDS
2,025	35,974
2,026	14,346
2,019	412,073
2,024	157,022
2,016	103,056
2,008	26,286
2,013	33,302
2,012	14,372
2,020	26,273
2,015	10,237
2,018	12,495
2,017	6,448
2,011	7,976
2,021	2,102
2,014	802
2,022	147
2,007	79
2,009	35
2,010	7,178
2,023	111

Breach source details

Every breach contributing to this report, largest first. 2 source(s) are not yet catalogued and are shown by identifier.

ApexSMS (MobileDrip)

235,449

Date	Passwords stored as	Category	Data exposed
2019	None	Marketing	Full names, Email addresses, Physical addresses, IP addresses, Phone numbers

In approximately April 2019, the cloud based sms platform ApexSMS (Also known as "MobileDrip") suffered a data breach that exposed 88 million entries. The breach included Full names, Email addresses, Physical addresses, IP addresses and Phone numbers.

CompDB

143,070

Date	Passwords stored as	Category	Data exposed
2019-2024	Cleartext	Comp	Email addresses, Passwords

This is a compilation of numerous untitled and unsorted email:password leaks. This data was cleaned up, parsed, and imported into Leaked.Domains. Only email:password combinations that did not already exists in the original CompDB are included here. This leak includes data from multiple compilation leaks including: 12billion XXS.is, BreachComp, CompilationOfManyBreaches or COMB, NewCompList, AP MYR & ZABUGOR, Collection 1-5, MasterComp, Pemiblanca as well a...

DailyMotion.com

VERIFIED 77,251

Date	Passwords stored as	Category	Data exposed
2016	Bcrypt	Entertainment	Email addresses, Passwords, Usernames

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.

1f6132c5ae0c

76,622

Info Stealer Logs (legacy)

VERIFIED SENSITIVE 50,168

Date	Passwords stored as	Category	Data exposed
2019-2025	stored as None	Info Stealer Logs	Email addresses, IP addresses, Names, Passwords, Phone Numbers, Credit Card Numbers, Social Security Numbers

Info Stealer Logs are a collection of dumped data found in hacker dark/deep/clear website and, more commonly, on encrypted messaging applications such as Telegram. These logs are gathered when a device such as a smart phone or computer are infected with stealer malware. Usually hidden inside game "cheat" software (used to cheat in many popular computer games) or in program cracks (used to bypass cd key or registration requirements), once the malicious fil...

MySpace.com

VERIFIED 26,286

Date	Passwords stored as	Category	Data exposed
2008	SHA1	Social	Email addresses, Passwords, Usernames

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.

ULP Combolists

VERIFIED**SENSITIVE****22,249**

Date	Passwords stored as	Category	Data exposed
2019-2025	None	ULP Combolists	URLs, Usernames, Passwords

ULP (URL / Login / Password) combolists compiled from info-stealer output. Each line pairs a site with the login and password used on it; there is no host or log behind a line.

Zynga.com

VERIFIED**15,635**

Date	Passwords stored as	Category	Data exposed
2019	MD5	Gaming	Email addresses, Passwords, Phone numbers, Usernames

In September 2019, game developer Zynga suffered a data breach. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes.

AdultFriendFinder.com

VERIFIED**SENSITIVE****14,335**

Date	Passwords stored as	Category	Data exposed
2016	SHA1	Dating	Email addresses, Passwords, Usernames

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

Badoo.com

SENSITIVE**13,784**

Date	Passwords stored as	Category	Data exposed
2013	MD5	Dating	Dates of birth, Email addresses, Genders, Names, Passwords, Usernames

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.

Verifications.io

VERIFIED**13,291**

Date	Passwords stored as	Category	Data exposed
2019	None	Aggregated Data	Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

In February 2019, the data aggregator service Verifications.io suffered a data breach. The breach was caused by an exposed MongoDB service which was accessible without authentication. This resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders.

Disqus.com

VERIFIED**12,816**

Date	Passwords stored as	Category	Data exposed
2012	SHA1	Social	Email addresses, Passwords, Usernames

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.

Minted.com

VERIFIED 10,193

Date	Passwords stored as	Category	Data exposed
2020	BCrypt	Market	Email addresses, Names, Passwords, Phone numbers, Physical addresses

In May 2020, the online marketplace for independent artists Minted suffered a data breach that exposed 4.4M unique customer records subsequently sold on a dark web marketplace. Exposed data also included names, physical addresses, phone numbers and passwords stored as bcrypt hashes.

Wattpad.com

VERIFIED 8,199

Date	Passwords stored as	Category	Data exposed
2020	BCrypt	Social	Bios, Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Names, Passwords, Social media profiles, Use

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

iMesh.com

VERIFIED 7,630

Date	Passwords stored as	Category	Data exposed
2013	MD5	Music	Email addresses, IP addresses, Passwords, Usernames

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.

Whois Source 1

6,947

Date	Passwords stored as	Category	Data exposed
2010-2024	as None	Whois Data	Email Address, Phone Numbers, Registrant Name, Registration Address, Registered Domain

This is a mostly complete database of newly registered Whois Data for domains registered between 2010 and 2024. This data comes from source 1 Whois Data.

InterPals.net

VERIFIED 5,615

Date	Passwords stored as	Category	Data exposed
2015	MD5	Social	Dates of birth, Email addresses, Geographic locations, Names, Passwords, Usernames

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.

Dubsmash.com

VERIFIED 4,807

Date	Passwords stored as	Category	Data exposed
2018	as SHA256/Cleartext	Social/Video	Email addresses, Geographic locations, Names, Passwords, Phone numbers, Spoken languages, Usernames

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.

Adobe.com

VERIFIED 4,307

Date	Passwords stored as	Category	Data exposed
2013	3DES	Software	Email addresses, Password hints, Passwords, Usernames

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.

VK.com

VERIFIED 3,679

Date	Passwords stored as	Category	Data exposed
2013	Cleartext	Social	Email addresses, Names, Passwords, Phone numbers

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.

Myheritage.com

3,205

Date	Passwords stored as	Category	Data exposed
2017	Cleartext	Genealogy	Email addresses, Passwords

In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more br...

Twitter2025

VERIFIED 3,135

Date	Passwords stored as	Category	Data exposed
2025	None	Social	Email Address, Name, Username, Phone Number

In 2025, a scrap of Twitter was leaked on multiple hacker forums and media sharing channels.

1win

VERIFIED 3,111

Date	Passwords stored	Category	Data exposed
2024	as	Gambling	Email addresses, Phone Number, IP addresses, Passwords, Usernames, Date of Birth, Name,
4	Sha256	g	Location

In November 2024, the gambling site 1win was allegedly hacked and its database was found being shared in hacker forums and channels. The leak contained multiple files including a user database that included over 94 million entries, a partners database, and some configuration data.

Fling.com

VERIFIED SENSITIVE 3,058

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	Dating	Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Passwords, Phone numbers, Sexual fetishes, Sexual

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.

Mate1.com

VERIFIED**SENSITIVE****2,914**

Date	Passwords stored as	Category	Data exposed
2016	stored as 6 Cleartext	Dating	Astrological signs, Dates of birth, Drinking habits, Drug habits, Education levels, Email addresses, Ethnicities, Fitness levels

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.

Zoosk.com

SENSITIVE**2,562**

Date	Passwords stored as	Category	Data exposed
2011	MD5	Dating	Email addresses, Passwords

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.

NitroPDF

VERIFIED**2,463**

Date	Passwords stored as	Category	Data exposed
2020	Bcrypt	Service	Email addresses, Names, Passwords

In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents.

Evony.com

VERIFIED**2,049**

Date	Passwords stored as	Category	Data exposed
2016	MD5/Cleartext	Gaming	Email addresses, IP addresses, Passwords, Usernames

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).

Neopets.com

VERIFIED**2,029**

Date	Passwords stored as	Category	Data exposed
2013	as 3 Cleartext	Gaming	Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Names, Passwords, Usernames

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.

Dropbox.com

VERIFIED**1,833**

Date	Passwords stored as	Category	Data exposed
2016	BCrypt/SHA1	File Sharing	Email addresses, Passwords

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).

NetEase

1,453

Date	Passwords stored as	Category	Data exposed
2015	Cleartext	Social	Email addresses, Passwords

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.

Edmodo.com

VERIFIED 1,441

Date	Passwords stored as	Category	Data exposed
2017	Bcrypt	Education	Email addresses, Passwords, Usernames

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.

AshleyMadison.com

VERIFIED SENSITIVE 1,427

Date	Passwords stored as	Category	Data exposed
2015	Bcrypt	Dating	Dates of birth, Email addresses, Ethnicities, Genders, Names, Passwords, Payment histories, Phone numbers, Physical addresses, S

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...

Sitepoint.com

VERIFIED 1,350

Date	Passwords stored as	Category	Data exposed
2020	BCrypt	Social	Bios, Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Names, Passwords, Social media profiles, Use

In late December 2020, a database claiming to be from learnable.com (which currently redirects to sitepoint.com) was discovered being sold on hacker forums. Sitepoint confirmed the hack in early February 2021 claiming the breach happened by a third-party and non-sensitive customer data was accessed.

LBSG.net

VERIFIED 1,319

Date	Passwords stored as	Category	Data exposed
2016	MD5	Gaming	Email addresses, Passwords, Usernames

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.

Animoto.com

VERIFIED 1,261

Date	Passwords stored as	Category	Data exposed
2018	SHA256	Video Editing	Dates of birth, Email addresses, Geographic locations, Names, Passwords

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.

Glofox.com

VERIFIED 1,058

Date	Passwords stored as	Category	Data exposed
2020	MD5	Fitness	Dates of birth, Email addresses, Genders, Names, Passwords, Phone numbers

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

Readnovel.com

995

Date	Passwords stored as	Category	Data exposed
2019	MD5	Novels	Email address, Password, Username

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.

Mathway.com

953

Date	Passwords stored as	Category	Data exposed
2020	MD5	Study	Device information, Email addresses, Names, Passwords, Social media profiles

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

Airtel (India)

949

Date	Passwords stored as	Category	Data exposed
2024	None	Telecom	Email addresses, Phone numbers, Physical addresses, Full Name

In July 2024, a threat actor ("xenZen") claimed to sell a database of ~375 million India telecom customers (phone numbers, email IDs, Aadhaar, addresses) in multiple files titled with different India Telecom companies. This portion of the leaked data was claimed to be from Airtel. Airtel investigated and stated no breach occurred. Marked as unverified/alleged.

Sharethis.com

838

Date	Passwords stored as	Category	Data exposed
2018	DES	Social	Dates of birth, Email addresses, Names, Passwords

In July 2018, the social bookmarking and sharing service ShareThis suffered a data breach. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly.

LinkedIn.com

VERIFIED 805

Date	Passwords stored as	Category	Data exposed
2012	SHA1	Social	Email addresses, Passwords

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.

Tumblr.com

VERIFIED 768

Date	Passwords stored as	Category	Data exposed
2013	SHA1	Social	Email addresses, Passwords

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.

MyFitnessPal.com

VERIFIED 766

Date	Passwords stored as	Category	Data exposed
2018	Cleartext	Fitness	Email addresses, IP addresses, Passwords, Usernames

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.

Xat.com

VERIFIED 765

Date	Passwords stored as	Category	Data exposed
2015	Crc32	Chatting	Email addresses, IP addresses, Passwords, Usernames, Website activity

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.

Clearvoicesurveys.com

VERIFIED 742

Date	Passwords stored as	Category	Data exposed
2021	as Cleartext	y Surveys	Dates of birth, Email addresses, Genders, IP addresses, Names, Passwords, Phone numbers, Physical addresses

In April 2021, the market research surveys company ClearVoice Surveys had a publicly facing database backup from 2015 taken and redistributed on a popular hacking forum. The data included 16M unique email addresses, names, physical and IP addresses, genders, dates of birth and plain text passwords. ClearVoice Surveys advised they were aware of the breach and confirmed its authenticity.

Peatix.com

732

Date	Passwords stored as	Category	Data exposed
2019	Cleartext	Productivity	Email addresses, Names, Passwords

In January 2019, the event organising platform Peatix suffered a data breach. The incident exposed 4.2M email addresses, names and salted password hashes.

Youku.com

VERIFIED 727

Date	Passwords stored as	Category	Data exposed
2016	MD5	Streaming	Email addresses, Passwords

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.

Vodafone (India)

703

Date	Passwords stored as	Category	Data exposed
2024	None	Telecom	Email Address, Full Name, Address, Phone Number, Birth Date

In July 2024, a threat actor ("xenZen") claimed to sell a database of ~375 million India telecom customers (phone numbers, email IDs, Aadhaar, addresses) in multiple files titled with different India Telecom companies. This portion of the leaked data was claimed to be from Vodafone.

Shopback.sg

VERIFIED 664

Date	Passwords stored as	Category	Data exposed
2020	SHA1	Retail	Email addresses, Geographic locations, Names, Passwords, Phone numbers

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

Canva.com

657

Date	Passwords stored as	Category	Data exposed
2019	Bcrypt	Design	Email addresses, Geographic locations, Names, Passwords, Usernames

In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins.

VimeWorld.ru

650

Date	Passwords stored as	Category	Data exposed
2018	MD5	Gaming	Email Address, Username, Password Hash, IP Address

Not much is known about this leak other than it showed up on a clearnet hacker forum in 2018. At least 3.3 million of the 5.2 million MD5 hashes were cracked at this time and available on the same forum.

Dodonew.com

591

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	Software	Email addresses, Usernames

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.

Leet.cc

VERIFIED 572

Date	Passwords stored as	Category	Data exposed
2016	SHA512	Gaming	Email addresses, IP addresses, Passwords, Usernames, Website activity

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.

Idea Cellular (India)

549

Date	Passwords stored as	Category	Data exposed
2024	None	Telecom	Email Address, Full Name, Address, Phone Number, Birth Date

In July 2024, a threat actor ("xenZen") claimed to sell a database of ~375 million India telecom customers (phone numbers, email IDs, Aadhaar, addresses) in multiple files titled with different India Telecom companies. This portion of the leaked data was claimed to be from Idea Cellular.

Luxottica.com

VERIFIED 481

Date	Passwords stored as	Category	Data exposed
2021-03-16	None	Retail	Full names, Birthdates, Email addresses, Home addresses, Phone numbers

In March 2021, Luxottica experienced a data breach that exposed personal information of over 70 million customers. The compromised data included full names, birthdates, email addresses, home addresses, and phone numbers. The breach was discovered on March 16, 2021, and the leaked data was subsequently found on various hacking forums between April 30 and May 12, 2023. An investigation revealed that the stolen database contained 305 million records, includi...

DailyQuiz.me

468

Date	Passwords stored as	Category	Data exposed
2021	MD5	Social	Email Addresses, Phone Number, IP Address, Birthdate, Gender

In 2021, the DailyQuiz Database, maintained by dailyquiz.me and accessible through thiscrush.com, suffered a significant data breach, exposing the personal information of over 8 million users.

Chegg.com

VERIFIED 456

Date	Passwords stored as	Category	Data exposed
2018	MD5	Rental	Email address, Password, Username, Names

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.

Last.fm

VERIFIED 456

Date	Passwords stored as	Category	Data exposed
2012	MD5	Music	Email addresses, Passwords, Usernames, Website activity

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.

Baihe.com

SENSITIVE 454

Date	Passwords stored as	Category	Data exposed
2019	MD5	Dating	Email address, Password, Username, Names

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.

Houzz.com

434

Date	Passwords stored as	Category	Data exposed
2018	as None	y Design	Email addresses, Geographic locations, IP addresses, Names, Passwords, Social media profiles, Usernames

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

R2games.com

VERIFIED 424

Date	Passwords stored as	Category	Data exposed
2015	vBulletin	Gaming	Email addresses, IP addresses, Passwords, Usernames

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.

Reliance_Jio (India)

404

Date	Passwords stored as	Category	Data exposed
2017	None	Telecom	Names, Mobile numbers, Email addresses, Address

In July 2024, a threat actor ("xenZen") claimed to sell a database of ~375 million India telecom customers (phone numbers, email IDs, Aadhaar, addresses) in multiple files titled with different India Telecom companies. This portion of the leaked data was claimed to be from Jio. Jio said the data on the site appeared unauthentic while filing a police complaint about unlawful access.

Eyeem.com

399

Date	Passwords stored as	Category	Data exposed
2018	SHA1	Photography	Bios, Email addresses, Names, Passwords, Usernames

In February 2018, photography website EyeEm suffered a data breach. The breach was identified among a collection of other large incidents and exposed almost 20M unique email addresses, names, usernames, bios and password hashes.

Yam.com

VERIFIED 399

Date	Passwords stored as	Category	Data exposed
2013	as MD5	y Social	Dates of birth, Email addresses, Names, Passwords, Phone numbers, Physical addresses, Usernames

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

Shein.com

VERIFIED 395

Date	Passwords stored as	Category	Data exposed
2018	Cleartext	Shopping	Email addresses, Passwords

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.

Zacks.com

VERIFIED 391

Date	Passwords stored as	Category	Data exposed
2024-06-01	as SHA-256	Investment Research	Full names, Email addresses, Physical addresses, Phone numbers, Usernames, Passwords

In June 2024, Zacks Investment Research experienced a data breach where unauthorized third parties gained access to customer records. The compromised data included full names, email addresses, physical addresses, phone numbers, usernames, and passwords stored as unsalted SHA-256 hashes. The breach was discovered in late January 2025, and the stolen information was reportedly put up for sale on hacker forums. Zacks has since implemented additional security...

VB.T.ru

390

Date	Passwords stored as	Category	Data exposed
2024	MD5	Finance	Full name, Date of birth, Phone number, Region, Email Address

In late 2024, a large-scale leak of 6.3 million rows of personal data from VTB Bank clients was found being circulated on a well known hacker channels.

StreamCraft

371

Date	Passwords stored as	Category	Data exposed
2020	MD5	Games	Email addresses, IP addresses, Passwords, Usernames

In July 2020, the Russian Minecraft service StreamCraft suffered a data breach that was later redistributed as part of a larger corpus of data. The data included 1.8M records of usernames, email and IP addresses and passwords stored as either MD5 or bcrypt hashes.

Tianya.cn

VERIFIED 368

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	Forum	Email addresses, Names, Usernames

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.

i-Dressup.com

VERIFIED 326

Date	Passwords stored as	Category	Data exposed
2016	Cleartext	Social	Email addresses, Passwords

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.

Certificates

VERIFIED 326

Date	Passwords stored as	Category	Data exposed
2022	None	Certificates	Certificates

Certificates is a consolidated, de-duplicated index of TLS certificates seen in public Certificate Transparency logs. Every certificate is stored once, keyed by its fingerprint, with its domains, validity dates and the CT log it came from, so researchers can see every hostname a certificate has covered, including staging and internal names.

Wishbone.io

VERIFIED 323

Date Passwords stored Category Data exposed

2016 as y Email addresses, Auth tokens, Passwords, Dates of birth, Genders, Names, Phone numbers,
6 None Social Usernames, IP addresses

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

17173.com

320

Date Passwords stored as Category Data exposed

2011 MD5 Social Email addresses, Passwords, Usernames

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.

Uuu9.com

320

Date Passwords stored as Category Data exposed

2011 Cleartext Gaming Email addresses, Passwords, Usernames

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.

Kaneva.com

308

Date Passwords stored as Category Data exposed

unknown MD5 Social Email Addresses, Names, IP Address, Username

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.

Desura.com

306

Date Passwords stored as Category Data exposed

2018 Cleartext Gaming Email addresses, Passwords

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

500px.com

291

Date Passwords stored Category Data exposed

2016 as Photograph Dates of birth, Email addresses, Genders, Geographic locations, Names, Passwords,
9 MD5 y Usernames

In mid-2018, the online photography community 500px suffered a data breach. The incident exposed almost 15 million unique email addresses alongside names, usernames, genders, dates of birth and either an MD5 or bcrypt password hash. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly.

JapanCombo

284

Date	Passwords stored as	Category	Data exposed
2017	Cleartext	Comp	Email addresses, Passwords

This database leak was found being spread on a cleartext '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.

CashCrate.com

VERIFIED 277

Date	Passwords stored as	Category	Data exposed
2018	Cleartext	Social	Email addresses, Names, Passwords, Physical addresses

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.

Toondoo.com

260

Date	Passwords stored as	Category	Data exposed
2019	Unknown	Entertainment	Email addresses, Genders, Geographic locations, IP addresses, Passwords, Usernames

In August 2019, the comic strip creation website ToonDoo suffered a data breach. The data was subsequently redistributed on a popular hacking forum in November where the personal information of over 6M subscribers was shared. Impacted data included email and IP addresses, usernames, genders, the location of the individual and salted password hashes.

Zomato.com

VERIFIED 260

Date	Passwords stored as	Category	Data exposed
2017	MD5	Guide	Email addresses, Passwords, Usernames

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).

DuelingNetwork

VERIFIED 258

Date	Passwords stored as	Category	Data exposed
2017	MD5	Gaming	Email addresses, IP addresses, Passwords, Usernames

In March 2017, the Flash game based on the Yu-Gi-Oh trading card game Dueling Network suffered a data breach. The site itself was taken offline in 2016 due to a cease-and-desist order but the forum remained online for another year. The data breach exposed usernames, IP and email addresses and passwords stored as MD5 hashes.

CouponMom.com

258

Date	Passwords stored as	Category	Data exposed
2014	Cleartext	Social	Email addresses, Passwords

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.

JD.com

249

Date	Passwords stored as	Category	Data exposed
2013	SHA1	Shopping	Email addresses, Passwords, Phone numbers, Usernames

In 2013 (exact date unknown), the Chinese e-commerce service JD suffered a data breach that exposed 13GB of data containing 77 million unique email addresses. The data also included usernames, phone numbers and passwords stored as SHA-1 hashes.

Zing.vn

VERIFIED 235

Date	Passwords stored as	Category	Data exposed
2018	MD5	Social	Dates of birth, Email addresses, Genders, IP addresses, Marital statuses, Names, Occupations, Passwords, Phone numbers, Physical

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 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...

Muzhiwan.com

227

Date	Passwords stored as	Category	Data exposed
2016	MD5	Gaming	Email addresses, Passwords

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.

Whois Source 3

227

Date	Passwords stored as	Category	Data exposed
2010-2024	None	Whois Data	Email Address, Phone Numbers, Registrant Name, Registered Domain, IP Address, Geo Location, Name Servers

This is a mostly complete database of newly registered Whois Data for domains registered between 2010 and 2024. This data comes from source 23 Whois Data.

BlankMediaGames.com

VERIFIED 221

Date	Passwords stored as	Category	Data exposed
2018	as Phpb3md5	Gaming	Browser user agent details, Email addresses, IP addresses, Passwords, Purchases, Usernames, Website activity

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.

Tokopedia.com

VERIFIED 220

Date	Passwords stored as	Category	Data exposed
2020	SHA2-384	Shopping	Dates of birth, Email addresses, Genders, Names, Passwords

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

CafePress.com

214

Date	Passwords stored as	Category	Data exposed
2019	SHA1	Market	Email addresses, Names, Passwords, Phone numbers, Physical addresses

In February 2019, the custom merchandise retailer CafePress suffered a data breach. The exposed data included 23 million unique email addresses with some records also containing names, physical addresses, phone numbers and passwords stored as SHA-1 hashes.

WeHeartIt.com

VERIFIED 214

Date	Passwords stored as	Category	Data exposed
2013	MD5/SHA1	Social	Email addresses, Passwords, Usernames

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.

Hautelook.com

VERIFIED 209

Date	Passwords stored as	Category	Data exposed
2018	Cleartext	Shopping	Email addresses, Passwords

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.

Cfire.mail.ru

VERIFIED 207

Date	Passwords stored as	Category	Data exposed
2016	MD5	Social	Email addresses, Passwords, Usernames

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.

Taobao.com

207

Date	Passwords stored as	Category	Data exposed
2012	Cleartext	Shopping	Email addresses, Passwords

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.

000Webhost.com

VERIFIED 206

Date	Passwords stored as	Category	Data exposed
2015	Cleartext	Hosting	Email addresses, IP addresses, Names, Passwords

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.

TGBUS.com

199

Date	Passwords stored as	Category	Data exposed
2014	VBulletin	Gaming	Email addresses, Passwords, Usernames

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.

bookmate.com

VERIFIED 195

Date	Passwords stored as	Category	Data exposed
2018	SHA512	Shopping	Dates of birth, Email addresses, Genders, Geographic locations, Names, Passwords, Usernames

In mid-2018, the social ebook subscription service Bookmate was among a raft of sites that were breached and their data then sold in early-2019. The data included almost 4 million unique email addresses alongside names, genders, dates of birth and passwords stored as salted SHA-512 hashes.

Wanelo.com

VERIFIED 194

Date	Passwords stored as	Category	Data exposed
2018	MD5/Bcrypt	Shopping	Email addresses, IP addresses, Names, Passwords, Physical addresses

In approximately December 2018, the digital mall Wanelo suffered a data breach. The data was later placed up for sale on a dark web marketplace along with a collection of other data breaches in April 2019. A total of 23 million unique email addresses were included in the breach alongside passwords stored as either MD5 or bcrypt hashes.

2games.com

190

Date	Passwords stored as	Category	Data exposed
2018	Cleartext	Gaming	Email addresses, Passwords

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.

AT&T

VERIFIED 188

Date	Passwords stored	Categor	Data exposed
202	as	y	Dates of birth, Email addresses, Government issued IDs, Names, Phone numbers, Physical
4	None	Services	addresses

In March 2024, tens of millions of records allegedly breached from AT&T were posted to a popular hacking forum. Dating back to August 2021, the data was originally posted for sale before later being freely released. At the time, AT&T maintained that there had not been a breach of their systems and that the data originated from elsewhere. 12 days later, AT&T acknowledged that data fields specific to them were in the breach and that it was not yet known whe...

Tata_Docomo (India)

186

Date	Passwords stored as	Category	Data exposed
2024	None	Telecom	Email Address, Full Name, Address, Phone Number, Birth Date

In July 2024, a threat actor ("xenZen") claimed to sell a database of ~375 million India telecom customers (phone numbers, email IDs, Aadhaar, addresses) in multiple files titled with different India Telecom companies. This portion of the leaked data was claimed to be from Jio. Jio said the data on the site appeared unauthentic while filing a police complaint about unlawful access.

Aptode.com

181

Date	Passwords stored as	Category	Data exposed
2020	Sha1	Marketplace	Browser user agent details, Email addresses, IP addresses, Names, Passwords

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

USA 280m Homeowners

VERIFIED 178

Date	Passwords stored as	Category	Data exposed
2019	as None	Aggregated Data	Names, Emails, Phone Numbers, Date of Birth, Addresses, Property Details, and Preferences

In late 2021, a database labeled "USA 280m Homeowners.7z" containing roughly 280M lines was found circulating on a hacker forum. This leak contained personal information such as Names, Emails, Phone Numbers, Date of Birth, Addresses, Property Details, and Preferences including health, hobbies, music, religion, etc.

VietnamAirlines

VERIFIED 177

Date	Passwords stored as	Category	Data exposed
2025	None	Travel	Email Address, Name, DOB, Address

In July 2023, Vietnam Airlines was impacted by a data breach after threat actors exploited a Microsoft SharePoint zero-day vulnerability affecting third-party systems, including a Salesforce environment used by the airline. The incident resulted in the unauthorized access and exfiltration of internal corporate data, which was later advertised for sale online. The exposed data primarily consisted of internal documents and operational information rather than...

Twitter.com

173

Date	Passwords stored as	Category	Data exposed
unknown	Cleartext	Social	Email addresses, Passwords

This database leak was found being spread on a cleartext '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.

Livejournal.com

VERIFIED 168

Date	Passwords stored as	Category	Data exposed
2017	Cleartext	Journal	Email addresses, Passwords, Usernames

In mid-2019, news broke of an alleged LiveJournal data breach. This followed multiple reports of credential abuse against Dreamwidth beginning in 2018, a fork of LiveJournal with a significant crossover in user base. The breach allegedly dates back to 2017 and contains 26M unique usernames and email addresses (both of which have been confirmed to exist on LiveJournal) alongside plain text passwords. An archive of the data was subsequently shared on a popu...

52pk.com

164

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	Social	Email address, Password, Username

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

US 185M Cell Phones 2019

VERIFIED 150

Date	Passwords stored as	Category	Data exposed
2019	None	Phone Number Dump	Names, Emails, Phone Numbers & Carrier, Gender

In 2020, a database file labeled "usa_cell_db_2019.rar" was found being shared on hacker forums and database trading Telegram channels. The data contained over 178M phone numbers and nearly 10M unique emails. It also had users names, gender, address, and the phone carrier.

BSNL_Mobile (India)

147

Date	Passwords stored as	Category	Data exposed
2024	None	Telecom	Email Address, Full Name, Address, Phone Number, Birth Date

In July 2024, a threat actor ("xenZen") claimed to sell a database of ~375 million India telecom customers (phone numbers, email IDs, Aadhaar, addresses) in multiple files titled with different India Telecom companies. This portion of the leaked data was claimed to be from BSNL Mobile.

Apollo v5 (Personal)

136

Date	Passwords	Categor	Data exposed
2018	stored as	y	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations,
8	None	Marketin	Social media profiles
		g	

In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're loc...

ModernBusinessSolutions

VERIFIED 133

Date	Passwords stored	Category	Data exposed
2016	as	Data	Dates of birth, Email addresses, Genders, IP addresses, Job titles, Names, Phone numbers,
6	None	Management	Physical addresses

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 ack...

LinkedIn Scrape

132

Date	Passwords stored	Categor	Data exposed
2021	as	y	Education levels, Email addresses, Genders, Geographic locations, Job titles, Names, Social media
1	None	Social	profiles

During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well a...

SubaGames.com

VERIFIED 130

Date	Passwords stored as	Category	Data exposed
2016	VBulletin	Gaming	Email addresses, Passwords

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.

PDL (People Data Labs)

130

Date	Passwords stored as	Category	Data exposed
2019	as None	Marketing	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email...

Romwe.com

129

Date	Passwords stored as	Category	Data exposed
2018	SHA1	Retail	Geographic locations, IP addresses, Names, Passwords, Phone numbers, Physical addresses

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

Evite.com

VERIFIED 126

Date	Passwords stored as	Category	Data exposed
2013	Cleartext	Social	Dates of birth, Email addresses, Genders, Names, Passwords, Phone numbers, Physical

In April 2019, the social planning website for managing online invitations Evite identified a data breach of their systems. Upon investigation, they found unauthorized access to a database archive dating back to 2013. The exposed data included a total of 101 million unique email addresses, most belonging to recipients of invitations. Members of the service also had names, phone numbers, physical addresses, dates of birth, genders and passwords stored in p...

Fashionfantasygame.com

VERIFIED 123

Date	Passwords stored as	Category	Data exposed
2016	Cleartext	Gaming	Email addresses, Passwords

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.

FantaseGame.com

123

Date	Passwords stored as	Category	Data exposed
2022	Cleartext	Unknown	Email Address, Password

Very little is know about this leak other than it showed up in multiple Telegram channels in late 2022. The domain and name of the file do not find any relevant information. As such, this leak is being marked as likely generated. More information will be added if it becomes available.

HiAPK.com

114

Date	Passwords stored as	Category	Data exposed
2014	VBulletin	Technology	Email addresses, Passwords, Usernames

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

Gfan.com

111

Date	Passwords stored as	Category	Data exposed
2016	MD5	Gaming	Email addresses, IP addresses, Passwords, Usernames

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

AnimalJam.com

VERIFIED 103

Date	Passwords stored as	Category	Data exposed
2020	as PBKDF2	Gaming	Dates of birth, Email addresses, Genders, IP addresses, Names, Passwords, Physical addresses, Usernames

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

Pconline.com.cn

102

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	PC News	Email address, Password, Username

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.

8tracks.com

VERIFIED 100

Date	Passwords stored as	Category	Data exposed
2017	SHA1	Streaming	Email addresses, Passwords

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.

Pizap.com

VERIFIED 100

Date	Passwords stored as	Category	Data exposed
2017	stored as SHA1	Photography	Email addresses, Genders, Geographic locations, Names, Passwords, Social media profiles, Usernames, Website activity

In approximately December 2017, the online photo editing site piZap suffered a data breach. The data was later placed up for sale on a dark web marketplace along with a collection of other data breaches in February 2019. A total of 42 million unique email addresses were included in the breach alongside names, genders and links to Facebook profiles when the social media platform was used to authenticate to piZap. When accounts were created directly on piZa...

Houdao.com

97

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	Gaming	Email addresses, Passwords

This database leak was found being spread on a cleartnet '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.

OwnedCore

96

Date	Passwords stored as	Category	Data exposed
2013	MD5	Gaming	Email addresses, IP addresses, Passwords, Usernames

In approximately August 2013, the World of Warcraft exploits forum known as OwnedCore was hacked and more than 880k accounts were exposed. The vBulletin forum included IP addresses and passwords.

Gaadi.com

VERIFIED 96

Date	Passwords stored as	Category	Data exposed
2015	as MD5	y Forum	Email addresses, Genders, Geographic locations, IP addresses, Names, Passwords, Phone numbers, Usernames

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.

Parkmobile.io

VERIFIED 94

Date	Passwords stored as	Category	Data exposed
2021	BCrypt	Mobile Parking	Email addresses, Licence plates, Names, Passwords, Phone numbers

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

7k7k.com

88

Date	Passwords stored as	Category	Data exposed
2011	MD5	Gaming	Email addresses, Passwords, Usernames

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.

China People Data

SENSITIVE 86

Date	Passwords stored as	Category	Data exposed
unknown	None	People Data	Email Address, Full Name, Username, Phone Number, Address, Chinese SSN. Date of Birth

Multiple leaks were found being shared on hacker forums and channels that contained sensitive information about Chinese citizens. The data contained emails, full names, usernames, phone numbers, locations, and Chinese ID numbers. The origin of this data is unknown. As such, this entry has become a compilation of any leaked Chinese citizen data that can not be attributed to a source.

Bit.ly

VERIFIED 85

Date	Passwords stored as	Category	Data exposed
2014	Bcrypt/MD5	Linking	Email addresses, Passwords, Usernames

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.

Email2Name

82

Date	Passwords stored as	Category	Data exposed
2017	None	SpamList	Email, Real names

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.

Renren.com

VERIFIED 79

Date	Passwords stored as	Category	Data exposed
2012	Cleartext	Social	Email addresses, Passwords

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

GPotato.com

VERIFIED 79

Date	Passwords stored as	Category	Data exposed
2007	MD5	Gaming	Dates of birth, Email addresses, Genders, IP addresses, Names, Passwords, Physical addresses, Security questions and answers, Usernames

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.

Cheat-master.net

79

Date	Passwords stored as	Category	Data exposed
2018	Cleartext	Gaming	Email addresses, Passwords

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.

Duolingo

78

Date	Passwords stored as	Category	Data exposed
2023	None	Study	Email addresses, Names, Spoken languages, Usernames

In August 2023, 2.6M records of data scraped from Duolingo were broadly distributed on a popular hacking forum. Obtained by enumerating a vulnerable API, the data had earlier appeared for sale in January 2023 and contained email addresses, names, the languages being learned, XP (experience points), and other data related to learning progress on Duolingo.

Weibo.com

75

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	Social	Email addresses, Passwords

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

Snail Games

73

Date	Passwords stored as	Category	Data exposed
2019	MD5	Gaming	Email addresses, IP addresses, Passwords, Usernames

In March 2015, the gaming website Snail suffered a data breach that impacted 1.4 million subscribers. The impacted data included usernames, IP and email addresses and passwords stored as unsalted MD5 hashes.

Duowan.com

71

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	Gaming	Email addresses, Passwords, Usernames

In approximately 2011, data was allegedly obtained from the Chinese gaming website known as Duowan.com and contained 2.6M accounts. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses, user names and plain text passwords.

Shadi.com

VERIFIED

SENSITIVE

71

Date	Passwords stored as	Category	Data exposed
2016	Cleartext	Dating	Email addresses, Passwords, Religion, Addresses, Gender, Phone Numbers, Complexion, Children, Wedding Plan, Family Status, Marit

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.

SumoTorrent.sx

69

Date	Passwords stored as	Category	Data exposed
2014	MD5	Torrents	Email addresses, IP addresses, Passwords, Usernames

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.

Homechef.com

VERIFIED

69

Date	Passwords stored as	Category	Data exposed
2020	BCrypt	Social	Email addresses, Geographic locations, IP addresses, Names, Partial credit card data,

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

Aircel (India)

69

Date	Passwords stored as	Category	Data exposed
2024	None	Telecom	Email Address, Full Name, Address, Phone Number, Birth Date

In July 2024, a threat actor ("xenZen") claimed to sell a database of ~375 million India telecom customers (phone numbers, email IDs, Aadhaar, addresses) in multiple files titled with different India Telecom companies. This portion of the leaked data was claimed to be from Aircel.

Gamigo.com

VERIFIED 67

Date	Passwords stored as	Category	Data exposed
2016	MD5	Gaming	Email addresses, Passwords

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.

Gigasize.com

64

Date	Passwords stored as	Category	Data exposed
2020	Cleartext	File Share	Email addresses, Passwords

This database leak was found being spread on a cleartnet '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.

GameSalad.com

63

Date	Passwords stored as	Category	Data exposed
2019	Sha256	Gaming	Email addresses, IP addresses, Passwords, Usernames

In February 2019, the education and game creation website Game Salad suffered a data breach. The incident impacted 1.5M accounts and exposed email addresses, usernames, IP addresses and passwords stored as SHA-256 hashes.

Mop.com

62

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	Social	Email addresses, Passwords

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

Atraf.com

SENSITIVE 61

Date	Passwords stored as	Category	Data exposed
2021	MD5	Dating	Email Address, Username, Password, Birthdate, Location, Phone Number, IP Address

In October 2021, the Israeli hosting provider CyberServe was breached and ransomed before having a substantial amount of their customer data leaked publicly by a group known as "Black Shadow". Amongst the data was a database for the LGBTQ dating site Atraf.

JDBBX.com

61

Date	Passwords stored as	Category	Data exposed
2016	MD5	Gaming	Username, Email addresses, Passwords

In November 2016, the Chinese gaming website JDBBX suffered a data breach. The breach included Usernames, Email addresses and Passwords stored as MD5 hashes. In total, 4.8 million users were affected.

Onverse.com

VERIFIED 61

Date	Passwords stored as	Category	Data exposed
2016	MD5	Social	Email addresses, IP addresses, Passwords, Usernames

In January 2016, the online virtual world known as Onverse was hacked and 800k accounts were exposed. Along with email and IP addresses, the site also exposed salted MD5 password hashes.

Promo.com

VERIFIED 60

Date	Passwords stored as	Category	Data exposed
2020	SHA256	Marketing	Email addresses, Genders, IP addresses, Names, Passwords

In July 2020, the self-proclaimed "World's #1 Marketing Video Maker" Promo suffered a data breach which was then shared extensively on a hacking forum. The incident exposed 22 million records containing almost 15 million unique email addresses alongside IP addresses, genders, names and salted SHA-256 password hashes.

LiveAuctioneers.com

55

Date	Passwords stored as	Category	Data exposed
2020	as	y	Email addresses, IP addresses, Names, Passwords, Phone numbers, Physical addresses,
0	MD5	Market	Usernames

In June 2020, the online antiques marketplace LiveAuctioneers suffered a data breach which was subsequently sold online then extensively redistributed in the hacking community. The data contained 3.4 million records including names, email and IP addresses, physical addresses, phones numbers and passwords stored as unsalted MD5 hashes.

MPGH.net

VERIFIED 54

Date	Passwords stored as	Category	Data exposed
2015	vBulletin	Gaming	Email addresses, IP addresses, Passwords, Usernames

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.

8fit.com

51

Date	Passwords stored as	Category	Data exposed
2018	Bcrypt	Health	Email addresses, Genders, Geographic locations, IP addresses, Names, Passwords

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

Adengi

49

Date	Passwords stored as	Category	Data exposed
------	---------------------	----------	--------------

2024	BCrypt	Finance	Email Address, Full Name, Phone Number, Birth Date, Gender, Address, Tax ID, Passport
------	--------	---------	---

In February 2024, Adengi, a microfinance financial organization was hack and had nearly 6.8 million users data posted online. Data include full name, telephone number, email, date of birth, address, gender, tax identification number, passports and more.

Geniusu.com

VERIFIED 48

Date	Passwords stored as	Category	Data exposed
------	---------------------	----------	--------------

2020	BCrypt	Education	Email addresses, Genders, IP addresses, Names, Passwords, Social media profiles
------	--------	-----------	---

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

TruthFinder

48

Date	Passwords stored as	Category	Data exposed
------	---------------------	----------	--------------

2019	script	Service	Email addresses, Names, Passwords, Phone numbers
------	--------	---------	--

In 2019, the public records search service TruthFinder suffered a data breach that later came to light in early 2023. The data included over 8M unique customer email addresses, names, phone numbers and passwords stored as script hashes.

MGMGrandResorts

VERIFIED 48

Date	Passwords stored as	Category	Data exposed
------	---------------------	----------	--------------

2019	None	Resorts	Dates of birth, Email addresses, Names, Phone numbers, Physical addresses
------	------	---------	---

In May 2022, a database containing almost 25M unique email addresses and 38M phone numbers across 142M rows was discovered being extensively shared on Telegram.

Aipai.com

47

Date	Passwords stored as	Category	Data exposed
------	---------------------	----------	--------------

2011	MD5	Gaming	Email addresses, Passwords
------	-----	--------	----------------------------

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.

InstantCheckmate

46

Date	Passwords stored as	Category	Data exposed
------	---------------------	----------	--------------

2019	script	Service	Email addresses, Names, Passwords, Phone numbers
------	--------	---------	--

In 2019, the public records search service Instant Checkmate suffered a data breach that later came to light in early 2023. The data included almost 12M unique customer email addresses, names, phone numbers and passwords stored as script hashes.

Yoreparo.com

45

Date	Passwords stored as	Category	Data exposed
------	---------------------	----------	--------------

unknown	MD5	Social	Email addresses, Passwords, IP Address, Username
---------	-----	--------	--

This database leak was found being spread on a cleartext '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.

Funny-Game

VERIFIED 45

Date	Passwords stored as	Category	Data exposed
2018	MD5	Gaming	Email addresses, IP addresses, Passwords, Usernames

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

Startribune.com

40

Date	Passwords stored as	Category	Data exposed
2019	BCrypt	News	Dates of birth, Email addresses, Genders, Names, Passwords, Physical addresses, Usernames

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

Stratfor.com

VERIFIED 40

Date	Passwords stored as	Category	Data exposed
2011	as	y	Credit cards, Email addresses, Names, Passwords, Phone numbers, Physical addresses,
1	VBulletin	Forum	Usernames

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 p...

HLTV

VERIFIED 37

Date	Passwords stored as	Category	Data exposed
2016	Bcrypt	Gaming	Email addresses, Names, Passwords, Usernames, Website activity

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

Lifebear

37

Date	Passwords stored as	Category	Data exposed
2019	MD5	App	Email addresses, Passwords, Usernames

In early 2019, the Japanese schedule app Lifebear appeared for sale on a dark web marketplace amongst a raft of other hacked websites. The breach exposed almost 3.7M unique email addresses, usernames and passwords stored as salted MD5 hashes.

FlashFlashRevolution.com

VERIFIED 37

Date	Passwords stored as	Category	Data exposed
2019	MD5	Gaming	Email addresses, Passwords, Usernames

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.

Diet.com

VERIFIED 36

Date	Passwords stored	Category	Data exposed
------	------------------	----------	--------------

2014	as Cleartext	y Health	Dates of birth, Eating habits, Email addresses, IP addresses, Names, Passwords, Physical attributes, Usernames
------	--------------	----------	--

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.

Game-Tuts.com

VERIFIED 35

Date	Passwords stored as	Category	Data exposed
------	---------------------	----------	--------------

2016	vBulletin	Gaming	Email addresses, IP addresses, Passwords, Usernames
------	-----------	--------	---

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.

MoneyBookers.com

VERIFIED 35

Date	Passwords stored as	Category	Data exposed
------	---------------------	----------	--------------

2009	Cleartext	Finance	Dates of birth, Email addresses, IP addresses, Names, Phone numbers, Physical addresses
------	-----------	---------	---

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.

123rf.com

VERIFIED 35

Date	Passwords stored	Category	Data exposed
------	------------------	----------	--------------

2020	as MD5	Photograph y	Email addresses, IP addresses, Names, Passwords, Phone numbers, Physical addresses, Usernames
------	--------	--------------	---

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

Pipl.com

VERIFIED 35

Date	Passwords stored as	Category	Data exposed
------	---------------------	----------	--------------

2019	None	Identity	Email Addresses, Name, Gender, Address, Phone Number, Personal details
------	------	----------	--

In June of 2019 a database was found Pipl Identity Verification Service. The data contained data obtained from 3rd parties which included emails, names, genders, address and additional personal details such as AKAs, race, religion, political parties, court cases, and owned vehicles.

BigBasket.com

VERIFIED 34

Date	Passwords stored	Category	Data exposed
------	------------------	----------	--------------

2020	as SHA1	Shoppin g	Dates of birth, Email addresses, IP addresses, Names, Passwords, Phone numbers, Physical addresses
------	---------	-----------	--

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

17.media

VERIFIED 34

Date	Passwords stored as	Category	Data exposed
2016	MD5	Social	Device information, Email addresses, IP addresses, Passwords, Usernames

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.

Nihonomaru.net

VERIFIED 31

Date	Passwords stored as	Category	Data exposed
2015	vBulletin	Anime	Email addresses, IP addresses, Passwords, Usernames

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.

StoryBird.com

VERIFIED 31

Date	Passwords stored as	Category	Data exposed
2021	SHA1/PBKDF2	Social	Email addresses, Names, Passwords, Usernames

In August 2015, the storytelling service StoryBird suffered a data breach exposing 4 million records with 1 million unique email addresses. Impacted data also included names, usernames and passwords stored as SHA1 and PBKDF2 hashes.

Roll20.net

31

Date	Passwords stored as	Category	Data exposed
2018	BCrypt	Gaming	Email addresses, IP addresses, Names, Partial credit card data, Passwords

In December 2018, the tabletop role-playing games website Roll20 suffered a data breach. Almost 4 million customers were impacted by the breach and had email and IP addresses, names, bcrypt hashes of passwords and the last 4 digits of credit cards exposed.

FotoBoom.com

VERIFIED 29

Date	Passwords stored as	Category	Data exposed
2017	Cleartext	Market	Email addresses, Passwords

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.

USAConsumer

29

Date	Passwords stored as	Category	Data exposed
2019	None	Phone Number Dump	Names, Phone Numbers, Addresses, Gender

A database of US Phone data was discovered in an archive being shared on hacker forums and Telegram. The source of the data is unknown and contained Names, Address, and Phone Numbers.

Poshmark.com

28

Date	Passwords stored as	Category	Data exposed
2018	Bcrypt	Market	Email addresses, Genders, Geographic locations, Names, Passwords, Usernames

In mid-2018, social commerce marketplace Poshmark suffered a data breach that exposed 36M user accounts. The compromised data included email addresses, names, usernames, genders, locations and passwords stored as bcrypt hashes.

Kreditplus

28

Date	Passwords stored as	Category	Data exposed
2020	None	Services	Dates of birth, Email addresses, Employers, Family structure, Genders, Income levels, Living costs, Marital statuses, Mothers maiden names, Names, Phone numbers, Physical addresses

In June 2020, the Indonesian credit service Kreditplus suffered a data breach which exposed 896k records containing 769k unique email addresses. The breach exposed extensive personal information including names, family makeup, information on spouses, income and expenses, religions and employment information.

DFB.de

27

Date	Passwords stored as	Category	Data exposed
2016	Cleartext	Sports	Email addresses, Passwords

This database leak was found being spread on a cleartext '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.

Daniweb.com

VERIFIED 27

Date	Passwords stored as	Category	Data exposed
2015	MD5	Technology	Email addresses, IP addresses, Passwords

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.

Straffic.io

VERIFIED 26

Date	Passwords stored as	Category	Data exposed
2020	MD5	Marketing	Email Address, Username, Password, Full Name

In February 2020, Israeli marketing company Traffic exposed a database with 140GB of personal data. The publicly accessible Elasticsearch database contained over 300M rows with 49M unique email addresses. Exposed data also included names, phone numbers, physical addresses and genders.

XSpllit.com

26

Date	Passwords stored as	Category	Data exposed
2015	MD5	streaming	Email addresses, Names, Passwords, Usernames

In November 2013, the makers of gaming live streaming and recording software XSpllit was compromised in an online attack. The data breach leaked almost 3M names, email addresses, usernames and hashed passwords.

Exodus.com

26

Date	Passwords stored as	Category	Data exposed
2021	MD5	Crypto	Email addresses, Passwords, Names, Usernames

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.

ArmorGames.com

24

Date	Passwords stored as	Category	Data exposed
2019	as SHA1	y Gaming	Bios, Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Passwords, Usernames

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.

Wongnai.com

VERIFIED 23

Date	Passwords stored as	Category	Data exposed
2020	stored as MD5	ry Service	Dates of birth, Email addresses, Geographic locations, IP addresses, Names, Passwords, Phone numbers, Social media profiles

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

Jefit.com

VERIFIED 22

Date	Passwords stored as	Category	Data exposed
2017	Cleartext	Fitness	Email Addresses, Passwords

Jefit is a workout and fitness tracking software that had its vBulletin based forum compromised in January 2017; as per result accounts of 2,892,644 users were stolen and now being sold on the Dark Web. Multiple versions of this leak were available. This version contained only emails and cleartext passwords. Other data leaked in other versions include user id, username, emails, hashed passwords, and IP address for over 4.6 million users.

FinalFantasyShrine

22

Date	Passwords stored as	Category	Data exposed
2015	MD5	Forum	Email addresses, Passwords, Usernames, Website activity

In September 2015, the Final Fantasy discussion forum known as FFShrine was breached and the data dumped publicly. Approximately 620k records were released containing email addresses, IP addresses and salted hashes of passwords.

Bolt.cd

21

Date	Passwords stored as	Category	Data exposed
2017	MD5	File Sharing	Email addresses, IP addresses, Passwords, Usernames

In approximately March 2017, the file sharing website Bolt suffered a data breach resulting in the exposure of 995k unique user records. The data was sourced from their vBulletin forum and contained email and IP addresses, usernames and salted MD5 password hashes.

Artsy.net

VERIFIED 19

Date	Passwords stored as	Category	Data exposed
2018	SHA512	Social	Email addresses, IP addresses, Names, Passwords

In April 2018, the online arts database Artsy suffered a data breach which consequently appeared for sale on a dark web marketplace. Over 1M accounts were impacted and included IP and email addresses, names and passwords stored as salted SHA-512 hashes.

1win Partners

VERIFIED 19

Date	Passwords stored as	Category	Data exposed
2024	as	Gambling	Email addresses, Phone Number, IP addresses, Passwords, Usernames, Date of Birth, Name,
4	Sha256	g	Location

In November 2024, the gambling site 1win was allegedly hacked and its database was found being shared in hacker forums and channels. The leak contained multiple files including a user database that included over 94 million entries, a partners database, and some configuration data.

Cannabis.com

VERIFIED 18

Date	Passwords	Category	Data exposed
2014	stored as	ry	Dates of birth, Email addresses, Geographic locations, Historical passwords, Instant messenger
4	vBulletin	Social	identities, IP addresses, Passwords

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

Chatbooks.com

VERIFIED 17

Date	Passwords stored as	Category	Data exposed
2020	SHA512	Photography	Email addresses, Names, Passwords, Phone numbers, Social media profiles

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

Goninja.de

VERIFIED 17

Date	Passwords stored as	Category	Data exposed
2019	MD5	Gaming	Email addresses, Passwords, Usernames, IP

In December 2019, the German online multiplayer game Go Ninja was allegedly breached. The stolen data contains usernames, IPs, passwords, salts, email addresses and additional personal information. This breach is being privately shared on the internet.

Kassy

16

Date	Passwords stored as	Category	Data exposed
2024	MD5	Ticket Sales	Email Address, Username, Password Hash, Name, Phone number, Date of Birth

In April 2023, hackers from the CAS and UHG groups claim to have hacked the Kassy.ru ticket sales service for various city events. The leak affected both information about registered users and their orders. The dump was put up for sale on the darknet.

Elephant Insurance

VERIFIED**SENSITIVE****16**

Date	Passwords stored as	Category	Data exposed
2022	None	Insurance	Email Address, Name, Location, Phone Number, Date Of Birth

In April 2022, Elephant Insurance ("Elephant") was hacked by a group of cybercriminals. Elephant began notifying impacted people in May 2022, confirming that unauthorized third parties obtained access to Elephant's systems. Multiple databases were stolen, including a client table including individuals' names, driver's license numbers and, for some, dates of birth.

ForumCommunity

VERIFIED**15**

Date	Passwords stored as	Category	Data exposed
2016	MD5	Forum	Email addresses, Passwords, Usernames

In approximately mid-2016, the Italian-based service for creating forums known as ForumCommunity suffered a data breach. The incident impacted over 776k unique email addresses along with usernames and unsalted MD5 password hashes.

LuminPDF.com

VERIFIED**14**

Date	Passwords stored as	Category	Data exposed
2019	Bcrypt	PDF	Email addresses, Genders, Spoken language, Bcrypt password or Google auth token

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 ...

Taringa.net

VERIFIED**14**

Date	Passwords stored as	Category	Data exposed
2017	MD5	Social	Email addresses, Passwords, Usernames

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.

CDProjektRed.com

VERIFIED**14**

Date	Passwords stored as	Category	Data exposed
2016	MD5	Gaming	Email addresses, Passwords, Usernames

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.

Reddoorz.com

VERIFIED**14**

Date	Passwords stored as	Category	Data exposed
2020	BCrypt	Hotel	Email addresses, IP addresses, Passwords, Usernames, Phone, DOB

In September 2020, the hotel management & booking platform RedDoorz suffered a data breach that exposed over 5.8M user accounts. The breached data included names, email addresses, phone numbers, genders, dates of birth and passwords stored as bcrypt hashes.

Nexusmods.com

VERIFIED 14

Date	Passwords stored as	Category	Data exposed
2013	MD5	Forum	Email addresses, Passwords, Usernames

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.

MangaFox.me

VERIFIED 14

Date	Passwords stored as	Category	Data exposed
2016	vBulletin	Manga	Dates of birth, Email addresses, IP addresses, Passwords, Usernames

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.

TheTVDB.com

13

Date	Passwords stored as	Category	Data exposed
2017	MySQL	Media	Email addresses, Passwords, Usernames

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

DLH.net

VERIFIED 11

Date	Passwords stored as	Category	Data exposed
2016	SHA1/MD5	Gaming	Dates of birth, Email addresses, Names, Passwords, Usernames, Website activity

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.

MyRepoSpace.com

VERIFIED 11

Date	Passwords stored as	Category	Data exposed
2015	MD5	Software	Email addresses, IP addresses, Passwords, Usernames

In July 2015, the Cydia repository known as myRepoSpace was hacked and user data leaked publicly.

MyRepoSpace.com

11

Date	Passwords stored as	Category	Data exposed
2015	MD5	Software	Email addresses, IP addresses, Passwords, Usernames

In July 2015, the Cydia repository known as myRepoSpace was hacked and user data leaked publicly. Cydia is designed to facilitate the installation of apps on jailbroken iOS devices. The repository service was allegedly hacked by @its_not_herpes and 0x8badf100d in retaliation for the service refusing to remove pirated tweaks.

Hurb.com

10

Date	Passwords stored	Category	Data exposed
2019	as MD5	Travel Agency	Dates of birth, Email addresses, IP addresses, Names, Passwords, Phone numbers, Social media profiles

In approximately March 2019, the online Brazilian travel agency Hurb (formerly Hotel Urbano) suffered a data breach. The data subsequently appeared online for download the following year and included over 20 million customer records with email and IP addresses, names, dates of birth, phone numbers and passwords stored as unsalted MD5 hashes. Phone numbers were missing the region number.

JobStreet.com

VERIFIED 10

Date	Passwords stored as	Category	Data exposed
2017	Unknown	Employment	Dates of birth, Email addresses, Genders, Geographic locations, Government issued IDs, Marital statuses, Names, Nationalities, P

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 ...

Habbo.st

9

Date	Passwords stored as	Category	Data exposed
2014	Cleartext	Gaming	Email addresses, Passwords

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.

Nullled.io

VERIFIED 9

Date	Passwords stored	Category	Data exposed
2016	as VBulletin	Forum	Dates of birth, Email addresses, IP addresses, Passwords, Private messages, Usernames, Website activity

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

BitcoinTalk.org

VERIFIED 9

Date	Passwords stored as	Category	Data exposed
2015	as Cleartext	Forum	Dates of birth, Email addresses, Genders, IP addresses, Passwords, Security questions and answers, Usernames, Website activity

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.

Eye4Fraud

9

Date	Passwords stored as	Category	Data exposed
2023	as	Commerce	Email addresses, IP addresses, Names, Partial credit card data, Phone numbers, Physical
3	None	e	addresses

In February 2023, data alleged to have been taken from the fraud protection service Eye4Fraud was listed for sale on a popular hacking forum. Spanning tens of millions of rows with 16M unique email addresses, the data was spread across 147 tables totalling 65GB and included both direct users of the service and what appears to be individuals who'd placed orders on other services that implemented Eye4Fraud to protect their sales. The data included names and...

Binbank.ru

9

Date	Passwords stored as	Category	Data exposed
2023	None	Finance	Email Address, Full Name, Address, Phone Number, Birth Date

In 2023, Binbank, now owned by the Sberbank service, became publicly available. Leaked data included emails, names, address, phone numbers and date of birth. Only a sample 10% of the entire database was found so far.

Brandi

8

Date	Passwords stored as	Category	Data exposed
2021	MD5	Market	Email Address, Password Hash, Username, Registration Date

In late 2021, a major data breach occurred when the personal information of millions of people was exposed on the internet. The breach was linked to brandi.co.kr, a popular online marketplace that allows individuals to buy and sell goods.

212300.com

7

Date	Passwords stored as	Category	Data exposed
2012	MD5	Various	Email addresses, IP addresses, Passwords, Usernames

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.

51cto.com

VERIFIED 7

Date	Passwords stored as	Category	Data exposed
2017	MD5	Social	Email addresses, Passwords, Usernames

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

MagazineDee.com

6

Date	Passwords stored as	Category	Data exposed
2017	Cleartext	Magazine	Email addresses, Passwords

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.

Rendez-Vous.ru

6

Date	Passwords stored as	Category	Data exposed
2024	MD5	Market	Email Address, Full Name, Phone Number, Date of Birth, Gender, Address, Password

In early 2024, the online shoe and clothing store "Rendez-Vous"'s database was found being sold and shared on hacker channels.

pixlr.com

VERIFIED 6

Date	Passwords stored as	Category	Data exposed
2020	SHA512	Photography	Email, Passwords, Names, Home country, Social media profile

In October 2020, the online photo editing application Pixlr suffered a data breach exposing 1.9 million subscribers. Impacted data included names, email addresses, social media profiles, the country signed up from and passwords stored as SHA-512 hashes

RussianAmerica

6

Date	Passwords stored as	Category	Data exposed
2017	MD5	Social	Email addresses, Names, Passwords, Phone numbers

In approximately 2017, the website for Russian speakers in America known as Russian America suffered a data breach. The incident exposed 183k unique records including names, email addresses, phone numbers and passwords stored in both plain text and as MD5 hashes.

StockX.com

VERIFIED 6

Date	Passwords stored as	Category	Data exposed
2019	MD5	Trading	Email addresses, Names, Passwords, Physical addresses, Purchases, Usernames

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

Gamerzplanet

VERIFIED 6

Date	Passwords stored as	Category	Data exposed
2015	MD5	Gaming	Email addresses, IP addresses, Passwords, Usernames

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.

Brazzers

SENSITIVE 6

Date	Passwords stored as	Category	Data exposed
2013	SHA1	Adult	Email addresses, Passwords, Usernames

In April 2013, the adult website known as Brazzers was hacked and 790k accounts were exposed publicly. Each record included a username, email address and password stored in plain text.

Telegram Scrape

6

Date	Passwords stored as	Category	Data exposed
2023	None	Social	Username, Name, Email Address, Phone

In 2023, over 2 millions Telegram users had their data scraped. Not much information is known about who or how this happened.

Evermotion

VERIFIED 5

Date	Passwords stored as	Category	Data exposed
2015	MD5	Social	Dates of birth, Email addresses, Passwords, Usernames

In May 2015, the Polish 3D modelling website known as Evermotion suffered a data breach. The data was sourced from a vBulletin forum and contained email addresses, usernames, dates of birth and salted MD5 hashes of passwords.

Pampling

VERIFIED 5

Date	Passwords stored as	Category	Data exposed
2020	MD5	Retail	Email addresses, Names, Passwords, Usernames

In January 2020, the online clothing retailer Pampling suffered a data breach that exposed 383k unique customer email addresses.

CSDN.net

VERIFIED 5

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	News	Email addresses, Passwords, Usernames

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.

PubPit.com

VERIFIED 5

Date	Passwords stored as	Category	Data exposed
unknown	Cleartext	unkn	Email addresses, Passwords

This database leak was found being spread on a cleartext '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.

ddo.com

VERIFIED 4

Date	Passwords stored as	Category	Data exposed
2016	MD5	Gaming	Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity

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

Morele.net

4

Date	Passwords stored as	Category	Data exposed
2018	Md5crypt	Video Editing	Email addresses, Names, Passwords, Phone numbers

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.

MajorGeeks

4

Date	Passwords stored as	Category	Data exposed
2015	MD5	File Sharing	Email addresses, IP addresses, Passwords, Usernames

In November 2015, almost 270k accounts from the MajorGeeks support forum were breached. The accounts were being actively sold and traded online and included email addresses, salted password hashes and IP addresses.

Hemmakväll

4

Date	Passwords stored as	Category	Data exposed
2015	MD5	Market	Email addresses, Names, Passwords, Phone numbers, Physical addresses

In July 2015, the Swedish video store chain Hemmakväll was hacked and nearly 50k records dumped publicly. The disclosed data included various attributes of their customers including email and physical addresses, names and phone numbers. Passwords were also leaked, stored with a weak MD5 hashing algorithm.

BinWeevils.com

VERIFIED 4

Date	Passwords stored as	Category	Data exposed
2017	PeopleSoft(UID)	Gaming	Ages, Email addresses, Genders, IP addresses, Passwords, Usernames

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.

Acne.org

4

Date	Passwords stored as	Category	Data exposed
2014	MD5	Forum	Dates of birth, Email addresses, IP addresses, Passwords, Usernames

In November 2014, the acne website acne.org suffered a data breach that exposed over 430k forum members' accounts. The data was being actively traded on underground forums and included email addresses, birth dates and passwords.

Gamess.co.kr

4

Date	Passwords stored as	Category	Data exposed
2011	Cleartext	Gaming	Email addresses, Passwords, Names, Usernames

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.

MindaCorporation.com

4

Date	Passwords stored as	Category	Data exposed
unknown	Cleartext	unkn	Email addresses, Passwords

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.

Ticketfly.com

4

Date	Passwords stored as	Category	Data exposed
2018	None	Market	Email addresses, Names, Phone numbers, Physical addresses

In May 2018, the website for the ticket distribution service Ticketfly was defaced by an attacker and was subsequently taken offline. The attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a reply and subsequently posted the breached data online to a publicly accessible location. The data included over 26 million unique email addresses along with names, physical addresses and phone numbers. Whils...

Grayscale Investments

4

Date	Passwords stored as	Category	Data exposed
2025	None	Digital Currency	Email Address, Full name, Address, Phone Number

In October 2024, Grayscale Investments, a leading digital asset management firm was breached and subsequently had its database shared on hacker forums. The compromised database, containing over 693,000 records, is currently being offered for sale on underground forums. The data includes detailed investor profiles, making it particularly valuable to attackers targeting high-net-worth individuals.

dBforums

3

Date	Passwords stored as	Category	Data exposed
2016	MD5	Forum	Dates of birth, Email addresses, IP addresses, Passwords, Usernames

In July 2016, a data breach of the now defunct database forum "dBforums" appeared for sale alongside several others hacked from the parent company, Penton. The breach of the vBulletin based forum contained usernames, IP addresses, dates of birth and salted MD5 password hashes.

Gamevn.com

3

Date	Passwords stored as	Category	Data exposed
2016	MD5	Gaming	Email addresses, IP addresses, Passwords, Usernames

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.

Orteka.ru

3

Date	Passwords stored as	Category	Data exposed
2024	BCrypt	Shopping	Full Name, Email Address, Registration Date, Phone Number, Address, Gender, Date of birth

Not much is known about this leak other than it was found in multiple hacking forums and Telegram chat rooms around January of 2024

DriveSure.com

3

Date	Passwords stored as	Category	Data exposed
2020	BCrypt	Market	Email addresses, Names, Passwords, Phone numbers, Physical addresses, Vehicle details

In December 2020, the car dealership service provider DriveSure suffered a data breach. The incident resulted in 26GB of data being downloaded and later shared on a hacking forum. Impacted personal information included 3.6 million unique email addresses, names, phone numbers and physical addresses. Vehicle data was also exposed and included makes, models, VIN numbers and odometer readings. A small number of passwords stored as bcrypt hashes were also incl...

FutureShop.co.uk

3

Date	Passwords stored as	Category	Data exposed
2017	Cleartext	Market	Email addresses, Passwords

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.

MoDaCo

VERIFIED 3

Date	Passwords stored as	Category	Data exposed
2016	MD5	Social	Email addresses, IP addresses, Passwords, Usernames

In approximately January 2016, the UK based Android community known as MoDaCo suffered a data breach which exposed 880k subscriber identities. The data included email and IP addresses, usernames and passwords stored as salted MD5 hashes.

Xpgamesaves.com

3

Date	Passwords stored as	Category	Data exposed
2017	MD5	Gaming	Email addresses, IP addresses, Passwords, Usernames

In approximately early 2016, the gaming website Xpgamesaves (XPG) suffered a data breach resulting in the exposure of 890k unique user records. The data contained email and IP addresses, usernames and salted MD5 hashes of passwords.

Rbx.Rocks

3

Date	Passwords stored as	Category	Data exposed
2018	BCrypt	Forum	Email addresses, Names, Passwords

In August 2018, the Roblox trading site Rbx.Rocks suffered a data breach. Almost 25k records were sent to HIBP in November and included names, email addresses and passwords stored as bcrypt hashes.

MortalOnline

VERIFIED 2

Date	Passwords stored as	Category	Data exposed
2018	MD5	Gaming	Email addresses, Names, Passwords, Physical addresses, Usernames

In June 2018, the massively multiplayer online role-playing game (MMORPG) Mortal Online suffered a data breach. A file containing email addresses and cracked passwords was subsequently distributed online.

Groupon.co.id

2

Date	Passwords stored as	Category	Data exposed
2015	Cleartext	Social	Email addresses, Passwords

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.

Klerk.ru

2

Date	Passwords stored as	Category	Data exposed
2014	Cleartext	Financial	Email addresses, Passwords

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.

DivXSubTitles

2

Date	Passwords stored as	Category	Data exposed
2010	Cleartext	Social	Email addresses, Passwords, Usernames

In approximately 2010, the now defunct website DivX SubTitles suffered a data breach that exposed 783k user accounts including email addresses, usernames and plain text passwords.

Xiaomi

2

Date	Passwords stored as	Category	Data exposed
2012	MD5	Forum	Email addresses, IP addresses, Passwords, Usernames

In August 2012, the Xiaomi user forum website suffered a data breach. In all, 7 million email addresses appeared in the breach although a significant portion of them were numeric aliases on the bbs_ml_as_uid.xiaomi.com domain. Usernames, IP addresses and passwords stored as salted MD5 hashes were also exposed.

AhoyGames

2

Date	Passwords stored as	Category	Data exposed
2017	MD5	Gaming	Email address, Password

In approximately 2017, the gaming website AhoyGame suffered a data breach that impacted 191k users. The breach included Email Addresses and Passwords stored as Vbulletin hashes.

AndroidForums.com

VERIFIED

2

Date	Passwords stored as	Category	Data exposed
2011	as VBulletin	y Social	Dates of birth, Email addresses, Homepage URLs, Instant messenger identities, IP addresses, Passwords

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.

Eatigo.com

VERIFIED

2

Date	Passwords stored as	Category	Data exposed
2020	MD5	Services	Email addresses, IP addresses, Passwords, Usernames, Phone

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

ButterFlyLabs.com

2

Date	Passwords stored as	Category	Data exposed
2015	Cleartext	Market	Email addresses, Passwords

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.

Forex-Investor.net

2

Date	Passwords stored as	Category	Data exposed
unknown	Cleartext	Software	Email addresses, Passwords

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.

CheapAssGamer

VERIFIED 2

Date	Passwords stored as	Category	Data exposed
2015	as MD5	y Gaming	Email addresses, IP addresses, Passwords, Usernames Email addresses, IP addresses, Passwords, Usernames

In approximately mid-2015, the forum for CheapAssGamer.com suffered a data breach. The database from the IP.Board based forum contained usernames, email and IP addresses and salted MD5 password hashes.

EloBuddy.com

2

Date	Passwords stored as	Category	Data exposed
2016	vBulletin	Gaming	Email Addresses, Passwords, IP Addresses, Usernames

This database leak was found being spread on a cleartext '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.

PSX-Scene

2

Date	Passwords stored as	Category	Data exposed
2015	vBulletin	Forum	Email addresses, IP addresses, Passwords, Usernames

In approximately February 2015, the Sony Playstation forum known as PSX-Scene was hacked and more than 340k accounts were exposed. The vBulletin forum included IP addresses and passwords stored as salted hashes.

Mac-Forums.com

2

Date	Passwords stored as	Category	Data exposed
2016	vBulletin	Forum	Dates of birth, Email addresses, IP addresses, Passwords, Usernames

In July 2016, the self-proclaimed "Ultimate Source For Your Mac" website Mac Forums suffered a data breach. The vBulletin-based system exposed over 326k usernames, email and IP addresses, dates of birth and passwords stored as salted MD5 hashes.

Alora.io

2

Date	Passwords stored as	Category	Data exposed
2018	MD5	Gaming	Usernames, Email addresses, IP addresses, Passwords

In January or February of 2018, the RuneScape Private Server Alora suffered a data breach that impacted 207k users. The breach included Usernames, Email addresses, IP addresses and Passwords stored as IPB hashes. Alora denies that any data was accessed in their announcement.

Hacker.co.kr

2

Date	Passwords stored as	Category	Data exposed
2010	Cleartext	Market	Email addresses, Passwords

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.

AtlasBus.ru

2

Date	Passwords stored as	Category	Data exposed
2023	SHA1	Travel Agency	Phone Number, Full Name, Passwords

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.

QantasAirlines

VERIFIED 2

Date	Passwords stored as	Category	Data exposed
2025	None	Travel	Email Address, Name, DOB, Address

Qantas Airways was impacted by a data exposure after attackers exploited Microsoft SharePoint vulnerabilities affecting a Salesforce system used by the airline. While the intrusion occurred in 2023, the data did not surface publicly until 2024–2025, when it was circulated by threat actors. The exposed information included internal and customer-related records but did not contain passwords.

Dymocks

VERIFIED 2

Date	Passwords stored as	Category	Data exposed
2023	None	Commerce	Dates of birth, Email addresses, Genders, Names, Phone numbers, Physical addresses

In September 2023, the Australian book retailer Dymocks announced a data breach. The data dated back to June 2023 and contained 1.2M records with 836k unique email addresses. The breach also exposed names, dates of birth, genders, phone numbers and physical addresses.

1ffe024393ca

2

ClassicKorea.co.kr

1

Date	Passwords stored as	Category	Data exposed
2019	MD2	Music	Email addresses, Passwords, Usernames

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.

MrExcel

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2016	MD5	Forum	Dates of birth, Email addresses, IP addresses, Passwords, Usernames

In December 2016, the forum for the Microsoft Excel tips and solutions site Mr Excel suffered a data breach. The hack of the vBulletin forum led to the exposure of over 366k accounts along with email and IP addresses, dates of birth and salted passwords hashed with MD5.

Forbes.com

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2014	MD5	News	Email addresses, Passwords, User website URLs, Usernames

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.

Guntrader

1

Date	Passwords stored as	Category	Data exposed
2021	as Bcrypt	y Market	Email addresses, Geographic locations, IP addresses, Names, Passwords, Phone numbers, Physical addresses

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

SK Car Navigation Update

1

Date	Passwords stored as	Category	Data exposed
2021	MD5	Automotive	Email Address, Username, Full Name, Address, Phone Number, Birth Date, Password Hash

A database attributed to a Korean car navigation update website was found circulating in hacker forums beginning around 2021. Data found in the leak includes email, username, name, address, birth date, password and phone number.

FacePunchForums

1

Date	Passwords stored as	Category	Data exposed
2016	MD5	Forum	Dates of birth, Email addresses, IP addresses, Passwords, Usernames

In June 2016, the game development studio Facepunch suffered a data breach that exposed 343k users. The breached data included usernames, email and IP addresses, dates of birth and salted MD5 password hashes. Facepunch advised they were aware of the incident and had notified people at the time.

BotOfLegends.com

1

Date	Passwords stored as	Category	Data exposed
2014	MD5	Social	Email addresses, IP addresses, Passwords, Usernames, Website activity

In November 2014, the forum for Bot of Legends suffered a data breach. The IP.Board forum contained 238k accounts including usernames, email and IP addresses and passwords stored as salted MD5 hashes.

ClixSense.com

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2016	Cleartext	Survey	Account balances, Dates of birth, Email addresses, Genders, IP addresses, Names, Passwords, Payment histories, Payment methods,

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.

kickstarter.com

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2014	SHA1	Social	Email addresses, Passwords

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.

Insanelyi

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2014	MD5	Forum	Email addresses, Passwords, Usernames

In July 2014, the iOS forum Insanelyi was hacked by an attacker known as Kim Jong-Cracks. A popular source of information for users of jailbroken iOS devices running Cydia, the Insanelyi breach disclosed over 104k users' emails addresses, user names and weakly hashed passwords (salted MD5).

Ajarn.com

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2018	MD5	Social/Study	Dates of birth, Education levels, Email addresses, Genders, Geographic locations, Job applications, Marital statuses, Names, Nationalities, Passwords, Phone numbers, Profile photos

In September 2021, the Thai-based English language teaching website Ajarn discovered they'd been the victim of a data breach dating back to December 2018.

icross.co.kr

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2017	MD5	Forum	Email addresses, Passwords

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.

Catho.com.br

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2020	Cleartext	Recruitment	Email addresses, Names, Passwords, Usernames

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

EuroNics.it

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2018	Cleartext	Market	Email addresses, Passwords

In early 2018, a large dataset consisting of over 1400 individual databases was found online. This leak contained a file named lavoroconnoi.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.

LyricsMania.com

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2017	Cleartext	Music	Email addresses, Passwords, Usernames

In December 2017, the song lyrics website known as Lyrics Mania suffered a data breach. The data in the breach included 109k usernames, email addresses and plain text passwords.

Bizbilla.com

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2019	Cleartext	Market	Email addresses, Passwords

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.

AhaShare.com

VERIFIED 1

Date	Passwords stored as	Category	Data exposed
2013	as MD5	y Torrent	Email addresses, Genders, Geographic locations, IP addresses, Passwords, Usernames, Website activity, Years of birth

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.

MineField

1

Date	Passwords stored as	Category	Data exposed
2015	vBulletin	Gaming	Dates of birth, Email addresses, IP addresses, Passwords, Usernames

In June 2015, the French Minecraft server known as Minefield was hacked and 188k member records were exposed. The IP.Board forum included email and IP addresses, birth dates and passwords stored as salted hashes.

Rhode Island Voter List - 2017

1

Date	Passwords stored as	Category	Data exposed
2017	None	Voters List	Email, Names, Phone Numbers, Addresses, Date of Birth, Gender, Political Party

A voters list for Rhode Island from 2017 was found being share on hacker forums and Telegram. While this data can be considered, 'public' many data points are sensitive and in conjunction with data from other leaks, could be used maliciously.

Experian

SENSITIVE 1

Date	Passwords stored as	Category	Data exposed
2015	None	Finance	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

In September 2015, the US based credit bureau and consumer data broker Experian suffered a data breach that impacted 25+ 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.

Methodology and metadata

How this report was produced

Every dataset was searched for example . com on its own domain field, the same query the search console runs, so the figures here match what an analyst sees interactively.

Totals are exact. Record counts, breach breakdowns, distinct-value counts and year series are aggregations computed over the entire result set, not extrapolated from a sample.

Samples are bounded and labelled. The supporting rows, and the password statistics, are drawn from a capped random sample. Wherever a sample is used, its size is stated beside the figure.

Distinct-value counts are approximate within a fraction of a percent, being computed with a cardinality estimator rather than by materialising every value.

Report metadata	
Subject domain	example . com
Generated	12 Oct 2026 08:51 KST
Report identifier	8799a434 - a2e3 - 4cf4 - 865c - 45945926db64
Datasets with findings	9
Datasets returning nothing	1
Total records	823 , 015
Distinct breach sources	290
Highest severity	CRITICAL
Redaction	Standard: credentials partially redacted

Datasets searched		
DATASET	RESULT	RECORDS
Infostealer credentials	CRITICAL	50,168
Combolist credentials (ULP)	CRITICAL	22,249
Leaked credentials	HIGH	408,797
LinkedIn profiles	MEDIUM	398
Personal records	MEDIUM	257,019
TLS certificates	LOW	326
DNS records	LOW	76,624
Subdomains	LOW	260
Domain registration	INFO	7,174
Facebook profiles	CLEAN	0

Prepared by Leaked.Domains. This report is confidential and intended solely for the organisation named on the cover. Findings reflect data available at the time of generation; exposure is cumulative and a later report may differ.

About Leaked.Domains



Leaked.Domains monitors breach corpora, infostealer logs and internet infrastructure data, and turns them into findings an organisation can act on. This report was produced from that data for the domain named on the cover.

Contact	
PREPARED BY	Leaked.Domains
WEB	https://leaked.domains
EMAIL	info@leaked.domains

Leaked.Domains legal disclaimer

The information provided herein is for general and informational 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 circumstances and may not reflect the most current data. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented. **Leaked.Domains** reserves the right to modify the contents of this document at any time without prior notice.

All data obtained by **Leaked.Domains** pertaining to entities or individuals not associated or connected to **Leaked.Domains** in any way was discovered on the public internet and known dark-web sites, and as such is considered public domain.

Leaked.Domains takes every measure to maintain strict security controls over all data in its possession.

Although **Leaked.Domains** uses reasonable efforts to include accurate and up-to-date information herein, **Leaked.Domains** makes no warranties or representations of any kind as to its accuracy, currency or completeness. By accepting this document you agree that access to, use of, and reliance on this document and its contents is at your own risk. **Leaked.Domains** disclaims all warranties of any kind, express or implied. Neither **Leaked.Domains** nor any party involved in creating, producing or delivering this document shall be liable for any consequence, loss or damage, including direct, indirect, special or consequential damages, or loss of business profits, arising out of access to, use of, or inability to use this document, or any errors or omissions in its content. 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 question arises related to the accuracy of a translation, please refer to the original English version of this document. Any discrepancies created in translation are not binding and have no legal effect for compliance or enforcement purposes.

Any data found on **Leaked.Domains**, in this report, or in exported data is provided "as is". **Leaked.Domains** undertakes substantial efforts to process millions of lines of data and employs filtering mechanisms to exclude erroneous or obviously bad data. Nevertheless it is possible that inaccurate or unreliable data may bypass those filters and become accessible through the platform. Users are encouraged to exercise discretion and diligence when interpreting these findings.