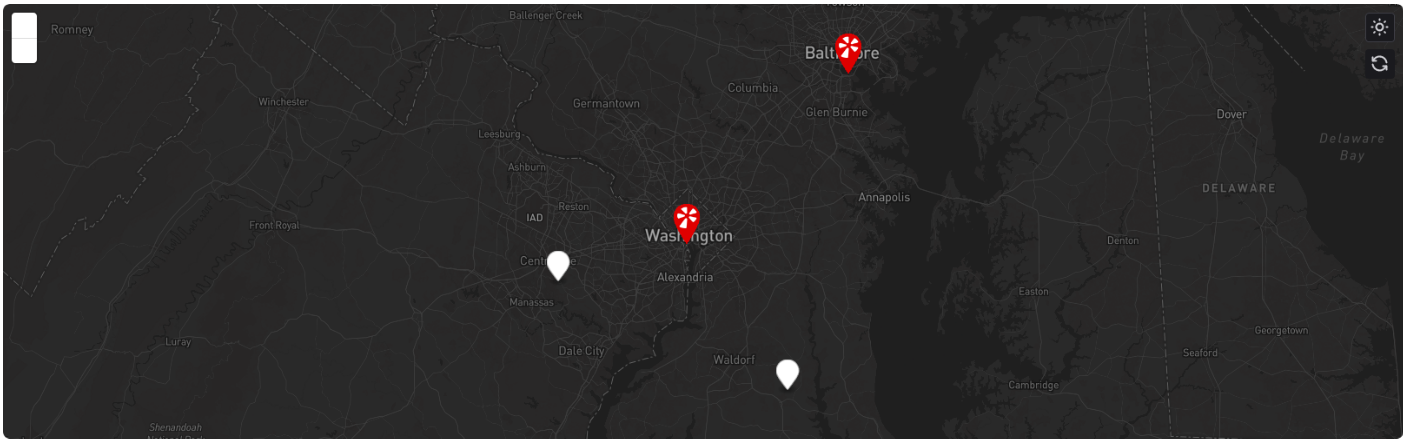
OSINT Industries

Report for: littlebr85@gmail.com
As of 2024-07-02T00:09:55.919Z

Map • Modules • Timeline

Map Outline



Module Responses

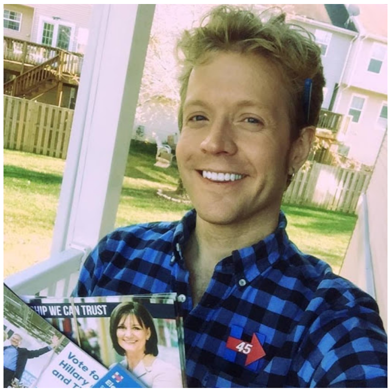
GOOGLE

Registered : true

Id : 106440942632611842156

Name : John M. Becker

Last Seen : 2024-06-15T00:12:09



YOUTUBE

Registered : true

Id : UC2KR327VB83_EFSTy8JWs8g

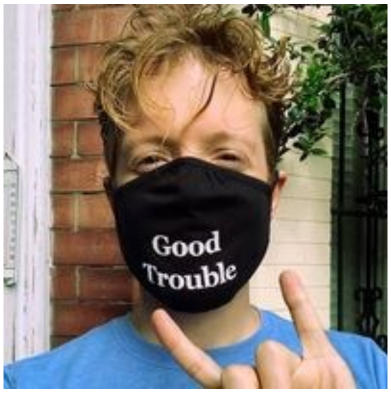
Name : John M. Becker

Profile Url : https://www.youtube.com/channel/UC2KR327VB83_EFSTy8JWs8g

AIRBNB

Registered : true

First Name : John



POSHMARK

Registered : true

Id : 638127c175f02a3428faeb32

Name : John Becker

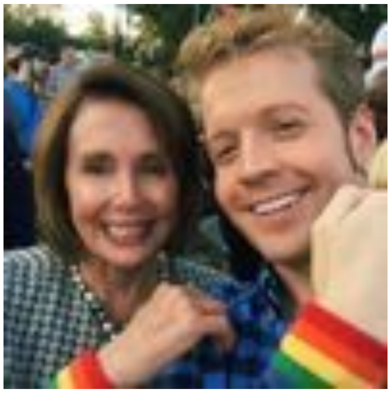
Gender : male

Location : us

Username : johnmbecker85

Profile Url : https://poshmark.com/closet/johnmbecker85

Creation Date : 2022-11-25T20:38:25



SKYPE

Registered : true

Id : john.m.becker85

Name : John Becker

Location : United States

Username : john.m.becker85

FACEBOOK

Registered : true

Email Hint : j*****l@gmail.com, j*****5@gmail.com

DUOLINGO

Registered : true

Id : 482925052

Name : John Becker

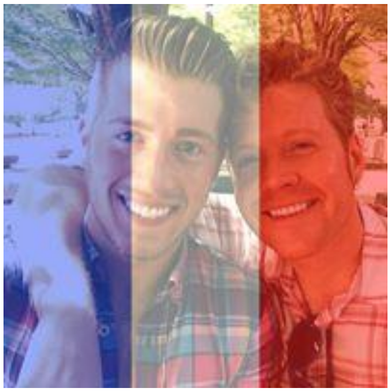
Username : JohnBecker262486

Profile Url : https://www.duolingo.com/profile/JohnBecker262486

Premium : false

Creation Date : 2019-03-12T15:34:41

VIVINO



Registered : true

Id : 11555112

Name : John Becker

Language : en

Location : us

Username : johnbecker0

Profile Url : https://www.vivino.com/users/johnbecker0

Banner Url : https://images.vivino.com/users/backgrounds/default_1.jpg

Followers : 20

Following : 0

Premium : false

Private : false

LINKEDIN

Registered : true

MYFITNESSPAL

Registered : true

HIBP

Registered : true
Breach : true
Name : Adobe
Website : adobe.com
Bio : In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, <em>encrypted</em> 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 <a href="http://www.troyhunt.com/2013/11/adobe-credentials-and-serious.html" target="_blank" rel="noopener">disclosed much about the passwords</a> adding further to the risk that hundreds of millions of Adobe customers already faced.
Creation Date : 2013-10-04T00:00:00

Registered : true
Breach : true
Name : Avvo
Website : avvo.com
Bio : In approximately December 2019, an alleged data breach of the lawyer directory service Avvo was published to an online hacking forum and used in an extortion scam (it's possible the exposure dates back earlier than that). The data contained 4.1M unique email addresses alongside SHA-1 hashes, most likely representing user passwords. <a href="https://troyhunt.com/breach-disclosure-blow-by-blow-heres-why-its-so-hard" target="_blank" rel="noopener">Multiple attempts at contacting Avvo over the course of a week were unsuccessful and the authenticity of the data was eventually verified with common Avvo and HIBP subscribers.</a>
Creation Date : 2019-12-17T00:00:00

Registered : true
Breach : true
Name : Bitly
Website : bitly.com
Bio : In May 2014, the link management company <a href="https://bitly.com/blog/urgent-security-update-regarding-your-bitly-account/" target="_blank" rel="noopener">Bitly announced they'd suffered a data breach</a>. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a

small number using bcrypt.
Creation Date : 2014-05-08T00:00:00

Registered : true
Breach : true
Name : Bonobos
Website : bonobos.com
Bio : In August 2020, the clothing store <a href="https://www.bleepingcomputer.com/news/security/bonobos-clothing-store-suffers-a-data-breach-hacker-leaks-70gb-database/" target="_blank" rel="noopener">Bonobos suffered a data breach</a> that exposed almost 70GB of data containing 2.8 million unique email addresses. The breach also exposed names, physical and IP addresses, phone numbers, order histories and passwords stored as salted SHA-512 hashes, including historical passwords. The breach also exposed partial credit card data including card type, the name on the card, expiry date and the last 4 digits of the card. The data was provided to HIBP by <a href="https://dehashed.com/" target="_blank" rel="noopener">dehashed.com</a>.
Creation Date : 2020-08-14T00:00:00

Registered : true
Breach : true
Name : Collection #1
Bio : In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 <em>billion</em> records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post <a href="https://www.troyhunt.com/the-773-million-record-collection-1-data-reach" target="_blank" rel="noopener">The 773 Million Record "Collection #1" Data Breach</a>.
Creation Date : 2019-01-07T00:00:00

Registered : true
Breach : true
Name : Combolists Posted to Telegram
Bio : In May 2024, <a href="https://troyhunt.com/telegram-combolists-and-361m-email-addresses" target="_blank" rel="noopener">2B rows of data with 361M unique email addresses were collated from malicious Telegram channels</a>. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a

combination of existing combolists and info stealer malware.
Creation Date : 2024-05-28T00:00:00

Registered : true
Breach : true
Name : Data Enrichment Exposure From PDL Customer
Bio : In October 2019, <a href="https://www.troyhunt.com/data-enrichment-people-data-labs-and-another-622m-email-addresses" target="_blank" rel="noopener">security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data</a>. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.
Creation Date : 2019-10-16T00:00:00

Registered : true
Breach : true
Name : Dropbox
Website : dropbox.com
Bio : In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, <a href="https://motherboard.vice.com/read/dropbox-forces-password-resets-after-user-credentials-exposed" target="_blank" rel="noopener">they forced password resets for customers they believed may be at risk</a>. A large volume of data totalling over 68 million records <a href="https://motherboard.vice.com/read/hackers-stole-over-60-million-dropbox-accounts" target="_blank" rel="noopener">was subsequently traded online</a> and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).
Creation Date : 2012-07-01T00:00:00

Registered : true
Breach : true
Name : Evite
Website : evite.com
Bio : In April 2019, the social planning website for managing online invitations <a href="https://www.evite.com/security/update?usource=lc&lctid=1800182" target="_blank" rel="noopener">Evite identified a data breach of their systems</a>. Upon investigation, they found unauthorised access to a database archive dating back to 2013. The exposed data included a total of 101 million unique email addresses,

most belonging to recipients of invitations. Members of the service also had names, phone numbers, physical addresses, dates of birth, genders and passwords stored in plain text exposed. The data was provided to HIBP by a source who requested it be attributed to &quot;JimScott.Sec@protonmail.com&quot;.
Creation Date : 2013-08-11T00:00:00

Registered : true
Breach : true
Name : Gravatar
Website : gravatar.com
Bio : In October 2020, <a href="https://www.bleepingcomputer.com/news/security/online-avatar-service-gravatar-allows-mass-collection-of-user-info/" target="_blank" rel="noopener">a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars </a>. 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, <a href="https://en.gravatar.com/support/data-privacy" target="_blank" rel="noopener">Gravatar release an FAQ detailing the incident</a>.
Creation Date : 2020-10-03T00:00:00

Registered : true
Breach : true
Name : Kickstarter
Website : kickstarter.com
Bio : In February 2014, the crowdfunding platform <a href="https://www.kickstarter.com/blog/important-kickstarter-security-notice" target="_blank" rel="noopener">Kickstarter announced they'd suffered a data breach</a>. The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.
Creation Date : 2014-02-16T00:00:00

Registered : true
Breach : true
Name : LinkedIn
Website : linkedin.com
Bio : In May 2016, <a href="https://www.troyhunt.com/observations-and-thoughts-on-the-linkedin-data-breach" target="_blank" rel="noopener">LinkedIn had 164 million email addresses and passwords

exposed</a>. 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.
Creation Date : 2012-05-05T00:00:00

Registered : true
Breach : true
Name : Lumin PDF
Website : luminpdf.com
Bio : In April 2019, the PDF management service <a href="https://www.zdnet.com/article/data-of-24-3-million-lumin-pdf-users-shared-on-hacking-forum/" target="_blank" rel="noopener">Lumin PDF suffered a data breach</a>. 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 &quot;contacted multiple times, but ignored all the queries&quot;. The exposed data included names, email addresses, genders, spoken language and either a bcrypt password hash or Google auth token. The data was provided to HIBP by a source who requested it be attributed to &quot;JimScott.Sec@protonmail.com&quot;.
Creation Date : 2019-04-01T00:00:00

Registered : true
Breach : true
Name : MGM Resorts (2022 Update)
Website : mgmresorts.com
Bio : In July 2019, <a href="https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/" target="_blank" rel="noopener">MGM Resorts discovered a data breach of one of their cloud services</a>. The breach included 10.6M guest records with 3.1M unique email addresses stemming back to 2017. In May 2022, <a href="https://www.vpnmentor.com/blog/mgm-leaked-on-telegram/" target="_blank" rel="noopener">a superset of the data totalling almost 25M unique email addresses across 142M rows was extensively shared on Telegram</a>. On analysis, it's highly likely the data stems from the same incident <a href="https://www.zdnet.com/article/a-hacker-is-selling-details-of-142-million-mgm-hotel-guests-on-the-dark-web/" target="_blank" rel="noopener">with 142M records having been discovered for sale on a dark web marketplace in mid-2020</a>. The exposed data included email and physical addresses, names, phone numbers and dates of birth.

Creation Date : 2019-07-25T00:00:00

Registered : true
Breach : true
Name : MyFitnessPal
Website : myfitnesspal.com
Bio : In February 2018, the diet and exercise service <a href="https://content.myfitnesspal.com/security-information/FAQ.html" target="_blank" rel="noopener">MyFitnessPal suffered a data breach</a>. 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, <a href="https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/" target="_blank" rel="noopener">the data appeared listed for sale on a dark web marketplace</a> (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to &quot;BenjaminBlue@exploit.im&quot;.
Creation Date : 2018-02-01T00:00:00

Registered : true
Breach : true
Name : MyHeritage
Website : myheritage.com
Bio : In October 2017, the genealogy website <a href="https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/" target="_blank" rel="noopener">MyHeritage suffered a data breach</a>. 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, <a href="https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/" target="_blank" rel="noopener">the data appeared listed for sale on a dark web marketplace</a> (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it be attributed to &quot;BenjaminBlue@exploit.im&quot;.
Creation Date : 2017-10-26T00:00:00

Registered : true
Breach : true
Name : MySpace
Website : myspace.com
Bio : In approximately 2008, <a href="http://motherboard.vice.com/

read/427-million-myspace-passwords-emails-data-breach" target="_blank" rel="noopener">MySpace suffered a data breach that exposed almost 360 million accounts</a>. In May 2016 the data was offered up for sale on the &quot;Real Deal&quot; 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 <a href="https://www.troyhunt.com/dating-the-ginormous-myspace-breach" target="_blank" rel="noopener">analysis of the data suggests it was 8 years before being made public</a>.
Creation Date : 2008-07-01T00:00:00

Registered : true
Breach : true
Name : Naz.API
Bio : In September 2023, <a href="https://www.troyhunt.com/inside-the-massive-naz-api-credential-stuffing-list/" target="_blank" rel="noopener">over 100GB of stealer logs and credential stuffing lists titled &quot;Naz.API&quot; was posted to a popular hacking forum</a>. The incident contained a combination of email address and plain text password pairs alongside the service they were entered into, and standalone credential pairs obtained from unnamed sources. In total, the corpus of data included 71M unique email addresses and 100M unique passwords.
Creation Date : 2023-09-20T00:00:00

Registered : true
Breach : true
Name : NetGalley
Website : netgalley.com
Bio : In December 2020, the book promotion site <a href="https://www.bleepingcomputer.com/news/security/netgalley-discloses-data-breach-after-website-was-hacked/" target="_blank" rel="noopener">NetGalley suffered a data breach</a>. The incident exposed 1.4 million unique email addresses alongside names, usernames, physical and IP addresses, phone numbers, dates of birth and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by a source who requested it be attributed to pom@pompur.in.
Creation Date : 2020-12-21T00:00:00

Registered : true
Breach : true
Name : ShareThis
Website : sharethis.com

Bio : In July 2018, the social bookmarking and sharing service <a href="https://www.sharethis.com/data-privacy-incident/" target="_blank" rel="noopener">ShareThis suffered a data breach</a>. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and password hashes. In 2019, <a href="https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/" target="_blank" rel="noopener">the data appeared listed for sale on a dark web marketplace</a> (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by <a href="https://dehashed.com/" target="_blank" rel="noopener">dehashed.com</a>.
Creation Date : 2018-07-09T00:00:00

Registered : true
Breach : true
Name : StarTribune
Website : startribune.com
Bio : In October 2019, the Minnesota-based news service <a href="https://www.startribune.com/hacker-group-claims-to-have-stolen-star-tribune-user-information/570384542/" target="_blank" rel="noopener">StarTribune suffered a data breach</a> which was subsequently sold on the dark web. The breach exposed over 2 million unique email addresses alongside names, usernames, physical addresses, dates of birth, genders and passwords stored as bcrypt hashes. The data was provided to HIBP by <a href="https://dehashed.com/" target="_blank" rel="noopener">dehashed.com</a>.
Creation Date : 2019-10-10T00:00:00

Registered : true
Breach : true
Name : Ticketfly
Website : ticketfly.com
Bio : In May 2018, the website for the ticket distribution service <a href="https://motherboard.vice.com/en_us/article/mbk3nx/ticketfly-website-database-hacked-data-breach" target="_blank" rel="noopener">Ticketfly was defaced by an attacker and was subsequently taken offline</a>. The attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a reply and subsequently posted the breached data online to a publicly accessible location. The data included over 26 million unique email addresses along with names, physical addresses and phone numbers. Whilst there were no passwords in the publicly leaked data, <a href="https://support.ticketfly.com/customer/en/portal/articles/2941983-ticketfly-cyber-incident-update" target="_blank" rel="noopener">Ticketfly

later issued an incident update</a> and stated that &quot;It is possible, however, that hashed values of password credentials could have been accessed&quot;.
Creation Date : 2018-05-31T00:00:00

Registered : true
Breach : true
Name : tumblr
Website : tumblr.com
Bio : In early 2013, <a href="https://staff.tumblr.com/post/144263069415/we-recently-learned-that-a-third-party-had" target="_blank" rel="noopener">tumblr suffered a data breach</a> 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.
Creation Date : 2013-02-28T00:00:00

Registered : true
Breach : true
Name : Twitter (200M)
Website : twitter.com
Bio : In early 2023, <a href="https://www.bleepingcomputer.com/news/security/200-million-twitter-users-email-addresses-allegedly-leaked-online/" target="_blank" rel="noopener">over 200M records scraped from Twitter appeared on a popular hacking forum</a>. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.
Creation Date : 2021-01-01T00:00:00

Registered : true
Breach : true
Name : Zynga
Website : zynga.com
Bio : In September 2019, game developer <a href="https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/" target="_blank" rel="noopener">Zynga (the creator of Words with Friends) suffered a data breach</a>. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by <a href="https://dehashed.com/" target="_blank" rel="noopener">dehashed.com</a>.
Creation Date : 2019-09-01T00:00:00

VIMEO

Registered : true

DISNEYSTORE

Registered : true

MYSPACE

Registered : true

TUMBLR

Registered : true

NAPSTER

Registered : true

profile

Id : 3E4C4CDFDFFDD044E043C0A87FE4D044
Username : Silver65081
Followers : 0
Following : 0
Private : false

PINTEREST

Registered : true

NEXTDOOR

Registered : true

INSTAGRAM

Registered : true

DISQUS

Registered : true

ESPN

Registered : true

INSTACART

Registered : true

CARE2

Registered : true

HELLOFRESH

Registered : true

MEDIUM

Registered : true
Id : 8b75bec506dc
Name : John Becker
Username : john_m_becker
Profile Url : https://medium.com/@john_m_becker
Followers : 455
Following : 460
Premium : false

LASTPASS

Registered : true

APPLE

Registered : true
Phone Hint : (???) ???-??23

TWITTER

Registered : true

FOURSQUARE

Registered : true
Id : 21092010
First Name : John
Last Name : Becker
Gender : male
Location : US
Username : freedom2marry
Profile Url : https://foursquare.com/freedom2marry
Private : false

CASHAPP

Registered : true
Id : C_0ew940yt7
Name : John Becker
Location : USA
Username : jboygb
Verified : false

MAPS

Registered : true
Profile Url : https://www.google.com/maps/contrib/106440942632611842156/reviews
Private : false

SPOTIFY

Registered : true

DROPBOX

Registered : true
Id : dbid:AABiFZkRK71vludUC4PkhD_t1dyUKAL0_Tw
Name : John Becker
First Name : John
Last Name : Becker
Email : littlebr85@gmail.com
Verified : true

YELP

Registered : true

Id : vzRpdIo9Ic7DoinrGtSeEg

Name : John B.

First Name : John

Gender : m

Location : Washington, DC

Profile Url : https://www.yelp.com/user_details?userid=vzRpdIo9Ic7DoinrGtSeEg&utm_source=ishare

Followers : 152

Following : 0

Creation Date : 2012-04-15T17:57:43

Timeline

Content: Breached 7 times in 2019. (HaveIBeenPwnd!)

Date/Year: 2019

Content: Breached on Adobe

Date/Year: 2013-10-04T00:00:00

Content: Breached on Bitly

Date/Year: 2014-05-08T00:00:00

Content: Breached on Bonobos

Date/Year: 2020-08-14T00:00:00

Content: Breached on Combolists Posted to Telegram

Date/Year: 2024-05-28T00:00:00

Content: Breached on Dropbox

Date/Year: 2012-07-01T00:00:00

Content: Breached on Evite

Date/Year: 2013-08-11T00:00:00

Content: Breached on Gravatar

Date/Year: 2020-10-03T00:00:00

Content: Breached on Kickstarter

Date/Year: 2014-02-16T00:00:00

Content: Breached on LinkedIn

Date/Year: 2012-05-05T00:00:00

Content: Breached on MyFitnessPal

Date/Year: 2018-02-01T00:00:00

Content: Breached on MyHeritage

Date/Year: 2017-10-26T00:00:00

Content: Breached on MySpace

Date/Year: 2008-07-01T00:00:00

Content: Breached on Naz.API

Date/Year: 2023-09-20T00:00:00

Content: Breached on NetGalley

Date/Year: 2020-12-21T00:00:00

Content: Breached on ShareThis

Date/Year: 2018-07-09T00:00:00

Content: Breached on Ticketfly

Date/Year: 2018-05-31T00:00:00

Content: Breached on tumblr

Date/Year: 2013-02-28T00:00:00

Content: Breached on Twitter (200M)

Date/Year: 2021-01-01T00:00:00

Content: Created (poshmark)

Date/Year: 2022-11-25T20:38:25

Content: Reviewed 3DUBs Hauling & Removal LLC

Date/Year: 2022-04-08T00:38:53

Content: Reviewed Perfect For Small Moves LLC

Date/Year: 2017-12-07T16:37:02

Content: Last Seen (google)

Date/Year: 2024-06-15T00:12:09

Content: Created (duolingo)

Date/Year: 2019-03-12T15:34:41

Content: Created (yelp)

Date/Year: 2012-04-15T17:57:43

Content: Reviewed Angie's Seafood.

Date/Year: 2019-06-17T02:21:21

Content: Reviewed Carriage House.

Date/Year: 2013-09-02T23:20:59