OSINT Industries

Report for: csismondo@gmail.com

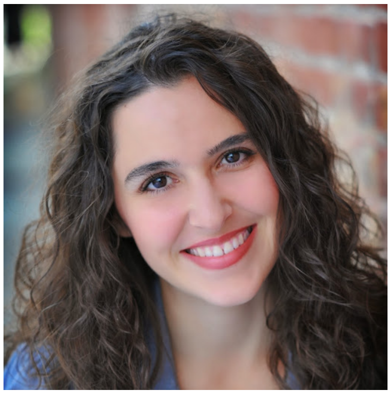
As of 2024-08-12T20:36:21.295Z

Map • Modules • Timeline

Map Outline

Module Responses

GOOGLE



Registered : true
Id : 110558092168644537849
Name : Christene Sismondo
Last Seen : 2024-06-15T00:10:42

Registered : true
Devices : NIKON CORPORATION NIKON D700
Last Seen : 2013-09-09T19:22:06

YOUTUBE

Registered : true
Id : UCf4r23sG1SOtUIAkAvgPCng
Name : Christene Sismondo
Profile Url : https://www.youtube.com/channel/UCf4r23sG1SOtUIAkAvgPCng

LINKEDIN

Registered : true

HIBP

Registered : true
Breach : true
Name : CloudPets
Website : cloudpets.com
Bio : In January, the maker of teddy bears that record children's voices and sends them to family and friends via the internet <a href="https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-

and-ransomed-exposing-kids-voice-messages" target="_blank" rel="noopener">CloudPets left their database publicly exposed and it was subsequently downloaded by external parties</a> (the data was also subject to 3 different ransom demands). 583k records were provided to HIBP via a data trader and included email addresses and bcrypt hashes, but the full extent of user data exposed by the system was over 821k records and also included children's names and references to portrait photos and voice recordings.
Creation Date : 2017-01-01T00:00:00

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 : 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 : Exploit.In
Bio : In late 2016, a huge list of email address and password pairs appeared in a &quot;combo list&quot; referred to as &quot;Exploit.In&quot;. The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for &quot;credential stuffing&quot;, that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read <a href="https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned" target="_blank" rel="noopener">Password reuse, credential stuffing and another billion records in Have I Been Pwned</a>.
Creation Date : 2016-10-13T00:00:00

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 : LinkedIn Scraped Data (2021)
Website : linkedin.com
Bio : During the first half of 2021, <a href="https://www.businessinsider.com.au/linkedin-data-scraped-500-million-users-for-sale-online-2021-4" target="_blank" rel="noopener">LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online</a>. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on <a href="https://

news.linkedin.com/2021/june/an-update-from-linkedin" target="_blank" rel="noopener">An update on report of scraped data</a>.
Creation Date : 2021-04-08T00:00:00

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 : Onliner Spambot
Bio : In August 2017, a spambot by the name of <a href="https://benkowlab.blogspot.com.au/2017/08/from-onliner-spambot-to-millions-of.html" target="_blank" rel="noopener">Onliner Spambot was identified by security researcher Benkow moʞuƎq</a>. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled <a href="https://www.troyhunt.com/inside-the-massive-711-million-record-onliner-spambot-dump" target="_blank" rel="noopener">Inside the Massive 711 Million Record Onliner Spambot Dump</a>.
Creation Date : 2017-08-28T00:00:00

Registered : true
Breach : true
Name : Verifications.io
Website : verifications.io
Bio : In February 2019, the email address validation service <a href="https://securitydiscovery.com/800-million-emails-leaked-online-by-

email-verification-service" target="_blank" rel="noopener">verifications.io suffered a data breach</a>. Discovered by <a href="https://twitter.com/mayhemdayone" target="_blank" rel="noopener">Bob Diachenko</a> and <a href="https://twitter.com/vinnytroia" target="_blank" rel="noopener">Vinny Troia</a>, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although <a href="https://web.archive.org/web/20190227230352/https://verifications.io/" target="_blank" rel="noopener">an archived copy remains viewable</a>.
Creation Date : 2019-02-25T00:00:00

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

PINTEREST

Registered : true

ZILLOW

Registered : true

SPOTIFY

Registered : true

MYSPACE

Registered : true

INSTAGRAM

Registered : true

ESPN

Registered : true

DISNEYSTORE

Registered : true

PANDORA

Registered : true
Username : csismondo
Profile Url : https://pandora.com/content/mobile/profile.vm?webname=csismondo
Followers : 1
Following : 0

CYBERBACKGROUNDCHECKS

Registered : true
Name : Catrina M Sismondo
Age : 42
Location : 7588 Kurthwood Rd, Leesville, LA, 71446, US
Email : trinasismondo@yahoo.com, csismondo@gmail.com, trinasismondo@gmail.com, issysismondo@gmail.com, csismondoh4@netscape.net, csismondoy5@netscape.net, rcsismondo6@netscape.net, sismondo79@hotmail.com, tsismondo@yahoo.com, trina_2001@hotmail.com, csismondo@netscape.net, sismondo@aol.com, sismondo301@aol.com, trina_2004@hotmail.com, sismondo301@gateway.com, sismondo301@gateway.net, sismondo@gateway.net, pastorbryan@ocwc.net
Phone : (337) 353-1309, (337) 239-9591, (719) 559-7348, (719) 659-3239, (701) 570-8330, (757) 823-2381, (801) 836-2801, (740) 282-7695, (402) 367-2860, 565-7169

APPLE

Registered : true
Phone Hint : (???) ???-??40

PAYPAL

Registered : true

Email Hint : *******do@gm***.com

Phone Hint : +1 4**-***-1240

MAPS

Registered : true

Profile Url : https://www.google.com/maps/contrib/110558092168644537849/reviews

Private : false

DROPBOX

Registered : true

Id : dbid:AAB9_HdKflg3qWdN8n4oZ3bJTaAa3x_QuM8

Name : Christene Sismondo

First Name : Christene

Last Name : Sismondo

Email : csismondo@gmail.com

Verified : true

SUBSTACK

Registered : true

Id : 122103203

Name : Christene Sismondo

Profile Url : https://open.substack.com/users/122103203-christene-sismondo

Timeline

Content: Breached on CloudPets

Date/Year: 2017-01-01T00:00:00

Content: Breached on Data Enrichment Exposure From PDL Customer

Date/Year: 2019-10-16T00:00:00

Content: Breached on Evite

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

Content: Breached on Exploit.In

Date/Year: 2016-10-13T00:00:00

Content: Breached on LinkedIn

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

Content: Breached on LinkedIn Scraped Data (2021)

Date/Year: 2021-04-08T00:00:00

Content: Breached on MySpace

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

Content: Breached on Onliner Spambot

Date/Year: 2017-08-28T00:00:00

Content: Breached on Verifications.io

Date/Year: 2019-02-25T00:00:00

Content: Breached on Zynga

Date/Year: 2019-09-01T00:00:00

Content: Reviewed El Arriero

Date/Year: 2023-06-16T02:26:36

Content: Last Active (Google)

Date/Year: 2024-06-15T00:10:42

Content: Last Active (Device (Google))

Date/Year: 2013-09-09T19:22:06