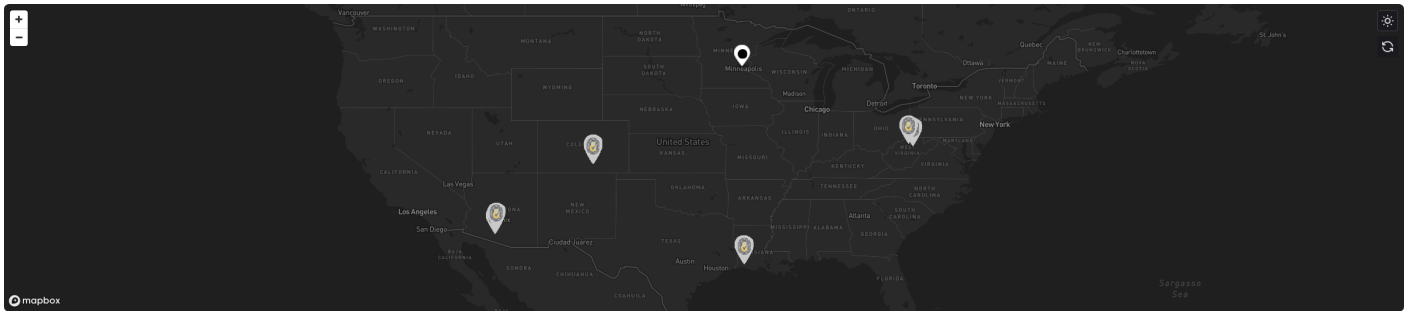
OSINT Industries

Report for: sismondo79@hotmail.com

As of 2024-08-12T20:28:19.618Z

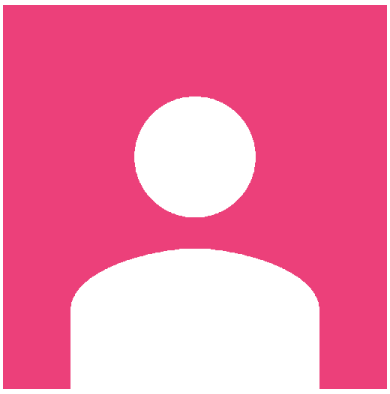
Map • Modules • Timeline

Map Outline



Module Responses

GOOGLE



Registered : true
Id : 104495674504335180563
Name : groundburst
Last Seen : 2024-08-11T17:09:50

SKYPE

Registered : true
Id : live:.cid.a4beaf64fe499ad1
Name : Michael Sismondo
Username : live:.cid.a4beaf64fe499ad1

FACEBOOK

Registered : true
Phone Hint : +*********71

LINKEDIN

Registered : true

MYFITNESSPAL

Registered : true

HIBP

Registered : true
Breach : true
Name : Advance Auto Parts
Website : advanceautoparts.com
Bio : In June 2024, Advance Auto Parts confirmed they had suffered a data breach which was posted for sale

to a popular hacking forum. Linked to unauthorised access to Snowflake cloud services, the breach exposed a large number of records related to both customers and employees. In total, 79M unique email addresses were included in the breach, alongside names, phone numbers, addresses and further data attributes related to company employees.
Creation Date : 2024-06-05T00:00:00

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 billion 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 The 773 Million Record "Collection #1" Data Breach.
Creation Date : 2019-01-07T00:00:00

Registered : true
Breach : true
Name : Data Enrichment Exposure From PDL Customer
Bio : 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 addresses, phone numbers, social media profiles and job history data.
Creation Date : 2019-10-16T00:00:00

Registered : true
Breach : true
Name : Exactis
Website : exactis.com
Bio : In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of

personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.
Creation Date : 2018-06-01T00:00:00

Registered : true
Breach : true
Name : Exploit.In
Bio : In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.
Creation Date : 2016-10-13T00:00:00

Registered : true
Breach : true
Name : LinkedIn
Website : linkedin.com
Bio : 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.
Creation Date : 2012-05-05T00:00:00

Registered : true

Breach : true
Name : MyFitnessPal
Website : myfitnesspal.com
Bio : 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. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".
Creation Date : 2018-02-01T00:00:00

Registered : true
Breach : true
Name : MySpace
Website : myspace.com
Bio : 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.
Creation Date : 2008-07-01T00:00:00

Registered : true
Breach : true
Name : River City Media Spam List
Website : rivercitymediaonline.com
Bio : In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was

used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.
Creation Date : 2017-01-01T00:00:00

Registered : true
Breach : true
Name : Straffic
Website : straffic.io
Bio : In February 2020, Israeli marketing company Straffic 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. In their breach disclosure message, Straffic stated that "it is impossible to create a totally immune system, and these things can occur".
Creation Date : 2020-02-14T00:00:00

Registered : true
Breach : true
Name : Verifications.io
Website : verifications.io
Bio : In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, 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 an archived copy remains viewable.
Creation Date : 2019-02-25T00:00:00

TWITTER

Registered : true

TUMBLR

Registered : true

PINTEREST

Registered : true

INSTAGRAM

Registered : true

MYSPACE

Registered : true

BODYBUILDING

Registered : true

WIX

Registered : true

TOYOTA

Registered : true

CYBERBACKGROUNDCHECKS

Registered : true
Name : Micheal A Sismondo
Age : 45
Location : 7588 Kurthwood Rd, Leesville, LA, 71446, US
Email : greenud5@yahoo.com, sismondo79@hotmail.com, issysismondo@gmail.com, trinasismondo@yahoo.com, det75@yahoo.com, msismondo@yahoo.com, msismondo1@aol.com, msismondo@aol.com, melosh79@aol.com
Phone : (337) 239-9591, (740) 282-7695, (719) 559-7348, (724) 206-1677, (719) 331-3264, (719) 331-3132

TAGGED

Registered : true

CASHAPP

Registered : true
Id : C_5jdxr8y0h

Name : Michael Sismondo
Location : USA
Username : knapperjm

YELP

Registered : true
Id : RvPZTfKxU-Db30SDxpUx8w
Name : Groundburst ..
First Name : Groundburst
Location : Madisonville, TX
Profile Url : https://www.yelp.com/user_details?userid=RvPZTfKxU-Db30SDxpUx8w&utm_source=ishare
Followers : 0
Following : 0
Creation Date : 2019-12-11T00:28:46

SAMSUNG

Registered : true
Phone Hint : +133**23**71

MICROSOFT

Registered : true
Id : A4BEAF64FE499AD1
Name : Michael Sismondo
Location : US
Last Seen : 2024-08-10T06:38:57.537000+00:00
Creation Date : 2007-11-14T22:43:07.680000+00:00

APPLE

Registered : true

MAPS

Registered : true
Profile Url : https://www.google.com/maps/contrib/104495674504335180563/reviews
Private : false

EBAY

Registered : true
First Name : groundburst
Location : United States
Username : grounsism0
Profile Url : https://www.ebay.com/usr/grounsism0
Creation Date : 2020-10-19T00:00:00

Timeline

Content: Breached on Advance Auto Parts
Date/Year: 2024-06-05T00:00:00

Content: Breached on Collection #1
Date/Year: 2019-01-07T00:00:00

Content: Breached on Data Enrichment Exposure From PDL Customer
Date/Year: 2019-10-16T00:00:00

Content: Breached on Exactis
Date/Year: 2018-06-01T00:00:00

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

Content: Breached on MySpace
Date/Year: 2008-07-01T00:00:00

Content: Breached on River City Media Spam List
Date/Year: 2017-01-01T00:00:00

Content: Breached on Straffic
Date/Year: 2020-02-14T00:00:00

Content: Breached on Verifications.io
Date/Year: 2019-02-25T00:00:00

Content: Created Account (Yelp)
Date/Year: 2019-12-11T00:28:46

Content: Last Active (Microsoft)
Date/Year: 2024-08-10T06:38:57.537000+00:00

Content: Created Account (Microsoft)
Date/Year: 2007-11-14T22:43:07.680000+00:00

Content: Reviewed Anoka Goodfellas Barber Studio

Date/Year: 2022-03-25T12:46:06

Content: Last Active (Google)

Date/Year: 2024-08-11T17:09:50

Content: Created Account (Ebay)

Date/Year: 2020-10-19T00:00:00