OSINT Industries

Report for: a_schaefers@msn.com

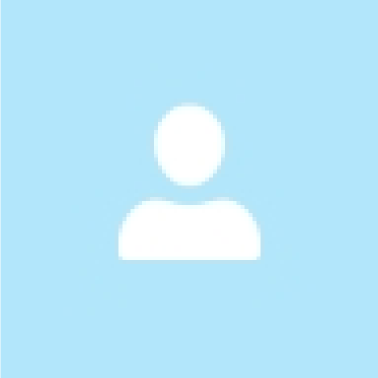
As of 2024-07-22T23:07:46.113Z

Map • Modules • Timeline

Map Outline

Module Responses

SKYPE



Registered : true

Id : live:a_schaefers_1

Name : AARON SCHAEFERS

Username : live:a_schaefers_1

FACEBOOK

Registered : true

Email Hint : l*****3@gmail.com, s*****1@yahoo.com, l*****0@gmail.com

Phone Hint : +*********36

FLICKR

Registered : true

Id : 41390546@N08

Username : schaea2009

Profile Url : https://www.flickr.com/photos/41390546@N08

Creation Date : 2009-08-10T08:02:25

HIBP

Registered : true

Breach : true

Name : 2,844 Separate Data Breaches

Bio : In February 2018, <a href="https://www.troyhunt.com/ive-just-added-2844-new-data-breaches-with-80m-records-to-have-i-been-pwned/" target="_blank" rel="noopener">a massive collection of almost 3,000 alleged data breaches was found online</a>. Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single &quot;unverified&quot; data breach.

Creation Date : 2018-02-19T00:00:00

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 : 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 : Dungeons & Dragons Online
Website : ddo.com
Bio : In April 2013, the interactive video game <a href="https://www.ddo.com" target="_blank" rel="noopener">Dungeons &amp; Dragons Online</a> 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.
Creation Date : 2013-04-02T00:00:00

Registered : true
Breach : true
Name : Exactis
Website : exactis.com

Bio : In June 2018, <a href="https://www.wired.com/story/exactis-database-leak-340-million-records/" target="_blank" rel="noopener">the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data</a>. Security researcher <a href="https://www.nightlionsecurity.com/" target="_blank" rel="noopener">Vinny Troia of Night Lion Security</a> 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 &quot;compiler and aggregator of premium business &amp; consumer data&quot; 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 &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 : Modern Business Solutions
Website : modbsolutions.com
Bio : In October 2016, a large Mongo DB file containing tens of millions of accounts <a href="https://twitter.com/0x2Taylor/status/784544208879292417" target="_blank" rel="noopener">was shared publicly on Twitter</a> (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 <a href="http://news.softpedia.com/news/hacker-steals-58-million-user-records-from-data-storage-provider-509190.shtml" target="_blank" rel="noopener">attributed to &quot;Modern Business Solutions&quot;

</a>, a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.
Creation Date : 2016-10-08T00:00:00

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 : Pemiblanc
Website : pemiblanc.com
Bio : In April 2018, a credential stuffing list containing 111 million email addresses and passwords known as <a href="https://www.troyhunt.com/the-111-million-pemiblanc-credential-stuffing-list" target="_blank" rel="noopener">Pemiblanc</a> was discovered on a French server. The list contained email addresses and passwords collated from different data breaches and used to mount account takeover attacks against other services. <a href="https://www.troyhunt.com/the-111-million-pemiblanc-credential-stuffing-list" target="_blank" rel="noopener">Read more about the incident.</a>
Creation Date : 2018-04-02T00:00:00

Registered : true
Breach : true
Name : River City Media Spam List
Website : rivercitymediaonline.com
Bio : In January 2017, <a href="https://web.archive.org/web/20170426084052/https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire" target="_blank" rel="noopener">a massive trove of data from River City Media was found exposed online</a>. 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 : Special K Data Feed Spam List
Website : data4marketers.com
Bio : In mid to late 2015, a spam list known as the <a href="http://www.data4marketers.com/d4m_SpecialKfeed2015.html" target="_blank" rel="noopener">Special K Data Feed</a> was discovered containing almost 31M identities. The data includes personal attributes such as names, physical and IP addresses, genders, birth dates and phone numbers. <a href="https://www.troyhunt.com/have-i-been-pwned-and-spam-lists-of-personal-information" target="_blank" rel="noopener">Read more about spam lists in HIBP.</a>
Creation Date : 2015-10-07T00:00:00

Registered : true

Breach : true

Name : Unverified Data Source

Website : astoriacompany.com

Bio : In January 2021, over 11M unique email addresses were discovered by Night Lion Security alongside an extensive amount of personal information including names, physical and IP addresses, phone numbers and dates of birth. Some records also contained social security numbers, driver's license details, personal financial information and health-related data, depending on where the information was sourced from. Initially attributed to Astoria Company, <a href="https://astoriacompany.com/cyber-update/" target="_blank" rel="noopener">they subsequently investigated the incident and confirmed the data did not originate from their services</a>.

Creation Date : 2021-01-26T00:00:00

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 : Washington State Food Worker Card

Website : foodworkercard.wa.gov

Bio : In June 2023, <a href="https://tpchd.org/news/data-breach-exposed-food-worker-card-records-we-are-notifying-those-affected/" target="_blank" rel="noopener">the Tacoma-Pierce County Health Department announced a data breach of their Washington State Food

Worker Card online training system</a>. The breach was published to a popular hacking forum the year before and dated back to a 2018 database backup. Included in the data were 1.6M unique email addresses along with names, post codes, dates of birth and approximately 9.5k driver's licence numbers.

Creation Date : 2022-11-17T00:00:00

SAMSUNG

Registered : true

CYBERBACKGROUNDCHECKS

Registered : true

Name : Connie Diane Schaefers

Age : 79

Location : 500 W River Rd, Centralia, WA, 98531, US

Email : a_schaefers@msn.com, connie_schaefers@hotmail.com, legofreak2010@gmail.com, connir_schaefers@hotmail.com, connie-schaefers@hotmail.com, cschaefers@hotmail.com

Phone : (360) 304-3979, (360) 807-6129, (360) 520-0016, (360) 237-4025, (360) 740-0906, (360) 668-5593, (360) 736-4773, (360) 748-8061, (360) 807-6188

XVIDEOS

Registered : true

MYSPACE

Registered : true

MICROSOFT

Registered : true

Id : 39B47EFA33015649

Name : AARON SCHAEFERS

Location : US

Last Seen : 2024-07-22T01:21:05.910000+00:00

Creation Date : 2005-05-12T04:52:36.763000+00:00

EA

Registered : true

ACTIVISION

Registered : true

CALLOFDUTY

Registered : true

YELP

Registered : true

Id : _l7vta1E_vnvik9Bb9GJYg

Name : Aaron S.

First Name : Aaron

Gender : m

Location : WA, WA

Profile Url : https://www.yelp.com/user_details?userid=_l7vta1E_vnvik9Bb9GJYg&utm_source=ishare

Followers : 1

Following : 0

Creation Date : 2023-03-25T21:27:58

DROPBOX

Registered : true

Id : dbid:AABDXno7R5ke0x1BtC9qQEl198l_YrX8j_w

Name : AARON SCHAEFERS

First Name : AARON

Last Name : SCHAEFERS

Email : a_schaefers@msn.com

Verified : true

Timeline

Content: Created (Flickr)

Date/Year: 2009-08-10T08:02:25

Content: Breached on 2,844 Separate Data Breaches

Date/Year: 2018-02-19T00:00:00

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 Dungeons & Dragons Online

Date/Year: 2013-04-02T00:00:00

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 Modern Business Solutions

Date/Year: 2016-10-08T00:00:00

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 Pemiblanc

Date/Year: 2018-04-02T00:00:00

Content: Breached on River City Media Spam List

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

Content: Breached on Special K Data Feed Spam List

Date/Year: 2015-10-07T00:00:00

Content: Breached on Unverified Data Source

Date/Year: 2021-01-26T00:00:00

Content: Breached on Verifications.io

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

Content: Breached on Washington State Food Worker Card

Date/Year: 2022-11-17T00:00:00

Content: Last Seen (Microsoft)

Date/Year: 2024-07-22T01:21:05.910000+00:00

Content: Created (Microsoft)

Date/Year: 2005-05-12T04:52:36.763000+00:00

Content: Created (Yelp)

Date/Year: 2023-03-25T21:27:58