OSINT Industries

Report for: **complete@ctrl.it**

As of **2024-04-04T01:01:04.888Z**

Map • Modules • Timeline

Module Responses

GOOGLE

Registered: true
Id: 113439178557444658555
Name: Filippo Moncelli
First Name: Filippo
Last Name: Moncelli
Last Seen: 2024-03-29T09:20:28

POSHMARK

Registered: true
Id: 617598d5f065fe5141d07ab0
Gender: 2male2222
Location: us
Username: vkenjbzgvnvh
Profile Url: https://poshmark.com/closet/vkenjbzgvnvh
Creation Date: 2021-10-24T17:33:09

SKYPE

Registered: true
Id: filippo.moncelli
Name: Filippo Moncelli
Location: Italy
Username: filippo.moncelli

FOURSQUARE

Registered: true
Id: 19638596
First Name: Filippo
Last Name: Moncelli
Gender: male
Location: IT
Username: filippom8104041
Profile Url: https://foursquare.com/filippom8104041
Private: false

MICROSOFT

Registered: true
Id: 01D583A299BFC228
Name: complete@ctrl.it
Last Seen: 2019-05-20T16:36:30.440000+00:00
Creation Date: 2009-02-23T21:58:41.850000+00:00

IMAGESHACK

Registered: true

Username: felipe22

Profile Url: https://imageshack.com/user/felipe22

INSTAGRAM

Registered: true

APPLE

Registered: true

Phone Hint: ??? ??? ??73

MAPS

Registered: true

Profile Url: https://www.google.com/maps/contrib/113439178557444658555/reviews

DROPBOX

Registered: true

Id: dbid:AADxWzWS6HnhA_HRiaCXtZ9wxQLHSAQaEAE

Name: complete ctrl

First Name: complete

Last Name: ctrl

Email: complete@ctrl.it

Verified: true

EMAILCHECKER

Registered: true

Website: pinterest.com

Registered: true
Website: freelancer.com

Registered: true
Website: ubisoftconnect.com

Registered: true
Website: myspace.com

Registered: true
Website: paypal.com

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, *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.

Creation Date: 2013-10-04T00:00:00

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: 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, 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).
Creation Date: 2012-07-01T00:00:00

Registered: true
Breach: true
Name: Gravatar
Website: gravatar.com
Bio: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 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, Gravatar release an FAQ detailing the incident.
Creation Date: 2020-10-03T00:00:00

Registered: true
Breach: true
Name: Last.fm
Website: last.fm

Bio: In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. Whilst Last.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.
Creation Date: 2012-03-22T00:00:00

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: Nexus Mods
Website: nexusmods.com
Bio: 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.
Creation Date: 2013-07-22T00:00:00

Registered: true
Breach: true
Name: Onliner Spambot
Bio: In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moʞuƎq. 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 Inside the Massive 711 Million Record Onliner Spambot Dump.
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 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

Timeline

Content: Last Seen (google)
Start: 2024-03-29T09:20:28

Content: Created Account (poshmark)
Start: 2021-10-24T17:33:09

Content: Breached on Gravatar (HaveIBeenPwnd!)
Start: 2020-10-03T00:00:00
End: null

Content: Breached on Data Enrichment Exposure From PDL Customer (HaveIBeenPwnd!)
Start: 2019-10-16T00:00:00
End: null

Content: Last Seen (microsoft)
Start: 2019-05-20T16:36:30.440000+00:00

Content: Breached on Verifications.io (HaveIBeenPwnd!)
Start: 2019-02-25T00:00:00
End: null

Content: Breached on Collection #1 (HaveIBeenPwnd!)
Start: 2019-01-07T00:00:00
End: null

Content: Breached on Onliner Spambot (HaveIBeenPwnd!)
Start: 2017-08-28T00:00:00
End: null

Content: Breached on Adobe (HaveIBeenPwnd!)
Start: 2013-10-04T00:00:00
End: null

Content: Breached on Nexus Mods (HaveIBeenPwnd!)
Start: 2013-07-22T00:00:00
End: null

Content: Breached on Dropbox (HaveIBeenPwnd!)
Start: 2012-07-01T00:00:00
End: null

Content: Breached on Last.fm (HaveIBeenPwnd!)
Start: 2012-03-22T00:00:00
End: null

Content: Created Account (microsoft)
Start: 2009-02-23T21:58:41.850000+00:00

Content: Breached on MySpace (HaveIBeenPwnd!)
Start: 2008-07-01T00:00:00
End: null

osint.industries