

# OSINT Industries

Report for: [nofrynofun@gmail.com](mailto:nofrynofun@gmail.com)

As of **2024-04-03T22:36:43.649Z**

[Map](#) • [Modules](#) • [Timeline](#)

## Module Responses

### GOOGLE

**Registered:** true

**Id:** 104304059703928926333

**Name:** GIF VR

**First Name:** GIF

**Last Name:** VR

**Last Seen:** 2024-03-27T11:22:14



# YOUTUBE

**Registered:** true

**Id:** UCOtZG0HAPqyea4FOsdCLKUA

**Name:** GIF VR

**Profile Url:** <https://www.youtube.com/channel/UCOtZG0HAPqyea4FOsdCLKUA>

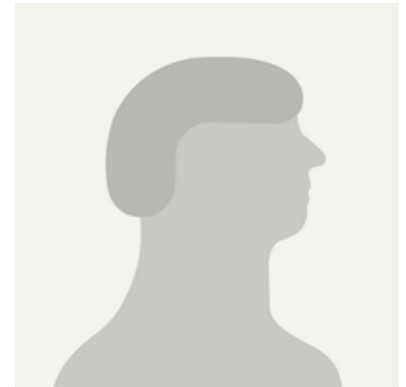
**Creation Date:** 2011-01-01T00:00:00



# ETSY

**Registered:** true

**Name:** no



# GITHUB

**Registered:** true

**Id:** 18617082

**Username:** signornessuno

**Profile Url:** <https://github.com/signornessuno>

**Followers:** 0

**Following:** 0

**Last Seen:** 2016-04-22T14:48:36+00:00

**Creation Date:** 2016-04-22T14:48:36+00:00



# MEDIUM

**Registered:** true

**Id:** a843da0d271f

**Name:** Marmos.eth

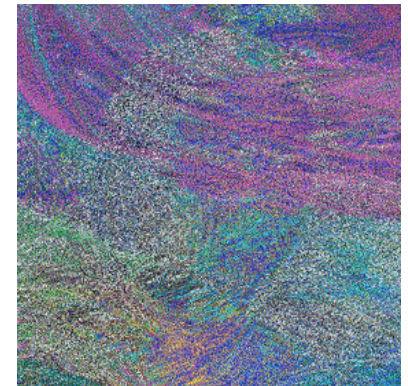
**Username:** marmoseth

**Profile Url:** <https://medium.com/@marmoseth>

**Followers:** 0

**Following:** 2

**Premium:** false



## AIRBNB

**Registered:** true

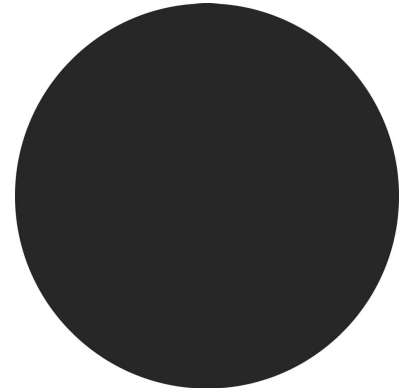
**Id:** 50640092

**First Name:** Maximiliano

**Profile Url:** <https://www.airbnb.com/users/show/50640092>

**Verified:** false

**Creation Date:** 2015-12-06T13:31:51+00:00



## FITBIT

**Registered:** true

**Id:** 26BX4M

**Name:** Black M.

**Profile Url:** [https://asset-service.fitbit.com/ef3b313f-1dd8-11b2-7f7f-7f7f7f7f7f7f\\_profile\\_150\\_square.gif](https://asset-service.fitbit.com/ef3b313f-1dd8-11b2-7f7f-7f7f7f7f7f7f_profile_150_square.gif)

## MYFITNESSPAL

**Registered:** true

## MAPS

**Registered:** true

**Profile Url:** <https://www.google.com/maps/contrib/104304059703928926333/reviews>

## APPLE

**Registered:** true

## CRYPTOINTEL

**Registered:** true

**Website:** <https://www.htx.com/>

**Registered:** true

**Website:** <https://www.binance.com>

## EMAILCHECKER

**Registered:** true

**Website:** [ubisoftconnect.com](https://ubisoftconnect.com)

**Registered:** true

**Website:** [twitter.com](https://twitter.com)

**Registered:** true

**Website:** [academia.edu](https://academia.edu)

**Registered:** true

**Website:** [envato.com](https://envato.com)

**Registered:** true

**Website:** [vimeo.com](https://vimeo.com)

**Registered:** true

**Website:** [adobe.com](https://adobe.com)

**Registered:** true

**Website:** komoot.com

**Registered:** true

**Website:** spotify.com

**Registered:** true

**Website:** paypal.com

**Registered:** true

**Website:** samsung.com

**Registered:** true

**Website:** pinterest.com

**Registered:** true

**Website:** soundcloud.com

## HIBP

**Registered:** true

**Breach:** true

**Name:** Artsy

**Website:** artsy.net

**Bio:** In April 2018, the online arts database [Artsy](#) suffered a data breach which consequently appeared for sale on a dark web marketplace. Over 1M accounts were impacted and included IP and email addresses, names and passwords stored as salted SHA-512 hashes. The data was provided to HIBP by a source who requested it be attributed to "nano@databases.pw".

**Creation Date:** 2018-04-01T00:00:00



**Registered:** true

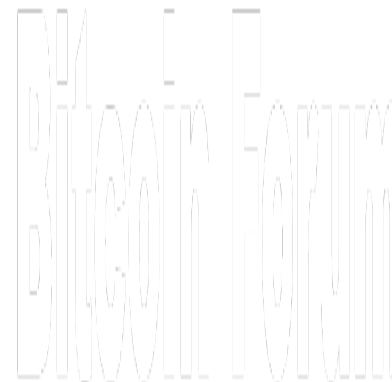
**Breach:** true

**Name:** Bitcoin Talk

**Website:** bitcointalk.org

**Bio:** In May 2015, the Bitcoin forum [Bitcoin Talk](#) was hacked and over 500k unique email addresses were exposed. The attack led to the exposure of a raft of personal data including usernames, email and IP addresses, genders, birth dates, security questions and MD5 hashes of their answers plus hashes of the passwords themselves.

**Creation Date:** 2015-05-22T00:00:00



**Registered:** true

**Breach:** true

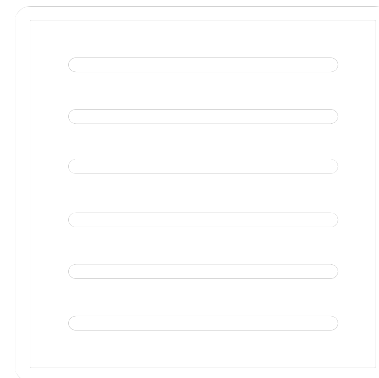
**Name:** Collection #1

**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:** 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:** Money Bookers

**Website:** moneybookers.com

**Bio:** Sometime in 2009, the e-wallet service known as Money Bookers [suffered a data breach which exposed almost 4.5M customers](#). Now called Skrill, the breach was not discovered until October 2015 and included names, email addresses, home addresses and IP addresses.

**Creation Date:** 2009-01-01T00:00:00



**Registered:** true

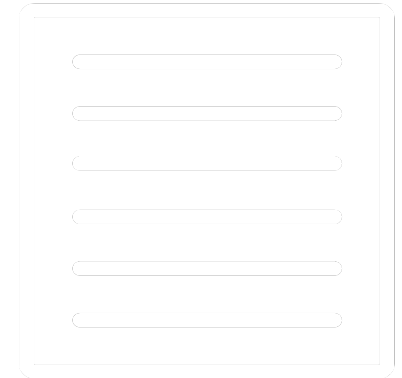
**Breach:** true

**Name:** Naz.API

**Bio:** In September 2023, [over 100GB of stealer logs and credential stuffing lists titled "Naz.API" was posted to a popular hacking forum](#). 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 [NetGalley suffered a data breach](#). 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

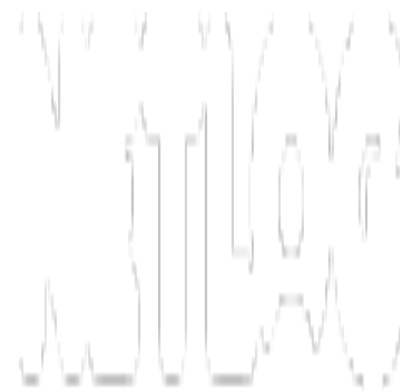
**Name:** Netlog

**Website:** netlog.com

**Bio:** In July 2018, the Belgian social networking site [Netlog identified a data breach of their systems dating back to November 2012 \(PDF\)](#). Although the service was discontinued in 2015, the data breach still impacted 49 million subscribers for whom email addresses and plain text

passwords were exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Creation Date:** 2012-11-01T00:00:00



**Registered:** true

**Breach:** true

**Name:** Twitter (200M)

**Website:** twitter.com

**Bio:** In early 2023, [over 200M records scraped from Twitter appeared on a popular hacking forum](#). 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:** 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



**Registered:** true

**Breach:** true

**Name:** Wattpad

**Website:** wattpad.com

**Bio:** In June 2020, the user-generated stories website [Wattpad suffered a huge data breach that exposed almost 270 million records](#). The data was initially sold then published on a public hacking forum where it was broadly shared. The incident exposed extensive personal information including names and usernames, email and IP addresses, genders, birth dates and passwords stored as bcrypt hashes.

**Creation Date:** 2020-06-29T00:00:00



## Timeline

**Content:** Last Seen (google)

**Start:** 2024-03-27T11:22:14

**Content:** Breached on Naz.API (HavelBeenPwnd!)

**Start:** 2023-09-20T00:00:00

**End:** null

**Content:** Breached on Twitter (200M) (HavelBeenPwnd!)

**Start:** 2021-01-01T00:00:00

**End:** null

**Content:** Breached on NetGalley (HavelBeenPwnd!)

**Start:** 2020-12-21T00:00:00

**End:** null

**Content:** Breached on Gravatar (HavelBeenPwnd!)

**Start:** 2020-10-03T00:00:00

**End:** null

**Content:** Breached on Wattpad (HavelBeenPwnd!)

**Start:** 2020-06-29T00:00:00

**End:** null

**Content:** Breached on Data Enrichment Exposure From PDL Customer (HavelBeenPwnd!)

**Start:** 2019-10-16T00:00:00

**End:** null

**Content:** Breached on Verifications.io (HavelBeenPwnd!)

**Start:** 2019-02-25T00:00:00

**End:** null

**Content:** Breached on Collection #1 (HavelBeenPwnd!)

**Start:** 2019-01-07T00:00:00

**End:** null

**Content:** Breached on Artsy (HavelBeenPwnd!)

**Start:** 2018-04-01T00:00:00

**End:** null

**Content:** Created Account (github)

**Start:** 2016-04-22T14:48:36+00:00

**Content:** Last Seen (github)

**Start:** 2016-04-22T14:48:36+00:00

**Content:** Created Account (airbnb)

**Start:** 2015-12-06T13:31:51+00:00

**Content:** Breached on Bitcoin Talk (HavelBeenPwnd!)

**Start:** 2015-05-22T00:00:00

**End:** null

**Content:** Breached on Netlog (HaveIBeenPwnd!)

**Start:** 2012-11-01T00:00:00

**End:** null

**Content:** Created Account (youtube)

**Start:** 2011-01-01T00:00:00

**Content:** Breached on Money Bookers (HaveIBeenPwnd!)

**Start:** 2009-01-01T00:00:00

**End:** null

[osint.industries](https://osint.industries)