# OSINT Industries

Report for: **polipoli35@hotmail.com**

As of **2024-04-04T04:52:07.963Z**

Map • Modules • Timeline

## Module Responses

### GOOGLE

**Registered:** true
**Id:** 105151112062360898340
**Name:** Joe Scaduto
**First Name:** Joe
**Last Name:** Scaduto
**Last Seen:** 2024-03-26T13:19:52

# YOUTUBE

**Registered:** true
**Id:** UCnOnf2k6H2q9j7iDgeXhwtA
**Name:** Joe Scaduto
**Profile Url:** https://www.youtube.com/channel/UCnOnf2k6H2q9j7iDgeXhwtA
**Creation Date:** 2012-01-01T00:00:00

# MAPS

**Registered:** true
**Profile Url:** https://www.google.com/maps/contrib/105151112062360898340/reviews

# EMAILCHECKER

**Registered:** true
**Website:** twitter.com

**Registered:** true
**Website:** myspace.com

# HIBP

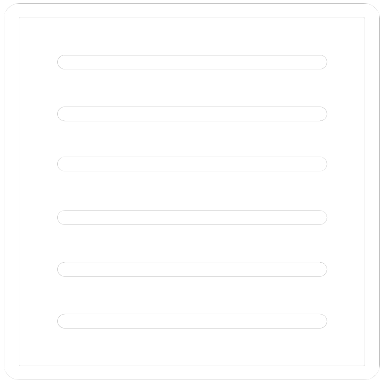
**Registered:** true
**Breach:** true
**Name:** Adobe
**Website:** adobe.com
**Bio:** In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many 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:** 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:** 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:** 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

# Timeline

**Content:** Last Seen (google)
**Start:** 2024-03-26T13:19:52

**Content:** Breached on Twitter (200M) (HaveIBeenPwnd!)
**Start:** 2021-01-01T00:00:00
**End:** null

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

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

**Content:** Breached on Exploit.In (HaveIBeenPwnd!)
**Start:** 2016-10-13T00:00:00
**End:** null

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

**Content:** Breached on Netlog (HaveIBeenPwnd!)
**Start:** 2012-11-01T00:00:00
**End:** null

**Content:** Created Account (youtube)
**Start:** 2012-01-01T00:00:00

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

osint.industries