

OSINT Industries

Report for: **johnnie_walker_angel@yahoo.com**
As of **2024-06-27T23:41:40.294Z**

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

Module Responses

DUOLINGO

Registered : true
Id : 307970570
Name : Yona
Username : Yona516870
Profile Url : <https://www.duolingo.com/profile/Yona516870>
Premium : false
Creation Date : 2017-08-24T14:59:27



LINKEDIN

Registered : true

MYFITNESSPAL

Registered : true

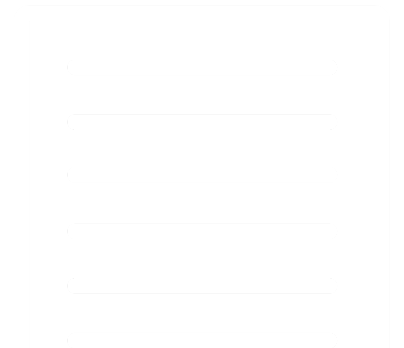
HIBP

Registered : true

Breach : true

Name : Anti Public Combo List

Bio : In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 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 [a href="https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned" target="_blank"](https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned)



rel="noopener">Password reuse, credential stuffing and another billion records in Have I Been Pwned.

Creation Date : 2016-12-16T00:00:00

Registered : true

Breach : true

Name : LinkedIn

Website : linkedin.com

Bio : In May 2016, <a href="https://www.troyhunt.com/observations-and-thoughts-on-the-linkedin-data-breach" target="_blank"

rel="noopener">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 : Trik Spam Botnet

Bio : In June 2018, the command and control server of a malicious botnet known as the "Trik Spam Botnet" <a

href="https://www.bleepingcomputer.com/news/security/trik-spam-botnet-leaks-43-million-email-addresses/" target="_blank"

rel="noopener">was misconfigured such that it exposed the email addresses of more than 43 million people. The researchers who



discovered the exposed Russian server believe the list of addresses was used to distribute various malware strains via malspam campaigns (emails designed to deliver malware).

Creation Date : 2018-06-12T00:00:00

APPLE

Registered : true

Phone Hint : (???) ???-??79

SMULE

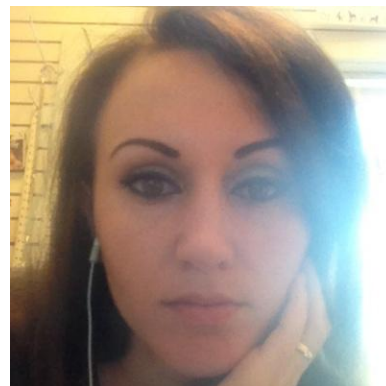
Registered : true

Id : 116801282

Username : johnnie_walker_a

Profile Url : https://www.smule.com/johnnie_walker_a

Verified : false



Timeline

Content: Breached on Anti Public Combo List

Date/Year: 2016-12-16T00:00:00

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 Trik Spam Botnet

Date/Year: 2018-06-12T00:00:00

Content: Created (duolingo)

Date/Year: 2017-08-24T14:59:27

osint.industries