

Report for: nanamiya\_zeke@yahoo.com

As of 2025-07-08T19:31:35.886Z

*Minified and concise search report.*

---

## Module Responses:

**ROLL20**

Registered: true

---

**OPGG**

Registered: true

---

**HUGGINGFACE**

Registered: true

---

**SEOCLEKRS**

Registered: true

---

**FIVERR**

Registered: true

---

**HIBP**

## [Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Patreon

**Website:** patreon.com

**Bio:** In October 2015, the crowdfunding site <a href="http://www.zdnet.com/article/patreon-hacked-anonymous-patrons-exposed/" target="\_blank" rel="noopener">Patreon was hacked</a> and over 16GB of data was released publicly. The dump included almost 14GB of database records with more than 2.3M unique email addresses, millions of personal messages and passwords stored as bcrypt hashes.

**Creation Date:** 2015-10-01T00:00:00

**Logo:** <https://logos.haveibeenpwned.com/Patreon.png>

**Website:** patreon.com

**Description:** In October 2015, the crowdfunding site <a href="http://www.zdnet.com/article/patreon-hacked-anonymous-patrons-exposed/" target="\_blank" rel="noopener">Patreon was hacked</a> and over 16GB of data was released publicly. The dump included almost 14GB of database records with more than 2.3M unique email addresses, millions of personal messages and passwords stored as bcrypt hashes.

**Title:** Patreon

**Modified Date:** 2021-08-10T06:52:47Z

**Breach Count:** 2330382

---

## HIBP

### [Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Artsy

**Website:** artsy.net

**Bio:** In April 2018, the online arts database <a href="https://www.theregister.co.uk/2019/02/11/620\_million\_hacked\_accounts\_dark\_web/" target="\_blank" rel="noopener">Artsy suffered a data breach which consequently appeared for sale on a dark web marketplace</a>. 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 &quot;nano@databases.pw&quot;.

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

**Logo:** <https://logos.haveibeenpwned.com/Artsy.png>

**Website:** artsy.net

**Description:** In April 2018, the online arts database <a href="https://www.theregister.co.uk/2019/02/11/620\_million\_hacked\_accounts\_dark\_web/" target="\_blank" rel="noopener">Artsy suffered a data breach which consequently appeared for sale on a dark web marketplace</a>. 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 &quot;nano@databases.pw&quot;.

**Title:** Artsy

**Modified Date:** 2020-05-25T21:08:08Z

Breach Count: 1079970

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Wattpad

**Website:** wattpad.com

**Bio:** In June 2020, the user-generated stories website <https://www.bleepingcomputer.com/news/security/wattpad-data-breach-exposes-account-info-for-millions-of-users/> 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

**Logo:** <https://logos.haveibeenpwned.com/Wattpad.png>

**Website:** wattpad.com

**Description:** In June 2020, the user-generated stories website <https://www.bleepingcomputer.com/news/security/wattpad-data-breach-exposes-account-info-for-millions-of-users/> 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.

**Title:** Wattpad

**Modified Date:** 2020-07-19T22:49:19Z

**Breach Count:** 268765495

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Naz.API

**Bio:** In September 2023, <https://www.troyhunt.com/inside-the-massive-naz-api-credential-stuffing-list/> 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

**Logo:** <https://logos.haveibeenpwned.com/List.png>

**Description:** In September 2023, [over 100GB of stealer logs and credential stuffing lists titled "Naz.API"](https://www.troyhunt.com/inside-the-massive-naz-api-credential-stuffing-list/) 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.

**Title:** Naz.API

**Modified Date:** 2024-01-17T13:24:27Z

**Breach Count:** 70840771

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Combolists Posted to Telegram

**Bio:** In May 2024, [2B rows of data with 361M unique email addresses were collated from malicious Telegram channels](https://troyhunt.com/telegram-combolists-and-361m-email-addresses). The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a combination of existing combolists and info stealer malware.

**Creation Date:** 2024-05-28T00:00:00

**Logo:** <https://logos.haveibeenpwned.com/List.png>

**Description:** In May 2024, [2B rows of data with 361M unique email addresses were collated from malicious Telegram channels](https://troyhunt.com/telegram-combolists-and-361m-email-addresses). The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a combination of existing combolists and info stealer malware.

**Title:** Combolists Posted to Telegram

**Modified Date:** 2024-06-11T07:01:09Z

**Breach Count:** 361468099

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Storenvvy

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

**Bio:** In mid-2019, [the e-commerce website Storenvvy suffered a data breach that exposed millions of customer records](https://hackread.com/e-commerce-firm-storenvvy-hacked-accounts-leaked/). A portion of the breached records were

subsequently posted to a hacking forum with cracked password hashes, whilst the entire corpus of 23M rows was put up for sale. The data contained 11M unique email addresses alongside usernames, IP addresses, the user's city, gender date of birth and original salted SHA-1 password hash.

**Creation Date:** 2019-04-04T00:00:00

**Logo:** <https://logos.haveibeenpwned.com/Storenvvy.png>

**Website:** storenvvy.com

**Description:** In mid-2019, [the e-commerce website Storenvvy](https://hackread.com/e-commerce-firm-storenvvy-hacked-accounts-leaked/) suffered a data breach that exposed millions of customer records. A portion of the breached records were subsequently posted to a hacking forum with cracked password hashes, whilst the entire corpus of 23M rows was put up for sale. The data contained 11M unique email addresses alongside usernames, IP addresses, the user's city, gender date of birth and original salted SHA-1 password hash.

**Title:** Storenvvy

**Modified Date:** 2025-02-16T08:31:34Z

**Breach Count:** 11052071

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** ALIEN TXTBASE Stealer Logs

**Bio:** In February 2025, [23 billion rows of stealer logs](https://www.troyhunt.com/processing-23-billion-rows-of-alien-txtbase-stealer-logs) were obtained from a Telegram channel known as ALIEN TXTBASE. The data contained 284M unique email addresses alongside the websites they were entered into and the passwords used. This data is now searchable in HIBP by both email domain and the domain of the target website.

**Creation Date:** 2025-02-15T00:00:00

**Logo:** <https://logos.haveibeenpwned.com/List.png>

**Description:** In February 2025, [23 billion rows of stealer logs](https://www.troyhunt.com/processing-23-billion-rows-of-alien-txtbase-stealer-logs) were obtained from a Telegram channel known as ALIEN TXTBASE. The data contained 284M unique email addresses alongside the websites they were entered into and the passwords used. This data is now searchable in HIBP by both email domain and the domain of the target website.

**Title:** ALIEN TXTBASE Stealer Logs

**Modified Date:** 2025-02-25T19:25:18Z

**Breach Count:** 284132969

---

## WIX

**Registered:** true

---

## WIZARDINGWORLD

Registered: true

---

## LOOPERMAN

Registered: true

---

## AUTODESK

Registered: true

---

## SMULE

[Picture Url](#)

[Profile Url](#)

Registered: true

Id: 586947127

Name: Setia Rahayu

First Name: Setia

Last Name: Rahayu

Username: ZekeUtaite

Bio: A 15 year old birb

Verified: false

Followers: 51

Following: 24

---

## NEXON

Registered: true

---

## EA

Registered: true

---

## VRCHAT

Registered: true

---

## FACEBOOK

Registered: true

Phone Hint: +\*\*\*\*\*08, +\*\*\*\*\*29

---

## ADOBE

Registered: true

Status: passwordResetRequired

Type: individual

---

## GITHUB

Registered: true

---

## WORDPRESS

Registered: true

---

## PINTEREST

Registered: true

---

## GRAMMARLY

Registered: true

---

## DROPBOX

Registered: true

---

## MICROSOFT

[Picture Url](#)

Registered: true

Id: 24A4102C2097A62C

Name: Zeke Nanamiya

Location: MY

Last Seen: 2025-07-04T04:54:51.157000+00:00

Creation Date: 2019-05-01T14:59:32.090000+00:00

---

## SKYPE

[Picture Url](#)

Registered: true

Id: live:nanamiya\_zeke

Name: Zeke Nanamiya

Username: live:nanamiya\_zeke

Contact Type: Skype4Consumer

---

## QUORA

[Picture Url](#)

[Profile Url](#)

Registered: true

Id: 260362094

**Name:** Nabila Hani

**First Name:** Nabila

**Last Name:** Hani

**Location:** Shinjuku-ku, Tokyo, Japan

**Followers:** 26

**Creation Date:** 2017-02-09T12:49:20.028000

---