

# Report for: natesmith1016@yahoo.com

As of 2025-07-08T21:55:07.353Z

*Minified and concise search report.*

---

## Module Responses:

### KICK

Registered: true

---

### ACTIVISION

Registered: true

---

### DISNEY

Registered: true

---

### FIREFOX

Registered: true

---

### BETHESDA

Registered: true

---

### DISQUS

Registered: true

---

## TRIVAGO

Registered: true

---

## NEWYORKTIMES

Registered: true  
Id: 92316522

---

## GIPHY

Registered: true

---

## BUNPRO

Registered: true

---

## WEFORUM

Registered: true

---

## ADOBE

Registered: true  
Status: active  
Type: individual

---

**NFL**

Registered: true

---

**MYANIMELIST**

Registered: true

---

**THESTUDENTROOM**

Registered: true

---

**BOEHMIA**

Registered: true

---

**FACEBOOK**

Registered: true

---

**WIZARDINGWORLD**

Registered: true

---

**PEARSON**

Registered: true

---

## FOTOR

Registered: true

---

## BIBLE

[Profile Url](#)

Registered: true

Id: 31220838

Name: Nathan Smith

First Name: Nathan

Last Name: Smith

Language: English

Username: natesmith1016

Creation Date: 2014-03-22T16:25:46.706842+00:00

Country: US

Timezone: America/Chicago

---

## APPLE

Registered: true

Phone Hint: (\*\*\*) \*\*\*-\*\*\*41

---

## FLICKR

[Picture Url](#)

[Profile Url](#)

Registered: true

Id: 139213858@N07

Name: Nathan Smith Jr

Username: Elitealice1

Followers: 11

Creation Date: 2017-12-28T00:31:06

---

## ARCGAMES

Registered: true

---

## ASUS

Registered: true

---

## MEDIUM

[Picture Url](#)

[Profile Url](#)

Registered: true

Id: 4a826d1a52f6

Name: Nathan Smith Jr.

Username: nathansmithjr

Followers: 0

Following: 1

Membership Date: 0

---

## WBGAMES

Registered: true

---

## EVENTBRITE

Registered: true

Id: 350073714631

Verified: true

---

## NEXTDOOR

Registered: true

---

## GENERALMOTORS

Registered: true

---

## ESPN

Registered: true

---

## HIBP

[Picture Url](#)

Registered: true

Breach: true

Name: tumblr

Website: tumblr.com

**Bio:** In early 2013, <a href="https://staff.tumblr.com/post/144263069415/we-recently-learned-that-a-third-party-had" target="\_blank" rel="noopener">tumblr suffered a data breach</a> which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

**Creation Date:** 2013-02-28T00:00:00

**Logo:** https://logos.haveibeenpwned.com/Tumblr.png

**Website:** tumblr.com

**Description:** In early 2013, <a href="https://staff.tumblr.com/post/144263069415/we-recently-learned-that-a-third-party-had" target="\_blank" rel="noopener">tumblr suffered a data breach</a> which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

**Title:** tumblr

**Modified Date:** 2016-05-29T22:59:04Z

**Breach Count:** 65469298

---

## HIBP

[Picture Url](#)

Registered: true

Breach: true

**Name:** MyFitnessPal

**Website:** myfitnesspal.com

**Bio:** In February 2018, the diet and exercise service <a href="https://content.myfitnesspal.com/security-information/FAQ.html" target="\_blank" rel="noopener">MyFitnessPal suffered a data breach</a>. 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, <a href="https://www.theregister.co.uk/2019/02/11/620\_million\_hacked\_accounts\_dark\_web/" target="\_blank" rel="noopener">the data appeared listed for sale on a dark web marketplace</a> (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

**Logo:** https://logos.haveibeenpwned.com/MyFitnessPal.png

**Website:** myfitnesspal.com

**Description:** In February 2018, the diet and exercise service <a href="https://content.myfitnesspal.com/security-information/FAQ.html" target="\_blank" rel="noopener">MyFitnessPal suffered a data breach</a>. 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, <a href="https://www.theregister.co.uk/2019/02/11/620\_million\_hacked\_accounts\_dark\_web/" target="\_blank" rel="noopener">the data appeared listed for sale on a dark web marketplace</a> (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".

**Title:** MyFitnessPal

**Modified Date:** 2019-02-21T20:00:56Z

**Breach Count:** 143606147

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** piZap

**Website:** pizap.com

**Bio:** In approximately December 2017, the online photo editing site <a href="https://www.zdnet.com/article/hacker-puts-up-for-sale-third-round-of-hacked-databases-on-the-dark-web/" target="\_blank" rel="noopener">piZap suffered a data breach</a>. The data was later placed up for sale on a dark web marketplace along with a collection of other data breaches in February 2019. A total of 42 million unique email addresses were included in the breach alongside names, genders and links to Facebook profiles when the social media platform was used to authenticate to piZap. When accounts were created directly on piZap without using Facebook for authentication, passwords stored as SHA-1 hashes were also exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Creation Date:** 2017-12-07T00:00:00

**Logo:** https://logos.haveibeenpwned.com/piZap.png

**Website:** pizap.com

**Description:** In approximately December 2017, the online photo editing site <a href="https://www.zdnet.com/article/hacker-puts-up-for-sale-third-round-of-hacked-databases-on-the-dark-web/" target="\_blank" rel="noopener">piZap suffered a data breach</a>. The data was later placed up for sale on a dark web marketplace along with a collection of other data breaches in February 2019. A total of 42 million unique email addresses were included in the breach alongside names, genders and links to Facebook profiles when the social media platform was used to authenticate to piZap. When accounts were created directly on piZap without using Facebook for authentication, passwords stored as SHA-1 hashes were also exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Title:** piZap

**Modified Date:** 2019-07-16T05:43:27Z

**Breach Count:** 41817893

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** YouNow

**Website:** younow.com

**Bio:** In February 2019, <a href="https://techcrunch.com/2019/02/14/hacker-strikes-again/" target="\_blank" rel="noopener">data from the live broadcasting service YouNow appeared for sale on a dark web marketplace</a>. Whilst it's not clear what date the actual breach occurred on, the impacted data included 18M unique email addresses, IP addresses, names, usernames and links to social media profiles. As authentication is performed via social providers, no passwords were exposed in the breach. Many records didn't have associated email addresses thus the unique number is lower than the reported total number of accounts. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Creation Date:** 2019-02-15T00:00:00

**Logo:** https://logos.haveibeenpwned.com/YouNow.png

**Website:** younow.com

**Description:** In February 2019, <a href="https://techcrunch.com/2019/02/14/hacker-strikes-again/" target="\_blank" rel="noopener">data from the live broadcasting service YouNow appeared for sale on a dark web marketplace</a>. Whilst it's not clear what date the actual breach occurred on, the impacted data included 18M unique email addresses, IP addresses, names, usernames and links to social media profiles. As authentication is performed via social providers, no passwords were exposed in the breach. Many records didn't have associated email addresses thus the unique number is lower than the reported total number of accounts. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Title:** YouNow

**Modified Date:** 2019-07-18T08:59:45Z

**Breach Count:** 18241518

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Chegg

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

**Bio:** In April 2018, the textbook rental service <<https://techcrunch.com/2018/09/26/chegg-resets-40-million-user-passwords-after-data-breach/>> that impacted 40 million subscribers. The exposed data included email addresses, usernames, names and passwords stored as unsalted MD5 hashes. A small number of records also contained physical address or phone number. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Creation Date:** 2018-04-28T00:00:00

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

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

**Description:** In April 2018, the textbook rental service <<https://techcrunch.com/2018/09/26/chegg-resets-40-million-user-passwords-after-data-breach/>> that impacted 40 million subscribers. The exposed data included email addresses, usernames, names and passwords stored as unsalted MD5 hashes. A small number of records also contained physical address or phone number. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Title:** Chegg

**Modified Date:** 2024-04-27T05:34:09Z

**Breach Count:** 39721127

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Data Enrichment Exposure From PDL Customer

**Bio:** In October 2019, <<https://www.troyhunt.com/data-enrichment-people-data-labs-and-another-622m-email-addresses>> security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data</a>. 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

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

**Description:** In October 2019, <a href="https://www.troyhunt.com/data-enrichment-people-data-labs-and-another-622m-email-addresses" target="\_blank" rel="noopener">security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data</a>. 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.

**Title:** Data Enrichment Exposure From PDL Customer

**Modified Date:** 2019-11-22T20:13:04Z

**Breach Count:** 622161052

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Mathway

**Website:** mathway.com

**Bio:** In January 2020, the math solving website <a href="https://www.zdnet.com/article/25-million-user-records-leak-online-from-popular-math-app-mathway/" target="\_blank" rel="noopener">Mathway suffered a data breach that exposed over 25M records</a>. The data was subsequently sold on a dark web marketplace and included names, Google and Facebook IDs, email addresses and salted password hashes.

**Creation Date:** 2020-01-13T00:00:00

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

**Website:** mathway.com

**Description:** In January 2020, the math solving website <a href="https://www.zdnet.com/article/25-million-user-records-leak-online-from-popular-math-app-mathway/" target="\_blank" rel="noopener">Mathway suffered a data breach that exposed over 25M records</a>. The data was subsequently sold on a dark web marketplace and included names, Google and Facebook IDs, email addresses and salted password hashes.

**Title:** Mathway

**Modified Date:** 2020-06-05T23:59:45Z

**Breach Count:** 25692862

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** MangaDex

**Website:** mangadex.org

**Bio:** In March 2021, the manga fan site <a href="https://portswigger.net/daily-swig/mangadex-website-taken-offline-following-cyber-attack-data-breach" target="\_blank" rel="noopener">MangaDex suffered a data breach</a> that resulted in the exposure of almost 3 million subscribers. The data included email and IP addresses, usernames and passwords stored as bcrypt hashes. The data was subsequently circulated within hacking groups.

**Creation Date:** 2021-03-22T00:00:00

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

**Website:** [mangadex.org](https://mangadex.org)

**Description:** In March 2021, the manga fan site <a href="https://portswigger.net/daily-swig/mangadex-website-taken-offline-following-cyber-attack-data-breach" target="\_blank" rel="noopener">MangaDex suffered a data breach</a> that resulted in the exposure of almost 3 million subscribers. The data included email and IP addresses, usernames and passwords stored as bcrypt hashes. The data was subsequently circulated within hacking groups.

**Title:** MangaDex

**Modified Date:** 2021-04-25T21:41:24Z

**Breach Count:** 2987329

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** ParkMobile

**Website:** [parkmobile.io](https://parkmobile.io)

**Bio:** In March 2021, the mobile parking app service <a href="https://krebsonsecurity.com/2021/04/parkmobile-breach-exposes-license-plate-data-mobile-numbers-of-21m-users/" target="\_blank" rel="noopener">ParkMobile suffered a data breach which exposed 21 million customers' personal data</a>. The impacted data included email addresses, names, phone numbers, vehicle licence plates and passwords stored as bcrypt hashes. The following month, the data appeared on a public hacking forum where it was extensively redistributed.

**Creation Date:** 2021-03-21T00:00:00

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

**Website:** [parkmobile.io](https://parkmobile.io)

**Description:** In March 2021, the mobile parking app service <a href="https://krebsonsecurity.com/2021/04/parkmobile-breach-exposes-license-plate-data-mobile-numbers-of-21m-users/" target="\_blank" rel="noopener">ParkMobile suffered a data breach which exposed 21 million customers' personal data</a>. The impacted data included email addresses, names, phone numbers, vehicle licence plates and passwords stored as bcrypt hashes. The following month, the data appeared on a public hacking forum where it was extensively redistributed.

**Title:** ParkMobile

**Modified Date:** 2021-04-30T03:07:24Z

**Breach Count:** 20949825

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** LinkedIn Scraped Data (2021)

**Website:** linkedin.com

**Bio:** During the first half of 2021, <a href="https://www.businessinsider.com.au/linkedin-data-scraped-500-million-users-for-sale-online-2021-4" target="\_blank" rel="noopener">LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online</a>. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on <a href="https://news.linkedin.com/2021/june/an-update-from-linkedin" target="\_blank" rel="noopener">An update on report of scraped data</a>.

**Creation Date:** 2021-04-08T00:00:00

**Logo:** https://logos.haveibeenpwned.com/LinkedIn.png

**Website:** linkedin.com

**Description:** During the first half of 2021, <a href="https://www.businessinsider.com.au/linkedin-data-scraped-500-million-users-for-sale-online-2021-4" target="\_blank" rel="noopener">LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online</a>. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on <a href="https://news.linkedin.com/2021/june/an-update-from-linkedin" target="\_blank" rel="noopener">An update on report of scraped data</a>.

**Title:** LinkedIn Scraped Data (2021)

**Modified Date:** 2023-11-07T06:51:33Z

**Breach Count:** 125698496

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** TheGradCafe

**Website:** thegradcafe.com

**Bio:** In February 2023, the grad school admissions search website TheGradCafe suffered a data breach that disclosed the personal records of 310k users. The data included email addresses, names and usernames, genders, geographic locations and passwords stored as bcrypt hashes. Some records also included physical address, phone number and date of birth. TheGradCafe did not respond to multiple attempts to disclose the breach.

**Creation Date:** 2023-02-26T00:00:00

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

**Website:** thegradcafe.com

**Description:** In February 2023, the grad school admissions search website TheGradCafe suffered a data breach that disclosed the personal records of 310k users. The data included email addresses, names and usernames, genders, geographic locations and passwords stored as bcrypt hashes. Some records also included physical address, phone number and date of birth. TheGradCafe did not respond to multiple attempts to disclose the breach.

**Title:** TheGradCafe

**Modified Date:** 2023-03-24T04:12:17Z

**Breach Count:** 310975

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Naz.API

**Bio:** In September 2023, <a href="https://www.troyhunt.com/inside-the-massive-naz-api-credential-stuffing-list/" target="\_blank" rel="noopener">over 100GB of stealer logs and credential stuffing lists titled &quot;Naz.API&quot; was posted to a popular hacking forum</a>. 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, <a href="https://www.troyhunt.com/inside-the-massive-naz-api-credential-stuffing-list/" target="\_blank" rel="noopener">over 100GB of stealer logs and credential stuffing lists titled &quot;Naz.API&quot; was posted to a popular hacking forum</a>. 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, <a href="https://troyhunt.com/telegram-combolists-and-361m-email-

addresses" target="\_blank" rel="noopener">2B rows of data with 361M unique email addresses were collated from malicious Telegram channels</a>. 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, <a href="https://troymhunt.com/telegram-combolists-and-361m-email-addresses" target="\_blank" rel="noopener">2B rows of data with 361M unique email addresses were collated from malicious Telegram channels</a>. 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:** Stealer Logs Posted to Telegram

**Bio:** In July 2024, <a href="https://troymhunt.com/begging-for-bounties-and-more-info-stealer-logs" target="\_blank" rel="noopener">info stealer logs with 26M unique email addresses were collated from malicious Telegram channels</a>. The data contained 22GB of logs consisting of email addresses, passwords and the websites they were used on, all obtained by malware running on infected machines.

**Creation Date:** 2024-07-18T00:00:00

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

**Description:** In July 2024, <a href="https://troymhunt.com/begging-for-bounties-and-more-info-stealer-logs" target="\_blank" rel="noopener">info stealer logs with 26M unique email addresses were collated from malicious Telegram channels</a>. The data contained 22GB of logs consisting of email addresses, passwords and the websites they were used on, all obtained by malware running on infected machines.

**Title:** Stealer Logs Posted to Telegram

**Modified Date:** 2025-03-04T02:06:27Z

**Breach Count:** 26105473

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Not SOCRadar

**Bio:** In August 2024, over 332M rows of email addresses were posted to a popular hacking forum. The post alleged the addresses were scraped from cybersecurity firm SOCRadar, however [an investigation on their behalf concluded that](https://socradar.io/socradars-response-to-the-usdods-claim-of-scraping-330-million-emails/) "the actor merely utilised functionalities inherent in the platform's standard offerings, designed to gather information from publicly available sources". There is no suggestion the incident compromised SOCRadar's security or posed any risk to their customers. In total, the data set contained 282M unique addresses of valid email address format.

**Creation Date:** 2024-08-03T00:00:00

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

**Description:** In August 2024, over 332M rows of email addresses were posted to a popular hacking forum. The post alleged the addresses were scraped from cybersecurity firm SOCRadar, however [an investigation on their behalf concluded that](https://socradar.io/socradars-response-to-the-usdods-claim-of-scraping-330-million-emails/) "the actor merely utilised functionalities inherent in the platform's standard offerings, designed to gather information from publicly available sources". There is no suggestion the incident compromised SOCRadar's security or posed any risk to their customers. In total, the data set contained 282M unique addresses of valid email address format.

**Title:** Not SOCRadar

**Modified Date:** 2024-08-09T09:28:24Z

**Breach Count:** 282478425

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Hot Topic

**Website:** [hottopic.com](https://www.hottopic.com)

**Bio:** In October 2024, [retailer Hot Topic](https://au.pcmag.com/security/107921/hacker-may-have-breached-hot-topic-stolen-data-on-millions) suffered a data breach that exposed 57 million unique email addresses. The impacted data also included physical addresses, phone numbers, purchases, genders, dates of birth and partial credit data containing card type, expiry and last 4 digits.

**Creation Date:** 2024-10-19T00:00:00

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

**Website:** [hottopic.com](https://www.hottopic.com)

**Description:** In October 2024, [retailer Hot Topic](https://au.pcmag.com/security/107921/hacker-may-have-breached-hot-topic-stolen-data-on-millions) suffered a data breach that exposed 57 million unique email addresses. The impacted data also included physical addresses, phone numbers, purchases, genders, dates of birth and partial credit data containing card type, expiry and last 4 digits.

**Title:** Hot Topic

**Modified Date:** 2024-11-11T07:50:58Z

**Breach Count:** 56904909

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Stealer Logs, Jan 2025

**Bio:** In January 2025, <a href="https://troymhunt.com/experimenting-with-stealer-logs-in-have-i-been-pwned/" target="\_blank" rel="noopener">stealer logs with 71M email addresses were added to HIBP</a>. Consisting of email address, password and the website the credentials were entered against, this breach marks the launch of a new HIBP feature enabling the retrieval of the specific websites the logs were collected against. The incident also resulted in 106M more passwords being added to the <a href="https://haveibeenpwned.com/Passwords" rel="noopener">Pwned Passwords service</a>.

**Creation Date:** 2025-01-13T00:00:00

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

**Description:** In January 2025, <a href="https://troymhunt.com/experimenting-with-stealer-logs-in-have-i-been-pwned/" target="\_blank" rel="noopener">stealer logs with 71M email addresses were added to HIBP</a>. Consisting of email address, password and the website the credentials were entered against, this breach marks the launch of a new HIBP feature enabling the retrieval of the specific websites the logs were collected against. The incident also resulted in 106M more passwords being added to the <a href="https://haveibeenpwned.com/Passwords" rel="noopener">Pwned Passwords service</a>.

**Title:** Stealer Logs, Jan 2025

**Modified Date:** 2025-01-15T00:04:36Z

**Breach Count:** 71039833

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** ALIEN TXTBASE Stealer Logs

**Bio:** In February 2025, <a href="https://www.troymhunt.com/processing-23-billion-rows-of-alien-txtbase-stealer-logs" target="\_blank" rel="noopener">23 billion rows of stealer logs were obtained from a Telegram channel known as ALIEN TXTBASE</a>. 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, <a href="https://www.troymhunt.com/processing-23-billion-rows-of-alien-txtbase-stealer-logs" target="\_blank" rel="noopener">23 billion rows of stealer logs were obtained from a Telegram channel known as ALIEN TXTBASE</a>. 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

---

## HIBP

[Picture Url](#)

**Registered:** true

**Breach:** true

**Name:** Operation Endgame 2.0

**Bio:** In May 2025, <a href="https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source" target="\_blank" rel="noopener">a coalition of law enforcement agencies took down the criminal infrastructure behind the malware used to launch ransomware attacks</a> in a new phase of &quot;Operation Endgame&quot;. This followed <a href="https://www.troyhunt.com/operation-endgame/" target="\_blank" rel="noopener">the first Operation Endgame exercise a year earlier</a>, with the latest action resulting in 15.3M victim email addresses being provided to HIBP by law enforcement. A further 43.8M victim passwords were also provided for <a href="https://haveibeenpwned.com/Passwords">HIBP's Pwned Passwords service</a>.

**Creation Date:** 2025-05-23T00:00:00

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

**Description:** In May 2025, <a href="https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source" target="\_blank" rel="noopener">a coalition of law enforcement agencies took down the criminal infrastructure behind the malware used to launch ransomware attacks</a> in a new phase of &quot;Operation Endgame&quot;. This followed <a href="https://www.troyhunt.com/operation-endgame/" target="\_blank" rel="noopener">the first Operation Endgame exercise a year earlier</a>, with the latest action resulting in 15.3M victim email addresses being provided to HIBP by law enforcement. A further 43.8M victim passwords were also provided for <a href="https://haveibeenpwned.com/Passwords">HIBP's Pwned Passwords service</a>.

**Title:** Operation Endgame 2.0

**Modified Date:** 2025-05-25T21:41:13Z

**Breach Count:** 15436844

---

## TWITTER

**Registered:** true

---

## GRAMMARLY

**Registered:** true

---

## FIVERR

Registered: true

---

## IMAGESHACK

[Picture Url](#)

[Profile Url](#)

Registered: true

Username: natesmith1016

Photos: 1

---

## AUTODESK

Registered: true

---

## GUCCI

Registered: true

---

## TRENDYOL

Registered: true

---

## PINTEREST

Registered: true

---

## MAPMYRUN

[Picture Url](#)

[Profile Url](#)

Registered: true

Id: 53554932

Name: Nate Smith Jr

First Name: Nate

Last Name: Smith Jr

Language: English

Username: Nate53554932

---

## PANDORA

[Picture Url](#)

[Profile Url](#)

Registered: true

Username: natesmith1016

Followers: 0

Following: 0

Likes: 225

Stations: 47

---

## SNAPCHAT

Registered: true

---

## INSTACART

Registered: true

---

## SPOTIFY

Registered: true

---

## TUMBLR

Registered: true

---

## CALLOFDUTY

Registered: true

---

## EA

Registered: true

---

## QUORA

[Picture Url](#)

[Profile Url](#)

Registered: true

Id: 100579747

Name: Nathan Smith Jr

First Name: Nathan

Last Name: Smith Jr

Location: Los Angeles, CA

Followers: 132

Creation Date: 2015-09-17T13:38:54.358000

Bestcredential: USC-International Public Policy and Management 2020

---

## LINKEDIN

[Picture Url](#)

[Profile Url](#)

Registered: true

Id: urn:li:person:DgFauTb7EiQdZDJGlo8C8XFiXLo0u0-ldNEMwAeo-I

Name: Nathan S.

First Name: Nathan

**Last Name:** S.  
**Language:** en (us)  
**Location:** Clarkston, Michigan, United States  
**Username:** natesmithjr  
**Bio:** Impact-Driven team member at AmeriCorps: Serving with Purpose and Passion to Create Lasting Change ☑  
**Private:** false  
**Headline:** Impact-Driven team member at AmeriCorps: Serving with Purpose and Passion to Create Lasting Change ☑  
**Company Name:** AmeriCorps  
**Report Profile Url:** <https://linkedin.com/in/natesmithjr/report>  
**Connection Count:** 293

---

## MICROSOFT

[Picture Url](#)

**Registered:** true  
**Id:** C6247365CE8F6B69  
**Name:** Nathan Smith Jr  
**Location:** UK  
**Phone Hint:** \*\*\*\*\*41  
**Last Seen:** 2025-06-07T05:16:04.380000+00:00  
**Creation Date:** 2021-10-13T02:04:20.643000+00:00  
**Devices:** iOS (Authenticator)

---

## SKYPE

[Picture Url](#)

**Registered:** true  
**Id:** live:natesmith1016  
**Name:** Nathan Smith Jr  
**Username:** live:natesmith1016  
**Contact Type:** Skype4Consumer

---

## YELP

[Picture Url](#)

[Profile Url](#)

**Registered:** true

**Id:** ma0knfOdsJU1kZDJjkIKXA

**Name:** Nathan S.

**First Name:** Nathan

**Gender:** Male

**Location:** Los Angeles, CA

**Followers:** 123

**Following:** 0

**Creation Date:** 2014-08-23T23:31:11

**Name Without Period:** Nathan S

**Name With Nickname:** Nathan S.

**Share Url:** [https://www.yelp.com/user\\_details?userid=ma0knfOdsJU1kZDJjkIKXA&utm\\_source=ishare](https://www.yelp.com/user_details?userid=ma0knfOdsJU1kZDJjkIKXA&utm_source=ishare)

**Last Initial:** S

**Review Count:** 293

**Check In Count:** 565

**Tagline:** Youtuber, Photographer, Otaku, World Traveller and Language Nerd.

**Quicktip Count:** 0

**Regular Count:** 2

**Weekly Check In Count:** 3

**Thanx Count:** 20

**Business Photo Count:** 881

**User Photo Count:** 2

**First To Tip Count:** 0

**First To Review Count:** 2

**Video Count:** 3

**Moment Count:** 0

**Business Answer Count:** 0

**Business Question Count:** 0

**Follower Count:** 5

**Badge Count:** 14

**Weekly Check In Rank:** 99071

**Friend Check In Rank:** 4

**Friend Active Count:** 32

**Fmode:** 0

---