SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

The Top 12 Data Breaches of 2019

December 5, 2019

Maria Henriquez

If you do a quick search on the Have I Been Pwned website, you will get a list of how many times your personally identifiable information (PII) has been found online.

The free service aggregates data breaches and is managed by Troy Hunt, a known expert cybersecurity developer. It also helps establish if your credentials, such as IP addresses, emails, passwords, usernames, geographic locations, name and social media profiles have

been found in data breaches. According to my search, an old email I used has been compromised in 10 data breaches dating back to the Adobe 2013 data breach, and various education websites, shopping sites and more.

Just in 2018, there were 500 million personal records stolen. How many records will be stolen by year's end?

According to the RiskBased Data Breach QuickView Report 2019 Q3, at the end of September, there were 5,183 breaches, exposing 7.9 billion records. Compared to the 2018 Q3 report, the total number of breaches was up 33.3 percent and the total number of records exposed more than doubled, up 112 percent.

Will this year be the worst on record?

Security magazine brings you a list of 2019's Top 12 Data Breaches and a few honorable mentions.

12. ElasticSearch Server Breach – 108 Million Records

In January 2019, *ZDnet* reported that an online casino group leaked information on more than 108 million bets, including details about customers' personal information, deposits and withdrawals. The data leaked from an ElasticSearch server that was left exposed online without a password. ElasticSearch is a portable, high-grade search engine that companies install to improve their web apps' data indexing and search capabilities.

Justin Paine, the security researcher who discovered the server, found the user data included a lot of sensitive information, such as real names, home addresses, phone numbers, email addresses, birth dates, site usernames, account balances, IP addresses, browser and OS details, last login information and a list of played games. *ZDnet* reported that it is unclear how long the server was left exposed online, how many users were impacted, if anyone else accessed the leaky server and if customers were notified that their personal data was left exposed.

11. Canva Data Breach – 139 Million Records

In May 2019, *Security* Magazine reported that Canva, a graphic-design tool website, suffered a data breach that affected 139 million users. The data exposed included customer usernames, real names, email addresses, passwords and city and country information. In addition, of the total 139 million users, 78 million users had a Gmail address associated with their Canva account.

According to *ZDnet*, the hacker responsible for this breach has put up for sale on the dark web the data of 932 million users, which they stole from 44 companies from all over the world.

10. Chinese Job Seekers MongoDB Data Breach – 202 Million Records

In January 2019, Bob Diachenko, a cybersecurity expert and researcher from Hacken, a cybersecurity company, found a 854 gigabyte MongoDB database that contained 202,730,434 records about job candidates from China. The data contained candidate's skills and work experience, as well as PII, such as phone numbers, email addresses, marriage status, political leanings, height, weight, driver's license information, salary expectations and other highly personal data.

BJ.58.com, a Chinese classifieds company, told Diachenko the data originated from a third-party firm that collects data from many professional sites. The database was secured about a week after Diachenko discovered the breach.

9. Indian Citizens MongoDB Database – 275 Million Records

In May 2019, Diachenko once again revealed that he had discovered a MongoDB database exposing 275,265,298 records of Indian citizens that contained highly PII. The database was left unprotected for more than two weeks.

Diachenko said the publicly accessible MongoDB database hosted on Amazon AWS, included information such as name, gender, date of birth, email, phone numbers, education details, professional information (employer, employment history, skills, and functional areas) and current salaries.

8. Third-Party Facebook App Data Exposure – 540 Million Records

In April 2019, UpGuard security researchers revealed that two third-party developed Facebook app datasets were exposed to the public internet. One database originated from Cultura Colectiva, a Mexico-based media company, and weighed in at 146 gigabytes with more than 540 million records detailing comments, likes, reactions, account names, Facebook IDs and more.

The other third-party app, "At the Pool," was exposed to the public internet via an Amazon S3 bucket, say the researchers. This database backup contained columns for user information such as username IDs, friends, likes, music, movies, books, photos, events, groups, check-ins, interests, passwords and more.

7. Dream Market Breach – 620 Million Records

In February, *The Register* reported that some 617 million online account details stolen from 16 hacked websites were on sale on the dark web. The following account databases were being sold on Dream Market:

- Dubsmash (162 million)
- MyFitnessPal (151 million)
- MyHeritage (92 million)
- ShareThis (41 million)
- HauteLook (28 million)
- Animoto (25 million)
- EyeEm (22 million)
- 8fit (20 million)
- Whitepages (18 million)
- Fotolog (16 million)
- 500px (15 million)
- Armor Games (11 million)
- BookMate (8 million)
- CoffeeMeetsBagel (6 million)
- Artsy (1 million)
- DataCamp (700,000)

According to the report, sample account records consisted mainly of account holder names, email addresses and passwords. These passwords were hashed, or one-way encrypted, and had to be cracked before they could be used. Other information revealed depended on the site and included location personal details, and social media authentication tokens.

6. "Collection #1" Data Breach – 773 Million Records

In January, Troy Hunt announced he had found a set of email addresses and passwords totaling 2,692,818,238 rows, made up of many different individual data breaches from thousands of different sources. In total, there were 1,160,253,228 unique combinations of email addresses and passwords. Unique email addresses totaled 772,904,991. Unique passwords totaled 21,222,975.

Multiple people reached out to Hunt and directed him to the collection of files on the cloud service MEGA, which contained over 12,000 separate files and more than 87GB of data. In addition, he was pointed to a popular hacking forum where the data was being advertised. In the files, Hunt found his own personal data, such as email addresses and a password he used many years ago.

5. Verifications.io Data Breach – 808 Million Records

In April, Diachenko and Vinny Troia, security researcher, reported that they had found a publicly accessible MondoDB database that contained 150 gigabytes of detailed marketing data. The databased was owned by the email validation firm Verifications.io and was taken offline the same day Diachenko reached out to the company.

The database contained four separate collections of data, totaling 808,539,939 records. The largest part of it was named 'mailEmailDatabase' – and inside it contained three folders, says Diachenko:

- Emailrecords (count: 798,171,891 records)
- emailWithPhone (count: 4,150,600 records)
- businessLeads (count: 6,217,358 records)

4. First American Data Breach – 885 Million Records

In July, a data leak at First American Financial Corp., the largest real estate title insurance company in the U.S., exposed transaction records of 885 million individuals. According to Brian Krebs, American journalist and investigative reporter, First American leaked hundreds of millions of documents related to mortgage deals going back to 2003.

Records included bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts and drivers license images. The records were available without authentication to anyone with a Web browser, says Krebs.

3. TrueDialog Data Breach – More Than 1 Billion Records

Earlier this week, expert cybersecurity researchers at vpnMentor, Noam Rotem and Ran Locar, detailed their findings on the TrueDialog database leak, an American communications company. Based in Austin, Texas USA, TrueDialog creates SMS solutions for large and small businesses and currently works with over 990 cell phone operators and reaches more than 5 billion subscribers around the world.

The researchers say that the TrueDialog database, hosted by Microsoft Azure and run on the Oracle Marketing Cloud in the USA, included 604 GB of data. This included nearly 1 billion entries of highly sensitive data. The sensitive data contained in millions of SMS messages included, but was not limited to:

- Full Names of recipients, TrueDialog account holders and TrueDialog users

- Content of messages
- Email addresses
- Phone numbers of recipients and users
- Dates and times messages were sent
- Status indicators on messages sent, like Read receipts, replies, etc.
- TrueDialog account details

2. Orvibo Leaked Database – 2 Billion Records

In July, Rotem and Locar discovered an open database linked to Orvibo Smart Home products, exposing more than 2 billion records. According to the researchers, Orvibo, which runs an IoT platform, claims to have around a million users, including private individuals who connected their homes, as well as hotels and other businesses with Orvibo smart home devices.

The data breach affected users from around the world. Rotem and Locar found logs for users in China, Japan, Thailand, the US, the UK, Mexico, France, Australia and Brazil.

They first contacted Orvibo via email on June 16, and tweeted the company to alert them to the breach after they did not hear from the company. The database was open for more than two weeks. The type of data included:

- Email addresses
- Passwords
- Account reset codes
- Precise geolocation
- IP address
- Username
- User ID
- Family name
- Family ID
- Smart device
- Device that accessed account
- Scheduling information

1. Social Media Profiles Data Leak – 4 Billion Records

In October, Diachenko and Troia found a trove of data exposed and easily accessible to the public on an unsecured server, which contained 4 terabytes of PII, or about 4 billion records. A total count of unique people across all data sets reached more than 1.2 billion people, making this one of the largest data leaks from a single source organization in history, Troia and Diachenko say. The leaked data contained names, email addresses, phone numbers, LinkedIN and Facebook profile information.

The discovered ElasticSearch server containing all of the information was unprotected and accessible via a web browser. No password or authentication of any kind was needed to access or download all of the data. What makes this data leak unique is that it contains data sets that appear to originate from two different data enrichment companies, the report says.

Hunt, who found his information in the leak, says, "The recurring theme I'm finding with exposed data of this nature is increasing outrage that the data aggregator obtained and used personal information in a fashion the owner of the data (i.e. me) didn't consent to. It's not about how public the data might be through the channels people choose to publish it, rather it's about the use of the data outside its intended context."

A few other data breaches *Security* reported throughout the year are:

Capital One – 106 million records

State Farm – Unknown

Biometric Records – 27 million records

Quest Diagnostics/AMA – 24 million records

Ecuador Breach – 20 million records

Hostinger – 14 million records

DoorDash Breach – 5 million records

Choice Hotels – 700,000 records

European Hotel Group – 600,000 records

Sprint Data Breach – Unknown

This article originally ran in *Today's Cybersecurity Leader*, a monthly cybersecurity-focused eNewsletter for security end users, brought to you by *Security* Magazine. Subscribe here.

Recent Articles By Maria Henriquez

Product Spotlight on Guardhouses & Guarding Tools

How K-9 Programs are Force Multipliers

Eric Clay: Addressing Healthcare Security Challenges

Product Spotlight on Video Management Systems

Security's Choice: Our Favorite Articles From 2019

Maria Henriquez is *Security* Magazine's Associate Editor. She works with *Security*'s editor and staff to produce Newswire articles, Web Exclusive features, eNewsletter articles and more. She obtained her bachelor's degree from the University of Illinois at Urbana-Champaign in English and Creative Writing.