Devolutions

The Biggest Data Breaches of 2020

HACKERS DID NOT GO INTO "LOCKDOWN MODE."

It goes without saying that the biggest story of 2020 — or make that the 21st century so far — was the coronavirus pandemic. However, while that crisis raged on, hackers did not go into "lockdown mode." Instead, they accelerated their attacks.

Below we highlight some of the **biggest data breaches of 2020** (note that in some cases the following dates are not when the breaches initially occurred, but rather when they were first discovered and publicly revealed).

January

- The London-based currency exchange Travelex went offline due to a malware attack.
- A school district in Texas was bilked out of $2.3 million due to a phishing scam.
- A widespread data breach at the U.S. convenience store chain Wawa exposed the sensitive information of millions of customers.
- A breach at the online educational platform Unacademy exposed over 20 million user accounts.

February

- A breach at Estee Lauder exposed more than 440 million records.
- Twitter suspended a large network of fake accounts that were used to match phone numbers to users.
- The U.S. Defense Information Security Agency suffered a data breach that exposed the personal details of around 200,000 individuals.
- Clearview AI's entire client list was stolen in a data breach.
- General Electric warned its employees that an unauthorized individual was able to access their sensitive information due to security failures with a supplier.
- MGM Resorts revealed that the personal details of more than 142 million guests who stayed at the company's properties in 2019 had been published on the dark web (the number of affected guests was initially stated as 10.6 million, but it has since been revised).

March

- A breach at telecommunication provider T-Mobile allowed hackers to gain access to employee and customer data (note: in early January 2021 T-Mobile disclosed yet another breach that potentially exposed customer phone numbers and call records).
- Hotel chain Marriott suffered a cyberattack that impacted 5.2 million guests (in 2019, hackers stole the personal details from more than 383 million Marriott guests after breaching the hotel's reservation system).
- The anonymous secret sharing app Whisper was hacked, exposing the private profiles of millions of users.

- Hackers breached the social network Weibo, stealing the personal details of more than 538 million users, and offering them for sale on the dark web.
- A breach at Virgin Media exposed the data of 900,000 users, whose private information was left unsecured and accessible online for 10 months.
- Cam site CAM4.com left its production server unprotected, which exposed 10.88 billion records.
- Advanced Info Service, a Thailand-based mobile network operator, left its database exposed and publicly accessible, resulting in the leak of 8 billion records.
- Antheus Tecnologia, a Brazil-based biometrics company, left sensitive information exposed on an unsecured server, including 76,000 unique fingerprint records.

April

- The U.S. Small Business Association revealed that as many as 8,000 applicants for emergency loans may have had their personal information exposed.
- 300,000 users were impacted by a mass account hijacking campaign at Nintendo.
- A breach at email provider Email.it led to the data of 600,000 users being offered for sale on the dark web.
- More than 500,000 Zoom accounts were breached and then offered on the dark web.
- Magellan Health fell victim to a ransomware attack in which more than 365,000 patient records were compromised.

May

- A breach at the budget airline EasyJet exposed the data of 9 million customers, including some financial records.
- A ransomware attack at cloud service provider Blackbaud may have impacted hundreds of non-profit organizations (and which has subsequently led to 23 proposed consumer class action lawsuits).
- Hackers stole 220 gigabytes worth of data in a ransomware attack at Australian transportation group Toll Group.
- A breach of the voting/poll app Wishbone led to the data of 40 million users being offered on the dark web.

June

- The social media marketing firm Preen.Me disclosed that the personal data of an estimated 100,000 social media influencers had been leaked. The same breach also led to over 250,000 social media users having their data exposed on a deep web hacking forum.
- Amtrak disclosed that hackers breached the company's Amtrak Guest Rewards system and accessed customer data.
- The University of California at San Francisco paid $1.14 million to hackers in a ransomware attack.
- Rogue insiders at the South African bank Postbank stole the personal data of millions of account holders.
- A card-skimming campaign at the accessory company Claire's allowed hackers to scrape sensitive customer information.
- Wattpad suffered a data breach that exposed nearly 271 million records.

July

- The UK'S University of York disclosed a data breach that led to the theft of staff and student records (the university blamed its third-party cloud platform provider Blackbaud, mentioned above).
- A breach at the popular online casting agency MyCastingFile exposed the personal data of more than 260,000 users.
- A breach at the fitness company V Shred exposed the personal data of nearly 100,000 users.
- Energy provider EDP revealed that over 10TB in business records were stolen due to a ransomware incident.
- The Twitter accounts of some of the world's best-known personalities were compromised by hackers who used spear phishing attacks to drive traffic to Bitcoin scams.

August

- A database of nearly 235 million social media profiles connected to Instagram, TikTok, and YouTube were exposed, and unprotected by passwords or any other type of authentication.

- A security engineer at Cisco hacked his employer, which cost the company $2.4 million to fix (the rogue insider was later sentenced to two years in prison).
- YouTube took down 2 million channels and 51 million videos over scams.
- Canon disclosed that it was the victim of a ransomware attack, and that hackers stole data from the company's server.
- The same hacker group (Maze) that attacked Canon with ransomware struck LG and Xerox.
- 20GB of sensitive corporate data — including documents and records marked confidential and secret belonging to Intel — were published online.
- A breach at the luxury hotel The Ritz London allowed hackers to carry out convincing phishing attacks against guests.
- A data breach at the free photos' platform app Freepik exposed the data of 8.3 million users.
- A ransomware attack at the University of Utah compelled the institution to pay over $450,000 to stop hackers from publishing student information.
- The Experian branch in South Africa disclosed a data breach that involved 24 million users.
- Cruise operator Carnival suffered a ransomware attack that impacted customers across three different cruise lines (Carnival Cruise Line, Holland America Line, and Seabourn).

September

- A school in Nevada refused to give into ransomware demands, and in retaliation hackers published student data online.
- A hospital in Germany fell victim to a ransomware attack (initially, it was reported that this led to the death of a patient, but a subsequent investigation has concluded that the patient in question had such poor health that her death was likely not attributable to the attack — although police say that it is only a matter of time before ransomware does result in the loss of life).
- The Chilean bank BancoEstado was forced to temporarily close all of its branches due to a ransomware attack.
- Email marketing firm Mailfire was hit by a cyberattack that exposed more than 320 million records from over 70 websites.

October

- A ransomware attack at bookseller Barnes & Noble exposed customer transaction history and email addresses.
- The United Nations International Maritime Organization (UN IMO) was hit by what it called a "sophisticated cyberattack" against its IT systems.
- The telecom service provider Boom! Mobile fell victim to a card-skimming attack.
- U.S. restaurant chain Dickey's disclosed that between July 2019 and August 2020 more than three million of its customers had their card details posted online.
- The ransomware gang Egregor struck Ubisoft and Crytek, and published sensitive corporate information online.

November

- Insurance technology company Vertaforce disclosed a data breach between March 2020 and August 2020 that potentially exposed the sensitive information for 27.7 million customers.
- Beverage company Campari was temporarily kicked offline after a ransomware attack, and the company revealed that a data breach had potentially affected around 6,000 current and former employees, as well as more than 10,000 customers and suppliers.
- The hacker group ShinyHunters leaked the database belonging to Mashable.com, exposing more than 5.2GB worth of data.
- Video game maker Capcom was hit by a ransomware attack that potentially compromised the data of nearly 400,000 users.
- Brazilian aerospace company Embraer was the victim of a cyberattack that resulted in data theft.

December

- Flight Center disclosed that a hackathon in 2017 was responsible for a leak that involved the credit card data and passport numbers for nearly 7,000 customers.
- A ransomware attack at Vancouver TransLink disrupted transactions and ticketing for two days.

- A rogue employee at South African bank Absa sold the personal information of 200,000 clients to third parties.
- The UK tax office HMRC was accused of being "incompetent" regarding 11 severe data breaches that affected nearly 24,000 people.
- Leonardo SpA, the world's largest defense contractor, was hit by a malware attack that exfiltrated up to 10GB of data.
- Hackers inserted malicious code into an update of the SolarWinds software, called Orion. This hack is called supply-chain attack, since it infects software as it's under assembly. SolarWinds said that around 18,000 customers installed the tainted update onto their systems. Supply-chain attacks are to be taken seriously and are very powerful. This attack had a huge impact, which continues to grow with the discovery of new information.

Looking Ahead

Hackers stole or exposed billions of records in last year, and this year the onslaught will continue — especially against SMBs. Fortunately, there are things that SMBs can do to safeguard their data and reputation. **Click here for a look at 7 lessons learned from the biggest data breaches of 2020.**