cyber attacks in previous 10 years

2011 - Sony's PlayStation Network and Sony Pictures Suffers Multiple Attacks

2011 was a banner year for electronics conglomerate Sony, although not in a good way. Sony has become one of the most commonly cited cyber attack examples of this decade.

- The PlayStation Network (PSN), Sony's online gaming service, was attacked in April 2011. The event leaked the user data of 77M users, including names, passwords, emails, and more. Unable to control the spread of the breach, Sony's PSN platform suffered an outage for 23 days.
- Sony Online Entertainment (the company's game developer and publisher) and Qriocity (Sony's streaming service) were also closed for a month.

Sony was not only fined $400,000 by authorities in the U.K. for the above events; the company also ended up compensating the affected players in the form of digital goods.

Still, Sony's troubles that year weren't finished yet. Sony experienced a second security breach, this time by hackers' group LulzSec. Hackers said the names, credit card details, and other data they stole from Sony Pictures' websites were unencrypted. According to LulzSec's press release, "Sony stored over 1,000,000 passwords of its customers in plaintext… which means it's just a matter of taking it."

2012 - Global Payment Systems Data Breach

In April 2012, Global Payment Systems revealed a data breach due to a cyber attack. Global Payment Systems is one of the largest third-party payment system providers.

initially estimated that 1.5 million accounts were exposed. However, further news reports suggested that the number of breached accounts could go as high as seven million. As a consequence, the company incurred a huge expense of $93.9 million.

2013 Singapore cyberattacks

https://www.notion.so/cyber-attacks-in-previous-10-years-a98ae468137947d084c16fbab6e58b20?pvs=4#14e5a67641db4f88bd119edf9b423035

Anonymous

perhaps one the more iconic hacking groups in the world from the early 2000s, was linked to several security events in the news around this time. The group, an international hacktivist group which started in 2003 and was responsible for several high-profile cyber attacks against governments and large organizations, initiated a series of cyber attacks on the Singaporean government in 2013. One reason for the attacks was purportedly Singapore's web censorship regulations, particularly on news outlets. James "The Messiah" Raj, an Anonymous representative, was eventually later charged that year in a Singapore court

2013 - #OpIsrael Coordinated Yearly Cyber Attack

OpIsrael

OpIsrael (#OpIsrael), is an annual coordinated cyber-attack where hacktivists attack Israeli government and even private websites with DDoS attacks and more.[1] The inaugural campaign was launched in 2013 by Anonymous hackers on the eve of Holocaust Remembrance Day. The campaign has since been held annually.[2]

W https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiFv_6poL__AhUva2wGHZX6AiwQFnoECAwQAw&url=https://en.wikipedia.org/wiki/OpIsrael&usg=AOvVaw3q4s8CDdpl7SxnT8xhF2WQ

#OpIsrael, an “anti-Israel" attack, is a yearly, coordinated cyber attack done by hacktivists towards Israel’s government and private websites. The first #OpIsrael in 2013 was performed by Anonymous on the eve of Holocaust Remembrance Day. Per Israel’s National Cyber Bureau and security experts, that inaugural event was a failure.

adobe data breach 2013

Adobe’s CSO talks security, the 2013 breach, and how he sets priorities

Brad Arkin has led Adobe’s new approach to security and aims to make sure one of history’s biggest data breaches doesn’t happen again.

https://www.csoonline.com/article/3268035/adobe-s-cso-talks-security-the-2013-breach-and-how-he-sets-priorities.html

Despite being one of the most recognizable names in software, Adobe announced in October 2013 that its system was massively hacked.

Over 38 million users and over 152 million breached records were involved in the incident. To perform the hack, the perpetrators took advantage of Adobe’s poor encryption practices, but that’s not all: Hackers were also able to obtain over 40 GB of source code for three Adobe programs: Acrobat, ColdFusion, and ColdFusion Builder.

2013 and 2014 – Target and Home Depot Credit Card Data Stolen

It wasn't until December 2013, when credit and debit card data belonging to Target shoppers surfaced on Rescator, a Ukrainian cybercrime shop, that the cybersecurity world realized something especially massive was afoot.

- During Thanksgiving break of November 2013, Target's point of sale system was infected with malware. Customers who shopped between November 27th and December 15th of 2013 were affected. A year later, card data surfaced on Rescator. This time the card data belonged to Home Depot customers.
- Data from 110M Target consumers, including PIN data, names, credit/debit card numbers, and expiration dates were leaked. Later on, data belonging to 56M Home Depot consumers was leaked

resource

https://www.cnet.com/news/privacy/home-depot-offers-19m-to-settle-customers-hacking-lawsuit/

2013 and 2014 - Yahoo! Suffers a Massive Data Breach

In late 2014, pioneer Internet company Yahoo! experienced one of the biggest (if not the biggest) data breach in history. In this attack, a total of 500 million Yahoo! users were compromised. Every credential – names, passwords, answers to security questions – were stolen.

There’s also a separate report that Yahoo! had an earlier breach in 2013. The initial estimate of breached accounts in this particular incident was 1 billion users. Later, Yahoo! confirmed that the total number of impacted users for this breach was actually 3 billion!

What’s worse, Yahoo! didn’t report these breaches until 2016. The Securities and Exchange Commission (SEC) fined Yahoo! $35 million for untimely reporting. More than 40 class-action lawsuits were filed against Yahoo! The events also brought down the company’s sale price by around $350 million.

Yahoo! data breaches

The Internet service company Yahoo! was subjected to the largest data breach on record.[1] Two major data breaches of user account data to hackers were revealed during the second half of 2016. The first announced breach, reported in September 2016, had occurred sometime in late 2014, and affected over 500 million Yahoo! user accounts.[2] A separate data breach, occurring earlier around August 2013, was reported in December 2016. Initially believed to have

https://en.wikipedia.org/wiki/Yahoo!_data_breaches

2014 - Sony Dealt Another Blow with Attack on Sony Pictures Entertainment

Sony Pictures hacked: the full story

The Verge is about technology and how it makes us feel. Founded in 2011, we offer our audience everything from breaking news to reviews to award-winning features and investigations, on our site, in video, and in podcasts.

https://www.theverge.com/2014/12/8/7352581/sony-pictures-hacked-storystream

Three years after Sony's 2011 breaches, Sony was dealt another blow. The group Guardians of Peace claimed to have hacked Sony Pictures Entertainment's network. They stole 100 TB of data, which included film scripts, emails, and personal data of Sony employees. Sony had to cancel the airing of some of its movies and paid compensation to current and former employees.

2015 – Snapchat Users Personal Information Leaked

In 2015, messaging app service Snapchat was exposed for being not so anonymous at all. Hackers posted usernames, phone numbers, and location of 4.6 million accounts. This alarmed thousands of Snapchat users, especially those who use the app to share intimate pictures.

Snapchat was said to have been warned by hackers to address the vulnerability, but the company did not act. While Snapchat users didn't lose money here, it took over a year for the company to recover from this incident.

Snapchat hacked, info on 4.6 million users reportedly leaked

https://www.nbcnews.com/technolog/snapchat-hacked-info-4-6-million-users-reportedly-leaked-2d11833474

2015 - Office of Personnel Management (OPM) Suffers Significant Data Breach

In April 2015, the U.S. Office of Personnel Management (OPM) discovered that it was hacked. The incident was dubbed as one of the most significant breaches of government data in U.S. history.

Based on OPM and an inter-agency team's investigation, "sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases… including 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants..." The breach also included findings from interviews conducted by background investigators and approximately 5.6M fingerprints.

Office of Personnel Management data breach

The Office of Personnel Management data breach was a 2015 data breach targeting Standard Form 86 (SF-86) U.S. government security clearance records retained by the United States Office of Personnel Management (OPM). One of the largest breaches of government data in U.S. history, the attack was carried out by an advanced persistent threat based in China, widely believed to be the Jiangsu State Security Department, a subsidiary of China's Ministry of State Security spy

https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

2017 – Equifax Breach Results in Compromised Data for Nearly 150 Million

In 2017, another big credit bureau was mired in a recent data breach: Equifax.

Equifax failed to apply patches to correct a vulnerability in Apache Struts. This jeopardized the data of 147.9 million Americans, as well as Canadian and British nationals. Hackers obtained access to roughly 209,000 credit card details and social security numbers.

While it happened years ago, the Equifax breach could have far-reaching effects, particularly when it comes to exposing victims to future ID thefts. What happened to Equifax also brought up a valid question: Whether it's okay to centralize credit reporting agencies.

2017 - Shadow Brokers Leaks NSA Hacking Tools

The Shadow Brokers are an anonymous group which stole and leaked hacking tools from NSA (National Security Agency). As computers running on Windows were the ones affected, Microsoft provided a patch. However, many users didn't install the patch and were compromised.

The leaked tools led to other cyber security incidents in 2017, including NotPetya and WannaCry.

2017 – The World's First Ransomworm: WannaCry

As the world's first "ransomworm" (ransomware cryptoworm), WannaCry affected 230,000 Windows-operated computers across 150 countries. It spread through EternalBlue, an exploit made by the NSA. (EternalBlue was one of the tools stolen and leaked by the Shadow Brokers.) The perpetrators demanded ransom payments of $300 in Bitcoin cryptocurrency in exchange for unlocking files encrypted by WannaCry.

WannaCry ransomware attack

The WannaCry ransomware attack was a worldwide cyberattack in May 2017 by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated by using

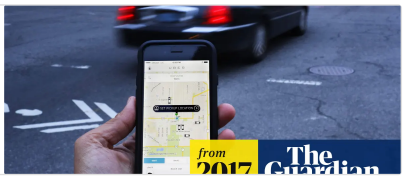
W https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

2017 – Uber Suffers Breach Impacting 57 Million Customer Data Points

Uber concealed massive hack that exposed data of 57m users and drivers

Company paid hackers $100,000 to delete data and keep the breach quiet, it emerged on Tuesday, as CEO says 'I will not make excuses for it'

https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack



Uber concealed massive hack that exposed data of 57m users and drivers

Company paid hackers $100,000 to delete data and keep the breach quiet, it emerged on Tuesday, as CEO says 'I will not make excuses for it'

https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

2018 – Hundreds of Thousands of Records Breached in British Airways Cyber Attack

15 months after British Airways' system failure at Heathrow Airport, the airline company apologized to customers for cyber attacks between August and September of 2018. Around 500,000 card payments were affected in this breach. Hackers stole names, emails, addresses, and credit card numbers, among other data.

British Airways faces a $230 million GDPR fine, about 1.5% of its 2017 revenue, over the breach.

2019 - Breaches in Singapore's Health Sectors

SINGAPORE — The personal data of more than 808,000 blood donors ended up on the Internet in January — and was left there for nine weeks — by a vendor of the Health Sciences Authority (HSA), the authorities said on Friday (March 15).

The data was taken down two days ago and secured, after a cyber-security expert discovered the vulnerability and alerted the Personal Data Protection Commission.

Personal data of 808,000 blood donors compromised for nine weeks; HSA lodges police report

SINGAPORE — The personal data of more than 808,000 blood donors ended up on the Internet in January — and was left there for nine weeks — by a vendor of the Health Sciences Authority (HSA), the authorities said on Friday (March 15).

https://www.todayonline.com/singapore/personal-data-808000-blood-donors-compromised-nine-weeks-hsa-lodges-police-report

Adult Friend Finder

Date: October 2016

Impact: 412.2 million accounts

The adult-oriented social networking service The FriendFinder Network had 20 years' worth of user data across six databases stolen by cyber-thieves in October 2016. Given the sensitive nature of the services offered by the company – which include casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, and Stripshow.com – the breach of data from more than 414 million accounts including names, email addresses, and passwords had the potential to be particularly damning for victims. What's more, the vast majority of the exposed passwords were hashed via the notoriously weak algorithm SHA-1, with an estimated 99% of them cracked by the time LeakedSource.com published its analysis of the data set on November 14, 2016.

Marriott International (Starwood)

Date: September 2018

Impact: 500 million customers

Hotel Marriot International announced the exposure of sensitive details belonging to half a million Starwood guests following an attack on its systems in September 2018. In a statement published in November the same year, the hotel giant said: "On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott quickly engaged leading security experts to help determine what occurred."

Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. "Marriott recently discovered that an unauthorized party had copied and encrypted information and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database," the statement added.

The data copied included guests' names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, and communication preferences. For some, the information also included payment card numbers and expiration dates, though these were apparently encrypted.

Marriot carried out an investigation assisted by security experts following the breach and announced plans to phase out Starwood systems and accelerate security enhancements to its network. The company was eventually fined £18.4 million (reduced from £99 million) by UK data governing body the Information Commissioner's Office (ICO) in 2020 for failing to keep customers' personal data secure. An article by New York Times attributed the attack to a Chinese intelligence group seeking to gather data on US citizens.

Facebook

Date: April 2019

Impact: 533 million users

In April 2019, it was revealed that two datasets from Facebook apps had been exposed to the public internet. The information related to more than 530 million Facebook users and included phone numbers, account names, and Facebook IDs. However, two years later (April 2021) the data was posted for free, indicating new and real criminal intent surrounding the data. In fact, given the sheer number of phone numbers impacted and readily available on the dark web as a result of the incident, security researcher Troy Hunt added functionality to his HaveIBeenPwned (HIBP) breached credential checking site that would allow users to verify if their phone numbers had been included in the exposed dataset.

"I'd never planned to make phone numbers searchable," Hunt wrote in blog post. "My position on this was that it didn't make sense for a bunch of reasons. The Facebook data changed all that. There's over 500 million phone numbers but only a few million email addresses so >99% of people were getting a miss when they should have gotten a hit."

LinkedIn

Date: June 2021

Impact: 700 million users

Professional networking giant LinkedIn saw data associated with 700 million of its users posted on a dark web forum in June 2021, impacting more than 90% of its user base. A hacker going by the moniker of "God User" used data scraping techniques by exploiting the site's (and others') API before dumping a first information data set of around 500 million customers. They then followed up with a boast that they were selling the full 700 million customer database. While LinkedIn argued that as no sensitive, private personal data was exposed, the incident was a violation of its terms of service rather than a data breach, a scraped data sample posted by God User contained information including email addresses, phone numbers, geolocation records, genders and other social media details, which would give malicious actors plenty of data to craft convincing, follow-on social engineering attacks in the wake of the leak, as warned by the UK's NCSC.

Sina Weibo

Date: March 2020

Impact: 538 million accounts

With over 600 million users, Sina Weibo is one of China's largest social media platforms. In March 2020, the company announced that an attacker obtained part of its database, impacting 538 million Weibo users and their personal details including real names, site usernames, gender, location, and phone numbers. The attacker is reported to have then sold the database on the dark web for $250.

China's Ministry of Industry and Information Technology (MIIT) ordered Weibo to enhance its data security measures to better protect personal information and to notify users and authorities when data security incidents occur. In a statement,

Sina Weibo argued that an attacker had gathered publicly posted information by using a service meant to help users locate the Weibo accounts of friends by inputting their phone numbers and that no passwords were affected. However, it admitted that the exposed data could be used to associate accounts to passwords if passwords are reused on other accounts. The company said it strengthened its security strategy and reported the details to the appropriate authority

Aadhaar [tie with Alibaba]

Date: January 2018

Impact: 1.1 billion Indian citizens' identity/biometric information exposed

In early 2018, news broke that malicious actors has infiltrated the world's largest ID database, Aadhaar, exposing information on more than 1.1 billion Indian citizens including names, addresses, photos, phone numbers, and emails, as well as biometric data like fingerprints and iris scans. What's more, since the database – established by the Unique Identification Authority of India (UIDAI) in 2009 – also held information about bank accounts connected with unique 12-digit numbers, it became a credit breach too. This was despite the UIDAI initially denying that the database held such data

The actors infiltrated the Aadhaar database through the website of Indane, a state-owned utility company connected to the government database through an application programming interface that allowed applications to retrieve data stored by other applications or software. Unfortunately, Indane's API had no access controls, thus rendering its data vulnerable. Hackers sold access to the data for as little as $7 via a WhatsApp group. Despite warnings from security researchers and tech groups, it took Indian authorities until March 23, 2018, to take the vulnerable access point offline.

Alibaba [tie with Aadhaar]

Date: November 2019

Impact: 1.1 billion pieces of user data

Over an eight-month period, a developer working for an affiliate marketer scraped customer data, including usernames and mobile numbers, from the Alibaba Chinese shopping website, Taobao, using crawler software that he created. It appears the developer and his employer were collecting the information for their own use and did not sell it on the black market, although both were sentenced to three years in prison.

A Taobao spokesperson said in a statement: "Taobao devotes substantial resources to combat unauthorized scraping on our platform, as data privacy and security is of utmost importance. We have proactively discovered and addressed this unauthorized scraping. We will continue to work with law enforcement to defend and protect the interests of our users and partners."

CAM4 Data Breach

Date: March 2020

Impact: 10.88 billion records.

Adult video streaming website CAM4 has had its Elasticsearch server breached exposing over 10 billion records.

The breached records included the following sensitive information:

- Full names

- Email addresses
- Sexual orientation
- Chat transcripts
- Email correspondence transcripts
- Password hashes
- IP addresses
- Payment logs

Many of the exposed email addresses are linked to cloud storage services. If hackers were to launch successful phishing attacks on these users, they could gain deeper access to personal photos and business information.

Due to the licentious connection of the breached database, compromised users could fall victim to blackmail and defamation attempts for many years to come.

Aadhaar Data Breach

Date: March 2018

Impact: 1.1 billion people

In March of 2018, it became public that the personal information of more than a billion Indian citizens stored in the world's largest biometric database could be bought online.

This massive data breach was the result of a data leak on a system run by a state-owned utility company. The breach allowed access to private information of Aadhaar holders, exposing their names, their unique 12-digit identity numbers, and their bank details.

The type of information exposed included the photographs, thumbprints, retina scans and other identifying details of nearly every Indian citizen.

Alibaba Data Breach

Date: July 2022

Impact: 1.1 billion users

In mid-2022, Chinese e-commerce giant Alibaba suffered a major data breach that contained customer data including:

- Names
- ID numbers
- Phone numbers
- Physical addresses
- Criminal records
- Online papers

In total, over 23 terabytes of data had been compromised from Alilbaba's cloud hosting servers, Alibaba Cloud, also the largest public cloud service provider in China. The breach was

first announced by a hacker through online forums, claiming to have data on the Shanghai police force, whose data was also hosted on Alibaba Cloud. Alibaba and its founder, Jack Ma, faced massive criticism for leaving critical servers completely unprotected with no password lock, despite handling extremely sensitive government information.

This was not Alibaba's first data breach incident, as just one year earlier, they were exposed by a third-party developer who had been scraping Alibaba's shopping site, TaoBao, for user data. Again, over a billion users were exposed and despite a three-year prison sentence for the developer and his employer, Alibaba showed that they continued to practice lax security going into 2022.

Verifications.io Data Breach

Date: February 2019

Impact: 763 million users

In February 2019, email address validation service verifications.io exposed 763 million unique email addresses in a MongoDB instance that was left publicly facing with no password. Many records also included names, phone numbers, IP addresses, dates of birth and genders.

LinkedIn Data Breach (2021)

Date: June 2021

Impact: 700 million users

Data associated with 700 million LinkedIn users was posted for sale in a Dark Web forum on June 2021. This exposure impacted 92% of the total LinkedIn user base of 756 million users.

The data was dumped in two waves, initially exposing 500 million users, and then a second dump where the hacker "God User" boasted that they were selling a database of 700 million LinkedIn.

Preview of leaked data - Source: 9to5mac.com

The hackers published a sample containing 1 million records to confirm the legitimacy of the breach. The data included the following:

- Email addresses
- Full names
- Phone numbers
- Geolocation records
- LinkedIn username and profile URLs
- Personal and professional experience
- Genders
- Other social media accounts and details

The hacker scraped the data by exploiting LinkedIn's API.

LinkedIn claims that, because personal information was not compromised, this event was not a 'data breach but, rather, just a violation of their terms of service through prohibited data scraping.

Learn about the difference between a data breach and a data leak.

But the leaked data is sufficient to launch a deluge of cyberattacks targeting exposed users, which makes the incident heavily weighted towards a data breach classification.

Canva Data Breach

d**ate:** May 2019

Impact: 137 million users

In May 2019, Australian business, Canva - an online graphic design tool - suffered a data breach that impacted 137 million users. The exposed data included email addresses, names, usernames, cities and passwords stored as bcrypt hashes.

The suspected culprit(s) — Gnosticplayers — contacted ZDNet to boast about the incident, saying that Canva had detected and remediate the cyber threat that caused the data breach. The attacker also claimed to have gained OAuth login tokens for users who signed in via Google.

Canva confirmed the incident, notified users, and prompted them to change passwords and reset OAuth tokens. This event was one of the biggest data breaches in Australia.

Heartland Payment Systems Data Breach

Date: March 2008

Impact: 134 million credit cards exposed

At the time of the breach, Heartland was processing north of 100 million credit card transactions per month for 175,000 merchants. The breach was discovered by Visa and MasterCard in January 2009 when Visa and MasterCard notified Heartland of suspicious transactions. The attackers exploited a known vulnerability to perform a SQL injection attack.

The company paid an estimated $145 million in compensation for fraudulent payments.

Badoo Data Breach

Date: July 2013

Impact: 112 million users

In June 2013, a data breach allegedly originating from social website Badoo was found to be circulated. The breach contained 112 million unique email addresses and PII such as names, birthdates and passwords stored as MD5 hashes.

Suzuki Data Breach: Car manufacturer Suzuki had to halt operations at a plant in India after a cyberattack, reports this week have alleged. According to Autocar's sources, “production has been stalled since Saturday, May 10, and it is estimated to have incurred a production of loss of over 20,000 vehicles in this timeframe.” The perpetrators of the attack have not been publicly identified by Suzuki.

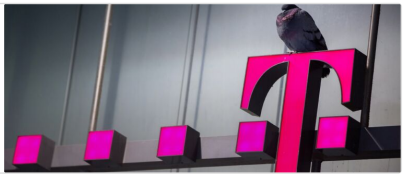
T-Mobile Data Breach: T-Mobile has suffered yet another data breach, this time affecting around 800 of the telecom provider's customers. According to recent reports, customer contact information, ID cards, and/or social security numbers were scraped from PIN-protected accounts, as well as other personal information pertaining to T-Mobile customers.

A data breach notification letter sent out to customers by T-Mobile, and subsequently published by Bleeping Computer, details the full extent of the data accessed by the threat actors. Unfortunately, this is the company's second data breach of the year. The first one, which took place in January, affected 37 million customers. T-Mobile was also breached in December 2021 and November 2022.

T-Mobile discloses 2nd data breach of 2023, this one leaking account PINs and more

Hack affecting 836 subscribers lasted for more than a month before it was discovered.

https://arstechnica.com/information-technology/2023/05/t-mobile-discloses-2nd-data-breach-of-2023-this-one-leaking-account-pins-and-more/

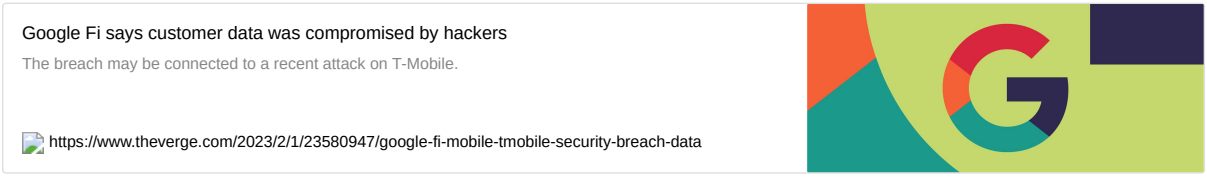


Pizza Hut/KFC Data Breach: Yum! Brands, which owns fast food chains Pizza Hut, KFC, and Taco Bell, has informed a number of individuals that their personal data was exposed during a ransomware attack that took place in January of this year. The hospitality giant confirmed that names, driver's license, and ID card info was stolen. An investigation into whether the information has been used to commit fraud already is currently underway.

MSI Data Breach/Ransomware Attack: Computer vendor **Micro-Star International has suffered a data breach**, with new ransomware gang Money Message claiming responsibility for the attack. The group says they've stolen 1.5TB of information from the Taiwanese company's systems and want $4 million in payment – or they'll release the data if MSI fails to pay.

“Say [to] your manager, that we have MSI source code, including framework to develop bios, also we have private keys able to sign in any custom module of those BIOS and install it on PC with this bios,” a member of the ransomware gang said to an MSI agent in a chat seen by Bleeping Computer.

Google Fi: February 2023 Breach



Luxottica

Rumours began to circulate late last year that Luxottica, one of the world’s largest eyewear companies, had been targeted in a cyber attack.

Luxottica – which owns popular brands including Ray-Ban, Oakley and Costa and makes sunglasses and prescription frames for the likes of Giorgio Armani, Versace and Dolce and Gabbana – has suffered several security incidents in recent years.

In August 2020, it was embroiled in a data breach affecting more than 800,000 EyeMed and Lenscrafters patients. A month later, a ransomware attack shut down the company’s operations in Italy and China.

It initially seemed as though the latest batch of stolen data might have come from one or both of those incidents.

However, cyber security researcher Andrea Draghetti discovered that the information was exfiltrated on 16 Match 2021, and concluded that the data might likely came from a separate, previously undisclosed data breach.

His research also revealed that the stolen data contains 305 lines of data, including 74.4 million unique email addresses and 2.6 million unique domain email addresses.

The information was offered for a private sale on the now-defunct hacking forum Breached, and it was later leaked in its entirety for free.

According to the seller, the database contained customers’ full names, email addresses, home addresses and dates of birth.

Luxottica says that it is investigating the incident, and in a statement added: ““We immediately reported the incident to the FBI and the Italian Police. The owner of the website where the data was posted has been arrested by the FBI, the website was shut down and the investigation is ongoing.

harMerica

The US pharmacy network PharMerica began notifying 5.8 million patients in May that it had suffered a data breach earlier this year.

In a disclosure notice to the Maine Attorney General’s Office, the organisation explained that an unauthorised party had compromised its computer systems between 12 March and 13 March.

Personal information compromised during the incident includes patients' names, addresses, dates of birth, Social Security numbers, health insurance data and medical data.

In some instances, the stolen data belongs to deceased individuals, and PharMerica has encouraged executors or surviving family members to contact the national credit reporting agencies to notify them of the breach.

The organisation did not explain how the intrusion occurred, although some reports speculate that it was a ransomware attack. One criminal gang said that it had targeted the organisation and encrypted its systems.

However, PharMerica has made no mention of ransomware in neither public statements nor its breach disclosure.

200 million Twitter users Data Breaches

200 million Twitter users' email addresses allegedly leaked online

A data leak described as containing email addresses for over 200 million Twitter users has been published on a popular hacker forum for about $2. BleepingComputer has confirmed the validity of many of the email addresses listed in the leak.

https://www.bleepingcomputer.com/news/security/200-million-twitter-users-email-addresses-allegedly-leaked-online/

Reference

https://www.digitalguardian.com/blog/biggest-moments-cybersecurity-history-past-10-years

https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

The 70 Biggest Data Breaches Ranked by Impact

Latest Breaches

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiemLOf3L__AhWTXGwGHcxTAuIQFnoECAkQAQ&u
big-company-data-breaches&usg=AOvVaw0rIHkAnx7Jb7wxzXizB58S

https://www.hackmageddon.com/2023/03/02/the-biggest-data-breaches-of-2023/