FireCompass

www.firecompass.com

October 2021

Breach Trends And Ransomware Statistics

July - Oct’ 2021

In this Breach Report, we like to present the recent Data Breaches, Ransomware attacks and also highlight the trends observed from the data breaches and attacks that happened in the first half of 2021. This Breach report covers the publicly disclosed data compromise events reported between July’21 till Oct’ 21.

In the first half of 2021, there were 352 reported data compromise events that also included ransomware as a component of the attack. The most common attack vector for enterprises experiencing a data breach was compromised credentials and the healthcare sector accounted for the most breaches during this period.

Data Breaches In The First Half Of 2021 Exposed 18.8 Billion Records

Key Trends From Recent Data Breaches & Ransomware Attacks

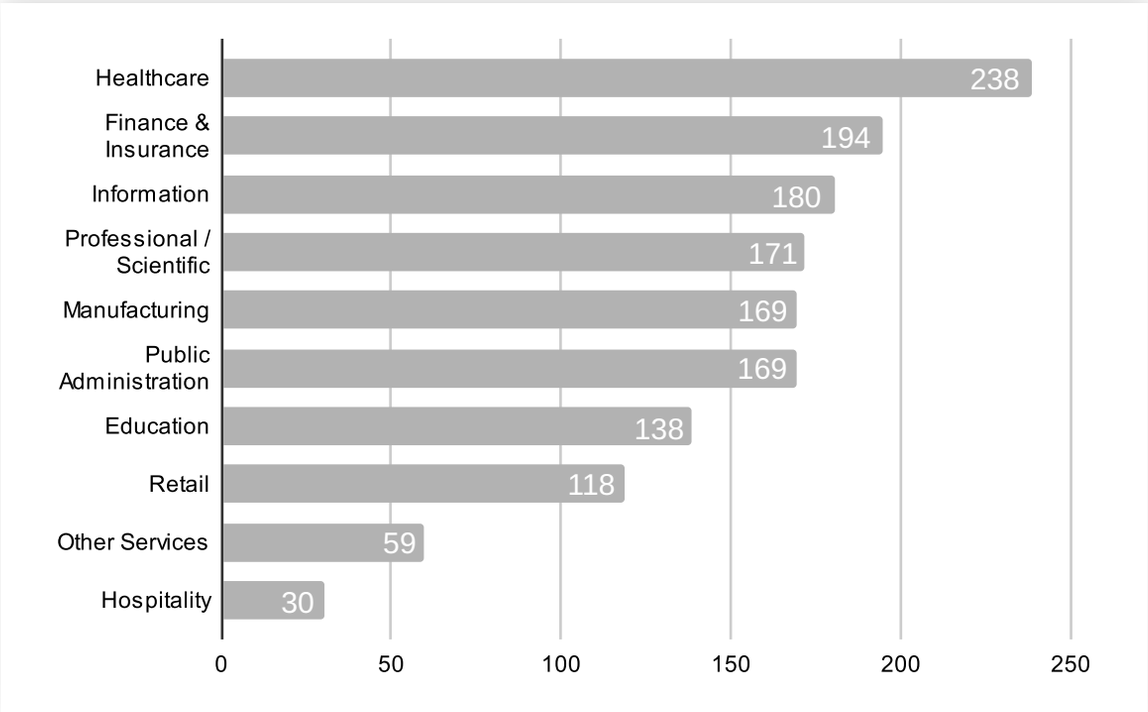
Data Breaches In The First Half Of 2021 Exposed 18.8 Billion Records

01 There were 1,767 publicly reported breaches in the first six months of 2021, which exposed a total of 18.8 billion records.

02 One breach, at the Forex trading service FBS Markets, accounted for approximately 85% of the records exposed through June 30th

03 After a high-water mark left by 2019, the percentage of breaches exposing access credentials in the form of email addresses and passwords remained consistent with other years, appearing in approximately 40% and 33% of breaches,respectively.

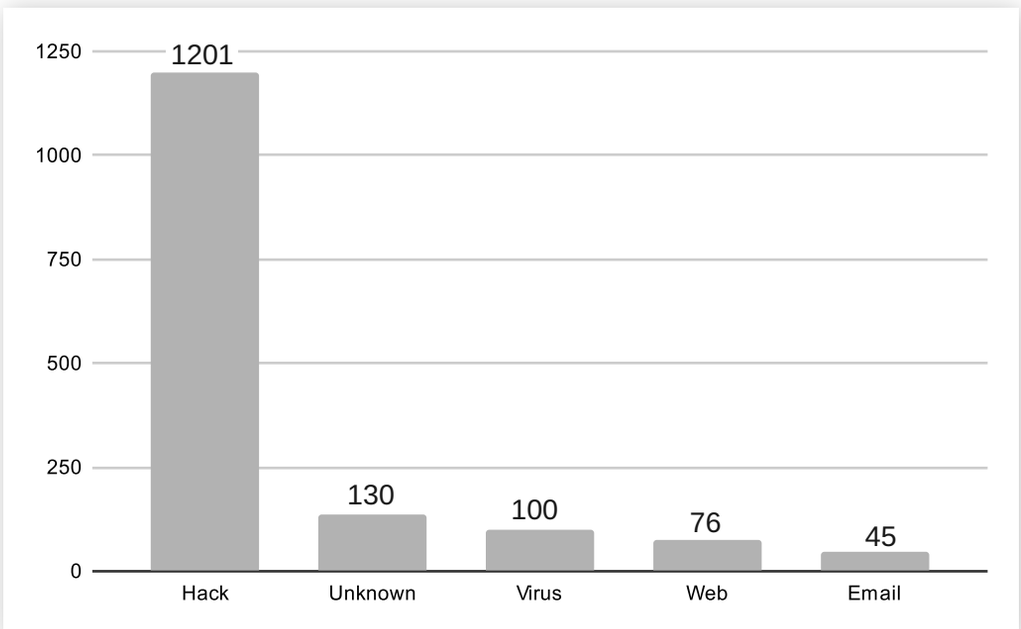
04 ## Number of breaches by industry reported by Q2, 2021



Source: Risk Based Security: 2021 Mid Year Report (Data Breach Quickview)

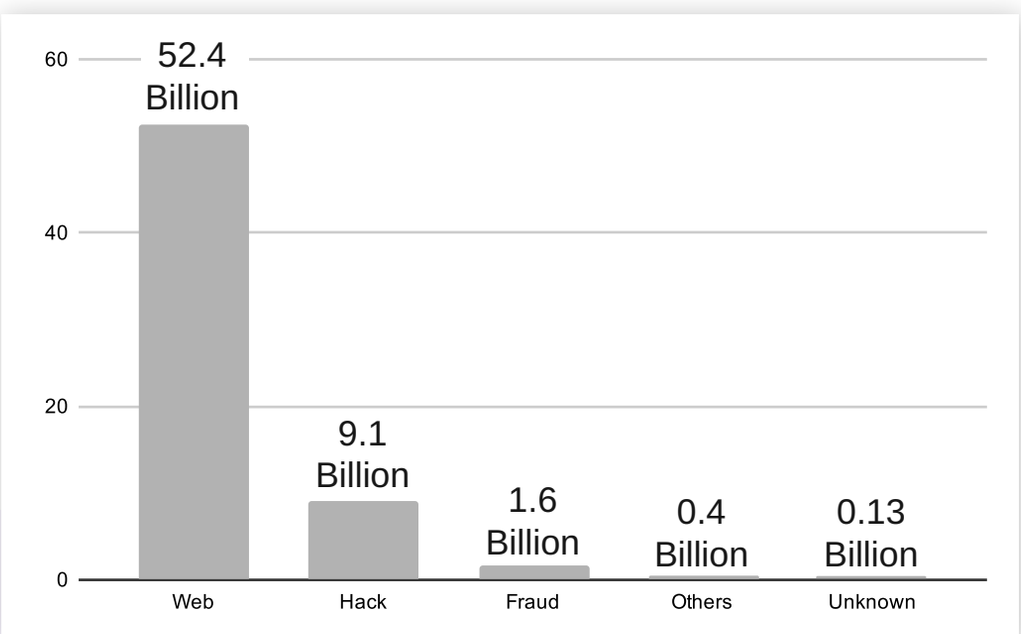
Data Breaches In The First Half Of 2021 Exposed 18.8 Billion Records

05 Number of breaches by breach type reported by Q2, 2021



Source: Risk Based Security: 2021 Mid Year Report (Data Breach Quickview)

06 Number of records lost by breach type reported by Q2, 2021



Source: Risk Based Security: 2021 Mid Year Report (Data Breach Quickview)

Enterprise Data Breach Cost Reached Record High During COVID-19 Pandemic

IBM Security released its annual "Cost of a Data Breach" report, which estimates that in 2021, a typical data breach experienced by companies now costs $4.24 million per incident, with expenses incurred now 10% higher than in 2020 when 1,000 - 100,000 records are involved.

The most common attack vector for enterprises experiencing a data breach was compromised credentials, either taken from data dumps posted or sold online, or obtained through brute-force attacks. Once a network was infiltrated, customer’s Personally Identifiable Information (PII) including names and email addresses were stolen in close to half of the cases.

Data breaches in the healthcare industry were the most expensive, at an average of $9.23 million, followed by financial services - $5.72 million - and pharmaceuticals, at $5.04 million.

Source: Cost of a Data Breach Report by IBM

Average Organization Is Targeted By Over 700 Social Engineering Attacks Each Year

A new report from cybersecurity company Barracuda has found that IT staffers and CEOs continue to face a barrage of phishing attacks throughout the year.

Barracuda analysts examined more than 12 million spear phishing and social engineering attacks impacting more than 3 million mailboxes at over 17,000 organizations between May 2020 and June 2021.

The "Spear Phishing: Top Threats and Trends Vol. 6 - Insights" report found that 43% of phishing attacks impersonate Microsoft and the average organization is targeted by over 700 social engineering attacks each year.

Nearly 80% of Business Email Compromise attacks target employees outside of financial and executive roles, with the average CEO receiving 57 targeted phishing attacks each year and IT staffers getting an average of 40 targeted phishing attacks annually. Business email compromise attacks only made up 10% of the attacks Barracuda analysts saw but have cost companies in the education, healthcare, commercial, and travel sectors millions.

Source: Spear Phishing: Top Threats and Trends Report by Barracuda

Malware Makers Using ‘Exotic’ Programming Languages

Malware authors are increasingly using rarely spotted programming languages such as Go, Rust, Nim and DLang in order to create new tools and to hinder analysis.

Reference: https://threatpost.com/malware-makers-using-exotic-programming-languages/168117

Ransom Demands Reaching $1.2M, Smaller Companies Increasingly Targeted

Ransom demands have grown substantially over the past year, smaller companies are increasingly targeted, and cyber criminals continue to take advantage of dislocations.

In first half of 2021, percentage of reported claims by category are

- Business Email Compromise (BEC) Attacks - 23%
- Funds Transfer Fraud (FTF) - 25%
- Ransomware Attacks - 22%
- Others - 30%

These attacks are also increasingly targeting small and micro businesses. In 2021, there was a 57% increase in the frequency of attacks against organizations with under 250 employees. The increased automation of cyber attacks, as well as the more widespread use of insecure remote access tools during the pandemic, has left these organizations exposed and created new opportunities for cyber criminals.

Source: Coalition Report

Significant Breaches In Q3’ 2021

Neiman Marcus Sends Notices Of Breach To 4.3 Million Customers

Neiman Marcus, the Texas-based luxury department stores chain, is sending notices of a data breach to roughly 4.3 million customers. The data breach unfolded back in May 2020 when a cyber-intruder gained access to a large number of online account credentials and used them to access private customer information. The firm discovered the incident only on September 9, 2021.

While Neiman Marcus has not explained how their systems were breached, they state that sensitive customer information was exposed, including:

- Online account username
- Online account password
- Credit card number and expiration date
- Security questions and the matching answers
- Neiman Marcus virtual gift card number
- Shipping address
- Contact information

Over 85% of the 3.1 million virtual gift cards that have been compromised were already invalidated (used) or expired. And finally, no gift card PINs were exposed to hackers. Neiman Marcus forced a reset on the affected customers' online accounts, and recipients will have to set up a new password to access their accounts.

Impact: 4.3 Million customers' data got exposed. Details like Account username & password, credit card details, virtual gift card number, contact information were exposed

Cause: A cyber-intruder gained access to a large number of online account credentials and used them to access private customer information.

Reference:
https://www.bleepingcomputer.com/news/security/neiman-marcus-sends-notices-of-breach-to-43-million-customers/

Significant Breaches In Q3’ 2021

Android Apps With 5.8 Million Installs Caught Stealing Users' Facebook Passwords

Google intervened to remove nine Android apps downloaded more than 5.8 million times from the company's Play Store after the apps were caught furtively stealing users' Facebook login credentials.

The list of apps are as follows -

- PIP Photo (>5,000,000 installs)
- Processing Photo (>500,000 installs)
- Rubbish Cleaner (>100,000 installs)
- Horoscope Daily (>100,000 installs)
- Inwell Fitness (>100,000 installs)
- App Lock Keep (50,000 installs)
- Lockit Master (5,000 installs)
- Horoscope Pi (>1,000 installs)
- App Lock Manager (10 installs)

Researchers from Dr.Web said "The applications were fully functional, which was supposed to weaken the vigilance of potential victims. With that, to access all of the apps' functions and, allegedly, to disable in-app ads, users were prompted to log into their Facebook account”.

The offending apps masked their malicious intent by disguising as photo-editing, optimizer, fitness, and astrology programs, only to trick victims into logging into their Facebook accounts and hijack the entered credentials via a piece of JavaScript code received from an adversary-controlled server.

The latest disclosure comes days after Google announced new measures for the Play Store, including requiring developer accounts to turn on 2-Step Verification (2SV), provide an address, and verify their contact details as part of its ongoing efforts to combat scams and fraudulent developer accounts.

Impact: This attack could have been easily expanded to load the login page of any legitimate web platform with the goal of stealing logins and passwords from a variety of services.

Cause: The offending apps masked their malicious intent by disguising as photo-editing, optimizer, fitness, and astrology programs, only to trick victims into logging into their Facebook accounts and hijack the entered credentials via a piece of JavaScript code received from an adversary-controlled server.

Reference:
https://thehackernews.com/2021/07/android-apps-with-58-million-installs.html

Significant Breaches In Q3’ 2021

Meat Giant JBS Pays $11m In Ransom To Resolve Cyber-Attack

The world's largest meat processing company has paid the equivalent of $11m (£7.8m) in ransom to put an end to a major cyber-attack. Computer networks at JBS were hacked in June, temporarily shutting down some operations in Australia, Canada and the US.

JBS, a Brazil-based company, said that, "preliminary investigation results confirm that no company, customer or employee data was compromised," in the hack on its systems. The company added that it paid the money because of the sophistication of the attack, even though the "vast majority" of its plants remained operational.

Impact: The company was forced to halt cattle slaughtering at all of its US plants for a day.

Cause: Ransomware attack: Hackers get into a computer network and threaten to cause disruption or delete files unless a ransom in cryptocurrency is paid

Reference:
https://www.bbc.com/news/business-57423008

UC San Diego Health Breach Tied To Phishing Attack

Authorities at the University of California San Diego Health reported a phishing attack led to a major breach of its network, which allowed an adversary to gain access to sensitive patient, student and employee data.

Post investigation, UCSD Health said it will contact individuals whose personal data was exposed and offer them a year of free identity theft protection services. However, experts point out, the potential risks associated with this type of data loss could impact victims for years.

Robert Prigge, CEO of Jumio said, “Fraudsters can leverage the medical records, lab results, Social Security numbers and government identification numbers to impersonate legitimate patients and commit insurance fraud, seek covered medical care and refill unauthorized prescriptions. It’s also possible the exposed information is already circulating on the dark web – where it can command a high value since there’s more personal information in health records than any other electronic database.

Impact: 700M users' data got exposed. The database is for sale on the dark web, with records including phone numbers, physical addresses, geolocation data, and inferred salaries.

Cause: Employee email takeover exposed personal, medical data of students, employees and patients. Exposed personal information includes full names, addresses, date of birth, email, social security number and the date and cost of medical services.

Reference:
https://threatpost.com/uc-san-diego-health-breach/168250/

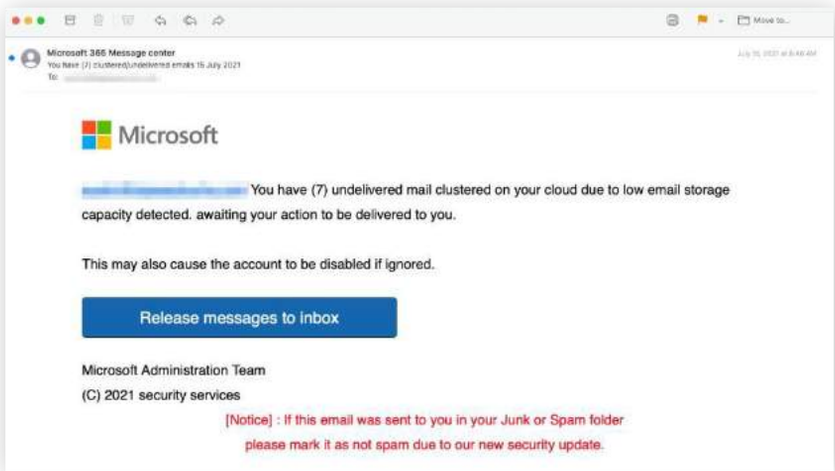
Significant Breaches In Q3’ 2021

Spam Is Chipotle's Secret Ingredient: Marketing Email Hijacked To Dish Up Malware

Between July 13 and July 16, someone took over the Mailgun account owned by restaurant chain Chipotle Mexican Grill and placed an order for login credentials using misappropriated marketing messages. Phish-fighting firm INKY said that it spotted 121 phishing emails during this period originating from Chipotle's Mailgun account. This particular approach to phishing was employed successfully by the Nobelium group infamous for its attack on SolarWinds.

The phishing messages included two fake voicemail notifications with attached malware, otherwise known as "vishing" among those who make such distinctions. They also included 14 emails designed to look like USAA Bank communiques and 105 messages dressed up as if they came from Microsoft. These faked missives pointed recipients to credential harvesting websites designed to mimic USAA Bank and Microsoft Sign-in pages respectively.

But a sample Microsoft phishing message (originating from mail.chi-potle.com) published by INKY suggests that inconsistency would not have been visible to recipients.



One advantage of hijacking email marketing accounts is that such services tend to make an effort to ensure their messages get delivered by minimizing reputation-tarnishing spam and applying messaging security technology like SPF, DKIM, and DMARC.

Impact: If a Chipotle employee opens an email attachment with malware then it's possible to compromise the employee's account or device.

Cause: Hijacking email marketing accounts (emails originated from Mailgun servers) to filch credentials from customers of USAA Bank, Microsoft. 14 emails designed to look like USAA Bank communiques and 105 messages dressed up as if they came from Microsoft.

Reference:
https://www.theregister.com/2021/07/29/mailgun_chipotle_malware_spam/

Significant Breaches In Q3’ 2021

Thorchain Suffers $8 Million Loss By Hacker Wanting To 'Teach Lesson'

Thorchain has been exploited for the third time in July month, bringing total losses to around $13 million. The platform, which looks after $100 million in funds, is designed for exchanging crypto tokens across different blockchains.

In this attack, the platform was exploited for $8 million as the hacker was able to trick the network into thinking they had deposited a range of funds, when they hadn’t, and then somehow getting a refund. But the hacker made sure to leave a note explaining that the attack could have been much more damaging.

Thorchain acknowledged that it had suffered a “sophisticated attack” and that the hacker knowingly limited its impact. It said that the hacker requested a 10% bounty of the stolen funds and that the treasury has the money to cover the exploit. But it added that now's the “time to slow down.”

Prior to this attack, Thorchain suffered a relatively minor $140,000 incident in late June and a $5 million hack just a week before this sophisticated attack.

Impact: Thorchain planned to keep the network halted for now as it is reviewing the code. Then it will restore solvency (which could include paying the bounty). Once everyone is satisfied with the security of the network, it will be restarted.

Cause: Sophisticated Attack: The hacker was able to trick the network into thinking they had deposited a range of funds, when they hadn’t, and then somehow getting a refund.

Reference:
https://www.theblockcrypto.com/post/112308/thorchain-suffers-8-million-loss-by-hacker-wanting-to-teach-lesson

Significant Breaches In Q3’ 2021

Amazon Gets $888 Million GDPR Fine For Behavioral Advertising

Amazon has quietly been hit with a record-breaking €746 million fine for alleged GDPR violations regarding how it performs targeted behavioral advertising. The fine was issued by Luxembourg's Commission nationale pour la protection des données (CNPD), an independent public agency established to monitor the legality of the collection and use of personal information.

Amazon states that this massive fine came out of CNPD in July 2021, which fined them for improper processing of personal data.

"On July 16, 2021, the Luxembourg National Commission for Data Protection (the “CNPD”) issued a decision against Amazon Europe Core S.à r.l. claiming that Amazon’s processing of personal data did not comply with the EU General Data Protection Regulation," reads an SEC 10-Q filing submitted by Amazon in July month.

The complaint alleges that Amazon is analyzing users' behavior to build profiles used for targeted advertising. This creation of these behavioral profiles is being done without a user's consent and thus violates GDPR. Amazon has told BleepingComputer that this fine is not related to a data breach or unauthorized access to customer data but rather how they perform advertising.

Reference:
https://www.bleepingcomputer.com/news/technology/amazon-gets-888-million-gdpr-fine-for-behavioral-advertising/

Swedish Coop Supermarkets Shut Due To US Ransomware Cyber-Attack

500 Coop supermarket stores in Sweden have been forced to close due to an ongoing "colossal" cyber-attack affecting organisations around the world.

The supermarket was not itself targeted by hackers - but is one of a growing number of organisations affected by an attack on a large software supplier the company uses indirectly. Cyber-security firm Huntress Labs said the hack targeted Florida-based IT company Kaseya before spreading through corporate networks that use its software. The firm believes the Russia-linked REvil ransomware gang was responsible.

Impact: Coop Sweden closed more than half of its 800 stores after point-of-sale tills and self-service checkouts stopped working.

Cause: "colossal" cyber-attack affecting organisations around the world.

Reference:
https://www.bbc.com/news/technology-57707530

Significant Breaches In Q3’ 2021

GETTR, Social Media App Hacked On Launch Day As Half Million Sign Up

GETTR, a Twitter-style platform with posts and trending topics launched by Jason Miller, was briefly hacked, and more than 500,000 people have registered to use the site

"The problem was detected and sealed in a matter of minutes, and all the intruder was able to accomplish was to change a few user names," Miller said in an emailed statement to Reuters.

Reference:
https://www.reuters.com/world/us/pro-trump-social-media-app-hacked-launch-day-half-million-sign-up-2021-07-04/

About FireCompass

FireCompass is a SaaS platform for Continuous Automated Red Teaming (CART) and External Attack Surface Management (EASM).

FireCompass continuously indexes and monitors the deep, dark and surface webs using nation-state grade reconnaissance techniques. The platform automatically discovers an organization’s digital attack surface and launches multi-stage safe attacks, mimicking a real attacker, to help identify breach and attack paths that are otherwise missed out by conventional tools.

Use Cases

- Red Team Augmentation / Adversary TTP Emulation
- Risk Based Prioritization using Custom Attack Playbooks
- Attack Surface Reduction / Shadow IT Monitoring
- Ransomware Attack Surface Testing
- SOC Augmentation/Effectiveness Testing
- Post Compromise Assessment / Breach Risk Assessment
- Management Assurance / Control Effectiveness Testing
- Enrich Threat Intelligence Program

To learn more, visit: www.firecompass.com