Top 5 highest-profile data breaches

Cybercriminals are coming for corporate wallets

Cybercriminals are currently exploiting the COVID-19 pandemic to carry out highly advanced cyberattacks, irregardless of industry or company size. In 2020, several Fortune 500 businesses became victims of major data breaches, after which hackers were able to sell account credentials and sensitive data, as well as confidential and financial records of these organizations.

Here are the 5 highest-profile data breaches in the past year.

1. Zoom credentials hack

In the first week of April 2020, more than 500,000 stolen Zoom passwords were reported to be available for sale on the dark web, concerning many of the millions of brand-new users of the application. Some of the credentials were given away for free, while others were sold for as little as a penny each. The credentials each contained the username, password, registered email address, host key, and personal meeting URL. Such data gives a malicious actor access not just to the account, but to the contents of any meetings it might have either hosted or been a part of. So, in terms of the leaked private or confidential information, the total number of impacted users is probably far greater than the number of accounts for sale.

2. Twitter phishing attack

On July 15, a tweet was shared on a number of high-profile accounts, including Barack Obama's, Joe Biden's, Bill Gates's, and Elon Musk's. "I'm giving back to the community. All bitcoin sent to the address below will be sent back doubled! If you send $1000, I will send back $2000. Only doing this for 30 minutes." The tweet reached more than 350 million people and resulted in the recovery of $121,000 (£86,800) bitcoin in stolen "donations" within hours.

As Twitter announced later, "This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to our internal systems."

The company described it as a case of "social engineering", where a hacker uses psychological manipulation to trick someone into giving away their login credentials or other sensitive information.

3. Marriott social engineering attack

In March 2020, the Marriott Hotel Group suffered a huge data breach, which compromised the records of 5.2 million hotel guests.

Hackers were able to siphon off the data of 5.2 million guests by hacking the user credentials belonging to just two members of Marriott's staff. This attack highlights the importance of company employees using multi-factor authentication and the potentially huge penalties for

failing to do so.

“Zero Standing Privileges could also be used as part of a company’s defense strategy in such cases. This means that a user is granted access privilege only for a particular task and only for a time needed to complete it. Afterwards, the privilege is rescinded. If the user’s credentials get compromised, even an insider perpetrator will not have immediate access to the business’s data and systems,” comments NordLayer Chief Technology Officer Juta Gurinaviciute.

4. Nintendo credential stuffing attack

In April 2020, the online gaming pioneer Nintendo suffered a major data breach, when more than 160,000 user accounts were compromised in a single attack. Hackers initiated a credential stuffing attack and later used the online accounts to buy digital products through the Nintendo network.
Such attacks are common in the gaming and media sector, with Disney, Spotify, and the streaming giant Netflix all falling victim to similar attacks over the past year.

After the attack, Nintendo stopped allowing users to log in using their Nintendo Network ID (NNID). The company also recommended that users secure their data by using two-factor authentication mechanisms.

5. easyJet credential theft

The UK-based low-cost airline easyJet announced that cybercriminals had stolen data records of 9 million customers. With Europe’s strict GDPR rules, companies that breach data protection regulations could be in for some eye-watering penalties. The law firm PGMBM filed a class action lawsuit on behalf of the affected easyJet customers for $23 billion (£18bn).
In addition to the 9 million easyJet customers who had their personal details compromised, 2,200 also had their credit card details exposed, compounding the potential damage.
While easyJet promptly reported the matter to the Information Commissioner's Office and other regulatory authorities, critics have claimed that the low-cost airline was slow to inform its customers about the breach, with some customers not finding out about it for up to 4 months after the events.

Corporate security challenges

According to IBM’s 2020 Cost of a Data Breach Report, stolen or compromised credentials and cloud misconfigurations are the most common causes of malicious breaches.

“With over 8.5 billion records exposed in 2019, and attackers using previously exposed emails and passwords in one out of five breaches, businesses should rethink their security strategy and consider the adoption of a zero-trust approach – reexamining how they authenticate users and the extent of access users are granted,” comments Juta Gurinaviciute, Chief Technology Officer at NordLayer.

Similarly, companies' struggle with security complexity – a top breach cost factor – is likely contributing to cloud misconfigurations becoming a growing security challenge. The same report also revealed that attackers used cloud misconfigurations to breach networks nearly 20% of the time, increasing breach costs by more than half a million dollars to $4.41 million on average. This was also mentioned as the third most expensive initial infection vector.

Companies and their employees have been thrust into a remote working environment rather suddenly, with many organizations’ remote networking capabilities still not as shielded as their

on-premise IT infrastructures. This rapid shift has left many unsecured gaps that malicious actors are looking to exploit for financial gain — or to simply disrupt usual operations. The priority now is to secure endpoints and implement stronger authentication protocols for the cloud and other off-premise networks.

“Security teams have to develop strong policies to respond to the security challenges the world is facing, but their work doesn’t end there. They need to effectively communicate those policies to entire workforces and train employees on how to respond to them. Without a security awareness program, risk management strategies can become less effective, and we continue seeing the damaging effects this can have,” concludes the NordLayer expert.