There were 12,449 serious data breaches recorded in 2018, an increase of 424% compared to 2017

A recent statistical report showed alarming facts. Specifically, the number of confirmed data violations in 2018 has reached 12,449 cases, an increase of 424% compared to 2017.

A recent statistical report showed alarming facts. Specifically, the number of confirmed data violations in 2018 has reached 12,449 cases, an increase of 424% compared to 2017. In addition, up to 47% of all records are identified as infringing comes from organizations related to the United States and China.

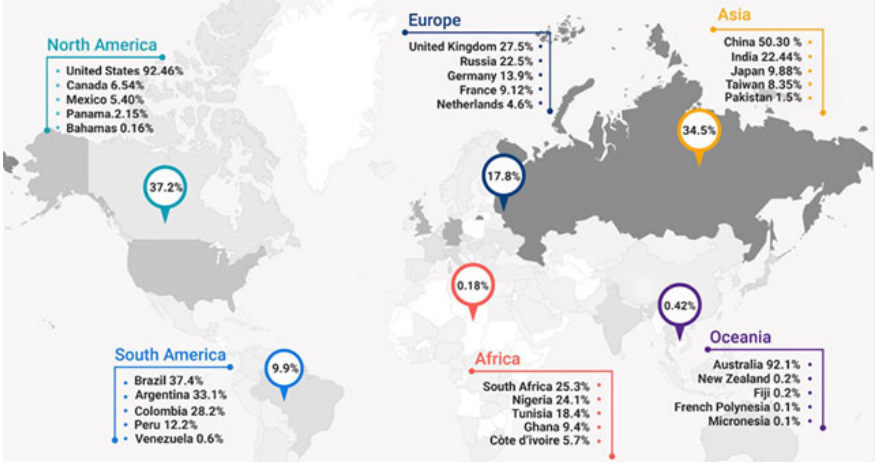
4IQ, the intelligence company identified network security has published this report. Considering the context and trend of data infringement, the company also discovered that although the number of violations has increased sharply last year, but the scale and scope of their average influence has Significantly decreased, down to 216,884 files illegally violated, 4.7 times less than the previous year (2017).

The company has defined data breaches as 'confirmed incidents', in which most data such as personal, medical, financial or other types of records contain sensitive data. Feelings have been accessed or disclosed due to hacked or leaked, either intentionally or unintentionally.

1. McAfee expert explained how deepfake and AI are drilling through the cyber security wall

The United States leads the list of losses caused by unauthorized access

The 4IQ report also revealed the fact that crooks are moving away from the direction of action, from trying to penetrate large, but profitable and extremely large organizations and corporations. , to attack small businesses that are less protected. This is also one of the factors contributing to the increase in the number of violations related to data discovered in 2018.



Although overall, the number of data breaches is not much like the United States, but the scale of the cases tends to be larger, causing more damage to this country.

In addition, 2018 saw a 'jump' in the number of underground internet activities exposed, up to 71%, with 14.9 billion identity records stolen, circulated and exchanged and worn. Although only 3.6 billion of them are new and authentic.

"As our personal data continues to be exposed and circulated in the underground data buying and selling markets, that indicates an obvious problem is that identity-based attacks are on the rise. On the other hand, users also need to be more proactive in implementing measures to prevent incidents, such as activating two-factor authentication, using a password manager, etc. However, they also need to take a more proactive approach to protecting themselves, such as registering identity theft services, such as exposure warnings and security troubleshooting. and risk insurance, '4iQ CEO, Mr. Monica Pal shared.

1. Supercomputers can completely detect cyber threats

In 2018, the number and scale of violations became a "new standard".

In addition, CTO Julio Casal, co-founder of 4iQ, also said that last year, politics and related fields were the target of receiving the most attention from hackers, with an increase of more than 291. % compared with 2017. The cause can be attributed to the increased tension in political elections and disputes between multiple parties, or more widely, among countries. In 2018, underground data moguls were particularly interested in data types such as citizen identities or voter databases . as part of a list of outstanding data purchases.

In addition, 2018 is also the year when the number of data storage devices with Internet connection leaks is increasing rapidly, and this trend is expected to continue in this 2019 year. Therefore, companies, organizations and businesses, regardless of their size and size, need to be more careful in securing their databases.

4iQ also emphasized the occurrence of similar serious data violations, affecting large companies, leading to millions of important records that were leaked to billions of dollars:

'In 2018, big companies like Google, Facebook, Marriott . have been' named 'on the hackers' preferred target list with new reports reported almost daily, and it is This has contributed to the new assessment criteria for data breaches, in both incremental and quantitative directions. '

1. DDoS is ranked as the top threat for businesses in 2018

4iQ's identity violation report of 2018 uses data compiled from extensive statistics on both leaked and infringing data obtained from many publicly available open sources, in deep web and dark web , as well as from the black market, social networks and underground forums and communities.

The data in the report is collected with the help of automated crawlers and analyzed by the company's violating hunting team, using intensive data verification methods.