Customer data collected during Capital 14's 14 years was stolen

This may be considered the biggest data theft ever recorded in the US.

Capital One, one of the largest financial-banking groups in the United States, is the latest victim of a massive security breach, affecting data from 2005 to 2019.

This may be considered the largest data theft ever recorded in the US when the amount of leaked data is valid for about 14 years, with the number of records stolen the most, simultaneously in the time The longest ever known in the history of global computing.

Due to the seriousness of the incident and pressure from customers, Capital One was forced to issue an emergency release, providing more details about the case before the press and the public.

1. Alarming statistics on the situation of network security in our country in the first half of 2019

Capital One, one of America's largest financial corporations, has been hacked

According to statistics, the incident affected more than 100 million Capital One customers in the US and about 6 million people in Canada. The personal information of 106 million people was stolen from the company's general database, after a series of complex network attacks, 'drill straight' into unpatched system vulnerabilities. Among the leaked data, there were 140,000 Social Security numbers - the most important information in the US, 1 million Canadian Social Insurance numbers and 80,000 bank account numbers. In addition, there are many other information related to name, address, credit score, credit limit, balance sheet . and other information that has not been disclosed in detail, according to the bank. and the US Department of Justice (DOJ). Capital One's

board of directors said that the investigation is still being implemented actively, and apologizes to customers.

The giant financial group confirmed that the data breach was discovered through important disclosures from a number of white-hat hacker groups on July 17, 2019. The company's internal security team was officially confirmed the incident after the internal investigation result was released on July 19, 2019. Thus, within a short period of time from 22 to 23 March 2019, the attackers obtained amount of customer data is equivalent to 14 years (from 2005 to 2019) of Capital One.

In the latest press release, the company announced it had overcome the flaw and said that no sign of unauthorized use of user information has been found, at least until August 2, 2019. .

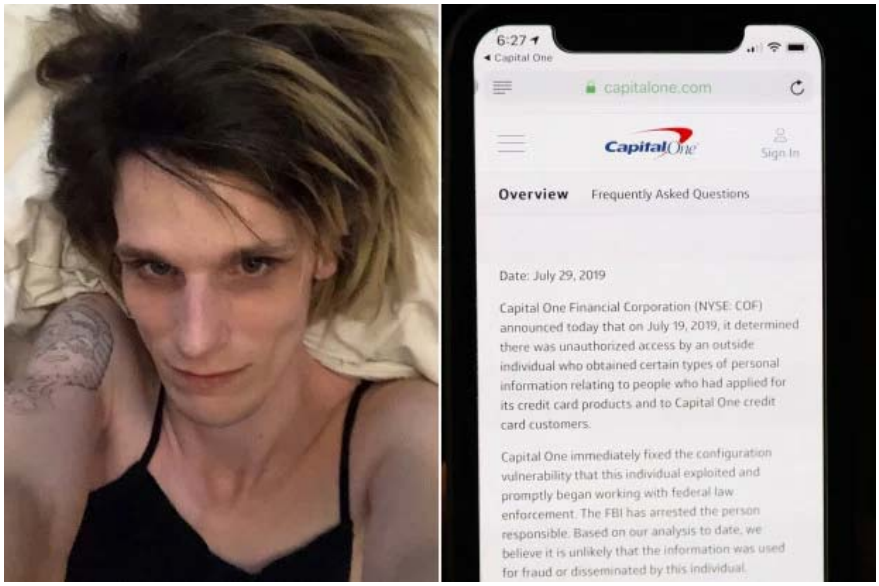
1. More than 1 million payment card information from Korea is sold on Dark Web

'I am very grateful that the security agencies have quickly entered and made the attackers pay for their behavior. However, I also want to send the most sincere apology to Capital One's customers for all the trouble that this unfortunate incident caused, and committed to do all my responsibility to make every attempt to the right trajectory. " Richard D. Fairbank, CEO and Board Chairman Capital One, told a news conference.

According to the latest information provided in a press release, Capital One confirmed the suspect caused the incident was currently detained by the Federal Bureau of Investigation, and very unexpectedly, a female hacker.

Paige Thompson was the woman who had been accused of infiltrating the Capital One server and gaining access to the company's huge user database. The investigation agency said the suspect was found trying to share the information she had obtained with several other individuals online. This 33-year-old woman currently lives in Seattle, once a software engineer at the company providing cloud platform for Capital One.

1. Ransomware (ransomware) is showing signs of explosion worldwide, paying is no longer the most effective option.



Paige Thompson - the main suspect of the hack

Paige Thompson's behavior was quite amateurish and quickly discovered when she used her real name to post information on GitHub and 'show off' on social media that she was holding Capital One's data.

It is not yet possible to determine whether the stolen information has been used for identity theft campaigns. However Capital One bluntly dismissed the initial rumors of data breaches stemming from uncontrolled cloud access activities. At the same time, affirming the cloud infrastructure that Capital One uses is a separate system and is not affected by this incident.

In addition, Capital One also affirmed that there were no cases of credit card information related to the breach. Approached information mainly includes data from both individual customers and business customers who have traded with Capital One in the period from 2005 to 2019. Profile of customers within that 14-year time frame including:

1. First and last name
2. Residential address
3. ZIP code
4. Email address
5. Contact number
6. Birthday
7. Income declared by itself

After this serious incident, Capital One pledged to provide maximum support policies for affected customers, while providing free credit monitoring and identity protection packages.

1. What is data exfiltration? How to prevent this dangerous behavior?

The hack could cost Capital One a lot of damage, up to $ 150 million

The hack is likely to cost the Capital One 100 to 150 million dollars in related costs, including giving users alerts, credit tracking, technical costs and legal assistance, as well as strengthen the intranet system.