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

Data related to personal payment cards of more than 1 million Koreans were sold by hackers on various Dark Web platforms.

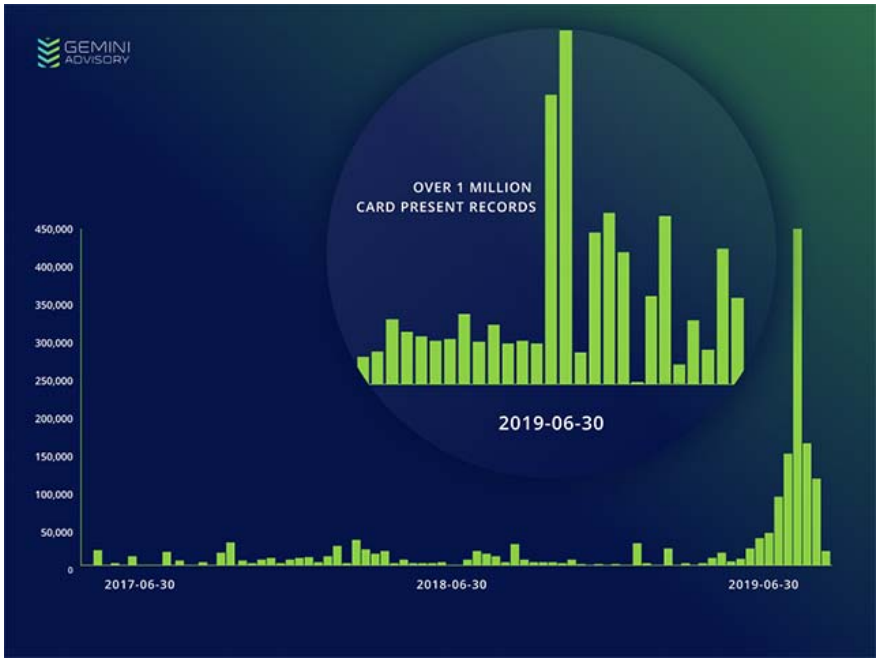
Recently, a large amount of detailed information regarding personal payment cards of more than 1 million Koreans has been sold by hackers on various Dark Web platforms. This information coincides with reports on the situation of cybersecurity having complicated developments in Korea over the past few months, leading to an alarming increase in the number of stolen personal data, especially especially data related to the financial sector - banking.

1. Honda's database leaked, revealing many "deadly" weaknesses in the intranet system

*A large amount of Korean citizens' payment information was stolen and sold*

## The act of stealing payment card information tends to increase strongly in Korea

In June, international security researchers recorded more than 230,000 cases of personal financial records sold publicly on black web exchanges originating in South Korea. This can be seen as an alarmingly unusual increase compared to the 42,000 records recorded in May - which is an 'acceptable' level, often seen many months earlier.




*The amount of personal payment records of Korean citizens was raised for sale in June 2019*

The source of this increase has not been determined at the present time, however, the amount of data leaked mainly comes from transactions related to domestic enterprises.

This supports the assumption that all points of sale (point-of-sale - PoS) across Korea have been illegally trespassed and have resulted in leakage of registration information. The reason PoS became a "lucrative" target in the eyes of cyber criminals is because this service interacts with many payment devices from different sources.

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

## Great demand is that data selling prices nearly doubled

Gemini Advisory security researchers conducted monitoring activities related to the sale of payment card information on multiple Dark Web platforms over the past few years, and said the need to purchase records Payments by Korean citizens last year only reached a relatively low level compared to other countries in the region and the world. The reason may be due to a large supply, exceeding demand. However, this situation has changed completely in the first 6 months of this year when the supply for personal financial data is not too volatile but the demand has increased significantly.


*Large demand for bank card data made the price nearly doubled*

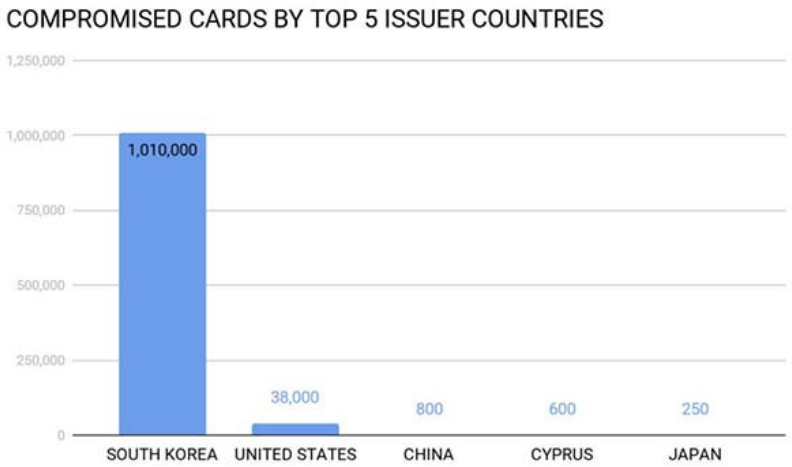
The current context also makes the average selling price per set of records increase significantly. Last year, each set of records for payment cards of Korean citizens sold for an average of $ 24. However, the increasing demand for this type of data this year has pushed prices up dramatically, hitting an average of $ 40, and is expected to increase further in the last months of the year.

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

## US cardholders are also affected

The researchers also observed a rather strange phenomenon, as up to 3.7% of the compromised payment card records in Korea originated from the United States.

"One of the most affected financial institutions in the United States is a credit union primarily serving the US Air Force. It is known that the US Air Force currently maintains many important bases in Korea. A closer look at the compromised data shows that many of the payment cards belong to US citizens and have been to Korea, 'Gemini Advisory experts said.




The number of cardholders leaking information by nationality, 3.7% came from the United States

Stealing payment data from bank card transactions is usually done through the spread of malware on systems that connect to PoS devices at business establishments. In many cases, an attack vector is a remote computer connection that is protected by default or easily guessed password.

1. Hacker successfully stole 100,000 photos from border control database

Malware installed in this way after spreading on the target system can silently copy payment data stored in RAM (memory scan) after each customer uses a bank card. to transaction. This is entirely possible because most of the card information stored in RAM is not encrypted.