

Taiwan ATM heist linked to European hacking spree: security firm

 [reuters.com/article/us-taiwan-cyber-atms/taiwan-atm-heist-linked-to-european-hacking-sprees-security-firm-idUSKBN14P0CX](https://www.reuters.com/article/us-taiwan-cyber-atms/taiwan-atm-heist-linked-to-european-hacking-sprees-security-firm-idUSKBN14P0CX)

Jim Finkle, J.R. Wu



Banks

Updated

By Jim Finkle, J.R. Wu

3 Min Read

BOSTON/TAIPEI (Reuters) - The group that orchestrated the theft of over \$2 million from cash machines at Taiwan's First Commercial Bank in July was also behind an ATM hacking spree in more than a dozen European nations last year, according to cyber security firm Group-IB.

The methods that the so-called Cobalt group used in Europe matched those used in Taiwan, Group-IB said in its latest client report.

Three Eastern European men were arrested in Taiwan in July on suspicion of collecting cash stolen from ATMs owned by First Commercial Bank, a unit of First Financial Holding Co Ltd.

Attorneys for the three defendants in an ongoing trial in Taipei told Reuters their clients were not familiar with Cobalt.

The men - identified in court documents as Peregudovs Andrejs of Latvia, Colibaba Mihail of Romania and Pencov Nicolae of Moldova - were among a total of 22 individuals, all foreign nationals, that Taiwanese authorities suspect of taking part in the theft, where most of the money was subsequently recovered.

The suspects used malware dubbed "ATM spitter" in the First Commercial Bank attacks, as well as similar hacks in countries including Armenia, Belarus, Britain, Bulgaria, Estonia, Georgia, Kyrgyzstan, Moldova, the Netherlands, Poland, Romania, Russia and Spain, Group-IB said in a report to its customers that Reuters reviewed on Thursday.

Group-IB first detailed the European spree in a report published in November, identifying the hackers as the Cobalt group.

The firm linked Cobalt to the Taiwan heist in its report last week.

Investigators in Taiwan told Reuters they were not aware of any links between Cobalt and the hackers behind the First Commercial Bank heist.

"What we can say is the people behind this hacking were very good," a Taiwanese investigator familiar with the case told Reuters, on condition of anonymity because the investigator was not authorized to speak with media.

The defendants, who maintain their innocence, said in a court hearing on Wednesday that they were not members of any international crime organization. Taipei prosecutors have said they suspect First Commercial Bank's network was breached at a London branch office.

Reporting by Jim Finkle in BOSTON and J.R. Wu in TAIPEI; Editing by Christopher Cushing

Our Standards: [The Thomson Reuters Trust Principles.](#)

for-phone-onlyfor-tablet-portrait-upfor-tablet-landscape-upfor-desktop-upfor-wide-desktop-up