Beat: News

Police dismantled an international criminal organization that hacked e-mails

To make million dollar scams

Madrid, 06.05.2016, 19:10 Time

USPA NEWS - The Spanish Police have dismantled an international criminal organization dedicated to "hack" e-mail accounts of senior managers of companies to commit millions scams. This is the ultimate method of fraud internationally known as "Swindle CEO" or "Business Email Compromise."

They have been detained 44 people -43 in Spain and one in UK-, among which are the 17 most responsible for the plot. Among those arrested are a lot of Spanish businessmen who were part of the branch support swindled money laundering. Of the 17 records made three have occurred in the UK and the rest in the Spanish provinces of Madrid and Toledo. In a storage room of a London airport hiding large amount of cash to be sent later to Nigeria. The defrauded amounts ranging from 20,000 euros to 1,800,000 euros, leaving about 600,000 euros most committed fraud.

Investigations began in November 2014 with the complaint filed by a Pakistani citizen whom he had swindled allegedly 34,000 euros after hacking their bank account and having transferred the money to an account in Spain. Crossing data with other similar complaints led officers to realize that they were facing a criminal organization with several ringleaders and a clear division of tasks between all the people who constituted. Some of the leaders, of Nigerian origin, were extremely zealous in their actions, hiding his true identity in their actions.

Advanced the investigation, the researchers could check in October last year cyber criminal clear how they looked in their modus operandi, which was to hack into the e-mail accounts of business executives by the known method of "spear phishing". This type of scam that is transmitted via email is intended to gain unauthorized access to sensitive data. The differential element with phishing scams, throwing wide massive attacks, spear phishing is that the objective focuses on a specific organization or group.

Thus they obtained the credentials of the e-mail accounts of senior managers to monitor and analyze their economic efforts and through them to determine whether they were used or not depending on the economic steps that made. One time they had access to their emails, sent a malicious mail from it all contacts to take into account and were of the same responsibility. In that message they pretended to have shared a document storage services in the cloud, for which access would have to enter the user name and password. Once captured credentials simulating an error in downloading to prevent suspected that the access data to their account had been stolen.

Swindle CEO or Business Email Compromise

This modus operandi is known internationally as the "Swindle CEO" or "Business Email Compromise" (BEC) which is having a major impact because of its highly effective, low risk for cyber criminals and strong corporate profits. Once scammers have control access to mail accounts of victims, two things can happen. Sometimes, criminals directly impersonate account holders and operate directly with banks of enterprises. This requires that knowledge that the victim and the bank that operate through e-mail, knowledge they have by the authors through monitoring of communications made the victim is taken.

At other times scammers keep track of the movements of the account compromised mail for transactions that are being carried out with customers or suppliers of the company. To complete the fraud involved at the last moment by sending an email that impersonate the monitored account, and once agreed the consideration of the contract, to modify the target account the economic consideration of the business claiming problems with the original entity. Thus, they get a sufficient cause mistake by the victim at the time of the transfer, running out of money in an account controlled by the organization.

The organization, perfectly structured, was composed on the one hand by hackers, whose task is to obtain access credentials to emails, mainly of companies that are performing large international bank transfers. On the other are the "mules", which are captured by members of the leadership and, in exchange for a commission, facilitated a "count bridge" for illicit transfers. In addition, they were also "qualified mules" to convince responsible people close to also act as intermediaries. The vast majority of these members were

Spanish citizens, managers of medium-sized enterprises, which provided bank accounts on behalf of legal persons of which were starters.

These members "facilitators" who provided false documents to the "mules" to justify to the banks the origin of the large transfers received and that they would not be returned to the issuer are added. In the last step of the criminal structure are the "carriers" which did get the benefits to their final destination by the known "Euro to Euro", a variant of the "Hawala" method, used by criminal organizations made up of citizens Nigerian nationality.

Such procedure is to deposit the cash in a "delivery point" in the place of origin -a commercial establishment of African products or parlor-, receiving a code with which to withdraw money in the country of destination, this case Nigeria. Responsible for this delivery point receives a management fee and also coordinates a network of constant remittances through people who travel regularly to Nigeria with the money hidden in their luggage or inside their organism, in exchange for a percentage.

The evolution of the investigations led the Police to give seven individuals who ran a booth in the Madrid suburb of Mostoles, who receive all cash and organizing shipments to Nigeria on weekly flights. One of these shipments was intercepted at the Adolfo Suarez-Madrid Barajas airport, where they were seized over 135,000 euros in bills hidden in garbage bags rolled up and hidden in the underwear of one checked bag in the hold of an aircraft.

In addition, thanks to international police cooperation has been able to combine research organization with branches in other countries like Nigeria, United States, United Kingdom, Turkey and Malta, where many companies are being affected by this kind of scam. In total 44 people have been arrested, 43 in Spain and one in UK. In addition, it have carried out 17 house searches, 14 in Spain and two in the United Kingdom thanks to the special involvement in research of the Unit Cybercrime TITAN (Police Investigation of Organized Crime in Region Northwest UK).

One of the records held in the British capital took place in the cellar of one of the London airports that those arrested used as a store of cash to send money to Nigeria. The agents have intervened in cash 200,000 euros, 12,820 dollars in cash, 10,000 pounds and 500,000 euros that have been blocked in three banks, from the latest fraudulent transfers received. In addition eleven vehicles have been seized in Spain and one in London, 35 computers, 80 cells, 20 tablets and extensive documentation.

Article online:
https://www.uspa24.com/bericht-7917/police-dismantled-an-international-criminal-organization-that-hacked-e-mails.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Jose A. Martin

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619