How hackers pulled off a $20 million bank heist

Buyenlarge | Getty Images

reader comments

40 with 28 posters participating

Share this story

In January 2018 a group of hackers, now thought to be working for the North Korean state-sponsored group Lazarus, attempted to steal $110 million from the Mexican commercial bank Bancomext. That effort failed. But just a few months later, a smaller yet still elaborate series of attacks allowed hackers to siphon off 300 to 400 million pesos, or roughly $15 to $20 million from Mexican banks. Here’s how they did it.

At the RSA security conference in San Francisco last Friday, penetration tester and security advisor Josu Loza, who was an incident responder in the wake of the April attacks, presented findings on how hackers executed the heists both digitally and on the ground around Mexico. The hackers’ affiliation remains publicly unknown. Loza emphasizes that while the attacks likely required extensive expertise and planning over months, or even years, they were enabled by sloppy and insecure network architecture within the Mexican financial system, and security oversights in SPEI, Mexico’s domestic money transfer platform run by central bank Banco de México, also known as Banxico.

Easy pickings

Thanks to security holes in the targeted bank systems, attackers could have accessed internal servers from the public Internet, or launched phishing attacks to compromise executives—or even regular employees—to gain a foothold. Many networks didn't have strong access controls, so hackers could get a lot of mileage out of compromised employee credentials. The networks also weren't well segmented, meaning intruders could use that initial access to penetrate deep into banks's connections to SPEI, and eventually SPEI's transaction servers, or even its underlying code base.

To make matters worse, transaction data within internal bank networks wasn't always adequately protected, meaning attackers who had burrowed in could potentially track and manipulate data. And while communication channels between individual users and their banks were encrypted, Loza also suggests that the SPEI app itself had bugs and lacked adequate validation checks, making it possible to slip bogus transactions through. The app may have even been directly compromised in a supply chain attack, to facilitate successful malicious transactions as they moved through the system.

All of these vulnerabilities collectively made it possible for hackers to lay extensive groundwork, eventually establishing the infrastructure they needed to begin carrying out actual cash grabs. Once that was in place, the attacks moved quickly.

The hackers would exploit flaws in how SPEI validated sender accounts to initiate a money transfer from a nonexistant source like "Joe Smith, Account Number: 12345678." They would then direct the phantom funds to a real, but pseudonymous account under their control and send a so-called cash mule to withdraw the money before the bank realized what had happened.

Each malicious transaction was relatively small, in the range of tens or hundreds of thousands of pesos. “SPEI sends and receives millions and millions of pesos daily, this would have been a very little percentage of that operation,” Loza says.

Attackers would have potentially needed to work with hundreds of mules to make all of those withdrawals possible over time. Loza says that recruiting and training that network could be resource-intensive, but that it wouldn’t cost much to incentivize them. Perhaps 5,000 pesos per person—less than $260—would be enough.

Wake-up call

SPEI itself and the infrastructure surrounding the app were apparently ripe for attack. Banxico, which could not be reached by WIRED for comment, said in a forensic analysis report released at the end of August that the attacks weren’t a direct assault on Banxico’s central systems, but were instead targeted at overlooked or weak interconnections in the larger Mexican financial system. The attackers’ approach required “a deep knowledge of the technological infrastructure and the processes of the victim institutions as well as access to them,” Banxico wrote. “The attack was not intended to render SPEI inoperable or penetrate the defenses of the Central Bank.”

Similar fraud using the international money transfer system Swift have cropped up around the world, including notorious incidents in Ecuador, Bangladesh, and Chile. But SPEI is owned and operated by Banxico, and only used within Mexico. In the aftermath of the April attacks, the bank tightened its policies and controls around fund transfers, to establish minimum cybersecurity standards for Mexican banks that link their systems to SPEI.

“Mexican people need to start to work together. All the institutions need to cooperate more,” Loza says. “The main

problem on cybersecurity is that we don’t share knowledge and information or talk about attacks enough. People don’t want to make details about incidents public.”

Loza adds that while there is still always the threat of a new rash of attacks, Mexican banks have invested heavily over the last year in strengthening their defenses and improving network hygiene. “From last year to today the focus has been implementing controls. Control, control, control,” he says. “And I think the attacks aren’t happening today because of it. But the most important thing is the change of mind that makes business users want to pay for better security.”

These types of heists have been so successful around the world, though, that they won’t be easy to stop. And while they take effort for attackers to set up, they can still net tens of millions of dollars. And all without having to crack a safe.

This post originally appeared on wired.com.

https://arstechnica.com/?p=1474621