Global bank network reports new cyberheist

BY MICHAEL CORKERY

Thieves have again found their way into what was thought to be the most secure financial messaging system in the world and stolen money from a bank. The crime appears to be part of a broad online attack on global banking.

New details about a second attack involving Swift — the messaging system used by thousands of banks and companies to move money around the world — are emerging as investigators are still trying to solve the $81 million heist from the central bank of Bangladesh in February. In that theft, the attackers were able to compel the Federal Reserve Bank of New York to move money to accounts in the Philippines.

The second attack involves a commercial bank, which Swift declined to identify. But in a letter Swift planned to share with its users on Friday, the messaging network warned that the two attacks bore numerous similarities and were very likely part of a "wider and highly adaptive campaign targeting banks."

The unusual warning from Swift, a copy of which was reviewed by The New York Times, shows how serious the financial industry regards these attacks to be. Some banking experts say they may be impossible to solve or trace. Swift said the thieves somehow got their hands on legitimate network credentials, initiated the fraudulent transfers and installed malware on bank computers to disguise their movements.

"The attackers clearly exhibit a deep and sophisticated knowledge of specific operation controls within the targeted banks — knowledge that may have been gained from malicious insiders or cyberattacks, or a combination of both," Swift said in its warning, which was expected to have been posted on a secure part of its website on Friday.

Security experts who have studied the attacks said the thieves may have been lurking inside the bank systems for months before they were detected.

In its warning, Swift pointed to another worrying situation: that the thieves may have been able to recruit bank employees to hand over credentials and other key details.

A.M. AHAD/ASSOCIATED PRESS

Atiur Rahman resigned as head of the Bangladeshi central bank after an attack in February.

In both cases, the core messaging system of Swift was not breached; rather, the criminals attacked the banks' connections to the Swift network. Each bank is responsible for maintaining the security of its connection to Swift. Criminals have found ways to exploit loopholes in bank security to obtain login credentials and dispatch fraudulent Swift messages.

"As a matter of urgency, we remind all customers again to urgently review controls in their payments environments," Swift was telling its customers in the letter to have been posted on Friday.

Banks — like many major corporations — are constantly under attack by criminals, seeking to find the weak point in their defenses. An attack in the summer of 2014 on JPMorgan Chase compromised the accounts of 76 million households and seven million small businesses, but no money was stolen. Thieves frequently steal bank customer's A.T.M. and credit card credentials.

But these attacks involving Swift stand out, because millions of dollars were stolen — not from a large number of customers, but from the banks themselves. It is as if the thieves used their hacking skills to reach inside a bank vault.

Emboldened and enriched, the thieves are likely to strike again, security experts predict.

"An event like this changes the risk profile for the banking system, since the attackers will inevitably reinvest some of their profits in new large-scale attacks," said Paul Kocher, a security and encryption expert who is the president of Cryptography Research, a division of Rambus.

Initially, many banks and security experts dismissed the Bangladesh attacks as brazen, but probably isolated, events in a developing country. A stream of news reports from the capital of Dhaka cited rudimentary technology at Bangladesh Bank, like a $10 router and an absence of firewalls. Bangladesh officials had blamed the New York Fed, saying it failed to block the fraudulent transfers.

On Tuesday, representatives from Swift, the New York Fed and Bangladesh Bank met in Basel, Switzerland, to discuss the breach and the vulnerabilities it exposed in the system.

In a joint statement, the three sides said that they had agreed to cooperate in trying to "bring the perpetrators to justice, and protect the global financial system from these types of attacks."

But the details of the second attack — which Swift said occurred in the last few months — suggested a highly sophisticated threat that did not necessarily hinge on weak digital defenses. Swift declined to say how much money was stolen from the bank, which was not located in Bangladesh.

Somehow the thieves obtained a valid Swift credential that allowed them to "create, approve and submit" messages on the network. Those messages — sent from PCs in the bank's back offices or from laptops — were then used to move money from one of the bank's accounts.

Many banks have a system of checks and balances by which they can validate and review transactions to root out fraud.

But in this latest case, the thieves used a form of malware that targeted a PDF reader that the bank used to confirm that payments had been made. The malware, according to Swift, then manipulated the PDF to "remove traces of the fraudulent instructions."

That the thieves knew that the bank used a PDF program to confirm its payments shows the level of detail gleaned about how the particular system worked. At Bangladesh Bank, Swift transactions were tracked using physical printouts. So the thieves tailored their malware in that attack to interfere with the printer and cover their tracks.

The attacks have been a major headache for the ubiquitous and publicity-shy Swift, an acronym for the Society for Worldwide Interbank Financial Telecommunication. Based in Belgium, Swift is partly owned and overseen by the world's biggest banks, which have used the technology to facilitate money transfers since the 1970s. It prides itself on not disclosing any information about its users.

Nicole Perlroth contributed reporting.