

Case 1: Bangladesh Bank Heist

The attack

Bangladesh Bank was recently compromised. According to forensic investigation, an unauthorized user obtained the computer credentials of a SWIFT operator at Bangladesh Bank, installed six types of malicious software (malware) on the bank's systems (through a harmful email sent to the employee) and began probing them in January 2017. The hackers did a series of test runs, logging into the system briefly several times between January 24, 2017 and February 2, 2017. During this period the hackers left monitoring software running on the bank's SWIFT system and also deleted files from a critical bank database.

On Thursday, February 4, 2017 the hackers began sending fraudulent payment orders via SWIFT. It was late evening in Bangladesh and most of the bank's staff had gone home. The hackers appear to have timed the heist to coincide with the weekend that in Bangladesh began the following day.

The first SWIFT message arrived at the New York Fed just after 9:55 a.m. and ordered the transfer of \$20 million from the central bank of Bangladesh to an account in Sri Lanka. Over the next four hours, 34 more orders arrived asking the U.S. central bank to move a total of nearly \$1 billion from the account it holds for Bangladesh Bank.

New York Fed

The Fed received 35 requests from Bangladesh and all these lacked the names of "correspondent banks". This is a necessary requirement. Also, most of the payments were to individuals rather than institutions. These requests were rejected for incorrect formatting. The hackers simply fixed the formatting and sent another 35 requests for payment to the same beneficiaries as before. This time the New York Fed cleared five of them, despite the oddities. They were properly formatted, SWIFT authenticated and went through automatically.

It is important to note that:

The slew of payments that morning was out of whack with the usual pattern of orders from Bangladesh Bank. Over the eight months leading to January 2016, Bangladesh Bank had issued a total of 285 payment instructions to the Fed, averaging fewer than two per working day. Also, none of those payments had been to an individual.

Also, although the U.S. central bank allows payments to individuals, but it's not common and is generally discouraged.

The Fed monitors for unusual transactions, but its system had a weakness: such that it did not have capabilities to monitor and spot unusual patterns in real time, the New York Fed typically looks back through payments, usually the day after they are requested.

After the five payments had been made, staff did flag "several" other requests for review to check whether they complied or not with U.S. sanctions. That manual review found that the payments were "potentially suspicious. But it was nearly 4 a.m. on the weekend in Bangladesh and no one was available to respond. Besides, the hackers had sabotaged Bangladesh Bank's systems to stop messages getting through.

It was only the following day, Friday Feb. 5 that the Fed began a full manual review of the orders from Bangladesh Bank.

It was at this stage that the presence of the name Jupiter in the payment orders rang alarm bells. One of the Fed's responsibilities is to avoid violating U.S. laws and prevent payments to sanctioned companies or individuals. It was just a stroke of luck that the name Jupiter featured on a sanctions list, thus raising a red flag. Otherwise the transaction would have been processed.

Delay in Swift Message

The hackers had infected the system with malware that disabled the printer, and Bangladesh Bank officials did not see the Fed's query and knew nothing of the fraudulent transactions. The team assumed there was simply a printer problem. Since Friday, the Islamic holy day, all other officials left the office at around 12:30 p.m., leaving the printer fix until later. Later that day, Fed officials sent two other SWIFT messages to Bangladesh. The first asked the same question for four of the five transactions that had already been cleared – and those four transactions included the name Jupiter. The second message asked about the 30 other payment instructions, including those queried the day before.

The messages did not get through. And the New York Fed did not reach out to Bangladesh in any other way. It would often take up to three days for clients like Bangladesh to respond to SWIFT messages.

On Saturday, Feb. 6, around 9 a.m., the Bangladesh team discovered that the printer didn't have a problem only that the SWIFT software was not starting. Whenever they tried to boot it up, a message appeared on the monitor, saying "a file is missing or changed."

Only around 12:30 p.m. did bank staff finally manage to print the SWIFT messages. That's when they first saw the fraudulent transactions and the Fed's queries, and realized something had gone horribly wrong.

Since Bangladesh Bank's SWIFT system was still not fully working, officials there hunted for other ways to contact the Fed in New York. Lacking any obvious point of contact, they searched the Fed's website and found an email address – but it was only monitored during weekday business hours. On Saturday they fired off three emails to that address over several hours. The first included the line: "Our system has been hacked. Please stop all payment (debit) instructions immediately."

It was the weekend and Fed staff did not respond. That email address was unlikely to be synced to their mobile phones.

Bangladesh followed up with several calls and a fax to numbers obtained from the Fed website, but those numbers were also marked as weekday-only contacts and the Fed still did not respond.

On Monday, staff at Bangladesh Bank finally managed to get their SWIFT system operating and sent a message headed "Top urgent" to the New York Fed saying 35 payment orders were fake. "Please recall back funds if transferred from your accounts," it said.

That message, sent around 1 a.m. in New York, would have been seen when NY Fed employees arrived at 7:30 a.m. However, it was only on Monday evening in New York and Tuesday morning in Bangladesh – four days after the heist began – that the New York Fed told Bangladesh Bank that it had alerted the correspondent banks to the fraud. A payment of \$20 million to an account in Sri Lanka had already been reversed because of a spelling error in the request. But for four other payments made out to individuals it was too late: \$81 million had gone to a Philippines bank and from there disappeared into the giant money-go-round that is the country's casino industry.

Money Lost

When the Federal Reserve Bank of New York cleared five transactions made by the Bangladesh Bank hackers, the money went in two directions. On Thursday, Feb. 4, 2017 the Fed's system sent \$20 million to Sri Lanka and \$81 million to the Philippines.

The Sri Lankan transaction contained a small but crucial error: The electronic message had a misspelling "fundation." That prompted Deutsche Bank, an intermediary in the transaction, to contact Bangladesh Bank, which led to the payment being cancelled and the money returned.

As for the money sent to Philippines, each account was in the name of an individual, all the names were false. The accounts were at a branch of RCBC in Jupiter Street, on the edge of Manila's business district. \$22.7 million was withdrawn from one of the RCBC accounts during the afternoon of Friday, Feb 5. But the rest of the money stayed in RCBC.

Bangladesh Bank sent messages via the SWIFT bank messaging system to RCBC asking it to freeze the money that had arrived in the four individuals' accounts. It was a holiday in the Philippines for Chinese New Year celebrations.

The following morning nearly \$58 million was moved out of those accounts giving a total of about \$81 million.

RCBC officials claimed that the SWIFT messages from Bangladesh Bank had been wrongly formatted and were not marked as urgent, so they had gone into a large pile of unread messages for almost the whole day. Staff had only got to them in the evening, RCBC said.

Under Philippine banking laws, the stolen funds could not be frozen until a criminal case was lodged, even though they were still in the banking system. And over the next few days, most of the \$81 million disappeared into the country's casino industry, which is exempted from anti-money laundering laws. Though \$18 million was recovered, otherwise the trail went cold.

Case 2: Kenya-Chinese Money Laundering

How it operates: A Chinese lands into the country with multiple credit cards belonging to one or several leading companies operating in either mainland China or Hong Kong.

They then approach a Kenyan business owner, preferably those whose daily turnover is in hundreds of thousands, and whose clients prefer to pay using credit or debit cards.

LUXURY RESORTS

Alternatively, these business people could be owners of establishments, such as high-end hotels and luxury resorts, whose main clientele are foreigners who prefer using plastic cash as opposed to hard cash.

Typically, such businessmen or establishments operate point of sale terminals — which are usually portable machines issued by local banks depending on the volume of their transactions.

The electronic devices are used to process card payments at retail locations and they accept all card types and prints receipts.

BUY NOTHING

The foreigners in the syndicate run a credit card loaded with cash on these machines purporting to be purchasing goods or services rendered by the Kenyan business — yet in actual sense they end up buying nothing.

In a matter of minutes, the money will reflect in the firm's accounts. But in reality, no actual business — that is purchase of goods and services — has taken place. Interestingly, most of the amounts entered supposedly for ordinary goods are huge. What has happened is that the Chinese national and the Kenyan businessman have simply engaged in money laundering and tax fraud.

CONTINENT WIDE

It is then time for Part two: After running the credit card, the Kenyan businessman then leaves his POS machine with the Chinese as collateral. When the money hits the account, the Kenyan businessman then withdraws it and shares it with the Chinese getting the bigger share.

For example, if the Chinese had run the card for Sh1 million, he will be given back Sh600,000 while the Kenyan businessman remains with a cool Sh400,000 for his troubles.

Our sources say that Kenya has become a favoured operational point for the syndicate, due to its well-developed economy, modern banking systems and fairly developed IT systems. However, we established that the scam is continent wide.

BANKING RULES

Africa has emerged as the last frontier for Chinese scammers who are unable to carry out their schemes in China due to the country's high penalties for corruption.

Neither can they perpetuate these schemes abroad in Europe or America due to the stringent banking rules in these continents which will smoke them out soonest.

"It is easy for them to do this in Africa, but Kenya is really ideal for them," said a source in the business world who has known about the scam for months now.

The strict rules requiring full declaration of sources of huge amounts of money that were introduced by the Central Bank of Kenya (CBK) in the wake of corruption scandals has limited the amounts of cash that can be transacted at a time.

Many local businessmen, we learn, are hesitant to run more than Sh1 million at a time, fearing that they might call attention of their respective banks who in turn might report them to the CBK.

UNPAID TAXES

They also fear attracting the attention of the Kenya Revenue Authority who might come for money in unpaid taxes and penalties on undeclared income.

Mr James Mburu, the KRA Commissioner Intelligence, said he was not aware of the scam, but said "I would be interested in the tax side of it."

The Director of Criminal Investigations George Kinoti did not respond to our requests for comment on whether they are aware of the scam.

In an SMS to this writer, Mr Boniface Ngatia Iregi, the head of Banking Fraud Investigations Unit, said he was also aware of such a syndicate.

SH1.75 MILLION

The Sunday Nation has seen a receipt of such a transaction that took place on September 11, 2018 at 2.16pm involving a popular shoe store on Kimathi Street and a Chinese identified in the receipt as Lin Zhi Ke.

Transaction details indicate that the Chinese bought shoes worth Sh250,000. However, our sources say no such purchase took place.

Our sources say that the Chinese had made two previous “fake” purchases at the same store of Sh750,000 each, bringing his total purchases in a span of two weeks to Sh1.75 million.

Based on the 60:40 ratio, the Chinese went home with Sh1,050,000 while shoe dealer made a cool Sh700,000 in a fortnight without selling a single pair of shoe.

When the Sunday Nation visited the store for a comment three weeks ago, the staff said the owner was not in. Our reporter then left his details. However, two days later, the reporter was called by a man who first identified himself as “Adan”, a lawyer to the store owner. “I can assure you that my client has done nothing wrong,” he said calmly.

MOBILE PHONE

When we called the mobile phone number later to ask for clarification, “Adan” turned hostile and threatened unspecified action.

“First of all I am not a lawyer. Secondly, you need to stop this nonsense,” he said as he began a 15-minute long rant on phone.

“Who do you think you are to spoil other people’s businesses? I dare you to write that story and we will deal with you firmly.”

In the phone conversation, “Aden” also said he was “the government” and the authorities knew what was going on.

OPEN DISPLAY

“There is no way you would know about us. Tell us who has sent you and how much they want, but don’t ever threaten us with writing stories,” he said.

Our sources said “Adan” could be working on behalf of a faction within the security agencies which is benefiting from the fraud. He was most likely a middleman between the Chinese owning the credit cards and the Kenyan businessmen who are seeking to make a quick kill.

For a week last month, the middleman with some of his companions had put up the Chinese at a five-star hotel within the Central Business District where local businessmen thronged with their machines in an open display of impunity, according to our source with knowledge of the operations.

SIX GROUPS

So many were the businessmen that they got impatient at the slow pace of the queue that they caused a commotion.

“After this, the middlemen became wary of exposing the Chinese to a lot of people for his own safety,” said our source.

The so-called Mr Lin Zhin Ke, is said to have quietly slipped out of Nairobi this week and gone back to China to “refill” his cards. He is thought to be the head of one of the six groups of suspected foreign criminals running money laundering schemes in Nairobi.