Bank Hackers Steal Millions via Malware

By DAVID E. SANGER and NICOLE PERLROTHFEB. 14, 2015

Photo

“The goal was to mimic their activities,” said Sergey Golovanov of Kaspersky, about how the thieves targeted bank employees. Credit Raphael Satter/Associated Press

PALO ALTO, Calif. — In late 2013, an A.T.M. in Kiev started dispensing cash at seemingly random times of day. No one had put in a card or touched a button. Cameras showed that the piles of money had been swept up by customers who appeared lucky to be there at the right moment.

But when a Russian cybersecurity firm, Kaspersky Lab, was called to Ukraine to investigate, it discovered that the errant machine was the least of the bank’s problems.

The bank’s internal computers, used by employees who process daily transfers and conduct bookkeeping, had been penetrated by malware that allowed cybercriminals to record their every move. The malicious software lurked for months, sending back video feeds and images that told a criminal group — including Russians, Chinese and Europeans — how the bank conducted its daily routines, according to the investigators.

Then the group impersonated bank officers, not only turning on various cash machines, but also transferring millions of dollars from banks in Russia, Japan, Switzerland, the United States and the Netherlands into dummy accounts set up in other countries.

How Hackers Infiltrated Banks

Since late 2013, an unknown group of hackers has reportedly stolen $300 million — possibly as much as triple that amount — from banks across the world, with the majority of the victims in Rssia. The attacks continue, all using roughly the same modus operandi:

BANK COMPUTERS

Hackers send email containing a malware program called Carbanak to hundreds of bank employees, hoping to infect a bank’s administrative computer.

Programs installed by the malware record keystrokes and take screen shots of the bank’s computers, so that hackers can learn bank procedures. They also enable hackers to control the banks’ computers remotely.

By mimicking the bank procedures they have learned, hackers direct the banks’ computers to steal money in a variety of ways:

- Transferring money into hackers' fraudulent bank accounts
- Using e-payment systems to send money to fraudulent accounts overseas
- Directing A.T.M.s to dispense money at set times and locations

In a report to be published on Monday, and provided in advance to The New York Times, Kaspersky Lab says that the scope of this attack on more than 100 banks and other financial institutions in 30 nations could make it one of the largest bank thefts ever — and one conducted without the usual signs of robbery.

The Moscow-based firm says that because of nondisclosure agreements with the banks that were hit, it cannot name them. Officials at the White House and the F.B.I. have been briefed on the findings, but say that it will take time to confirm them and assess the losses.

Kaspersky Lab says it has seen evidence of $300 million in theft through clients, and believes the total could be triple that. But that projection is impossible to verify because the thefts were limited to $10 million a transaction, though some banks were hit several times. In many cases the hauls were more modest, presumably to avoid setting off alarms.

The majority of the targets were in Russia, but many were in Japan, the United States and Europe.

No bank has come forward acknowledging the theft, a common problem that President Obama alluded to on Friday when he attended the first White House summit meeting on cybersecurity and consumer protection at Stanford University. He urged passage of a law that would require public disclosure of any breach that compromised personal or financial information.

But the industry consortium that alerts banks to malicious activity, the Financial Services Information Sharing and Analysis Center, said in a statement that "our members are aware of this activity. We have disseminated intelligence on this attack to the members," and that "some briefings were also provided by law enforcement entities."

The American Bankers Association declined to comment, and an executive there, Douglas Johnson, said the group would let the financial services center's statement serve as the only comment. Investigators at Interpol said their digital crimes specialists in Singapore were coordinating an investigation with law enforcement in affected countries. In the Netherlands, the Dutch High Tech Crime Unit, a division of the Dutch National Police that investigates some of the world's most advanced financial cybercrime, has also been briefed.

The silence around the investigation appears motivated in part by the reluctance of banks to concede that their systems were so easily penetrated, and in part by the fact that the attacks appear to be continuing.

The managing director of the Kaspersky North America office in Boston, Chris Doggett, argued that the "Carbanak cybergang," named for the malware it deployed, represents an increase in the sophistication of cyberattacks on financial firms.

“This is likely the most sophisticated attack the world has seen to date in terms of the tactics and methods that cybercriminals have used to remain covert,” Mr. Doggett said.

As in the recent attack on Sony Pictures, which Mr. Obama said again on Friday had been conducted by North Korea, the intruders in the bank thefts were enormously patient, placing surveillance software in the computers of system administrators and watching their moves for months. The evidence suggests this was not a nation state, but a specialized group of cybercriminals.

But the question remains how a fraud of this scale could have proceeded for nearly two years without banks, regulators or law enforcement catching on. Investigators say the answers may lie in the hackers’ technique.

In many ways, this hack began like any other. The cybercriminals sent their victims infected emails — a news clip or message that appeared to come from a colleague — as bait. When the bank employees clicked on the email, they inadvertently downloaded malicious code. That allowed the hackers to crawl across a bank’s network until they found employees who administered the cash transfer systems or remotely connected A.T.M.s.

Then, Kaspersky’s investigators said, the thieves installed a “RAT”— remote access tool — that could capture video and screenshots of the employees’ computers.

“The goal was to mimic their activities,” said Sergey Golovanov, who conducted the inquiry for Kaspersky Lab. “That way, everything would look like a normal, everyday transaction,” he said in a telephone interview from Russia.

The attackers took great pains to learn each bank’s particular system, while they set up fake accounts at banks in the United States and China that could serve as the destination for transfers. Two people briefed on the investigation said that the accounts were set up at J.P. Morgan Chase and the Agricultural Bank of China. Neither bank returned requests for comment.

Kaspersky Lab was founded in 1997 and has become one of Russia’s most recognized high-tech exports, but its market share in the United States has been hampered by its origins. Its founder, Eugene Kaspersky, studied cryptography at a high school that was co-sponsored by the K.G.B. and Russia’s Defense Ministry, and he worked for the Russian military before starting his firm.

When the time came to cash in on their activities — a period investigators say ranged from two to four months — the criminals pursued multiple routes. In some cases, they used online banking systems to transfer money to their accounts. In other cases, they ordered the banks’ A.T.M.s to dispense cash to terminals where one of their associates would be waiting.

But the largest sums were stolen by hacking into a bank’s accounting systems and briefly manipulating account balances. Using the access gained by impersonating the banking officers, the criminals first would inflate a balance — for example, an account with $1,000 would be altered to show $10,000. Then $9,000 would be transferred outside the bank. The actual account

holder would not suspect a problem, and it would take the bank some time to figure out what had happened.

“We found that many banks only check the accounts every 10 hours or so,” Mr. Golovanov of Kaspersky Lab said. “So in the interim, you could change the numbers and transfer the money.”

The hackers’ success rate was impressive. One Kaspersky client lost $7.3 million through A.T.M. withdrawals alone, the firm says in its report. Another lost $10 million from the exploitation of its accounting system. In some cases, transfers were run through the system operated by the Society for Worldwide Interbank Financial Telecommunication, or Swift, which banks use to transfer funds across borders. It has long been a target for hackers — and long been monitored by intelligence agencies.

Mr. Doggett likened most cyberthefts to “Bonnie and Clyde” operations, in which attackers break in, take whatever they can grab, and run. In this case, Mr. Doggett said, the heist was “much more ‘Ocean’s Eleven.’ ”