Vietnamese Bank Blocks $1 Million SWIFT Heist

bankinfosecurity.com/vietnamese-bank-blocks-1-million-online-heist-a-9105

Data Loss Prevention (DLP) , Fraud Management & Cybercrime , Governance & Risk Management

Attempted Heist Reportedly Targeted TPBank's SWIFT Software With Trojanized PDF Reader Mathew J. Schwartz (euroinfosec) • May 16, 2016

A Vietnamese bank says it foiled a plot to transfer $1.36 million out of its accounts - via the interbank SWIFT messaging system - in the fourth quarter of 2015 as part of a suspected malware attack launched by fraudsters (see *SWIFT Warns Banks: Coordinated Malware Attacks Underway*).

See Also: The Power and Scale of XDR

Tien Phong Commercial Joint Stock Bank, based in Hanoi, on May 15 said in a statement to *Reuters* that it detected the suspicious transfer requests quickly enough to contact receiving banks and put a stop to the transfers. The attempted attack "did not cause any losses," TPBank's statement reportedly said. "It had no impact on the SWIFT system in particular and the transaction system between the bank and customers in general."

SWIFT, which stands for the Society for Worldwide Interbank Financial Telecommunication, is a Brussels-based cooperative, owned by 3,000 banks, that was founded in 1973, and which maintains a messaging system used by 11,000 banks.

The State Bank of Vietnam - the country's central bank - is probing the attack after having received related information from TPBank on May 16, spokeswoman Le Thi Thuy Sen tells *Bloomberg*.

TPBank and the State Bank of Vietnam couldn't be immediately reached for comment on those reports.

SWIFT declined to comment on those reports, except to point to a May 13 security alert that it sent to its customers, warning them of "a highly adaptive campaign targeting banks' payment endpoints." That warning said an unnamed Vietnamese bank had also been targeted by the same attackers who attempted to transfer $1 billion out of the central bank of Bangladesh's account at the Federal Reserve of New York.

In the Bangladesh Bank case, the attackers successfully transferred $100 million to overseas accounts, of which $81 million is still missing. Investigators say the stolen funds were laundered via casinos in the Philippines. SWIFT says the attack was carried out in part after attackers used malware to infect a PDF reader used by bank employees.

TPBank Blames Third-Party Vendor

TPBank's statement said the fraudulent transfer requests were made using an unnamed third-party vendor with which the bank had contracted, to allow it to interface with the SWIFT network. The bank said that in the wake of the fraudulent transfer requests, it stopped working with the third-party provider and now has a more secure system which directly interfaces with the SWIFT platform.

TPBank told *Reuters* that the attack against it might have been carried out using the Trojanized PDF reader detailed in SWIFT's customer alert.

SWIFT: 'Small Number' of Similar Cases

In its May 13 customer alert, SWIFT warned that beyond Bangladesh Bank, it was aware of a "small number" of similar cases at other banks, involving attackers successfully infecting an unnamed PDF reader used at victim banks, which could be used to alter statements and disguise fraudulent transfers. Its alert did not name TPBank.

British defense contractor BAE Systems on May 13 released research saying that "a commercial bank in Vietnam ... also appears to have been targeted in a similar fashion using tailored malware, but based off a common code base" (see *Bangladesh Bank Attackers Hacked SWIFT Software*).

Threat-intelligence firm iSight Partners says there is at least one more victim that has not yet been publicly disclosed. "We believe that at least three financial institutions in the region were affected by these actors, and in two instances, malware was deployed that had functionality specifically associated with SWIFT fraud," the firm says in a research note that also names the PDF reader targeted by attackers.

"The malware used to target the Vietnamese bank replaces Foxit's popular PDF reader software to mask records of SWIFT transactions when read," iSight Partners says. "When reports are read through the PDF reader, SWIFT records are altered to remove traces of fraudulent transactions."

The Lazarus Group Connection

Based on its digital forensic investigation, BAE Systems said the malware appeared to be tied to the Lazarus Group, as detailed in a February report into Operation Blockbuster that was coordinated by anti-fraud and analytics firm Novetta. BAE Systems said the group also appeared to use a code compiler named Kordllbot, and to have focused its attacks on organizations in South Korea and the United States.

The Novetta report said the Lazarus Group "has been active since at least 2009, and potentially as early as 2007, and was responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment."

BAE Systems said that it did not have enough evidence to incontrovertibly attribute the Bangladesh and Vietnamese bank hacks to the same group that hacked Sony. But it said currently available evidence strongly suggests a connection. "We believe that the same coder is central to these attacks," it said. "Who the coder is, who they work for, and what their motivation is for conducting these attacks cannot be determined from the digital evidence alone."

Who's Responsible for Securing SWIFT?

The bank hacking campaign has revealed uneven information security practices at some SWIFT-using banks. In the wake of the February theft from Bangladesh Bank, which came to light in March, bank officials publicly said the Federal Reserve Bank of New York and SWIFT were at least partially to blame. But the New York Fed fired back, saying that it had honored valid SWIFT requests, and SWIFT said that the attackers had been able to gain access to Bangladesh Bank's back-end systems and submit what appeared to be legitimate SWIFT messages.

A subsequent Bangladesh police investigation reportedly concluded that a SWIFT technician left exploitable loopholes after connecting the bank to SWIFT's network, to facilitate real-time payments. But other reports suggested that the bank lacked robust passwords and authentication controls, or even firewalls (see *SWIFT to Banks: Get Your Security Act Together*).

On May 10, representatives from SWIFT, Bangladesh Bank and New York Fed met to discuss the attack and related investigations, and issued a joint statement pledging greater cooperation.

SWIFT has also continued to urge all customers to conduct a top-to-bottom review of their security defenses. "Please remember that as a SWIFT user you are responsible for the security of your own systems interfacing with the SWIFT network and your related environment - starting with basic password protection practices - in much the same way as you are responsible for your other security considerations," its May 13 security alert reads. "Whilst we issue, and have recently reminded you about, security best practice recommendations, these are just a baseline and general advice."