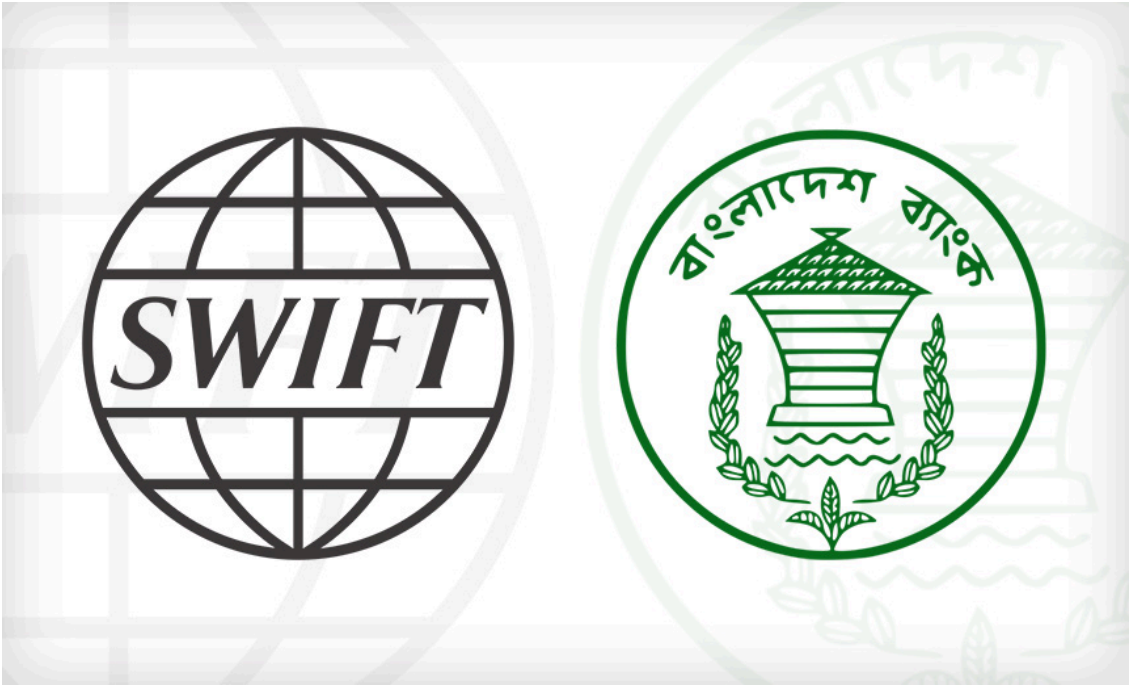
Bangladesh Eyes Insider Angle for SWIFT Bank Attack

By Mathew J. Schwartz

Card Not Present Fraud , Fraud Management & Cybercrime , Incident & Breach Response

Will SWIFT's Forthcoming Security Improvements Blunt Hack-Attack Spree? (euroinfosec) • May 31, 2016



Officials at SWIFT have announced a range of new security proposals designed to better secure - and restore confidence in - the global money-transfer network as news of yet another suspected attack against the network has come to light, this time in the Philippines.

See Also: Securing Patient Data: Shared Responsibility in Action

The messaging system maintained by SWIFT - formally known as the Society for Worldwide Interbank Financial Telecommunication - is designed to guarantee that money-moving messages between banks are authentic. But the reliability of the system, which is used by more than 11,000 institutions, has been called into question following revelations that SWIFT-using banks were falling victim to malware-wielding attackers (see *Another SWIFT Hack Stole $12 Million*).

Following the $81 million theft from the central bank of Bangladesh in February, SWIFT warned that a "wider and highly adaptive campaign" was underway. Investigators now suspect that a dozen or more banks may have been targeted by a group of attackers - possibly with ties to North Korea - who have been using fraudulent SWIFT messages to transfer millions into attacker-owned accounts, aided by customized malware that's designed to trick SWIFT's client software.

Bangladesh Suspects Insider Help

The head of a government-appointed panel investigating the Bangladesh Bank attack - the largest cyber heist in history - reportedly now suspects that one or more insiders may have aided attackers.

"Earlier we thought no one from Bangladesh Bank was involved, but now there is a small change," Mohammed Farashuddin, a former governor of the Bangladesh central bank, told reporters on May 30, without elaborating as to the precise nature of the change, *Reuters* reported.

The results of the new investigation will be made public in the next 15 to 20 days, Bangladesh Finance Minister Abul Maal Abdul Muhith told *Reuters*.

Previously, Bangladesh officials had blamed both SWIFT and the Federal Reserve Bank of New York for failing to spot and block the four fraudulent money-transfer messages that were processed. SWIFT, however, dismissed those claims, blaming the bank's poor security instead. But earlier this month, all three organizations met and pledged to work more closely together.

Bangladesh Bank spokesman Subhankar Saha couldn't be immediately reached for comment about the report's findings. But Saha told *Reuters* that the central bank had yet to see a copy of the report. "The Bangladesh Bank management will follow all instructions given by the government," he said. "Actions will be taken as per instruction by the government if any central bank officials were found guilty."

Security researchers now suspect that the same group of attackers may have targeted at least five different banks: Sonali Bank in 2013; an as-yet-unnamed bank in the Philippines in Octpber 2015; Vietnam's Tien Phong Bank in December 2015; Ecuador's Banco del Austro the following month; and Bangladesh Bank in February.

Last week, incident response firm FireEye told *Bloomberg* that it was investigating eight more suspected incidents involving banks in Asia - including the Philippines - as well as New Zealand. FireEye declined to comment on that report.

Report: Philippines Bank Attacked

Now, Symantec says it has identified three more pieces of "backdoor" malware - named Fimlis, Fimlis.B and Contopee - designed to give attackers remote access to systems. Symantec says these malware strains share significant code commonalities with the malware used against Bangladesh Bank and TPBank, which researchers have tied to the Lazarus Group, which was previously tied to the 2014 Sony Pictures Entertainment hack. The U.S. government controversially attributed the Sony attack to "North Korea actors" (see *FBI Attributes Sony Hack to North Korea*).

"Symantec believes distinctive code shared between families and the fact that [Contopee] was being used in limited targeted attacks against financial institutions in the region, means these tools can be attributed to the same group," Symantec says in a blog post.

Symantec said it recovered the malware from an October 2015 attack against a Philippines bank which - as noted above - it has declined to name.

Nestor Espenilla, the deputy governor of the Philippines' central bank, told *Reuters* that being attacked was not the same as being hacked and losing money. "We are checking if there are similar attacks on Philippine banks," Espenilla said. "However, no reported losses so far."

SWIFT Will 'Expand' Two-Factor Authentication

On May 27, SWIFT announced that it would be launching a set of five security changes to help better secure and authenticate SWIFT messages, including helping banks to better trade threat intelligence as well as detect related fraud. The measures were previewed last week by SWIFT CEO Gottfried Leibbrandt (see *SWIFT Promises Security Overhaul, Fraud Detection*).

SWIFT says the effort will commence with "cooperation with and facilitation of information sharing among overseers, banks, law enforcement and cybersecurity firms," and in the event of an attack include digital forensic analysis "on products and services related to SWIFT connectivity at affected banks, so that other users can protect themselves."

SWIFT has also promised to beef up the security of the software that it offers customers. "For example, our interface products support two-factor authentication, but we will further expand this and add additional tools," according to SWIFT's security announcement (see *Gartner's Litan Analyzes SWIFT-Related Bank Heists*). "We will also increase remote monitoring capabilities of customer environments."

Weakest Link Warning

But the five security improvements being proposed by SWIFT won't be a "silver bullet" that suddenly stops related attacks, says Ricardo Villadiego, CEO of anti-fraud firm Easy Solutions. "Those five points look to me more like a recipe for damage control than really going deeper into the problem," he says.

What's required, he contends, is not just mandatory use of multifactor authentication, but a much more layered system of security defenses. "The system is only as secure as the weakest link," he says, and right now that weak link appears to be so many SWIFT-using banks.
