Vulnerability Alert

Alert No: AVA180219 Date: 19-Feb-18 13:36 PM

Multiple SWIFT related incidents in India: Sri Lanka to be vigilant

Overview	Multiple SWIFT related attacks all over India. Sri Lankan Financial Sector is also to be vigilant.
Description / Impact	**Incident 1:** City Union Bank in Kumbakonam - Tamil Nadu, India, has detected a set of fraudulent transactions during the reconciliation process of SWIFT on 7th February 2018. It was discovered that 3 transactions were not initiated by the Bank and no entries were made in the ledgers but was reconciled within the period. Immediately following the discovery, all three transactions were contacted and acted upon. According to the current information, following are the said transactions and their status. 1. 500,000 USD: Standard Charted Bank, New York to a Dubai Based Bank - Transaction is already Reversed. 2. 300,000 Euro: Standard Charted Bank, Frankfurt to a Turkish Based Bank - Fund is Blocked in the beneficiary account. 3. 1,000,000 USD: Bank of America, New York to a Chinese Based Bank - The Beneficiary had already claimed the funds by submitting forged documents (Criminal Investigation is ongoing). While possible, there are no reports on internal staff involvements at the moment. This incident has supposedly happened via a cyber breach in the SWIFT network in the referenced bank. **Incident 2:** Punjab National Bank(PNB) in India has suffered a major fraudulent act with related to SWIFT related transactions. Unlike a standalone incident, this incident has been progressing from 2011 to 2017. According to the current information, a major jeweler in India has reached PNB for a foreign currency guarantee for his imports and exports business, and a fraudulent Bank employee has issued a series of forged guarantees throughout 2011 to 2017 totaling up to 1.77 Billion USD. The guarantees were sent using SWIFT messages, but as SWIFT system was not integrated in to the Core Bank System of PNB, the transactions were not detected by the banking officials. The existing security features such as separation of duties in SWIFT systems using maker, checker and verifier, has been bypassed simply using a reused shared password (According to the current public information).
Risk Reduction Recommendations	**Immediate Actions to be taken:** 1. Strictly follow the SWIFT security guidelines for the enforcement of security in the SWIFT network. 2. Security policies should be strictly followed rather than used for compliance. 3. Educate related staff about current and previous incidents 4. Extreme cautious should be maintained on approving and reconciliation of cyber related transactions.
References	1. https://www.theregister.co.uk/2018/02/19/crims_pull_another_swiftie_indian_bank_stung_for_nearly_us2m/ 2. https://www.cityunionbank.com/downloads/Press_Release_swift.pdf 3. http://www.livemint.com/Opinion/oiMKS98wBunYNviWCVq6hJ/The-anatomy-of-the-PNB-fraud.html 4. https://www.ndtv.com/india-news/former-pnb-official-used-shared-bank-passwords-to-help-nirav-modi-1814294 5. http://indianexpress.com/article/explained/punjab-national-bank-nirav-modi-fraud-how-the-system-was-gamed-5069107/ 6. http://www.aljazeera.com/news/2018/02/indias-punjab-national-bank-reports-18-bn-fraud-180215131603991.html
Disclaimer	**The information provided herein is on "as is" basis, without warranty of any kind.**