



Informational Alert

Alert No : AIA171009

Date : 09-Oct-17 10:10 AM



Another SWIFT Attack – Taiwan Bank got affected

Overview	Taiwanian Bank " <i>Far Eastern International Bank</i> " got affected by a malware to its SWIFT account where the attackers had tried to move US\$60 million to few foreign destinations including Sri Lanka
Description / Impact	<ul style="list-style-type: none">• We got confirmation from TWCERT (Taiwan CERT) and SL CERT CC on yesterday night (08th Oct 2017) that a SWIFT related financial fraud has been attempted on one Taiwan bank.• According to yesterday's update, the attack has been supposedly happening on Friday (06th Oct 2017)• This has been reported immediately to the Taiwan Financial Supervisory Commission (FSC) and all the relevant departments.• Attackers tried to transfer US\$60 million out of Taiwan to foreign destinations like the United States, Cambodia and Sri Lanka.• Attack was initiated as per the sources, using a currently unknown malware (Which the TWCERT CC is still investigating) and the investigation is still ongoing• According to TWCERT, the incident is an isolated incident where no other incidents are related within Taiwan.• As the bank reported the incident immediately to the relevant entities, the loss is supposedly less than US\$500, 000. Most of the other transactions have been recovered at this moment.• According to unverified reports, several perpetrators have been identified and currently being investigated on the incident within Sri Lanka
Risk Reduction Recommendations	<ul style="list-style-type: none">• Be vigilant on high value transactions, especially within local and international holidays.• Immediately report and share the information so that the damage to you and other entities can be minimized.• Take necessary measures to ensure the SWIFT network and related infrastructure is secure in accordance with the SWIFT mandatory security controls and more. <i>(https://www.swift.com/myswift/customer-security-programme-csp/security-controls)</i>• Educate related staff on these fraudulent incidents so that they are more aware of finding anomalies
Disclaimer	The information provided herein is on "as is" basis, without warranty of any kind.