NCR SECURITY UPDATE

DATE: February 13, 2015 **INCIDENT NO:** 2015-01 **REV:** #1

Description

Man in the Middle Network Attacks

Summary

NCR has been made aware of a “Man-in-the-Middle” network attack in Mexico. This class of “Man-in-the-Middle” network attack can occur when network infrastructure is compromised and malware is placed within the banks network. The malware will monitor the network traffic and listen specifically for transaction messages from ATMs. When a cash withdrawal transaction message is recognised from a specific bank card, the malware will then intercept the corresponding host response and modify the authorised dispense amount to a larger sum than requested and approved by the host.

To execute the fraud, an attacker will initiate a withdrawal transaction at an ATM on a compromised bank network. The card used will be pre-defined known card number. The malware will intercept the transaction and recognise the card number and wait for the host response to the withdrawal request. The host response message will be intercepted and modified to a larger cash value, such that the ATM will dispense far more than has been debited from the account. In a variant of the attack, the malware will intercept the request, and return an authorisation such that the transaction host is unaware of the request.

Guidance and Recommendation from NCR

- The bank follows industry best practice for securing their TCPIP network.
- Standard communications authentication and encryption protections must be applied to all ATM network traffic. The recommendation is to use TLS or a VPN, and by implementing MAC’ing to provide cryptographic authentication of sensitive messages.

Contacts

ATM Crime Reporting : global.security@ncr.com
Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com
Further information on this alert: owen.wild@ncr.com