NCR SECURITY UPDATE

DATE: June 22, 2015 **INCIDENT NO:** 2015-05 **REV:** #1

Description

New variation of Card Reader Eavesdropping Attacks

Summary

NCR has been investigation a new method to capture card data by means of Card Reader Eavesdropping.

This methodology has been confirmed in the United Arab Emirates and has been carried out on Personas ATMs.

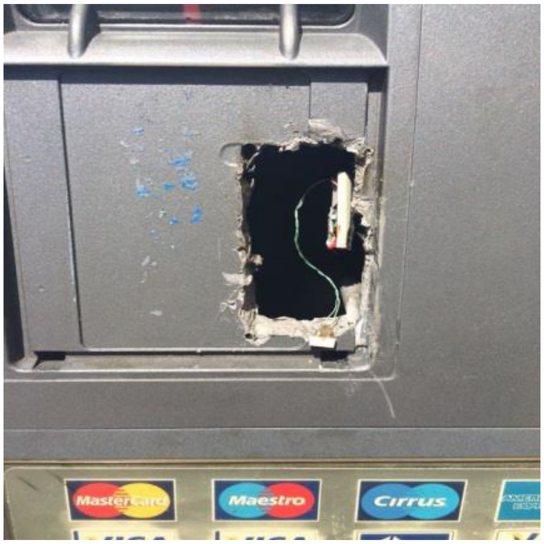
In this variation of the attack, criminals are attacking freestanding lobby ATMs, not Through the Wall ATMs. The criminals are gaining access to the card reader by breeching the security of the ATM top box. They are then attaching a similar electronic device to that observed in previous attacks to attach directly to the card reader to capture the card data. No holes are drilled in the fascia to gain access; therefore the attack is invisible from the exterior of the ATM once the top box is closed.

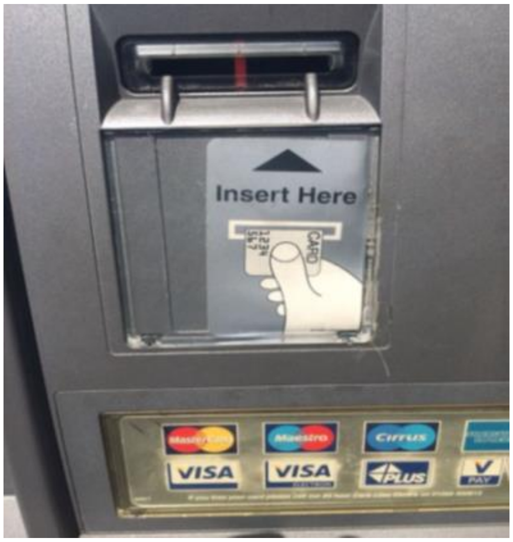
This is a variation from the MO from previous Eavesdropping attacks. (Reference ATM Security Update 2014-14)

In the previous attack, the ATM fascia is penetrated close to the card reader to create a hole large enough for the attacker to reach inside the ATM and place a tap directly onto the card reader in order to skim card data as it is read by the ATM. One end of the device is attached to the contacts on the back of the magnetic stripe read head of the card reader, whilst the other is attached to a data storage device. Once the tap is in place, the hole in the fascia can be disguised by placing a sticker, or some other cover over the hole.

The typical location for the previous type of attack is to penetrate the fascia at the Card Orientation Window (COW). This provides the ideal access location to the card reader for the criminal, and the COW can be replaced to disguise the hole.

NCR SECURITY UPDATE





The emergence and growth of Eavesdropping attacks is due to the widespread availability of Anti-Skimming technology which is successful at preventing successful capturing of card data using a traditional skimmer, placed on the outside of the ATM. Card Reader Eavesdropping is successful because skimmers are placed in a location that Third Party Anti-Skimming technology cannot protect, since the ATM must be capable of reading the card.

NCR notes that all observed cases of eavesdropping to date have been against Personas ATMs, however all ATMs must be protected against this form of attack.

Guidance and Recommendation from NCR

For SelfServ and Personas ATMs, NCR has an Anti-Eavesdropping kit. This kit provides a physical protective shield around the ATM Card reader. This barrier provide additional prevention to having any external connections made with the ATM card readers,

With the emergence of more reliable anti-skimming solutions, such as SPS with its anti-drill mat, traditional skimming and card reader eavesdropping through a fascia hole are less likely to be successful, which increases the risks of attacks on front access ATMs in public environments. As such, NCR recommends that all ATM deployers upgrade the Top Box Lox on standalone ATMs and CD. A strengthened UL 437 pick resistant lock is now available for SelfServ ATMs

Please contact your NCR Account manager for specifics on the solutions.

In addition, NCR Skimming Protection Solution will also provide notification top box accesses, SPS also has and Anti-COW penetration mat that can prevent and detect penetration of the fascia in this area around the card reader bezel.

.

Additionally, NCR recommends that bank employees and service personnel regularly inspect the ATM fascia for holes and other evidence of tampering when servicing or replenishing the equipment. With through the wall ATMs this can be done from the back side of the ATM and with front access ATMs it can be done when the hood is lifted. ATM deployers should also ensure its service providers carry sufficient documentation to establish that they are legitimate service personnel, and provide off-site staff with instructions on checking this documentation to confirm anyone accessing the ATM represents a legitimate service vendor.

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