NCR ATM SECURITY UPDATE

DATE: August 29, 2018 **INCIDENT NO:** 2018-09 **REV:** #1

Deep Insert Skimming on Motorized Card Readers

Summary

NCR has been made aware of intelligence from the Middle East and Africa (MEA) region which indicates that criminals have developed a method to install a Deep Insert Skimmer inside a motorized card reader such that it cannot be detected by the NCR APTRA platform software. NCR recommends using the Tamper Resistant Card Reader as the prevention mechanism for both Deep Insert Skimming and Eavesdropping Skimming techniques.

Description:

A function was added to the NCR software platform that is capable of detecting certain deep insert skimmers using the device sensors in the motorized card reader. This function was released in APTRA XFS 06.05. The function operated by causing an alert when media input to the card reader was detected as being dimensionally different from a standard bank card. The alert is configurable and can be used as a simple alarm, or to shut down the ATM upon detection of non-standard media. Video evidence received by NCR indicates that criminals have developed a technique which masks the dimensions of the deep insert skimmer such that it can no longer be distinguished from a standard bank card.

Guidance and Recommendation:

NCR recommends using the NCR Secure™ Tamper Resistant Motorized Card Reader as a measure to prevent Deep Insert Skimming attacks. The Tamper Resistant Card Reader has

modified internal dimensions which reduce space to successfully install a Deep Insert Skimmer. This reader was launched in 2017 and is now the standard reader in NCR SelfServ™ ATMs. Upgrade kits are available for 30 series and 80 series NCR ATMs. The Tamper Resistant Motorized Card Reader also has features which can help protect against Eavesdropping Skimming. This is a skimming technique that places an electronic bug onto the card reader circuitry to 'eavesdrop' card data during normal operation of the ATM.

The APTRA XFS Internal Skimmer Detect (ISD) function can continue to be used to monitor for attempts to place deep insert skimmers, but this must not be relied upon as the only line of defense.

General Skimming Guidance:

Criminals can skim card data from any point, either inside or outside of the ATM, or by tapping into electronic and software systems to harvest data. Any ATM anti-skimming strategy must take into account all points within the ATM subsystem that carry card data, and protection must be applied at every point.

Fascia Skimming – deploy NCR Skimming Protection Solution
Deep Insert Skimming – deploy NCR Tamper Resistant Card Reader
Eavesdropping Skimming - deploy NCR Tamper Resistant Card Reader
Software Skimming – deploy NCR Hard Disk Encryption and NCR Solidcore Suite for APTRA
External Communications Skimming – deploy TLS1.2 encryption
Internal USB Communications Skimming – deploy USB encryption with APTRA XFS 06.06

NCR ATM SECURITY UPDATE

Skimming exploits magnetic strip data used on bank cards. Alternative technologies exist and should be used instead e.g. EMV chip cards. Where magnetic strip data remains on a card, additional authorization controls should be used to prevent skimming.

Deploy GeoBlocking – block all magnetic strip transactions received from non-EMV capable regions.
Disallow fallback – block all magnetic strip transactions received from EMV capable ATMs.
Deploy Contactless EMV – 'tap and PIN' EMV contactless transactions at an ATM are immune to skimming.

Applicability:

The Tamper Resistant Card Reader represents a hardware upgrade only, there are no software or firmware dependencies.

Release Version:

- F505 for Tamper Resistant Card Reader – Track 2
- F507 for Tamper Resistant Card Reader – Track 3

- 6634-K505-V001 - Tamper Resistant Card Reader for SelfServ – Track 2
- 6634-K507-V001 - Tamper Resistant Card Reader for SelfServ – Track 3
- 6684-K505-V001 - Tamper Resistant Card Reader for 80series – Track 2
- 6684-K507-V001 - Tamper Resistant Card Reader for 80series – Track 3

NCR ATM SECURITY UPDATE

Please contact your NCR Account Manager if you have any questions or need additional information.

NCR Security Summit

NCR will hold our 5th Annual Security and Fraud Summit on October 8, 2018 in London. This interactive executive session is focused on creating discussions on key issues and strategies for ATM Security and Fraud prevention.

Key topics will include:

- Discussion on the Windows 10 and its' impact ATM security and what steps are needed to ensure protection during the migration
- The continuing growth of Fraud and how the ATM channel fits in to the situation and why Fraud protection must be part of your overall strategy
- New PCI Compliance requirements and deadlines are coming, learn from NCR and PCI experts as to what you need to do to remain compliant
- How NCR is looking to the future with new next generation ATM design, new security concepts and solutions
- And finish the evening at a dinner with your peers

But spaces at the NCR Security Summit are limited so please register today to secure your place at this event.

NCR ATM SECURITY UPDATE

Security 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 please contact Owen Wild
Please refer any media inquiries or questions to Aaron Gould