NCR ATM SECURITY UPDATE

DATE: June 12, 2017 **INCIDENT NO:** 2017-06 **REV:** #1

Black Box Attacks on SelfServ™ ATMs in the UK

Summary

NCR has been made aware of a number of Black Box attacks in the UK targeted at Through-The-Wall (TTW) NCR SelfServ ATMs. Some of the attacks have been successful.

In a Black Box attack, the criminal gains access to the internal infrastructure of the ATM. The cash dispenser is disconnected from the ATM system and an external electronic device (the "Black Box") is connected to the dispenser. This device sends commands to the dispenser which results in an unauthorized dispense of cash from the ATM. All ATM models from all manufacturers are potentially at risk.

In previous Black Box attacks against SelfServ ATMs, the criminal has gained access to the ATM internal infrastructure by opening the top box on lobby ATMs. In this new attack vector, TTW ATMs are attacked by breaking through the fascia. This is done by drilling holes in the fascia such that the ATM screen can be removed. This removal allows enough access to an internal USB hub where the attacker can connect a Black Box and operate the attack from the street.

In addition to cash losses, this attack causes significant damage to the ATM.

The model targeted in the recent attacks is the NCR 6626, but all TTW models are potentially at risk.

NCR ATM SECURITY UPDATE

Guidance and Recommendations for Self Serv ATMs

It is imperative that ALL NCR SelfServ ATMs globally are upgraded with Black Box protection AS SOON AS POSSIBLE. As with the Personas Black Box attacks, it is expected that the SelfServ attacks will migrate very soon beyond the UK.

Black Box attacks can be readily prevented by using standard protection available in the APTRA XFS platform software, and by ensuring that this software is kept up to date.

- Set the dispenser security to PHYSICAL (LEVEL 3) Authentication
- The dispenser XFS software component must be upgraded to the version included in APTRA XFS 06.03. This is the MANDATORY minimum version. The recommended version is APTRA XFS 06.04.01. This component may be upgraded by either:
    - Upgrading the ATM platform software to APTRA XFS 06.04.01; or
    - For ATMs with older supported platforms (APTRA XFS 6.02 or earlier), please contact your NCR Professional Services representative or account manager.
- Other Dispenser Security Authentication levels WILL NOT protect against Black Box attacks. The only protection against Black Box attacks is a combination of Level 3 Authentication AND the USB dispenser component included in APTRA XFS 06.03 (minimum), APTRA XFS 06.04.01 (recommended minimum).

NCR ATM SECURITY UPDATE

Personas ATMs

As reported in NCR Security Update 2016-11 there has previously been an increase in activity against NCR Personas ATMs. These attacks are continuing in Europe.

Guidance and Recommendations for Personas ATMs

- Fleet modernization is an important part of staying secure. Modern architectures, containing modern technologies are critical in the defense against criminals. **NCR recommends that all customers plan their strategic migration to newer and more secure models of ATMs as well as newer versions of APTRA XFS software.**
- During this transition, NCR has made available the Personas Dispenser Encryption Enhancement upgrade kit. This kit will provide an enhanced encryption that will reduce the risk from Black Box attacks. The PDEE upgrade kit has a pre-requisite of APTRA XFS 06.01 platform software, or the application of Hotfix APTRA Personas Dispenser Enhancement 01.00.00 to older supported platforms.

Note: After deployment of the PDEE functionality, please ensure that PDEE authentication level is set to LEVEL 3 – PHYSICAL.

For comprehensive guidelines to protect against logical attacks please refer to the NCR Logical Attacks Configuration and Implementation Guidelines Document.

Contacts

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