NCR SECURITY UPDATE

DATE: August 18, 2016 **INCIDENT NO:** 2016-11 **REV:** #1

Personas Black Box attacks continue to grow in Europe, now reported in UK

Summary

As we have previously communicated, we are seeing an increase in the frequency and geographic expansion of Black Box attacks. We are now able to confirm attempts of Black Box attacks on Personas ATMs in the UK. Black box attacks were previously reported in Mexico, Brazil, Germany, Spain, Poland, Russia, Italy and the Czech Republic.

In this mode of logical 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.

Attached below are some images of the "black box" devices that were recently seized by law enforcement in the Czech Republic.

Guidance and Recommendations:

For SelfServ ATMs:

- Set the dispenser security to PHYSICAL (LEVEL 3) Authentication Levels
- The dispenser software component must be upgraded to the version included in APTRA XFS 06.03. **This is also mandatory**. This component may be upgraded by either;
  - Upgrade the ATM platform software to APTRA XFS 06.03; 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.

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 recommendation is for all customers to 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 solution will provide 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.

Physical Security:

These attacks can occur on both front and rear access ATMs. Thus, it is important to consider the environment, and scale the physical security protecting the ATM accordingly. ATMs in unattended public locations are at highest risk. The following are specific recommendations, particularly for ATMs in higher risk environments.

- Upgrade cabinet locks to a higher security lock
- Utilize an alarm that will alert when the Top Box is opened; NCR Skimming Protection Solution provides this functionality
- Periodic remote surveillance monitoring where capabilities to do so exist
- Staff monitoring for suspicious activity around the ATM
- Periodic checks for holes in the fascia of the ATM, or in the vicinity of the EPP keyboard
- Procedures to validate the authenticity of CIT and maintenance activity at the ATM

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