NCR SECURITY UPDATE

DATE: August 20, 2015 **INCIDENT NO:** 2015-08 **REV:** #1

Black Box Attacks in Germany

Summary

NCR is tracking and investigating a series of Black Box Attacks in Germany. In this series of attacks, freestanding front access Personas ATMs located in lobby environments have been targeted.

In this form of black box attack the ATM PC is not used. The criminals access the ATM top box, disconnect the communications cable to the currency dispenser from the ATM PC Core, and then connect the cable to their own device (the 'Black Box').. Commands are then sent by the external electronic device directly to the dispenser to result in an unauthorized dispense of cash from the ATM.

Guidance and Recommendation from NCR

Once again, we want to provide you with the following information with NCR's recommendations on implementation of security practices:

For Black Box Attacks

- SelfServ ATMs: Set the Dispenser Security to PHYSICAL (Level 3) authentication level.
  - This recommendation is consistent with our recommendations contained within Security for APTRA guidance.
  - Other authentication levels WILL NOT protect against Black Box attacks.
- Personas ATMs: Upgrade with the PDEE kit to add encryption to the dispenser communications.

- 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.
- Utilize an alarm that will alert when the Top Box is opened

NCR SECURITY UPDATE

For Malware attacks:

As a priority:

- Prevent booting from a removable media (including disabling auto play)
- BIOS editing must be password protected. Password management policies must be robust.
- Deploy an effective anti-virus mechanism
    - NCR recommends active whitelisting applications which go beyond traditional anti-virus programs - specifically the deployment of Solidcore Suite for APTRA. (Solidcore Suite is different from Solidcore. Solidcore Suite contains an enterprise level monitoring function which provides additional functionality, notification, and reporting.)
    - Solidcore Suite is necessary to prevent malware attacks that are physically deployed (i.e. through physical access to the ATM). Solidcore Standalone will prevent network borne attacks.

Additional mandated recommendations:

- Establish an adequate operational password policy for all passwords
- Implement communications encryption (SSL encryption or VPN)
- Establish a firewall
- Remove unused services and applications
- Establish a policy for secure software upgrades
- Ensure the application runs in a locked down account with minimum privileges required.
- Define different accounts for different user privileges
- Establish a regular patching process for all software installed
- Deploy a responsive, real-time fraud system
- Ensure your fraud system identifies suspicious patterns of behavior to stop fraud
- Monitor fraud across the enterprise to protect from all forms of attack
- 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 best practice guidelines for all ATM's are strongly recommended, but specifically for those in higher risk ATM environments.
- Utilize an alarm that will alert when the Top Box is opened

If you are not currently receiving direct distribution of these alerts please subscribe via on online site:
http://response.ncr.com/security-alerts

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