NCR SECURITY UPDATE

DATE: September 29, 2015 **INCIDENT NO:** 2015-13 **REV:** #1

Update to NCR Security Update 2015-08
New Black Box Attack in Poland

Summary

NCR is issuing this update alert to inform that Personas Black Box attacks have spread to Poland. Mitigation advice remains the same as issued for pervious Personas Black Box attacks.

Guidance and Recommendations:

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

For Malware attacks:

As a priority:

- Prevent booting from a removable media
- Disable 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 Security Measures

- 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
- 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

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