NCR SECURITY UPDATE

DATE: May 25, 2016 **INCIDENT NO:** 2016-07 **REV:** #1

Reports on “Skimer” and “ATM infector” malware

Summary

Last week, Kaspersky, a software security firm published a report on ATM malware (Skimer / ATM Infector). We have not seen this form of malware used successfully on NCR ATMs.

This particular malware is reportedly able to capture cardholder data (including PIN) from consumers who use the ATM and perform an unauthorized dispense of cash from the ATM.

Guidance and Recommendations:

With regards to all malware attacks, NCRs Security Strategy is designed to provide guidelines and solutions that will prevent any malware from being loaded onto the ATM.

This is achieved by following the guidelines summarized in the NCR Logical Attacks Configuration and Implementation Guidelines Document

NCR provides several solutions that also help enable many of the recommendations contained in the whitepaper:

- NCR Secure Hard Disk Encryption
- Solidcore Suite for APTRA
- NCR Secure Remote BIOS Update
- Security for APTRA

Adherence to all of the guidelines and use of these solutions are required to provide a layered and comprehensive approach to preventing malware and other logical attacks. If some rules are not followed, and some solutions are not deployed, the ATM remains vulnerable to attacks.

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