NCR SECURITY UPDATE

DATE: March 4, 2015 **INCIDENT NO:** 2015-03 **REV:** #1

Description

Update on Carbanak Attacks on Bank Network Computers

Summary

NCR has done further investigation into the report. At this point there have been no reported losses on NCR ATMs using this class of attack to dispense cash or to compromise information. In addition, NCR has not been able to verify that there have been any attacks of this nature outside of Russia and the Ukraine at this point.

Guidance and Recommendation from NCR

Based on our review and investigation of the attack, NCR also strongly recommends that ATM deplorers review their Enterprise Security process and ensure that they implement the following practices:

- Ensure that all remote access to ATMs
  - Restricts the functionality & user privileges required by the role (i.e. log retrieval)
  - Supports two factor authentication (e.g. password + certificate or password + token)
  - Traces and or logs all activities at the ATM during the remote session.

- Anti-malware signatures across the enterprise are updated
- Scans are initiated to detect Carbanak.
- Review the enterprise to ensure that all end-points (including routers) do not have default passwords
- Ensure that no unnecessary test utilities are installed on the ATM estate
- Implement TLS for all sensitive communications.

Please see previous NCR alerts for guidance on how to protect your ATMs against Black Box Attacks, ATM Malware attacks and Man in the Middle attacks. For additional information on any of the above, please contact your NCR representative or the contact below.

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