

NCR SECURITY UPDATE

DATE: February 17, 2015

INCIDENT NO: 2015-02

REV: #1

Description

Network Inserted Malware Attacks on Bank Computers (Carbanak APT)

Summary

NCR is aware and reviewing a report issued by Kaspersky relating to recent malware attacks conducted using the bank's network architecture. This report is receiving attention from the media as "the great bank heist."

This attack vector is different from the malware attacks that NCR has previously alerted you about. This was a long term attack targeting the computer infrastructure of the bank, inserting malware into the network and using the bank systems to steal money by:

- Transferring money into hackers' fraudulent bank accounts
- Using an e-payment system to send money to fraudulent accounts overseas
- Directing ATMs to dispense money at set times and locations.

Guidance and Recommendation from NCR

NCR is continuing to investigate this report and gathering more data about the attack vector and method. NCR recommends that all customers review their network security controls against industry best practices. Network segments that are used to control the ATM network are especially attractive to criminals as a source of access to cash. For these segments particular care must be taken in implementing security measures.

NCR would also like to point out that this alert is not related at all to the recent alert issued describing a Man in the Middle attack in Latin America (Alert 2015-01) . While both attacks involved a network breach, the Man in the Middle attack was a specific attack on the ATM cash dispense functionality and specific ATM countermeasures are required to protect against this form of attack.

The alert is also not related to previous NCR alerts describing ATM malware or Black Box attacks. Again these were specific attacks on the ATM cash dispense functionality, and specific ATM countermeasures are required to protect against this form of attack.

NCR SECURITY UPDATE

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