NCR SECURITY UPDATE

DATE: March 19, 2015 **INCIDENT NO:** 2015-04 **REV:** #1

Description

New Logical Attacks being reported in India

Summary

NCR has been made aware of series of logical attacks being conducted on ATMs in India. We are still investigating the method of attack. The initial findings may indicate this could be a new variant on the types of attacks that we have seen in the past.

In this attack the criminals are gaining access into the top box and connecting a device (currently not identifiable) to a USB port. The criminal is connecting a keyboard to enter commands to cause the ATM to dispense cash.

We are in the process of gaining additional forensic data from the impacted ATMs and will provide updates on the findings when available.

Guidance and Recommendation from NCR

NCR again encourages all ATM deployers to take the following actions as part of the broader guidance to protect against these forms of logical attacks.

Protect against Black Box Attacks:

- **For customers with Self Serv ATMs:**
  - Set the Dispenser Protection Authentication Level to Level 3, Physical Protection
  - Install Release 01.01.00 of the USB Dispenser Encryption Enhancement Release Package for APTRA XFS
- **For customers with Personas ATMs**
  - Install the Personas Dispenser Encryption Enhancement Solution

Protect against Malware Attacks

- This is widely documented in the communications we have sent to the field over the last 18 months. I have attached this information, and speed is of the essence.

As a priority:

NCR SECURITY UPDATE

• Prevent booting from a removable media
• 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.)
o Solidcore Suite is necessary to allow notification alerts to be sent for malware attacks that are physically deployed (i.e. through physical access to the ATM). Solidcore Standalone will prevent online attacks.

Additional mandated recommendations:
• Establish an adequate operational password policy for all passwords
• Disable AutoRun/Autoplay
• 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 user accounts with role based 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 o NCR Skimming Protection Solution provides this functionality

• NCR also recommends the use of other deterrence methods such as; Surveillance monitoring, which will also detect and record suspicious activities around the ATM
o Appropriate signage
o Adequate ambient lighting

For additional information on any of the above, please contact your NCR representative or the contact below.

Contacts

NCR SECURITY UPDATE

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