NCR SECURITY UPDATE

DATE: July 2, 2015 **INCIDENT NO:** 2015-06 **REV:** #1

Malware attacks on ATMs in Brazil

Summary

NCR has confirmed a series of malware attacks on ATMs in Brazil. Initial analysis indicated that the MO used is consistent with what we have seen with attempts to load malware onto the ATM.

While the version of malware used in this case was a variant from previous attacks, the insertion of the malware was successful due to the fact that the ATMs were not protected properly.

NCR does not expect that these attacks will stop, unless ATM deployers take immediate action to protect their ATMs from this known form of attack. These malware attacks have expanded into nearly every global region and are increasing in frequency.

All ATM operators need to take aggressive proactive measures to ensure that they deploy the highest level of security defenses to prevent against these forms of attacks.

Guidance and Recommendation from NCR

Once again, we want to provide you with the full list of NCR's recommendations on implementation of security practices to help mitigate risks of these logical attacks as well as for more traditional forms of ATM attacks.

As a priority:

- The BIOS to be set to only boot from the Hard Drive
- BIOS editing must be password protected.
- Password management policies must be robust.
- Disable Autoplay
- 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.)

NCR SECURITY UPDATE

Additional mandated recommendations:

- Establish an adequate operational password policy for all passwords
- Implement communications encryption (TLS 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
- 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
    - 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
    - Appropriate signage
    - Adequate ambient lighting

If you are not currently receiving direct distribution of these alerts please subscribe via on online site:
http://response.ncr.com/security-alerts

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