NCR SECURITY UPDATE

DATE: December 8, 2015 **INCIDENT NO:** 2015-16 **REV:** #1

Host Ghosting Attacks in Eastern Europe

Summary

NCR has received reports that a customer has been attacked via an attack that took advantage of unencrypted communications and no MACing at the ATM allowing an unauthorized dispense of cash.

Guidance and Recommendations:

ATM operators can protect against these forms of host ghosting attacks by deploying strong communications encryption between the ATM and host e.g. TLS 1.2/VPN. This can be obtained through NCR Secure TLS Encrypted Communications Product. Customers should also enable MACing within their application

NCR also strongly recommends that ATM deployers review their Enterprise Security process and ensure that they implement the following practices:

1. Secure your BIOS
- Only allow boot from the primary hard disk
- BIOS editing must be password protected

2. Establish an adequate operational password policy for all passwords
- One password for every ATM is not secure

3. Implement communications encryption (TLS encryption or VPN)
- Mandatory if you are using public wide area networks

4. Establish a firewall
- Mandatory if you are using public wide area networks

5. Remove unused services and applications
- Basic Security Principals, any code is a source vulnerability, so minimize it

6. Deploy an effective anti-virus mechanism
- NCR Recommends active whitelisting applications: Solidcore Suite for APTRA

7. Establish a patching process for Operating System Patches

8. Establish a regular patching process for ALL software installed

9. Disable Windows Auto-Play

10. Ensure the application runs in a locked down account with minimum privileges required

11. Define different accounts for different user privileges
- Remotely & securely control passwords with enhanced permissions

12. Deploy a network authentication based Hard Disk Encryption Solution

13. Ensure there is protected communications to the dispenser of the ATM

14. Perform a Penetration Test of your ATM production environment annually

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