NCR SECURITY UPDATE

DATE: Nov 30, 2016 **INCIDENT NO:** 2016-14 **REV:** #1

Media coverage of recent Cobalt Logical Attacks on ATMs

Summary

Recently, there has been media coverage of an IT security report, *COBALT Logical Attacks on ATMs*, which detailed network-based ATM attacks as well as other online malware attacks against ATMs.

The main subject of the report are network attacks against non-NCR ATMs that took place in the summer of 2016. This report suggests that attackers have targeted countries within Asia and Europe. While no European customers have reported attacks using this modus operandi to NCR, there is no reason to assume this could not occur, given the same vulnerabilities within the bank.

The specific approach is to target FI employees with a 'spear phishing' attack. Spear phishing is a technique that sends malware to specific individuals at the FI in emails disguised to look like they are from a credible source. If the individual opens the email and/or clicks on a link, the malware can become resident on that computer, and then propagate itself elsewhere within the FI. Once the malware is running inside the FI, the malware takes advantage of unpatched vulnerabilities and poor configuration of servers within a bank's enterprise to further penetrate the FI's network. This can ultimately allow malware to be installed onto an ATM using standard remote access tools applied in the bank. For example, Microsoft Remote Desktop Protocol can be used for this purpose.

The attack vector described within the report is very different from the recent Thailand attack which the report also references. Nonetheless, both were the result of attackers compromising the bank's network.

Mitigations against this attack vector are:

- Follow NCR's best-practice guidelines that are outlined within **NCR Logical Attacks Configuration and Implementation Guidelines Document.**

- NCR recommends consulting a security enterprise specialist to deploy industry best-practice security controls within your enterprise. For example:
    - Security Awareness Training for employees to minimize the risk of spear phishing
    - Ensure a robust patching process is in place across the FI's enterprise
    - AV signatures should be up to date
    - Banks need to have role-based access control
    - Restrict functionality allowed via remote desktop access to ATMs
    - If remote desktop access is required, enforce two-factor authentication
    - We strongly recommend removing any remote desktop access (including Microsoft Remote Desktop Protocol (RDP))
    - Configure the ATM firewall to allow only known authorized incoming and outgoing connections per program rather than per port
    - Implement Network Access Control (for example, Kerberos).

- Deploy a Network Intrusion Detection/Prevention system. Create a custom rule to detect and respond to unusual traffic behavior. Specifically, alert and block ATM-to-ATM traffic.
- Deploy endpoint authentication to allow only authorized devices (ATM) and applications to connect to the domain, and only authorized devices to access specific services (e.g. Active Directory)

The above bulleted list are examples of areas to focus on. However, your Security Consultant will advise on best-practice controls specific to your enterprise.

General Guidance and Recommendations for ATM endpoint security:

With regards to malware attacks, NCR's security strategy is designed to provide guidelines and solutions to help prevent malware from being loaded onto the ATM.

This is done through the customer following the guidelines that we outline in the NCR Logical Attacks Configuration and Implementation Guidelines Document.

NCR provides several solutions that when deployed will help defeat the loading of malware on the ATM:

- NCR Secure Hard Disc Encryption
- Solidcore Suite for APTRA
- NCR Secure Remote BIOS Update
- Security for APTRA

All of these solutions are required to provide a layered and comprehensive approach to combating malware and other logical attacks. If some rules are not followed, or some solutions are not deployed, ATM vulnerability to attack can be increased.

. The following items outline the steps needed to protect the ATM from Black Box attacks:

- **Self Serv**
  - Dispenser Encryption with Physical Authentication (Level 3) **AND** the USB CDM software component from APTRA XFS 06.03
  - (Minimum component version = USBCurrencyDispenser 03.01.00)
- **Personas**

- PDEE upgrade kit, including SDC CDM software component from APTRA XFS 06.01, with Physical Authentication
- (Minimum component version = SdcCurrencyDispenser 03.06.00)

Informational Webinar:

Please register to join an NCR Security Webinar **"ATM Global Logical Attacks - Updates and Defenses"** to learn more about the nature of these logical attacks as well as to receive information on security strategies, recommendations and solutions designed to reduce the risk to your ATM fleet. The Webinar will be delivered live on 6 December 2016 at 11:00 AM US Eastern Time / 16.00 UK time. The Webinar will also be recorded and available on demand.

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