# NCR SECURITY UPDATE

**DATE:** March 9, 2017 **INCIDENT NO:** 2017-02 **REV:** #1

# Fileless Malware

## Summary

NCR is aware of the reported emergence of a new variation of ATM malware that has been reported by a security solution firm. The report indicates that hackers are targeting banks and other organizations with this from of **Fileless** malware. At this point, NCR has not had any reports of customers affected by this malware.

According to the report, Fileless malware is a piece of software that does not copy any files or folders to the hard drive in order to get executed. Instead, payloads are directly injected into the memory of running processes, and the malware executes in the system's RAM. Since the malware runs in the memory, the memory acquisition becomes useless once the system gets rebooted, making it difficult for digital forensic experts to find traces of the malware.

## General Guidance and Recommendations for ATM endpoint security:

With regards to malware attacks, NCR's security strategy is designed to provide guidelines and solutions that will prevent any malware from being loaded onto the ATM. In this case the use of NCR Solidcore Suite for APTRA, as part of the layered solution approach, would protect the ATM.

**The guidelines are set out in the NCR Logical Attacks Configuration and Implementation Guidelines Document,**

NCR provides several solutions that customers can deploy to prevent the loading of malware on to 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 preventing malware and other logical attacks. The failure to follow all of the guidelines and implement all of these solutions can result in ATMs remaining vulnerable to attacks.

All customers, regardless of geographic region and ATM model type, MUST be made aware of the protection needed to protect against Black Box attacks to NCR ATMs.

# NCR SECURITY UPDATE

**For NCR SelfServ ATMs**

- 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

- **For NCR Personas ATMs**
  - 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:**

NCR recently hosted an informational webinar **"ATM Global Logical Attacks - Updates and Defenses"** providing details of these logical attacks and information on security strategies, guidelines and solutions designed to reduce the risk to your ATM fleet. The webinar is 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