NCR SECURITY UPDATE

DATE: September 15, 2015 **INCIDENT NO:** 2015-10 **REV:** #1

Reports of new form of ATM Malware

Summary

NCR is aware of the blog post from a security products company claiming to have identified a new variant of malware which targets all ATMs from a range of ATM vendors.

We have had discussions with the authors of the blog and have recieved additional information regrading this malare.

There are no reports that this malware has been used to compromise ATMs. The MD5 hashes for the malware are:

4bdd67ff852c221112337fecd0681eac
f74755b92ffe04f97ac506960e6324bb

An updated stinger dat file will be made available which will identify and remove this malware if it is found on an ATM

Current analysis indicates that if the customers follow NCR best practice guidelines then they will not be vulnerable to this malware.

If you have experienced an attack of this nature, please contact Owen Wild at owen.wild@ncr.com.

Guidance and Recommendations:

From our intial review of this information, NCR believes that the previously communicated guidance and recommendations for protection from logical attacks should be adequate to protect from this new variant.

Key mandatory requirements include:

- Apply a robust administrator password
- Ensure AUTORUN has been fully and effectively disabled
- Deployment of Hard Disc Encryption to prevent unauthorized files from being loaded on to the ATM.
- Deploy only PCI compliant firmware in the EPP
- 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 performed when the ATM Hard disk is offline. Solidcore Standalone will prevent online attacks

NCR SECURITY UPDATE

NCR also recommends that ATM deployers ensure robust passwords and password management is in place for all ATMs, specifically the BIOS and Administrator passwords. This should include appropriate password differentiation, security checks and controls to maintain the integrity of that process and policy.

Passwords should be as complex as possible. Best practice recognizes that these passwords should be at least 14 characters long (where possible), and should consist of characters from three of the following groups of characters:

- Lower case
- Upper case
- Numeric
- Special
- No more than two consecutive characters from the account user name may appear in the account password

ATM Operatators also need to continue to deploy physical security measures to prevent access to core, as well as validating the credentials of individuals claiming to represent an ATM service provider.

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