NCR SECURITY UPDATE

DATE: March 2, 2016 **INCIDENT NO:** 2016-02 **REV:** #1

Offline Malware Attack in Ukraine

Summary

NCR has received reports that a customer has had a successful Offline Malware attack. The actual malware used to dispense cash from the ATM is similar to previous malware we have seen.

However one important difference with this attack was that the BIOS had been locked down to only allow boot from the primary hard disk and also had a BIOS password to prevent BIOS editing. This means the attacker had information as to how to circumvent these BIOS security measures.

Similar to other offline malware attacks, additional online malware protection was also bypassed.

Guidance and Recommendations:

For OFFLINE malware attacks:

- Hard Disk Encryption MUST be deployed as the primary layer of defense against this mode of attack.
- ATM BIOS MUST be configured such that it will boot ONLY from the ATM primary hard disk.
- Passwords used to protect the BIOS MUST be changed regularly and stored securely.

In addition to the above, NCR recommends the use of whitelisting solutions, such as NCR's Solidcore Suite for APTRA to protect against ONLINE malware attacks.

An updated .dat file is available for use with Stinger. NCR Customers can contact their Account Manager or Professional Services Partners to receive the .dat File.

NCR continues to reinforce the need for ATM deployers to implement a layered set of security measures. This layered approach will provide a range of defenses to help prevent ATM attacks from being successful. NCR's full guidance on protecting against logical attacks is available **here**.

Learn more at the webinar "Card Data Breach at the ATM: Trends and new threats affecting ATM operators" on 12 April, 2016.

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**