NCR SECURITY UPDATE

DATE: June 11, 2018 **INCIDENT NO:** 2018-07 **REV:** #1

Continued Expansion of Logical Attacks on ATMs in the United States

Summary

Following up on NCR Security Update 2018-03 in January, NCR has seen increasing frequency and spread of Logical Attacks in the United States. These attacks include both Black Box and Malware type attacks, both of which are designed to “jackpot” the cash in the ATM.

Recent media coverage has indicated that these attacks are now expanding in geography. The report cites FBI confirmation and some data on the frequency of these attacks. Click here to view the report.

This should be treated by all ATM deployers as a call to action to take appropriate steps to protect their ATMs against these forms of attack and mitigate any consequences.

Specific Guidance and Recommendations:

The most common forms of logical attack against ATMs are "Black Box" and "Offline Malware.”

- Configuring Dispenser Protection on your NCR ATMs to Level 3, and ensuring that the dispenser’s driver software is patched with the latest updates, are important protections to mitigate the impact of Black Box attacks.

- Protections for Offline Malware include deploying NCR Secure Hard Drive Encryption and/or locking the ATM BIOS configuration and protecting the configuration with a password. This can be enabled by using NCR Secure Remote BIOS Update.

NCR SECURITY UPDATE

- Further protection from Online Malware attacks can be achieved by deploying a whitelisting solution such as NCR Solidcore Suite for APTRA.

General Guidance and Recommendations:

The impacts of logical attacks can be mitigated by following the NCR best practice recommendations and guidelines.

Customers who currently do not have the security controls in their own environments that are described within NCR Logical Security: Security Requirements to Help Protect Against Logical Attacks are advised to review the document and apply the security controls as quickly as possible. These guidelines are provided within the NCR Logical Attack Protection Whitepaper.

Protection and mitigation are functions not only of ATM provider updates, but also the deployer's own security environment.

Informational Webinars:

This development, along with recent announcements highlight new vulnerabilities in PC processing chips and reports of new organized criminal activities, reinforce the need for ATM operators to make security a priority. Join and engage experts from NCR Security during a series of informational and interactive webinars to learn more about these risks and the steps that you can take to proactively protect your ATMs from logical attacks. Click below to register for one of the upcoming NCR Secure webinar series:

- Online Malware Attacks – June 12
- ATM Network Protection – June 19
- Account Take Over Fraud – June 19
- Black Box Attacks – June 26
- PCI Compliance – July 3
- Card Protection Trends – July 10

NCR SECURITY UPDATE

- Upgrading ATMs to Enhance Security – July 17
- How Fraud Protection fits into Security Strategy – July 18

NCR Security Summit:

NCR will be holding our 5th Annual NCR ATM Security Summit on Oct 8, 2018. This Security peer event, which will occur in London prior to the RBR Cyber and Security conference, will present and discuss critical topics relating to ATM Security. Please view our online information for more details and to register for this event.

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 please contact Owen Wild
Please refer any media inquiries or questions to Aaron Gould