

NCR SECURITY UPDATE

DATE: July 23, 2015

INCIDENT NO: 2015-07

REV: #1

Card Skimming attacks in the US and Mexico

Summary

NCR is tracking an increasing frequency of card skimming attacks in both the US and in Mexico.

The reports of these attacks have been seen on all manufacturers of ATMs. Card Skimming remains the most frequent form of attack on ATMs and still results in significant losses for card issuers and financial institutions.

As a result of our investigations with law enforcement, we have seen that devices that have been used in the US have been bezel mounted card skimming devices similar to the image provided here.



In this attack the skimming device is part of the false overlay bezel. This bezel is attached on top of the legitimate card reader bezel. In addition some form of device or method is also installed to capture the user PIN data.

The attacks in the US were able to defeat legacy third party anti skimming devices. Our testing using the captured skimmer found that NCR Skimming Protection Solution would have been effective in detecting the skimmer and preventing the attack.

The attacks in Mexico were targeted at non-NCR ATMs. For more information about these attacks please reference the post written by industry expert Brian Krebs, at www.krebsonsecurity.com (<https://krebsonsecurity.com/2015/07/spike-in-atm-skimming-in-mexico/>)

Guidance and Recommendation from NCR

NCR recommends that all ATM deployers implement current versions of anti-skimming technology.

NCR SECURITY UPDATE

NCR's Skimming Protection Solution provides market leading protection for NCR SelfServ ATMs with both Motorized and DIP card readers. NCR's Skimming Protection Solution has been tested against the skimmer used in the US attacks. It was successful at detecting the skimmer and would have prevented the attack.

In addition to deploying anti skimming technology NCR recommends that financial institutions have their employees and service personnel regularly inspect the ATM card readers for these forms of skimmers as well as other areas of the fascia for holes and other evidence of tampering when servicing or replenishing the equipment.

If you are not currently receiving direct distribution of these alerts please subscribe via on online site:
<http://response.ncr.com/security-alerts>

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