NCR SECURITY UPDATE

DATE: November 12, 2015 **INCIDENT NO:** 2015-15 **REV:** #1

Card Skimming Advisory

Evolution in Card Skimming Attacks on ATMs

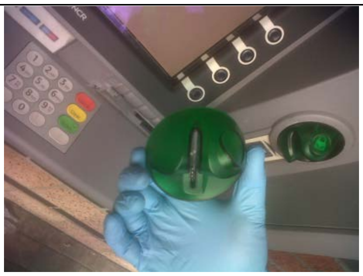
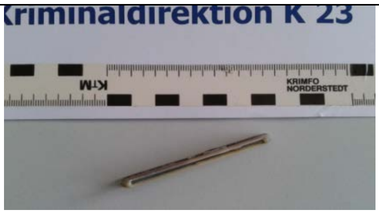
Summary

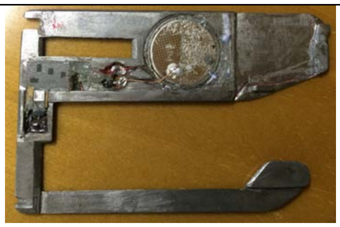
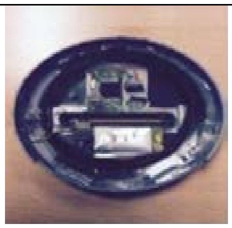
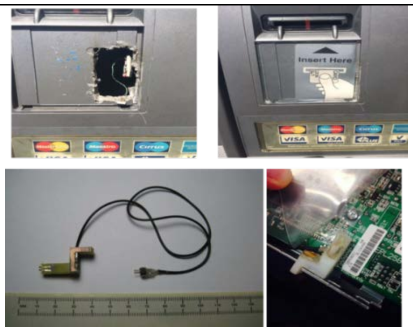
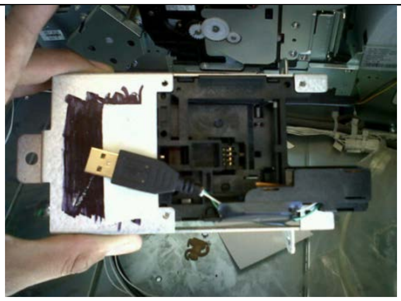
Data from a variety of sources show that 2015 has seen an alarming increase in card skimming attacks at ATMs. This trend also is consistent with reports of increases in card skimming attacks at other point of sale terminals, particularly the United States.

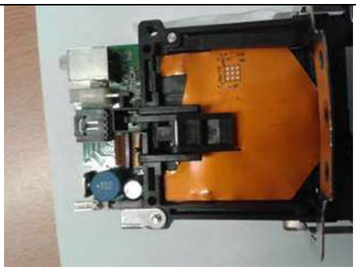
The trend does show some inconsistency in frequency. Some regions like Europe have seen lower reports of card skimming attacks. Others such as the United States have seen skimming levels reach their highest levels in decades.

In addition to the growing frequency of traditional attacks, we are seeing continued evolution and increased sophistication as to the MO used by criminals to capture card data. This evolution is a result of criminals now modifying the crime to either circumvent, or bypass forms of anti-skimming protection.

NCR currently categorizes card skimming into the following types. In addition to the original skimming categories, this list now also includes the new categories that have been developed specifically to circumvent anti-skimming technology.

Bezel Mounted Skimming	The use of an external skimming device that fits over the ATM card insert bezel.	
Insert Skimmers	Use of a skimming device that is placed inside the card bezel	

Deep Insert Skimmers	A skimming device that is placed inside of the card reader in order as to defeat bezel mounted anti-skimming solutions	
Differential Skimming (or Stereo Skimming)	Use of twin skimming read heads for the purpose of filtering out the protection provided by electromagnetic anti-skimming jamming signals. This defeats bezel mounted anti-skimming solutions that exclusively employ electromagnetic jamming.	
Eavesdropping / Card reader Tap - Destructive	Attempts to capture the card data by connecting a skimming device directly to the internal card reader via a hole created in the ATM fascia or cabinet.	
Eavesdropping / Card reader Tap – Non-Destructive	Attempts to capture the card data by connecting a skimming device directly to the internal card reader by opening the ATM Top box.	

Card Shimming	Placing a device inside the card reader which can intercept the communications between the card chip and the chip reader. This is an intercept of the chip data, not of the magnetic strip data. The attack is exploited by copying the captured chip data onto a magnetic strip. Correct implementation of EMV will detect this during authorization, thus preventing the attack.	
Malware based card skimming	Installing malicious software on to the ATM with the intent to capture card data.	

Guidance and Recommendations:

Card skimming crimes will continue as long as cards continue to be produced with the magnetic stripe. True strategic prevention of card skimming can only occur by eliminating the use of static identification data at the ATM, and removing the insertion of legacy magnetic strips into the ATM. One practical example of this would be the use of contactless EMV.

However, while the ATM industry is required to support magnetic strip technology, occurrences of card skimming can be significantly reduced through the implementation of a layered solutions strategy.

Bezel Based Skimming requires anti skimming solutions which provide the ability to detect skimming devices, and prevent the ATM from operating while a foreign object is detected at the ATM. NCR customers are strongly advised to deploy NCR's Skimming Protection Solution on all ATMs. For SelfServ ATMs, NCR Skimming Protection Solution provides the capability to detect the presence of a skimmer. On motorized card readers, the NCR Skimming Protection Solution also provides electromagnetic jamming, providing and additional layer or protection. Additionally, frequent inspections of the ATMs are strongly advised to attempt to note the attempts to attach any devices to the card bezel.

Eavesdropping / Card reader Tap - Destructive This attack involves a destructive breach of the ATM fascia or cabinet (e.g. drilling a hole), with the intent to place a skimmer directly onto the card reader control board through the hole created in the fascia. NCR's Skimming Protection Solution provides anti-drill detectors which protect the ATM fascia at the Card Orientation Window. NCR customers are also advised to install the Anti-Eavesdropping Kit which will physically protect the card reader. This is a hardware kit that can be installed on SelfServ ATMs with motorized card readers.

Eavesdropping / Card reader Tap – Non-Destructive ATM operators need to take careful consideration of the location of the ATM and ensure that the site is monitored as part of an overall physical security strategy. It is also recommended that operators add additional security to strengthen the top box. This is critical for standalone and drive up ATMs. NCR customers can achieve this protection by installing strengthened UL437 rated top box locks. These locks are pick resistant and have a more controlled access to key distribution.

Deep Insert Skimming is a relatively new form of attack. It has been seen in the Middle East and parts of Europe. NCR is actively investigating these attacks and working with our card reader manufacturers to finalize modifications to design to further protect against this form of attack. In the interim, NCR is working to release both a hardware and firmware upgrade for existing card readers that will protect from this form of attack. NCR will provide updates advising customers to the release of these kits.

Differential Skimming (stereo skimming) is also a new occurrence of attack and to this point has only been confirmed in Ireland. However, as with all ATM attacks, there are no restrictions on the crime expanding into other regions. The reported cases of differential skimming were able to defeat an anti-skimming device. Anti-skimming solutions without detect capabilities (i.e. solutions that rely exclusively on electromagnetic jamming) can be vulnerable to Differential Skimming attacks. NCR customers are advised to deploy the NCR Skimming Protection Solution and operate the solution with the Detect functionality. Used in this manner, SPS would effectively detect the presence of the Stereo Skimmer and allow the ATM to be protected from skimming any cards.

Card Shimming, is not actually an attempt to capture magnetic card data. Card shimmng is achieved by inserting a device into the ATM card reader that can intercept and record the data that flows between the chip card and the ATM reader. This data could then potentially be reused to then clone a magnetic card. However, the data that can be captured from a chip card cannot be reused to clone a magnetic strip, because chip data and mag strip data have different CVVs. (check values). This means that counterfeit cards can be immediately detected during transaction authorisation. The only way for this attack to be successful is if an issuer neglects to check the CVV when authorising a transaction. All issuers MUST make these basic checks to prevent this category of fraud. Card Shimming is not a vulnerability with a chip card, nor with an ATM, and therefore it is not necessary to add protection mechanisms against this form of attack to the ATM.

Malware has been more commonly used in the attempt to "jackpot" or cause the complete withdrawal of cash from the ATM. However, NCR is aware of cases where malware has been inserted onto the ATM with the attempt to capture the card data. All ATM operators are advised to deploy preventive measures to protect against the unauthorized installation of malware on the ATM. This includes deployment of whitelisting software security solution such as NCR's Solidcore Suite for APTRA. In addition ATMs must have their BIOS protected from allowing boot from external media and with a password. NCR customers can automate this through the deployment of the NCR Remote BIOS Update Solution. Hard Disc Encryption is also recommended as further protection against Malware being loaded onto the ATM using offline techniques. PIN data can be protected against malware attacks by using PCI approved firmware in the EPP.

In addition to the above, NCR also encourages ATM deployers and their service providers to regularly inspect ATMs for suspicious damage or attachments (internal or external), and to validate the bona fides of persons purporting to be service personnel.

Please contact NCR if you have any questions or need any further information about this advisory.

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