Moneris

BE PAYMENT READY

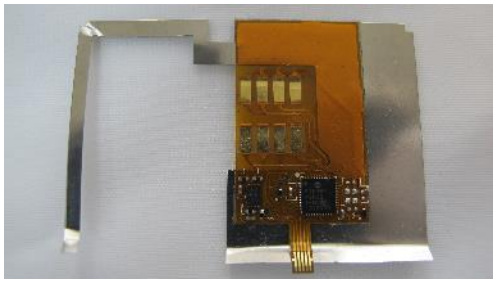
FRAUD ALERT for Merchants & Partners: Skimming Attack Using Shim

Issue:
A data skimming threat has been discovered that can affect payment terminals. Fraudsters use a skimming device to steal card data from your customers. This attack steals the data exchanged between the chip card and the terminal.

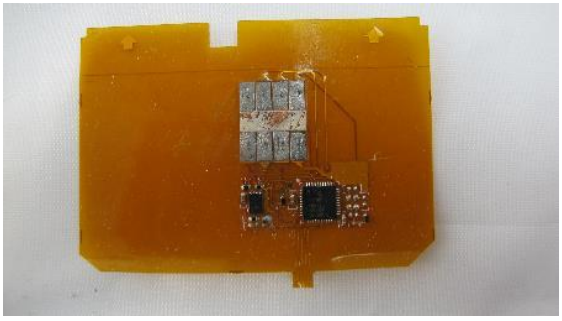
Details:
This skimming threat targets terminals from any acquirer/processor. The attack is accomplished using two devices:

1. The “Skimming Device”, this is a small shim which is inserted into the terminal.

First generation shim device used in early to mid-2016



Second generation shim device used in late 2016



2. The “Retrieving Device” is then used to download the data from the Skimming Device. The Retrieving Device is a card approximately the size of a Chip card, the card is inserted in the terminal and is able to communicate with the Skimming Device in order to transfer the recorded data from the Skimming Device.

Attackers transfer this data to traditional magnetic stripe cards and attempt fraudulent transactions on non-compliant EMV (Chip & PIN) terminals and bank machines, or manual entry transactions on terminals. It may also be possible for the data be used for ecommerce fraud on Web sites that do not use card validation checks like Address Verification, CVV2 etc.

What you can do to prevent this:

Terminals should be properly secured and if possible, do not leave them unattended for extended periods of time. Attackers must gain access to an unattended device and may use distractions to misdirect employees or take advantage of an isolated location to tamper with the terminal.

Regular inspections should be completed on terminals that are frequently left unattended to ensure they haven't been tampered with. If a shim has been discovered inserted into the card reader of a terminal, immediately stop using the terminal and contact Moneris and your local authorities.

For additional information and resources on anti-skimming best practices visit www.moneris.com/fraud or see this PCI SSC resource.