# Retail-BCG
# ATM Jackpotting Kits

**October 2017**
*BN055*

**Retail-BCG**
**Transaction House**
**Summerlea Court**
**Herriard Business Park**
**Basingstoke. Hants**
**RG25 2JZ**

# 1 ATM Jackpotting Kit

Retail-BCG have become aware of an ATM jackpotting kit that is for sale on the Dark Web which provides step-by-step instructions for gaining access to a cash machine for the purpose of unauthorized ATM dispense.

The kit known as 'Cutlet Maker' consists of three components and can allow ATM jackpotting if the attacker is able to gain physical access to the machine.

Criminals would need to gain direct access to the ATMs top cabinet in order to access the USB ports which are used to upload malware via a software toolkit. The toolkit would relay information such as currency & number of notes in each cassette to provide as much detail to the criminal as possible.

## 1.1 ATM Protection

To protect against these type of attacks, the ATMs have Symantec protection (SCSP) enabled. The key benefit to this protection is that it locks down the PC Cores ports (USB included) and will actively search for and detect any unknown devices inserted and then terminate any unknown processes that may attempt to run from these.

For the above-mentioned attack, should a criminal gain access to the top cabinet and insert the software toolkit into the USB port, SCSP will spot this and stop any processes from running.

## 1.2 Black Box Attacks

Most Black Boxes do not attack the PC core but attempt to enable the Black Box on the connection between the PC Core and cash dispenser. If successful, the criminals will then send dispense commands from the Black Box to the dispenser to fraudulently obtain cash.

To tackle this threat, the Multi-Vendor software will, before an application is able to communicate to the dispenser, request that a special function be completed by the operator which requires them to physically open the safe door. Until this is completed the dispenser will remain unauthorized meaning the Black Box will not be able to control the dispenser.

Despite these levels of protection, sites should of course always remain vigilant for any unusual activity or use.

## 1.3 Queries

For any queries regarding this type of attack, please contact operations@retail-bcg.com