

How the Carbanak cybergang stole \$1bn

A targeted attack on a bank

1. Infection



100s of machines infected in search of the admin PC



2. Harvesting Intelligence

Intercepting the clerks' screens



3. Mimicking the staff

How the money was stolen

Online-banking

Money was transferred to fraudsters' accounts

E-payment systems

Money was transferred to banks in China and the US

Inflating account balances

The extra funds were pocketed via a fraudulent transaction

Controlling ATMs

Orders to dispense cash at a pre-determined time