Issued 10/19/17

Dangerous Malware Allows Anyone to Empty ATMs

Hackers are selling ready-made ATM malware on an underground hacking forum that anybody can simply buy for around $5000, researchers at Kaspersky Lab discovered after spotting a forum post advertising the malware, dubbed Cutlet Maker.

The forum post provides a brief description and a detailed manual for the malware toolkit designed to target various ATMs models with the help of a vendor API, without interacting with ATM users and their data. Therefore, this malware does not affect bank customers directly; instead, it is intended to trick the bank ATMs from a specific vendor to release cash without authorisation.

In order to operate, the application needs a special library, which is part of a proprietary ATM API and controls the cash dispenser unit—this shows how cyber "criminals are using legitimate proprietary libraries and a small piece of code to dispense money from an ATM."