GMV PERSPECTIVE

The weaknesses of whitelisting

Juan Jesús León Cobos
GMV

By Juan Jesús León Cobos, Director of Products and New Developments at GMV Secure e-Solutions

Any software loaded onto ATMs to obtain data, steal cash or perform an action intended to commit fraud is by definition ATM malware. It does not need to be a virus or have any specific replication or infection capabilities. The critical factor is that it is not your software, but that of a fraudster.

Because ATM malware does not have much in common with PC malware and is not widespread on the internet, antivirus and other generic PC solutions have difficulty stopping it. This is why whitelisting technology has been largely adopted by the ATM security community as the best technique to secure an ATM.

Whitelisting solutions prevent fraudsters' software from running by not allowing any unauthorised processes to run on the ATMs. The cost of using this approach, however, is that a whitelist containing all authorised processes must be built and constantly maintained.

Whitelisting has two main drawbacks: It makes the ATM software updating process cumbersome, and it interferes with field servicing

Experience following several years of maturing technology has shown that whitelisting has two main drawbacks. First, it makes the ATM software updating process cumbersome. Second, it interferes with ATM field servicing. As a result, a force often emerges within the organisation that works against whitelisting, not by fighting it – it is too late for that – but by trying to find workarounds to make everyone's lives easier. These workarounds represent a major weakness in the protection of today's ATMs, for a false sense of security might in some cases be worse than no security at all.

Securing the process of software distribution

To get around the first problem of a cumbersome software updating and distribution process, some ATM cyber security solutions rely on the security of the software distribution server – i.e. any software that comes from the software distribution tool is automatically whitelisted and installed. It comes as no surprise that most reported network attacks have been perpetrated by exploiting this 'feature'.

The best way to secure software distribution is to keep software distribution and software security servers separated and strictly segregated. Every time new software needs to be sent to the ATM, a new whitelist needs to be created in the security server. That these are two different tasks that should not be done automatically is a well-known security principle called segregation of duties. Building an updated whitelist every time software is distributed should not be that onerous, unless you are updating software every few days – but if that is the case, you are already in trouble. Even OS patches should not be sent often, but only after extensive testing and whitelist updating. An ATM is not an office PC and should not be treated as such.

Securing the process of field servicing

The issue related to field servicing requires a different approach. Security solutions have to acknowledge that the agility and efficiency of field servicing must be preserved. It is security that must adapt, and not the other way round.

The wrong but typical approach of securing this process is to relax the whitelist to include field service tools (even to pre-install them at the ATM) and to allow the connection of field service USB pen drives. This itself is a risk in some countries where field technicians cannot be fully trusted. But even if we assume that technicians are completely trustworthy, it is usually the case that ATM field engineers need to perform special tasks using executable files that would not be wise to whitelist as a general rule, since once they are there, these could be used to attack the ATMs later. Field service engineers also often use USB pendrives to both bring tools to the field and extract logs or other files from the ATM for analysis. Making this compatible with the general rule that USB storage devices should not be allowed in the ATM leads to cumbersome field USB whitelisting,

and increases administration costs. It is also a poor solution from a security standpoint, since regular USB identifiers can easily be forged.

At GMV, we believe that security must be designed for actual use and only minimally interfere with regular ATM procedures. In order to accomplish this, GMV's Checker has leveraged the experience of many customers and features a specific Operator Mode that can be entered into when a properly authenticated field engineer accesses an ATM. This mode allows the engineer to execute any application during a limited time slot. In addition, every action performed will be recorded and sent to the Checker Server. When the time slot has expired or the ATM is rebooted, the agent resumes full protection. No need to whitelist dangerous tools or trust every technician. No need to coordinate the whitelisting process with the life cycle of servicing tools either.

This special Operator Mode can be either commanded from the Checker console or entered into automatically at the ATM by authenticating the field engineer using so-called Operator Mode USBs. These special USBs allow the engineer to engage the Operator Mode simply by plugging the pen drive into the ATM computer. Operator Mode USBs are not special; they are based on regular USB pen drives and are universally identified by their serial numbers. But unlike regular USBs, Operator Mode USBs are encrypted. Encryption is done in a standalone application for PCs included within Checker and its purpose is twofold: it provides better authentication than serial numbers because an encrypted USB cannot be forged, and it hides the contents of the USB thus preventing reverse engineering. Encrypted Operator Mode USBs will automatically be recognised in those ATMs running Checker and cannot be used anywhere else.

Balancing security and operations

Extensive experience with Checker has demonstrated that the management of an efficient coexistence between ATM security and operations requires special attention. Successful ATM cyber security must be designed with field servicing needs in mind. This is not something that you will find in all ATM protection suites, let alone in generic end-point protection solutions, which are most certainly not designed to secure ATMs. ■

Security must be designed for actual use and only minimally interfere with regular ATM procedures