GMV PERSPECTIVE

ATM logical security: the day after

By Juan Jesús León Cobos, Director, Products and New Developments, GMV Secure e-solutions

Today, most ATM security managers are well aware of the need to protect ATMs against logical fraud. Managers are making considerable efforts to ensure the best products are selected for this purpose. However, the increasing urgency in dealing with malware threats sometimes forces them into deploying a logical security solution without fully understanding all of its operational implications. At GMV, having overseen dozens of such deployments, we have observed a number of recurring situations of which we feel deployers must be made aware.

Overcoming initial resistance

In undertaking the installation of a new security system, a common first sticking point is the resistance which may be encountered within the organisation due to anxiety over potential problems and downtime. Despite acceptance of the need to secure ATMs, there will be demands for a guarantee of minimum practical disruption. The organisation will not only expect limited disruption in the ATM service but also in the company's day-to-day operations.

The first thing you should know is that *there will be some disruption*. In fact, the amount of disruption can be predicted; it will be a function of how the ATM software lifecycle is currently being managed. This is because preventing software-based attacks requires having control over software following well-defined procedures. Assuming these procedures exist, you need to get involved and to some extent get in control. And that is always disrupting.

So assuming the organisation will embrace your participation in delicate matters such as managing the software in the ATMs, it is important to gain everyone's trust that your role will not be too disruptive.

Gain trust with the easy wins

In order to gain trust, it is important to show that you understand and can anticipate the impact of the various actions and controls that will be applied. Actual impact is sometimes far from evident. Some of the actions needed are almost transparent yet will raise great concerns. Other things seem simple at first, but will turn out to be rather invasive.

A good place to start is with something that looks frightening but is actually quite harmless: ATMs' Hard Disk Encryption (HDE). For some reason, HDE sounds terribly invasive, but it is very simple, easy to deploy and once deployed makes almost no difference to nominal operations – just as encrypting a laptop is essentially transparent to the user. This is because it does not interfere with the ATM software. Assuming your selected HDE solution is adequate and runs smoothly, it has the potential to be a great start, acting as a quick win to show colleagues that you know what you are doing.

Navigating deployment

Once successful with that quick win, it is time to move on to the trickier aspects. HDE by itself is useless; the main purpose of HDE (besides protection against reverse engineering) is to protect against off-line ATM malware infection by preventing deployed security controls – or 'whitelisting' – being disabled.

Whitelisting is a mature technology nowadays, so enforcing whitelisting looks easy. However, despite being highly secure, whitelisting is also quite inflexible. It assumes the organisation knows (or might eventually get to know) the software that runs in the ATMs. It also assumes the organisation controls the flow and tempo of software changes. If, on the contrary, the operations rely on some improvisation ('flexibility' as it is often called) every now and then, there will certainly be problems in enforcing whitelisting.

Whitelisting enforcement requires several steps: you

▶

Juan Jesús León Cobos
GMV

Increasing urgency in dealing with malware threats sometimes forces managers into deploying a logical security solution without fully understanding its operational implications

▶ need to make sure the software is clean, compliant and trustworthy. You need to get the software tested in the lab and then derive the right security policies. You need to deploy security policies (in whatever form) every time software is deployed. Finally, you need to activate control to enforce security in the ATMs. Whitelisting security enforcement is the act of stopping anything happening at the ATM that is not expected according to the security policy.

The concern here is that any mistake in the whitelisting definition, deployment, change control, or software updating and change management procedures is theoretically able to bring down the ATMs. It is not that whitelisting is difficult. The problem is that it is potentially risky. It does not leave any room for confusion. While this risk can be reduced by defining somewhat lax policies, this is not recommended as it reduces security.

Any mistake in the whitelisting definition, deployment, change control, or software updating and change management procedures is theoretically able to bring down the ATMs

Enforcement is necessary

One possibility to consider in trying to minimise such issues is to deploy whitelisting at first without enforcement. This means that the security control will report alerts but take no action at the ATM. If any policy is wrongly configured, security alerts will be triggered, but the system will not experience any ATM downtime. Parameters can then be refined and errors fixed until alerts cease – properly configured whitelisting sends alerts only during actual attacks, which do not happen every day.

Deploying whitelisting without enforcement for a short period of time will ensure that all policies are correct to the extent that there are no security alerts from your ATMs. This should calm everyone involved and provide a smooth deployment.

However, this approach has a risk. Some individuals will argue that monitoring in itself is sufficient and that actual enforcement of security is not necessary. They will suggest that as long as someone is monitoring the alerts and no red flags appear, then the system is uncompromised... right?

In order to prevent attacks on ATMs, one cannot rely solely on monitoring

Wrong! Experience shows that this option is not effective in stopping a real attack. The fact is that there will be false alarms every now and then (e.g. an ATM loses connection – which may be a network problem, not an actual attack). False alarms mask the real attacks, and response teams may become complacent.

To illustrate this situation, consider a home alarm system, where most owners are notified every now and then of false alarms. Not enforcing whitelisting is like leaving the front door without a lock, just trusting the alarm system for notification, and planning to respond to every alert... and simply due to the fear of losing one's house keys.

The purpose of the home alarm system is to dissuade the thieves, not to make intrusion difficult. Similarly, in order to prevent attacks on the ATMs, one cannot rely solely on monitoring. Security must be enforced.

Ensure appropriate governance

Once the logical security solution is deployed and working, you need to deal with day-to-day administration and operation.

One of the weakest links in the security chain is the people. The solution should support as a minimum centralised management, Role Based Access and extensive audit capabilities. In addition to that, personnel should be screened, administrators kept to a minimum and duties segregated, particularly between security, development and operations personnel. For example, no single person should be able to deploy software and approve security policies.

Keep control of monitoring, at first

Most ATM estates already have mature incident response mechanisms in place, usually related to ATM hardware problems or physical security incidents. You will have to assess the convenience of merging your solution's event reporting and alarm systems with the existing ones. Obviously there are pros and cons to doing this, essentially having to do with cost reductions versus control.

When making this decision, it is important to keep in mind that a mistake in policy definition will have visibility in event reporting. Failure to account for one process in the whitelist will not only impact upon service, but will trigger a multitude of alerts. And such an alert overflow could collapse the whole system.

Its highly recommended that you keep control over the monitoring of events from the security solution, and run it for some time before turning the responsibility over to others.

Be ready for action

In case of a security alarm being triggered, actions to investigate the alarm should be well-defined beforehand. The most important consideration is for all alarms to be thoroughly investigated to determine whether they are false or real incidents. Know that as long as enforcement is in place, the ATMs should be secure, so taking time to properly investigate an alarm is time well spent (although the noise disruption made by false alarms needs to be well managed).

The contingency for forensic analysis must be planned for in advance, as this usually involves ATM forensic experts, who are not always easy to find.

Finally, there should be reaction capabilities designed to deal with cases in which a misconfigured security policy or an operator mistake impacts ATM service availability. The advice here is straighforward: once an incident is determined to be a mistake rather than an attack, security enforcement should be suspended in some ATMs or even in the whole estate for a short period of time using a sort of panic button. The probability that a genuine attack would occur at exactly the same time is low, while the importance of ATM availability is enormous. When choosing a solution, make sure to understand how to deal with administrative or operational mistakes to minimise impact on service.

Think ahead

Once everything is in place and working, there are still two long-term aspects which must be addressed.

The first is Security Intelligence. It is important to keep up to date about cyberattacks on ATMs. This can be done in a number of ways, such as by receiving alerts provided by ATM manufacturers, logical security solution vendors or specialised forums, or by even having one's own cyber intelligence or digital surveillance solution.

The other long-term issue is the future evolution of the ATM logical security solution. Ensure the vendor is one that you trust will deal with emerging threats, periodically release new controls and is devoted to ATM security as its core business. Otherwise, there is a risk of becoming stuck with an incomplete or obsolete solution.

Then again, on second thought, this is something you should have taken into account when selecting your security solution in the first place. ■

When choosing a solution, make sure to understand how to deal with administrative or operational mistakes to minimise impact on service