GMV PERSPECTIVE

Will recent network attacks change the landscape of ATM cyber security?

Juan Jesús León Cobos
GMV

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

Ten years ago when GMV was trying to work out how to bring logical security to ATMs, we were taken aback by the difficulties we faced in conveying our message to potential customers' organisations. A common problem was the lack of interoperability between the ATM software and servicing staff, and the corporate IT security staff. They spoke different languages, with the ATM group knowing almost nothing about logical security, and the corporate IT security team knowing very little about ATMs.

As the cyber threat in ATMs has become recognised, ATM logical security teams have emerged within deployers' organisations. They typically stand separate from their corporate IT security colleagues as their areas of expertise differ; the threats that corporate security deals with – password stealing, ransomware, phishing, etc. – are to an extent meaningless in the ATM context, which features its peculiar jackpotting or software skimming attacks. Indeed ATM logical security experts need not be skilled on, say, cloud security, and corporate IT security teams need not know what XFS or an SDC bus is.

There is a lack of interoperability between the ATM software and servicing staff and the corporate IT security staff

A typical GMV Checker customer would be the ATM logical security team that sits within the ATM management organisation. They would be experts specialised in countering ATM attacks, but their idea of logical security would not be fully in line with that of those in corporate IT security. However, they make their own decisions regarding ATM logical security policies and controls. In turn, corporate IT security takes care of seemingly more pressing and 'traditional' matters, and contents itself in ensuring that the ATM logical security team enforces a few generic corporate rules regarding things such as strengths of passwords and the deployment of corporate antivirus software in ATMs, an utterly useless notion. Some other typical requirements such as daily OS patching could even be conveniently disregarded for ATMs due to practical implications. Other than these areas of overlap, the day-to-day operations of both teams are normally uncoordinated.

Asian attacks signal a warning to corporate IT security

To some extent, the situation in which ATM logical security finds itself resembles that of corporate IT security years ago – an exciting new field but having little budget and certainly not a lot of attention within the organisation. However, I anticipate the latest ATM cyber-attacks in Asia will soon make the two aforementioned teams cooperate more closely, which I regard as extremely beneficial for their organisations and ATM security in general.

For those that are not familiar with these latest attacks, here is the low-down: Criminals have hacked into some ATM deployers' corporate networks, gained access to the server that distributes the software to ATMs, and used it to distribute malware. This is typically followed by massive, coordinated cash-outs, resulting in million-dollar frauds.

Network-based infection attacks have not been completely unheard of in past years, yet the recent cases in Asia should be regarded as a major shift in methodology – until one year ago, criminals usually accomplished this by physically accessing each ATM. But this technique has been rendered ineffective due to widespread ATM HDD encryption. The new 'remote distribution' approach, however, has a flavour of sophistication and scalability that is probably here to stay.

Surely, hacking into the corporate network

and taking control of the server that is used to deploy software applications to ATMs would be considered by corporate IT security as a matter for its own team. To some extent, this criminal move might ricochet insofar as they now have the full attention of corporate IT security in the attacked organisations. Classic security governance would demand that this asset (the ATM full of cash) and associated risk (jackpotting), unrelated to information security but undoubtedly valuable, be fully considered in corporate IT security planning and budgeted for adequate protection. This would include refined risk mitigation actions such as threat assessment intelligence, with implications that are yet to be seen.

Many current 'whitelisting' measures are inadequate

Another interesting observation following on from these attacks is how it was possible for malware to be deployed and run on ATMs that ought to be enforcing whitelisting. It so happens that some whitelisting solutions are designed to fully trust the software deployment tool. The rationale behind this trust is that software can be deployed without the need for explicit, case-by-case coordination with the ATM logical security team, thus avoiding the need for security clearance of applications or OS patches each time. This rationale should be challenged, as testing and approval of new versions of legitimate applications, or patches for that matter, are actually an underlying requirement for whitelisting to be effective at all. Automatic uploading of software to ATMs without previous clearance from security should be avoided.

Certainly there are cost implications of doing things this way, and the benefits of automating software upgrades should be considered. While I do not regard this trust in the software deployment server to be fully misplaced, it certainly goes against the security principle known as 'segregation of duties'. It is healthy to have different people programming and approving the ATM applications, just as it is healthy to conduct personnel security screening. There is a cost associated to these security principles, though, and a risk assessment is needed in each organisation to come up with adequate procedures. Of course now these decisions have to consider the reality of network attacks.

In cases where automatic software deployment needs to be employed, a few actions can be taken to mitigate the risks associated with these attacks:

- Keep the ATM network segregated from other corporate networks. Where this is not the case, for instance for ATMs in branch networks, a full network redesign might be necessary.
- Make sure that any server that is placed within the ATM network is secured and has its patches up to date, and schedule them for penetration testing. Software attacks may come through other servers in the network masquerading as the legitimate software deployment server
- In cases where automatic deployment is used only for the operating system, it might be preferable to take the ATMs out of the corporate Windows updating process. Evidence shows that a slower patch rate for ATMs results in much lower risk than an automatic deployment process that can be used to penetrate ATM defences.

An Advanced Persistent Threat

Corporate IT security should understand what it is facing. A criminal organisation that coordinates dozens of cash-outs in a matter of minutes is a different beast from the one that operates a botnet for DDoS attacks or runs a site to infect an organisation's PCs with ransomware hoping to get a few bitcoins. These risks are all important, but ATM attacks through network intrusion would fit what corporate IT security would call the APT (Advanced Persistent Threat) category. The potential scalability of these malware infections is huge, and so are the potential benefits for the criminals. There are few 'business cases' in which criminals hacking into an organisation could obtain such huge gains as in the jackpotting of numerous ATMs simultaneously.

A final word on the geographical nature of the attacks. It has been the case in the past that countries were chosen for attacks based on how easy or difficult it was to find insiders to perpetrate physical infections. Europe has traditionally not been the first target for these attacks. However, by penetrating the networks of organisations remotely, criminals can now employ local hackers to target ATMs in foreign countries – those that dispense cash in an internationally accepted currency, such as the euro.

Consider why black box attacks have been hitting western Europe so strongly in the past months. Just think, if you were the criminal, which countries would you choose to run multiple, simultaneous jackpotting attacks over hundreds of ATMs? ■

Some whitelisting solutions are designed to fully trust the software deployment tool

The potential scalability of these malware infections is huge, and so are the potential benefits for the criminals