GMV PERSPECTIVE

The unprotected afterlife of Windows XP

By Juan Jesús León, Director of Products, GMV

Juan Jesús León
GMV

Chances are you already know that Windows XP support ends 8th April 2014. The impact of this situation on ATMs running Windows XP is basically twofold. On the one hand, there will be no more updates by Microsoft, particularly security updates. A second effect, that we will not discuss today, is that manufacturers in the ATM ecosystem may no longer provide support to hardware or software that is associated with XP. In this article we will discuss the implications of not having security updates, fixes or patches for Windows XP.

If we were to judge by the multitude of press releases on the topic, migration would seem to be the only way forward, since most voices suggest that ATM security will abruptly degenerate starting 9th April. The consensus seems to be that ATMs with outdated security will be zombies – but unlike the 'walkers' from TV's *The Walking Dead*, which are less vulnerable to attacks precisely because they are already dead, the almost defunct Windows XP is expected to enter a new age of fragility that will inexorably deteriorate the cyber-security of our ATMs out of the blue. This need not be the case. It just happens that the risk management strategy for your ATM network (hopefully you have such a thing in place) will need to be reassessed in light of the new situation.

Most voices suggest that ATM security will abruptly degenerate starting 9th April

A note on compliance

Before discussing actual ATM cyber security, we will briefly address the issue of compliance. Requirement 6.1 of the PCI DSS specifically demands that all system components and software be protected from known vulnerabilities by having the latest vendor-supplied security patches installed. This is a typical best practice and one that usually makes sense.

It is thus sensible to question how compliance can be achieved when there are no more security patches available. There is some controversy here. Some argue that diligent risk mitigation actions should be considered as the best option next to compliance. Others openly discuss applicability of PCI SSC standards to ATMs. Indeed the PCI PIN Transaction Security Point of Interaction (PTS POI) Security Requirements issued last year clearly state that *"the financial industry needs a global ATM security standard"*, while adjustment of existing PCI standards to ATMs *"is currently under consideration at the PCI SCC"*, and until that happens both PCI PTS POI Security Requirements and PCI PIN Security Requirements *"fill the perceived current guidance gaps"*. This implies that PCI only provides guidance at this point and there are no real compliance issues specific to ATMs.

It is also worth mentioning that a significant number of ATMs are currently not at the last level of security patching (not even SP2 or SP3), which suggests that patching is not a priority for some ATM network managers and thus the absence of any further patches can hardly be a major concern for them.

This last statement might sound a bit surprising, but it must be said that this 'lack of patches' situation is not necessarily unreasonable. As in any production environment, the continuous patching of the operating system should be done with caution, within a policy of systematic regression testing and service availability. This has a cost. If there is no perception of risk, one might feel to be better off without it.

So ATMs running unpatched Windows XP are not new. Yet we have to admit that this is not the general situation, and making it the rule rather than the exception is a context that deserves rigorous analysis. But we have seen little rigor and many admonitions such as *"migrate or face the consequences"*. Very well, but exactly what would these consequences be?

Security consequences of not migrating

In a nutshell, here is the rationale for why you do not need to expend a lot of money in migrating from Windows XP right away:

- Current ATM cyber-attacks follow well-understood patterns and do not make use of the presence of Windows vulnerabilities. Prevention of these attacks today is achieved by installing a suitable cyber-protection solution in your ATM.
- While there is a risk that attack patterns change because of new unpatched vulnerabilities, new vulnerabilities will only turn out to be relevant to ATM security if attacks follow completely different patterns than those used today.
- The risk associated with these new attack patterns can be analysed, and such attacks could be effectively prevented by installing a state-of-the-art ATM cyber-protection solution and adopting a few precautions such as avoiding use of certain Windows services over the network.

In order to justify this rationale, we first need to recall how ATMs are being attacked today. Current cyber-attacks are based on introducing malware into ATMs. In order to do this, criminals have almost always had physical access to the ATMs and have not specifically taken advantage of any Windows vulnerabilities. A good cyber-protection solution for your ATM, such as Checker ATM Security, properly deployed and configured, is in this context definitely more important than a good level of patching. And if you already have cyber-protection in place, you are well-focused in your XP end-of-life risk mitigation strategy. You just need to consider a few 'residual risks' and take a few additional actions.

I am now about to get fairly technical... If you prefer to bypass the security lingo, feel free to jump to *Simple guidelines to reduce risk* for a summary.

Breaking an unpatched ATM

Let us start by assuming a new vulnerability is found in XP and that there are no patches to remedy it. A vulnerability is just a weakness. It causes no harm by itself. For an attacker to take advantage of its existence, he needs what is called an 'exploit'.

We do not need to discuss what an exploit actually is. Just think of it as the instrument that a criminal uses to take advantage of a vulnerability. It might be a chain of commands or actions, but for the sake of simplicity we will assume it is a piece of software that the attacker can use to subvert a legitimate programme. It is this exploit that the attacker needs to deliver to the ATM, and it can be done in two ways: locally – requiring physical access to the ATM, or remotely – over the network.

So far vulnerabilities have not played a very substantial role in cyber-attacks to ATMs and neither have exploits. The main effect of XP end-of-life could be that this changes. Let us see why.

The crook's dilemma

As we have explained, so far cyber-attacks to ATMs have been performed by criminals who gain physical access to the ATM and introduce malware. Getting the right malware was the essential element. Criminals have not needed exploits, nor paid much attention to them. This is because local exploits usually focus on privilege escalation, a concept that makes sense for servers available to many users, when the purpose of the attacker is to access resources that he cannot from his low privilege account. However this concept is not so relevant to ATMs. We are assuming that the ATM is protected by a state-of-the-art cyber-protection solution, which does not (or at least should not) rely on user privileges to decide what a user can or cannot do. Instead it should rely on a security policy that is enforced and cannot be broken by any user, no matter his privileges. Of course we are not only talking about whitelisting here, but a resilient and exhaustive protection including registry access, keyboard control, devices authorisation and much more. Top ATM security products such as Checker have been designed to protect against any user because often insiders with physical access to ATMs have been part of the context of attacks.

A good cyber-protection solution for your ATM is more important than a good level of patching

However, where attacks based on physical access are becoming increasingly difficult because of sophisticated sandboxing, whitelisting and encryption solutions, the absence of new patches might raise interest and make remote exploits more relevant. Traditionally they have been the crème de la crème of exploits. They have dominated the general purpose malware market. When we discuss home PCs, for instance, it is obvious that gaining control of a PC using its internet connection is easier and less risky than breaking and entering a residence in order to physically access the computer. However, the reverse is actually true when it comes to ATMs, since they stand in isolated networks and at the same time they are (to some extent) physically exposed.

Where attacks based on physical access are becoming increasingly difficult, the absence of new patches might make remote exploits more relevant

Although so far remote exploits have received little attention from the ATM cyber-mafias, they might now come in for new consideration. Criminals ▶

could effectively turn to the network when a new vulnerability is found and there is no patch ready to fix it. How likely is it that they would do that? What realm of new possibilities would now be open to them? Let us now discuss this scenario.

Turning to the network

To make a long story short, we will focus on vulnerabilities that allow arbitrary code execution. Typically these can be exploited when a vulnerable service is accessible via the network.

If possible, do not use Windows services that are exposed to the network

Once again, an ATM protected with a comprehensive cyber-security solution such as our Checker product – which combines application level firewalling with whitelisting in a coordinated manner – will significantly reduce ATM exposure. Faced with an ATM so protected, an attacker with network access will only be able to access the vulnerable service from specific IPs. However, an IP can be simulated (for instance using IP hijacking). So let us assume a worst case scenario, where an attacker has access to an ATM network service which is legitimately allowed to run in the ATM.

The attack would more or less proceed as follows: a readily available exploit is used by the attacker to take advantage of the existing vulnerability. The vast majority of these remote vulnerabilities are of the so called 'buffer overflow' type, which essentially means that the exploit will be able to upload and run a specific piece of malware code – called the 'payload' – within the frame of the running service. So using remote exploits and network access, the network would become just a new way to introduce malware into the ATMs, complementing USBs or CD-ROMs. But there is an important difference. Introducing malware as an injected payload renders whitelisting useless because the now infected process is already up and running. Still, Checker – which does much more than whitelisting – will prevent the payload from accessing any devices or data files. That is, unless the infected process had a legitimate reason to access these resources.

Most risks associated with unpatched vulnerabilities can be mitigated by installing a state-of-the-art cyber-protection solution designed for ATMs

Is it likely that this will be the case? Recall that we are implicitly assuming that the infected process is not part of the ATM application software, but part of the Operating System! Indeed, this is the whole point. The service must be a Windows service. That is why it was known to be vulnerable and why it could not be patched. So it would be a generic XP service (such as any DCOM based service or Samba or Terminal Server, etc.) that your ATM requires to function. And you must have given it some privileges for this attack to be successful.

Even if this were the case, it should be mentioned that starting with SP2, Microsoft put in place a feature called Data Execution Prevention (DEP), which further reduces the risk of a potential buffer overflow vulnerability being exploitable by preventing injected code from running. So if at least you have SP2 installed, you already have some protection in place.

Simple guidelines to reduce risk

Summarising the discussion above, most risks associated with unpatched vulnerabilities can be effectively mitigated by installing a state-of-the-art cyber-protection solution specifically designed for ATMs, such as Checker ATM Security. Moreover, the residual risks can be significantly reduced by considering the following simple guidelines:

- If possible, do not use Windows services that are exposed to the network.
- If you must use them, restrict the access that these services have to sensitive resources, such as data files, USB devices or the dispenser.
- If your service must have this access, then replace that particular Windows service with a commercial one (or a developed one) that is fully supported from a security point of view.
- Make sure you have at least SP2 installed.

Let us wrap up by summarising the situation: you have an ATM equipped with Checker ATM Security and well-configured security policies and encrypted disk drives. Crooks are having trouble breaking into it in the usual way. Instead of trying some other unprotected ATMs they turn to their supportive mafias for new network exploits. Now these mafias can no longer use maintenance personnel but require skilled people with internal network access. Further, they need to find a vulnerable network XP service that you inadvertently left running and that required access to sensitive ATM resources, so that a payload can be constructed to unload a malware that in any case will very likely be blocked by Checker.

And in order to avoid this slight and distant risk, you are about to spend an enormous budget to migrate your entire ATM network out of the moribund XP, which has well served you for years. And you want to do that in a very short time period.

Or maybe the point is that you do not have Checker installed. ■