Cash
Your transaction is complete
Please take your cash and receipt
CASH
INSERT CARD
Cancel
Correct
Confirm

Cyber-protection for today's embedded devices

Safeguarding ATMs

kaspersky

A whole lot of problems for the ‘hole in the wall’

In the beginning...

ATMs have always attracted the attention of criminals. To get at the contents of these machines, attackers have resorted (and sometimes still resort) to drastic measures such as power drills, circular saws, blowtorches, explosives and even using vehicles to try towing them away.

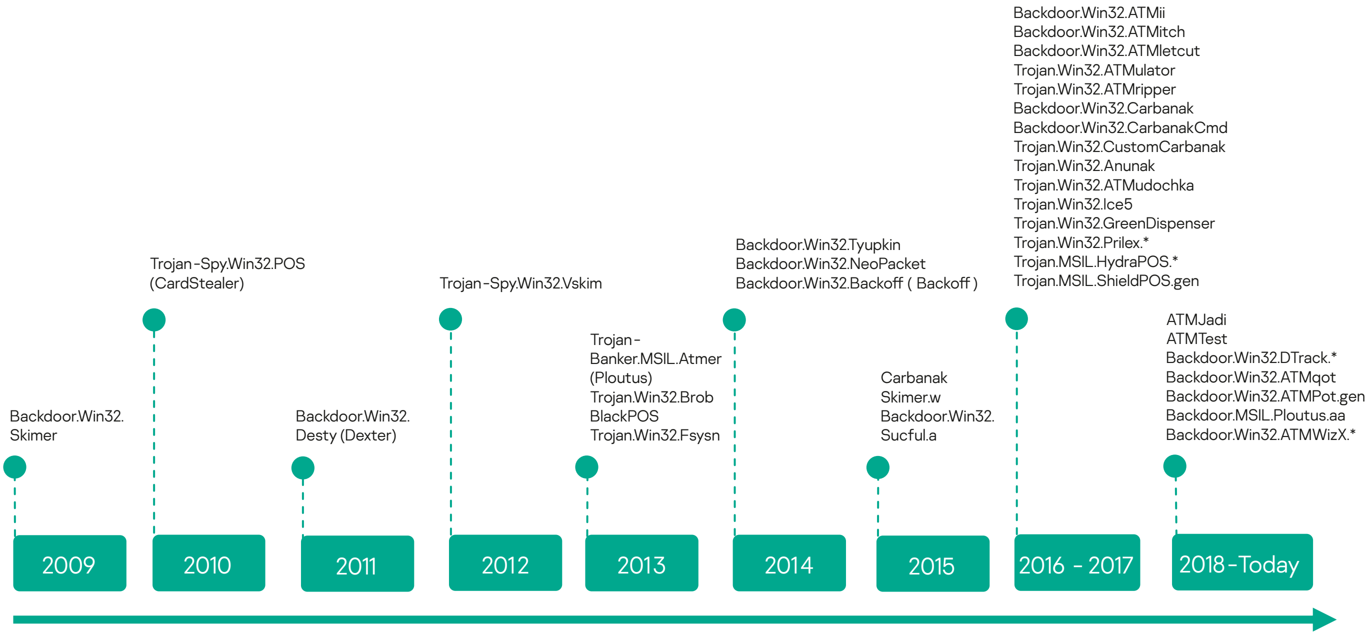
Next came skimmers – devices designed to steal the bank card details that ATMs work with. Since the introduction of the international standard ‘EMV’ (Europay MasterCard VISA), which defines requirements for interaction between a credit card and a payment device, levels of ATM skimming have, fortunately, dropped noticeably.

Trojan wars

However, the criminals haven’t given up. Now rather than power tools, they use specially crafted malware. Instead of explosives or a ‘white plastic[1]’ card, they need only infect an ATM with a Trojan, allowing them to withdraw all the banknotes from the ATM whenever they want. As well as stealing money, criminals can also disrupt the operation of the machine, and launch a DoS (Denial of Service) attack, causing further financial losses for the bank that owns the ATM.

Over the years, a number of malicious software samples developed to target ATMs have been uncovered. The first malware aimed at ATMs – **Backdoor.Win32.Skimmer** – was detected by Kaspersky back in 2009. This Trojan steals the user’s bank card data and can also dispense cash without the account holder’s knowledge: it can still be found infecting machines to this day.

During the course of our work, we’ve accumulated and analyzed enough examples of Trojans to know which are the most widely used, and how best to counter them.



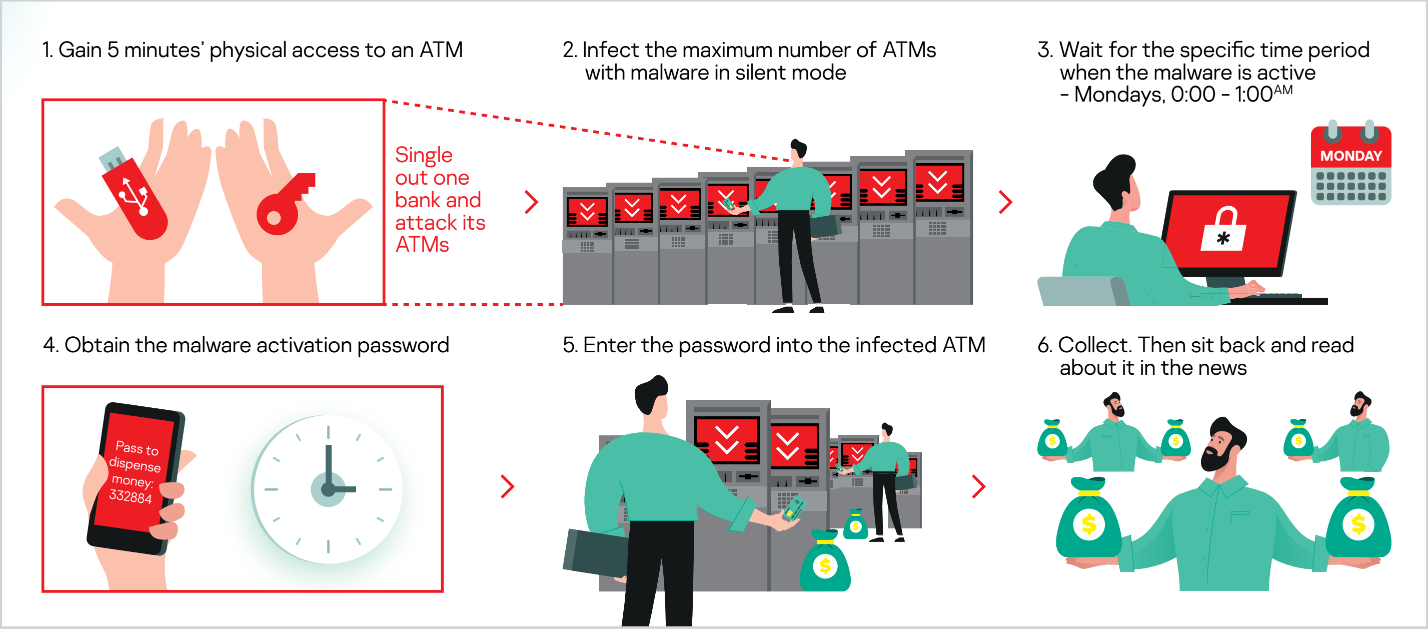
Timeline of ATM & POS malware detection – remembering that new specimens emerge while the old ones are still out there

[1] A specially prepared card containing data from a stolen payment card

Tyupkin

In March 2014, the world learned about **Tyupkin** - malicious software installed on ATMs that allowed criminals to withdraw huge sums of money. All the attacker had to do was approach an infected ATM, enter a code on the keyboard, and the machine disgorged all the money it contained.

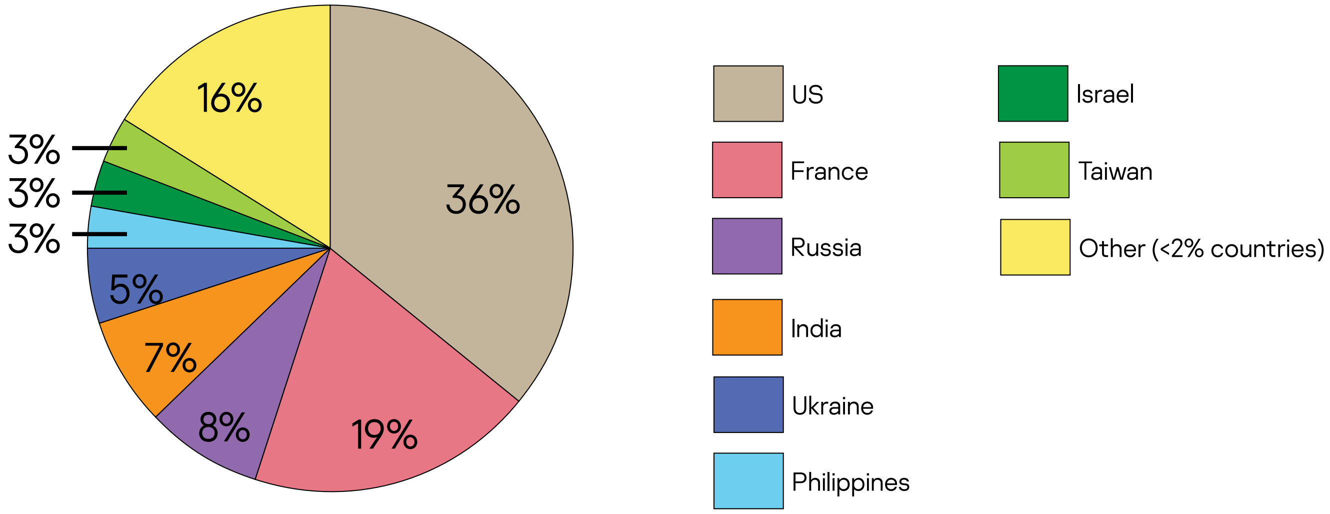
Before we talk about how malicious code works and how it ends up on an ATM, it's important to understand that each ATM is a computer designed to perform specific tasks, reliant on practically the same operating systems as traditional workstations and servers, containing the same vulnerabilities and subject to the same cyberthreats.


1. Gain 5 minutes' physical access to an ATM
Single out one bank and attack its ATMs
2. Infect the maximum number of ATMs with malware in silent mode
3. Wait for the specific time period when the malware is active - Mondays, 0:00 - 1:00AM
MONDAY
4. Obtain the malware activation password
Pass to dispense money: 332884
5. Enter the password into the infected ATM
6. Collect. Then sit back and read about it in the news

ATM malware 'Tyupkin' forces ATMs into maintenance mode and makes them spew cash

Our experts found that the Tyupkin malware (**Backdoor.Win32. Tyupkin**) was installed on ATMs with the help of a bootable CD which required direct access to the ATM's computing system. Having penetrated the ATM's operating system, the malware maintained its presence on the infected machine, giving the attacker access to its contents.

First, it disabled the installed protection solution by removing its software components. It then launched an infinite loop, waiting for user input. And, to hamper detection, it only accepted commands on Sunday and Monday nights. Armed with the commands and the special code the Trojan accepted, the criminal could then gain access to the contents of the ATM cassettes and withdraw the cash.



The number of Tyupkin samples by country (according to VirusTotal statistics)

Carbanak

In the spring of 2014 Kaspersky was involved in a forensic investigation after the ATMs of one bank started dispensing cash without any physical interaction between recipient and the ATM. That's how investigation into the **Carbanak** campaign, and research into the eponymous malware, all started.

Carbanak is a backdoor Trojan, designed for espionage, data collection and the provision of remote access to infected computers. It's known to incorporate code fragments of the infamous **Carberp**[2]. Once the attacker has gained access to a machine, the network is explored for opportunities to spread the infection to critical systems – processing, accounting, and ATMs. This is done manually, trying to hack key computers (such as administrators' machines) and using tools to spread the infection to other computers on the network. So having gained network access, the attackers could move from one computer to another until they found an object of interest. The choice of objects varied between attacks, but the result was always the same: money was stolen from a financial organization, and ATMs were a main channel for withdrawals.

If they can manage to penetrate computers with access to an internal ATM network, or if the bank itself has remote access to its ATM devices, fraudsters can use this to withdraw money, and more. They don't even need special tools to infect ATM software – in Carabanak attacks, standard tools designed for legitimately controlling and testing ATM equipment were used.

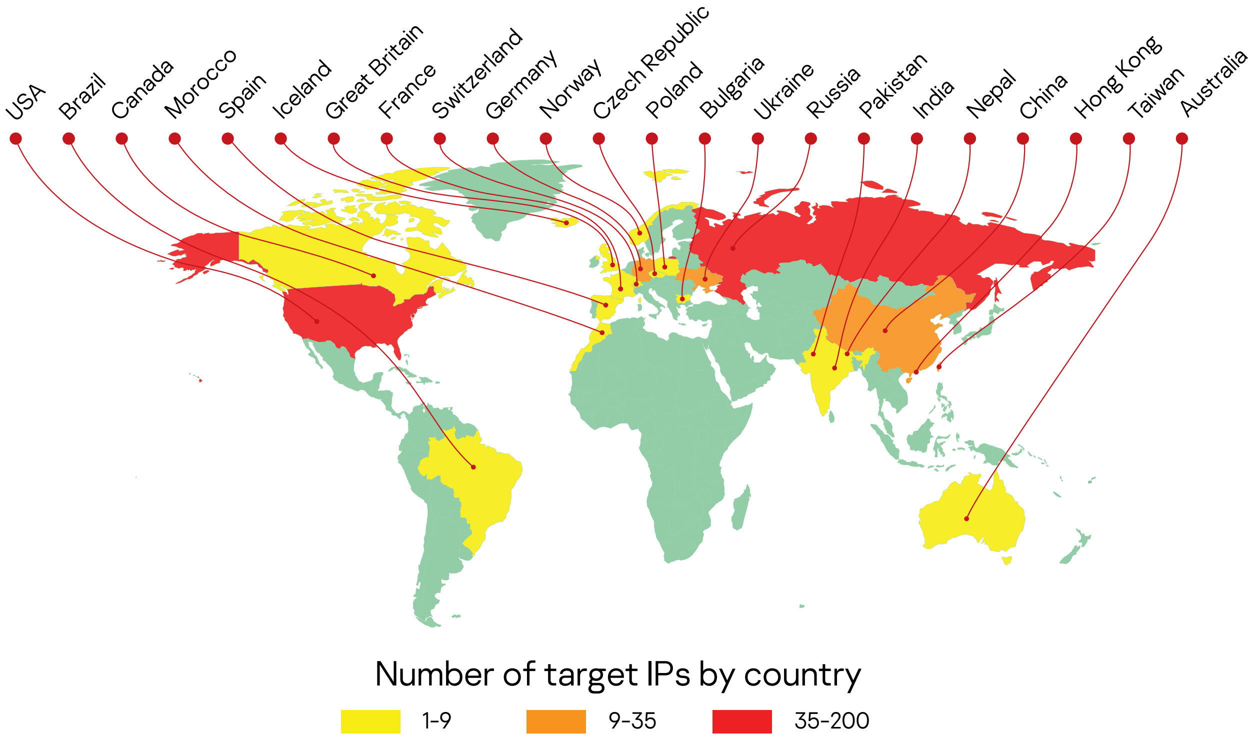
Legitimate tools and solutions installed onto ATMs for monitoring purposes are generally agent programs that receive commands from special workstations on the bank's internal network, to which they then send data.

These agents may:

- Monitor events inside the ATM
- Distribute software across all the bank's ATMs
- Download files from ATMs to a dedicated server inside the bank
- Provide remote access to ATMs.

These agents are used for remote administration and ATM configuration by bank employees, so they naturally appear in the 'permitted' list of software operating on the ATM device. This makes them particularly useful to attackers who've gained access to the bank's internal network.

Up to 100 financial institutions were hit at more than 300 IP adresses in almost 30 countries worldwide.



Carbanak infection by country at the height of activity

[2] The Carberp cybercrime group was one of the first to make serious use of specialist malware targeting remote banking systems. Long after many group members had been arrested, the malware remained active and evolving

Ploutus – Latin American expansion

The Latin American cybercriminal scene has experienced a recent boom. Local blackhat hackers have built up their tools and abilities, evolving from crude copycats of Eastern European malware to producers of advanced specimens marketed as easy-to-use Malware-as-a-Service: a great option for low-skilled cybercriminals. ATMs have earned special attention as offering the shortest route to hard cash, without the complication of long laundering chains.

A good example is **Ploutus**[3], first detected in 2013 and now established as one of the most developed ATM-busting malware families. In 2017, it's self-named Peralta strain established a new record - helping hackers steal almost $65,000,000 from 73,258 compromised ATMs. The malware was usually installed manually, often by low-paid and bribable service technicians – or just by picking the lock on the ATM's service door.

Another interesting strain of Ploutus, now known as version 'Q', was coincidentally also discovered in 2017. Analysis of the infection revealed that the Trojan was using an opensource library responsible for wireless connectivity – as well as the Team Viewer remote management application. All this meant that the perpetrators were clearly using a USB wireless dongle to remotely control the jackpotting process – but still without channeling any suspicious traffic across the ATM owner's corporate network. The usual mode of operation here is to use a directly connected keyboard, so this demonstrates how ingenious cybercriminals can be when the situation requires it. For as long as malware-building design continues to adopt an increasingly modular, assemble-malware-around-a-purpose approach, cybercriminals will be well placed to adapt their operations to the specifics of their selected targets.

That such huge numbers of ATMs are susceptible to being easily hijacked via direct contact is partly due to a general lack of efficient anti-intrusion countermeasures. The number of aging, often second-hand ATMs out there is much greater than owners publicly admit – and fitting them with effective protection isn't easy. With budgetary constraints also being a factor, it's tempting not to bother – to the benefit of threats like Ploutus.

The Ploutus story doesn't end here. In 2021, the ATMs of a Brazilian vendor were targeted. The techniques employed included gaining admin privileges to enable the use of mouse commands, as well as modifications to the vendor's testing utility, so the dispenser system could be requested to 'jackpot' all its contents. This successful Ploutus campaign once again used a direct contact scenario.

Today's global threat

Ploutus/Peralta is just one example – there are many more stories still unraveling. Latin America's ATM-busting operations in Europe and other parts of the world are becoming more and more bold. It would be a grave mistake to underestimate this developing threat, especially given the staggering number of old ATMs running no-longer-supported - and vulnerable – software.

[3] Kaspersky detects Ploutus family as Backdoor.MSIL.Ploutus, Trojan-Spy.Win32.Plotus, HEUR:Trojan.Win32.Generic, Backdoor.MSIL.Ploutus.aa, Backdoor.MSIL.Ploutus.q

Securing embedded systems

An embedded system is a specialized computer located directly on the device it's managing. In the case of cash machines, it's a control computer embedded in the ATM. Most often, these computers run specialized versions of the Windows operating system, such as Windows Embedded or the later Windows IoT. Although only a limited set of the software included in this operating system is necessary to ATM functioning, any of it may contain vulnerabilities. So additional means of protection are needed in just the same way as for desktop and servers.

The Tyupkin and Ploutus attackers above faced little difficulty in copying from CD-ROMs or USB drives to an ATM, and then running malicious tools. Clearly, recommendations for the physical protection of ATMs aren't always followed, giving cybercriminals the chance to access the bootable CD. But it's not just about the physical vulnerability of the device: the attackers were also able to execute arbitrary malicious code, using this to gain access to ATM cassettes full of cash.

Eliminating unauthorized downloads

The Tyupkin and Ploutus operators use specialized bootable CD- ROMs or external USB-connected storages to download malicious code. They then gain access to the ATM operating system directories and manipulate the files. This makes it possible to introduce further malicious code that then receives all the necessary privileges to function inside the operating system.

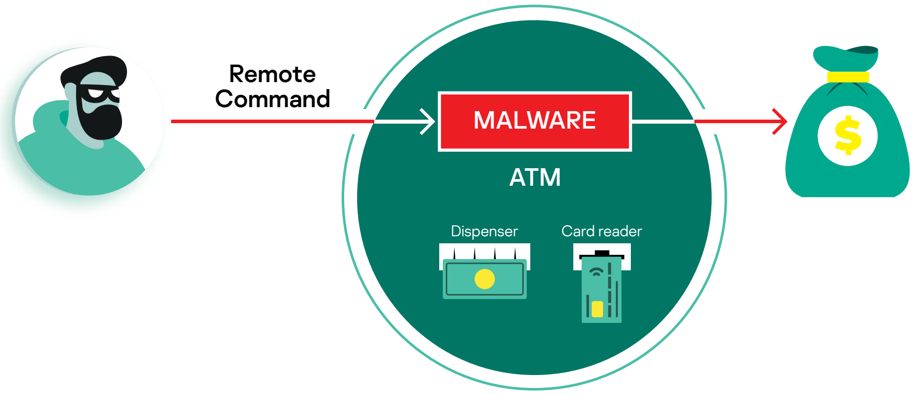
To protect ATMs from this kind of threat, unauthorized downloads from external media that may contain malicious code, or that allow cybercriminals to disable an installed protection solution, must be prevented. This can be done by setting the correct load order in the BIOS (loading the ATM operating system from the hard drive should come first) and protecting the BIOS settings with a password.

Another approach to ATM protection is Full Disk Encryption (FDE) of the disk from which the ATM operating system is loaded. This can block attempts by cybercriminals to modify operating system files, manipulate the ATM file system, or launch malicious code when the operating system is run. But this can cause problems in terms of integrity and device availability (if you reboot the system while managing it remotely, for example, you won't be able to enter the password) so FDE often isn't the best solution.

Monitoring for safety

To forestall any attack that makes use of the standard tools installed on ATMs, it's important to:

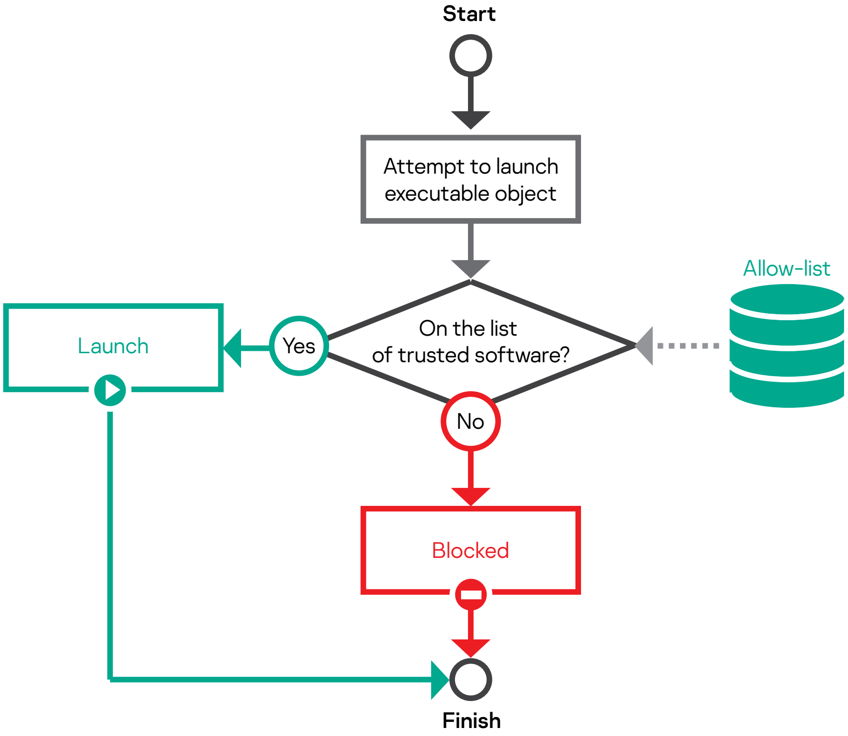
- Eliminate the possibility of unauthorized remote access to the ATM (remembering Carbanak, this may mean introducing multi-factor authentication for mission-critical activities such as managing ATM operations).
- Prevent any critical manipulation of its equipment (if you can't block remote access to the ATM device, at least keep workstations controlling ATMs separated from the office network).
- Monitor and ensure ATM safety in conjunction with the security of the rest of the corporate IT network.



Even if the ATM doesn't include remote access tools, criminals can use malicious software to illegally withdraw money or steal payment data

Hardening the system

System hardening relies on closing entry routes for malware and other threats by limiting or blocking some applications, websites or devices - by type or functionality or even individually - and permitting others. A 'Default Deny' approach, allowing only the use of very specific 'allow-listed' business-related resources (including both software and devices like storages and mice) on corporate machines, is the gold standard here. It's an approach that can be tough to implement in complex and fluid working environments, but it's ideal for systems built around a specific purpose. As a result, Default Deny is the de-facto scenario of choice for ATM protection, hardening the system against attempts to introduce malware. It can also, to an extent, help prevent attackers from messing with the ATM's software stack.


Start
Attempt to launch executable object
Allow-list
Launch
Yes
On the list of trusted software?
No
Blocked
Finish

In specific ATM operating conditions, system hardening-based protection alone, without the addition of anti-virus, can provide reliable protection - as is acknowledged by banking & finance regulators across the globe. This is important for older devices which may not have the power to run any form of anti-malware software - systems hardening is not resource-heavy. But there's a catch.

Unfortunately, even legitimate, allow-listed software can be hijacked using a number of different techniques. Some examples include vulnerability exploitation, the 'living-off-the- land' approach and the leveraging of PowerShell scripting, a standard Windows administration instrument.

Integrity control

ATMs are susceptible to direct contact attacks. Most reside not in protected buildings monitored by security guards, but in public spaces where someone in overalls opening the device's service door is unlikely to be noticed. Even with system hardening countermeasures up and running, it's easy enough to switch off the machine, rip out the hard drive, plug in a computer and copy malicious code right into the file system, or even modify legitimate files. A Default Deny scenario would prevent stray applications from running – but it's still possible to tamper with non-executable but critical files.

For this reason, regulators recommend installing File Integrity Monitoring to address violations that basic system hardening tools alone can't be expected to prevent.

Security system self-protection

The integrity of the system is crucial - but preventing the security solution itself from being compromised is fundamental. Security solutions tend to operate at a high privilege level, but this can be exploited by insiders. So ATM security must possess powerful self-protection capabilities, both at the level of the machine's own system and that of (remote) management instruments. The protective service should not be capable of being disarmed, and configuration change attempts must be prevented. Cases of security solutions being switched off manually or even used for hacking tools' delivery are not unknown, so this prevention functionality must be built into the solution's architecture.

Vulnerability exploitation prevention…

Cyberattackers can use existing vulnerabilities in ATM software, starting from its often-obsolete or rarely updated OS, to coerce legitimate apps into doing things they're not supposed to – including starting new processes right in the memory, without ever manifesting as an application on the hard drive.

Exploit Prevention is a countermeasure generally associated with classic malware protection and it's among the most important security layers in modern cyber-defenses. If the option's available, and your ATM hardware can handle it, it's well worth running this technology.

… and opt for anti-malware, too

Low on processing power, memory and storage, ATMs struggle to support today's power-hungry endpoint security solutions. Regular endpoint protection isn't built with embedded devices in mind. Even with everything except application and device (if available) controls switched off, expect to see the software hanging, crashing or slowing the device almost to a halt.

What's needed is a purpose-built security solution lean enough to run comfortably on ATMs but ready to offer a multi-layered stack of protective layers which can then be fine-tuned to make the most of the device's available resources. If you're stuck with ancient ATMs offering the system-power of a modern calculator, opt for system hardening and self-protection. Got something better? Enable the features that work for you, ideally including anti-malware and exploit prevention designed specifically for embedded systems, to protect your devices against more sophisticated threats.

Running on Windows XP?

This can be a big problem. Nearly all vendors have now dropped this venerable – and vulnerable - Operating System from their support list. Kaspersky, however, has not, and is committed to supporting Windows XP for as long as is necessary.

Kaspersky Embedded Systems Security

ATM security is tricky because these machines are both similar to regular computers – and very different. They can be hit by regular malware, and they can also suffer from specialized attacks leveraging their unique weaknesses. The task of creating a solution that offers 'the best of both worlds' in terms of protection power and a light resource footprint is equally complicated. Fortunately, this IS possible – particularly if you have more than two decades of cybercrime fighting experience and a history of technological excellence to draw upon.

We've created Kaspersky Embedded Systems Security as a specialized solution based on our full understanding of the nuances of ATMs. It's extremely lean, even with all its security layers switched on - and an even leaner profile can be achieved through configuring the system's opt-in layers according to your specific needs. All the cybersecurity protection techniques mentioned above are available. And we continue to support obsolete OSs like Windows XP and Windows 7.

The solution fully supports low-maintenance modes of operation, allowing the equipment to run securely for months and years without direct administrator contact. And it's managed from the same console as other workstations, servers or virtual machines protected by Kaspersky technologies - either on-prem or cloud hosted, as preferred.

Your next steps….

Just how vulnerable are your ATMs?

Many aspects of overall ATM security - such as ensuring their physical security, thoroughly vetting maintenance engineers and third party suppliers, and restricting internal access to your ATM network - are beyond the scope of a cybersecurity solution.

But is the software guarding your ATMs doing its job effectively? If you're not 100% sure, it may be worth investing in a cybersecurity assessment service. You'll need to use one specifically geared to ATMs and payment systems – such as Kaspersky's Payment Systems Security Assessment Service.

Once you're ready to explore further options, you'll want to draw up a shortlist of potential solution providers. In addition to what you'd look for in any cybersecurity vendor, we advise that you home in on those who offer:

- Security software designed and built very specifically for ATMs – not just adapted from mainstream endpoint security products.
- Multi-level protection – not just a single mechanism such as system hardening controls or anti-malware, but a strong combination.
- Opt-in elements – so you can tailor your protection in line with device capabilities and available resources as well as threat considerations.
- A commitment to long-term professional support – particularly if you're running on Windows XP.

A world of expertise in Kaspersky Technologies

The effectiveness of Kaspersky products is regularly confirmed in independent tests worldwide. In 2020, we again headed the Top 3 rating of security solution manufacturers, taking first place in over 75% of all tests conducted. Undeniable proof that Kaspersky provides the industry's best protection. Over 400 million users are protected by Kaspersky technologies, and we help 270,000 corporate clients protect what matters most to them.

Find out more about what Kaspersky can offer you here!

Enterprise Cybersecurity: www.kaspersky.com/enterprise
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Kaspersky Technologies: kaspersky.com/technowiki

www.kaspersky.com