KASPERSKY lab

ATM AND POS SECURITY GUIDE

Achieving effective, efficient security for critical payment systems

www.kaspersky.com

CONCERNS

Embedded systems present specific security concerns. They are generally geographically scattered, they can be challenging to manage and they are rarely updated. Operating as they do with real money and credit card credentials, ATMs and Point of Sale devices are targets of choice for cybercriminals, so require the highest levels of focused, intelligent protection.

Obsolete software is a very common problem, and it's not just consumer operating systems that are affected. it's a well-known fact that some still-functioning space satellites are running on decades-old hardware and software. Industrial control systems, too, have a problem with very old operating systems and very long renewal cycles. The same is true for banking systems, and not just endpoints - internal automated banking systems often aren't updated for years. In terms of the ATMs themselves, 80% of smaller banks prefer to wait for the next end-of-cycle (which may take 5-10 years, or even more), then purchase new machines with fresh software already installed, rather than updating as new versions become available.

Windows XP families are still the most popular operating systems for ATMs and POS devices. The ending of support for this operating system has affected vast numbers of businesses and government bodies. The banking and retail sectors, where so many ATMs worldwide run on Windows XP Professional for Embedded Systems, have been particularly impacted. The fact is, though, that this system actually ceased to be supported back in April 2014, along with consumer versions of Windows XP.

The overall replacement of ATM and POS systems software is a long, expensive, and painful process. Besides which, replacing software often means also having to replace still-functional, if technically obsolete, hardware.

THE THREAT LANDSCAPE

ATMs, operating outside the bank's physical security perimeter and containing actual cash, and POS systems, capturing verified personal data and credit card details, are inevitably both high on the cyber-criminal's hit-list.

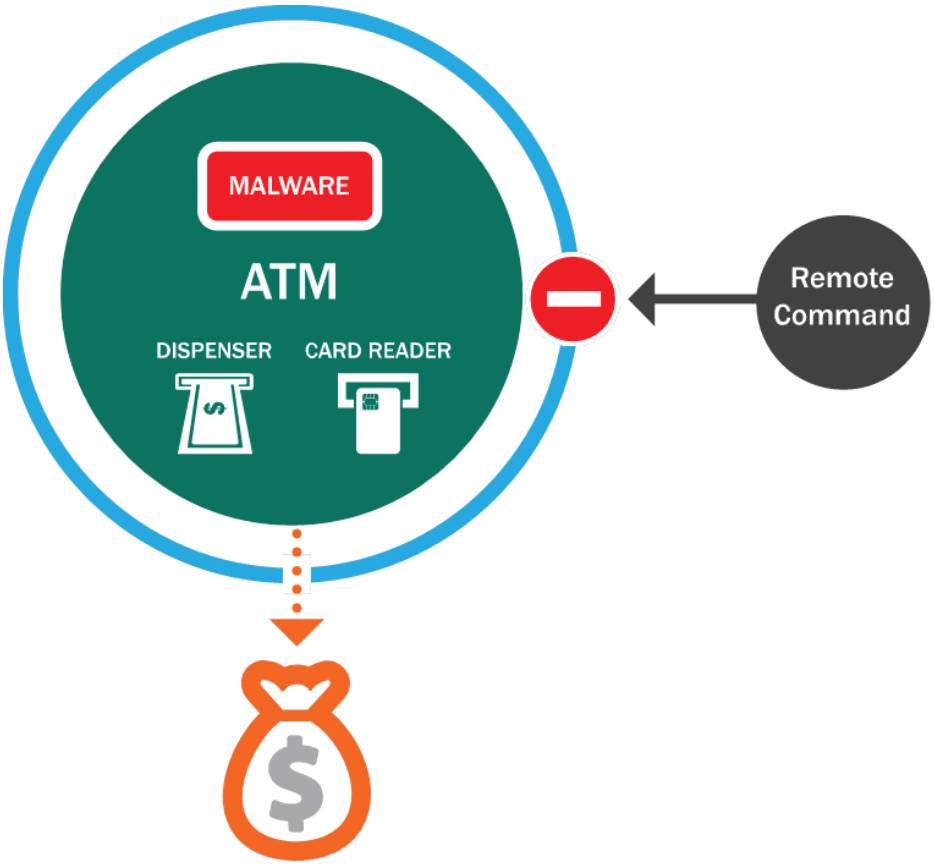
Since 2009, which saw the first serious attack on ATMs with the activities of Skimer malware, the quantity and quality of attacks has increased dramatically year on year. 2015 has seen attacks on ATM and POS systems reaching a new high, with malware including Ploutus, Tyupkin, Carbanak, CardStealer, vSkimmer, Chewbacca, POSeydon and FindPOS.

Conventional antivirus software cannot fully protect against all these threats, and the limitations of ATM and POS systems – weak channels, low-end hardware and obsolete software – make its installation and deployment challenging and often impractical. As a result, these viruses continue to succeed in penetrating the ATM and POS systems of major financial institutions and retailers on a daily basis.

Meanwhile, increasing volumes of highly targeted ATM and POS malware are being created by professional developers, themselves supported by the very latest and most powerful systems and hardware.

A simple ATM attack is a fast and easy way to obtain ready money. But ATM infections can also be part of a wider attack scenario. We have seen how Advanced Persistent Threat Attacks, like Carbanak in 2015, can result in financial losses totaling more than 1 Billion US Dollars worldwide.

ATM ATTACK SCHEME

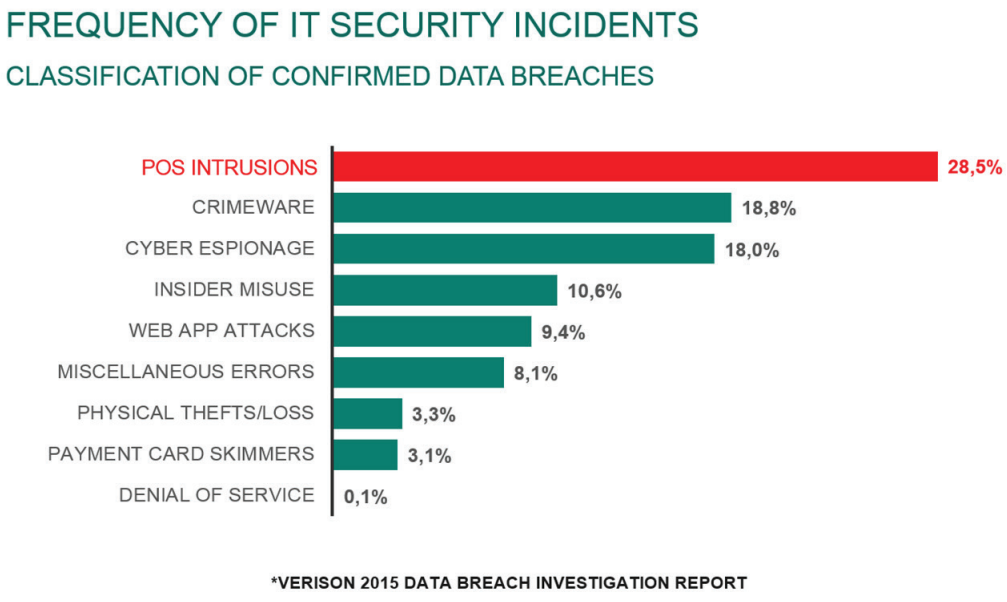


Geographically scattered ATM endpoints are ideal for the introduction of malware infections as part of a targeted attack, particularly as USB access ports and keyboards are conveniently located in a system servicing cabinet, secured only by a basic lock, at the back of the ATM itself.

In fact, even the lock may not be an issue. It's by no means unusual for local service engineers to install a semi-permanent USB or LAN/modem cable leading out of the ATM service cabinet, to avoid the bother of having to keep unlocking the door. Improving security by simply disabling USB ports or CD/DVD drives in the cabinet is not, alas, practical, as service engineers do need to use them regularly for machine maintenance.

Once malware has entered an ATM system through one machine, it may well hide there for some time, leaving the system to function normally while it acquires information and makes preparations. Then, when the time is right, a specific card or PIN may be used to trigger the change in system logic which results in each infected ATM dispensing its contents to the criminals on request.

POS BASED THREATS

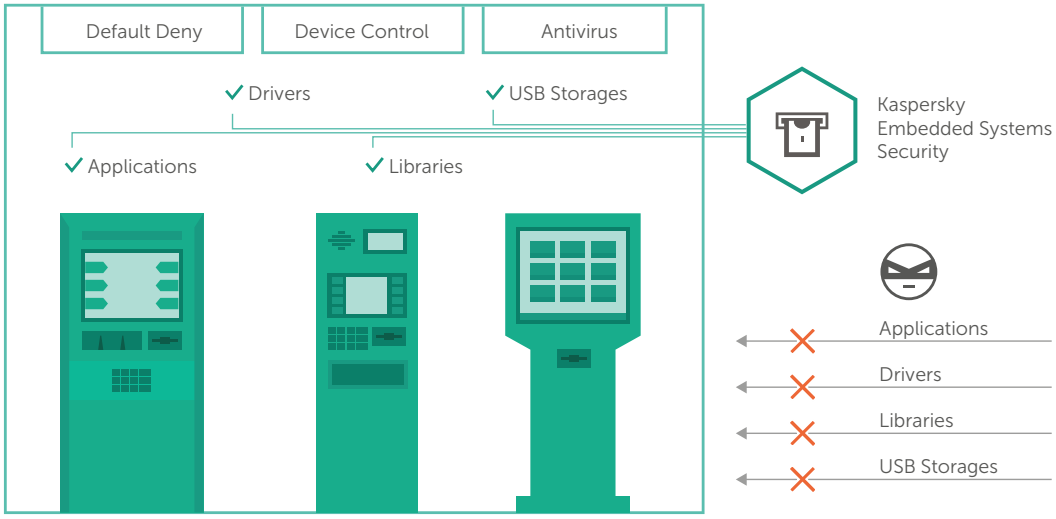


*VERISON 2015 DATA BREACH INVESTIGATION REPORT

A specific area of vulnerability for Point of Sale systems is the middleware they depend on. This middleware tends to be created by small third-party vendors or in-house. Functionality may well take precedence over security as a design consideration and, as with ATMs, easy access to USB ports and CD/DVD drives may be seen as a convenience, rather than a security weakness.

Most POS systems operate with credit/debit cards so are, like ATMs, subject to PCI DSS regulation. All without exception work with personal customer data, the protection of which is the responsibility of the POS systems owner. And all are connected to an intranet, making the POS a useful entry point for a Targeted Attack.

KASPERSKY EMBEDDED SYSTEMS SECURITY



Kaspersky Lab has created a security solution specifically for organizations operating ATM and POS systems and the threat environment they face, reflecting their unique functionality and OS, channel and hardware requirements, while fully supporting the Windows XP family.

Kaspersky Embedded Systems Security mitigates the security risks inherent in embedded systems. The solution has been designed specifically for ATM and POS systems, protecting the attack surfaces unique to these architectures while respecting related hardware and efficiency considerations. A single intuitive console gives the control and visibility you need to manage effective multi-layered security for your endpoints, your critical systems and your whole IT infrastructure.

Implementing Default Deny for Applications, Drivers and Libraries, boosted by Device Control functionality, is the only approach which can ensure the safety of technically 'obsolete' systems in continuing use.

Kaspersky Embedded Systems Security offers a 'Default Deny only' operational mode, with system requirements starting from 256Mb of RAM and 50Mb HDD space - ideal for Windows XP based systems running on low-end hardware. On-demand scanning is supplied through an optional Antivirus module powered by the Kaspersky Security Network, which also provides Patch Management facilities as required.

So this single solution meets three key objectives:

- Efficiently securing 'difficult to manage' systems
- Compliance with PCI DSS requirements 5.1, 5.1.1, 5.2, 5.3 and 6.2
- Enabling a soft timeline for obsolete systems and hardware replacement.

Default Deny

Most traditional antivirus solutions cannot fully defend against the advanced, targeted, malware threats the industry is currently facing. Default Deny functionality takes a different, more fundamental, approach. No executable files, drivers and libraries, other than software protection, are able to run on any ATM or POS endpoint without central approval from the Security Administrator.

Device Control

Device Control from Kaspersky Lab provides the ability to control USB storage devices trying to connect physically to systems hardware, preventing access to the ATM or POS unit by any unauthorized device. So these vulnerable systems entry-points, used regularly by cybercriminals as the first step in a malware attack, are blocked.

Windows XP – Windows 10 Ready

After 12 years, support for Windows XP Embedded ended on January 12, 2016 and for Windows Embedded for Point of Service on April 12, 2016. There will be no more security updates or technical support for the Windows XP operating system. Kaspersky Embedded Systems Security provides 100% support for the Windows XP family.

Designed for Embedded Systems Hardware

Kaspersky Embedded Systems Security is designed to be fully effective on the low-end systems which are a feature of most ATM and POS hardware. Requirements start from only 256Mb RAM for the Windows XP family, with around 50Mb space required on the system hard drive. When operating in 'on-demand' mode, the separately-installed antivirus module is designed to use hardware resources only during manual or scheduled scans.

Antivirus and Kaspersky Security Network

PCI DSS regulations specify that all systems interfacing with credit or debit cards must have antivirus installed and regularly updated. Kaspersky Embedded Systems Security delivers efficient antivirus protection, together with regular automatic or manual malware signature updates as required. As over half of all malware found in ATM and POS systems has entered through zero-day/zero-second exploits, Kaspersky Lab also recommends applying intelligent security in the form of the Kaspersky Security Network knowledge base, to prevent and mitigate exploit-based security risks and minimize reaction time.

PCI DSS COMPLIANCE

Kaspersky Security for Embedded Systems functionality meets and exceeds all security standards laid out in PCI DSS v3.1 sub-points:

5.1: Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).

5.1.1: Ensure that antivirus programs are capable of detecting, removing, and protecting against all known types of malicious software.

5.2: Ensure that all antivirus mechanisms are kept current, perform periodic scans, and generate audit logs which are retained per PCI DSS Requirement 10.7.

5.3: Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

6.2: Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

BEYOND ANTIVIRUS

The Payment Card Industry Data Security Standard (PCI DSS) regulates many technical requirements and settings for credit card data based systems. However, security regulations for ATMs and Point of Sale devices appear to cover only antivirus based security. As has been stated above, and has been amply demonstrated in recent attacks, a purely antivirus approach is of limited effectiveness against current ATP/POS threats. So now is the time to apply Device Control and Default Deny, already well-proven in other security contexts, to critical embedded systems.

To learn more about securing your critical payment systems endpoints more effectively, please contact the Kaspersky Lab Enterprise Sales Team.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab