Kaspersky® Embedded Systems Security

ATM and PoS Security Guide

Embedded systems are all around us, in devices as diverse as ticketing machines and kiosks to medical equipment, ATMs and PoS systems. These devices and the systems which run on them present very specific security concerns – they're usually geographically dispersed, can be challenging to manage and often run on out-of-date software. And in most cases, existing protection (if in place) is not sufficient against growing current and evolving embedded systems threats – they need specially designed, multi-layered, intelligent protection.

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.

Even the lock may not be an issue. It's not 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 inconvenience of having to keep unlocking the door.

Improving security by simply disabling USB ports or CD/DVD drives in the cabinet isn't practical, as service engineers need to use them regularly for machine maintenance.

Once malware has entered an ATM system through one machine, it can hide there for some time, leaving the system to function normally while it acquires information and makes preparations to cause havoc.

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.

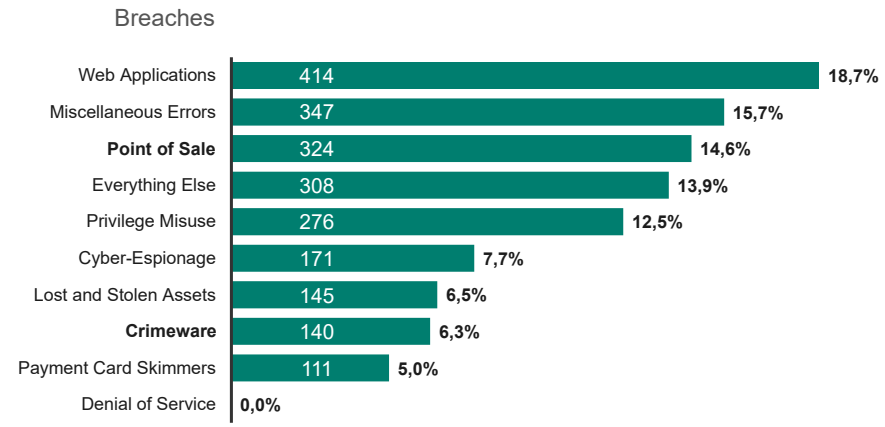
The Threat Landscape

ATMs and PoS systems are attractive targets for cybercriminals. ATMs have been under attack since at least 2008, when the first malicious program targeting ATM Backdoor.Win32.Skimer was discovered. The first incident of ATM malware-as-a-service took place in 2017, when cybercriminals packaged all the necessary malicious programs together with video instructions and released them onto the market for anyone wanting to gain access to ATMs. In the same year, Kaspersky Lab researchers uncovered attacks on ATM systems that involved new malware, remote and fileless operations.

In the first seven months of 2018 alone, malware directed at ATMs/PoS systems infected 57% more targets than in all of 2017. Experts predict that attacks via software designed specifically for financial organizations, including software for ATMs and PoS terminals, will continue to rise. PoS breaches are in the top 3 most popular breach patterns.

PoS-based threats

Percentage and count of breaches per pattern



Source: 2018 Verizon Data Breach Investigations Report

Cybercriminals attack embedded systems to steal cash, credit card credentials and personal data, and penetrate systems – malware-based attacks and operating systems, library or middleware modifications are all popular methods of gaining control over the entry device and then every device within the wider network.

ATM Security Specifics

- Most run on Windows XP which is no longer supported directly by Microsoft
- Easy-to-reach control panel
- Activated USB ports and CD/DVD drives
- Connectivity is essential for financial transactions
- Middleware legally obliged to be able operate with ATM hardware without confirmed transactions.

PoS Security Specifics

- Ransomware
- Key loggers
- Memory dumpers
- Network sniffers (can be installed on the POS, although this is rare)
- Verified personal data collection
- Typical entry point for advanced persistent threat attacks.

Unique Challenges

Obsolete software

This scenario is further exacerbated by some unique issues that exist when it comes to ATMs and PoS systems. The majority of banks wait for their ATMs to reach end-of-cycle before upgrading them. Replacement cycles often run to 10 years – and usually involve replacing the entire machine (complete with new software) rather than updating their existing software regularly when new versions become available. In addition to the newest embedded systems threats, old ATM and PoS malware, some originating as far back as 2009, remain active today.

Windows XP is still the most popular OS for ATMs and PoS devices. Even though support for XP officially ended in 2014, most ATMs today still run on Windows XP Professional for Embedded Systems.

Convenience over security?

A specific area of vulnerability for PoS systems is the middleware they depend on. This middleware tends to be created by 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.

Location and device specifics

Another issue to take into account is the physical location of ATMs and PoS systems and how they're used – they're invariably in public spaces, and each device is accessed by thousands of different users. They're also usually serviced by third parties.

In this unique and challenging environment, a one-technology approach – just antivirus or Default Deny only – is not effective, and does not provide the sufficient protection. In addition, 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 threats continue to penetrate the ATM and PoS systems of financial institutions and retailers around the world every day.

Only multi-layered protection that has been specifically designed to address these unique challenges can protect ATMs and PoS systems reliably and successfully.

Protection against the latest threats

Kaspersky Embedded Systems Security delivers multiple layers of essential security technologies (including system control, antimalware and network protection) to protect ATM and PoS systems from the latest threats.

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.

Windows XP and later

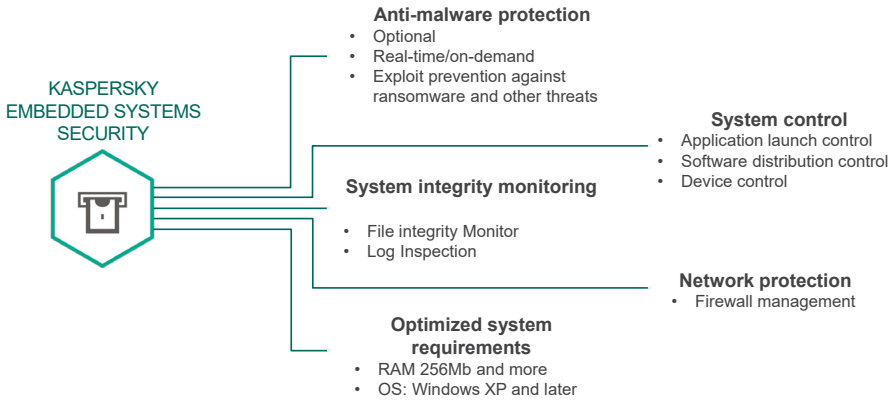
Microsoft ended support for Windows XP Embedded on January 12, 2016 and for Windows Embedded for Point of Service on April 12, 2016. Kaspersky Embedded Systems Security provides 100% support for the full Windows range, from Windows XP to the latest Windows 10.

PCI DSS Compliance

Kaspersky Security for Embedded Systems functionality meets PCI DSS v3.2 sub-points: 1.4, 2.4a, 5.1, 5.1.1, 5.2, 5.3, 6.2, 10.5.5, 11.5.

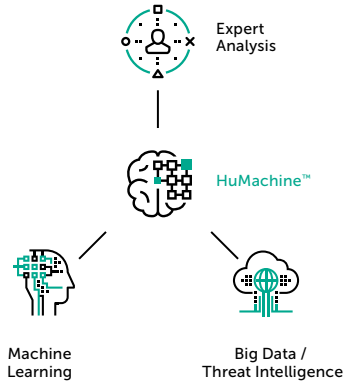
Kaspersky Embedded Systems Security

Kaspersky Lab Embedded Systems Security has been specifically designed for organizations operating ATM and PoS systems and the threat environment they operate in. It protects the attack surfaces unique to these architectures, reflecting their unique functionality and OS, channel and hardware requirements, while fully supporting the Windows XP family. A single intuitive console gives the control and visibility you need to centrally manage effective multi-layered security for your endpoints, your critical systems and your entire IT infrastructure.



Kaspersky Embedded Systems Security efficiently secures 'difficult to manage' systems like ATMs and PoS systems, is fully compliant with the relevant PCI DSS requirements and enables a 'soft' timeline for obsolete systems and hardware replacement.

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



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

#truecybersecurity
#HuMachine

www.kaspersky.com