KASPERSKY lab

ATM 和 POS 机安全指南

为关键支付系统提供可靠高效的安全保护

www.kaspersky.com.cn

安全隐患

地理分布广、难以管理以及很少更新等特点，使嵌入系统存在着特定的安全隐患。用于处理现金和信用卡交易凭证的自动取款机（ATM）和 POS 机已成为网络罪犯的首选攻击目标，因此这些设备需要最高级别的专业保护。

过时的软件作为一大常见问题，不仅仅影响个人用户操作系统。众所周知，一些仍然在运作的空间卫星，其硬件和软件已运行了数十年之久。工业控制系统存在着诸多问题，比如非常陈旧的操作系统和较长的更新周期。银行系统更是如此，而且不仅仅是端点，其内部自助银行系统也长年未更新。就 ATM 机本身而言，80%的小银行宁愿等待下一周期结束（这可能需要5至10年，甚至更长时间）购买已安装新软件的机器，而非更新可用的新版本。

Windows XP 系列对于 ATM 和 POS 设备而言仍然是最流行的操作系统。不再支持该操作系统已影响到大量的企业和政府机构。在全球范围内的银行和零售业中，很多 ATM 嵌入式系统均在 Windows XP Professional 上运行，所以尤其受到影响。实际上，该系统以及 Windows XP 个人用户版本早已于2014年4月就停止支持。

但是 ATM 和 POS 系统软件的整体更换不仅耗时较长，而且花费不菲。此外，更换软件往往意味着必须更换仍可运行但技术过时的硬件。

威胁概况

银行周边含有现金的 ATM 机以及获取真实个人数据和信用卡详细信息的 POS 系统，都不可避免地沦为网络犯罪的攻击目标。

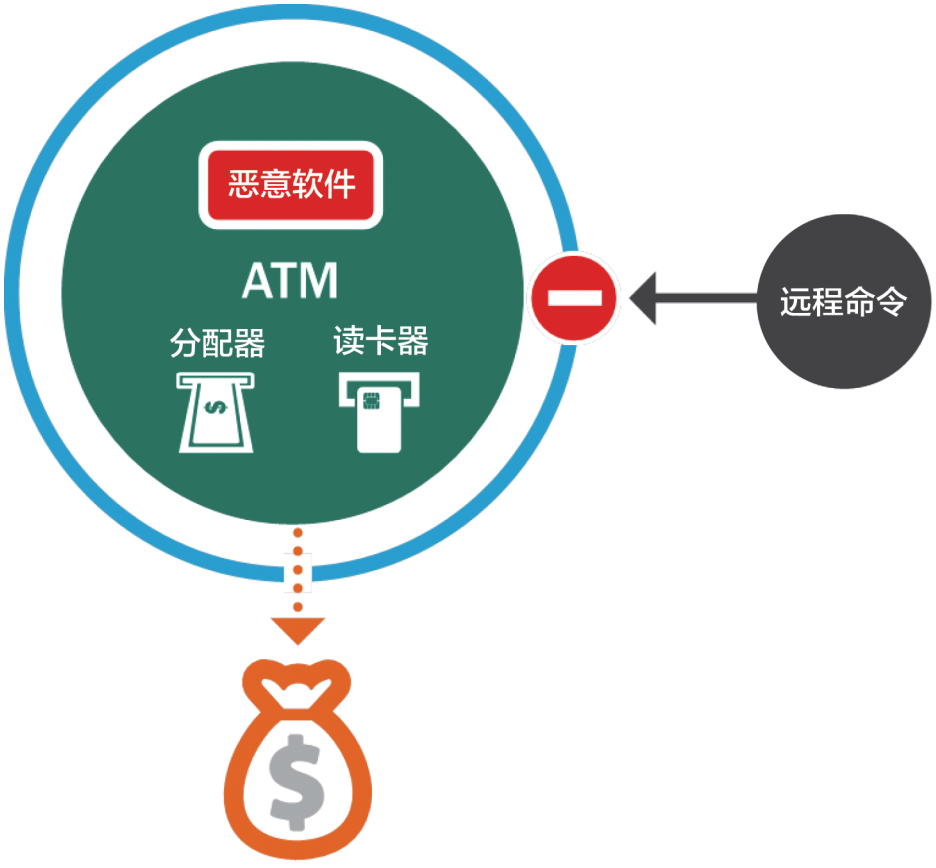
2009年出现了首例针对 ATM 机的 Skimer 恶意软件活动，此后攻击的数量和质量同比出现大幅增加。2015年利用恶意软件对 ATM 和 POS 系统实施的攻击数量已创新高，其中恶意软件包括 Ploutus、Tyupkin、Carbanak、CardStealer、vSkimmer、Chewbacca、POSeydon 和 FindPOS。

传统的反病毒软件无法抵御上述网络威胁。此外，ATM 和 POS 系统的局限性 （信道较弱、硬件低端和软件过时） 也使安装和部署反病毒软件不仅具有挑战性，并且非常不实用。其结果是，大型金融机构和零售商的 ATM 和 POS 系统频频遭受攻击。

与此同时，网络罪犯正在创建越来越多针对 ATM 和 POS 机的恶意软件。这些软件本身支持最新和最强大的系统和硬件。

网络罪犯只需实施一次 ATM 攻击即可快速获得大量现金。然而，ATM 感染不过是各类支付系统攻击中的冰山一角。事实证明，高级可持续性威胁（如2015年的Carbanak）在全球范围内造成超过10亿美元的经济损失。

ATM攻击



作为针对性攻击的一部分，恶意软件能够轻而易举地感染随处可见的 ATM 机，因为位于系统维护柜中的 USB 访问端口和键盘仅由机身背面的普通锁保障其安全，为网络罪犯提供可乘之机。

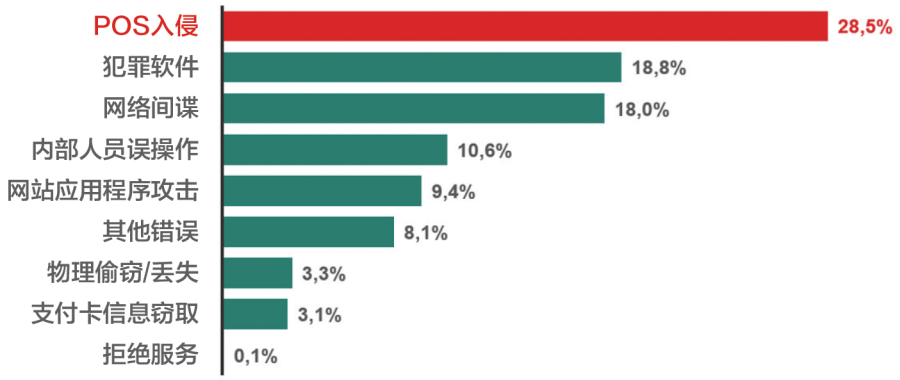
事实上，安全锁并非问题的关键。本地服务工程师常常会安装一种连接至 ATM 服务柜的半永久性 USB 或 LAN/调制解调器电缆，从而使柜门保持开启状态。然而，仅仅通过禁用机柜中的 USB 端口或CD/DVD驱动器，提高安全性并不可行，因为服务工程师确实需要定期使用 USB 端口或CD/DVD驱动器进行机器维护。

一旦恶意软件通过一台机器进入 ATM 系统，很可能先会隐藏一段时间。此时系统保持正常运行，而恶意软件却在获取信息和做准备。然后，当时机成熟时，网络罪犯会使用特定的卡或 PIN 更改系统逻辑，使每台受感染的 ATM 机按要求将内容发送给向网络罪犯。

基于POS的威胁

IT安全事故的发生频率

数据泄露类型

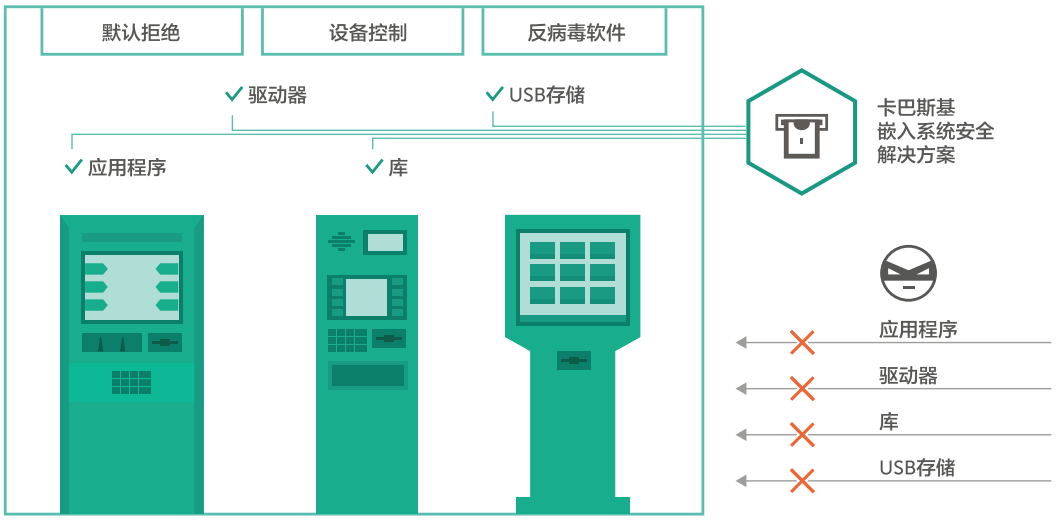


*VERISON 2015数据泄露调查报告

POS 系统的薄弱点在于它所依赖的中间软件。中间软件往往是由小型第三方供应商创建或内部创建。在设计考虑因素中，功能性往往优先于安全性。并且对于 ATM 而言，易于访问 USB 端口和 CD/DVD 驱动器被视为一种便利，而非安全漏洞。

大多数处理信用卡/借记卡的 POS 系统如 ATM 机一样需要遵守 PCI DSS 法规。因此，POS 系统持有者理应对客户数据的安全性责任。此外，由于 POS 系统需要连接至一个内部网络中，使其易于沦为针对性攻击的切入点。

卡巴斯基
嵌入系统安全解决方案



卡巴斯基嵌入系统安全解决方案专为使用 ATM 机和 POS 系统的机构及其面临的安全挑战而打造，具有专门的功能和特殊的 OS、信道和硬件要求，同时全面支持 Windows XP 系列系统。

该解决方案可降低嵌入式系统中特有的安全风险，充分满足 ATM 和 POS 系统的安全需求，在兼顾硬件和性能等因素的同时，保护这些架构免遭网络攻击。卡巴斯基嵌入系统安全解决方案不仅提供有效的多层次安全保护，通过直观简洁的统一控制台，用户还可以轻松洞察、管理与保护终端、关键系统和全部 IT 基础设施。

此外，通过增强的设备控制功能，用户可为应用程序、驱动程序和库实施默认拒绝，从而确保 ATM 机和 POS 等使用 “过时”系统的持续安全性。

卡巴斯基嵌入系统安全解决方案提供了“仅默认拒绝”操作模式，仅占用256Mb RAM 和50Mb HDD 的系统空间 – 适用于在低端硬件上运行的基于 Windows XP 的系统。该解决方案可通过基于卡巴斯基安全网络的可选反病毒模块进行按需扫描，还可以按照要求提供补丁管理功能。

因此，卡巴斯基嵌入系统安全解决方案能够满足三大主要目标：

- 高效保障“难以管理”的支付系统的安全；
- 符合 PCI DSS 规定中5.1、5.1.1、5.2、5.3和6.2的要求；
- 针对过时系统和硬件更换启用软时间表。

默认拒绝

多数传统的反病毒解决方案并不能保护支付系统免遭高级针对性恶意软件威胁。默认拒绝功能则采用一种更为重要的安全方法。未经安全管理员批准，可执行文件、驱动程序和库（不包括软件保护）将无法在任何 ATM 或 POS 终端上运行。

设备控制

卡巴斯基实验室的设备控制功能可控制试图连接至系统硬件的 USB 存储设备，以阻止网络罪犯通过任何未经授权的设备访问 ATM 或 POS 机。这样就封锁了恶意软件入侵 ATM 或 POS 机的入口——这是网络罪犯使用恶意软件攻击时惯用的第一步。

全面支持Windows XP - Windows 10系统

在 Windows XP 嵌入系统运行12年后，微软公司于2016年1月12日停止该系统的支持服务，并于2016年4月12日起不再对 Windows 嵌入式 POS 系统提供支持服务。这表明微软将不再为 Windows XP 操作系统提供任何安全更新或技术支持。卡巴斯基嵌入系统安全解决方案可为 Windows XP 系列系统提供100%支持。

专为嵌入式系统硬件

卡巴斯基嵌入系统安全解决方案能够在低端系统上高效运行，而多数 ATM 和 POS 机硬件均采用低端系统。该方案仅占用 Windows XP 系列系统中 256Mb 的内存容量，在"按需模式"操作时只需约 50Mb 的系统硬盘空间，反病毒模块仅在手动或定期反病毒扫描时才使用硬件资源。

反病毒软件和卡巴斯基安全网络

《支付卡行业数据安全标准》规定，与信用卡或借记卡连接的所有系统必须安装反病毒软件并定期更新。卡巴斯基嵌入系统安全解决方案能够提供有效的反病毒保护，并定期自动更新或按要求手动更新恶意软件特征码。由于超过半数恶意软件都通过零日/零时漏洞入侵 ATM 和 POS 系统中，卡巴斯基实验室建议企业使用卡巴斯基安全网络知识库，运用安全情报预防和减轻基于漏洞的安全风险，并减少响应时间。

符合PCI DSS

卡巴斯基嵌入系统安全解决方案的功能完全符合 PCI DSS v 3.1 中列出的所有安全标准，并且超过该标准的要求：

5.1: 在可能遭受恶意软件影响的所有系统上部署反病毒软件（特别是个人电脑和服务器）。

5.1.1: 确保反病毒软件能够检测、清除和防止所有已知类型的恶意软件。

5.2: 确保所有反病毒机制保持最新状态，定期进行扫描，生成审计日志。并按照 PCI DSS 要求10.7保留审计日志。

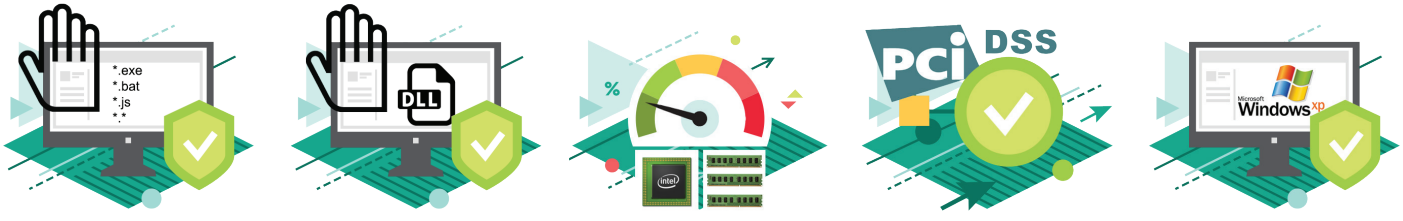
5.3: 除管理层在特定时间内逐一进行特殊授权的情况外，应确保反病毒机制正在运行，并且不能由用户禁用或改变。

6.2: 确保所有系统组件和软件均可通过安装供应商提供的相应安全补丁防止已知漏洞。关键安全补丁须在其发布后一个月内安装完毕。

仅靠反病毒保护并不能保障安全

《支付卡行业数据安全标准（PCI DSS）》对信用卡数据系统的技术要求和设置做出了许多规定。然而，ATM 和 POS 机的安全标准却只涉及反病毒保护。近期发生的多起攻击事件已充分证明，纯粹的反病毒技术并不足以应对当前的 ATM/POS 机威胁。现在，是时候使用设备控制和默认拒绝等应用于其他安全系统环境中的成熟技术，保护企业重要的嵌入系统。

请联系卡巴斯基实验室的企业销售团队，获取有关保护 ATM 和 POS 端点的更多信息。



卡巴斯基实验室：
www.kaspersky.com.cn

关于互联网安全的所有事项：
www.securelist.com

寻找您附近的合作伙伴：
www.kaspersky.com/buyoffline

KASPERSKY lab