AhnLab

安全月刊

Vol. 29

POS 系统面临的安全威胁及
AhnLab EPS

POS系统面临的安全威胁及AhnLab EPS

黑客的枪口瞄准POS系统

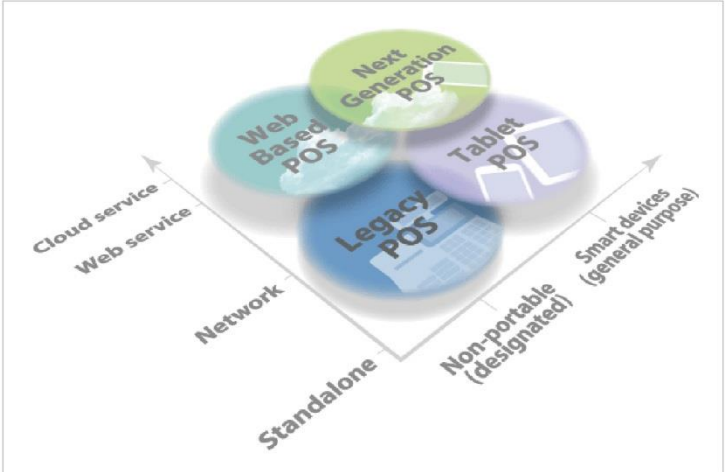
2013年末，美国发生了大型折扣零售商 Target 公司的POS系统被黑客攻击事件，其攻击规模和损失金额之大震惊了全世界。被人们普遍认识为只是付款系统而已的POS机成为了黑客攻击的对象，并且发生了庞大的金钱损失。其实早在2009年就已发现了首次的POS机恶意软件“Tracker”。安全专家们也曾警告过POS系统存在的安全威胁。当时，“安全”这个问题并没有引起人们的广泛注意。直到 Target 公司的POS系统被攻击事件发生以后，世界各国陆续发生黑客攻击百货店、饭店等的POS系统，盗取信用卡信息的事件，POS系统的安全问题才开始受到关注。2014年，来自POS恶意软件的威胁急剧性地增长，可以说是零售商数据泄漏之年。但是，目前符合POS系统环境的安全体系和安全解决方案很不足。
本刊曾经已介绍过几次POS系统的恶意软件。本期将着重介绍POS系统本身的特殊性和其安全漏洞。然后，详细介绍 AhnLab 推出的POS系统专用安全解决方案-AhnLab EPS。

为什么黑客瞄准POS系统

AhnLab 在今年发表的“2015年安全威胁趋势报告”中，预测了今年瞄准POS系统的安全威胁将进一步加深。根据报告，今年POS系统的恶意软件还会继续增加，并且会出现多种的攻击方式。而且，攻击对象不仅是POS机，POS机制作商也会成为黑客攻击的对象。

在正式谈论POS系统存在的安全威胁之前，先简单了解一下：POS系统是什么？为什么黑客瞄准POS系统？

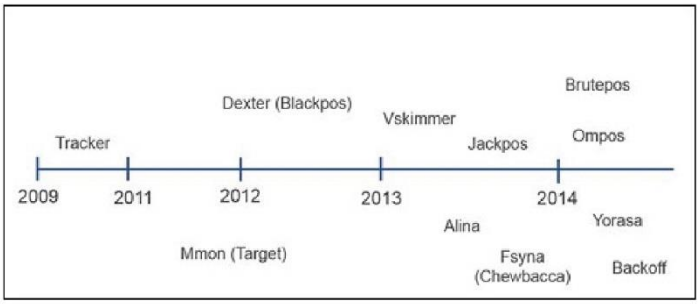
POS(Point of Sales)系统，即销售时点信息系统，是指通过自动读取设备（如收银机）在销售商品时直接读取商品销售信息（如商品名、单价、销售数量、销售时间、销售店铺、购买顾客等），并通过通讯网络和计算机系统传送至有关部门进行分析加工以提高经营效率的系统。POS系统在商品管理中担任非常重要的作用，通过POS系统不仅可以结算货款，还可以实时掌握销售趋势、管理库存等。还有些POS机用于积分管理和会员管理等客户管理。尤其，最近有些POS机提供商通过结合POS系统里的客户信息和客户的智能手机位置信息，提供有用的信息以改善客户方便和提高客户忠诚度。预计该领域今后将联动云计算持续发展。



【图 1】POS系统的运营方式 *来源：epson-biz.com

如此，POS机的利用率越来越高并且掌管重要的信息。相比之下，POS系统的安全对策却非常欠妥。大部分的POS系统在内存空间在256MB~1GB之间的低配置的 Windows 操作系统下运行，其中还有 Windows XP。因此，别说是防病毒软件，就连 Windows 更新也无法正常进行。另外，POS机除了用在原先的使用目的以外，还用在连接互联网等，这就容易成为黑客的攻击对象。

总而言之，黑客瞄准POS系统的理由很明确。POS系统存在安全漏洞，并存有大量的重要信息。



【图 2】2009年~2014年发现的主要POS系统恶意软件

POS系统面临的安全威胁和目前响应方案的局限性

通过多种网络连接渠道的安全威胁

大部分的大型折扣零售商的POS系统和网络可能会使用专用线。但是为了联动客户信息和积分信息等客户管理信息，需要与其他网络连接。中小规模的企业或零售商店通过公用网络(Public Network)或蜂窝网络(Cellular Network)连接POS机，或使用基于软件即服务(Software as a Service, SaaS)的云计算的POS系统。如此的网络状态下，不可避免地存在安全漏洞。尤其与无线网络连接的时候，通过网络入侵的可能性更高。

使用服务结束的操作系统

目前大部分的POS系统还在使用服务已结束的微软公司的 Windosw XP 及基于 XP 的 Windows Embedded for Point of Service 和 Windows Embedded POSReady 2009。Windows XP 操作系统在2001年上市，存在诸多的漏洞。加上已经是服务结束的操作系统，不再提供安全补丁等安全更新，这使大多数还在使用该操作系统的POS机面临了重大的危险。

应用程序漏洞

POS系统为了管理和方便而安装一些应用程序，如“远程控制程序”、“IE”、“Adobe Reader”和“Microsoft Office”等。这使得POS机也同一般的PC一样存在相同的应用程序漏洞。黑客便利用“IE”、“PDF”、“DOC”等文档和JAVA漏洞来攻击POS系统。

通过互联网和U盘等移动设备感染

互联网的使用是POS系统感染恶意代码的主原因。除了网上冲浪，随着社交网络的发展，有时还需要访问社交网络。此时，如果该社交网络被黑客攻击，POS系统也有可能被恶意软件感染。另外，POS机与一般的PC相同，可以连接U盘等移动设备。为了库存管理等，实际将U盘连接POS机的情况较多，恶意代码便通过U盘入侵到POS系统。

如上述，POS系统存在诸多漏洞，已面临着社会工程学攻击等多种威胁。但是除了使用防病毒软件和数据加密及加密通信之外没有更好的对策。被恶意软件控制的POS系统，加密及加密的通信已没有意义。再加上低配置的POS系统和有限的网速，即使安装了防病毒软件，但是无法及时更新特征码。因此，基于特征码的防病毒软件也对恶意软件也没有很大效果。

POS系统需要与一般PC不同的安全策略

黑客攻击POS系统不仅盗取信用卡\现金卡信息，还盗取客户信息、积分和会员卡信息。黑客将盗取的信用卡复制后利用在2次犯罪。如此，POS系统保存的是信用卡号等顾客敏感信息，并且泄漏的信息直接联系到金钱损失，更加需要强有力且多角度的安全对策。

首先，POS系统需要设置安全的登录密码，并定期进行更换。然后，最好不要使用“VNC”、“Remote Desktop”等远程控制程序。

最后，POS系统除了它原来的用途以外，不要以其他目的使用。除了POS系统所需的程序之外，禁止使用其他的程序。特别注意，要防止使用互联网，因为通过互联网感染恶意代码的可能性很高。除了POS系统结算所需的网络连接外，不要使用公用网络或无线网络等。不得已连接互联网的时候，启用防火墙并只允许所需的连接。

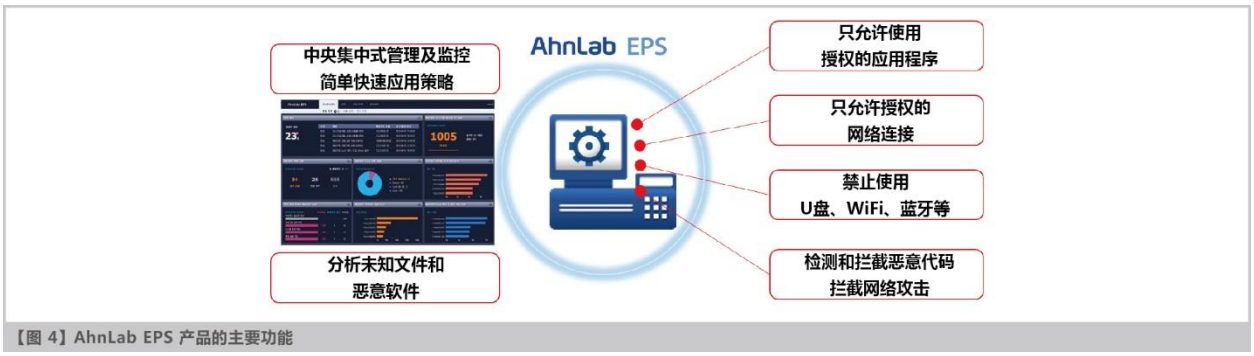
最重要的是，拦截恶意软件的流入和运行，使攻击无法开始。这就需要除了做好基本的措施以外，最好是安装POS系统专用的安全程序来保护POS系统。因为POS系统在低配置的计算机运行，所以引进基于白名单的只运行授权程序且超轻型的安全解决方案是最佳的选择。

谈到POS系统专用安全解决方案，可能会有人想到应用程序控制产品。但是，该产品需要管理员专门知识和高级的应用程序控制策略管理。又由于不是安全产品，因此无法检测恶意软件入侵和感染与否，最终还得靠安全专家来管理。

【图 3】办公用电脑和POS机的系统环境比较

POS系统专用安全解决方案，AhnLab EPS

AhnLab EPS(Endpoint Protection System)是一款针对要求系统稳定性高、使用明确而有限的应用程序的，适用于诸如社会基础设施、大规模自动化设备的工厂、POS 机等工业系统的最优化安全解决方案。AhnLab EPS 采用白名单技术，系统只能使用授权的程序，既能防止病毒和恶意代码入侵，又能抑制恶意代码活动并防止信息丢失。



【图 4】AhnLab EPS 产品的主要功能

AhnLab EPS 的主要功能如下：

√ 强有力的恶意软件检测及防止扩散
- 通过服务器上的TS引擎来检测和修复恶意软件
- 通过拦截IP/端口和阻止U盘等移动设备自动运行，防止恶意软件感染
- 即使没有安装OS补丁和更新产品，也可确保系统安全

√ 非业务行为控制及可移动设备控制
- 只允许使用授权的应用程序，阻止非业务行为
- 通过阻止使用可移动设备，防止信息泄漏

√ 超轻量级安全及控制解决方案
- Agent 的内存和CPU的占有率小
- 不需要定期进行更新
- 所有消耗系统资源的任务都在另外的服务器执行

√ 中央集中式端点安全管理系统

- 通过仪表板，可以随时查看所有系统状态
- 通过 Agent 分组功能，简单快速应用策略
- 通过搜索未安装 Agent 计算机和远程控制，迅速方便检查系统
- 提供重要事件通知及日志综合管理

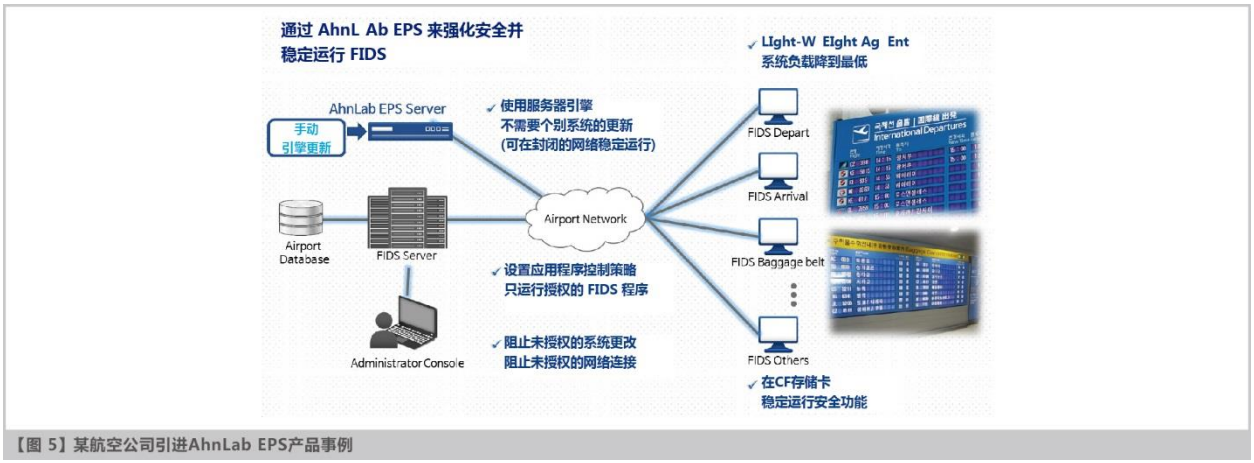
AhnLab EPS 的高级的白名单方式的应用程序控制功能无需专门的安全知识便可以操作和运营，并通过中央统一管理减少了加盟店的运营负担。

为了区分客户端系统上合符需要和不合符需要的文件，当启动服务器与客户端之间的通信时，系统将会检查每个文件的完整性。AhnLab EPS 将其功能强大的反病毒引擎放置在中央服务器上，这样 IT 管理员就无需更新和维护每个端点上的特征码。尤其，几乎不占有系统本身的资源可以对系统生成的所有可执行文件进行实时检查和分析。由此来响应POS终端设备的恶意软件，还可以对未知的安全威胁进行分析。如果引进 AhnLab EPS 产品，就不需要另外的反病毒解决方案。

AhnLab EPS 通过“应用程序控制”、“Agent系统控制”、“移动设备控制”和“网络连接控制”等技术，从外部的威胁和未知的安全威胁中保护POS系统，使POS系统维持安全的状态。还通过服务器提供的恶意软件检测及分析功能和安全策略管理，维持所有系统文件的安全性。

“DAISO”和“新世界”等韩国大型折扣零售商的POS系统已引进了AhnLab EPS，其性能和安全性也得到了验证。除了POS系统，AhnLab EPS 可以应用在半导体、家电生产线、工业控制系统、自助服务机(KIOSK)、ATM机等多样的领域。

下面简单介绍一下应用 AhnLab EPS 的韩国的某个航空公司的事例。该航空公司的 FIDS 共有1800多台，并在没有硬盘的低配置的终端机安装了 Windows XP Embedded 操作系统。除了普遍使用的防病毒软件，没有另外的安全对策。由于防病毒软件系统占有率较高，还需要持续更新，对系统存在负担。通过安全软件的安全响应已面临局限。为了解决这些问题，该航空公司引进 AhnLab EPS 来代替防病毒软件，构筑了可以稳定运行 FIDS 的安全体系。



【图 5】某航空公司引进AhnLab EPS产品事例

如此，AhnLab EPS 是专用于特殊目的系统的安全解决方案，不影响系统资源和相关业务进程，可以预先阻止恶意软件，最终达到防止信息泄漏、提供生产率和节俭管理和运营费用等效果。

http:// cn.ahnlab.com

http://global.ahnlab.com

http://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。

AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室

电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | sales@ahn.com.cn