AhnLab

安全月刊

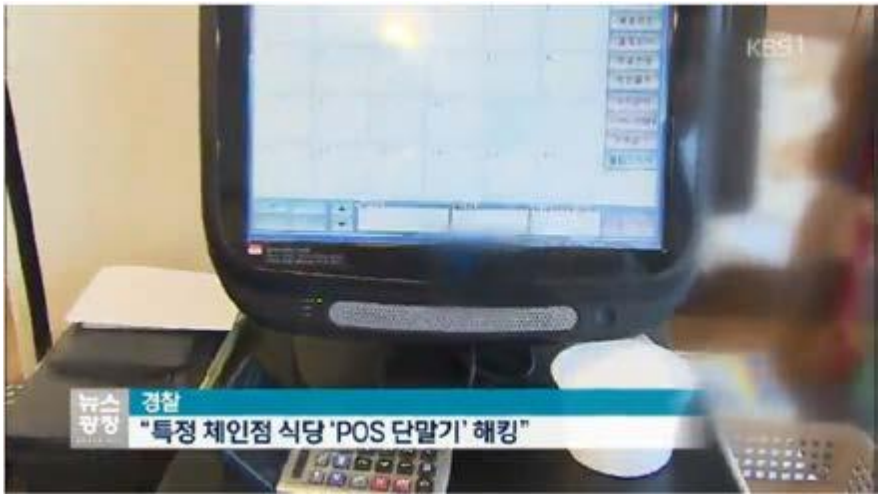
2015.09 Vol. 35

POS 威胁和 AhnLab EPS

曾一度减缓的 POS 威胁，寻隙而入

我的信用卡在我不知晓的情况下被刷200万？！
被刷卡的地方我根本就没去过，而且我的信用卡没有借给他人，也没有丢失过。这到底是怎么回事？
据警方了解，是公司附近的一家餐厅的 POS 被黑客攻击，而我的信用卡也是在那里刷卡时被复制。不只我一个人的信用卡被复制，利用该餐厅的其他人的信用卡也有被复制。
POS 威胁和信用卡被复制只是听说过而已，万万没有想到我竟然成为其受害者！

上一段内容不是故事或电视剧，而是实际发生的案件。就在今年7月初，韩国仁川市陆续发生了信用卡在用户不知晓的情况下被狂刷巨额的事件。受害者表示，本人从来没有丢失过信用卡，也没有借给过他人。据信用卡公司和警方调查，受害者中的一些人曾经去过同一个餐厅并有刷卡记录。由此可以判断，黑客攻击该餐厅的 POS 机并盗取信用卡信息。自2013年末发生大规模 POS 系统被攻击导致大量信用卡信誉被泄漏事件以后，曾一度减缓的 POS 威胁，今年再次活跃起来。最近，在国外也陆续发现针对 POS 系统的新种恶意软件，呈现出针对 POS 系统的攻击将重新加剧。



【图 1】韩国媒体报道 POS 机被黑客攻击事件(来源：韩国电视台 KBS 信息广场，2015年7月)

加快脚步树立POS安全策略，但其效果呢？

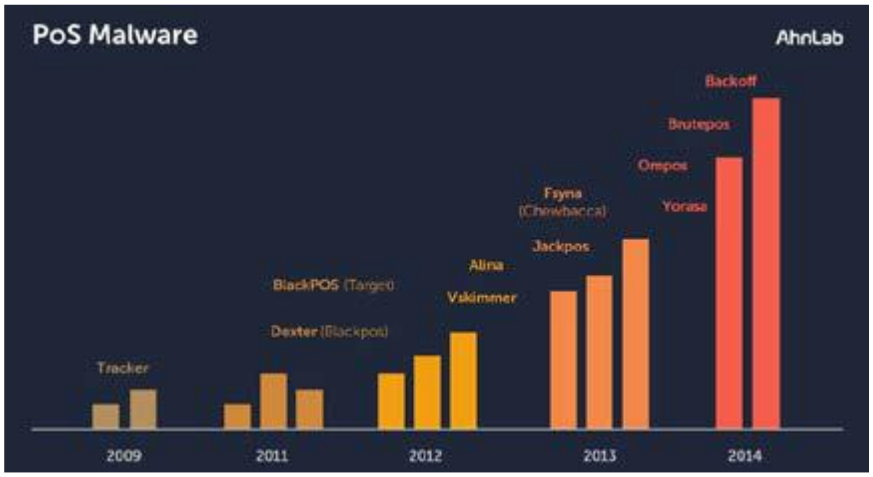
金融监督院和“信用卡结算终端机 IC 转换行动小组(TF)”在今年7月1日发表了“POS 终端机安全标准规格”。该 POS 终端机安全标准从今年3月开始经过了4个月的讨论，主要考虑以下两个方面：▲ 当 POS 终端机面临物理攻击时，终端机内存自动被破坏 ▲ 采用端对端(End-to-End)方式的全部加密，以防止信息泄漏

金融监督院同时与信贷金融协会一起修订《信贷专门金融业法(以下简称为“信专法”)》，制订了信用卡结算代办企业(Value Added Network, 以下简称为“VAN”)登记制度。根据该制度，从今年7月21日开始，新加盟店欲安装 POS 终端机时必须遵从安全标准制作并还需要通过认证，才可以安装并使用。如果违反此项，VAN 和加盟店各罚款5千万（韩元）。但，对于现有加盟店的 POS 终端机给予3年的宽限期，引导替换为新的终端机。但是，如果现有加盟店的 POS 终端机发生故障时，必须无条件替换为新的终端机。问题是，替换新的终端机的费用不菲，这对小本经营的加盟店不是件容易的事情。另外， IC 终端机转换项目指定发展商 VAN 企业中，两家的终端机还未通过认证，新的终端机产品量无法满足市场需求。

前面所提及的利用 POS 终端机复制信用卡事件，刚好发生在金融监督院发表 POS 终端机安全标准以后。这也是对金融当局制定的防止信用卡复制及 POS 攻击事件对应策略的有效性心存怀疑的原因。加上，陆续发现了更加进化的 POS 恶意软件，可见 POS 安全威胁眼下不会那么容易解决。

POS 威胁，恶意软件的进化？还是先天的威胁？

POS 恶意软件受到全世界注目的转折点是2013年12月在美国发生的大型折扣零售商 Target 公司的 POS 系统被黑客攻击事件。黑客利用了被称为 BlackPOS 的恶意软件，约有4千万个信用卡信息被盗，7千万人受到了损失。2014年7月出现了感染 POS 系统后盗取客户姓名、地址和信用卡号等信息的恶意软件，该恶意软件被称为 Backoff。主要传播在北美地区，具有收集内存的追踪数据和键盘记录功能，还被确认存在多种变种。今年发现的 POS 恶意软件有“PoSeidon”和“MalumPOS”等。“PoSeidon”发现在今年3月份，它是由利用在攻击Target 公司 POS 系统的恶意软件 BlackPOS 和 典型的网上银行恶意软件 Zeus 的功能结合形式的恶意软件。PoSeidon 不仅找出 POS 系统内存领域保存的信用卡信息，而且还可以检查信用卡号的有效性，即使重启系统，它还是原样留在系统中。



【图 2】主要的 POS 恶意软件趋势(2009年~2014年)

MalumPOS 出现在今年6月，在 Oracle 的 POS 系统的操作平台“MICROS”中盗取客户姓名和信用卡号。MICROS 在全世界有33万客户，潜在的威胁令人担忧。

POS 恶意软件在韩国也是频频被发现。典型的有去年初发现的被称为“Ompos”的恶意软件。黑客利用该恶意软件首先攻击 POS 系统管理企业的服务器，然后再感染 POS 系统并盗取信用卡信息。不仅是恶意软件，POS 系统本身的特殊性也是重要的威胁因素之一。POS 系统先天的威胁因素有▲ 多样的网络连接 ▲ 不合规的 POS 终端机的使用 ▲ 应用程序漏洞等。大部分的 POS 系统使用一般的商用互联网，而不是封闭式网络。有些大型的折扣零售商的 POS 系统和结算核对网络可能会使用专用线，但是中小规模的企业和零售商店大部分使用商用网络来运营 POS 系统。另外，最近有些零售商为了联动客户信息、积分信息和客户智能手机的位置信息等客户管理信息，需要连接其他网络。而在这种网络环境下，不可避免地存在安全漏洞。尤其是利用无线网络，那么通过无线网入侵的可能性就越高。

互联网的使用是POS系统被恶意软件感染的主要原因。POS 机就如同使用个人计算机一样，用来网上冲浪、网上购物，还访问社交网站。最近利用社交网站攻击用户计算机的恶意软件事例也频繁出现，如果通过 POS 机访问被黑客攻击的社交网站，POS 系统也很有可能被恶意软件感染。而且，POS 系统根据需要安装各种应用程序，如“远程控制程序”、“互联网浏览器(IE)”、“Adobe Reader”和“Microsoft Office”等。黑客就利用“IE”、“PDF”和“DOC”等文档漏洞和 JAVA 漏洞攻击 POS 系统。这种威胁与一般计算机存在的安全威胁相同，但是考虑到 POS 系统本身低配置而无法安装防病毒软件，这些威胁对于 POS 系统是致命的。目前大部分的 POS 系统还在使用服务已结束的 Windows XP 及基于 Windows XP 的 Windows Embedded for Point of Service 和 Windows Embedded POSReady 2009 操作系统。这些操作系统不再提供安全补丁，而且还存在安全漏洞，使用这些操作系统的 POS 机也面临了重大的危险。

如上述，大部分的 POS 系统，由于所处环境的特殊性而存在诸多的安全威胁。尽管由金融当局主导进行着应用全部加密安全技术的 IC 终端机的交替工作，但是将所有的 POS 机替换为新的终端机，预计需要相当的时间。在这期间，POS 系统仍然面临着威胁。

即使这样，我们也不能放手不管。目前可能的方法有“使用防病毒软件”或“数据加密”和“加密通信”。但是已被恶意软件感染的系统，即使数据加密或加密通信已无济于事。另外，防病毒软件已无法应对未知威胁，加上在低配置系统和网速受限制的环境下运营的 POS 系统，即使安装了防病毒软件，但由于资源问题而无法及时更新特征码。
综合上述，选择 POS 系统安全解决方案的时候，需要考虑 POS 系统所处的特殊环境因素，还要考虑针对 POS 系统的最新的安全威胁。并且，对这种 POS 系统专用的安全解决方案的需求越来越高。

AhnLab EPS 是唯一解决 POS 安全威胁的解决方案

AhnLab 提供如 POS 终端机之类的具有特殊性的工控系统的专用安全解决方案 AhnLab EPS(Endpoint Protection System)。
AhnLab EPS 是一款针对系统稳定性较高、使用明确而有限的应用程序的诸如社会基础设施、大规模自动化设备的工厂、POS 机等优化于工控系统的安全解决方案，提供强大的防御恶意软件和安全功能。

AhnLab EPS 基于白名单方式，阻止一些不必要的程序运行并防止恶意软件的流入。而这些功能无需专门的安全知识便可以操作和运营，还通过中央统一管理减少了加盟店的运营负担。另外，还通过强大的“应用程序控制”、“Agent系统控制”、“移动设备控制”和“网络连接控制”技术，从外部威胁和未知的安全威胁中保护 POS 系统，使 POS 系统始终维持安全的状态。

【图 3】工控系统专用安全解决方案 AhnLab EPS

AhnLab EPS 通过服务器装载的恶意软件分析引擎，几乎不占有 Agent 系统本身的资源，可以对 Agent 系统生成的所有的可执行文件进行实时检查和分析。这使得管理员无需更新和维护每个端点上的特征码，因此也不需要考虑更新和维护带来的网络和系统资源的占有。尤其，不仅可以应对 POS 终端机的恶意软件，还可以对未知的安全威胁进行分析。即，AhnLab EPS 的强点在于将重点放在 POS 系统的稳定运行，然后再通过恶意软件检测和响应来强化安全策略。如此，AhnLab EPS 不影响系统资源和业务稳定运营，并可以预先防止和控制恶意软件，可以达到提高生产率和节俭运营费用的效果。

“DAISO”和“新世界”等大型零售公司的 POS 系统已应用了 AhnLab EPS。半导体、家电生产线、工业设备控制、自助服务机(KIOSK)和 ATM 机等领域的工控系统也有应用 AhnLab EPS，其性能和安全性已得到了验证。

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

© 2015 AhnLab, Inc. All rights reserved.