AhnLab

安全月刊

2015.08 Vol. 34

加强APC等端点安全管理解决方案

单独或联动，更加强大的端点安全管理

AhnLab 最近改善和增加了 AhnLab Policy Center 4.6（以下简称为 APC 4.6）等四种端点安全管理解决方案的对端点系统的安全管理功能。本次修补(版本：4.6.3)以“强化安全”和“提高管理方便”为重点，提高了 APC 4.6、AhnLab Patch Management(以下简称为 APM）、AhnLab Privacy Management Suite(以下简称为 AprM Suite) 和 My PC Inspector 等个别解决方案的功能。通过本次修补，期待这些解决方案之间相互联动或联动 V3 防病毒软件时，能够取得强大的协同效应。尤其，通过强化“自动或强制适用”功能，提高了安全管理员使用方便的同时，还通过强大的安全策略，有望进一步提高企业和机关的端点安全水准。

下面，让我们一起来了解 AhnLab 四种端点安全管理解决方案改善和增加了哪些功能，这些功能又有何特征？

APC 4.6：在线补丁和热修复(Hotfix)，安全空白控制到最低

端点中央管理解决方案 APC 4.6 在此次功能改善中强化了管理员的使用方便性。改善了 Agent PC 的“托盘菜单”和“分组管理用户”功能，并在联动 V3 产品的功能中添加了多样的选项。 密码方面，首先强化了“管理员帐户的密码设置规则”，然后添加了 OTP 身份验证选项。如果选择 OTP 身份验证，则管理员登录时需要通过 OTP 身份验证进。在更改策略时，可以设置为 Agent 应用个别策略，从而提高了端点管理的效率。

本次修补最大的变化是通过网上的在线修补和热修复(hotfix)。以前，APC 产品只能在网下安装及应用修补程序或热修复。现在可以通过网上下载最新的补丁程序到 APC 服务器，安装并应用。如 OpenSSL 漏洞等紧急修补的程序，安全管理员可以即刻从网上下载修补程序并应用，使可以更加稳定运营和管理安全解决方案。

APM：简单检查侵犯软件著作权与否

本次修补程序中添加了检测和管理非法软件的功能。该功能不仅可以查看 Agent PC 安装的软件情况，还可以掌握各软件的著作权情况，事前应对韩国著作权委员会实行的非法软件检查。同时，可以简单确认需要补充的软件数量，减少了购买不需要软件导致的费用。（* 该功能仅提供在CC认证版本）

此外，修补包括提供 Agent PC 安装的微软修补程序的 KB 号信息，实现了详细和准确的补丁管理。微软补丁通常是一个补丁包含多个 KB号，因此确认 KB号才可以正确掌握哪些补丁还未应用，从而可以防止未适用补丁带来的潜在威胁。

APrM Suite：通过自动化措施更加彻底、安全保护个人信息

通过本次修补，AprM Suite 更加强化了自动化措施功能，不仅减轻了管理员的负担，而且更加提高了个人信息文件的安全。管理员可以将个人信息文件或包含个人信息的文件根据“危险”、“警告”、“注意”等三个等级，设定处理规则为“自动隔离”或“自动加密”。原先是由各 Agent PC 的用户可以选择“隔离”或“加密”处理方式，而现在是由管理员设定处理规则后强制应用到各 Agent PC。对于设置密码的文件、未包含个人信息的文件，也可以根据扩展名设定自动处理规则，“强制自动隔离”或“强制加密”。

另外，将用户分为个人信息“办理人”和“非办理人”，防止了个人信息的乱使用，更加提高了个人信息管理的安全性。管理员可以随时查看“办理人”和“非办理人”的个人信息持有情况。当 “非办理人”持有个人信息时，管理员易于掌握并采取相应措施，实现了更加简单方便的个人信息管理。

My PC Inspector：扩大检测项目及强化自动化措施

为了提高管理方便和强制性，My PC Inspector 将检测项目从5个大幅扩大为19个，并强化了自动强制措施功能。通过 My PC Inspector，管理员检测如【表 1】所示的19个项目漏洞，设置自动化措施或强制措施，始终维持各PC的安全。

No.	检测项目
1	检测反病毒软件是否应用最新补丁
2	检测登录密码安全性
3	检测登录密码是否每一季度更新一次以上
4	检测是否设置了屏幕保护
5	检测是否允许U盘自动运行
6	检测是否存在三个月以上未使用的ActiveX程序
7	检测事件日志覆盖漏洞
8	检测密码错误次数超过时，是否锁定帐户
9	检测是否运行安全中心
10	检测是否使用最近使用的密码
11	检测是否设置了密码最长和最短使用期间
12	检测是否使用Simple TCP服务
13	检测是否使用Web服务
14	检测是否使用FTP服务
15	检测是否控制未授权用户访问
16	检测是否使用无线网卡(即使没有网卡，使用时存在漏洞)
17	检测可信站点列表
18	检测在安装ActiveX程序时，是否显示提示信息
19	检测是否自动完成浏览器(IE)表单

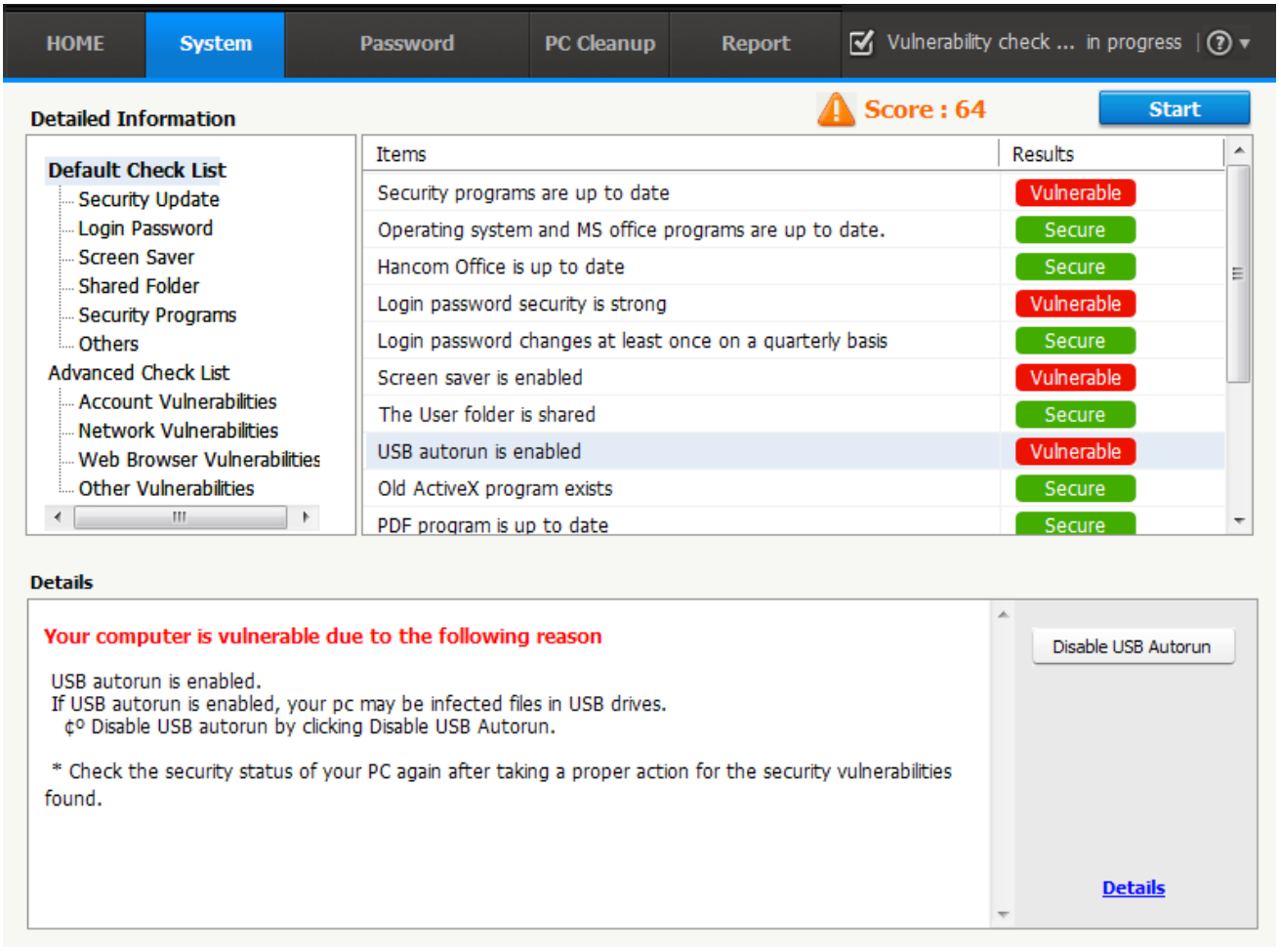
【表 1】 My PC Inspector 漏洞检测项目(补丁版本：4.6.3)

另外，还增加了“用户定义的漏洞检测”功能，可以更加细致地管理漏洞。以前，通过“收集进程列表”的功能收集进程或当运行特定的服务时判断为“漏洞”。但是，未来将组合管理员指定的进程、服务、注册表路径和文件路径状态等判断漏洞与否。尤其，服务检测的提供如【表 2】所示，共检测基本的12个服务项目。但是，根据企业环境，可以另外提供EPR服务等检测项目。

No.	检测项目
1	检测 Messenger 服务停止
2	检测 Remote Registry Service 服务停止
3	检测 Telnet 服务停止
4	检测 Protected Storage 服务停止
5	检测 Cryptographic Service 服务运行
6	检测 System Event Notification 服务运行
7	检测 IPSEC 服务运行
8	检测 SNMP 服务停止
9	检测 Server 服务停止
10	检测 NetMeeting Remote Desktop Sharing 服务停止
11	检测 ClipBoo 服务停止
12	检测 Indexing service 服务停止

【表 2】 My PC Inspector 检测管理员设置的服务检测基本项目

此外，对于不到管理员设置的分数线的 PC，可以设置为 My PC Inspector 主界面显示在桌面的最前端，强制用户采取措施。与此同时，用户 PC 的桌面提供 Widget，直观显示 PC 当前的状态，使用户可以快速方便打开措施菜单，提高了用户的方便，并诱导用户主动参与。My PC Inspector 目前支持英文版 Windows 操作系统。



【图 1】 My PC Inspector 英文版

结合更为强大！

AhnLab 同时提供了四种端点安全管理解决方案的补丁，不仅强调个别解决方案的功能提高，而且加强了四种解决方案之间的联动功能，体现了更强大的端点安全管理体系。

首先，APC 4.6 与 AhnLab 端点综合安全解决方案 V3 产品群联动功能中添加了多样的选项。管理员通过设置，可以选择端点进行病毒扫描。特别是，在预设扫描中提供了“CPU占有率进程优先级设置”选项，降低了端点系统的性能低下。

My PC Inspector 通过与 APM、AprM Suite 的联动，可以实现全方位的端点安全管理。利用 APM 的“检查软件著作权”功能，检查非法软件的安装与否并采取措施。联动 APrM Suite ，管理员检查每端点存有的个人信息文件数。根据搜索到的个人信息文件数，将检查结果分为“危险”、“警告”和“注意”，并树立策略。另外，确认对个人信息的措施情况后，如果低于管理员设置的基准，则判断为“脆弱”，诱导用户采取措施。

产品企划部门的部长金昌熙对此次推出的修补很是期待，说道：“端点仍然面对着安全威胁的矛头。此次推出的 AhnLab 多种端点安全管理解决方案的修补在功能和安全性方面大大被改善。通过单独运营或联动，更加安全保护企业和机关的端点，最终可以稳定开展企业业务。”

2015年上半年五大网络安全威胁及下半年五大趋势

2015年上半年，没有发生大规模的隐私信息泄露或网络瘫痪事件。然而，我们需要注意到，专家们预测到的威胁已经被具体和特定的事件所证实。勒索软件以前在韩国影响不大，但是现在已正式开始了活动。
在2014年年底，韩国水电与核电公司（KHNP）发生了隐私外泄事件，并且意大利黑客团队事件成为了公众关注的中心。这次攻击作为高级持续性威胁（APT）的一个严重案例受到了关注，从中可以得知，把“零日漏洞(zero-day)”作为高价值的网络攻击武器进行交易的黑市活动正越来越猖獗。
从2015年下半年的前景来看，预计对移动设备的威胁将会增加。由于智能手机用户和移动业务的数量发生了难以置信的增长，移动设备特别容易受到危害。在这一时期，我们另一个关注点是，针对应用程序漏洞的零日漏洞攻击变得越来越猛。
本刊，将介绍AhnLab安全应急响应中心(ASEC)的专家们选定的2015年上半年网络安全威胁及下半年网络安全威胁五大趋势。

2015年上半年五大威胁

01 在韩国的勒索软件攻击

2015年4月，通过韩国社区网站横幅链接传播的勒索软件 ***CryptoLocker***，成为了上半年最大的网络安全主题。CryptoLocker 首次被发现于2013，2014年已在海外成为了最热门的安全主题。
勒索软件主要通过电子邮件传播，但正如韩国事件中那样，它们也会利用网页漏洞，例如横幅。 通常，勒索软件感染用户计算机之后，即在桌面显示勒索信息，并将计算机上的私人文档和图片等加密导致无法打开。如果用户不支付赎金，文件将可能永久无法解密。在韩国，已发现的最臭名昭著的勒索软件是 ***CryptoLocker***。勒索软件的其他例子包括:

- ***TeslaCrypt***，针对计算机游戏文件
- ***Nabucur***，对文件进行编码，而非加密。
- ***CryptoWall***，这是一个发现于韩国的很常见的攻击工具，通过电子邮件进行传播。

受 ***TeslaCrypt*** 和 ***Nabucur*** 影响的文件可以用反病毒程序来恢复。然而，受害者在还原受到其它勒索软件影响的文件时必须小心，因为没有特定的关键数值，就无法恢复文件。
在韩国目前还没有发现以移动设备为目标的勒索软件攻击事件。然而，在国外已经发现了限制移动设备使用并向受害者索取金钱以解除限制的移动勒索软件，而且仍在扩散。

02 金融欺诈事件频频发生

2015年上半年发生的另一个严重的安全问题是试图非法获取金融信息的攻击。 ***Dyre*** 是于2014年首次发现的恶意软件，而且还在继续蔓延，在对国外金融机构的很多攻击中都出现了它的踪迹。 ***Dyre*** 攻击将恶意软件 ***Downloader.Upatre*** 作为附件附在垃圾邮件中，当附件被运行，它就开始偷窃隐私和金融信息。
另一个发现于韩国的恶意软件是Banki，它使一些系统持续受到欺骗攻击。像 ***Banki*** 这种恶意软件会不断地进化，以此来逃避反病毒（AV）解决方案的检测。它们用动态链接库（DLL）等方法把远程可执行代码植入应用，或把恶意文件注入系统文件。
目前，由于攻击手段的不同，安全环境正在日益变得多样化。这些多样化的战术包括利用安全漏洞的基于下载的攻击，还有修正模块更新过程以安装可能有害的程序。

03 多样形式进化的恶意电子邮件的扩散

尽管我们建议不要打开可疑的电子邮件附件，但是通过电子邮件附件的恶意软件感染事件还是经常发生。一些传统的传播方式仍在使用，比如伪装成国际航运或金融公司发送恶意电子邮件。
电子邮件内容包含了当前重大新闻或社会问题，以引诱收件人。最近的例子中，引用了中东呼吸综合征（MERS）和吸引人的金融问题。2015年上半年，通过电子邮件传播的恶意软件的类型大多是勒索软件、后门软件和下载器等恶意软件。这些攻击对文件进行加密、盗取用户的金融信息，给用户造成了很大的损失。

特别令人关注的是那些针对特定的人或团体的恶意电子邮件。这些攻击被称为"鱼叉式网络钓鱼"，并且仍在进化成技术上更先进、更为精心策划的形式。所以用户在打开电子邮件时需要注意。

04 对路由器和家庭网络产品的攻击正在增加

黑客团体 Lizard Squad 于2014年11月和12月，针对 Xbox Live 和索尼 PlayStation Network 发起了 DdoS 攻击，使用的手段就是通过感染互联网路由器攻击。

这种类型的攻击已经开始扩展到针对其他设备的漏洞，如IP摄像机（婴儿监视器）和闭路电视。这种利用互联网路由器安全漏洞的攻击事件在韩国也持续发生。攻击者利用路由器的漏洞篡改DNS地址后，将诱导用户打开假冒网站或分发恶意软件。虽然设备制造商提供固件更新以解决这些漏洞，大多数用户既不了解更新固件的重要性，也不知道如何更新它。预想，日后对连接互联网的设备的攻击可能会越来越增加。

类似的手段被用来攻击安卓移动设备。伪装成 Chrome 等应用程序，虚假警报通知用户更新最新版本，诱导用户安装恶意软件。在2015年上半年，许多这种类型的恶意应用程序的例子已被发现。一旦这些应用程序被安装，他们就会窃取用户的个人信息和金融信息。

05 应用程序漏洞在不断增多

2014年4月，OpenSSL 出现一个代号为 ***HeartBleed***（CVE-2014-0160）的安全漏洞，中文名称叫做“心脏出血”、“击穿心脏”等。从此之后，一系列常用协议中的漏洞被陆续检测出来。Bash Shell 漏洞 ***Shellshock***（CVE-2014-6271）以及 SSL 3.0 协议漏洞 ***Poodle***（CVE-2014-3566）分别于2014年9月和10月被检测到。***Shellshock*** 仍然利用在下载和运行恶意软件，因此是一个重大的威胁因素。

2015年上半年已有各种各样的应用程序漏洞被公开。2015年1月公开了 GLIBC 库函数的叫做 ***Ghost***（CVE-2015-0235）的缓冲区溢出漏洞，3月公开了一个被称为 ***freak***（CVE-2015-0204）的 SSL 协议漏洞。在4月公开的 HTTP.sys 远程代码运行漏洞 ***MS15-034***（CVE-2015-1635），它采取的攻击方式是对一个简单的 HTTP 协议 Range Header 进行操纵，已发现很多攻击试图。

所有这些应用程序漏洞主要存在于服务器中，它们令安全顾问和负责准备紧急补丁程序的服务器管理员更加焦虑不安。基于活动的水平，预计2015年下半年会出现更多的应用程序漏洞。为了解决这个问题，常备紧急补丁程序处理工具是有必要的。

2015年下半年五大趋势

01 针对移动支付服务的恶意软件

随着电子支付服务从PC迁移到移动平台，FinTech（金融技术）正在迅速发展。发展的结果将导致智能手机拥有信用卡的功能，而移动通信安全的优先级将会提升。

中国支付巨头支付宝提供了一些现有的安全漏洞例子。支付宝的经验提醒安防行业注意涉及重复付款的问题以及与苹果支付系统有关的犯罪活动。随着FinTech服务出现在韩国，这些例子是有用的情报。三星、Naver 和 Kakao 是一些在韩国研发支付解决方案的公司。

在这个早期阶段，韩国的FinTech服务中尚未发现恶意软件和漏洞。然而，鉴于通常的威胁模式，以及犯罪集团对金融交易环境的兴趣，这将成为恶意软件的目标。预计随着风险和安全威胁的出现，FinTech 企业将不断对它们进行评估和快速应对。

02 移动勒索软件将成为现实

随着智能手机的用户继续增加，保存在其中的个人信息量也越来越庞大 。这一点对勒索软件攻击者而言是很有吸引力的攻击对象。国外报道安卓设备上出现了多样的勒索软件，其被害事例也在增加。针对安卓智能手机的移动勒索软件主要是感染并控制手机使无法正常使用，或者将手机上的数据加密使无法打开，然后向用户索取赎金。

这种移动勒索软件主要发生在北美、欧洲和俄罗斯等地，赎金要求支付美元、比特币和卢比等。在韩国曾流行被称为 ***Bankoon*** 的金钱目的的恶意应用。很有可能在韩国也会出现获取金融利益为目的的移动勒索软件。尤其，有可能伪装为知名的反病毒软件或银行应用程序来传播。也有可能利用色情来传播病毒。类似于传播的方式，攻击者利用勒索软件限制移动设备使用或加密数据等，并通过难以追踪的方式来索取赎金。

03 恶意软件的本地化及扩张

恶意软件的本地化在过去10年不断地持续。例如，今年5月在日本发生的窃取个人信息的事件，利用的恶意软件是彻底针对日本受害者订制的。
另外，有些恶意软件开发者为了增加收益不断扩张攻击地区。针对韩国网上银行用户的恶意软件制作者将攻击活动范围移到了在日本并展开了类似的攻击。，针对欧洲地区网上银行用户的恶意软件Dyre将亚洲地区银行添加到了攻击对象，接着扩展范围攻击韩国的银行。刚开始针对美国和欧洲地区的勒索软件，目前已开始扩张到韩国语和日本语。
恶意软件的本地化伴随着彻底的本地化战略，并为了收益最大化，演变为扩展地区和语言的方向。

04 高级持续性威胁（APT）变得更精致

随着国家之间的网络间谍行为和企业之间的产业间谍行为，APT等针对性攻击预计也将越来越进化。美国人事管理局（OPM）和德国联邦议院发生的入侵事件，足以说明针对特定单位精心策划的针对性攻击已是现实。
这种攻击很可能利用了常用或开放源码软件的零日漏洞制作了定制的恶意软件。这种基于定制型恶意软件的攻击是一种非常高级的攻击，如果特定机关或企业成为目标的话，很有可能造成严重的损失。此类攻击有针对反病毒提供商卡巴斯基 Duqu2.0 攻击，这种攻击就连安全专家组也难以防御。

05 应用程序漏洞攻击将变得越来越猛

最近发生的诸多安全事件中，不可缺少的关键词绝对是“漏洞”一词。
零日漏洞它的术语本身就带着从发现漏洞到提供安全补丁这期间的危险性和紧迫性。实际，在这发现漏洞到发布安全补丁期间发生很多的安全事件。Oracle Java 曾经是零日漏洞攻击的常见对象，但是从去年下半年开始到今年上半年 Adobe Alash Player 成为了零日漏洞攻击的主要对象。
今年上半年在韩国发生了利用 CVE-2014-0515 和 CVE-2015-5119 等漏洞并通过社交网站发布勒索软件的事件。最近发生了利用 CVE-2015-5119 漏洞用来暴露意大利黑客团队机密信息。相比过去相对较短的零日周期，最近的攻击在很难确定其使用时间，因为它们在实际发生攻击之前还未被认知。
在2015年下半年，利用如 Adobe Plash Player 等应用程序漏洞的大小安全问题预计将会持续发生。为了防止并将损害降到最低，需要增加安全资源的投资、安全专家们的努力和用户格外的注意。

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