安博士月刊

星 期 三
11月 27日
2 0 1 3年
Vol.14

【安博士月刊】是综合安全解决方案公司-安博士公司发行的网络安全信息月刊。

安博士，在 AhnLab ISF 2013 提示响应APT的蓝图

从新的角度来谈论威胁的可视性

2013年10月23日，AhnLab 综合安全博览会（AhnLab Integrated Security Fair, 简称为 AhnLab ISF 2013)在首尔市江南区三成洞COEX隆重举行。本次大会是历届规模最大且参加人数最多的一次，共有1600名的企业和公共机关的IT管理员和安全管理人士参加了本次大会。大会期间，首次试行的网上直播也大有收获，共有3000名的网友收看本次大会的直播现场。

另外，本次大会同时进行了世界知名的安全企业的展示，有 Barracuda Networks、EMC Korea、HP、IBM Korea、Inter Korea 和 Palo Alto Networks 等。由此可见， AhnLab ISF 已成为了名副其实的韩国规模最大的安全盛会。虽然规模越来越大， 但是它的最终的旨意没有变，仍然是掌握当前面临的安全威胁实体并提示实际的解决方案。

AhnLab 前任代表金弘善在 ‘Stop APTs Dead’ 为主题的演讲中强调，对于最近像 APT（Advanced Persistent Threat）高级安全威胁，必须明确理解其特征并具备有效的响应方案。说道：“为了响应此类未知的威胁，相应急变的环境同时具备网络级别的垂直的安全响应体系和端点级别的水平响应。”他还自信地说道：“AhnLab 多年来已积累了端点和网络安全威胁的经验和专门技术，并通过恶意软件分析和响应组织，托管组织，还有取证分析组织等专门的技术人力开创新的安全境界。”

国际市场调查机关 Gartner 分析师 Lawrence Pingree 以 ‘响应 APT 的下一代安全战略（Best Practices for Mitigating Advanced Persistent Threats）’ 为主题演讲。他指出，通过最新威胁的理解找出适合各企业的相应方案是最基本且最重要。为有效响应 APT，从 ‘流量分析’ 到 ‘端点响应’ ，还有找出隐匿在端点的威胁痕迹的 ‘端点取证分析’ 等技术是非常必要的。 还说道，今年的安全关键词为 ‘情景感知（Context Awareness）’ 的话，今年的核心主题将是通过各安全解决方案，掌握感知信息的相互联系并确保可视性的 ‘情景感知安全情报（Context Awareness Security Intelligence）’ 。

Track A：安全法规，不要逃避要去了解！

A会场主题是‘安全合规（Compliance）’，介绍了面对越来越强化的有关安全法规的企业和机关的苦恼，并提示了具体的解决方案。

《个人信息保护法》修订，我们需要准备什么？

管理咨询部门的李将雨董事介绍了个人信息保护法修订案的核心内容和为遵守该法律现职业务需要准备的事项。他说道：“在销毁公司内保管的个人信息之前首先要了解和掌握现况，而且必须清楚认知此业务不仅局限在IT部门，而是涉及到公司所有的部门。因此，现职业务负责人的作用非常重要，不仅需要得到有关部门的事前同意，还要进行持续的协议。”

个人信息保护的发展，从‘管理’到‘阻止外泄’

软件开发室的金在烈首席研究员在演讲中说道：“个人信息保护法的最终旨意在于个人信息不得保存在一般企业或机关的计算机。要保护个人信息需要‘搜索’、‘检测泄漏’和‘流通管理’等三个阶段的技术保护措施。”
他还介绍了两种有关个人信息保护的产品：个人信息泄漏防止解决方案‘AhnLab Privacy Management suite’和企业个人信息流通管理体系‘AhnLab Privacy Lifecycle Management’。

金融安全的新的模式

专门黑客攻击的最具魅力的目标非金融机关莫属。与此相关，融合产品开发室金起荣室长把黑客攻击比喻成广播电视局的现场直播，说道：“广播电台在现场直播之前做很多的一系列准备。黑客攻击也一样，在进行攻击之前做很多的准备。”接着说道：“仅仅依靠当前的安全体系无法响应围绕金融安全的威胁。这就需要对金融安全的思维转换。”
他还强调：“必须具备有效的安全体系，它应该是主动（active）的方式而不是被动（passive）的方式。该体系并不只是加强单点解决方案的功能，而是重定位当前的技术，相互补充的方向改善。”

综合安全体系的构筑方案

为了遵守围绕企业环境的复杂的安全合规，首先要提高系统的安全水准。与此相关，解决方案服务部门的李相九次长提示了为提高系统的安全水准的安全框架和解决方案构筑方案。他说道：“安全，不可能是完善的！”，接着强调：“通过综合与分析的反复的过程，理解综合威胁的含义和可视性，才能使威胁降到最低并提高安全水准。”
他还介绍了基于 AhnLab 安全框架的产品：▲网络分离 ▲个人信息综合管理 ▲融合安全托管系统的构筑 ▲ 整合内部和外部的安全托管流程等。

Track B：水平和垂直安全的联系

B会场的主题是‘高级威胁（Advanced Threats）’，提示了面对APT等最新威胁的实际响应方案。响应APT的关键在于，当企业端点中心的水平的响应方案和网络中心的垂直的响应方案相联系时，可以找出高级安全威胁的响应方案。

为什么是多层次分析？

市场销售部门李建龙课长将端点定义为业务相关的信息和个人信息所在的地方。因此，当前的防病毒软件必须积极响应而不是被动响应。AhnLab 最近推出了基于多层次分析平台的全新V3产品群。李课长自信， V3采用了多层次的分析平台，尽量减少了特征码更新，并通过多种功能可以轻松地确保用户计算机的安全。
他还强调， 防御恶意代码、检查安全漏洞、更新补丁和管理个人信息必须通过基于统一平台的综合的端点管理。

APT危机，我们该如何抵御？

战略产品事业部门吴常恩次长说道：“APT已不再是新的威胁，而是实际已发生的威胁，而防御APT的关键是恶意代码。” 对此的解释是，在这样的环境下重要的是检测通过各种渠道流入的恶意代码、通过监控来确保威胁可视性、还有在虚拟环境下通过行为分析得到的恶意代码详细、正确的信息等。
接着说道：“AhnLab MDS是垂直响应的方案，从网络层开始全面提供检测、分析、响应和监控恶意代码的功能。不仅可以通过虚拟机进行行为分析，还可以进行动态内容分析（DICA，Dynamic Inteligence Content Analysis），并应用 anti-ROP 技术有效响应像APT的智能安全威胁。

看不见的威胁：对安全死角地带确保可视性战略

市场销售部门的金昌熙次长说道：“传统的安全解决方案主要防御已知的威胁，因此，总有一些传统的安全解决方案检测不到的威胁，即安全死角必定存在。”他指出最近企业安全的关键词为‘全数检测’，‘自动分类’，‘详细分析’。还说道：“在端点层响应恶意文件的前提下，需要检讨从端点层收集网络上的所有文件，并通过先进的技术和高级的模式信息，智能分析并分类的方案。”
对此，他介绍了下一代安全解决方案 AhnLab MDS Enterprise。该产品是企业自主收集企业内部的所有文件，并分类后迅速分析，达到实时响应威胁的解决方案。

网络安全，指向哪里？

随着IT环境的急剧变化，企业的网络流量也暴增。战略产品事业部门的刘明虎次长说道：“业务连续性和减少网络流量瓶颈是企业必须要达到的。为此，网络安全设备的关键任务是通过正常验证的数据包，同时迅速检测并拦截恶意数据包，从而减少网络流量瓶颈。”
为解除网络流量瓶颈并保持网络稳定运行，需要引进具备‘大量网络流量处理技术’、‘高速数据包安全处理技术’、‘检测模式行为高速化技术’等的网络安全解决方案。AhnLab 统一网络安全解决方案 TrusGuard 除了这些技术以外，还提供恶意代码响应技术和被成为下一代安全技术‘应用程序控制技术’。

Track C：找出隐藏的威胁

C会场的主题是‘安全透视（Security Insight）’，介绍了预测安全威胁发展方向的同时通过先进的技术确保安全可视性和响应方案的方法。

高级化安全威胁的范围变化

通常把黑客和安全专家比喻成无止境的矛盾之战。AhnLab 安全响应中心的李浩雄室长说道：“只有追随时代潮流，才可以使安全这个‘盾’可以超越‘矛’。”紧接着说明了国内外代表的网络攻击事件和攻击技巧后，主张：“如同融合技术时代的IT领域，网络攻击大部分是融合过去的技术和当前技术的方式出现。”并强调：“为了主动响应此类安全威胁，重要的是掌握数据流量、确保可视性后导出连带关系” 他还忧虑，日后有可能在封闭的网络也会流入并活动像超级病毒之类的威胁。

基于威胁情报（Threat Intelligence）的下一代的安全托管服务

引进多数安全解决方案也无法防御智能攻击是为什么呢？AhnLab CERT 组的权东勋组长正是从这些数多的安全解决方案中找到了答案。多数的安全解决方案记录大量的日志，但是仅仅由几名安全专家管理实际上是不可能的。他说道：“安全解决方案随着先进的技术越来越高级化，与此相比，管理并运营的企业负责人的专业性却不足。
为了克服企业现实响应的局限，AhnLab 提供基于威胁情报的下一代安全托管服务。他说道：“收集看不见的信息并找到其意义，判断如何响应，这才是真正的情报。”并表示：“AhnLab 下一代的安全托管服务提供对威胁的可视性，实时认知威胁，从综合的来龙去脉中迅速做出决策。”

数据取证分析，最终消失的痕迹！

AhnLab 云分析组金志勋组长 强调数据取证分析，说道：“解决损害，并不能结束高级持续威胁APT。通过修复工作要考虑日后防御APT的方案，因为攻击者随时可以再次入侵。”他定义数据取证是在犯罪调查中确保犯罪证据的取证分析一样，在网络犯罪中提取入侵系统的数据后解释并找出证据的过程。

强调，为了早期检测和分析像APT的智能型的攻击，取证分析技术是必须的，而且取证分析在智能型攻击越来越增加的现实中，日后将称为主动响应的下一代安全解决方案的中心。
他自信，AhnLab 取证分析专门组织A-FIRST拥有自己的取证分析工具，基于分析专门技术和独步的基础设施，有效分析和响应APT等智能型威胁。

展示区：没有比这更有活力！

除了发表会和展位展示，会场各处进行技术展示、体验区和开放工作室等。本次大会，还进行了有意义的活动。一个是，将‘低碳亲环境’作为大会的一环，向利用公共交通来访的访客赠送一些礼物；另一个是，大会期间在 AhnLab 购物网销售额全额捐款。

在发表会聆听有关威胁和响应方案的最新信息的访客，在休息的时间访问技术展示区继续聆听有关多样的安全技术和解决方案的深度说明。

果然是百闻不如一见。访客根据对安全的各自的关心和苦恼访问展示最新安全解决方案的展位，他们每个人的眼神都是很认真。尤其，访客集中在AhnLab MDS、AhnLab Privacy Management Suit、AhnLab TrusZone 展位，这足以证明了对安全法规和APT响应仍然是安全的热门主题。

Barracuda Networks、EMC Korea、HP、IBM Korea、Inter Korea 和 Palo Alto Networks 等国际安全企业纵横在发表会、技术展示和展位，介绍了多样的技术和解决方案，受到了注目。

关于安博士（AhnLab,Inc.）

安博士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。
安博士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。

北京市朝阳区酒仙桥甲12号电子城科技大厦1206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 0935 / +86 21 6095 6780
http://www.ahn.com.cn / v3site@ahn.com.cn