



NetEvents

THE Meeting Place for Technology Leaders

THE Meeting Place For Technology Leaders

Publication:China ComputerWorld

Date: 2011/12/5

Subject: NetEvents - Direct witness mobile Internet security risks.

Report for: Palo Alto Networks, Fortinet, Blue Coat Systems, Sourcefire, IDC





热点透析
HOT TOPICS

建立基于云计算技术的防火墙，成为 NetEvents 大会的热议话题。

NetEvents 直击移动互联安全隐患

普吉岛的沙滩，热情的海风，都与 NetEvents（亚太记者峰会）会场中的热烈气氛遥相呼应。

11月16日-17日，NetEvents 在泰国普吉岛举行。来自美国硅谷和亚太地区的众多设备商、运营商、标准化组织和咨询机构，分享了各自对 ICT 产业未来发展的分析和预测。其中大数据的增长及社交媒体广泛普及所带来的安全隐患让安全问题成为现场的讨论主旋律。

大数据带来大隐患

智能手机的普及让成千上万的移动应用有了用武之地。然而由此产生的海量数据却给客户端带来巨大安全隐患。

据 IDC 预测，2012 年仅亚太区就有超过 2.3 亿的智能机用户，智能手机上的各种应用程序无时无刻不产生大量数据。

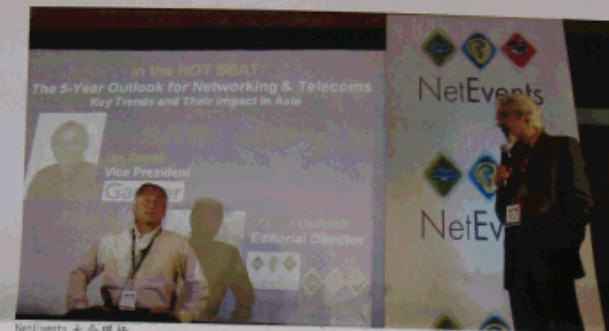
“到 2014 年预计将有 7ZB 的数据，如果把把这些数据打印在纸上，可以覆盖地球表面 12 - 14 圈。”IDC 澳大利亚研究副总裁 Tim Dillon 表示。如此庞大的数据量，即便是国

“随着智能终端的快速发展，2012 年将会有更多企业关注终端安全，这将是一个全新的领域。企业安全系统应该具有更多的智能性，并通过云端的分析引擎进行。”

——Blue Coat 公司产品主管 Jonathan Andresen

际知名 IT 厂商也无法避免安全问题的产生。

此前，苹果的 iOS 操作系统被发现漏洞，黑客通过漏洞可远程遥控 iPhone、iPad 和 iPod 等设备，在这些设备上秘密安装应用程序，从而窃取信息、发送短信或破坏数据。但 App Store 未能识别此恶意程序，使其通过了苹果的安全审批流程。



NetEvents 大会现场

“如今的黑客和以前有很大不同，他们已经变得非常职业化，行为也都是有组织、有功利性的。他们不再攻击传统网络安全设备，而是通过钓鱼的方式引诱终端用户访问，进而找到设备的弱点，让用户从网络上下载木马程序，对手机内数据进行窃取与攻击。”在开幕式上，第一位做主题演讲的硅谷新兴企业之一 Palo Alto Networks 创始人兼首席技术官 Nir Zuk 强调了当今企业面临的 IT 安全问题的复杂性。“上周，

我们发现了 700 个新的恶意病毒，其中 50% 已经不再对传统网络设备进攻。”他认为，传统的甚至是现有的 IPS 已经很难快速应对 PDF、Excel、电影、Flash、Facebook 等多种应用。

一般的安全公司要用两个月的时间对现在的攻击做出反应，因为现在的攻击目标性强，并且不常见，但是基于云环境的安全解决方案却

可以即时处理这种攻击。

记者在会上了解到，Palo Alto Networks 的“sandbox”防火墙产品可以实时通过网络中的反恶意软件定义、分析已知和未知的威胁。防火墙将可疑内容提交到一个虚拟的云环境中，用 70 个行为配置文件样本做判断，检测出文件是否有恶意，防止网络内部被恶意软件感染。

Fortinet 公司香港区域技术经理 Eric Chan 表示，移动设备的媒介都是无线网络，所以要与有线网一样的安全保障。在 Fortinet 对全球 700 个 CIO 进行安全调查中发现，2011 年 CIO 最关心的 IT 消费的主要趋势之一是无绳网络，未来一两年中用户希望使用的新技术是网络应用程序防火墙。

社交媒体成病毒重灾区

在产生大数据的移动应用之中，社交网络带来的安全问题最不容忽视。由于社交网络存储了很多用户与企业的敏感信息，可以给犯罪分子带来可观的经济效益，也给用户和企业带来了新的挑战和安全危机——网络钓鱼、垃圾邮件制造、僵尸网络控制、公司间谍谋取利润等。

虽然为了解决安全问题，很多企业曾经在工作环境中禁用社交网络，但随着社交网络的发展，社交媒体营销成为商业营销不可缺少的部分。《2011 年秋季企业态度和展望》报告显示，美国小企业对于社交媒体营销越来越得心应手。其中 81% 的企业使用社交媒体对企业进行宣传；83% 的受访企业认为，社交媒体营销方式可以有效降低成本，51% 的企业表示，它们的客户使用社交媒体渠道。

但由于社交网络在一般情况下都不会对用户进行鉴别，加之其“可信任的”文化，用户无法完全确认在线的所谓友人的身份，使攻击者可以轻易地成功入侵并获利。

2008 年，一个名为“Koobface”的蠕虫变种潜入 Facebook；在 Blue Coat 2011 年的一份网络安全报告中表明，社交网络是进入恶意软件交付网络的第五大流行切入点，以及第三大最受欢迎的内容。这些都使专注于网络安全的供应商们意识到社交网络的潜在威胁，并纷纷提出对策。

“在终端用户层，不仅要了解攻击情况，而且要清楚自己的网络状况。因此，我们希望提供一个透明、可视化的 IPS 系统。而对于下一代 IPS，希望能够研究黑客有哪些进攻方式，了解进攻对象特点等等。”来自美国安全公司 Sourcefire 的产品经理 Leon Ward 透露，Sourcefire 未来会推出基于云的、具有恶意软件检测能力的软件服务。

“也许我们对于安全的观点有点悲哀，因为安全问题会越来越多。”根据 Leon Ward 的判断，由于企业及个人用户对于各类应用软件的使用量急速增加，在未来的一两年内，防火墙，尤其是基于云技术的防火墙，将成为更多企业安全解决方案中最为重要的需求。