



NetEvents

THE Meeting Place for Technology Leaders

THE Meeting Place For Technology Leaders

Publication: China Network World

Date: 2011/12/2

Subject: Next generation network security to protect against new type of malware

Report for: Palo Alto Networks

Original address: http://www.cnw.com.cn/news-international/hm2011/20111202_238535.shtml



下一代网络安全防范新型恶意软件

2011年12月02日 14:44分 作者:高辉 来源:网界网

[查看评论](#) [发表评论](#)

摘要: 据IDC今年亚太区CIO创新研究调查报告显示,接近70%的CIO表示未来两年会将云计算嵌入到业务运营当中。顺应这一趋势,新一代网络和安全将如何发展?在日前举办的NetEvents亚太媒体峰会上,全球领先的网络厂商汇聚一堂,数据中心网络、下一代网络安全和运营商以太网成为中心议题。

关键字: [云计算](#) [数据中心网络](#) [下一代网络安全](#) [NetEvents亚太媒体峰会](#)

[思科创新解决方案,优化网络视频传](#)

【CNW.com.cn专稿】目前, [虚拟化](#)技术正在企业中快速普及,云计算的应用也加快了步伐。据IDC今年亚太区CIO创新研究调查报告显示,接近70%的CIO表示未来两年会将云计算嵌入到业务运营当中。顺应这一趋势,新一代网络和安全将如何发展?在日前举办的NetEvents亚太媒体峰会上,全球领先的网络厂商汇聚一堂, [数据中心网络](#)、[下一代网络安全](#)和[运营商以太网](#)成为中心议题。

推荐阅读:

[2011黑帽大会专题](#)
[IETF成立25周年](#)

当前的企业网络安全形势,越来越复杂。当我们用各种方法保护数据中心的时候,发现直接对数据中心攻击的现象在减少。入侵者不再直接攻击安全基础设施,而是通过恶意软件攻击最终用户来获得访问数据中心的权限。

然而传统的安全措施很难察觉到针对性攻击,无法及时生成签名让IPS和反病毒软件阻止针对性攻击。客户虽然有许多设备保护数据中心和网络边界,但却不能保护新型攻击的目标——用户。



现在专业的入侵者首先使用社交媒体锁定某个员工，让用户打开一个为其专门定制的文档，例如PDF。第二步，这些文档会利用Adobe PDF Reader、PowerPoint或浏览器等应用程序的漏洞，运行恶意代码。第三步恶意代码会通过互联网下载后门程序，在用户电脑上安装木马。接下来恶意程序会与外部的入侵者建立命令与控制链接，如此就进入第五步，入侵者就可以通过获得用户权限进入数据中心。

在应对这种针对性攻击上，传统安全设备显得力不从心。“现在的安全设备可以很好地应对大规模的攻击，” Palo Alto网络公司的创始人兼首席技术官Nir Zuk解释道，“而这种针对性攻击可能就是一个PDF文件，只进行了一次传输。”



Palo Alto网络公司的创始人兼首席技术官Nir Zuk

当前文档传播途径多种多样，除了Web浏览和电子邮件外，还有Skype、Dropbox、SharePoint、WebEx等等。Nir Zuk认为，解决之道首先要保护所有应用，不仅是浏览和电子邮件。第二，响应时间非常关键。第三，必须采用自动化技术，解决人力的问题。这就需要完全自动化的分析流程，并对攻击响应。可以采用沙盒技术，让目标文件在虚拟机中运行，如果恶意软件作出可疑动作，如更改注册表设置，产生一些不应该产生的互联网流量，软件就可以做出判断。接着会自动产生签名，包括IPS签名和反病毒软件签名。

为了阻止有针对性地恶意软件攻击，Palo Alto新推出了称为WildFire的技术，能够精确识别恶意软件产生的流量。一个恶意软件即使逃避过检查，它最终也会开始向计算机外发送流量。如果发现恶意行为，WildFire会生成一个签名来识别流量，并在今后阻止它。

“WildFire是一种云服务，” Nir Zuk介绍到，“我们在云上使用数千个CPU来自动分析文件。在试用的几个月时间里，我们发现了约700个以前未知的恶意软件。其中有57%当时没有被反病毒软件和IPS检测出来。” Nir Zuk认为，防范新型恶意软件，保护所有应用，且性能不受影响，是下一代防火墙的职责。