



NetEvents

THE Meeting Place for Technology Leaders

THE Meeting Place For Technology Leaders

Publication: CCTIME

Date: 2011/11/17

Subject: Traditional IPS have been incapable of responding quickly to various application attacks

Report for: Palo Alto Networks, Sourcefire

<http://www.cctime.com/html/2011-11-17/20111117130261318.htm>

http://www.cctime.com/html/2011-11-17/20111117130261318_2.htm



传统IPS已不能对各种应用攻击做出迅速反应

2011年11月17日 01:30 CCTIME飞象网

飞象网讯（崔玉贤/文）11月16日晚间消息，在2011秋季亚太媒体峰会上，网络安全厂商Palo Alto Networks以及Sourcefire分别介绍了各自的安全产品系列。

传统IPS已经很难应对现有各种应用

Palo Alto Networks公司的创始人之一Mir Zuk可以说是个“奇才小子”。他在CheckPoint公司时发明了防火墙，他接着发明了世界上第一个IPS。在这次亚太媒体峰会上他又再次提出他的新理念：“传统的甚至是现有的IPS已经很难快速应对PDF、EXE、Facebook等多种应用。”





Nir Zuk

“以前的网络攻击者和现在的有很大的不同，现在的网络攻击者都是有组织、有功利的行为；此外，现在的网络安全攻击者不再是对传统网络安全设备进攻，而是通过钓鱼的方式引诱终端用户访问，进而找到设备存在的弱点，从网络上下载巨大的木马程序，最后进行数据的窃取与攻击。” NirZuk解释道。

在网络攻击的每个步骤中都需要进行安全的保护。在对网络进行安全保护过程中，反应时间无疑是最为关键的一个环节。“无论攻击者目标性多强，时间很关键，必须要做出快速反应。同时要自动化，智能化。” NirZuk表示。

而对于不同的应用，比如说PDF或是Facebook，传统的网络安全设备很难进行防范，而现有的攻击者可以通过PDF等应用进行网络攻击。“现有的技术很难阻止有目的的攻击，而且IPS的反应速度很慢。” NirZuk认为。

NirZuk举例道：“上周，我们发现700个新的恶意病毒，有50%已经不是对传统网络设备的进攻。传统的供应商无法提供合适的解决办法。”

因此，Palo Alto Networks开发出了“sandbox”防火墙产品，它可以实时通过网络中的反恶意软件定义来分析已知和未知的威胁，防火墙将把可疑内容（包括DLL和EXE）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，这样可以检测出文件是否有恶意，防止网络内部被恶意软件所感染。“如此，就可以在一个小时之内即可产生保护，而不是一两个月。” NirZuk表示。

此外，NirZuk首次在亚洲宣布推出苹果的iOS全球保护工具。

IPS的可视化

对于传统IPS已经无法快速对攻击做出反应的论断有些不同的是Sourcefire公司。Sourcefire一直专注在IPS领域。“在终端用户侧，不仅想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，希望能够研究有哪些进攻、了解进攻对象等等。” Sourcefire公司的Field Product Manager Leon Ward表示。



Field Product Manager Leon Ward (中间)

据LeonWard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。“我们将会在今年（2011年）年底前推出这个新的应用。”

据了解，2011年年初Sourcefire以2100万美元收购了云安全初创企业Immunet。Immunet公司提供免费的基于云的杀毒软件。它使用一个通过社区模式驱动和更新的有名的检测引擎(reputation detection engine)，据称，该引擎拥有超过75万的用户。

编辑：崔玉贤

[1] [2]

关键字搜索：[2011秋季亚太媒体峰会](#) [Palo Alto Networks](#) [Sourcefire](#) [IPS](#) [防火墙](#)



NetEvents

THE Meeting Place for Technology Leaders

THE Meeting Place For Technology Leaders

传统IPS已不能对各种应用攻击做出迅速反应

2011年11月17日 01:30 CCTIME飞象网

“未来ISP产品将更多是混合了传统的ISP技术和下一代防火墙技术的混合体。” LeonWard表示。

下一代防火墙技术是由Gartner定义提出的。Gartner注意到，在应用模式、业务流程和安全威胁不断变化的今天，传统防火墙已经无法满足用户的需求。即便在此基础上再加入IPS，也很难有效识别并阻止存在滥用行为的应用程序。在这种形势下，Gartner定义了“NGFW”这个术语来形容防火墙的必然发展阶段，以应对攻击行为和业务流程使用IT方式的变化。

编辑：崔玉贤

[1] [2]

关键字搜索：[2011秋季亚太媒体峰会](#) [Palo Alto Networks](#) [Sourcefire](#) [IPS](#) [防火墙](#)