

CES2015--物联网与智能设备的盛会

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	CES2015 – A festival of uncontrolled IOT and Smart devices		
原文作者	Simon Hunt	原文发布日期	2015 年 1 月 14 日
作者简介	<p>Simon Hunt 是迈克菲公司的副总裁兼首席技术官，负责家庭网关安全技术，负责保护所有家庭设备免受数字威胁，而无需在游戏机、平板电脑、电视和恒温器上安装任何软件。</p> <p>https://blogs.mcafee.com/author/simon-hunt</p>		
原文发布单位	迈克菲		
原文出处	https://blogs.mcafee.com/consumer/ces2015-festival-uncontrolled-iot-smart-devices		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
免责声明	<p>本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。</p> <p>本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。</p> <p>译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。</p> <p>本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验</p>		

	<p>室并未授权任何人士和第三方二次分享本译文,因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为,及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的,基于上述问题产生的法律责任,译者与安天实验室一律不予承担。</p>
--	--

CES2015 –物联网与智能设备的盛会

Simon Hunt

2015 年 1 月 14 日

物联网及“智能设备”是今年 CES (国际消费类电子产品展览会) 的热门。展会上到处都是来自各制造商的新奇物件，有智能咖啡机、健康追踪设备、火灾报警器、住宅安全系统，甚至一些交通工具也被设想在将来可以佩带。

CES 大亨，三星首席执行官 Boo-Keun Yoon 在其幻灯片演示中用了很大一部分来说明“物联网已不再是科幻小说，而是科学事实。”-我可以用自家拥有的大量三星设备来证实这一点。

你看到的每个地方，都有物联网设备，要么是物联网设备控制其它设备，要么是其它设备控制物联网设备。当然了，在 Intel 的展位，我们也花了大量时间来讨论如何管理和确保物联网设备的安全。

我在之前的博客中曾提到过这些设备给我们带来的安全问题（并保证会更新）。有特权的设备如果与家庭网路相连，它就可以像间谍一样，并可发起更多的不法攻击。还有来自“聊天”设备的问题，这种设备会占用部分（昂贵的）带宽。我家就遭受了此类问题，大约 30% 的上传带宽被各种插件占用并用来与它们的家庭服务器进行毫无意义的对话。

如：你家的灯每天需要几次固件升级？

至此，在 Intel 安全方面，我们依然并一如既往地致力于我们的愿景：保护人们在个人及企业数字世界中的安全。我认为，当我们只是被一些简单的物联网设备（没有能力整合，无法与强大的安全生态系统合作）所环绕的时候，这一愿景无法实现。为了解决此问题，我们正在证明将 Intel Security Global Threat Intelligence 系统与 Intel Service Provider Division's Cable 调制解调器网关相结合，通过阻断恶意互联网访问来保护所有家庭设备，包括传统的平板电脑、个人计算机、及物联网家庭设备。

即使设备非常安全（考虑到市场发展速度和性能限制，这是一个难以实现的目标），人们也会受到钓鱼及社会工程学的攻击。当然，个人计算机还面临被高级恶意软件控制的风险，比如改编门禁或数码相框，如众所周知的 Stuxnet 蠕虫。

到目前为止,最好的办法就是剥离掉网络层面不好的内容,以一种简单易懂的方法告知屋主正在发生的事情。虽然这是新问题,但是,20 年来,网络检查和过滤技术在企业界已久经沙场并得到改善。

当前,是要将这个概念简化到人人都懂,并将其精简到家庭互联网经过的黑匣子内。

我们对此的解决办法是?将智能设备放置在每个智能家庭都有的互联网门户进行管理。

你或许没有意识到这点,但如果你是有线网络客户,这样比把有线网络服务接入 Intel 动力的调制解调器要好。这些智能设备拥有完全过滤及家庭控制网络体验所需的所有 CPU 动力。

在 CES 展会上,我们演示了保护 Windows RT 及 iOS 设备免受不适当的内容、恶意软件、钓鱼网站的攻击,对类“zombie”活动的检测,及一次 Kiosk 体验(智能设备只能与指定网站连接)。所有这些,都没有在智能设备自身安装任何软件,亦或是以特殊方式对它们进行配置。我们还演示了家长怎么样去使用“You’re Grounded!”特性,只需单击一次就可使所有儿童设备瘫痪。

对于移动运营商,我们向他们展示了可以帮助他们解决客户服务方面问题的技术。如:识别家中运转不良的设备、宽带杀手等等。还展示了我们如何识别诸如互联网与冰箱相连,并开始发送邮件这样不寻常活动的技术。

当然,这一技术并不局限于 Intel Puma 设备,它在其他平台也同样适用。但是,由于 x86 芯片组的进程动力问题,目前这一技术还是通过“Intel Inside”使用较好。

不管你使用的是什么设备,我们的目标一直都是保护家庭中的每件设备及用户的在线体验。如果你看到了我们在 CES2015 所做的演示,希望你认同我们距离将这一目标变为现实又进了一步。