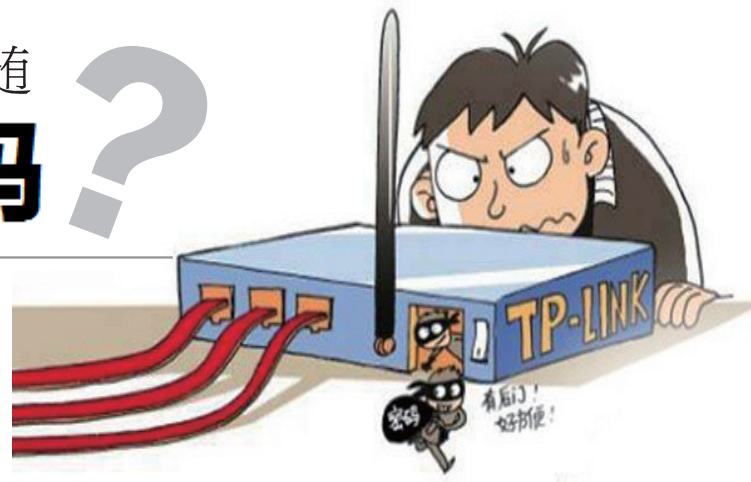
物联网迅猛发展，安全隐患也如影相随

您家的路由器安全吗？



如今，我们的生活越来越智能，万物互联时代悄然来临，小至路由器、智能音箱、冰箱，大到汽车、工业设备，越来越多的物品都接入了互联网。然而，迅猛发展的物联网（是指物物相连的互联网，即以互联网为基础，用户端延伸和扩展到了任何物品与物品之间）在给人们带来便利的同时，安全隐患也如影相随，成为物联网产业发展的一个痛点。

不久前，《2017物联网安全年报》（以下简称《年报》）由北京神州绿盟信息安全科技股份有限公司（以下简称“绿盟科技”）发布，显示了我国物联网安全的现状、特点以及面临的主要安全风险。

安全隐患你知道多少

现在路由器成了很多家庭的“标配”，大多数路由器通过IPv4地址单向连接互联网，外部网络无法反过来主动访问。但以路由器为代表的物联网设备数量众多，还有大量路由器不能被完全屏蔽，存在被外面“看见”的风险。《年报》显示，目前具有安全风险的物联网设备中，路由器和视频监控设备暴露在互联网上的数量最多。比如，国内暴露在互联网上的路由器就超过1000万台。这些暴露出来的设备，一旦存在漏洞，就有被攻击的风险。

绿盟科技物联网安全实验室研究员张星说，近年来许多新型智能设备接入互联网，但安全风险仍然集中在相对传统、应用比较成熟的设备上，它们也是感染恶意代码的主要物联网设备。

《年报》还监测到，一些数量较少的物联网设备也存在安全隐患。比如，商用车的远程通信统一网关、网络恒温器等可能面临远程登录无密码保护、设备停产缺乏安全维护等风险。不单是硬件，《年报》指出，物联网一些常用的操作系统同样存在不同程度的安全问题。

很多物联网设备通过云端连通，而长时间连接云服务，安全隐患将会增加。

“现实中，很多物联网设备工作场景不得不长期和‘云’连接。伴随着物联网应用的深入，云服务将更加普遍。我们监测到，一些攻击者已经把目光从网页和邮件等传统服务转向新兴的物联网服务。”绿盟科技首席架构师杨传安说，大数据时代，网络攻击的目的性更强，攻击的技术手段增多、技术更高、更隐蔽，黑客可能为了利益，而对物联网云服务实施攻击。

杨传安认为，物联网由多种设备组成，互联互通的环境使得安全风险快速扩散和传播。因此，要从整体全局考虑安全防护。某个物联网设备存在安全隐患，并不只影响单个设备，还可能引发系统性的安全事件。

比如，某些设备中存在的弱口令、已知漏洞等风险，可能被恶意代码感染成为“僵尸主机”。一方面，这些被感染的设备会“传染”其他设备，组成大规模的物联网“僵尸网络”；另一方面，它们接受并执行来自控制服务器的指令后，一旦发动大规模DDoS（分布式拒绝服务）攻击，将会对互联网基础设施造成严重的破坏。

一台设备被感染成为『僵尸主机』，就会『传染』其他设备，组成大规模的物联网『僵尸网络』

对物联网安全重视不够

物联网正加速融入人们的生产生活。知名IT咨询机构高德纳咨询公司（Gartner）预测，2015年至2020年，物联网终端年均复合增长率将达到33%，安装基数将达到204亿台，其中2/3为消费者应用。

哈尔滨工业大学计算机学院教授张伟哲介绍，当前主流的物联网管理模式有直连模式、网关模式和云模式。直连模式是指管理端与终端之间不经过其他节点直接相连，这种模式一般用于近距离通信，例如无线蓝牙、WiFi热点等；网关模式主要用于家庭和企业局域网，一般用于近距离管理多个终端；云模式是指用户通过云服务管理各种设备，其特点是突破了设备管理的地理区域限制，比如智能家居和工业云服务。

“不论在哪种模式下，目前都难以完全杜绝安全隐患。作为一种新技术，物联网的行业标准以及相关管理刚刚起步，但物联网基数大、扩散快、技术门槛低，已经成为互联网上不得不重视的安全问题。”张伟哲说。

2017年8月，浙江某地警方破获一个犯罪团伙，在网上制作和传播家庭摄像头破解入侵软件。查获被破解入侵家庭摄像头IP近万个，涉及浙江、云南、江西等多个省份。安全专家表示，一旦攻击者获得远程控制权限，即便是小小的摄像头也能够成为泄露用户隐私的元凶。

360无线电安全研究院负责人杨卿表示，不少物联网设备需要依赖WiFi、蓝牙、GPS卫星导航等无线电通信技术，一旦某个通信协议出现漏洞，将会引发大量安全问题及安全事故。比如，恶意WiFi热点可能设置钓鱼网站，摄像头、麦克风可能泄露人们隐私等。

当前不少物联网设备生产厂商侧重追求新功能，对安全重视不足

物联网安全如何防控

杨传安说，在大数据时代，任何一点安全风险都可能被放大，造成个人信息泄露、财产损失甚至人身安全等问题，给人们生活和社会运行带来影响。

“物联网的安全威胁远未见顶，物联网应用的最终追求是万物互联，实现信息共享，并通过搭建高度自动化和智能化的系统，为人们的日常生活提供便利。随着物联网在社会生活中的普及，应用场景不断丰富，安全风险也将随之增加。”杨传安说。

《年报》认为，物联网的DDoS大流量攻击在未来将成为常态。这是因为物联网设备增多带来规模效应，最直接的负面影响就是攻击者发起DDoS攻击应用将变得更加容易。安全专家表示，从实施的难度、运营的成本、风险与收益来看，DDoS攻击是一种有效的攻击形式，在相当长的时间内，仍将是一种常见的攻击方式。

《年报》分析，当前，物联网应用还较新，在监管机构出台相关法律法规前，厂商缺少动力将安全置于整个产业链中。

“从当下的市场环境看，厂商强调智能化的功能设计，求新求快是物联网行业中的主流，安全反倒是可有可无的选项，这让物联网环境更加具有脆弱性。”杨传安说。

绿盟科技物联网安全解决方案总监刘弘利说，应对物联网安全问题，涉及物联网设备提供商、物联网平台提供商、网络提供商和普通用户等多个参与方，每个环节、每个参与者都应有所作为。

“无论是家庭还是企业用户，都应把安全作为一个重要的关注点。选购产品时优先考虑采用有安全网关的产品。”刘弘利说。他还建议，用户在购买智能产品后，应该尽可能修改初始口令以及弱口令，加固用户名和密码的安全性。同时，修改默认端口为不常用端口，增大端口开放协议被探测的难度，并及时升级设备固件。

《人民日报》/喻思南

大流量攻击在未来将成为常态，每个物联网参与方都应针对性地部署防护措施

WiFi如果存在重大安全漏洞，几乎能影响所有无线设备。