安天周观察

主办：安天　　2015 年 8 月 24 日 (总第 6 期) 试行　本期 4 版　　微信搜索：antiylab

文评

“安全”的关联与流动

在天津港发生严重危险品爆炸事故的灰色而沉痛的日子里，笔者读到了兴东兄的“直面‘互联网 +’时代的安全与风险”一文。过往的两年间，是网络安全威胁大泛化、网络安全事故和灾难层出不穷的年代。但相比于“长江沉船”、“天津港爆炸”这些令人痛心疾首的重大生命灾难相比，网络安全事件相对显得微不足道。的确，相比于最基本的生命安全，网络信息安全似乎是一种高阶的顶层需求。

但需要警惕和关注的是，威胁本身是关联和“流动”的，网络空间与实体空间的融合，从有网络时代起就是一种必然，网络空间和实体空间的交织和映射是在不断加速的，Defcon 上 Marina Krotofi 的报告“Hacking chemical plants for competition and extortion”，就展示干掉一个化工厂的完整流程。从震网病毒展示了其对离心机和阀门级联的作用开始，网络威胁对实体设施的纵深影响能力，已经是一种必然。

对于期待用“互联网 +”全面激活与改造传统行业，以获得发展新动力的中国来说，安全是必须深入评价和考虑的风险。这种风险绝不仅仅是担心互联网络风险被引入传统领域，也同样要看到在传统领域极为不乐观的安全现状的连锁和放大的可能性。传统领域的安全很多依靠原始物理手段保证，很大程度上建立在封闭、低效之上，而没有经过公共安全、乃至国土安全视角的推敲。因此站在一个更为积极的角度来看，“互联网 +”的确可能在短时间内引入大量的安全风险，但同样也可以带入网络安全的思维和方法，来改善传统领域的安全。

因此，对“互联网 +”的安全问题，所需要的不是过度焦虑和渲染，而是寻找合理路径和平衡点。

在斯诺登大规模泄密事件出现后，美方的做法不是把信息和数据封闭起来，而是进一步坚决的推动信息共享，美方希望基于高效的信息共享所带来的高效率能拖垮其跟跑者，而同时，也将其下一代网络安全体系建立在一个高度共享的基础上，从而达成一种全新的攻防境界。这种审视发展与安全关系的视角，或者能给我们带来几分启示。

如何让互联网 + 战略不要因为安全风险变得畏手畏脚，但又如何避免变成一种对安全“无知者无畏”的夺路狂奔，其不仅取决于中国网络安全工作者的作为，也更取决于政府的综合战略设计，以及全民逐渐建立起对安全的信仰。(本文为安天技术负责人对《直面“互联网 +”时代的安全与风险》所做的推荐导读，该文章发表于《中国信息安全》，作者方兴东、胡怀亮)

安天 AVLTeam 发布《Sadstrot 木马分析报告》

安天 AVL 移动安全团队截获了一款恶意木马，该木马运行后会窃取用户 QQ 和微信账户、好友列表、消息记录等，同时会利用 SubtrateHook 框架监控键盘输入的任何信息。

此外，该应用还会接收云端指令，执行模块更新、删除指定文件等远程控制操作，严重影响系统安全。

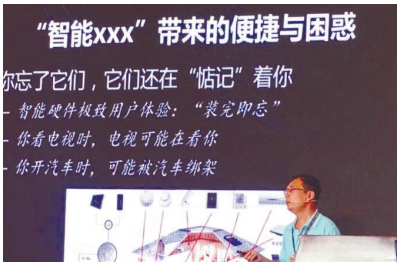
目前 AVL Pro 已经可以全面查杀，有效保护用户手机安全。

『由一个扫地机器人引发的信息安全风险』

——安天参加 XCon2015

8 月 18-20 日，2015 安全焦点信息安全技术峰会 (简称 XCon) 在京召开。该峰会已连续举办 14 届，是国内最高级别的信息安全技术交流平台。安天已经在历年的 XCon 上分享过 11 次的技术演讲。安天微电子与嵌入式安全研发中心总经理桑胜田做了《“斯文扫地” 的 Evil Maid—— 一个扫地机器人引发的信息安全风险》的报告。

桑胜田博士简要介绍了智能安全软硬件存在的安全隐患及物联网与智能硬件安全。以一款扫地机器人为例，重点为大家展示了研究小组对几款智能扫地机器人的软硬件结构分析和



拆解，阐述了可能存在的安全风险。分析了远程控制 WiFi 模块，将扫地机器人变成中间人攻击工具的过程。并演示了的机器人秘密“蠕动”接近目标的攻击场景，说明扫地机器人运动能力带来的特有威胁。安天作为 XCon2015 胸卡友情赞助商，从设计到制作融入了独具匠心的金属电路元素，这次 350 张 XCon 胸卡，是安天微嵌的兄弟连续奋战 20 小时完成焊接测试，加工后又经过了筛选，与桑博士的演讲一样，给参会者留下了深刻的印象。

每周安全事件

类 型	内 容
中文标题	Web.com 网站用户支付卡信息被盗
英文标题	Payment card info of 93,000 Web.com customers stolen
作者及单位	ZeljkaZorz，Help Net Security
内容概述	据报道，Web.com，一家美国著名互联网服务供应商，近 93000 名用户的姓名，地址以及信用卡信息因公司计算机系统遭受攻击而被盗取。 社会安全号和信用卡验证码并未受到攻击，只有支付 Web.com 的信用卡信息受到了影响。该供应商表示，已经与国内知名 IT 安全公司一同调查此次攻击事件。并向受到影响的消费者发送电子邮件通知；此外受影响的消费者将接受一年的信用卡监测，也会获得新的支付卡；同时建议用户密切关注有关信用卡 / 借记卡的可疑的或不正常的活动。
链接地址	http://www.net-security.org/secworld.php?id=18783
中文标题	Uber 为抵御黑客攻击 安全团队扩编 4 倍超 100 人
内容概述	据《金融时报》网站报道，美国打车应用 Uber 表示，为加强数据隐私保护、抵御黑客攻击，甚至保护其办事处和雇员免遭不法分子攻击，Uber 将加强其安全团队，计划到今年年底使该团队员工数量在目前约 25 人基础上扩编制超过 100 人。 今年 4 月，Uber 从 Facebook 公司挖来了乔·沙利文 (Joe Sullivan)，任命沙利文担任 Uber 首席安全官。沙利文在 Facebook 担任首席安全官已有 5 年时间，而此前他的身份则是负责网络犯罪业务的美国前联邦检察官。今年 2 月，Uber 被曝约超过 5000 名司机的个人信息遭到外泄。 沙利文及其团队在 Uber 负责司机的人身安全、信任调查以及包括司机事故调查等安全事务，同时还负责 Uber 的网络安全。
链接地址	http://www.net-security.org/secworld.php?id=18783

恶意代码信息

经安天【CERT】检测分析，本周有 5 个移动平台和 4 个 pc 平台的恶意代码家族值得关注

病毒分类	病毒名称	病毒特点
移动恶意代码	Trojan[Spy]/AndroidOS.SmThief 发现日期：2015.8.17	一类间谍型木马，该威胁会监视系统信息，窃取重要机密。
	GrayWare[AdWare]/AndroidOS.Mmaro 发现日期：2015.8.17	一类广告的灰色软件家族，是恶意广告推广 (威胁较低)。
	GrayWare[AdWare]/AndroidOS.Dianjoy 发现日期：2015.8.17	一类广告的灰色软件家族，是恶意广告推广 (威胁较低)。
	RiskWare[Monitor]/AndroidOS.Babyjc 发现日期：2015.8.18	一类带有监控功能的风险软件，能监控手机流量和行为，搜集用户信息，可能会泄露信息，威胁较低。
	RiskWare[RiskTool]/AndroidOS.Mars 发现日期：2015.8.19	一类风险软件，提供一些带有风险性功能的控件，可能会泄露信息，威胁性较低。
PC 恶意代码	Trojan/Win64.DLLhijack 发现日期：2015.8.16	一类木马家族，会释放恶意软件，窃取用户信息。
	Trojan[Downloader]/Win32.Cryni 发现日期：2015.8.18	一类下载者木马家族，该家族成员会从指定服务器下载恶意应用，安装并运行。
	GrayWare[AdWare]/JS.Znoozer 发现日期：2015.8.18	一类广告推广的灰色软家族，该家族成员是一些 JS 脚本，当浏览网页时时候，会自动运行，弹出广告。
	Trojan[Dropper]/Win32.LuckyMouse 发现日期：2015.8.19	一类捆绑类木马家族，该家族成员运行后会释放其他恶意程序，未经用户授权自动安装，并设置后门。

黑客能够控制电动滑板

Kim Zetter / 文　　安天公益翻译小组 / 译

去年，瑞奇·希利 (Richo Healey) 在澳大利亚墨尔本滑着电动滑板，到一个路口时，滑板冷不丁地停住了，他被甩到了路上。他无法控制滑板，也不知道出了什么问题。滑板没有明显的机械毛病，作为一名计算机安全工程师，他自然地想到了一个场景：会不会是被黑客攻击了？没有多久，他就确定了附近的蓝牙噪音可能是罪魁祸首。这个路口靠近联邦广场，是射频噪音集结地，所以结论是，他没有被黑客攻击，而是周围的蓝牙流干扰了遥控器与滑板的连接。

希利是一家支付公司的安全工程师，他联手同行研究员迈克·瑞安 (eBay 安全工程师) 研究了希利的滑板和其他电动滑板，看看他们是否被黑客攻击。其结果是，他们开发了名为 FacePlant 的漏洞利用代码，能够完全控制电子滑板。“攻击基本上是墨尔本那个路口的射频噪音的合成版本”他说，该攻击能够使滑板停止滑行，或者使其倒退行驶，这两种情况都会使驾驶人甩下滑板。这一研究成果在拉斯维加斯的 DefCon 黑客大会上得以展示。

希利实验用的 Boosted 滑板使用一个应用程序运行，该程序控制着两个 1000 瓦的电动马达。其中一个是体积较小的手持遥控器，驾驶人用它调整滑板的速度 (通过蓝牙低耗能无线技术)；另一个是电池，一次充电可滑行 6 英里。驾驶人按住“滑行”开关，滑板就会保持运动，如果松开该开关，电机就会被切断。

由于蓝牙通信没有进行加密或认证，附近的攻击者可以轻松地插入在遥控器和应用程序之间，迫使滑板连接到他的笔记本电脑。一旦实现了这一点，攻击者就能够使滑板突然停止滑行，使驾驶人被甩出。攻击者还能发送恶意漏洞利用代码，导致车轮突然改变方向，以最快的速度反向滑行，或使刹车失效。当驾驶人位于陡峭的山坡上时，攻击者也可以简单地干扰遥控器和滑板之间的通信，造成刹车失效。

根据美国联邦通信委员会认证蓝牙设备的要求，它必须能够承受干扰。但是，研究人员测试的这 3 个滑板都不能抗干扰。

攻击者蓝牙连接到滑板需要 2 到 10 秒的时间，之后在驾驶人的遥控器重新连接到滑板之前，漏洞利用代码只用 10 毫秒的时间注入。漏洞利用代码能够获取足够的蓝牙连接信息，从而控制遥控器，并用一个脚本使漏洞利用代码自动运行，且速度更快。

“关键是，蓝牙嗅探并不是完全成熟的，如果没有加密和签名，一旦我们获得了连接，也就掌握了滑板。”希利说。

研究人员发现，他们也可以改变滑板运行的最高速度。电动滑板在固件中编码了最高速度，以防止它们速度过快。各个滑板的最高速度不尽相同。

由于Boosted应用程序能够更新固件，所以攻击者可以冒充该应用程序。Boosted 滑板不要求更新其固件被签名，因此研究人员发现，他们可以安装用于消除或改变速度限制的更新，使得能够更快的运行或者只能低速运行。安装更新所需的时间超过2分钟，且要求滑板重启才能生效。但是，此时黑客能够控制滑板，他可以关闭滑板并重启来安装更新。

“一旦你能够编写任意固件，你就可以改变最高速度，改变最低速度，使滑板不受遥控器控制地持续滑行。”瑞恩说。重写固件后，滑板所有者需要刷新固件来重新控制滑板。

“此研究的意图可不是为了找到让驾驶人被甩下滑板的方法而是在于提醒厂商，他们确实有责任给用户做出安全的产品”希利说，“他们应该将缺陷上报机制设置得更加简单，而且应该积极主动地修复缺陷。在电动汽车市场上，我们尚未看到任何的安全性，生产商业没有严肃地对待安全问题。”

去年 9 月，他们将该漏洞报告给 Boosted 公司。但是，到目前为止，该公司还没有修复这一问题。Boosted 告诉研究人员，它计划在周六 Def Con 会议前给出减灾技术。他们还没有与其他厂商沟通，因为他们还在研究这些滑板的漏洞。

但是，这个问题可能不只存在于电动滑板。他们知道市场上至少有一个电动自行车也使用了蓝牙，不过他们还没有研究它。“最坏的情况，你可以随时被甩下滑板。但是，如果自行车被控制全速运行，这将会更危险。”希利说。他说，除了攻击自行车，攻击者还可能攻击驾驶人的电话，并将自行车作为破解手机的支点。

原文名称	Hackers Can Seize Control of Electric Skateboards and Toss Riders
作者简介	Kim Zetter，《连线杂志》一位屡获殊荣的资深记者，研究范围包括网络犯罪、隐私和安全。
原文信息	2015 年 8 月 4 日发布于《连线杂志》，原文地址 http://www.wired.com/2015/08/hackers-can-seize-control-of-electric-skateboards-and-toss-riders-boosted-revo/

安天发布《利用路由表阻止杀软联网样本分析》报告

近期，安天发现了一种通过篡改路由表，使本应发送到杀软 IP 的数据包，发送到错误的网关，防止杀软正常联网的现象，这使得杀软不能进行升级、上报、云查杀，阻止杀软对电脑进行杀毒检测。安天【追影高级持续威胁分析系统】无需更新病毒库，依据行为即可对该恶意程序进行有效检测，下为其自动形成的分析报告。

恶意程序

文件被页面手工提交发现，经由 BD 静态分析鉴定器、美国软件交叉索引 (NSRL) 鉴定器、数字证书鉴定器、可交换信息 (EXIF) 鉴定器、静态分析鉴定器、动态行为 (默认环境) 鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

依据 BD 静态分析鉴定器、静态分析鉴定器、动态行为鉴定器、智能学习鉴定器最终将文件判定为恶意程序。该文件具有以下行为：删除自身；可疑进程名称；遍历进程；复制自身文件；释放 PE 文件；获取驱动器类型；独占打开文件；打开自身进程文件。

文件名	0EE8F1F397A68D94920E3A0362AB0E1F
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	201 KB
MD5	0EE8F1F397A68D94920E3A0362AB0E1F
病毒类型	恶意程序
恶意判定 / 病毒名称	Trojan[PSW]/Win32.Bjlog.dtwr
判定依据	静态分析

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
删除自身	★★★★	可疑进程名称	★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
遍历进程	★	复制自身文件	★★
释放 PE 文件	★	获取驱动器类型	★
打开自身进程文件	★	独占打开文件	★

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=0EE8F1F397A68D94920E3A0362AB0E1F

“爱”的味道温暖安全业界

近期，安全界朋友圈在大量转载一个“专注安全　品味希望”的南俊苹果帖。南俊，曾经是中国电信集团系统集成公司网络信息安全部的高级工程师，负责渗透和风评工作。2013 年 11 月底在北京遭遇车祸，致使他颈椎第 4 椎体以下神经损毁，肩部以下肢体全部瘫痪。时隔两年，这位年轻同行用他的坚强和乐观，给大家带来的不仅是无公害的香甜苹果，更是顽强的意志和坚定的信念。

8 月 20 日，安天采购 289 箱南俊绿色苹果与每位同事分享，希望把这份关爱传递下去，一起为南俊加油、为天津消防员祈福，望每一位处在困难中的人都能“苹”安，幸福。下为南俊本人撰写：

南俊苹果记

“我叫南俊，是土生土长的山西人，说起山西，大家可能会觉得是一个到处弥漫着浓浓醋香的地方，可是在我心里，却是充满苹果甜甜香气的家乡。俺们村是一个名副其实的“苹果村”，家家户户都种苹果，打俺记事起，每到苹果成熟的季节，整个山上里都是苹果的清香味，趁着爹娘不注意溜进苹果园里，随手从树上揪下一个红彤彤的大苹果，咔嚓咬上一口，又脆又甜，这样的味道贯穿了我的整个童年。

师范学院毕业后，我来到了北京打拼，从小在《电脑报》和《电脑爱好者》的熏陶下，我开始了“不当老师的程序猿却是位好工程狮”的北漂生活，每天都在网络的空间里漫无目的奋斗，一次偶然的机会我进入了互联网安全的世界，每天面对着“黑”与“白”的交锋，我也从一枚热衷技术的“小黑”转身成了一名“小白”，我喜欢互联网，更爱充满各种奇葩怪才的网络安全圈。

后来因为一些变故，我暂时离开了我所热爱的互联网安全圈和正常人的生活，这些难熬的日子里，我的“兄弟姐妹”给了我很多的帮助，可并不富裕的我无以为报，只能在苹果成熟的季节给他们送去了一箱俺爹娘亲手种的苹果，没想到大伙儿都觉得很好吃。

朋友们的点赞让我看到新希望，我决定让俺家种植的苹果连上互联网，不光是为了生活，也不光是为了和大家分享我家乡的味道，更是为了让像我这样突然遭受变故的人，看到坚持的希望。