安天周观察

主办：安天　2016 年 2 月 1 日 (总第 27 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天“变革前夜”2015 年终总结及公司年会召开

1 月 27-30 日，安天 2015 年终总结会暨 2016 年会在安天总部哈尔滨举行。公司总部及北京、武汉、深圳等各地研发中心的小伙伴相聚冰城，总结 2015 年的经验和工作，展望 2016 年的布局和发展。本次年会的题目为“变革前夜”，意味着随着安天的规模成长与发展，开始重新调整自身定位。目前安天已经从提供威胁检测技术的实验室风格小团队走向以安天实验室为总部，以企业安全、移动安全业务线为两翼的集团化布局。

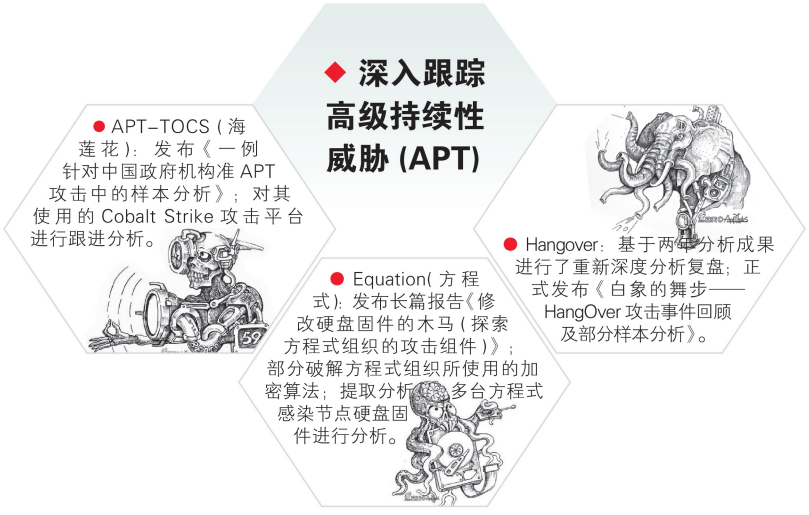
面对威胁情报这一新兴热点，安天移动首先发力，发布了 AVL Insight 移动威胁情报系统，从 AVL Inside 到 AVL Insight，安天正在全力挖掘检测引擎卡位特色和能力优势，使之达成更有效的用户价值。

而安天企业安全则形成了包括探海威胁检测、追影威胁分析、智甲终端防御等产品组成的高级持续性威胁解决方案，并发布了威胁预警监控平台与对接安全产品的业务价值。

新的征途需要新的目标，新的发展需要新的支点。安天必须要用更强有力的决策、执行能力和组织结构对接自己的新目标与使命。这其中必然会有压抑、有阵痛、有割舍，才能看到晨曦，才能走向成功。

下为安天人的乙未年答卷。

◆ 深入跟踪高级持续性威胁 (APT)



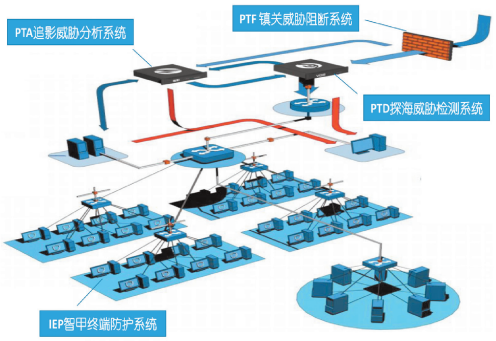
◆ 应对威胁，解决问题

安天 2015 继续坚持在刀锋上的战斗，深入分析具有典型威胁的恶意代码、漏洞等，共形成近 50 余篇分析报告。

◆ 移动安全继续保持检测能力领先优势

2015 年安天移动团队自主研发的手机安全软件 Antiy AVL 在 2015 年上半年的二次评测中，均取得 100% 检出率，成为 2015 年 AV-Comparatives(AV-C) 唯一取得检出率双百成绩的厂商。

◆ 反高级威胁产品和解决方案已经成型



形成流量、边界、终端检测防御与一体，辅助纵深化分析的解决方案。

◆ 服务客户，保障价值

中标东三省直连点监控预警系统建设项目掌握安全态势，及时通报结果，提高应急响应能力及风险预警能力。

中标海关总署信息安全产品采购项目帮助用户“看见”威胁，并认清威胁，让高级威胁无所遁形。

◆ 入围 CV 网络空间安全百强

2015 上半年，安天入围 Cyber security Ventures 网络空间安全百强名单，并在四个季度始终位于上榜中国厂商的最高排名。

每周安全事件

类 型	内 容
中文标题	木马 SlemBunk 再次进化，瞄准全球 Android 手机银行用户
英文标题	Android banking malware SlemBunk continues to evolve
作者及单位	Pierluigi Paganini，Security Affairs
内容概述	专家们最近发现 SlemBunk 再次进化，这次它变身成了一个瞄准全球手机银行用户的强大的 Android 木马。据推测 SlemBunk 的进化之快可能源于组织性的犯罪。这个安卓木马背后的组织已经将至少 31 个不同的银行目标和 2 个移动支付服务供应商作为恶意软件的目标。现在检测到的最新变种是通过驱动下载入侵到手机里，它将目标指向了那些访问色情网站并下载的用户。新版本的 SlemBunk 通过向色情网站的用户频繁弹送下载一个 Adobe Flash 以查阅更多色情图片视频的提示，诱导用户下载恶意软件。为了保护您的设备免受这种威胁，专家建议：不要从第三方应用商店安装 app；保证安卓设备更新。
链接地址	http://securityaffairs.co/wordpress/43604/malware/slembunk-banking-trojan.html

每周值得关注的恶意代码信息

经安天检测分析，本周 10 个移动平台和 4 个 PC 平台的恶意代码家族值得关注

平台分类	关注方面	名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	RiskWare/Android.benbenidc.a[exp，prv]2016-01-25	该应用程序运行后会上传账号密码等隐私信息，类似注册登陆的功能，包含发送短信及拦截短信模块，存在一定的资费损耗和隐私泄漏风险。(威胁等级低)
		Trojan/Android.androidhome.a[pay，rog，rmt]2016-01-26	该应用程序运行时，会请求指令，根据指令发送扣费短信，拨打指定电话，下载安装指令 app，下载升级包。获取 root 权限，禁用安全软件，监听用户收件箱，获取用户接收的短信，并将短信设置为已读，删除扣费回执短信。造成用户资费消耗，建议用户谨慎使用。(威胁等级中)
		Trojan/Android.TensterCare.a[prv，spy]2016-01-27	该应用安装无图标，运行后远程接收短信指令，获取地理位置相关信息上传到指定服务器，并通过短信向远程控制号码反馈运行结果，造成用户隐私泄露，建议卸载。(威胁等级中)
		RiskWare/Android.GppSpy.a[prv] 2016-01-28	该程序为一款阅读器应用，包含开机自启、监听短信、监听电话等风险代码，可能造成用户隐私泄露，建议谨慎使用。(威胁等级低)
		RiskWare/Android.Salestracker.a[sys] 2016-01-28	该应用可能为手机销售统计跟踪程序，运行后会拦截特定短信，有一定风险，建议谨慎使用。(威胁等级低)
		Tool/Android.TrickyTaka.a[prv，rmt，spy]2016-01-29	该类应用安装会要求激活设备管理器，然后置顶勒索界面勒索付费。后台监听短信，接收短信指令修改手机设置，接受联网指令，上传用户隐私，发送短信，造成用户隐私泄露及资费损耗，同时还会影响用户用机体验。(威胁等级低)
	较为活跃的样本	Trojan/Android.Downloader.bf[exp]	该应用植入在游戏下载器中，私自下载恶意 apk，推广色情广告，会造成用户资费损耗，建议卸载。(威胁等级中)
		Trojan/Android.SmsSpy.n[prv]	该程序运行会监听短信，将短信信息发送到指定邮箱，另外还会拦截指定号码的短信，造成用户隐私泄露。(威胁等级中)
		Trojan/Android.InfoStealer.s[prv]	该应用运行后诱导用户点击，窃取用户手机固件信息、电子邮箱账号、通讯录等隐私信息，建议卸载。(威胁等级中)
		Tool/Android.SMSBomber.t[exp]	该程序是一款短信炸弹工具，运行后输入攻击号码，以发送验证码的消息形式实现对手机号的短信轰炸，会造成资费消耗，建议谨慎使用。(威胁等级中)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	CVE-2012-0158 漏洞	该漏洞是一个栈溢出漏洞，在 MSCOMCTL.OCX 中存在错误，可被利用破坏内存，导致任意代码执行，主要通过电子邮件进行传播。(威胁等级高)
	较为活跃的样本	Trojan[Dropper]/Win32.Dycler.ah	此威胁是一种木马类捆绑程序，它安装恶意程序到受害者电脑。这种类型的恶意程序通常保存到受害者的驱动 (Windows 目录，Windows 系统目录，临时目录等)，并在没有任何通知的情况下启动。(威胁等级中)
		GrayWare[AdWare]/Win32.AirAdInstaller.hr	此威胁是一类推送广告的木马类灰色软件程序。一般通过捆绑于其他软件的安装文件中，或是通过挂在网站上吸引用户点击进行传播。广告软件在安装进用户系统后，会隐藏自身的存在，防止被用户卸载。(威胁等级低)
		GrayWare[AdWare]/Win32.Gamevance.aar	此威胁是一种广告类木马类程序。用户为了换取免费游戏服务，同意通过软件的文本链接，横幅和弹出窗口的形式接收广告。这些广告可能会弹出无论是在前面或您的浏览器后面，通常认定为 Gamevance 广告。所选择的广告是根据你的网页浏览历史记录和有关您的利益由您访问最频繁的网站确定。(威胁等级低)

联邦政府督促汽车制造商与黑客合作

Andy Greenberg/ 文　安天公益翻译小组 / 译

美国交通部 (DOT) 及其汽车安全分支美国高速公路安全管理局 (NHTSA)，都意识到了联网汽车和卡车存在能够被黑客破解的漏洞。现在，他们正督促汽车巨头也意识到这一点。

近日，交通部和几乎所有的主要汽车制造商，包括克莱斯勒、通用汽车公司和特斯拉，发布了一份关于“积极安全原则”的声明，他们将在 2016 年推行该原则，以消除 2014 年和 2015 年震撼汽车工业的安全和工程丑闻。该声明包含网络安全的新方法，包括通过汽车产业信息共享和分析中心共享网络安全威胁数据，推动汽车供应商加入信息共享合作伙伴关系，并开发一套共享的网络安全“最佳实践”。也许最重要的是，交通部和 18 个汽车制造商说他们将“开发适当的方法与网络安全研究人员交互，将其作为识别和修复网络威胁的额外工具。”换句话说，更密切地听取发现车辆可利用漏洞的友好黑客的意见。一位匿名的交通部发言人说：“我们认为这是相当显著的立场改变：目前，业界已经采用各种方法与发现汽车 / 卡车安全漏洞的独立研究人员进行交互。我们认为，更密切地与他们开展合作是非常积极的第一步。”

交通部和汽车行业提出的新安全原则萌芽于交通部长安东尼·福克斯与业界领导人今年 12 月初举行的会议。这次会议的目的是解决最近几年的汽车召回事件、事故和丑闻，包括通用汽车和克莱斯勒启动故障及大众汽车的排放作弊软件。该交通

部发言人称，会议的另一个议题是安全研究人员查理·米勒和克里斯瓦·拉塞克演示的吉普车攻击，该演示证明黑客可以远程控制 2014 版吉普切诺基的变速器和刹车。这震惊了汽车和安全行业，并导致克莱斯勒在几天后宣布召回 140 万车辆。

得益于研究人员的演示，该漏洞在被用于恶意目的之前就被修复了，这可能导致其他汽车制造商重新考虑他们与独立黑客们的关系。本月早些时候，通用汽车公司悄悄公布了一个漏洞披露项目，向安全研究人员提供了一些保证：如果他们向通用汽车公司报告其黑客研究的结果，他们就不会遭到起诉。安全创业公司 HackerOne（一家致力于帮助企业和独立研究人员协调安全漏洞披露的公司）主持了通用公司的声明，称：“如果您有通用汽车产品和服务的安全漏洞的相关信息，我们希望收到您的反馈。我们非常重视您的工作产生的积极影响，提前对您的贡献表示感谢。”

发现吉普车漏洞的黑客之一查理·米勒对交通部的声明和通用汽车公司的漏洞披露项目仍持怀疑态度。他指出，通用汽车要求研究人员对他们提交的报告进行秘密，但是没有提供任何漏洞修复的时间表。而且公司也没有提供所谓的“漏洞赏金”，即一些公司为漏洞信息支付的奖金。对于汽车制造商和交通部提出的新承诺，他同样表示怀疑。“我希望，安全社区、制造商和 OEM 厂商之间会有更多的互动。”他说，“这个只能眼见为实。”

在交通部内部，美国高速公路安全管理局 (NHTSA) 至少显示出了网络安全新关注点的迹象。当加利佛尼亚大学圣地亚哥分校和华盛顿大学的研究人员披露了一种能够控制启用 OnStar 功能的通用汽车的黑客技术后，NHTSA 允许通用汽车公司用 5 年的时间来完全修复该漏洞。与此相对地，当《连线杂志》在 7 月份报道了吉普车攻击新闻后，NHTSA 立即要求克莱斯勒发布正式召回通知。

除了致力于改善安全社区与汽车制造商之间的关系，NHTSA 承诺会拿出一套完整的汽车网络安全最佳实践。交通部发言人表示，这些最佳实践将会“很快发布”。虽然他不排除如果更严重的安全漏洞被发现会导致新的网络安全规定或更多召回，但是他认为，与业界合作可能是一种更有效的跟上移动安全领域步伐的方式。“从监管的角度来看，网络安全是一个很困难的领域，因为它变化非常快。”他说，“与业界一起创建指导原则和最佳实践，将能够更迅速地采取行动。”

原文名称	Feds Prod Automakers to Play Nice With Hackers
作者简介	Andy Greenberg，《连线杂志》的资深作家，研究领域涵盖安全、隐私、信息自由和黑客文化。
原文信息	2016 年 1 月 15 日发布于《连线杂志》，原文地址 http://www.wired.com/2016/01/feds-prod-automakers-to-play-nice-with-hackers/
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，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。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。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。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，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。

安天 AVL Team 发布《新“马”新气象，拦你没商量》报告

俗话说新年新气象，但忙着“辞旧迎新”的并不只有我们。众所周知，短信拦截马在手机恶意事件中早已屡见不鲜，但因其明显的趋利性，不仅数量在不断攀升，技术手段也在不断升级。

揭开真面目

近日，安天移动安全团队 (AVL Team) 接到一例用户的可疑短信鉴别请求。随后，安全人员立即对该短信内容进行了响应分析。经分析发现，用户一旦点击短信中的 URL，就会导致下载木马并诱导用户安装。通过详细分析，安全人员发现该木马存在以下恶意行为：

1. 诱导用户激活设备管理器，隐藏图标，利用虚假卸载窗口躲避用户卸载。
2. 发送监控短信到主控手机。
3. 后台通过邮件上传用户通讯录及短信信息等隐内容。
4. 拦截用户短信并转发到主控手机上。
5. 接收远程短信指令，执行恶意行为。
6. 删除短信。
7. 手机系统高于 4.2.0. 时，木马后台私自发送短信时设置手机为静音模式。

行为趋势分析

通过对此拦截马进行跟踪分析，以及抽样分析近期出现的拦截马，安全人员发现以下几点趋势：

1. 使用 360，腾讯，阿里等最新的加固方式，且占比不断增大。
2. 对拦截马的使用进行期限设定。
3. 对拦截马自身进行证书效验防止他人篡改。
4. 以伪装成中国移动相关的应用名称最多，但同时伪装成“相片”“资料”类应用名的拦截马数量增长势头不断显现。

如何防护

1. 珍惜生命，远离山寨。拦截马一般通过钓鱼、诱骗、欺诈等方式诱导用户装上木马，建议用户保持良好的上网习惯，不要在不知名的应用市场下载应用。
2. 好奇害死猫，谨慎为好。不要随意点击任何短信中的链接，包含但不限于短信内容含“资料”“相册”“中国移动”等信息。
3. 切勿中了“熟人”的套。对“熟人”发送的带有 URL 的短信要格外警惕，因为可能他的手机已中毒。
4. 选用正规厂商的手机安全软件很有必要。AVL Pro 目前已经可以对该木马进行全面查杀。（报告原文：http://blog.avlyun.com/2015/12/2634/malware/）

高级威胁

本期第二版值得关注的【CVE-2012-0158 漏洞】是一个栈溢出漏洞，在 MSCOMCTL.OCX 中存在错误，可被利用破坏内存，导致任意代码执行，主要通过电子邮件进行传播。安天【追影高级持续威胁分析系统】无需更新病毒库，即可实现对上该漏洞进行有效检测，下为其自动形成的分析报告：

文件被网络威胁感知类设备发现，经由 BD 静态分析鉴定器、YARA 自定义规则鉴定器、美国软件交叉索引 (NSRL) 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。最终依据动态行为鉴定器、智能学习鉴定器将文件判定为高级威胁。

该文件具有以下行为：仿冒 SVCHOST；其他进程写入可疑数据；利用漏洞释放 PE 文件；格式漏洞；隐藏文件；增加 runonce 自启动项；创建互斥体 (mutex)；释放 PE 文件；获取系统内存；文档篡改；访问 DNS；获取系统版本；创建挂起的进程；访问其他进程内存；遍历进程；创建特定窗体；获取驱动器类型；独占打开文件；打开自身进程文件；获取主机用户名称；获取计算机名称；查找特定窗体；请求加载驱动的权限。同时，该文件利用了 CVE-2012-0158 漏洞。

文件名	inv.rtf.zy
文件类型	Document/Microsoft.RTF[:Rich Text Format]
大小	1.34 MB
MD5	5F8C39C4869DC8B2C5E4D040C290C757
病毒类型	高级威胁
恶意判定 / 病毒名称	Trojan[Exploit]/Win32.CVE-2012-0158
判定依据	智能学习

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
仿冒 SVCHOST	★★★★	其他进程写入可疑数据	★★★
格式漏洞	★★★★	利用漏洞释放 PE 文件	★★★★
隐藏文件	★★★★		

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
增加 runonce 自启动项	★	创建互斥体 (mutex)	★
隐藏文件	★★	释放 PE 文件	★
文档篡改	★★	获取系统内存	★★
创建挂起的进程	★★	访问 DNS	★
遍历进程	★	获取系统版本	★★
创建特定窗体	★	访问其他进程内存	★
获取驱动器类型	★	独占打开文件	★
打开自身进程文件	★	获取主机用户名称	★
查找特定窗体	★	获取计算机名称	★
请求加载驱动的权限	★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=5F8C39C4869DC8B2C5E4D040C290C757