安天周观察

主办：安天　2015 年 11 月 16 日 (总第 16 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天 AVL 杀毒引擎正式入驻 MIUI7

10 月 27 日，小米 MIUI 7 稳定版正式开放升级，全新的病毒扫描模块支持切换双杀毒引擎。除国内某知名厂商的产品外，由安天 AVL 移动安全团队独立研发的“安天 AVL 移动反病毒引擎”正式进驻 MIUI 7，经过数月内测与开发版本的沉淀，成为可供小米终端用户直接选用的安全引擎。

2013 年，安天移动反病毒引擎 AVL SDK for Mobile 凭借全年最高平均检出率，获得国际权威测试机构 AV-TEST 颁出的年度移动设备最佳保护奖，成为首个在国际反病毒领域获得此重量级年度奖项的亚洲厂商。

2015 年，在著名安全软件测试机构 AV-Comparatives(简称 AV-C) 公布的《移动安全软件评测报告》中，又成为唯一一家在上半年取得 2 次 100% 检出率的厂商。

目前，猎豹、LBE、Trustlook 等著名安全厂商选择了安天作为本地引擎合作伙伴，通过这些合作伙伴，安天引擎为接近一亿手机用户提供了病毒检测服务。而此次 Rom 大厂 MIUI 系统与 AVL 反病毒引擎达成合作，再次印证了行业内对安天专业能力的肯定。

安天党支部委员会正式成立

近日，经中共海淀区委海淀园工委组织部批复：北京安天电子设备有限公司符合成立“中共党支部委员会”的一切条件，**安天党支部委员会正式成立！**作为网络安全厂商，安天深感责任重大，更应该积极落实党建工作，充分发挥党在企业中的政治核心作用，发挥党指导下的安全企业的先锋模范作用，为打造标准化的党建工作、绿色健康的网络安全环境做出应有的贡献。

会议速递

第四届全国网络与信息安全防护峰会 (Xdef) 即将召开

第四届全国网络与信息安全防护峰会将于 11 月 19 日至 20 日，在湖北武汉举行。本次峰会由空天信息安全与可信计算教育部重点实验室主办，武汉大学计算机学院承办。安天武汉研发中心总工程师乔伟将于 19 日发表题为《面向威胁的移动反病毒工程化体系思考》的演讲，与各位专家交流经验。

FSI2015 暨第八届中国互联网安全研讨会 (ISF) 召开在即

第八届中国互联网安全研讨会 (ISF) 即将于 11 月 26 日至 27 日，在上海召开，主题为“新互联网金融安全”，由 CISRG 主办，安天实验室和 AVL 反病毒引擎开放平台协办。今年的研讨会将由 ISF 跃升为 FSI，从互联网安全论坛 (Internet Security Forum) 成为了安全创新之未来 (Future of Security Innovation)。会议期间，安天代表马志远将发表题为《多方联动打击社工诈骗》的演讲，同与会专家分享工作经验。

安天选派三位讲师参加东盟网络安全研讨会

11 月 3 日至 5 日，由工业和信息化部国际合作司主办，国家互联网应急中心 (CNCERT) 承办的第七届“中国 - 东盟网络安全研讨会”在北京召开。

11 月 4 日，来自缅甸，新加坡等 9 个东盟国家的应急响应组织代表参加了会议同期举办的网络安全技术培训环节。在本次培训中，由安天选派出的三位在安全研究和应急响应方面具有经验的工程师担任本次培训活动的讲师。

安天安全研究与应急响应中心 (安天 CERT) 病毒分析工程师贾琼发表了题为《关于擦除 MBR 的多事件关联分析》的演讲。介绍了关于重写 MBR 的四事件的关联分析，特别分析了四个事件的静态信息、动态信息、功能、关键代码的相似性，并指出，利用多插件、拥有多阶段、高复杂度攻击平台可能会在将来的一段时间内成为一种流行攻击方式。工程师白淳升发表了题为《APT 分析技术和案例研究》的演讲，介绍了一些常用 APT 事件分析技术，并引用安天在 APT-TOCS、APT-RATS 和 APT-xxHunter 等几起 APT 攻击事件中的分析方法加以说明。安天移动安全团队张丽红则侧重于移动互联网安全，分享了移动互联网的主要威胁、移动恶意代码对抗技术、移动病毒发展史、移动恶意代码逆向分析方法及分析工具等内容。

会议过后，在场代表向安天工程师提问并交流了相关问题，共同探讨了互联网安全领域的发展状况和技术趋势。

每周安全事件

类 型	内 容
中文标题	7000 万份囚犯通话记录数据遭泄露
英文标题	Database of 70 million prisoner phone calls breached，leaked
作者及单位	ZeljkaZorz，Help Net Security
内容概述	据 The Intercept 报道，匿名黑客盗取了美国监狱 7000 多万份的囚犯电话记录数据，这些数据来自美国 37 个不同的州，其中至少有 14000 份是囚犯与其律师的对话记录；另外，囚犯与检控官的通话记录也遭到泄露。 截止目前，美国监狱电话记录服务的主要供应商 Securus 发表声明称，据公司和相关执法机构的调查，并未发现遭到攻击的证据。
链接地址	http://www.net-security.org/secworld.php?id=19100

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周 8 个移动平台和 6 个 PC 平台的恶意代码家族值得关注

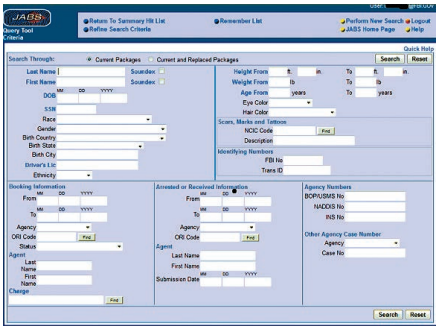
平台分类	关注方面	名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.dwreload.a[prv，spy] 2015-11-05	该应用程序安装会隐藏图标，监控用户地理位置信息、本机号码、通话记录、短信记录、通话录音并通过邮件或 FTP 方式上传这些数据，造成用户隐私泄露。(威胁等级中)
		Trojan/Android.lazyor.a[prv，exp] 2015-11-07	该应用程序运行后释放子包程序，隐藏自身，伪装成系统应用，自身会联网获取指令，向指定号码发送指定短信。释放子应用程序会打开色情页面，无实际意义，对用户的安全造成极大损害，建议用户立即卸载。(威胁等级中)
		Trojan/Android.SysChecker.e[exp] 2015.11.9	该应用程序安装无图标，触发启动释放恶意子包，联网下载未知应用静默安装，拦截回复指定短信，可能会造成资费损耗，建议卸载。(威胁等级中)
		G-Ware/Android.joygame.a[exp] 2015.11.11	该应用程序存在恶意代码，安装运行之后会激活设备管理器，使用户不能正常卸载。使用过程中可能会自动发送短信购买付费道具，并拦截回执短信。具有一定的流氓行为，为避免资费的额外损失，请不要安装该软件。(威胁等级中)
	较为活跃的样本	Trojan/Android.SmsThief.y[prv]	该应用伪装成其他软件，安装运行之后窃取用户短信收件箱详细数据联网上传，并删除指定短信，拦截短信，造成用户隐私泄露。(威胁等级中)
		Trojan/Android.Tiak.b[exp，rog]	该应用安装无图标，监听开机广播自启动，私自下载恶意应用，并通过监听手机行为释放广告，建议用户立即卸载。(威胁等级中)
		Trojan/Android.Fakegupdt.y[rog，exp]	该程序伪装成游戏及笑话应用，实际安装无图标，后台发送订阅短信，下载 apk，通过通知栏伪装系统更新诱导用户点击安装，后台拦截指定短信消息并自动回复，造成用户资费损耗，建议立即卸载。(威胁等级高)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 内存破坏漏洞 CVE-2015-1641	攻击者可以构造嵌入了 docx 的 rtf 文档进行攻击。word 在解析 docx 文档处理 displacedByCustomXML 属性时未对 customXML 对象进行验证。(威胁等级中)
	较为活跃样本	Trojan/Win32.VB.awcd	此威胁是一种木马类程序，运行后连接网络，访问指定的广告页面，进行刷流量。查找 [360 浏览器][世界之窗浏览器][IE 浏览器]，回传访问信息。(威胁等级中)
		Trojan[Backdoor]/Win32.Sdbot.aepa	此威胁是一种木马类后门程序，运行后可能会获取系统信息，用户信息等，发送数据到远程服务器，等待控制者命令。(威胁等级中)
		Trojan[Downloader]/Win32.VB.axph	此威胁是木马类程序，使用 VB 开发，运行后会连接网络，下载其他恶意程，还会获取系统信息，用户信息等，发送数据到远程服务器。(威胁等级中)
		Trojan[PSW]/Win32.Exeron.g	此威胁是一种木马类程序，该恶意代码会搜到系统中有用信息和文件上传到服务器，还带有键盘记录功能。(威胁等级中)
		Trojan/Win32.Inject.nuefa	此威胁是一种木马类程序，运行后会注入其他进程，并在其他进程中申请内存，查找指定浏览器进行注入访问代码。(威胁等级中)

CIA 电邮黑客再次来袭，攻击执法机构门户网站

Kim Zetter / 文　　安天公益翻译小组 / 译

近日，入侵 CIA(美国中央情报局) 局长约翰·布伦南个人电子邮件帐户的黑客再次来袭。这个名为 Crackas With Attitude 的攻击组织声称，他们能够访问更重要的目标——授权访问逮捕记录和其他敏感数据的执法门户，包括有关活跃射手和恐怖分子事件的信息共享工具，以及执法人员之间实时聊天的系统。

CWA 黑客发现了一个漏洞，使他们能够访问原本只提供给 FBI 和其他执法机构的私有门户网站。这些门户网站反过来又向他们提供了十几个用于信息共享的执法工具。CWA 目前不肯透露该漏洞的信息，但是其中一名自称为 Cracka 的黑客向《连线杂志》提供了他们访问美国逮捕记录数据库 JABS 的截图。



最新的漏洞非常严重，一旦黑客进入该系统，就能够直接访问逮捕记录。这对于八卦网站和其他媒体来说，是很有价值的信息。更重要的是，该系统还包括根据法院密令执行的逮捕，这些逮捕信息可能在数月或数年之内都不会公开，例如恐怖分子嫌疑人、团伙成员和毒品犯罪嫌疑人的逮捕信息。

Cracka 告诉《连线杂志》，他们能够查看 JABS 中杰里米·哈蒙德的逮捕纪录。哈蒙德是一名 Anonymous 黑客行动主义者，目前正在服刑。但是，他们并没有获得其他犯罪记录。因为他们不是要伤害无辜的人，只是对政府而已。

Cracka 没有透露用于访问门户网站的漏洞，因为，他们还在尝试从中获取更多的信息。通过这个有漏洞的执法门户网站，他们获得了约 3000 名政府雇员的姓名、职称、电子邮件地址和电话号码，并于周四将这些信息张贴到 Pastebin 网站。他们表示，这只是多部分泄漏行动的其中一部分。Cracka 向《连线杂志》提供了位于该门户网站主页上的敏感工具列表，包括：

企业文件传输服务：安全地共享和传输文件的网络接口。

网盾联盟：FBI 网络安全伙伴关系计划。

DFS 测试和 eGuardian 培训：对这两者没有说明。

IC3：接收、开发和指代犯罪分子刑事起诉的工具。

IDEAFX：面向跨组织团队的基于 web 的文件 / 文件夹共享功能。

Intelink：综合情报的传播和合作的安全门户。

Intelink IM：为登录到执法系统的用户提供相互间的实时聊天。

司法企业文件共享：该应用程序使用 http://box.com 作为基础技术构建，提供云托管能力，实现文件 / 文件夹共享的更高的稳定性和增长。

除了这些，该门户还能够访问：

特殊利益集团：描述为受控 / 结构化的访问领域，使专门机构或学科共享和存储信息。

虚拟命令中心：行动和事件的实时协作工具，包括活跃的射手事件、搜查令、自然灾害、儿童绑架、恐怖袭击和威胁，以及特殊事件。

全国数据交换 N-DEx：向地方、州、部落和联邦刑事司法机构提供一种机制，在全国范围内共享、搜索、关联和分析跨辖区的信息。

全国团伙情报中心：多机构的协作，整合来自地方、州和联邦执法机构的团伙的信息，并作为团伙的信息和分析支持的集中情报资源。

特别关注人士的数据库 RISC：允许执法人员在大街上使用移动标识 (ID) 设备，针对有限的指纹记录数据库执行“lightsout”快速搜索。

RISSNET：提供对各种执法敏感的、人员安全和公共安全资源的及时访问。

ViCAP 网络全国犯罪数据库：行为和调查信息的数据库，包括凶杀、性侵、失踪人员和不明身份人员遗体案例。

活跃射手资源页：可供执法机构和全国各地的其他第一反应者使用的材料交流中心。

恶意软件研究人员：自动化工具，分析可疑恶意软件样本，并迅速反馈有关样本给用户，使他们能够了解样本。

国土安全信息网络或 HSIN：共享敏感但非机密的信息。

eGuardian：允许执法机构、执法支持人员和部队保护人员报告、跟踪和共享与恐怖主义、网络或其他犯罪活动可能有关的威胁、事件和可疑活动。

Cracka 告诉《连线杂志》，他并不是为了名气或好玩才执行攻击的，他这么做是为了巴基斯坦。Cracka 称，目前他们没有计划泄漏更多的信息，至少不会在短时间内这样做。

原文名称	CIA Email Hackers Return With Major Law Enforcement Breach
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 11 月 6 日《连线杂志》发布，原文地址 http://www.wired.com/2015/11/cia-email-hackers-return-with-major-law-enforcement-breach/
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。

安天追影首次发现双平台流氓推广移动应用

近日，安天追影分析小组利用探海设备对网络犯罪活动进行监控的过程中发现了一例跨平台恶意推广的恶意代码。该恶意代码通过 Windows 平台利用 USB 连接，向手机推送应用，当用户使用 Android 手机通过 USB 与 PC 联接时，恶意程序会安装 Android USB 驱动包，通过 adb 与手机进行通信，命令把 Windows 平台上的 apk 文件安装到手机中。

安天技术人员对样本进行了分析，该样本是一个标准的 PE 程序，运行时无 GUI 界面，程序在后台运行时会联网下载 Android 手机 USB 联接 PC 时的驱动程序，以及用来对 Android 应用程序进行安装的 adb 指令相关文件。程序在后台通过联网 (http://222.186.60.89：1123/?action=getFileDL&files=deps.3) 请求服务器返回相应文件下载地址，进行二次联网后下载相应的文件到 PE(exe，dll) 程序的目录下。当用户使用 Android 手机通过 USB 与 PC 联接时，程序会尝试通过 dpinst.exe 安装与 adb 相关的驱动程序。程序会继续联网访问 http://222.186.60.89：2222/?api=giveApkList，获取后台要推送的 app 程序 list，并下载相应的 app，存放在本地的隐藏目录 app 下。

在 Windows 平台上，程序可以通过 adb 命令与 Android 手机通讯。比如 adb install 命令把 Windows 平台上的 apk 文件安装到手机中。程序在下载过程中会尝试启动 adb 命令当中的 install 指令来对存放在本地的 app 程序进行静默安装。由于 adb install 命令并不需要用户确认，因此该恶意代码可以悄无声息的把应用安装到手机上，而用户完全不知情。对安装的应用进行简单分析后可发现，当前推送的应用程序以游戏应用为主，部分是白样本，灰样本当中以 qyPay.a 和 WeimiPay.a 支付插件为主。

程序运行时，会通过 http://222.186.60.89：2222/?api=giveVersion 来请求最新版程序的下载地址，若有新版本则会进行下载替换。安天技术人员对 222.186.60.89 这个域名进行检索后，发现其中部分样本为 newpaysdk76 恶意家族。这个家族的特点是，在运行时会联网上传用户手机固件信息，获取配置文件，私自发送注册短信、模拟点击登录远程服务器发送付费短信、拦截回执短信并自动回复，给用户带来经济损失。

通过相关以上分析，可以确定 PE 程序以及相应的域名信息都是用来为后台流氓推送和刷流量服务。这些通过 PC 程序进入 Android 生态圈的恶意程序，会随着广告流量逐利性的增强而愈演愈烈。

恶意程序

安天【追影高级持续威胁分析系统】无需更新病毒库，即可实现对上述恶意程序进行有效检测，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、美国软件交叉索引 (NSRL) 鉴定器、可交换信息 (EXIF) 鉴定器、数字证书鉴定器、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。

依据动态行为鉴定器最终将文件判定为恶意程序。

该文件具有以下行为：连接异常端口；创建特定窗体；请求调试权限；请求加载驱动的权限；获取 socket 本地名称；增加 run 自启动项；查找特定窗体；获取计算机名称；连接网络。

文件名	E5C544BD4D928A2E5A5E105907C8A3E8
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	487 KB
MD5	E5C544BD4D928A2E5A5E105907C8A3E8
病毒类型	恶意程序
恶意判定 / 病毒名称	Trojan/Win32.Appmain.a
判定依据	动态行为

◆ 危险行为

行为描述	危险等级
连接异常端口	★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
创建特定窗体	★	请求调试权限	★
获取 socket 本地名称	★	请求加载驱动的权限	★
查找特定窗体	★	增加 run 自启动项	★
连接网络	★	获取计算机名称	★

◆ 网络监控

IP 地址	端口
222.186.60.89	8823

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=E5C544BD4D928A2E5A5E105907C8A3E8