安天周观察

主办：安天　2015 年 11 月 30 日（总第 18 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加“FSI 2015”发表主题演讲

2015 年 11 月 26 日至 27 日，由 CISRG 主办，安天及 AVL 反病毒引擎开放平台协办的“FSI 2015”，暨第八届中国互联网安全研讨会在上海举行。本次会议选取“新互联网金融安全”为主题，邀请到国内外数十位业内专家发表演讲，吸引了近 500 名信息安全技术爱好者前来参与。

安天移动研发中心马志远在 27 日发表了题为《基于威胁情报的企业安全价值观》的演讲。他介绍说，目前，部分企业普遍存在使用安全技术与实际安全威胁不对称的问题。主要包括企业的安全认知与用户威胁场景的不平衡；企业业务发展与企业安全意识的不平衡；安全诉求和威胁与实际安全能力的不平衡等等。想要消除这种盲人摸象般的不平衡状态，马志远认为重点在于“因地制宜”，要基于威胁情报数据，结合企业业务场景，对企业的安全问题进行有针对性的量化和度量，选择合理化的安全策略，这样才能使企业达到去不平衡化的目的。

报评

『沉淀与分享』移动互联网安全的捍卫者

2007 年，安天武汉研究小组成立，迅速确定以移动安全这一新兴领域为入口点，从此开始了新威胁的探索之旅。回顾过去的八年，有代码转化为引擎和工程能力的快意淋漓；也有很多与病毒短兵相接的应急响应，更多的则是经验与心得的积累。2012 年，我们将团队在移动安全领域的文献成果编撰成册，与业内人士分享。

最近两年，移动互联网的安全问题已变得愈发严峻，如履薄冰。2013 年预言的恶意代码加壳技术在 2014 年兵临城下；2014 年深度分析的 Android 内核级恶意代码在 2015 年卷土重来；2015 年年初披露的广告件 SDK 的所揭示的关联问题，也在 2015 年的下半年伴随着 XcodeGhost 和 Wormhole 的事件纷至沓来。

在此过程中，我们也遇到了各种不同的对手，有类似于短信拦截木马“相册”这种编写简单，但却给用户造成很大危害的恶意代码；亦有像 XcodeGhost 这种通过工具链污染对应用开发者、用户等造成严重后果的恶意代码。我们既关注具体的威胁，也对像广告件、恶意色情应用、具有情报价值的窃密工具等进行了分析总结，深入研究，以期望从中找到更多应对威胁的新方法。我们还对移动恶意代码以及其带来的安全威胁做了更细粒度的分析和思考。

2014 年初，安天的 AVL 移动反病毒引擎获得了全球著名的反病毒产品评测机构 AV-TEST

（下转第四版）

安天编印《移动安全专题第二分册》

安天近期编印了《移动安全专题第二分册》并在 FSI 会议期间向参会嘉宾发放。该技术文章汇编涵盖了 2014 年—2015 年间安天在移动安全领域的技术文献报告，主要包括恶意代码分析、会议报告、技术研究、专题报告四大部分。其中，恶意代码分析部分主要收录了包括 XcodeGhost 和“相册”木马在内的多篇重要的移动恶意代码分析报告。会议报告部分主要收录了 AVL Team 在多个业内安全会议进行的经验分享。技术研究部分主要收录了安天做过的一些分析尝试，包括：篡改脚本的流氓插件、利用 Mono for Android 开发的恶意代码、执行 Lua 脚本的 Android 恶意程序等。专题研究部分主要收录了近两年安天对 Android 恶意代码、广告件、恶意色情应用、具有隐私窃取行为的工具等趋势和特点的总结。

从 2006 年至今，安天技术文章汇编共印发 11 卷，包括《热点事件分析》、《移动安全分册》、《工控安全分册》、《专题报告分册》、《APT 专题分册》、《文献翻译分册》等以及部分英文版分册，印刷 60 余次，总印数超过 35000 多册，全部免费在各大安全会议发放，与同行分享。

安天举办健康知识讲座

11 月 25 日，在员工年度体检之后，安天哈尔滨总部举办了一场实用的健康知识讲座。

哈工大医院体检中心金主任对安天员工的体检情况进行了总结，对一些常见的疾病进行了介绍，对员工体检结果的问题进行了解答，并在讲座后进行一对一的健康咨询。针对脂肪肝的发病率较去年相比明显提高，以及 IT 行业的整体健康问题，建议大家要合理饮食，保持运动。

每周安全事件

类 型	内 容
中文标题	喜达屋集团旗下 54 家豪华酒店遭 PoS 恶意软件植入
英文标题	PoS malware hit 54 Starwood luxury hotels
作者及单位	ZeljkaZorz，Help Net Security
内容概述	近日，喜达屋集团旗下在北美地区的 54 家酒店支付系统遭到恶意软件感染。这种恶意软件专门收集支付卡信息，如持卡人姓名、支付卡号码、安全码和有效期等。现没有任何证据证明其他客户信息，如联系方式和 PINs 等，受到此次事件的影响。受影响的酒店已经及时采取措施，确保客户支付卡信息的安全，使这种恶意软件无法对在喜达屋酒店使用支付卡的客户造成威胁。 此外，该集团建议在北美地区酒店入住过的顾客仔细查看支付卡账单，若受到影响应及时通知相关银行或发卡机构；公司将对受影响的客户免费提供为期一年的身份保护与信用监控服务。
链接地址	http://www.net-security.org/malware_news.php?id=3158

每周值得关注的恶意代码信息

经安天检测分析，本周 9 个移动平台和 5 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.happ.a[exp，rmt] 2015.11.20	该应用运行后加载释放子程序，联网获取指令，执行私发短信、利用通知栏恶意推送广告，还含有提权代码，会静默安装卸载指定程序。(威胁等级中)
		Trojan/Android.Hongbao.a[exp] 2015.11.20	该应用运行即遍历联系人并向其发送包含特定内容链接的短信，造成用户资费损失。(威胁等级中)
		Trojan/Android.HUD.b[prv，fra，spy] 2015.11.21	该应用为间谍软件，伪装成谷歌应用，运行后会隐藏图标，后台获取用户联系人、谷歌账号邮箱等信息，上传用户联系人资料；监听短信和通话记录，删除通话记录，造成用户隐私泄露，建议卸载。(威胁等级中)
		Tool/Android.GPSSpy.e[prv，spy，rmt] 015.11.21	该应用是一款工具软件，安装运行之后，接收短信指令，拦截短信，并将地理位置信息转发至指定手机号码，可用于手机找回，如不是您主动安装该软件并输入信任的手机号码，请不要安装该软件。(威胁等级低)
	较为活跃的样本	Trojan/Android.Joyreach.c[rog，exp]	该应用为重打包应用非官方正版应用，运行时会私自推送广告，并且在后台私自下载 apk 静默安装，给用户造成严重地流量消耗，建议用户使用正版应用。(威胁等级中)
		G-Ware/Android.Fakegupdt.ad[exp，rog]	该应用运行后可激活设备管理器，隐藏图标，在后台加载广告，造成用户流量损耗，建议卸载。(威胁等级低)
		Trojan/Android.emial.cj[prv，exp]	该应用安装运行会隐藏图标，接收短信指令控制，可向指定号码转发接收短信及向远程服务器上传接收短信，造成用户隐私泄露。(威胁等级高)
		G-Ware/Android.simplelock.j[rog，sys]	该应用伪装成视频播放软件，安装运行之后激活设备管理器，置顶自身勒索界面，使用户不能正常使用，并勒索用户金钱。(威胁等级低)
		Trojan/Android.FakeQQ.f[exp，fra]	该应用伪装成 QQ 应用，运行后私自发送大量短信，造成用户资费损失，建议卸载。(威胁等级低)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office RTF 分析器堆栈溢出漏洞 CVE-2010-3333 (MS10-087)	Microsoft RTF 分析器在分析 pFragments 属性的值时，没有正确的计算属性值所占用的空间大小，导致堆栈溢出漏洞的产生。(威胁等级高)
	较为活跃样本	Trojan[GameThief]/Win32.Frethoq	此威胁是一种木马类程序，主要目的是盗取用户网游，网银密码等私密信息，具有关闭文件保护远程注入等功能。(威胁等级中)
		Trojan[Downloader]/Win32.VB.hbou	此威胁是一种具有下载行为的木马类程序。是以 VB 语言开发，运行后会在系统启动时自动运行。通常是从网页中下载或是捆绑正常程序。(威胁等级中)
		Trojan[Backdoor]/Linux.Mayday.f	此威胁是一种木马类后门程序，运行 linux 平台上。它可以连接远程服务器，接受攻击者恶意操作，包括下载与更新其它恶意代码、添加删除系统文件、窃取用户敏感信息等。(威胁等级中)
		Trojan[GameThief]/Win32.On Line Games.uig	此威胁是一种木马类程序，主要是窃取用户游戏信息。攻击者获取这些信息后，可能会盗卖账户中的虚拟装备、货币，也可能会直接盗卖账号本身，但最终目的都是为了来换取现实世界中的资产。(威胁等级中)

ISIS 作战安全手册揭示了它如何处理网络安全问题

Kim Zetter/ 文　　安天公益翻译小组 / 译

巴黎袭击后，美国政府官员公开谴责加密，指责美国公司 (如苹果和谷歌) 拒绝给情报和执法机构提供后门来解锁客户电话和解密受保护通信，因而手上沾染了鲜血。但是，巴黎袭击的新闻报道表明，至少在某些时候，袭击背后的恐怖分子并没有刻意使用加密通信，当局还是能够拦截和阅读他们的邮件的。

尽管如此，美国当局的言论已经充斥了媒体，他们指出 ISIS 使用的加密和其他反监视技术，挫败了有关部门追踪恐怖分子的能力。不过，当局狡猾地暗示，恐怖分子使用的某些加密技术的安全性不如他们的预期，或者没有以真正安全的方式配置和使用。那么，ISIS 袭击者究竟是如何实施 OPSEC(作战安全) 的?

ISIS 要求新兵遵守的一份 34 页的作战安全指南为我们提供了一些线索。西点军校打击恐怖主义中心的研究人员亚伦布兰特利等在 ISIS 论坛、社交帐户和聊天室中发现了该手册和其他相关文件。

该指南大约在一年前由名为 Cyberkovto 的科威特安全公司编写，目的是为了提醒加沙的记者和政治活动家如何保护他们的身份、他们线人的身份以及报道信息的完整性。但是，如今 ISIS 已将其收为己用。

该手册提供了一系列建议，包括如何保密通信和位置数据，如何保护几十个隐私与安全应用与服务的链接，包括 Tor 浏览器、Tails 操作系统，Cryptocat、Wickr 和 Telegram 加密聊天工具，Hushmail 和 ProtonMail 电子邮件服务，RedPhone 和 Signal 加密电话通信程序。手册指出，只

有当 Gmail 用假凭证打开并通过 Tor 或虚拟专用网络使用时，它才是安全的。只有当通信通过 Tor 路由时，Android 和 iOS 平台才是安全的。

手册建议，禁用手机上的 GPS 标记功能，以避免拍照泄露位置数据。另外，特工和记者可以使用 Mappr 应用程序 (可以用来伪造位置数据) 甩掉情报机构。

手册还建议不要使用 Instagram，因为它的母公司 Facebook 的保密性做得很差，并警告说，即使 GSM 网络进行了加密，移动通信仍可以被拦截。它建议读者使用加密手机，如 Cryptophone 或 BlackPhone。Dropbox 尤其被谴责，因为爱德华·斯诺登建议不要使用它，而且布什总统的前国务卿康多莉扎·赖斯是该公司的投资董事。

该文件还警告说，信徒应该使用强效密码，避免点击可疑链接，以防止情报机构和黑客侵入他们的系统。还有通信建议，例如，它教读者如何建立自己的私人 Wi-Fi 网络，或使用应用程序 (如 FireChat) 在无需网络连接时近距离共享照片和发送信息。

手册建议用户一直使用 VPN 网络对数据进行加密，防止互联网服务提供商和间谍机构获取他们的通信。但是，它警告用户远离美国 VPN 和加密聊天工具，而是使用德国公司的即时消息应用程序 (如 Telegram 和 Sicher)，或者计算机安全公司 F-Secure 的 VPN Freedome。苹果公司的终端到终端的加密服务 iMessage 也得到了肯定，因为它不受政府情报机构和苹果公司的监控。尽管美国政府官员多次声称 ISIS 使用 WhatsApp 来对抗监控，但实际上，该手册将这一聊天应用程序置于“禁用”之列。

总体来说，文件中并没有什么惊人的内容。大部分建议与世界各地的公民自由和记者团体给人权工作者、政治活动家、举报人和记者的建议 (保护通信、模糊身份或隐藏自己的位置) 是一样的。但科威特 OPSEC 手册并不是圣战者采用的唯一通信保护帮助，为了帮助他们掌握 OPSEC，ISIS 提供了 24 小时服务台。ISIS 论坛和社交媒体帐户上的这一 OPSEC 手册和其他文档表明，圣战者不仅密切研究了这些指导，同时也关注新闻动态，及时了解应用程序和软件的最新隐私和安全漏洞，并将其用于圣战中。

虽然布兰特利在 ISIS 论坛和聊天室中遇到的圣战者的技术良莠不齐。但是 ISIS 不仅愈发致力于保护自己的通信，还有兴趣对其他目标发动网络攻击。布兰特利说，“他们不是超级天才的黑客，但他们也是有点本事的。”

原文名称	ISIS’ OPSEC Manual Reveals How It Handles Cybersecurity
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 19 日《连线杂志》发布 原文地址 http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/
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。

安天发布《QQpass 分析报告》

近日，安天追影分析小组利用探海威胁检测系统 (PTD) 捕获到一起木马传输事件，某组织通过 QQ 盗号木马，盗取受害者账号及密码。此次事件受害机器数量颇多，波及范围已达 25 个省市以上，并且情况仍在持续恶化中。

经过安天追影分析系统 (PTA) 分析发现，该恶意样本 qqq.ico 首先下载一个可执行程序 qq1.css 文件，该程序可以结束掉 QQ 相关进程。当用户自行运行 QQ 程序时，qqq.ico 会检查进程里是否含有 QQ.exe，一经发现立即劫持，弹出高仿登录界面，欺骗用户。此时用户输入的账号密码则会被以明文的方式回传到盗号服务器，发送完毕后，QQ 会进行正常登录行为，使一般用户无法察觉。

追影分析小组进一步追踪后发现放马人的 IP 绑定过很多域名，其中一个域名的 whois 邮箱为 87548***@qq.com，对应有“长期收购一手安装量”的 QQ 说明，可以确认这是一个放马人。通过探海捕获的恶意事件，查看受害者 IP，可以看到受害者从放马站点下载 qqq.ico 后再从盗号 C2 下载 qq1.css，并提交 QQ 密码到盗号 C2 服务器，构成了一个完整的攻击链。

追影分析小组加紧跟进此事件后发现，除 QQ.exe 以外，地下城勇士、问道、魔兽、QQ 华夏、QQ 游戏大厅、8188 游戏中心等 55 个主流游戏客户端也被该木马劫持。被劫持的对象多为腾讯旗下的游戏，这些游戏的密码和 QQ 的账号密码是通用的。可以推测该组织通过盗取 QQ 账号和密码，去获得用户的游戏账号和密码，并进行针对游戏资源的犯罪，从而形成一条完整的游戏盗号产业链。追影分析小组提醒广大 QQ 用户，该木马弹出的高仿界面与真实 QQ 窗口相比不含菱形动画效果，二维码也无法打开，请用户在登录时谨慎操作，避免盗号事件发生。

木马程序

安天【追影高级持续威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，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 BD 静态分析鉴定器最终将文件判定为木马程序。

该文件具有以下行为：

文件名	0958B953A1030AC17C29083F4C0434BD
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	43 KB
MD5	0958B953A1030AC17C29083F4C0434BD
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Win32.SkSocket.B
判定依据	BD 静态分析

◆ 危险行为

行为描述	危险等级
疑似查找游戏进程	★★★★
Trojan[Backdoor]/Win32.SkSocket.B	★★★★

疑似查找游戏进程；Trojan[Backdoor]/Win32.SkSocket.B；连接特殊 URL；填充导入表 (疑似壳)；释放 PE 文件；获取系统内存；获取系统版本；访问文件尾部；获取计算机名称；获取 socket 本地名称；连接网络；创建特定窗体；获取驱动器类型；独占打开文件；遍历进程；获取主机用户名称；查找指定内核模块；查找特定窗体；请求加载驱动的权限。

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
连接特殊 URL	★	填充导入表 (疑似壳)	★★
获取系统内存	★★	释放 PE 文件	★
访问文件尾部	★	获取系统版本	★★
获取 socket 本地名称	★	获取计算机名称	★
创建特定窗体	★	连接网络	★
独占打开文件	★	获取驱动器类型	★
查找特定窗体	★	遍历进程	★
查找指定内核模块	★	获取主机用户名称	★
请求加载驱动的权限	★		

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=0958B953A1030AC17C29083F4C0434BD

(上接第一版)

颁发的“移动设备年度最佳保护奖”，实现了亚洲厂商零的突破；2015 年，我们又在世界著名的安全软件测试机构 AV-C 上下半年的测试中，成为唯一两次均取得 100% 检出率的安全厂商。纵然我们在移动安全的技术版图上打破了欧美厂商垄断的局面，在移动恶意代码的检测能力上取得了领先的位置，但我们也深刻地认识到：“攻守之势异也”。未来的移动安全威胁对抗，不仅仅需要我们守住恶意代码对抗的高地，也需要我们关注移动安全威胁相关的演进、泛化，以及其带来的实际威胁和相关的影响，并重新革新对抗体系和工程化体系。

如果说 2007 年的安天武汉研究小组是呱呱坠地的婴孩，那么现在的安天 AVL TEAM 则是正在为应对移动安全威胁不停奔跑的追风少年，无论移动安全技术如何发展，移动安全威胁如何变换，我们始终在战斗的第一线，并愿意将我们的知识、经验和成果与大家分享。(选自安天 AVL TEAM 移动安全团队负责人潘宣辰在“安天技术文章汇编八”《移动安全分册Ⅱ》所做的序言)