安天周观察

主办：安天　　2015 年 9 月 28 日（总第 10 期）试行　本期 4 版　　微信搜索：antiylab　　内部资料 免费交流

安天 AV-C 测试交出双百答卷

近日，安天移动安全团队自主研发的手机安全软件 AntiyAVL 继今年 2 月以 100% 检出率荣获 AV-C 移动安全软件评测第一之后，在 2015 年上半年的第二次评测中，再次以 100% 检出率从众多参与测评的国内外产品中脱颖而出！

国际权威测评机构 AV-Comparatives 简称 (AV-C) 是一家国际性独立杀毒软件测试机构，因提供针对安全产品的综合性与客观性评测结果而闻名。从 2010 年开始针对手机安全软件进行测评，测评每年进行一次，时间在当年的 7-8 月份。从 2015 开始，AV-C 开始每年提供 2 次针对手机安全软件的测试，其中增加了 2 月份针对手机安全软件检测率的测试。今年是安天 AVL 首次参加评测，在 2 月和 8 月两次评测中均得到 100% 检出率，成为参加测试中唯一一个交出双百成绩的安全厂商。

2 月评测成绩

Protection rate results

Rank	Vendor	Protection rate[6]	Product
1.	Antiy	100%	Antiy AVL for Android 2.3
	Qihoo 360		Qihoo 360 AntiVirus 1.3
2.	AVIRA	99.9%	Avira Antivirus Security 3.9
	ESET		ESET Mobile Security 3.0
3.	Avast	99.8%	Avast Mobile Security 4.0
4.	AhnLab	99.7%	AhnLab V3 Mobile 2.1
5.	Bitdefender	99.6%	Bitdefender Mobile Security 2.36
	Kaspersky Lab		Kaspersky Internet Security 11.7
6.	Trend Micro	99.3%	Trend Micro Mobile Security 6.0
7.	Quick Heal	98.6%	Quick Heal Total Security 2.0
8.	G Data	96.1%	G Data Internet Security 25.7
9.	Anguanjia	94.7%	Anguanjia 安全管家 5.0

8 月评测成绩

		Malware Protection	False Alarms
1.	Trend Micro	100%	0
2.	Bitdefender, G Data	100%	3
3.	Antiy	100%	5
4.	CM Security, CleanMaster	99.9%	0
5.	ESET	99.9%	1
6.	Tencent	99.9%	2
7.	AhnLab, Avira	99.9%	3
8.	Avast	99.9%	4
9.	Kaspersky Lab	99.7%	0
10.	McAfee	99.6%	2
11.	Baidu	99.4%	0
12.	Sophos	99.2%	0
13.	AVG	98.4%	4
14.	Android Baseline	unknown[4]	0

第四版：【安天联合分析小组】发布

《Xcode 非官方版本恶意代码污染事件的分析与综述》报告

安天参加互联网网络安全威胁治理行动研讨会

9 月 25 日上午，由国家互联网应急中心、中国互联网协会、网络与信息安全工作委员会共同牵头组织的“互联网网络安全威胁治理行动研讨会”在京召开。会议由 CNCERT 运行部副主任严寒冰主持，中国移动、电信、联通、阿里巴巴、百度、搜狗、360、启明星辰、安天、绿盟等多家行动单位参加了会议。

CNCERT 运行部工程师赵慧通报了行动阶段工作开展情况和成效：整个行动开展 56 天，共有 56 家企业参加了行动，接受的威胁举报 29,658 起，对威胁进行的分析和打击共 13573 起，同时在黑名单拦截上共搜集黑名单地址 18,502 条。在该行动通过多种方式获取威胁举报，包括 DDoS 攻击、网页篡改、漏洞等等，重点对于涉及此次涉及地下黑产 DDoS 攻击和网页篡改进行了处置。

参与单位积极举报威胁事件，威胁单位主要包括 CNCERT 及各省分中心、中国互联网协会及安天、杭州安恒、深信服、阿里巴巴、知道创宇等网络安全厂商。该行动取得的工作成效明显，DDoS 攻击事件数量呈断崖式下降、篡改网站数量稳步下降、浏览器黑名单拦截访问次超过千万。

习近平访美前谈网络安全问题

9 月 22 日，在对美国进行国事访问前夕，国家主席习近平 9 月 22 日接受了美国《华尔街日报》书面采访，在谈到网络安全问题时，习近平表示：

中国是网络安全的坚定维护者。中国是黑客攻击的受害国。中国政府不会以任何形式参与、鼓励或支持企业从事窃取商业秘密行为。不论是网络商业窃密，还是对政府网络发起黑客攻击，都是违法犯罪行为，都应该根据法律和相关国际公约予以打击。中美双方在网络安全上有共同关切，我们愿同美方加强合作。（文章来源 http://news.ifeng.com/a/20150922/44711066_0.shtml）

每周安全事件

类 型	内 容
中文标题	恶意应用程序侵入 Google Play 商店两次，百万用户受到影响
英文标题	Advanced malware gets into Google Play store twice，possibly 1M downloads
作者及单位	Adam Greenberg，SC Magazine
内容概述	近日，一款恶意应用程序伪装成安卓游戏侵入 Google Play 商店两次，每次造成 100，000 次到 500，000 次的下载，感染了近百万用户。此恶意程序被称作大脑测试程序 (Brain Test)，绕过 app 审核系统 – 谷歌保镖 (Google Bouncer)，利用权限提升获得设备的根存储权限，且不容易被移除。 据相关人士表示，该程序第一次进入 Google Play 商店的时间不能确定，曾于 8 月 24 日被删除；第二次是在 9 月 10 日，9 月 15 日谷歌将其删除。
链接地址	http://www.scmagazine.com/advanced-malware-gets-into-google-play-store-twice-possibly-1m-downloads/article/439803/

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/OSX.XcodeGhost 2015-9-22	由于第三方源下载的 Xcode(苹果平台 IDE) 被植入恶意代码，使用受感染的 Xcode 编译、生成的应用中会被植入后门。该应用能盗取用户隐私信息回传。
		Trojan[Backdoor]/Android.Ztorg 2015-9-19	该应用包含恶意模块，运行会私自下载提权工具，上传用户系统信息，自我更新子包，后台推送广告，防止卸载，存在流氓行为，同时私自下载会造成用户流量资费损失。(威胁等级中)
		Trojan/Android.Pawen 2015-9-17	该应用运行后会获取用户固件信息，加载敏感成人色情内容，同时诱导用户订阅付费信息，造成一定资费损失。(威胁等级中)
		Trojan[Spy]/Android.Fech 2015-9-17	该应用运行时会诱导用户激活设备管理器，并于后台隐藏图标，私自联网上传用户手机固件获取指令，执行私发短信、拦截短信等操作，给用户带来经济损失。(威胁等级中)
		Trojan/Android.Koler 2015-9-17	该木马运行后在用户解锁屏及运行其它应用会以非法浏览色情为由不断弹出警告信息，提示用户需缴罚款后才能解除，其行为极为流氓同时会恶意勒索用户产生高额费用。(威胁等级中)
		Trojan/Android.Nxuul 2015-9-17	该木马安装无图标，初次运行会监听解锁广播，弹出设置界面，执行私自上传短信箱、通话记录等操作，泄露用户隐私。(威胁等级中)
		Trojan/Android.Xshqi 2015-9-17	该应用运行后会隐藏图标，无实质功能，后台联网获取短信内容并向用户所有通讯录联系人发送包含 url 的短信，存在恶意传播行为，此外还会显示各种类型的广告，存在流氓行为。(威胁等级中)
	较为活跃的样本	GrayWare[AdWare]/Android.Inoco.b	该类应用安装后无图标，伪装成系统应用，后台推送广告，可能给用户带来资费消耗。
PC 平台恶意代码	新出现的 0day	VBox Satellite Express 2.3.17.3 – 任意写入漏洞 (CVE-2015-6923) 2015-9-16	该漏洞允许攻击者在 ndvbs 模块进行提取而执行任意代码。(威胁等级低)
	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	RiskWare[Downloader]/Win32.LMN.a	此威胁是下载者木马类程序，通常会收集信息回传给攻击者，并下载指定的其它程序执行。
		Virus/Win32.Virut.ce	此威胁是一种文件感染程序。能够感染受损系统中的 .exe 和 .scr 文件。
		GrayWare[AdWare]/Win32.MultiPlug.heur	此威胁是一种灰色软件程序。具有反虚拟机、反调试功能，运行会添加自启动项，会弹出广告，具有一定风险。
		Worm[Net]/Win32.Allaple.e	此威胁是一种多线程的多态感染型的网络蠕虫程序。它能够传播至其它连接了本地网络的计算机中并对特定的远程网站进行拒绝服务攻击。它利用网络共享进行传播，它能够在网络中通过发送完整且独立的副本来完成自我复制。

安全研究员曝光 FireEye 核心产品 0day 漏洞

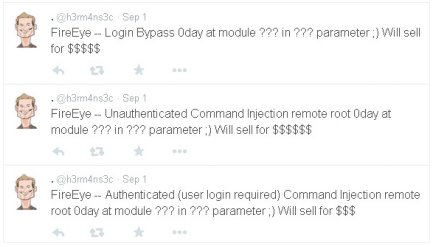
Steve Ragan / 文　　安天公益翻译小组 / 译

9 月 5 日，安全研究员 Kristian Erik Hermansen 在 FireEye(火眼公司) 的核心产品中发现了一个 0day 漏洞。Hermansen 表示，如果对该漏洞加以利用，它会导致未经授权的文件泄露。他还列出了触发漏洞的简短例子以及 /etc/passwd 文件副本作为证据。此外，他声称要将另外三个漏洞进行公开兜售。

Hermansen 要出售的三个漏洞是：一个登陆绕过漏洞，也称为命令注入漏洞，一个未经身份验证漏洞以及另一个身份验证漏洞。根据已经揭露的 Exploit-DB 和 Pastebin 所呈现信息，存在漏洞的设备其基本设置正如所预料的那样，以 root 权限运行着 Apache 和 PHP，另一些服务也被列举在了运行的网页设备中，包括 SSH 和 FTP。然而，被揭露的漏洞似乎存在于 FireEye 自身设备的 PHP 脚本中。

这只是 FireEye(或 Mandiant) 众多 0day 漏洞中的一个而已。在长达一年半的时间里，FireEye 的安全“专家们”对此竟然没有进行任何的修复，很肯定的是，Mandiant 的员工将这一漏洞以及其他缺陷编码进了产品中，更令人感到可悲的是，FireEye 竟然没有外部安全研究人员的上报程序。Salted Hash 已经就该事件联系 FireEye，但是适逢周末，FireEye 还未做出迅速回应。

2014 年初，Hermansen 因与 Covered California 网站的律师们打官司而上了头条 (Covered California 网站负责的是加州平价医疗法案的注册)，原因是他发现了该网站的一些漏洞并公之于众。起初 Hermansen 联系了网站方面，得到的结果却是加州政府和那些负责网站开发的人员的默不做声。一个月的等待之后，他将这些漏洞公之于众。不久，Covered California 的律师们找到了他，但他们的目的并不是修复漏洞，Hermansen 在接受福布斯采访时说，他们的目的是删除网上公开的漏洞信息以及涉及的事情。



该研究员声称还有另外三个未公开的漏洞，并要进行兜售。

FireEye 对待此事的方式似乎与 Hermansen 所经历的 Covered California 事件如出一辙，唯一不同的是，现在 Hermansen 想要出售这些漏洞。

“事件发生一段时间后，我们给 Hermansen 发送了邮件询问详情，他回复我们说：我与另一位研究员 Ron Perris 合作的时候，发现了 FireEye 产品中的 30 个漏洞，包括多个远程 root 权限漏洞。我通过正规的渠道与 FireEye 进行了一年半的沟通来解决问题，但是每次对方都有所回避。我认为这些情况应该被披露，因为平台存在漏洞，大家都应该对此了解，而且这些是存在远程 root 漏洞的政府批准的安全港设备，如果 FireEye 不愿意修复这些漏洞，大家就不应该信任网络中的这些设备，作为一家安全企业，他们的标准应该被定位的更高才对。”Hermansen 说，他本想将漏洞直接告知 FireEye 以获得相应报酬。然而事与愿违，他就选择对外出售，把每个漏洞的价钱都定在 1 万美金以上。

基于此事，FireEye 方面向 Salted Hash 发布了简短的声明：FireEye 已经从 KristianHermansen 公开揭露的漏洞信息中了解到其产品中的 4 个潜在安全漏洞。对于安全研究员发现潜在安全漏洞，我们感谢其在帮助我们完善产品性能方面所做出的努力，例如 KristianHermansen 和 Ron Perris，但是我们一直鼓励大家能够对公开揭露的信息负起责任。对于安全研究员揭露潜在安全漏洞并告知我们等行为，FireEye 有相关的明文规定和政策。关于这些潜在安全漏洞，我们已经联合这些安全研究员一起解决，以便快速确定并修复任何会影响我们平台与客户的潜在安全隐患。

在随后更新的报道中，FireEye 称 Hermansen 于 9 月 6 日揭露的漏洞是 HX 系统中曾经修补的漏洞。近期的更新已经降低了这一漏洞对运行旧版本 (HX 2.1.x 和 DMZ 2.1.x) 产品的影响。但是，为了立即解除风险，FireEye 强烈建议用户将 HX 产品升级为最新版本 (2.6.x 版本)。对于那些仍然保留旧版本的用户，FireEye 正极力修补已经报告的 HX 2.1.x 系列的漏洞，并将通过官方客户支持渠道告知受影响的客户。

在作出上述回应后，Hermansen 说：“我很高兴看到 FireEye 对这一漏洞及其他问题所做的修复工作。当你以 root 权限运行网页服务器，并且没有足够的 SDLC 进程时，你会受到严重的打击。因为即便是一个小小的漏洞都会导致全面的远程攻击受损。在当今的年代，安全企业不应该出现这样的问题。它们理应在客户网络中与 0day 漏洞进行抗争，并且不厌其烦地加固自身设备的安全性。”

原文名称	Researcher discloses zero-day vulnerability in FireEye
作者简介	Steve Ragan，资深编辑，在 2005 年加入新闻界之前，有 15 年的 IT 承包自由撰稿人的经历。
原文信息	2015 年 9 月 6 日 CSO 发布，原文地址 http://www.csoonline.com/article/2980937/vulnerabilities/researcher-discloses-zero-day-vulnerability-in-fireeye.html

【安天联合分析小组】发布

《Xcode非官方版本恶意代码污染事件的分析与综述》报告

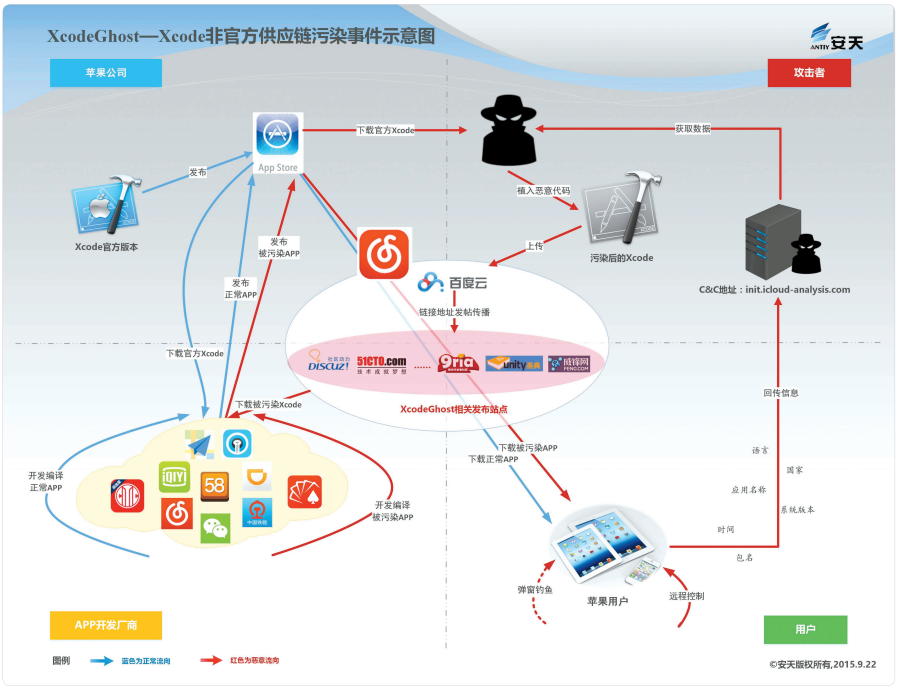
Xcode是由苹果公司开发的运行在操作系统MacOSX上的集成开发工具(IDE)，是开发OSX和iOS应用程序的最快捷的方式，其具有统一的用户界面设计，同时编码、测试、调试都在一个简单的窗口内完成。

截止到2015年9月20日，各方已经累计发现共692种(如按版本号计算为858个)App确认受到感染。同时，有分析团队认为，相同的攻击者或团队可能已经对安卓开发平台采用同样的思路进行了攻击尝试。从其感染面积、感染数量和可能带来的衍生风险来看，其可能是移动安全史上最为严重的恶意代码感染事件之一，从影响范围上来看能与之比肩的仅有此前臭名昭著的的CarrierIQ。

目前，Unity 3D也被发现由同一作者采取攻击Xcode手法类似的思路进行了地下供应链污染。

鉴于此事态的严重性，安天安全研究与应急处理中心(AntiyCERT)与安天移动安全公司(AVL Team)组成联合分析小组，结合自身分析进展与兄弟安全团队的分析成果，形成此报告。

安天根据Xcode非官方版本恶意代码污染事件(XcodeGhost)的相关信息形成了下图，其整体污染路径为官方Xcode被攻击者植入恶意代码后，由攻击者上传到百度云网盘等网络位置，再通过论坛传播等方式广播下载地址，导致被App开发者获取，同时对于攻击者是否利用下载工具通过下载重定向方式扩大散布，也有较多猜测。有多个互联网公司采用被污染过的Xcode开发编译出了被污染的App，并将其提交至苹果AppStore，且通过了苹果的安全审核，在用户获取相关App进行安装后，相关应用会被感染并回传信息至攻击者指定域名。



1. 从供应链上看

供应链上的各个环节，都有可能影响到最终产品和最终使用场景的安全性。在这个维度上，开发工具、固件、外设等“非核心环节”的安全风险，并不低于操作系统，而利用其攻击的难度可能更低。因此仅关注供应链的基础和核心环节是不够的。而同时，在实际应用场景中，往往存在着因盗版、汉化、破解等问题带来的地下供应链，以及下载重定向、第三方分发源等带来的不确定性，这些因素，在过去已经给信息系统制造了大量隐患。

2. 从场景和时域关联上看

开发商、分销商、配送通道的安全性与使用场景的安全同样重要，因此只关注最终场景的安全是不够的。苹果在中国缺少足够的CDN资源投入，尽管因其产品的强势，让中国的开发者和用户都能容忍，但无疑也助动了地下工具链的成长。而国内的网络速度和效率问题，看似一个体验问题，但其最终也同样可以转化为安全问题。

3. 从权限上看

在数据读取能力上，居于底层的操作系统和居于上层的应用程序可能是一致的，即使操作系统做出种种分层访问、沙箱隔离等限制，一旦受到污染程序进入系统，其攻击难度就瞬间从远程利用降低为提权，因此只关注操作系统的“底层”安全是不够的，追求系统数据安全和持续运维才是目的。而同时，在移动平台上，无论是安卓提供的安全产品与应用平权的策略，还是苹果彻底将反病毒产品逐出AppStore的方法，最终都导致安全厂商难以给予其更多的支持、防护和协同。从而使这些互联网霸王龙陷于与寄生虫们不可能取胜的战争当中。

4. 从信息链上看

互联网模式不是传统的信息流转，而是基于用户的方便性追求而进行的信息采集、聚合与分析，用户需要用主动提供信息来置换对应服务，因此，仅用传统的控制思维是不够的。而从这一恶意代码所表现出的信息采集和提交的特性来看，其似乎与常态的互联网客户端十分接近，这或许也是其未能被更早发现的原因。

这一问题再度提醒我们，要跳出单点迷思，从完整供应链、信息链角度，形成全景的安全视野、安全建模与评价、感知能力。同时，我们也要再度提醒，我们需要警惕“建立一个完全自闭合的供应链与自循环的信息链方能安全自保”的小农安全观的卷土重来，在互联网和社会生活场景下，这本身就不可能实现。而中国政企网络的市场空间，完全不足以保证一个健康的闭环供应链的有效生存，更谈不上还需要支撑这个闭环供应链安全性的持续改进。(完整报告：http://www.antiy.com/response.html)