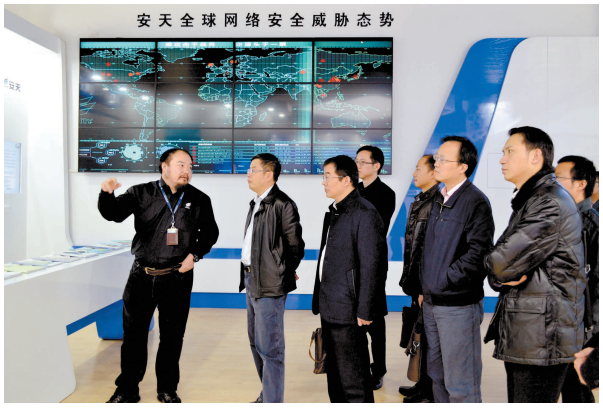
安天周观察

主办：安天　2015 年 11 月 2 日（总第 14 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

中国网安公司访问安天总部

10 月 25 日，由中国电子科技集团公司 (CETC) 第三十研究所所长、中国网安公司董事长李成刚带队的中国网安公司代表来到安天总部访问。

安天技术负责人为各位介绍了安天的情况，主要包括团队能力储备、公司的目标和定位及主要产品三方面，并陪同代表团观看了安天探海威胁检测系统、追影威胁分析系统、智甲终端防御系统等反 APT 解决方案的演示。在参观安天的反病毒博物馆、技术主题展室及安天安全威胁感知捕获体系和可视化演示后，双方在技术和战略合作方面进行了探讨。



李成刚董事长在对中国网安情况介绍及未来规划的合作方向的沟通中表示：“安天的基础技术特别突出，在恶意代码的分析和服务上的技术专业程度是受到国际认可的，中国网安公司和安天的合作有坚实的基础，比如在态势感知、工控安全等方面，今后将在监测预警、移动互联网、云计算和大数据等领域应该加强合作，希望形成“你中有我　我中有你　相互支持”的关系，共同把信息安全产业做大、做强。

安天荣获『反法西斯战争胜利 70 周年纪念活动网络安全保障工作』先进集体奖

10 月 29 日，北京市通信管理局召开纪念活动网络安全保障工作总结表彰大会。

安天、安恒、深信服、恒安嘉新、卫士通、知道创宇、启明星辰、360、中新软件共 9 家单位参加了会议。北京市通信管理局副局长魏健为 9 家单位颁发了“中国人民抗战暨世界反法西斯战争胜利 70 周年纪念活动网络安全保障工作”先进集体奖。

此次纪念活动保障期间，各基础运营企业和网络安全公司密切配合，所有网络安全事件均在第一时间得到了处置，圆满完整了网络安全保障任务。

百度多款App存在WormHole漏洞，安卓手机可被远程控制

目前，百度已经确认了该漏洞，并在回复中称“此漏洞已知晓且 mo+sdk 已修复”。

据了解，WormHole 漏洞影响许多安卓平台用户量过亿的 APP，目前已知受影响的 App 包括：百度地图、百度浏览器、百度贴吧、百度翻译、百度视频、百度手机助手、百度云、百度音乐、百度新闻、百度图片、百度输入法等。除此之外，还有口袋理财、萌萌聊天等多款 App。

攻击者可以达到远程静默安装应用、远程启动任意应用、远程获取用用户的 GPS 地理位置信息、获取 imei 信息、安装应用信息等目的。（文章来源：http://www.cnbeta.com/articles/442799.htm)

安天 2016 校园宣讲在北京、哈尔滨、武汉三地开展

金秋 10 月，安天 2016 校园招聘帷幕在北京、哈尔滨、武汉三地拉开。并在北京邮电大学、北京科技大学、哈尔滨工业大学、哈尔滨工程大学、华中科技大学、中国地质大学（武汉）等多所高校进行了校园宣讲和笔试环节。

安天是致力于提供先进威胁检测能力的安全厂商，也是一支秉承和坚持安全企业朴素信仰的团队。在网络安全界内对信息技术博弈攻防领域的专注度和知名度吸引了不少青年学生前来参加宣讲会，现场虚无坐席，十分火爆。

每周安全事件

类 型	内 容
中文标题	1300 万 000WebHost 用户明文密码被叫卖
英文标题	Hackers put up for sale 13 million plaintext passwords stolen from 000webhost
作者及单位	ZeljkaZorz，Help Net Security
内容概述	知名免费 Web 托管公司 000webhost 遭黑客入侵，导致 1300 万用户的姓名，电子邮件地址，和未加密的密码被盗。该公司表示，黑客使用了老版本 PHP 中含有的一个漏洞上传一些文件，从而能够访问系统；尽管整个数据库都被入侵，但最担心的是客户信息问题。同时，该公司已经将所有密码重置，部署了加密措施以避免这种灾难再次出现；并建议用户重置账号，电子邮件地址以及 MySQL 数据库密码。
链接地址	http://www.net-security.org/secworld.php?id=19041

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.SysChecker.e[exp] 2015-10-23	该程序安装无图标，触发启动释放恶意子程序，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)
		Trojan/Android.FakeFlashPlayer.i[prv，rmt，rog] 2015-10-23	该应用伪装成 FlashPlayer，运行会请求激活设备管理器，隐藏图标，上传用户收件箱信息，接受远程指令，发送指定的短信，并拦截特定的短信，可能导致扣费。给用户造成隐私泄露和资费消耗。(威胁等级中)
		AdWare/Android.YeahMobi.b[ads] 2015-10-25	该应用包含 YeahMobi.b 广告插件，会在通知栏推送广告，点击后会直接下载推荐应用，可能会造成资费损失，谨慎使用。(威胁等级中)
		G-Ware/Android.FakeSex.a[rog，exp] 2015-10-28	该应用伪装成色情播放器，诱骗用户下载安装未知应用，诱骗用户激活设备管理器，会调用支付模块发送短信进行支付，造成用户资费消耗。(威胁等级低)
	较为活跃的样本	Trojan/Android.Downloader.al[rog，exp]	该应用伪装色情视频播放器，运行会后台私自下载 apk 应用频繁弹框安装界面，调用支付接口进行短信支付，频繁联网，造成用户资费消耗。(威胁等级中)
		Trojan/Android.Fakegupdt.s[exp，rog]	该程序安装运行之后，伪装成系统升级服务，诱导用户点击下载广告，会造成用户大量的流量资费的损失。建议不要安装该软件。(威胁等级中)
		Trojan/Android.wsms.b[prv，exp]	该应用运行后隐藏图标，拦截用户所有短信并通过服务器上传，对用户隐私造成严重的损害，建议用户立即卸载。(威胁等级高)
		Trojan/Android.lazyor.a[prv，exp]	该应用运行后释放子程序，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，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)
PC 平台恶意代码	活跃的格式档漏洞、0day 漏洞	Flash 漏洞 (cve-2015-5122)	Hacking Team 中所披露的 Flash 漏洞 (cve-2015-5122) 用于网页挂马，影响 Windows、MacOSX 和 Linux 平台上的 IE、Chrome 浏览器等主流浏览器。中此病毒用户会下载大量推广软件。
	新出现的样本家族	Trojan/Win32.Reconyc.evdc	此威胁是一种木马类程序，运行后会释放动态链接库文件和可执行程序到系统文件夹，并设置消息钩子函数，获取系统相关信息。(威胁等级中)
		Trojan/Win32.Scar.ejkj	此威胁是一种木马类程序，可以将某些金融网站重定向到攻击者设置的另一个地址，模仿登录界面从而窃取用户密码。(威胁等级中)
		Trojan[Dropper]/Win32.Injector.mnmj	此威胁是一种木马类程序，是用于对指定文件或程序注入代码或线程的黑客工具软件。对于系统一般没有主动破坏能力，主要配合其它恶意程序进行入侵活动。(威胁等级中)
		Trojan/Win32.MicroFake.rf	此威胁是一种木马类程序，运行后，会关闭系统的部分进程，然后提示用户需要下载指定升级程序，并打开一个虚假的微软公司网页诱使用户下载其它恶意程序。(威胁等级中)
		Trojan/Win32.Qhost.lfs	此威胁是一种木马类程序，会改变 Host 文件内容以屏蔽某些网站的木马类程序。该家族能够通过专门用于改变 Host 文件的黑客服务器来重定向细节，从而实现对密码信息的窃取。(威胁等级中)

黑客可在 16 英尺外秘密控制 Siri

Andy Greenberg / 文　　安天公益翻译小组 / 译

Siri 可能是你的个人助理。但是，她并不只听从你一个人的语音命令。一组法国研究人员发现，Siri 也会听从与她交谈的任何黑客的命令，甚至在某些情况下，是可以听从从 16 英尺外通过无线电传输命令的黑客。

致力于信息安全的法国政府机构 ANSSI(法国信息系统安全局) 的两个研究人员已经展示，他们可以使用无线电波来触发任何启用 Google Now 或 Siri，且在麦克风插孔中插入耳机的 Android 或 iPhone 手机的语音命令。这种聪明的攻击将耳机线作为天线，利用耳机线把电磁波转换成电子信号，显示在手机的操作系统中，就是从用户的麦克风传来的音频。黑客不必说一句话，就可以利用这种无线攻击，告诉 Siri 或 Google Now 拨打电话和发送短信，拨打号码的黑客将手机变成一个窃听器，将手机浏览器发送到恶意软件网站，或者通过电子邮件、Facebook 或 Twitter 发送垃圾邮件和网络钓鱼消息。

“在语音命令功能设备的音频前端诱导寄生信号的可能性会引发严重的安全影响”，两名法国研究人员何塞·洛佩斯·埃斯特维斯和查欧基·卡斯米发表在 IEEE(电气和电子工程师协会) 的一篇论文写到。”

今年夏天，这项研究工作第一次在 Hack in Paris 会议上提出，但是除了几个法国网站，该研究并没有引起广泛的关注。该研究使用相对简单的设备集合：用运行开源软件 GNU Radio(USRP 软件定义的无线电) 的笔记本电脑、放大器和天线生成电磁波。研究人员说：“这些设备最小

可以容纳在一个背包里，攻击范围大约为 6.5 英尺。如果想要更强大，则需要更大的电池，只能放置于汽车或面包车内，这样就可以将攻击范围扩展为超过 16 英尺。”

有一个视频显示了攻击行动：在演示中，研究人员通过 Android 智能手机的无线电命令 Google Now 谷歌，迫使手机的浏览器访问 ANSSI 网站。研究人员说，为了遵守“禁止广播特定电磁波频率”的法国规定，该实验在无线电波阻断法拉第笼 (译者注：法拉第笼是一个由金属或者良导体形成的笼子，是一种用于演示等电势、静电屏蔽和高压带电作业原理的设备) 中进行。但是卡斯米和埃斯特维斯说：“在此攻击中，没有必要使用法拉第笼。”

研究人员声称，黑客可以把无线电设备藏在背包内，进入一个拥挤的区域，用它向周围所有的手机传输语音命令。“可以想像在有很多人的酒吧或机场，发送一些电磁波可能会导致大量的智能手机拨打付费号码，产生费用，”施特鲁贝尔说。

虽然 iOS 的最新版本现在有一个免提功能，允许 iPhone 用户简单地通过说“Hey Siri”发送语音命令，但是，卡斯米和埃斯特维斯说，他们的攻击针对旧版本的操作系统。iPhone 耳机的线上有一个按钮，允许用户长按该按钮启用 Siri。通过逆向工程并模仿该按钮的电子信号，他们的无线电攻击可以从锁屏触发 Siri，而无需用户进行任何交互。

至少在使用苹果手机的情况下，任何能够动手访问设备的人都能够使用这些语音命令功能，从手机中获取敏感信息 (包括联系人和最近通话等)，甚至劫持社交媒体帐户。但是，无线电攻击扩展了入侵的范围和隐蔽性，这使得用户从锁屏上禁用语音命令功能更加重要。

ANSSI 研究人员说，他们已经联系了苹果和谷歌，并建议了其他修复。例如，他们建议，在耳机线上使用更好的屏蔽来迫使攻击者使用较高功率的无线电信号，或者，在手机中使用电磁传感器可以阻断攻击。但是，他们指出，这种攻击也可以通过软件阻止，让用户创建自定义的“唤醒”语句来启动 Siri 和 Google Now，或者使用语音识别来阻挡陌生人的命令。截至目前，谷歌和苹果都没有回应《连线杂志》就该研究的提问。

如果没有卡斯米和埃斯特维斯说建议的安全功能，任何智能手机的语音功能都会带来安全风险。(风险可能来自获得手机的黑客，或者隐藏在隔壁房间的攻击者。)“要使用手机的键盘，你需要输入 PIN 码。但是，语音接口一直在监听，且不需要认证。这是本研究的主要问题：即指出安全模式中的这些缺陷。”埃斯特维斯说。

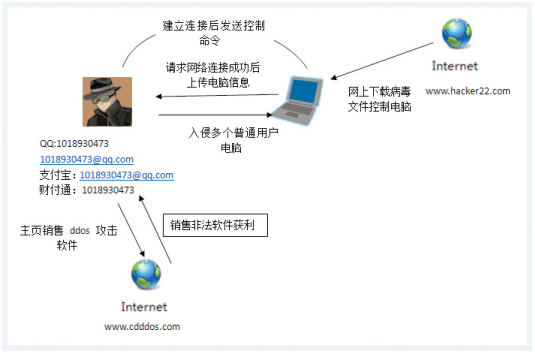
原文名称	Hackers Can Silently Control Siri From 16 Feet Away
作者简介	Andy Greenberg，《连线杂志》的资深作家，研究领域涵盖安全、隐私、信息自由和黑客文化。
原文信息	2015 年 10 月 14 日《连线杂志》发布，原文地址 http://www.wired.com/2015/10/this-radio-trick-silently-hacks-siri-from-16-feet-away/
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，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。

安天追影再次成功追踪捕获网络信息犯罪

安天追影分析小组最近发现了一个利用 DDoS(分布式拒绝服务攻击) 获利的黑客，可能会通过财付通、支付宝等来获取利益。

为了进一步搜索网络犯罪证据，获取恶意代码和作者的来源，安天追影分析小组利用安天自主研发的两款产品 PTA(追影威胁分析系统) 和 PTD(探海威胁检测系统) 的实现了对恶意代码分析与追踪。

分析后可以看到 DDoS 样本存在有多种恶意行为，该病毒样本运行后安装 .net clr 的服务，释放 hra33.dll，进行局域网弱口令的登录感染共享目录。PTA 标识出访问黑客控制服务器包括 aiqing.txddos.com、98syn.com、hacker22.com。 其 中 hacker22 的域名注册为 QQ 1018930473，黑客姓名有可能为“谭青”，在其搭建的网站 www.cdddos.com 有销售 DDoS 攻击



服务的广告，并留有 QQ 小号。该黑客注册的英文多以 DDoS、hacker 单词为主，包 括 hacker22.cn，cpddos.com、cdddos.com。信息表明，其主要的网络活动在重庆进行，主要以销售 DDoS 攻击和帮人建立灰色网站牟利。

无论是 DoS(Denial of Service，即拒绝服务) 攻击还是 DDoS 攻击，简单的看，都只是一种破坏网络服务的黑客方式，虽然具体的实现方式千变万化，但都有一个共同点，就是其根本目的是使受害主机或网络无法及时接收并处理外界请求，或无法及时回应外界请求。其具体表现方式有以下几种：

1. 制造大流量无用数据，造成通往被攻击主机的网络拥塞，使被攻击主机无法正常和外界通信。

2. 利用被攻击主机提供服务或传输协议上处理重复连接的缺陷，反复高频的发出攻击性的重复服务请求，使被攻击主机无法及时处理其它正常的请求。

3. 利用被攻击主机所提供服务程序或传输协议的本身实现缺陷，反复发送畸形的攻击数据引发系统错误的分配大量系统资源，使主机处于挂起状态甚至死机。

高级威胁

安天【追影高级持续威胁分析系统】无需更新病毒库，即可实现对上述高级威胁进行有效检测，下为其自动形成的分析报告

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、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。

依据动态行为鉴定器最终将文件判定为高级威胁。

该文件具有以下行为：利用漏洞释放 PE 文件；格式漏洞；连接特殊 URL；通过设置为系统属性隐藏文件；释放 PE 文件；获取计算机名称；获取 socket 本地名称；查找浏览器进程；连接网络；创建特定窗体；获取驱动器类型；打开自身进程文件；启动服务；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。

文件名	04397253C5AE37468A669FB309B78A3D
文件类型	Media/Adobe.SWF[:Flash]
大小	221 KB
MD5	04397253C5AE37468A669FB309B78A3D
病毒类型	高级威胁
恶意判定 / 病毒名称	Trojan/Win32.Danginex
判定依据	动态行为

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
利用漏洞释放 PE 文件	★★★★	格式漏洞	★★★★

◆ 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	★	通过设置为系统属性隐藏文件	★
获取 socket 本地名称	★	释放 PE 文件	★
连接网络	★	获取计算机名称	★
获取驱动器类型	★	查找浏览器进程	★★
启动服务	★	创建特定窗体	★
查找指定内核模块	★	打开自身进程文件	★
请求加载驱动的权限	★	获取主机用户名称	★
		查找特定窗体	★

完整报告地址：http://kingsoft.pta.center/_lk/details.html?hash=04397253C5AE37468A669FB309B78A3D