安天周观察

主办：安天　2015 年 11 月 9 日 (总第 15 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天中标某省监控预警系统建设项目

根据工业和信息化部发布的多项文件及通知，某省通信管理局公开招标，承建“某省国家级互联网骨干直联点质量监测系统新建工程”。安天以自主知识产权产品“探海威胁检测系统 (PTD)”、“追影安全分析系统 (PTA)”、“态势感知与通报预警平台”为依托，正式中标该项目中网络安全监控预警子系统的建设。

在该项目中，安天通过分布式部署的网络病毒监测探头 (探海威胁检测系统 PTD) 以及追影安全分析系统 (PTA)，可以实现对直联点互联互通流量进行信息采集，通过多个网络安全事件主动采集服务器及相关管理平台形成的主动捕获手段，在城域网监控点获取攻击者的攻击信息；通过开放式的事件和样本入口，兼容多来源样本文件和事件日志等，并完成多来源管理及调度，在实现了对流量的实时监测的基础上，利用 PTA 的分析能力实现对恶意代码的分析、判定以及对恶意代码源头的锁定。

该系统设计还将实现通过疫情预警系统，对关联安全事件进行挖掘和分析；建立针对未知威胁和 0day 攻击 /APT 的预警平台；运用业界领先的可视化展示，以清晰、直观、形象的视图与表格，帮助管理者发现不易被发现的 0day 攻击，并捕获攻击行为，确定攻击目的以及追踪攻击源，发现网络中的计算机病毒和网络安全事件，确定病毒传播和网络攻击的种类、数量和来源，为省管局掌握信息网络安全状况，打击网络违法犯罪活动、制定信息安全政策提供基础数据和决策依据。

安天通过对该省国家级互联网骨干直联点流量的实时监测，捕获并分析网络安全事件，关联分析网络安全数据的设计架构，帮助客户实现：了解并掌握网络安全态势，及时通报安全事件盘点结果，提高应对突发网络攻击事件的应急响应能力及风险预警能力。

安天参加 2015 中国互联网安全领袖峰会闭门会议

11 月 4 日，由中央网信办网络安全协调局指导，腾讯集团、中国信息安全认证中心、中国金融认证中心、中国电子技术标准化研究院共同主办的首届中国互联网安全领袖峰会 (CSS) 国家会议中心正式闭幕。

主题为“CSO 的 2016 第一步”的企业信息安全闭门交流会以圆桌交流分享的方式进行，安天首席安全官方华、腾讯玄武实验室负责人于旸、启明星辰首席战略官潘柱廷等各安全企业负责人应邀作为嘉宾出席了闭门会议，针对互联网安全状况和应对措施进行了深入探讨和交流。

新闻简报

恶意软件 XcodeGhost 已更新支持 iOS 9：瞄准美国多家机构

研究人员指出，恶意软件 XcodeGhost 已升级，以支持 iOS 9 中新增的特性，还增加了新的机制，已避免自己被检测到。此外，为了避免被基于静态检测的安全工具所发现，XcodeGhost 现已通过一种新的技术来掩盖其 C&C 服务器。除了新版 XcodeGhost S，旧版 XcodeGhost 也已经将目光瞄向了美国的企业，受影响的机构集中在教育、高科、制造、通信、电商、以及金融等领域。(文章来自 techtimes.com)

Chimera 勒索软件恐吓称要将受害人的数据公布到网上

Chimera 勒索软件的一个最新变体出现，它将恐吓软件和传统文件加密操作进行了结合，在对用户计算机中的文件进行加密过后威胁用户。研究发现，这种勒索软件是通过邮件的形式发给受害人的，邮件内中包含了前往 Dropbox 页面的链接。用户打开链接页面就感染 Chimera 勒索软件。(文章来自 securityaffairs.co)

知名论坛程序 vBulletin 5 曝远程命令执行漏洞，可能已泄露千万用户数据

有报道指出 vBulletin 开发者网站遭遇黑客攻击并且泄露了将近 48 万 vBulletin 用户的敏感信息。遭攻击后，vBulletin 官方紧急强制性要求用户重置密码。值得注意的是，即使该漏洞已经被利用并且对成千上万使用 vBulletin 程序套件的论坛网站造成了威胁，官方却并未就此漏洞给出一个明确的警告。(文章来自 nakedsecurity.sophos.com)

全球首位在身体中植入比特币芯片的黑客

瑞典黑客设计了一个巧妙的戏法，只需摇一下手就可以完成购买商品或者银行账户之间转账的行为。软件开发者 PatricLanhed 在其皮下植入了一个很小的 NFC(近场通信) 芯片，该芯片中包含比特币钱包的私人密钥，摇晃手腕，支付数据就会发送到客户端软件，确认密钥的真实性之后即完成比特币转移。(文章来自 thehackernews.com)

每周安全事件

类 型	内 容
中文标题	英国沃达丰公司近 2000 客户资料遭窃取
英文标题	Nearly 2，000 Vodafone UK customers' accounts compromised，blocked
作者及单位	ZeljkaZorz， Help Net Security
内容概述	近日，英国电信公司沃达丰 (Vodafone) 发表声明表示，黑客利用公司外部不明来源取得的电子邮件信箱及密码窃取了英国地区客户的个人资料，包括客户的姓名、手机号码和部分银行账号数据等，共有 1827 个账号遭入侵。少数客户已经遇到利用他们账号数据进行诈欺的行为。 现受影响的客户账号都已被封锁，该公司正直接联系这些用户；并且客户信息已经被下载到 CIFAS 数据库，确保银行或移动运营商进行附加检查，避免欺诈行为。
链接地址	http://www.net-security.org/secworld.php?id=19054

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.wsms.b[prv，exp] 2015.10.29	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。(威胁等级中)
		AdWare/Android.mjgame.a[ads] 2015.11.02	应用含有 mjgame.a 广告插件，运行会联网获取推送列表，执行插屏、通知栏推送等广告展示方式，会造成用户资费消耗，建议卸载。(威胁等级中)
		AdWare/Android.YeahMobi.b[ads] 2015.11.02	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)
		Trojan/Android.SysChecker.e[exp] 2015.11.03	该程序安装无图标，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)
	较为活跃的样本	Trojan/Android.SmsThief.x[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)
		G-Ware/Android.Rootperm.a	该游戏应用包含付费项目，运行后未经用户允许私自下载并启动其他应用，具有一定的流氓行为，请谨慎使用。(威胁等级中)
		Trojan/Android.Fakegupdt.s[exp，rog]	该程序安装运行之后，要求激活设备管理器，使用户不能正常卸载，并捆绑了恶意结构，就算主程序卸载之后还是能存在于设备上，并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。(威胁等级高)
		G-Ware/Android.poemsion.b	该应用运行会频繁联网推送广告，诱骗用户下载安装恶意应用，造成用户资费消耗。(威胁等级中)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Reader 和 Acrobat TIFF 图像处理缓冲区溢出漏洞 (CVE-2010-0188)	Adobe Reader 和 Acrobat 采用的开源 TIFF 图像解析库 libtiff 实现上存在缓冲区溢出漏洞，远程攻击者通过诱使用户使用 Adobe Reader 打开处理恶意 TIFF 图像文件来触发此漏洞，导致在用户系统上执行任意指令，从而控制用户系统。(威胁等级中)
	新出现的样本家族	Trojan[Downloader]/Win32.Genome.qg	此威胁是一种木马类下载程序。运行后链接网络下载配置文件，查找系统中装有的游戏然后判断是否在配置文件中，有则下载此游戏盗号程序。(威胁等级中)
		Trojan[Backdoor]/Linux.Gafgyt.b	此威胁是一种木马类后门程序，运行在 linux 平台，主要功能为 DDOS 攻击、更新和下载等。通过扫描 SSH 弱口令进行传播。(威胁等级中)
		Trojan/Win32.Diztakun.acvz	此威胁是木马类程序。使用 .NET 开发，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。(威胁等级中)
		Trojan[Packed]/Win32.Klone.d	此威胁是一种木马类程序。当用户访问恶意网站它会入侵用户的计算机，它还会通过 USB 进入用户的计算机。它会创建一些危险文件并将其储存在系统根目录中。(威胁等级中)
		Trojan[Backdoor]/Win32.Delf.acqk	此威胁是一种木马类后门程序，该家族的名称是通过开发语言 Delphi 命名来的，家族变种之间具有相同或者相似的源码和核心技术。(威胁等级中)

科技公司抗击解锁设备命令的新方法

Kim Zetter / 文　　安天公益翻译小组 / 译

虽然联邦政府最近不再迫使科技公司在他们的电子设备上安装后门程序，但是这并不意味着美国政府已经放弃了访问受保护电话和其他设备的想法。

上周，纽约一位联邦地方法官作出裁决，对持续 200 年之久，企图迫使苹果等公司解锁其客户的设备的法律条文提出了拒绝。去年，加州的一个地区法院下令苹果为调查人员解锁 iPhone。同样地，曼哈顿地区法院下令一位不愿透露姓名的手机厂商做同样的事情。但是，纽约一个联邦法官拒绝了政府访问调查人员查获的 Apple 设备 (.pdf) 的要求，引发了媒体和行政部门的激烈辩论，至此还没有结果。

纽约东区的大法官詹姆斯・奥伦斯坦并没有顾左右而言他地拒绝该请求，而是要求苹果本周作出回应：禁用问题设备的安全锁，从技术上来说是否可能？他还问苹果，这样做是否会对公司造成不合理的负担。如果事实证明，问题设备并非如《华盛顿邮报》报道的那样，并不运行旧版本的 iOS(旧版本具有内置的功能，苹果公司利用该功能解锁) 而是 iOS 8(苹果公司也无法解锁)，那么这可能是一个有争议的问题。

奥伦斯坦所说的负担，并不仅仅意味着苹果需要付出多大的努力来解锁设备。他还意味着，公司屈服于政府的要求，解锁客户设备所需要承担的成本。

围绕纽约案件的所有资料和文件，除了法官对政府议案的回应，都被密封了。但是，记录的响应表明，政府引用《所有令状法案》，迫使苹果解锁未指定的设备。

《所有令状法案》是《1789 年司法条例》的一部分，该法案在数百年前设立，允许联邦法院在适当的时候发出令状，以迫使第三方帮助执行另一个法院命令，例如搜查令。该令状并不是要结束现有的法规，而只是给法院一个执行现有法规的工具，特别是当法规有空可钻之时。

“总的来说，这是一个补充性的法案，允许法院命令第三方帮助执行搜查令或其他有效的法院命令。”电子前沿基金会的法律研究员安德鲁・克罗克说。

奥伦斯坦指出，如果现有的法律已经覆盖了手头的问题，则法院就不能使用该令状。也不能在“不便或不太合适”时采用现行法规或简单地使用该法令。最高法院也裁定，法院可以签发命令，只要不对第三方带来不合理的负担，就可以要求第三方执行其命令。

“事实上，目前并没有法规明确地给予法院要求公司解锁设备的权力，但是这不应该解释为立法者的疏忽，或者解释为法院应该介入来填补此空白”，奥伦斯坦这样争论说。相反地，缺乏明确的法规似乎也表明立法者颇为矛盾，不知这样的法律是否适当或必要。签发命令迫使苹果解锁设备可不是立法者的意图。

为了加强在目前案例中的要求，政府援引了一个 1977 年纽约电话公司的最高法院判例，法官裁定，法院可以使用《所有令状法案》，迫使纽约电话公司在其设施中安装笔录记录，以协助执行搜查令。法院认为，该电话公司是一个有责任提供服务和经常使用笔寄存器的公共事业机构，因此不应该命令它安装监视工具。法院还指出，令状是很重要的，因为研究人员没有其他方法来获取他们所需要的信息。

然而，奥伦斯坦否定了这种说法，称它不适合目前的情况。作为一个私人商业机构，苹果并不是能够“自由选择保护客户的隐私权，而不屈从于执法部门的竞争利益”的公共事业机构。

奥伦斯坦要求苹果公司在 10 月 15 日之前回应他的问题：解锁设备在技术上是否可行，且不会造成不必要的负担。

如果设备确实使用了 iOS 8 之前的旧版本，那么苹果就没有技术障碍了。不过，他似乎并没有排除另一种负担的可能性：经济和市场负担。

奥伦斯坦在结论中写到：“让消费者以阻碍执法部门访问的方式加密其设备，不可能是苹果匆忙之间决定的，或者没有谨慎地考虑客户的公众安全、个人隐私和数据安全。而苹果可能已经得出结论，即从业务前景来说，不能为客户提供隐私保护，因为这将导致产生长期的成本。”

原文名称	A New Way for Tech Firms to Fight Orders to Unlock Devices
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 10 月 13 日《连线杂志》发布，原文地址 http://www.wired.com/2015/10/a-new-way-for-tech-firms-to-fight-orders-to-unlock-devices/
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。

安天探海 + 追影

阻断 hacking team 两个 flash 漏洞传播的广告木马

近期，安天追影分析小组利用安天自主研发的探海威胁检测系统 (PTD) 捕获到利用 hacking team CVE-2015-5122、CVE-2015-5119 的 flash 漏洞文件传播广告木马。该木马传播范围广，更新变种速度快，受害机器数量多，该组织采用多款木马，在受害机上安装多款流氓软件，并会删除其它流氓软件的桌面快捷方式，使受害的机器桌面“惨不忍睹”。

经安天追影威胁分析系统 (PTA) 分析发现了木马作者注册的大量跳转域名指向阿里云服务器，最终跳转到广告的搜狐 CPA 静默安装包，通过安装 CPA 广告联盟获利。最终发现，相关黑域名之一的注册邮箱为 wangwu121121@yeah.net，注册人为 wanglei，与该名字相关的域名为 support@yinsibaohu.aliyun.com，该邮箱为万网阿里云提供的域名隐私保护域名的服务邮箱；相关黑域名之二为 support@yinsibaohu.aliyun.com，注册人为 xinliu。同时，分析后，可以看到恶意样本有访问“我要啦”网站 (http://www.51.la) 的行为，该网站的业务为统计网站访问量，黑客利用该网站来统计付费安装广告量从而获利。

目前 PTA 追影通过外围检测 (默认正常文件不会进行网络，创建文件等行为) 将其判定为格式漏洞类。以下主要为 PTA 没有体现的异常行为 (可能作为检出方案)：

1. 系统 API 调用方式异常

正常的 API 调用方式一般为在某个应用程序模块中被调用，形如：call XXX

API 调用方式异常体现为：㈠调用的地址不在某个模块中，更多的在用户自行申请的堆等空间中；②获取某个 API 地址为 XXX，直接 jmp xxx，在本例中 shellcode 在同一个 jmp xxx 中调用了 Loadlibrary，InternetOpenA，HttpOpenRequestA 等一系列 API。

2. 修改内存空间保护属性为可执行

在 windows vista 后的操作系统中有了 DEP 保护，为了能成功执行 shellcode 通常都会调用 virtualprotect，virtualalloc 等 API 修改内存区域为可执行，本例中确也执行了本操作但没调用到以上 API。

3. 对象缓冲区长度异常

通常为了实现全内存的读写，将某个对象的缓冲区长度设为超大为其中的一种途径，本例中便是将 vector 缓冲区设为 40000000 字节。

通过对该样本的分析，总结如下：

1) Hacking Team 的数据库泄露事件使网络安全面临新的威胁。

2) 广告联盟产业越来越成熟，驱使付费安装广告类病毒的获利模式日渐成熟。

3) 该木马的威胁还在持续，受害范围广，木马变种快，PTD 与 PTA 会持续监控、追踪。

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。

依据动态行为鉴定器最终将文件判定为木马程序。

文件名	350A0C0F9321E709806D1BD797F8C9A3
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	780 KB
MD5	350A0C0F9321E709806D1BD797F8C9A3
病毒类型	木马程序
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
Trojan/Win32.Danginex	★★★★	疑似查找游戏进程	★★★★

该文件具有以下行为：Trojan/Win32.Danginex；疑似查找游戏进程；创建特定窗体；获取主机用户名称；查找指定内核模块；连接网络；连接特殊 URL；获取计算机名称；获取 socket 本地名称；结束进程；查找特定窗体；启动服务；遍历进程。

◆ 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	★	获取主机用户名称	★
连接特殊 URL	★	查找指定内核模块	★
启动服务	★	连接网络	★
遍历进程	★	获取计算机名称	★
查找特定窗体	★	获取 socket 本地名称	★
		结束进程	★★

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=350A0C0F9321E709806D1BD797F8C9A3
http://antiy.pta.center/_lk/details.html?hash=40FD9150AEA70F3AB72296885409BD74