安天周观察

主办：安天　2015 年 10 月 19 日（总第 12 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天“云”端反恶意代码能力亮相云栖大会

“2015 杭州·云栖大会”10 月 14-15 日在杭州举行。无处不在的云计算与各行各业的交错连接在此次大会集中展示。云计算为产业升级和改革创新提供的源源动力，由“云”建设形成了一个庞大的行业链。

全面保障“云”计算的安全，需要安全生态体系的共同努力，更需要网络安全厂商提供专业的、先进的安全防护手段。“云”建设越是风起云涌，安全的“保驾护航”就越至关重要，“云”的创新越是霞思云想，检测能力的就越需要先进敏锐。

安天作为国内先进的基础检测能力创造者，为云中主机侧提供基于轻代理模式或无代理模式的恶意代码端点防护能力，与其他安全兄弟厂商一同积极维护建立安全的云计算生态环境。

在云栖大会的安天展台上，安天展示了适用于虚拟化平台，专注解决云计算安全问题，保障云平台安全的安天虚拟化安全技术。

中小企业面临更大的电脑黑客威胁

一份报告提到，越来越多的小型企业受到了黑客攻击，由于网络犯罪，澳大利亚的企业每年都要多花费大约 10 亿美元。另外报告称 60% 的企业在受到网络攻击后的六个月内会倒闭。然而大部分的小企业主表示，他们不相信自己的企业正处于被攻击的危险中。报告显示，只有四分之一的小企业主认为自己处于数据被窃取风险中，并且只有不到一半的人表示能坚持使用最新的防病毒软件。只有 2% 的小企业把防御黑客置于优先地位。(http://www.abc.net.au/news/2015-10-12/small-businesses-under-greater-threat-from-computer-hackers/6846024)

美军花费 460 亿构建网络安全数字弹药库

美国网络司令部下一个即将发出的 4.6 亿美金的有关合同中的第一份工作里涉及的所有任务中，除了其他活动，还包括很多电子军需品的制造。发布于 9 月 30 日的 84 页任务草案中包括黑客和反黑客工作，还有传统的 IT 支持活动。这些提出的要求来自完整的 5 年合同中的 114 页草案。文件中指出，最初，工作会按顺序支持“互联网 + 弹药效益” ——通过开发和部署 ——“网络武器”和间谍社区的“工具开发”。

此外，未来的供应商将计划并执行联合“网络大火。”CYBERCOM 公司要为世界各地的团队招募 6200 名网络战士。该命令旨在阻止针对身在美国的外国黑客，帮助美国海外作战部队，并保护密位点网络。(http://www.defenseone.com/technology/2015/10/460m-cybercom-contract-will-create-digital-munitions/122556/)

报评

「云」安全无法缺失反恶意代码检测能力

近几年，大量主机和设施都在向“云”中迁移。为了推动用户对云的信任，增加推广速度，在云的安全防护上产生了一些不正确的观点，有些人认为恶意代码和其他一些威胁可能在云的时代发生湮灭和被削弱。实际上，从现有云的情况和架构来看，云端是现有操作系统的一种虚拟化部署，传统操作系统所面临的各种安全威胁毫无疑问的依然会在云端出现。

安天通过在相关云设施中部署的大量密罐的监控中发现，现有的云中的操作系统无论是 Windows 系统架构，还是 Linux 系统架构都存在着大量的安全威胁，普遍的存在于云中的 Web 服务，计算服务，存储服务三方面。

在云中的 Web 服务上：存在 Webshell 等安全威胁。恶意代码作者利用 Webshell 控制 Web 服务，达到挂链，放马以及入侵和控制云端主机等目的。例如近年来出现的“网络菜刀”，“冰狐”，“魔鬼终结者”等。

在云中的计算服务上：存在 Rootkit，脚本后门，远控木马等。恶意代码作者利用这些恶意程序达到控制虚拟主机的目的。并且利用这些虚拟主机，进行 DDos 攻击，扫描，监控，窃取用户信息等恶意行为，造成了巨大的经济损失。近年来出现的如 Bubnix，木马 -Gh0st，肉鸡 MM，Bladabindi(NJRAT) 等恶意代码。

（下转第四版）

每周安全事件

类 型	内 容
中文标题	美国 Thrift Stores 遭受恶意攻击
英文标题	Malware attack targets America's Thrift Stores
作者及单位	Katie Bo Williams，The Hill
内容概述	10 月 12 日报道，美国 Thrift Stores 表示近日遭受一次东欧黑客的网络攻击。黑客攻击了第三方服务供应商，窃取了信用卡信息。该公司在一份声明中表示，攻击者访问了大量的支付卡号；根据特勤局的调查，客户信息并未遭到泄露，今年 9 月 1 日至 9 月 27 日期间的交易信息可能会受到影响。同时表示恶意软件已经被移除，公司将继续采取相应措施改善安全问题。
链接地址	http://thehill.com/policy/cybersecurity/256702-malware-attack-targets-americas-thrift-stores

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周 9 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	RiskWare[RiskTool]/Android.Koomer 2015-10-10	该应用拦截以指定号码开头的短信接收，同时未经用户允许私自发送短信确认 SP 订购业务，存在恶意扣费和流氓行为。(威胁等级低)
		Trojan[Downloader]/Android.Panev 2015-10-10	该应用为在线批量生成，图标与内容不完全一致，部分应用有下载行为，可能给用户造成一定困扰。(威胁等级中)
		Trojan/Android.SMSSora 2015-10-10	该应用伪装成 Google 相关软件，运行后自动隐藏图标，后台私自发送短信，可能用于订阅服务；拦截屏蔽特定短信，删除通话记录和短信，请用户及时卸载。(威胁等级中)
		Trojan/Android.oneh5 2015-10-11	安装无图标，开机自启动，生成桌面快捷方式，点击后静默下载安装 apk，且根据联网获取参数发送用户短信，造成用户隐私泄漏，建议用户立即卸载。(威胁等级中)
		Trojan/Android.darkmatter 2015-10-12	该程序包含危险代码，通过短信指令拦截短信，删除短信，可能会转发短信，以及下载未知文件，可能会造成用户隐私信息泄露以及流量资费的损失，请不要安装该软件。(威胁等级高)
	较为活跃的样本	RiskWare/Android.E4AQQspy.a	该样本是 E4A 编写，伪装刷 qq 图书 vip，诱导用户输入 qq 账号密码，有盗取用户 qq 账号的风险。(威胁等级高)
		AdWare/Android.linkpush.a 2015-10-08	该应用包含 linkpush.a 广告插件，运行后会联网下载子包动态调用并且在推送弹出广告，安装推广程序，可能造成用户流量资费损失，请谨慎使用。(威胁等级低)
		Trojan/Android.PornDownload.a 2015-10-09	该应用运行后会在桌面上创建色情应用图标，诱惑用户访问色情网址。后台私自下载色情应用，拦截屏蔽特定短信，私自发送短信，可能订阅付费内容。(威胁等级高)
		RiskWare/Android.adcontrolapp.a 2015-10-11	该应用运行时会弹出 pop 广告，点击广告后自动跳转到发送短信，拨打号码和跳转到指定网页，有私自下载安装和卸载的行为。建议用户谨慎安装。(威胁等级低)
PC 平台恶意代码	新出现的 0day	新的 Flash0day 漏洞正被利用钓鱼攻击 CVE-2015-7645	黑客组织 Pawn Storm 正利用该漏洞向多名外交事务人士发动钓鱼攻击，钓鱼邮件内容为国际事件如阿富汗汽车爆炸、叙利亚军队在普京帮助下前进，以色列向加沙目标发射导弹，等等。邮件包括了利用该漏洞入侵目标计算机的恶意链接。(威胁等级高)
		微软修复一严重安全漏洞 MS15-106	攻击者可以利用该漏洞创建一个恶意网站，当用户通过 IE 浏览器点击链接，进入该网站的时候就会让攻击者乘机而入，而攻击者可以通过该漏洞获取系统登陆用户一样的权限。(威胁等级高)
	活跃的格式文档漏洞、0day 漏洞	Office “组合” 式漏洞攻击 CVE-2014-1761	远程攻击者可借助特制的 RTF 数据利用该漏洞执行任意代码或造成拒绝服务 (内存损坏)。(威胁等级高)
	新出现的样本家族	Trojan/Win32.DLLhijack 2015-10-09	此威胁是一类可以劫持 DLL 文件的木马家族。该家族可以劫持系统 DLL 文件，在系统调用 DLL 时先调用恶意文件，完成相关功能后再跳回系统 DLL 里执行。(威胁等级中)
		RiskWare[Downloader]/Win32.FakeWindow2015-10-08	此威胁是一类使用伪装图标迷惑用户的风险软件家族。当用户运行时，即在后台连接网络开始静默下载推广程序并安装，占用系统资源，影响用户使用。(威胁等级低)
	较为活跃的样本	Trojan[Backdoor]/win32.DDOS	次威胁是一种后门类木马程序。运行后创建服务，通过 CMD 隐藏删除自身，链接控制端等待攻击指令。(威胁等级高)

iPhone 恶意软件攻击中国，我们切勿沦为下一个受害者

Andy Greenberg / 文　　安天公益翻译小组 / 译

苹果的 iOS 系统具有良好的安全性。8 年多来，它一直广受欢迎，几乎未曾遭受恶意软件攻击，因此赢得了“世界上最安全的消费者操作系统”的称号。但这一称号在现在的中国，却出现了例外情况。

在刚刚过去的一个月中，中国的 iPhone 和 iPad 用户遭受了两起截然不同的 iOS 大规模恶意软件感染事件。与之前的 iOS 针对性恶意软件不同，许多受害者并没有越狱自己的手机来安装未经授权的应用程序。这两起连续攻击事件 (其中一起远比另一起复杂，但是在 iOS 历史上它们都是前所未有的) 表明，世界各地的 iPhone 用户同样都会遭受讨厌的恶意软件攻击。如果是这样，那么他们怎样才能避免“中国大爆发式攻击”的覆辙?

“iPhone 用户已经很习惯生活在有围墙且舒适恬淡的‘花园中’了，”Palo Alto Networks 首席研究员瑞安・奥尔森表示。该安全公司首先公布了最近的两起中国 iOS 恶意软件疫情。他还说：“过去，他们不必担心犯错。但是现在，黑客们真正的利用这些错误来感染他们的手机了。”

至少，在最近的这两次攻击中，受害者需要执行一系列看似滑稽的失误操作，才能使他们的手机遭到攻击。Palo Alto Networks 详细的分析报告中将该恶意软件称为 YiSpecter，它欺骗用户绕过苹果严格控制的 App Store，安装一个色情视频播放器。众所周知，中国本地互联网服务提供商劫持流量会在网站中插入广告。所以，在某些情况下，黑客会利用在中国本地互联网服务提供商弹出的提示窗中来宣传色情视频应用程序。如果用户禁不住诱惑打开，黑客就能够绕过苹果的 App Store，并使用所谓的“企业证书”(这是一种不需要苹果

公司的审批，允许公司和机构在员工的手机中安装定制程序的系统) 安装应用程序。

恶意视频播放器被称为 QVOD，它会偷偷安装一系列隐藏的应用程序，这些程序利用手机操作系统的某些公开的 API(应用程序编程接口)，黑客能有限地观察手机上其他应用程序的活动。当正常应用程序启动时，YiSpecter 可以插入全屏广告。在越狱的手机中，它还会用中国的搜索引擎—百度替换默认的 Safari 浏览器，这有可能是为了利用百度的联盟来营销交易。另外，如果手机用户找到了恶意攻击并删除了三个隐藏应用程序中的任何一个，其他隐藏应用程序还能够顽强地重新安装。

尽管有这些招数，但细心的用户仍然可以很轻易地避免 YiSpecter。苹果公司已经表示，只有 iOS8.3 和更早的版本会遭受该攻击，后来的版本限制了对 API(YiSpecter 利用 API 植入广告) 的访问。即使在那些早期的、有漏洞的版本中，用户也必须点击提示，选择信任他们从来没有听说过的企业证书。“为了观看色情视频而犯这么一系列的错误，受害者可不是一般的愚蠢。也许，性吸引力让他们失去了理智。但是，他们忽略了一个事实：他们正在跳过一个重要的安全机制。”iOS 法医专家和安全顾问乔纳森・扎德尔斯基说。

换句话说，YiSpecter 的安全教训是相当明显的：不要安装出现在弹出窗口中、却不存在于苹果 App Store 的陌生应用程序；不要轻易地同意、信任或点击可疑企业的证书；不要越狱你的 iPhone。并持续更新你的软件。(事实上，iOS9 要求想要安装具有企业证书的应用程序的用户更改其设置，增加了更多的绕过苹果 App Store 的提醒。)

但是，对于三周前攻击 iOS 设备的恶意软件感染，长期解药也不是那么容易得到的。更早、更严重的攻击 (Palo Alto Networks 在一系列文章中将其称为 XcodeGhost) 至少感染了 39 个合法的应用程序，其中包括著名的中国社交媒体应用程序微信和优步在中国的最大竞争对手滴滴打车。Palo Alto Networks 怀疑它可能感染了数以百万计的设备，感染性和影响力很可能远远超过了 YiSpecter 恶意软件。

XcodeGhost 恶意软件的作者免费传播苹果开发程序 Xcode 的恶意版本，从而实现了前所未有的大规模感染。由于中国开发者与美国服务器的连接较慢，所以很多人转而从百度云存储平台下载了该开发工具的某个版本。这一非授权的 Xcode 副本旨在用恶意软件污染开发者的应用程序，而苹果的 App Store 评审者 并没有发现许多受感染的应用程序，让它们入驻 App Store。之后，恶意应用程序就通过钓鱼手段获取用户名和密码，并将它们发送回一个 C&C 服务器，这是一个真正成熟的、非常讨厌的黑客攻击。

苹果公司虽没有对最近两次 iOS 攻击发表评论，但它似乎已经学到了一些教训，它清除了 App Store 中被感染的应用程序，并在中国增设了服务器，以提高 Xcode 工具的本地可用性。相信，苹果在今后也会更加仔细地审查应用程序。

“iOS 用户能从此次攻击事件中学到什

(下转第四版)

原文名称	iPhone Malware Is Hitting China. Let’s Not Be Next
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 6 日《连线杂志》发布，原文地址 http://www.wired.com/2015/10/iphone-malware-hitting-china-lets-not-next/
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。

恶意程序

本周，一个恶意代码的感染量多达 4 万多次，安天 CERT 的研究人员发现这是一种后门类木马程序，主要通过扫描有漏洞或弱口令的主机自动进行下载执行来传播。安天【追影高级持续威胁分析系统】无需更新病毒库，即可实现对恶意程序码进行有效检测，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，经由安全云鉴定器、静态分析鉴定器、动态行为 (默认环境) 鉴定器等鉴定分析。

依据安全云鉴定器、静态分析鉴定器、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：使用 cmd 删除自身；访问 DNS；访问文件尾部；创建服务；增加 run 自启动项；获取计算机名称；更新服务配置信息；释放 PE 文件；获取驱动器类型；文档篡改；独占打开文件；结束进程；连接网络；启动服务。

同时，该文件会对虚拟机、沙箱技术进行检测。

文件名	get.exe1
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	84 KB
MD5	0B149F4EA7618A1D009409E889541B89
病毒类型	恶意程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Win32.DDOS
判定依据	安全云

◆ 危险行为

行为描述	危险等级
使用 cmd 删除自身	★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
访问 DNS	★	访问文件尾部	★
增加 run 自启动项	★	创建服务	★
更新服务配置信息	★★	获取计算机名称	★
释放 PE 文件	★	获取驱动器类型	★
独占打开文件	★	文档篡改	★★
启动服务	★	结束进程	★★
连接网络	★		

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=0B149F4EA7618A1D009409E889541B89

(上接第一版)

在云中的存储服务上：恶意代码作者利用分发和共享的机制传播恶意代码，虽然云中的存储服务给用户带来了便利，但同时也为恶意代码传播提供了更好的途径。恶意代码可以通过共享更加容易且快速的进行恶意代码的扩散，使大量云端主机被感染。

另外，在 Linux 平台下，出现了 Windigo 和 Hand of Thief 等恶意代码。同时，亦发现了云平台的大量主机因对破壳漏洞的修补不够彻底，或存在弱口令等情况，导致被大量的远控木马所植入，或被僵尸网络所感染。因此，形成有效的云端安全，并确保用户在云端的体验不被干扰，在云端虚拟化部署的节点中建立恶意代码的检测防护能力是十分必要的。

但从技术角度来看，云端的恶意代码检测与传统的主机端和服务器端的恶意代码检测有所不同，需要考虑的方向也有差异，很多都不是容易解决的问题。比如传统恶意代码检测资源的占用较高，现有的反病毒软件所占有的空间都在百兆以上，并且一个实体节点上存在多个虚拟节点，这意味着有极大的内存及磁盘会被反病毒软件所占用。同时，在扫描的问题上，如果多台机器并发扫描，会产生严重的 I/O 风暴，对系统的正常运行有很大影响。除此之外，还有部署难度高，缺少统一管理等需要考虑的问题。

从技术的角度来看，恶意代码检测需要有专业的反病毒技术和经验。其次，从虚拟化产品提供的接口来看，虽然 VMvare 为无代理检测技术预留有相应的接口，但如 kvm 等大量的开源虚拟产品在这一方向并没有给出相应的设计，而是需要使用者自己编写。

在这种情况下，国外厂商趋势、国内安全厂商安天等都陆续推出了具有高效资源利用率，快速安全反应力、部署力、能够统一管理、全面防护的云端安全解决方案，从全局视野把控云端安全。“云”建设越是风起云涌，安全的“保驾护航”就越至关重要，“云”的创新越是霞思云想，检测能力的就越需要先进敏锐，在“云”的时代，反恶意代码检测能力仍然是安全不可欠缺的基础能力。

(上接第三版)

么？这不是那么简单就能得出结论的。对用户来说，除了谨慎地下载应用程序，能做的其实并不多。”扎德尔斯基说。但是，他也承认，这是一个艰难的战略，因为信誉良好的公司 (如微信、滴滴打车和中国联通) 的开发者也被该伎俩欺骗了。扎德尔斯基指出，认为该攻击只针对中国是很愚蠢的，正如《拦截者》在 3 月份报告的，CIA(美国中央情报局) 正在考虑对目标启动同样的 Xcode 攻击。

苹果安全分析师理查·摩古尔表示：开发者最有责任防止下一个 XcodeGhost 式的爆发，而非用户 (包括苹果)。这将意味着，开发者应使用信誉良好的开发工具，并检查应用程序的加密哈希，以确保他们没有被改变。“开发者要醒一醒了，要意识到他们沦为了攻击目标。”他说道。

“好消息是，这两起恶意软件爆发采用有限的方式规避 iPhone 的安全措施，并不能从根本打破安全措施来执行更广泛的攻击；有趣的是，例如，这与 Windows XP 的恶意软件完全不同。”摩古尔说这样评论 Xcode 攻击。”

摩古尔还提到了黑客公司 Zerodium 近期公布的 100 万美元赏金计划，该公司悬赏能够通过短信或受感染网页攻击目标 iPhone 的入侵技术。摩古尔说：“这么大一笔奖金真是不错，有人愿意支付 100 万美元购买 iPhone 漏洞利用代码让我感觉更不错。”