安天周观察

主办：安天　2016 年 12 月 19 日（总第 69 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天应邀参加 2016 企业服务高峰论坛

12 月 16 日，由中科院《互联网周刊》、中国社会科学院信息化研究中心、eNet 硅谷动力网共同举办的 2016 中国互联网经济论坛在京开幕。安天应邀在企业服务高峰论坛发表讲话。

论坛由中企动力副总经理吴倩然主持，安天企业安全副总经理、解决方案负责人韩晟，南大通用副总裁、战略营销部总经理杜国旺，华云数据执行副总裁马杜等多位互联网企业高管参会。会议就企业服务解决方案展开讨论，集中探讨了企业服务市场现状、发展前景等内容。

会上，安天企业安全副总经理、解决方案负责人韩晟针对网络安全专业服务发表了讲话。他表示，目前网络安全专业服务市场空间较大，但行业正面临内部从业人员技术和服务标准化能力有待提高，外部市场对网络安全专业服务价值认识不足的困难。综合来说，网络安全行业的发展需要专业能力强、学习能力强的企业为用户提供更多的价值。这不仅需要从业者不断提升自身专业素质，更需要企业提升专业能力。

安天从反病毒引擎研发团队起步，目前已发展成为以安天实验室为总部，以企业安全公司、移动安全公司为两翼的集团化安全企业。安天始终坚持以安全保障用户价值为企业信仰，崇尚自主研发创新，在安全检测引擎、移动安全、网络协议分析还原、动态分析、终端防护、虚拟化安全等方面形成了全能力链布局。安天坚持“服务客户，解决问题。应对威胁，保障价值！”的产品和服务导向，将大数据分析、安全可视化等方面的技术与产品体系有效结合，以海量样本自动化分析平台延展工程师团队作业能力，缩短产品响应周期，目前监控预警能力覆盖全国、产品与服务辐射多个国家。

安天获得通信网络安全服务能力资质

12 月 16 日，安天获得中国通信企业协会通过的“通信网络安全服务能力（安全设计与集成一级）资质”。该资质是对通信网络安全服务单位从事通信网络安全服务综合能力的评定，包括：技术能力、服务能力、质量保证能力、人员构成与素质、经营业绩、资产状况等要素。

安天此次获得通信网络安全服务能力资质，是其获得进入运营商市场的重要条件之一。它标志着安天安全服务能力通过中国通信企业协会等组织的检验，也表明安天可以为通信运营商提供更有保障的安全服务。

安天将会充分发挥自身技术优势，为网络与信息安全保驾护航，为营造健康、文明的网络环境做出应有的贡献。

安天入选 2016 电信和互联网行业网络安全试点示范项目

近日，工信部根据《工业和信息化部关于开展 2016 年电信和互联网行业网络安全试点示范工作的通知》，经专家评审，遴选出 49 个拟纳入电信和互联网行业网络安全试点示范的项目，并予以公示。其中，安天网络安全态势感知与通报预警平台项目入选示范项目。

此次，网络安全试点示范工作，在 2015 年工作基础上，将试点示范工作覆盖对象拓展至互联网企业和网络安全企业。安天作为我国重要的网络安全技术自主创新企业，安天很早就承担起国家级网络安全应急支撑单位工作，并推出了应对高级持续性威胁 (APT) 和面向大规模网络与关键基础设施的态势感知与监控预警解决方案。

安全新闻

◆ Edge 浏览器新 Bug 曝光：SmartScreen 或被利用来欺诈

近日，在一份新报告中，阿根廷安全研究人员 Manuel Caballero 发现，欺诈者竟然可以强制 Edge 浏览器显示虚假的 SmartScreen 错误警告，然后提取用户的个人信息。Manuel Caballero 披露，如果欺诈者成功地利用了这个 bug，即可显示一条本地警告消息，并替换上一个请求更多信息的链接，欺骗用户去点击。他还表示：“我们创建了一个可以自动生成的，电话号码样式的链接，受害者可以‘一键呼叫’，这显然给诈骗者省了很多工夫。”

目前，微软暂未回应是否已在着手修复 Edge 浏览器中的这个 bug。（来源：http://www.cnbeta.com/articles/566901.htm)

◆ 低端 Android 设备固件发现恶意程序

近日，俄罗斯安全公司的研究人员从 26 款使用联发科平台的低端 Android 设备固件中发现名为 Android.DownLoader.473.origin 的木马，它会在用户设备上展示广告、安装用户不需要的应用、打开浏览器特定链接和拨打特定电话等。

这些智能手机都在俄罗斯销售，木马被认为是参与固件开发的外包公司所做。Dr.Web 已通知联发科和设备制造商。（来源：http://www.solidot.org/story?sid=50725)

每周安全事件

类 型	内 容
中文标题	雅虎官方证实 10 亿用户账户信息失窃
英文标题	Yahoo says hackers stole ONE BEELLION user accounts
作者及单位	Darren Pauli；The Register
内容概述	近日，雅虎官方证实超过 10 亿用户账户信息在 2013 年的 cookies 伪造攻击中失窃，这起事件与之前披露的 5 亿用户账户信息失窃不相关。雅虎称，未经授权的第三方在 2013 年 8 月窃取了超过 10 亿用户账号的数据，窃取的信息包括了用户名、电子邮件地址、电话号码、出生日期、MD5 未加盐哈希密码以及部分加密或未加密的安全问题和答案。雅虎称，密码不是明文的，但 MD5 哈希密码早就被认为不再安全。雅虎表示，银行账号信息和支付卡信息没有储存在被入侵的服务器上。雅虎称，调查显示攻击者通过学习雅虎的专有代码学会如何伪造成 cookies，然后利用伪造的 cookies 不用密码就能访问用户账户。雅虎已让伪造的 cookies 失效。它表示在 2013 年夏天开始使用 BCrypt 哈希加盐保护用户密码，但遭到攻击时尚未完成升级。
链接地址	http://www.theregister.co.uk/2016/12/14/one_billion_yahoo_accounts_stolen/?utm_source=tuicool&utm_medium=referral

每周值得关注的恶意代码信息

经安天检测分析，本周有 9 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

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.Exaspy.a[prv, exp]2016-12-12	该应用会伪装成正常应用，运行后会激活设备管理器，隐藏图标，后台窃取用户短信、联系人、地理位置等隐私信息，并控制完成拍照、录音等操作，私自下载色情应用，造成用户隐私泄露和资费损耗。建议卸载。(威胁等级高)
		Trojan/Android.PornAd.b[rog, exp]2016-12-14	该应用伪装成系统应用，安装后无图标显示，运行后会显示色情广告，私自下载色情应用，并频繁弹窗诱导用户安装，造成用户资费损耗。建议不要安装。(威胁等级高)
		Trojan/Android.Gudex.b[exp] 2016-12-15	该程序安装运行后，会在后台自动向指定号码拨出电话，给用户造成资费损失。请谨慎使用。(威胁等级中)
	较为活跃的样本	RiskWare/Android.FakeApp.cg[exp]	该应用为虚假的微信应用，无其他功能。建议卸载，使用正版应用。(威胁等级低)
		PornWare/Android.E4Asexplayer.d[pay, exp]	该应用为 E4A 开发的色情播放器，运行后会诱导用户点击付费下载，造成用户资费损耗。请使用绿色健康软件。(威胁等级低)
		Trojan/Android.QQspy.q[prv, exp]	该应用会伪装成 QQ 刷钻、监控类等应用，诱导用户输入 QQ、微信等账号和密码并短信转发，造成隐私泄露和资费损耗，建议卸载。(威胁等级中)
		Trojan/Android.Triada.t[exp]	该程序会运行动态加载恶意子包，在通知栏推送广告，私自下载应用程序并弹出安装提示，诱导用户安装。建议立即卸载，避免资费损耗。(威胁等级中)
		Trojan/Android.HiddenApp.k[exp, rmt]	该应用运行后会加载隐藏在 Assets 下的恶意代码，隐藏自身图标，监听用户收件箱，拦截短信，根据接收到的指令，删除包含特定字段的短信，获取用户固件信息，并上传和运行日志，静默安装未知应用，会造成用户隐私泄露和资费消耗。建议卸载。(威胁等级高)
		RiskWare/Android.Downloader.cs[exp]	该应用程序安装后无图标显示，动态加载释放并加载子包，会实现闹钟应用功能，当加载过程出现异常时，会不提示用户而私自从指定 URL 下载更新子包，也不会判断设备当前所处网络为 WiFi 还是数据流量，会造成用户流量资费一定程度上的损失。建议谨慎下载使用。(威胁等级中)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 损坏索引 CVE-2014-6334 内存破坏漏洞 (MS14-069)	Microsoft Word 在分析经特殊设计的 Office 文件时未正确处理内存中的对象，则会导致当前用户的上下文中存在远程执行代码漏洞。这可能允许攻击者执行任意代码，从而损坏系统内存。以下产品受到影响：Microsoft Word 2007 SP3、Word Viewer、Office Compatibility Pack SP3。(威胁等级高)
	较为活跃的样本	Trojan/Linux.PNScan	此威胁是一类基于 Linux 系统，可以通过扫描感染设备的木马家族，该家族样本运行后会接受参数，并根据这些数据决定攻击的类型以及需要扫描的 IP 地址范围，它会利用远程代码执行漏洞来运行一个相对应的 SH 脚本。感染设备后它可以加载多种恶意代码，有一定威胁。(威胁等级高)
		Trojan[Spy]/Win32.Bewymids	此威胁是一种收集用户信息并回传的木马家族，该家族样本运行后会将系统信息通过 GET 请求回传，会下载其他恶意代码。(威胁等级中)
		Trojan[Backdoor]/Win32.Volus	此威胁是一种可以窃取用户敏感信息的木马家族，该家族样本运行后会连接远程服务器，攻击者可以执行恶意操作，下载其他恶意代码，有一定威胁。(威胁等级高)
		Trojan[Backdoor]/Win32.Dluca	此威胁是一种可以窃取用户敏感信息的木马家族，该家族样本运行后会连接远程服务器，将系统版本、屏幕大小、使用语言等信息通过 GET 请求回传给攻击者。(威胁等级高)

Mirai 僵尸网络仍在肆虐

Lily Hay Newman / 文　安天公益翻译小组 / 译

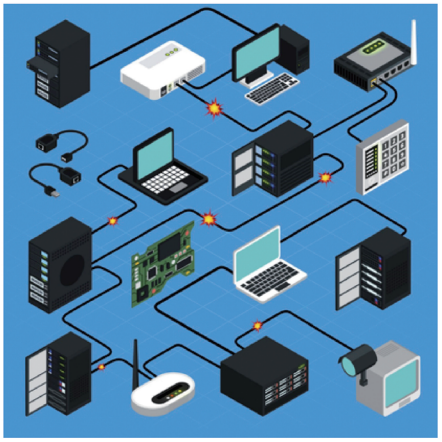
Mirai 僵尸网络在今年 9 月首次出现，它的登场让人“惊艳”。它利用僵尸物联网设备的流量发动洪泛攻击，通过攻击 Dyn(提供很大一部分的美国骨干网) 导致数百万用户无法上网。从那时起，攻击数量就不断增加，这也使我们越来越清楚地意识到，Mirai 具有强大的破坏力。

Mirai 是一种自动寻找物联网设备进行感染，并将其纳入僵尸网络的恶意软件。Mirai 的物联网设备发起了 DDOS 攻击，用大量的垃圾流量洪泛目标的服务器。

近期，Mirai 破坏了 90 多万德国电信客户的互联网服务，并感染了英国近 2400 个 TalkTalk 路由器。随后，研究人员发布的证据显示 80 个索尼相机型号容易受到 Mirai 的感染。

Mirai 控制了大量的调制解调器和网络摄像头。而且名为“Anna-senpai”的黑客在 9 月公开了它的代码，导致 Mirai 攻击层出不穷。虽然 Mirai 的软件没有什么特别的新奇之处，但是它非常灵活，适应性很强。因此，黑客可以开发不同的 Mirai 变种，来控制新的物联网设备，增加 Mirai 僵尸网络可以利用的设备。

Qualys 的产品管理副总裁克里斯 · 卡尔森 (Chris Carlson) 说：“因为大量的物联网设备处于开放、无保护的状态，所以 Mirai 正在加速增长，不断地将这些设备纳入僵尸网络。”



物联网恶意软件的崛起让人联想到，困扰早期互联网用户的病毒、蠕虫和垃圾邮件。当时，大多数电脑没有足够的安全措施，争相进入网络泡沫的公司也不一定了解互联网安全的重要性。现在也是如此，只是其目标从电脑转向网络摄像头和路由器。

然而，如今的技术时代有着明显的不同之处，即用户如何与被感染的设备交互。被感染的电脑通常会出现故障，运行速度减慢或弹出通知。有明显的表象在提示人们应该采取措施。企业用户可以再 PC 上安装安全软件，家庭用户也可安装反病毒软件。

Mirai 很难控制的一个原因是它潜伏在设备中，并且通常不会显著地影响它们的性能。普通用户很难想到他们的网络摄像头已经沦为了僵尸网络的一部分。即使能够确定，他们也基本无计可施，没什么有效的方法来修复被感染的产品。

网络安全防御公司 Digital Shadows 的战略副总裁瑞克 · 霍兰德 (Rick Holland) 说：“这类似于 21 世纪初的网络安全状况，设备缺乏安全性。漏洞设备的数量不会减少，反而会增加。”

Mirai 并不是唯一的物联网僵尸网络。越来越广泛的物联网设备安全问题不容易解决，数十亿设备面临各种恶意软件的攻击。

霍兰德指出，Digital Shadows 研究人员发现越来越多的 Mirai 用户寻求帮助 (有时恶意行为者也需要技术支持！)，彼此提供提示和建议。

消费者可以采取一些预防措施来提高个人物联网的安全性。通过评估家中使用的物联网设备的必要性，进行消除直接访问互联网的多余智能产品，减少攻击风险。此外，对于提供可访问接口的设备，可以更改默认密码和下载固件更新以获得更好的保护。

正如关键基础设施技术研究所发布的报告一样，在物联网安全全景中，Mirai 终将成为一个“阶段性威胁”。有了新玩具，黑客就会对 Mirai 失去兴趣，受 Mirai 感染的设备数量也会减少。

霍兰德说：“谁知道今年结束之前会出现什么呢。但是能够肯定的是，Mirai 不会很快消失。”

原文名称	The Botnet That Broke the Internet Isn't Going Away
作者简介	Lily Hay Newman，《连线杂志》安全领域作者。
原文信息	2016 年 12 月 9 日发布于《连线杂志》，原文地址 https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-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。

安天发布《Crane 样本分析报告》

近日，安天追影小组在整理网络安全事件时，针对 Windows 平台下名为 Crane 的木马进行了简要分析。该木马的攻击目标包括：两家专门从事起重机和辅助设备的大型公司。当发现恶意软件时，攻击者已经进行了一段时间的从受感染系统中窃取机密信息的活动。

Crane 一直被用来窃取财务文件、协议和内部业务通信，因此认为此次攻击是一些不道德的企业对手蓄谋的间谍活动的一部分。一旦设备被感染，Crane 就会连接其 C & C 服务器并等待指示。攻击者可以安装各种模块，每个模块用于执行特定任务，例如在命令提示符中执行命令、从指定链接下载文件、通过 FTP 或 HTTP 上传文件以及截图等操作。一些模块还下载了几个基于 Python 的木马，其中一个可以执行与 Crane 相同的命令，但它也可以从指定的路径获取文件和文件夹的列表、删除文件、终止进程、复制文件和终止本身等。另一个则可以在受感染的设备上打开一个 Shell。恶意软件的开发者错误地留下的“关于”窗口，表明 Crane 的第一个版本是在 2015 年推出的，但是目前发现的样本中也存在 2016 年 4 月编译的。

通过对 Crane 样本进行分析可知，Crane 木马程序启动后会创建不同的进程，并进行 Internet 网络连接。此木马对文件和注册表的操作比较频繁，Crane 会根据文件名在一个文件夹 (包括子文件夹) 中，搜索与指定的文件名相符的所有文件。同时，该木马会查询文件的基本信息，诸如文件的读写时间、属性等。此外，Crane 木马会创建文件，其创建的大多是 .dll 文件。由于某些原因，在创建某些 .dll 文件时会因找不到文件名而失败。最后，Crane 会通过创建一些具有扩展风格的重叠式窗口、弹出式窗口或子窗口来进行消息传递。

通过对后门程序 Crane 的分析可知，恶意软件的危害日益严重。安天提醒广大电脑使用者要提高网络安全意识，定时给电脑进行体检以确保在受到恶意软件入侵时能及时发现并处理。具备良好的数据备份习惯，重要文件须加密保存和备份，尽量减小在设备受到攻击时带来的损失。

安天在对恶意软件的防范进行着长期的工作，并会持续关注追踪恶意软件的发展态势，为客户提出更合理的建议。

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，以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、YARA 自定义规则鉴定器、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、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。

最终依据动态行为鉴定器将文件判定为木马程序。

该文件具有以下行为：

获取系统版本、获取主机用户名称、连接特殊 URL、文件下载、遍历进程、获取驱动器类型、获取系统内存、独占打开文件、获取计算机名称、疑似桌面控制。

文件名	361C983B94B3E07A3B509F0B9B34CAD7
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	330 KB
MD5	361C983B94B3E07A3B509F0B9B34CAD7
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Crane.a
判定依据	动态行为

报告地址：https://antiy.pta.center/_lk/details.html?hash=361C983B94B3E07A3B509F0B9B34CAD7

◆ 运行环境

操作系统	Windows XP 5.1.2600 Service Pack 3 Build 2600
内置软件	默认，IE6，Office 2007，Flash，WPS，FoxitReader，Adobe Reader

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
获取系统版本	★★	获取主机用户名称	★
连接特殊 URL	★	文件下载	★
获取驱动器类型	★	遍历进程	★
独占打开文件	★	获取系统内存	★★
获取计算机名称	★	疑似桌面控制	★