安天周观察

主办：安天　2017 年 8 月 14 日（总第 99 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天获《信息系统集成及服务资质证书》

近期，安天收到中国电子信息行业联合会颁发的《信息系统集成及服务资质证书》，核定安天的信息系统集成与服务资质为叁级。该资质由中国电子信息行业联合会认定、授予，用于证明持证单位从事信息系统集成业务的综合能力，包括技术水平、管理水平、服务水平、质量保证能力、技术装备、系统建设质量、人员构成与素质、经营业绩、资产状况等要素。

安天长期在威胁检测领域深耕细作，倡导技术创新，重视知识产权，凭借多年的积累和投入，成功成为国家知识产权优势企业和国家级专利示范企业，并且首批通过了《企业知识产权管理规范》国家标准认证。安天在方程式、白象、魔窟等重大安全事件中提供了先发预警、深度分析或系统的解决方案，多次在重大网络事故和网络安全事件的响应中发挥关键作用，技术实力得到行业管理机构、客户和伙伴的认可。

上述资质的取得，是对安天信息系统安全防护和服务能力的充分肯定，表明安天信息系统集成与服务方面具有较强的综合实力，为安天在网络安全领域深度发展提供了有力的保障。

中央网信办移动网络管理局局长方楠一行视察安天

近日，中央网信办移动网络管理局局长方楠、中央网信办移动网络管理局综合处副处长宋阳等一行领导莅临安天视察，安天相关负责人作了汇报。

在安天应急响应中心，安天技术负责人向来宾介绍了安天持续与网络安全威胁对抗的情况，特别汇报了对高级威胁发现、捕获、分析方面所做的工作，重点介绍了安天针对“APT-TOCS”、“白象”、“方程式”等攻击组织对我方 APT 攻击情况、所使用的攻击装备等的分析进展。

在参观过程中，方楠局长对安天的技术能力及取得成果表示认可，并针对安天的产品、发展历程等各方面情况进行询问，与安天负责人进行了详细交流。

哈尔滨市工信委科技合作处处长白玉一行莅临安天参观指导

近日，哈尔滨市工信委科技合作处处长白玉一行来到安天考察，并听取了关于安天最新发展状况和项目情况的汇报。

在展示厅内，安天负责人为考察组介绍了安天的发展历程、安天参与重大活动的网络安保支撑、安天总体规划以及在技术创新和专利技术方面取得的部分成果。同时，考察组详细了解了安天针对恶意代码和重大安全攻击事件所发布的分析报告和安天全线产品。

安天为用户提供端点防护、流量监测、深度分析、威胁情报和态势感知等相关产品、解决方案与服务。同时，全球超过一百家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎目前已为全球近十万台网络设备和网络安全设备、及超过六亿部手机提供安全防护。

白玉处长对安天所取得的技术成果给予肯定，参观过程中提出对信息安全产业和安天发展状况的疑问，安天负责人作了解答。

■ 乌克兰国家邮政服务机构两日连遭 DDoS 攻击

近日，乌克兰国家邮政服务机构 Ukrposhta 遭受黑客为期两天的分布式拒绝服务 (DDoS) 攻击，导致计算机网络系统运行缓慢，甚至出现中断现象。

据 Interfax 通讯社消息，受害计算机网络系统与包裹在线跟踪系统有关。黑客利用僵尸网络向 Ukrposhta 服务器发送大规模流量，强制网站离线。Ukrposhta 发言人表示，此次攻击活动导致官网与相应服务普遍遭受影响。7 月下旬，Ukrposhta 曾在一份季度报告中证实，黑客通过乌克兰会计公司使用的 MeDoc 软件自动更新传播勒索病毒 NotPetya，导致公司自动化邮件系统完全崩溃。（来源：http://hackernews.cc/archives/13280）

■ 英国新安全法案加强关键基础设施网络防御体系

近日，英国政府推出一项新安全法案，旨在保障国家关键基础设施安全。法案指出，提供能源与交通等基本服务的供应商需要制定一份安全紧急方案，以解决电力故障或环境灾难所带来的严重影响。倘若此类公司未能有效实施网络安全措施，或将面临巨额罚款，其金额最高可达 1700 万英镑。目前，该法案集数字、文化、媒体与运动为一体，符合欧盟《网络与信息安全指令》(NIS 指令）的要求并将于明年 5 月生效执行。调查显示，由于英国提供关键基础设施的组织于近期在勒索软件 WannaCry 与 NotPetya 攻击事件中普遍遭受影响，因此政府不得不加快安全法案的制定。（来源：http://hackernews.cc/archives/13276）

每周安全事件

类 型	内 容
中文标题	微软将不再信任沃通和 StartCom 颁发的证书
英文标题	Microsoft to Ban WoSign，StartCom Certificates
作者及单位	Eduard Kovacs；SecurityWeek
内容概述	近日，微软通知用户，旗下产品很快也将不再信任沃通和 StartCom 颁发的证书。从 2015 年一月开始，这两家 CA 就曝出了各种问题，包括恶意签署更早时间的 SHA-1 证书、在未授权的情况下颁发证书，还有就沃通和 StartCom 的关系误导浏览器厂商等，Mozilla、苹果和谷歌都相继决定不再信任沃通和 StartCom 的证书。微软最终也做出了这一决定，不过微软此后会继续信任今年 9 月 26 日之前颁发的证书，到其过期为止，在此之后颁发的证书则会直接不信任。值得一提的是，近期遭遇麻烦的 CA 机构并非只有沃通和 StartCom，谷歌宣布从明年 10 月开始不再信任赛门铁克颁发的所有证书，赛门铁克最近宣布将证书业务出售给 DigiCert。
链接地址	http://www.securityweek.com/microsoft-ban-wosign-startcom-certificates

每周值得关注的恶意代码信息

经安天检测分析，本周有 8 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	相关描述
移动恶意代码	较为活跃样本	Trojan/Android.FakeApp.cx[exp，rog]	该应用伪装成安全软件，无实际功能。运行会隐藏图标。获取电话号码、IMEI 等固件信息，损害用户隐私；会将短信插入收件箱，具有一定流氓性；推送广告，影响用户体验，建议谨慎使用。（威胁等级高）
		Trojan/Android.FakeSystem.g[exp，rog]	该应用安装运行后隐藏图标，会私自与指定 URL 建立网络连接，上传用户设备固件信息等隐私数据，并下载未知数据，静默安装未知应用，推送广告。会给用户造成流量资费损失及体验上的影响，建议立即卸载。（威胁等级高）
		Trojan/Android.oxti.r[exp]	该应用会隐藏图标，后台频繁访问色情网站，造成用户流量耗费，建议立即卸载。
		Trojan/Android.Joyreach.e[exp]	该应用运行会加载广告，私自提权，静默安装未知应用，建议立即卸载。（威胁等级中）
		Trojan/Android.SmsThief.be[prv]	该应用伪装成 Flash Player，程序运行会监听短信，获取短信信息联网上传，造成用户隐私泄露。（威胁等级高）
		Trojan/Android.FakeApp.db[exp]	该应用伪装成手机百度，程序运行会启动浏览器访问指定网址，安装桌面快捷图标，判断是否安装相关组件并启动，私自下载造成用户资费消耗。（威胁等级高）
		Trojan/Android.Triada.l[exp，sys]	该应用程序伪装成正常应用，安装无图标显示，运行后获取 root 权限，静默卸载应用；同时包含私自下载静默安装的风险方法，会造成用户资费损耗和影响系统安全，建议立即卸载。（威胁等级高）
		Trojan/Android.AnalyzerSpy.b[prv，rmt，spy]	该应用运行会请求激活设备管理器禁止卸载，窃取短信、通话记录，后台拍照录音，开启后门，造成用户隐私泄露，建议及时卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows Search 远程代码执行漏洞 (CVE-2017-8620)	Windows 搜索服务 (WSS) 是 Windows 的一项默认启用的基本服务。当 Windows 搜索处理内存中的对象时，存在远程执行代码漏洞， 成功利用此漏洞的攻击者可以控制受影响的系统。攻击者可以安装程序、查看，更改或删除数据、或创建具有完全用户权限的新账户。此外，在企业场景中，远程未经身份验证的攻击者可以通过 SMB 连接远程触发漏洞，然后控制目标计算机。
	较为活跃的样本	Trojan[Ransom]/Win32.CryptoBit	此威胁是一种勒索者家族程序。这种家族的样本伪造为播放器图标，对文档进行加密，连接 C&C 服务器 (laoismacau.com/58.64.142.89，未使用 DGA)，并在多个文件夹下留下勒索信 "HITLERHASYOURFILES"，在『我的文档』留下被加密过的文件的列表。CPU 占用较低，不易察觉。（威胁等级中）
		Trojan[Backdoor]/Win32.FinFish	此威胁是一类可以窃取用户信息并回传的木马家族。该家族样本运行后连接远程服务器，收集系统信息并回传，运行后会自删除。（威胁等级中）
		Trojan[Downloader]/Win32.VB	此威胁是木马类程序。使用 VB 开发，运行后会连接网络下载其它恶意程序，并获取系统信息及用户信息等，发送数据到远程服务器。（威胁等级中）
		Trojan[Backdoor]/Win32.Agent	此威胁是一种木马类后门程序，是一个通过代码基因来定性的木马类程序，家族变种之间具有相同或者相似的源码和核心技术。它可以连接远程服务器接受攻击者恶意操作，包括下载与更新其它恶意代码、添加删除系统文件、窃取用户敏感信息等。（威胁等级高）

机器人和 AI 技术在医疗领域的应用挑战

Ashley Amaral，Vashist Krishna / 文　安天公益翻译小组 / 译

尽管人工智能 (AI) 和机器人技术能够解决当今的许多医疗挑战，但是这些技术必须克服若干障碍，才能大大改善我们的医疗服务系统。

人工智能是指在复杂的医疗数据分析中使用近似人类认知的算法，目的是确定预防或治疗技术与治疗结果之间的关系。机器人技术主要涉及机器人的设计，开发和操作，将其用于患者监控、评估以及手术辅助等活动。AI 辅助的机器人技术有可能完全改变医疗方式，因为机器有可能变得足够强大和聪明，足以替代医师和医务人员。

此外，机器人 /AI 技术的临床应用正在不断增长，越来越多的大型提供商携新兴技术进入了这一领域。尽管 AI 和机器人技术潜力无限，但是有几个挑战阻碍了它们的迅速应用。

技术和数据限制

在电子病历 (EHR) 整合方面，最大的障碍之一是提供完整和全面的患者数据。许多 AI 技术依赖于输入大量数据来执行高级分析，但是如果不能全面了解患者的病史，AI 系统就无法运作。甚至会威胁患者的健康。

不幸的是，当前医疗提供商收集和维护患者数据的方法是不够全面的，互操作性的固有复杂性又加剧了这一问题。提供商面临数百种 EHR，每种都具有不同的数据架构，他们难以为患者维护单一、全面的病例。无法与其它 EHR 集成以了解病人的完整病史，对于任何机器学习技术都是一个挑战。

经济问题

除了技术限制之外，AI 和机器人技术对于中小型提供商来说也是一个重大的经济负担。高昂的采购和实施成本，以及年度维护和合同成本，会对组织造成重大的经济负担。此外，提供商还需要考虑机器人仪器和配件的成本，这些仪器和配件都是根据每个手术采购和更换的。最后，许多技术需要广泛的医师和员工培训，昂贵的工作流程更改，在某些情况下还需要更改 EHR。

有研究表明，机器人手术的费用大约是传统手术的 10 倍，没有证据表明其结果明显优于传统手术。在一些案例中，机器人故障导致患者受伤甚至死亡，从而导致法律费用和其它不可预见的费用。

最后，在当下的健康保险系统中，保险公司只愿意支付最低限度的保险金，提供商该如何在这种情况下为患者提供最好的医疗服务呢？像 Mayo Clinic，MD Anderson 和 Partners Healthcare 这样的大型医疗机构来有大量资金用于创新和探索 AI 项目；然而，较小的机构可能无法负担引入 AI 和机器人技术的高昂成本。

法律，法规和伦理风险

采用 AI 和机器人技术的提供商面临的最大问题是法律、法规和伦理方面的问题。由于机器人和 AI 技术的有效性具有敏感性和相对不确定性，所以这方面的风险更大，特别是当医生可以成功实施手术时。

在手术室中使用完全自主的 AI 机器人需要机器足够聪明，能够计算风险并做出“类似人类”的决策。此外，获得病人的完整医疗记录，是许多 AI 技术的必要条件，这也为患者的隐私和安全带来了重大挑战。对于准备并愿意采用机器人和 AI 技术的组织来说，他们需要深入了解各种风险以及各种技术的局限性，制定强有力的治理模式，实施非常严格的协议和工作流程。这样他们能够保护自己免受这些风险和诉讼，最终能够成功采用这些技术。

社会抵制

全面采用这些技术的最大障碍是社会抵制。当然，患者、提供商、医疗机构和政府必须转变思想，才能使机器人真正成为医疗市场的主流。组织必须将机器人和 AI 作为为患者争取更大利益的补充手段。

在不久的将来，机器人很可能比人类更有能力做人类的任务。然而，为了加快变革的步伐，想要采用这些技术的提供商必须提前思考，了解他们该如何适应未来的医疗世界，以及如何减轻他们面临的潜在挑战。通过了解技术和数据差距，法律和伦理限制，成本和社会问题，提供商可以适当地做准备，以采用 AI 和机器人技术。

原文名称	Why robotics and AI still face an uphill battle in healthcare
作者简介	Ashley Amaral，PA Consulting Group 的医疗专家。
原文信息	2017 年 8 月 3 日发布于 Dark Reading 原文地址 https://www.information-management.com/opinion/why-robotics-and-ai-still-face-an-uphill-battle-in-healthcare
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《新型利用 PPT 钓鱼传播“Gootkit”银行木马的分析报告》

近日，安天 CERT（安全研究与应急处理中心）分析人员发现，近期出现了一个新型的利用 PPT 钓鱼传播“Gootkit”银行木马。

该木马通过 PPT 进行传播，在 PPT 文档放映后会启动外部程序，执行 Powershell 代码。该攻击方式不需要 office 宏就能实现执行 Powershell 的功能，通过网络下载 Gootkit 木马对感染者计算机进行控制。

Gootkit 银行木马使用 Visual C++ 编写。样本运行后会执行一些无效操作来对抗模拟机和沙箱。之后解密出一段 shellcode 并执行，shellcode 会释放出一个 PE 文件加载到内存中运行。释放出来的样本会获取当前样本名称和 mstsc.exe 比较，如果不相同，则创建 mstsc.exe 并注入到系统进程中。样本通过 ShellExecuteEx 使用管理员权限启动。打开 BIOS 注册表查找当前是否在虚拟机中运行，如果在虚拟机或沙箱中运行，则程序进入死循环。将自身复制到指定目录下，重命名为 mqnets.exe 并执行，随后删除释放出的原文件。新执行的样本会创建环境变量、并打开多个线程。连接 " web.1901ospinosct.com " ，将从网站返回的文件内容放到注册表中，将注册表中的内容转存成文件并注入，将 IE 的保护模式设置位禁用，创建 inf 文件并添加注册表项保持持久化运行，随后进行盗取用户银行信息。

安天提醒广大网络使用者，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。

目前，安天追影产品已经实现了对该类勒索软件样本的检出。

木马程序

安天【追影威胁分析系统】无需更新病毒库，依据行为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：

文件被页面手工提交发现，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、动态行为（Windows7）鉴定器、静态分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

根据动态行为（Windows7）得出该文件具有以下行为：查找指定内核模块、创建特定窗体、获取驱动器类型、访问文件尾部、获取系统内存、打开自身进程文件、独占打开文件、设置文件属性为隐藏、获取计算机名称。

文件名	796a386b43f12b99568f55166e339fcf43a4792d292bdd05dafa97ee32518921
文件类型	Document/Microsoft.PPTX[:PowerPoint 2007-2012]
大小	34 KB
MD5	3BFF3E4FEC2B6030C89E792C05F049FC
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Downloader]/PowerShell.Agent
判定依据	静态分析

运行环境

操作系统	Windows 7 6.1.7600 Build 7600
内置软件	默认、ie9、office2007、flash、wps、FoxitReader、adobe reader

报告地址：https://antiy.pta.center/_lk/details.html?hash=3BFF3E4FEC2B6030C89E792C05F049FC

其他行为

行为描述	危险等级	行为描述	危险等级
查找指定内核模块	★	创建特定窗体	★
获取驱动器类型	★	访问文件尾部	★
获取系统内存	★★	打开自身进程文件	★
独占打开文件	★	设置文件属性为隐藏	★★
获取计算机名称	★		

运行环境

操作	文件路径
新建	c:\users\ks32\appdata\local\temp\cvr58f8.tmp.cvr
新建	c:\users\ks32\appdata\local\temp\36022776.od
新建	c:\progra~2\micros~1\office\data\opa12.dat
新建	c:\22910c66225b400b8716a3f5cc3da51a\share\~$target.pptx