安天周观察

主办：安天　2017 年 8 月 21 日（总第 100 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天助力中国移动集团为业务支撑网络提供多项安全服务

近期，中国移动官网公示，安天中标中国移动业务支撑网安全保障服务项目。

随着电信业务发展对业务支撑系统开放、互联需求的演进，业务支撑系统对集中化的安全可靠、稳定运行、合规管理等方面的需求日益迫切。本次项目中，安天提供的解决方案涵盖 10 个安全服务子项，围绕“业务高效、稳定、安全运行”的原则开展的安全服务，通过对中国移动的相关系统实施安全服务来保障中国移动相关业务系统的稳定性、可用性和安全性。针对中国移动业务支撑全网安全保障服务项目，安天在安全服务方面的独特优势在于：

1. 安全应急响应服务：安天是中国网络安全领域应急响应的重要节点，自 2001 年成立以来，每年都针对重大和突发性网络安全事件，提供快速感知、分析、响应、处置等服务，安天的应急响应能力及成果多次得到国家监管部门、同行业、重要客户的高度认可。

2. 安全事件深度分析服务：安天拥有十几年针对重大安全事件、高级持续威胁 (APT) 事件、恶意代码事件的监测发现和深度分析能力，团队分析能力处于业界领先地位，成果得到各行业的大力认可。

3. 网络安全保障服务：作为国家级网络安全应急服务支撑单位，自 2008 年以来，安天参与了奥运会、亚运会、G20 峰会、历届两会的网络安全保障工作，安天及参与保障的个人多次受到表彰。

安天将利用 17 年积累的经验和能力，发挥在应急响应、事件深度分析、网络安全保障服务等多方面的优势和特长，为中国移动支撑网提供优质安全服务，保障网络安全、稳定运行。

《安全周观察》100 期

服务客户 解决问题，应对威胁 保障安全

■ 外媒再度指控卡巴斯基与俄罗斯情报机构 FSB 勾结

8 月 16 日，据 ZDNet 网站消息，卡巴斯基 CEO EugeneKaspersky 与其员工自 2009 年 10 月以来的邮件，其中提到了针对“the Lybyanka side”的秘密项目，Lybyanka 这个地方和俄罗斯情报机构 FSB 办公室相关。

报道指出，卡巴斯基与 FSB 关系密切，并表示卡巴斯基已经确认了邮件是真实的。但卡巴斯基则否认了这一说法，并在声明中表示卡巴斯基与政府并无不正当关系，只是和政府在全球范围内进行常规合作对抗网络犯罪。卡巴斯基发言人表示，卡巴斯基实验室从未确认那些邮件的真实性。

报道提到，这些邮件实际是相关 DDoS 防护的，除了抗 DDoS 攻击，还包括与互联网供应商合作来识别攻击者和“活跃反对措施”。

报道中还提到，所谓的反对措施包括为 FSB 提供攻击者未知的实时情报，并给 FSB 和俄罗斯警方提供专家。（来　源：http://www.zdnet.com/article/claims-kaspersky-works-with-russian-intelligence-resurface/）

■ Netsarang 旗下多款产品源码被植入恶意后门

近日，卡巴斯基实验室发现 Netsarang 开发的远程终端模拟软件 Xmanager、Xshell、Xftp、Xlpd 等产品 nssock2.dll 模块源码被植入恶意后门。目前，研究人员已在 Xshell5.0.1322 与 Xshell5.0.1325 两个版本中确认后门存在。受影响的产品版本：Xmanager Enterprise5.0 Build1232、Xmanager5.0 Build1045、Xshell5.0 Build1322、Xftp5.0 Build1218、Xlpd5.0 Build1220。

如果用户当前使用了上述受影响的 Build 版本，可通过客户端进行检查更新，或通过官方网站手动下载最新版本以解决问题。

目前，Netsarang 已通知防病毒公司隔离 / 删除受影响的 dll 文件。官方于 8 月 5 日发布最新版本 Xmanager Enterprise Build1236、Xmanager Build1049、Xshell Build1326、Xftp Build1222 与 Xlpd Build1224 修补漏洞。（来源：http://hackernews.cc/archives/13448）

一周简讯

- 多个 Chrome 扩展程序劫持 480 万用户
- 研究者在 PS 样本中揭露恶意基础设施
- 勒索软件 Mamba 和 Locky 变种再度活跃
- 攻击者组合使用不同漏洞实现隐蔽攻击
- 远程终端管理工具 Xshell 被植入后门代码
- 安全厂商发现利用 0199 漏洞新型恶意样本
- 研究者发现 USB 工具可监听设备流量

安天 CERT 搜集整理，详情请见：

每周安全事件

类 型	内 容
中文标题	TrickBot 银行木马开始使用看似合法的网站与 SSL 证书
英文标题	TrickBot Using Legitimate Looking Sites With SSL Certificates
作者及单位	Ionut Arghire；SecurityWeek
内容概述	近日，安全研究人员发出警告称，TrickBot 银行木马程序一直在使用合法的 SSL 证书。自 TrickBot 出世已经有一年左右的时间了，这款银行木马在给银行惹麻烦之余还不断增加了各种新功能。 TrickBot 前一阵刚获得了类似蠕虫自传播的功能，且不仅仅瞄准用户的在线银行信息：还有 Outlook 和浏览器数据。Palo Alto Networks 分析师称，木马主要通过恶意电子邮件分发，收件人打开附件即可能受到感染。而近期观察到的假冒网站看似使用了正确的 URL 和 SSL 证书，由于和合法 URL 十分相似且具备 SSL 证书，用户不太可能发现网站是假冒的。TrickBot 通过显示网络银行的正确网址和合法的 SSL 证书，将银行凭证的网络钓鱼信息提升到了新的级别，用户会更难看出差异。
链接地址	http://www.securityweek.com/trickbot-using-legitimate-looking-sites-ssl-certificates

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	相关描述
移动恶意代码	较为活跃样本	Trojan/Android.QQspy.cp [prv，sms]	该应用伪装成 QQ 相关的第三方应用，诱导用户输入账号密码，盗取账号密码发送给指定手机号，建议卸载。（威胁等级中）
		G-Ware/Android.jianmo.cs[rog]	该应用程序伪装成永恒之蓝密码计算器，诱导用户安装，死循环创建文件，要求用户添加指定 QQ 解除，影响用户体验，建议不要安装。（威胁等级低）
		Trojan/Android.QQspy.co [prv，sys，lck]	该应用程序运行会强制置顶界面，二次锁屏，对用户进行勒索，诱骗获取 QQ 账号和密码并发送邮件，造成用户隐私泄露，建议卸载。（威胁等级中）
		G-Ware/Android.StealMoney Game.n[pay，rog]	该游戏应用付费信息不明显，以领取道具名义频繁加载弹窗，诱导用户点击付费，造成用户资费损耗，建议卸载。（威胁等级低）
		Trojan/Android.E4Aspy.af [prv，exp]	该应用程序运行后诱导用户输入账号信息，并上传到指定服务器，提示信息包含不雅词汇，会造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.locSpy.e[prv]	该应用程序运行会获取用户地理位置信息并通过短信发送，造成用户隐私泄露。（威胁等级中）
		Trojan/Android.BKspy.b [prv，exp]	该应用程序伪装成正常应用，会拦截用户短信接收指令，通过邮箱发送用户手机的图片、联系人、短信、证书等信息，造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.Vitamio.b[exp]	该应用程序包含风险代码，运行跳转推广页面，诱导用户点击下载，造成用户流量资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.Locker.k [rog，sys，lck]	该应用运行会强制置顶界面，三次锁屏勒索用户付费解锁，建议卸载。（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 远程代码执行漏洞 CVE-2017-8570	CVE-2017-8570 漏洞是一个逻辑漏洞，利用方法简单，影响范围广。由于该漏洞和三年前的 SandWorm（沙虫）漏洞非常类似，因此被称之为“沙虫”二代漏洞。该漏洞为 Microsoft Office 的一个远程代码执行漏洞。其成因是 Microsoft PowerPoint 执行时会初始化 Script Moniker 对象，而在 PowerPoint 播放动画期间会激活该对象，从而执行 sct 脚本 (Windows Script Component) 文件。攻击者可以欺骗用户运行含有该漏洞的 PPT 文件，导致获取和当前登录用户相同的代码执行权限。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Voila	此威胁是一种下载类的木马程序。该家族样本运行后，会与指定的远程服务器连接，下载其它的恶意软件到本地运行。（威胁等级中）
		Trojan[Backdoor]/Win32.AutoIt	此威胁是一种后门类木马程序。该家族是通过 AutoIt 编写的后门程序。样本运行后会执行连接远程服务器，等待接收上传下载文件、监视用户屏幕、记录键盘击键、查看进程和窗口等控制指令。（威胁等级高）
		Trojan[Banker]/Win32.Banbra	此威胁是一种以窃取网络银行敏感信息为目的的木马类程序。该病毒伪装成正常数据，以获取认证。该病毒利用各种途径，使黑客获得数字证书来伪造文件。该家族还会收集用户的机密信息，如网上银行详细信息和密码等，并将窃取的数据发送给远程黑客。（威胁等级中）
		Trojan[Downloader]/Win32.Zlob	此威胁是一种具有下载行为的木马类程序。Zlob 家族感染用户电脑后，会修改系统设置，在电脑中下载并执行多个恶意软件。该家族会伪装成 ActiveX 的视频编码欺骗用户下载并安装，安装后，用户会收到伪装成微软警告信息的弹窗，提示用户系统中可能存在间谍软件，需要下载反病毒程序进行清除。在用户点击弹窗后，将下载实为木马的虚假反病毒程序。（威胁等级高）

人工智能将要实现的 10 个 IT 工作

Cynthia Harvey / 文　安天公益翻译小组 / 译

在讨论人工智能 (AI) 对人类工作的影响时，有些极端情况值得关注。一方面，一些新闻头条警告说机器人将会取代人类工作；另一方面，一些专家说 AI 绝不会取代人类工作。在 IT 工作中，AI 已经开始产生影响。今天，自动化和机器学习工具可以处理以前由人类执行的许多任务。Gartner 预测，“AI 将最终取代 IT 组织的许多常规功能，特别是在操作方面。”

AI 能够执行哪些 IT 工作呢？以下是 10 个可能的候选项。

服务台专家

一些科技公司，推出了能够帮助组织创建与客户进行对话的聊天机器人的工具。许多组织已经开始尝试使用这些聊天机器人来回答简单的客户服务或技术支持问题。2017 年 HubSpot 调查发现，57% 的受访者表示更愿意与人对话获得帮助，40% 的受访者表示，只要能解决问题，他们不在乎是人类还是机器人在与其对话。

系统管理员

在 DevOps 趋势的推动下，系统管理员近年来越来越依赖自动化来帮助他们处理诸如服务器配置和软件更新这样的常规任务。许多监控工具开始引入机器学习和 AI 功能，从而减少误报数量，并且在某些情况下提前向系统管理员发出警报，以便他们采取预防措施。

网络管理员

网络管理员负责维护组织的网络并提供用户期望的服务。这包括配置和更新设备，如路由器、交换机、网关、集线器和接入点。在某些情况下，该工作还包括网络安全责任。专家说，为了实现真正的数字转型，未来的网络将需要 AI 能力，以跟上时代变化的步伐。

存储管理员

存储管理员处理存储硬件和存储软件的日常维护任务。存储专家指出，许多手动任务可以由自动化和 AI 工具来处理。因为它们能够分析海量数据，所以机器学习应用程序在优化 I/O 存储模式、管理数据生命周期和预测硬件故障方面可能会比人类更好。

质量保证 / 测试员

在组织部署内部或面向客户的应用程序之前，这些应用程序必须经过彻底的测试，以了解它们如何在真实环境中执行。质量保证或测试员已经开始使用自动化工具了。Infosysare 等厂商致力于将机器学习集成到质量保证解决方案中，以优化测试流程，更好地分析测试日志，更快地诊断和解决问题。

项目经理

Gartner 特别指出，项目经理是面临被 AI 取代的 IT 职位之一。典型的项目经理花费大量时间收集和输入有关谁做了什么的数据。AI 系统可以轻松地接管这类工作，向团队成员部署任务，甚至更好地自动收集数据。此外，项目经理经常需要估计一个项目需要多长时间，花费多少。机器学习工具能够分析类似项目的大量数据，以更准确地完成任务。

数据分析师

随着大数据趋势横扫美国各个行业，更多的人进入了数据分析领域。事实上，组织对高技能数据科学家的需求非常之高，以至于开始转向 AI，以便帮助技能较低的数据分析师执行高级分析。今天的许多预测分析工具集成了机器学习功能，可以帮助数据分析师更快地处理更多的数据，并提供宝贵的意见。

数据库管理员

数据库管理员处理数据库的部署、配置、优化、调优、监控、管理和故障排除等任务。一些计算机科学家指出 AI 可以执行其中的一些工作，特别是监控、诊断和解决问题。AI 趋势导致对数据库的需求不断增加，这反过来又对数据库管理员提出了越来越高的要求。

安全管理员

许多下一代安全信息和事件管理 (SIEM) 以及用户和实体行为分析 (UEBA) 解决方案包括机器学习功能。该技术允许组织为其网络和系统建立正常活动的基准，然后检测可能已被其它安全工具忽视的异常活动。

软件开发人员

多年来，组织对软件开发人员的需求持续走高，薪水更是一日千里。一些厂商已经开始提供低代码或无代码工具，帮助普通用户创建简单的应用程序。微软和剑桥大学的研究人员也在尝试开发能够编写代码的 AI。像许多人类程序员一样，AI 会检查现有的应用程序，以帮助创建有效的解决方案。

这种 AI 还远远不能自行编写整个程序，但是这些功能很快就可以帮助更多的人类员工开发软件了。这有助于减轻一些人才短缺的局面。

原文名称	10 IT Jobs That Will Be Done by AI
作者简介	Cynthia Harvey，一位自由撰稿人和编辑。
原文信息	2017 年 7 月 10 日发布于 Information Week 原文地址 http://www.informationweek.com/strategic-cio/10-it-jobs-that-will-be-done-by-ai/d/d-id/1329310
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《Pengex 病毒分析报告》

近日，安天追影小组在安全事件整理过程中，着重关注了 Pengex 病毒，该病毒为内核级后门病毒，以劫持用户首页流量牟利为目的，同时具有对抗安全防御软件能力。经分析发现 Pengex 病毒通过盗版系统盘和“注册机”软件进行传播，并在用户电脑中留下后门，同时会主动攻击各种主流杀毒软件，使杀毒软件失去内核防御能力危害极大。

安天追影小组针对 Pengex 的样本进行了相关分析。该样本主要通过第三方系统盘方式进行传播。当成功运行后该样本会在系统中进行驱动加载，会造成安全杀毒软件防御驱动无法进行正常加载，从而使安全软件失去防御杀毒能力，之后通过释放后门病毒，可以执行远端 C&C 服务器存放的任意病毒代码。

该样本根据功能主要分为两个部分：加载器部分与后门部分。

加载器部分主要用于绕过杀毒软件查杀。该部分代码首先在内存中的虚拟映射中加载一个新的 ntoskrnl 镜像，然后使用相同的虚拟映射方法将真正的病毒驱动加载到内存中，并将病毒驱动导入的 ntoskrnl 中的函数地址指向其虚拟加载的 ntoskrnl 镜像中的函数地址上。此方法可以绕过其他驱动在 ntoskrnl 中设置的内核钩子，进行免杀，这是绕过主流杀毒软件的驱动 HOOK 防御技术。同时原始的病毒驱动的镜像数据是经过 0XC0 异或加密的，防止主流杀毒针对数据进行静态查杀。

后门部分成功执行后，通过 7897 端口与域名为 caoduba.com 或 IP 为 139.129.234.76 的 C&C 服务器进行通讯。服务器通过解析控制码进行相关功能模块加载，劫持用户首页流量。控制码 0x2 主要向 C&C 服务器请求，获取病毒执行配置数据来进行流量劫持。控制码 0x3 主要向 C&C 服务器请求，获取远程驱动模块数据进行数据更新。控制码 0xA 主要向 C&C 服务器请求远程动态库来进行任意攻击模块加载。

通过分析可以看出，Pengex 病毒并不安于进行简单的浏览器流量劫持，而是通过主动攻击相关主流安全软件来扩大自己的生存率，使其威胁性变得更大。安天提醒广大网络用户，不要使用未知系统盘或未知系统镜像，提高自身安全意识，及时更新相关安全软件，不要轻易进行未知文件附加运行下载。

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：

文件被内部组件发现，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、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。

最终依据静态分析鉴定器将文件判定为木马程序。

文件名	./e3d08bc8cc9b154dc1638dd3f57cfd4a2729dac50f59acebc95cffb01e5a2518.danger
文件类型	BinExecute/Microsoft.SYS[:X64]
大小	99 KB
MD5	1A4AE84EF3D4E89F25EE6295D0F947AF
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Rootkit]/Win64.Agent
判定依据	静态分析

报告地址：https://antiy.pta.center/_lk/details.html?hash=1A4AE84EF3D4E89F25EE6295D0F947AF

◆ 数字签名信息

描述	值	
证书验证结果	校验成功	
有效终止日期	Tue Mar 5 23:59:59 2013 UTC (130305235959Z)	
序列号	71330901632515112285268795980983289714	
颁发者	国家	US
	参考信息	Terms of use at https://www.verisign.com/rpa (c)10, VeriSign Trust Network
	组织 / 单位	VeriSign, Inc.
	普通名称	VeriSign Class 3 Code Signing 2010 CA
有效起始日期	Mon Dec 12 00:00:00 2011 UTC (111212000000Z)	
使用者	国家	CN
	普通名称	Beijing Kylin Network Information Science and Technology Co.,Ltd
	所在地	BeiJing
	组织 / 单位	Beijing Kylin Network Information Science and Technology Co.,Ltd
	省 / 州	BeiJing
	参考信息	Research and Development Center, Digital ID Class 3-Microsoft Software Validation v2