安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 03 月 12 日 (总第 126 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

两会首日，安天首席架构师作为新任全国政协委员接受多家媒体采访

2018 年 3 月 3 日下午 3 时，全国政协十三届一次会议在人民大会堂开幕，习近平总书记等党和国家领导人出席了大会，俞正声作工作报告。

安天创始人、首席架构师肖新光，作为新任政协委员，在会前接受了多家媒体的采访。肖新光表示，作为新任全国政协委员深感责任重大，使命光荣。

对于自身所从事的网络安全领域工作，肖新光表示：过去五年，我国网络安全事业取得了很大进步，网络安全法颁布实施，关键信息基础设施保护得到进一步重视，人才培养如火如荼。作为网络安全从业者，有幸亲历这些发展进步，为这些进步欢欣鼓舞。但网络安全工作，依然有很多问题和短板，特别是缺少敌情想定，基础能力不够扎实，缺少深度有效的安全需求，距离总书记的“全天候全方位感知网络安全态势和有效防护”等系列工作要求还有很大差距。需要各方一起努力，加快把总书记“没有网络安全就没有国家安全”的战略判断和战略意志转化为全面的能力要求和刚性需求的速度。

习近平总书记在黑龙江考察期间强调改造升级“老字号”，深度开发“原字号”，培育壮大“新字号”。肖新光表示，这是解开东北老工业基地产业发展的一把钥匙。安天作为战略新兴产业的代表，作为在黑龙江创业的“新字号”企业，将依托自身基础，把握发展机遇，加速规模发展和研发布局，力争为黑龙江经济转型升级创造样板。

对于东北老工业基地如何留住人才的问题，肖新光表示，产业是人才的基本水土，产业规模和产业能力决定人才的吸引力。立足本地产业优势，形成标志性企业，带动产业规模，才能大量留住人才。从安天最近两年校园招聘的毕业生来看，985 院校占比不断增加，研究生的比例已经接近一半，大量德才兼备的优秀毕业生选择了安天。这一方面是安天自身规模发展和成长的结果；另一方面，也说明黑龙江的创业环境、营商环境在渐进改善，地域的吸引力在逐渐增强。安天创业于黑龙江，全国布局，产品和服务辐射全球。在过去两年中，有多位重量级的研发、学术、管理人才加盟，他们有的来自华为等知名企业，有的来自国家院所，有的是人民军队的军转干部，他们虽然大部分在其他城市工作，但他们也为黑龙江发展做出了贡献。

肖新光表示，他已经针对网络安全领域缺少敌情想定，网络安全领域的投入存在不充分、不平衡的问题，编写了提案建议。

安天发布《安天针对 CHM 银行木马的检测分析及有效防护》

安天在近期捕获的样本中发现了一种利用 CHM 传播的银行木马，该银行木马来源于一种垃圾邮件传播的附件中。当用户收到这种垃圾邮件并打开附件中的 CHM 文件时，恶意软件就会执行一个小的 PowerShell 命令，其下载并执行第二阶段的 PowerShell 脚本，当用户执行脚本时，会创建一个计划任务来运行恶意软件，从而获得持久性。

CHM 是微软专有的在线帮助文件，它由编译成单一压缩文件格式的 HTML 页面组成，最常用的 CHM 是离线软件文档和帮助指南，这种编译过的 HTML 帮助文件已经被恶意软件作者利用过多次，他们将恶意的 Downloader 代码偷偷放入文件中，使其难以被检测。

目前，此款恶意软件主要针对巴西的用户进行传播，但是利用 CHM 隐藏恶意软件代码逃避检测正在成为攻击者努力发展的攻击手段，不排除此类银行木马在全球大规模传播的可能，因此需提高警惕。

经验证，安天智甲终端防御系统、探海威胁检测系统等产品可通过安天自主先进的 AVL SDK for Network 威胁检测引擎（简称安天 AVL SDK）对该病毒做出精准检测和处置。作为网络安全产品的“发动机”，优质的威胁检测引擎可为产品注入强大的动力。安天 AVL SDK 不仅具有非常高的威胁检出率，并且可对威胁提供精准的命名和配套的知识体系；不仅可增强产品防御的有效性、灵活性，同时也可输出有效的安全知识和威胁情报。

针对该类威胁，安天 AVL SDK 可深度解析电子邮件、CHM 等十余种常见文件结构，细粒度地对文件进行解析还原，具有针对性地分离出文件中易于隐藏恶意代码的代码部分，为后续防御提供准确的检测结果。

报告原文

每周安全事件

类 型	内 容
中文标题	全球过半互联网邮件服务器受严重漏洞影响
英文标题	Vulnerability Affects Half of the Internet's Email Servers
作者及单位	Catalin Cimpanu
内容概述	一个严重漏洞影响了几十万台邮件服务器。虽然修复方案已发布，但由于影响范围过大，因此修复该问题至少要耗费数周甚至数月的时间。 该漏洞存在于邮件传输代理 (MTA) Exim 中，这是运行在邮件服务器上的软件，负责把邮件从发件人中继给收件人。该漏洞的编号为 CVE-2018-6789，它被归类为一个“预验证远程代码执行”漏洞，也就是说，攻击者可诱骗 Exim 邮件服务器在攻击者验证身份之前运行恶意代码。该漏洞是一个字节缓冲溢出漏洞，存在于 Exim 的六十四进制的解码功能中，而且影响所有已发布的 Exim 版本。 根据 2017 年 3 月发布的一项调查显示，56% 的互联网服务器运行 Exim，当时网上的邮件服务器超过 56 万台，而最近发布的报告将这个数字增加到了数百万台。
链接地址	https://www.bleepingcomputer.com/news/security/vulnerability-affects-half-of-the-internets-email-servers/

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 9 个移动平台恶意代码和 4 个 PC 平台的恶意代码值得关注

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.ITcastLockScreen.a[sys] 2018-03-06	该应用程序为恶意代码的测试程序，通常会请求设备管理器权限，可能包含设置密码锁屏、清除数据、私自发送短信等恶意功能，存在较高的风险，建议卸载。（威胁等级中）
		Trojan/Android.CedarSpy.a[prv,rog,spy] 2018-03-07	该应用程序包含恶意代码，运行后窃取联系人、通话记录、短信和照片、上传地理位置信息，造成用户隐私泄露，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.Downloader.cc[exp]	该应用程序安装无图标，伪装正常应用，运行后联网私自下载广告子包，推送广告。造成用户流量消耗，建议卸载。（威胁等级高）
		Trojan/Android.SmsSend.oj[prv,exp]	该应用程序运行隐藏图标，监听、拦截短信，私自发送短信到指定号码，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级中）
		G-Ware/Android.Hiddad.d[exp,fra]	该应用程序伪装成系统升级程序，无实际功能，包含 Google 广告插件，运行即隐藏图标并加载运行广告模块，会造成用户一定的资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.HiddenApp.ar[rmt,exp]	该应用程序运行后隐藏图标，接收远程指令，可能加载广告、私自下载安装应用、打电话以及发短信，建议立即卸载。（威胁等级高）
		G-Ware/Android.HiddenAds.ds[rog,exp]	该应用程序运行请求激活设备管理器，隐藏图标，后台推送广告，造成用户流量消耗，建议卸载。（威胁等级中）
		G-Ware/Android.HiddenAds.dr[exp,rog]	该应用程序伪装成系统应用，安装无图标，运行后激活设备管理器，加载广告，建议卸载。（威胁等级中）
		G-Ware/Android.HiddenApp.as[rog,prv]	该应用程序伪装色情应用，运行隐藏图标，私自下载恶意子包，上传用户手机号等信息，会造成用户隐私泄露，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	Adobe Acrobat Reader 中存在远程代码注入漏洞（CVE-2018-4901）	思科 Talos 研究员近期披露了在 Adobe Acrobat Reader DC 中的远程代码执行漏洞。攻击者可以将恶意 JavaScript 代码隐藏在 PDF 文件中。这些代码可以启用文档 ID 来执行未经授权的操作，以在用户打开 PDF 文档时触发堆栈缓冲区溢出问题。（威胁等级高）
	较为活跃样本	Trojan[Backdoor]/Win32.Gibbon	此威胁是一种可以窃取用户信息的木马类程序。该家族样本运行后连接远程服务器接受攻击者恶意操作，收集用户信息并回传。（威胁等级高）
		Trojan[Backdoor]/Win32.Contopee	此威胁是一种可以窃取用户信息的木马程序。该家族样本运行后连接远程服务器，接受攻击者恶意操作，收集用户敏感信息并回传。（威胁等级中）
		Trojan/BAT.DispMessage	此威胁是一种木马类程序。载体以 BAT 批处理文件的格式存在。该家族的样本在执行后会连接远程的服务器，上传所窃取的信息，并从远程服务器接受进一步的控制，例如更新自身程序，接受控制命令并执行等。（威胁等级中）

2018 年企业的五个技术趋势

Jessica Davis / 文　安天技术公益翻译组 / 译

埃森哲 2018 年技术展望报告为首席信息官（CIO）和其他高管确定了五个技术趋势。

人工智能可能是 CIO 的首要任务，但是清理数据以及其他大数据和分析项目也是企业在 2018 年度的重要任务。在名为《智能企业来临：请重新定义您的公司》的 2018 年技术展望报告中，埃森哲详尽分析了未来三年内将给企业带来颠覆性影响的五大关键技术趋势。

该报告将数据准确性确定为 2018 年的五大关键趋势之一，指出："企业运营基于数据驱动。不准确、被操纵和片面的数据将成为企业的新软肋，会严重损害企业洞察力，导致重大决策偏差。另外四个趋势是：公民人工智能（AI）、扩展现实、顺畅的商业合作和智联网（Internet of Thinking）。

数据准确性

事实上，数据准确性一直是企业面临的问题。埃森哲实验室技术展望部门总经理迈克尔·比尔茨（Michael Biltz）认为，如今数据准确性风险比以往任何时候都要高。

企业正在为分析项目投入更多资金。这些项目远不只推荐新衬衫或 Netflix 上的新视频那么简单。以美国太空探索技术公司 SpaceX 为例，如果该公司的数据不正确，那么可能会损失数百万美元的火箭，比尔茨说。后果是很严重的。

埃森哲采访了全球 6300 多位企业和 IT 高管，发现这些高管中有 82% 正在使用数据来推动关键和自动化决策。更重要的是，97% 的商业决策是基于经理们认为质量不过关的数据制定的，埃森哲援引 HBR 发布的一项研究报告指出。

"你拥有的数据要尽可能地真实和准确，这一点非常重要。"比尔茨说。目前，企业还

不具备这样的系统。

另外，现在有更多的数据来自各种不同的来源。比尔茨表示，在过去的 10 年中，企业已经实现了供应链的自动化。他们一直在增加新的数据流，与合作伙伴分享更多数据。他们可能保存着已经完全过时的客户记录；人们可能分享了不正确的地址或电话号码。

首席信息官和首席数据官（CDO）有多少工作要做？"我们有很多工作要做"比尔茨说。企业不仅要处理旧地址和电话号码，还将花费大量时间"弄清最新的真实信息。当你更深入地查看时，会发现数据收集方式存在着根本性的缺陷。"

顺畅的商业合作

这一趋势是关于建立企业架构，以便您能够大规模地进行合作。根据该报告，"企业依靠基于技术的合作伙伴关系来实现增长，但其传统系统无法大规模地支持合作伙伴关系。为了充分支持智能企业，企业必须更新系统，完成架构再造。"

比尔茨说，架构更新可能会以平台或 API 的形式出现。如今这一点至关重要，因为企业现在正在根据他们与其他公司的合作方式展开竞争。

例如，比尔茨说，一家制鞋公司设立了 Instagram 帐户来展示鞋子。当顾客点击鞋子时，会被指向购买这些鞋子的亚马逊页面。他们是在与社交媒体平台和亚马逊合作。但他们的竞争对手（比如阿迪达斯）与一家制造公司合作，让客户能够定制他们购买的鞋子。还有一家公司与 IBM 的沃森合作，将计步器和传感器整合到鞋中。所有这三家制鞋公司都在争夺合作关系。

比尔茨指出，沃尔玛相对来说先进一些，多年来一直在推进 API 和微服务。"我们现在处于这样一个阶段——每个人都开始与其他人更密切地联系在一起。"比尔茨说。

公民 AI：增强 AI 以使企业和社会受益

埃森哲表示："随着 AI 的能力不断增强，其对人们生活的影响也在不断增加。企业在充分利用 AI 的潜能时必须把握和利用好这种影响力，成为负责任的企业代言人。"

扩展现实：距离的终结

埃森哲指出，"虚拟和增强现实技术让人们、信息和体验之间的距离消失，完全颠覆了人们的工作与生活方式。"

智联网：创建智能分布式系统

埃森哲说："企业大力构建基于机器人、AI 和沉浸式体验的智能环境。要将智能环境应用于生活，企业不仅需要培养关键技能和员工能力，还需要改造现有的技术基础设施。"

在朝着这些趋势努力时，企业有很多的工作要做。但即将到来的变化是不可避免的。

"就像城市围绕港口和铁路发展，或者人们围绕电力重建生活一样，当今的世界正在围绕数字化创新——以及提供这些服务的公司——自我复兴。"埃森哲首席技术和创新官保罗·多尔蒂（Paul Daugherty）说，"这需要建立在信任和共享大量个人信息的基础上的新型关系。"

原文名称	5 Tech Trends for the Enterprise in 2018
作者简介	Jessica Davis。Jessica Davis 是一位高级编辑。
原文信息	2018 年 2 月 15 日发布于 Information Week 原文地址 https://www.informationweek.com/strategic-cio/executive-insights-and-innovation/5-tech-trends-for-the-enterprise-in-2018/d/d-id/1331058
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《锁机木马“ShimCache”分析报告》

近日，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时注意到，一例运行在 Windows 平台下的具有锁机功能的木马样本“ShimCache”在网络中开始传播。当用户运行恶意代码后，该木马会在 Windows 系统中添加自身为启动项，并使系统重启。当系统重启时，此锁机样本会一起启动，锁定计算机。在开机界面等待用户输入密码，用户需要与作者联系并交付一定赎金才能解开密码，密码错误则停留在锁机界面。该木马对用户的计算机安全产生了较大的威胁。

“ShimCache” 启动后，首先将自身拷贝到 C:\WINDOWS\system32\svchose.exe 目录下，随后修改注册表，将自身添加为开机启动项以保证持久化运行。使用 rand() 函数生成随机数并将此随机数、木马作者 QQ 号码以及随机数 +212 存储到指定的内存区域中。该木马会将计算机系统管理员密码设置为 123，并将主引导扇区的数据存储到第三扇区，然后将锁机代码存储到主引导扇区。当用户重新开机时便会执行锁机代码。锁机代码使用 int 10h 中断来显示 QQ 和随机数信息。调用 int 16h 中断，读取键盘输入的字符，若接收到回车键，则进行密码比对，若密码错误返回锁机代码开始处，若密码正确则将第三扇区的正确的主引导扇区数据读取出来写入主引导扇区。经过分析，密码为屏幕上显示的随机数加 212。

安天 CERT 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恶意代码的检出。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述高级威胁进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 YARA 自定义规则鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、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。

最终依据静态行为鉴定器、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	病毒 .exe_
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	64 KB
MD5	E7E125CA74AEF69D3FFC423CE3AA97D7
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.AGeneric
判定依据	静态分析

◆ 运行环境

操作系统	内置软件
Windows XP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 危险行为

行为描述	危险等级
修改用户密码	★★★
修改硬盘引导扇区，疑似感染引导区病毒	★★★★

◆ 常见行为

打开自身进程文件	★
释放 PE 文件	★
复制文件到系统目录	★
增加 run 自启动项	★
获取驱动器类型	★
查找指定内核模块	★★
获取计算机名称	★
自启动	★

◆ 监控预警

PID	创建
1424	C:\WINDOWS\system32\net.exe
1344	C:\WINDOWS\system32\cmd.exe
764	C:\WINDOWS\system32\shutdown.exe
1636	C:\WINDOWS\system32\cmd.exe