安天周观察

主办：安天　2017 年 8 月 28 日（总第 101 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

中央网信办网络安全协调局局长赵泽良一行视察安天

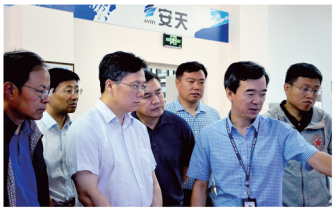
8 月 25 日，中央网信办网络安全协调局局长赵泽良、黑龙江省委网信办主任李耀东等一行领导莅临安天视察，安天技术负责人进行了汇报。

在汇报中，安天技术负责人向来宾介绍了安天的发展历程及现状，并展示了安天取得的各项资质和荣誉。在安天持续与网络安全威胁对抗方面，特别汇报了对高级威胁的发现、捕获、分析等方面所做的工作。在安天的产品方面，相关负责人也进行了详细的介绍，其中主要介绍了安天在网络靶场项目中所做的工作并进行了演示，重点展示了安天的态势感知系统在普通场景及应急场景下的响应过程及分析、研判过程。在 2016 年，安天协助黑龙江省委网信办建设黑龙江安全态势感知和应急处置平台，平台运行至今已实现网站监测、安全信息共享、态势感知和应急处置机制等客户价值。

中央网信办网络安全协调局局长赵泽良在听完安天负责人的介绍后，对安天的创业过程、技术能力及取得的成果表示肯定，对安天目前的发展状况及相关合作伙伴进行了关心与询问。他表示，安天所做的工作对国家十分有益，希望安天能不忘初心，继续奋进。

国家发展改革委振兴司、全国工商联研究室等多位领导视察安天

8 月 25 日，全国工商联研究室主任林泽炎、中国民营经济研究会常务副会长王忠明、全国工商联研究室调研处处长陈聚春、国家发展改革委振兴司政策体制处副处长陈定安等一行领导莅临安天视察。安天相关负责人为调研组领导介绍了安天的发展历程、现状以及安天的技术分布，并展示了安天取得的专利资质和国家应急响应资质等。同时，调研组领导在听取了有关安天针对重大安全攻击事件的应急与分析后详细询问了有关境外攻击的情况及攻击装备等问题，对安天在 WannaCry 事件中做出的应急响应工作进行了肯定。



各位领导对安天的技术能力及取得的成果表示认可，并对安天的产品、发展等各方面进行询问，与安天负责人进行了详细的交流。

安天亮相 XCon2017 峰会并发表演讲

8 月 23 日 -24 日，XCon2017 安全焦点信息安全技术峰会在北京举行。该峰会已连续举办 16 届，是国内最知名、最权威、举办规模最大的信息安全会议之一，其主要着眼于实际和解决问题的方法、技巧等内容，一般来看代表了国内安全思想和技术的前沿方向。在本次峰会上，来自安天微电子与嵌入式安全研发中心的工程师进行了题为《蓝牙 4.0 加密通信过程的流量分析攻击威胁与防护》的演讲。

随着物联网时代的开启，低功耗蓝牙设备的部署与应用日益广泛。但随着软件无线电技术的发展，在机器学习、数据分析技术的推动下，针对物联网通信的攻击不再仅限于传统的嗅探破解，通信信道的流量分析已经成为新的安全威胁。其可以在捕获通信数据包序列但无需解密的情况下，达到探究当前用户可能进行的通信行为的效果，进而用于行为特征识别、攻击对象身份判定、行动计划推测等。

在本次演讲中，安天工程师简述了蓝牙 4.0 通信的安全机制及机器学习预测模型的构建流程。并以蓝牙 4.0 通信过程为例，通过无线电设备跟踪跳频、捕获并破解蓝牙键盘键入的数据，将加密通信数据、破解后的明文信息与同时记录的流量特征进行对比分析，揭示了三者间的联系及由此可能带来的信息泄露威胁。他在演讲中同时进行了简单的实例演示以展现安全风险。

安天是较早关注 XCon 峰会的企业之一，在历届峰会上分享了多篇重要技术报告。今后，安天会依旧关注前沿技术并进行自我沉淀与对外分享，为信息安全领域的技术革新贡献自己的一份力量。

安天在历届 XCon 峰分享的技术报告

会议名称	演讲主题
XCon2017	蓝牙 4.0 加密通信过程的流量分析攻击威胁与防护
XCon2016	无线应用通信安全 SRAM 型 FPGA 的信息安全风险浅析
XCon2015	“斯文扫地”的 Evil Maid：一个扫地机器人引发的信息安全风险
XCon2014	信号的可发现性——wifi 之外我们还能做什么？
XCon2013	对 3D 打印的安全攻击浅析
XCon2012	攻击时间：传统计时器的安全风险
XCon2010	病毒分析流水线
XCon2009	设备与信号攻防的再次探索
XCon2008	还原冬天的神话：打印机“病毒芯片”事件之情景再现
XCon2005	网络病毒监控系统的架构体系与研究方法
XCon2004	细粒度可嵌入的反病毒引擎
XCon2003	病毒检测技术的取证应用：外延化的广谱检测引擎和技术体制
XCon2002	基于网络流和包的病毒检测

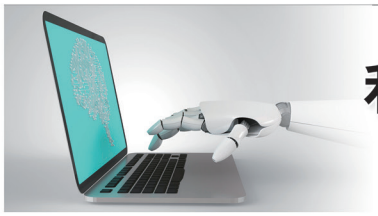
每周安全事件

类 型	内 容
中文标题	加密货币勒索软件 Miner 可利用 WMI 与“永恒之蓝”肆意传播
英文标题	Fileless cryptocurrency miner CoinMiner uses NSA EternalBlue exploit to spread
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	安全研究人员近期发现加密货币勒索软件 Miner，允许黑客利用 Windows 管理工具 WMI 与安全漏洞“永恒之蓝 (EternalBlue)”进行肆意传播。 研究人员表示，该勒索软件使用 WMI 作为无文件持久性机制，即由 WMI Standard Event Consumer 脚本应用程序执行。此外，Miner 还使用 EternalBlue 漏洞感染系统网络。研究显示，无文件 WMI 脚本与 EternalBlue 的结合可以使 Miner 隐蔽持久地感染目标设备。Miner 的感染流程分为多个阶段。首先，Miner 感染目标系统后会通过 EternalBlue 漏洞删除并运行系统后门；其次，系统在安装各种 WMI 脚本后，会将其连接到 C & C 服务器并获取指令；最终，目标系统将下载运行该恶意软件与其相关组件进行肆意传播。
链接地址	http://securityaffairs.co/wordpress/62254/cyber-crime/fileless-miner-coinminer.html

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	新出现的样本家族	Trojan/Android.WeddingCard.a[prv，exp，sys，rmt] 2017-08-21	该应用程序运行诱导激活设备管理器，隐藏图标，接收远程指令，上传用户短信、通讯录、本地文件等隐私信息，还会私自拨打电话、发送短信、下载未知文件、修改手机设置，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.lqads.a[exp，rog] 2017-08-23	该应用程序伪装 YunOS，运行后加载广告子包推送广告，包含恶意代码，会私自下载恶意子包。恶意子包会关联微信，恶意推送微信公众号。（威胁等级高）
		G-Ware/Android.ZMrogAd.a[rog，exp]2017-08-23	该应用程序包含流氓推广行为，运行私自下载的未知应用，并添加多个桌面图标用于安装，影响用户的使用体验，造成用户资费消耗，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.Mobilespy.ah[prv，spy]	该应用程序是一款间谍类软件，通过联网下载记录关键 URL 的文本文件，伪装成社交软件 Line 更新程序，运行后隐藏自身图标，上传固件信息、用户手机短信、电话、联系人、位置等各种隐私信息、静默安装未知应用，建议卸载。（威胁等级中）
		Trojan/Android.BankerSpy.b[prv，rmt，spy]	该应用程序伪装知名应用，运行隐藏图标，激活设备管理器，接收远程指令，窃取用户短信、电话、通讯录、位置、app 列表、浏览器书签等隐私信息，还有拦截、清空短信，私自打电话等恶意行为，利用钓鱼界面诱骗窃取用户的银行相关账号和密码，上传服务器，造成用户隐私泄露，请及时卸载程序。（威胁等级高）
		Trojan/Android.SmsSend.na[exp，spr]	该应用程序运行后静默向指定号码发送含指定内容的短信，拦截特定短信，包含私自下载风险代码，可能造成用户资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.FakeFB.i[prv]	该应用程序伪装 FaceBook，诱导用户输入账号密码，通过邮件发送，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.FakeInst.ex[exp，rog]	该应用伪装成正常应用，运行诱导激活设备管理器，隐藏图标，打开数据流量或者 wifi，私自下载 apk 文件；获取手机固件信息和手机号码，加载网址重定向跳转到广告和下载网址，拦截特定短信，造成用户资费损耗，请立即卸载。（威胁等级中）
PC 平台恶意代码		Windows Search 远程代码执行漏洞 (CVE-2017-8620)	Windows 搜索在内存中处理对象的方式存在安全问题，当攻击者向 Windows 搜索服务发送特制的消息时会触发该漏洞（可以通过 SMB 服务），成功触发该漏洞可以控制受影响的系统执行任意代码。（威胁等级高）
		Trojan/Win32.Carberp	此威胁是一木马类程序，该家族专门用于盗取银行信息。运行后能够感染硬盘的主引导记录，对包括使用 EV-SSL 的 HTTPS 在内所有类型的网络流量进行控制，在被窃取的信息发送到金融网站之前就被传送到远程服务器上。（威胁等级高）
		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）
		Trojan[Ransom]/Win32.Radam	此威胁是一类可以加密用户文件并勒索赎金的木马家族。该家族样本运行后加密用户文档并要求付费，只有按时付费才可以解密，有一定威胁。（威胁等级高）
		Trojan[Downloader]/MSWord.Steamilik	此威胁是一种具有下载行为的木马类程序。该家族通过垃圾邮件进行传播，样本为 Word 宏病毒，运行后连接网络下载其它恶意程序并运行。（威胁等级中）



利用 AI 解决网络安全人才短缺问题

Deborah Golden / 文　安天公益翻译小组 / 译

高失业率固然不是什么好事，但接近 0% 的行业失业率也不是件好事。极低或零失业率意味着：没有足够的网络安全专家填补职位空缺；对现有人才的需求旺盛，造成薪资上涨和较高的人才流失率；组织更有可能雇用技能不足的员工。这正是网络安全领域的现状，而且不太可能很快得到好转——到 2019 年全球预计将有超过 150 万个职位空缺。

无论组织如何努力，他们也将无法聘请足够的大学毕业生、招聘足够的技术专业人员或者对现有员工进行再培训以减轻这种短缺。但他们可以采用另一种方法：认知计算（学习、思考和与人类交互的系统）。通过使用人工智能、机器学习、高级分析技术和自动化等认知技术，组织可以提高现有员工的生产力并优化支持流程来解决人才短缺问题。

道理很简单：认知计算可以使组织更好地利用网络安全人才的时间和技能，并提高安全性。员工不必再花费大量时间响应潜在威胁或普通管理任务，他们可以聚焦于主动安全和复杂的调查。

例如，认知技术可以通过改进组织的工作流程来解决人才短缺问题。一家领先的投资公司指出，通过实现日常活动的自动化，之前耗费网络专家约 40 分钟的任务现在可以在 40 秒内完成，分析师的生产力提高了三倍。这就是自动化的价值：在时间和人才已经不足的情况下，不需花太多的时间在普通任务上。

除了节省时间，它还能省钱。最近的一项研究发现，组织每年花费大约 21 万小时调查误报，每年的平均成本为 130 万美元。这些警报可以由认知系统来处理，只有在需要进行更多调查时认知系统才会通知网络安全人员。

自动化才刚刚开始。其更强大的应用之一是使用高级分析。这种技术使用超级计算机的处理能力来筛选大量数据，以识别行为模式、恶意代码和不明显的网络异常。这可以帮助网络专业人士预测威胁最有可能发生的地方，然后在威胁发生之前予以阻止。

我们以一个大型有线和互联网服务提供商为例，该提供商每天接收超过 50 万个网络安全警报。它部署了一个行为分析应用程序，允许分析师设定基准网络活动，识别和关联安全警报，以隔离最具威胁性的警报并改进安全阈值。结果是：六个月后，该提供商的警报减少了 99.8%，其网络安全专家可以将精力放在最高优先级的警报上。

如何使用

行为分析的应用是无止境的。银行可以使用这种技术来识别偏离个人用户典型行为的可疑在线账户活动，从而阻止盗用、欺诈或进一步的网络渗透。网络安全公司可以使用行为分析来检测新病毒或未知攻击，并在损坏发生之前阻止恶意行为，从而以机器速度进行响应。

行为分析是认知技术对网络安全的最大贡献之一，因为它允许组织采取主动的方法。从大量网络流量中筛选异常行为的能力是一个巨大的安全优势。能够预测威胁最有可能发生的地方，然后在威胁发生之前阻止它们，从根本上改变安全态势。

认知技术解决网络安全人才短缺的另一种方法是帮助减少人才流失（员工对工作感到不满意会导致人才流失）。典型的工作日充斥着无休止的、不具有挑战性的任务或活动，这会导致员工另寻高就。根据人力资源管理协会的报告，48% 的员工认为工作本身对工作满意度至关重要。

自然地，有人担心认知计算意味着“机器人取代人类”，或认知技术的效率可能会导致人类失去工作。这种恐惧有些夸张了。当杂货店引进自助结账亭时，收银员也曾担心会失去工作。ATM 的出现和广泛采用使得许多人认为银行柜员会失业。但是实际情况是，杂货店收银员和银行柜员的数量仍然在不断增长。在网络安全领域，机器无法实现的人类交互和创造力仍然具有压倒性的需求。

关键是不要与机器对抗，而是与它竞争。认知技术可以管理安全任务、预测恶意攻击并帮助留住员工。这些能力使公司能够通过重新分配现有人员来解决人才短缺问题，而不必仅仅依靠雇用新的和有经验的人才，同时也能够改进流程并加强决策。

但是机器不是万能的。通过将机器与对组织网络的认识相结合，网络安全专家可以识别网络的弱点，了解组织易遭受的网络攻击类型，并优先处理相关的漏洞。通过这种方式，人机配合可以在更短的时间内产生更好的效果。

原文名称	Curbing the Cybersecurity Workforce Shortage with AI
作者简介	Deborah Golden，Deloitte & Touche 律师事务所咨询业务的主要负责人，拥有超过 20 年的信息技术、安全和隐私保护经验。
原文信息	2017 年 8 月 18 日发布于 Dark Reading 原文地址 http://www.darkreading.com/threat-intelligence/curbing-the-cybersecurity-workforce-shortage-with-ai/a/d-id/1329617?
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《Mamba 勒索软件变种分析报告》

安天的分析人员发现：虽然自 2016 年攻击旧金山交通系统后，与 Mamba 勒索软件相关的声音逐渐沉寂下来，然而近期，有研究人员发现 Mamba 勒索软件再度活跃，并在南美和中东地区对目标展开攻击。在最近的一次活动中，研究人员将目标范围锁定在巴西和沙特阿拉伯等地区。

Mamba 勒索软件在 2016 年被发现，主要针对巴西的目标和组织。2016 年 11 月，Mamba 勒索软件攻击旧金山交通机构，致使旧金山地铁系统瘫痪，市民免费乘车。值得注意的是，Mamba 是最早进行全盘加密的勒索软件家族之一，WannaCry 勒索软件也采取了类似的加密策略。与多数勒索软件有所不同的是，Mamba 新变种的开发者似乎无意追求经济利益，而是专注于加密目标的系统和文件。

最新的 Mamba 变种在感染受害者机器时，要经过两个步骤：首先，Mamba 会在目标机器上创建临时文件目录 C:\xampp\http\，然后释放开源磁盘加密应用程序 DiskCryptor 组件并安装响应驱动，在驱动程序安装结束后，创建 DefragmentService 服务并重启机器。在受害者系统重启后，Mamba 会覆盖现有的启动记录，设置新的 MBR 内容，并清理相关数据。

正如前文所提到的，Mamba 新变种最大的威胁之处，并不仅是它对主机数据和文件的加密行为，而在于其背后开发者与利益驱动截然不同的单纯专注于破坏的取向。如果在未来有更多的攻击者将类似的模式用于针对性攻击当中，那么受害者面临的威胁，绝不仅是窃密，而是自身重要的数据和信息处于攻击者随心所欲的控制之下。对于一些部门、机构和个人来说，即使数据只是单单被加密而没有被窃，那种损失也是相当大的。

由于 DiskCryptor 使用强加密算法，目前在密钥未知的情况下，Mamba 变种尚无有效解密方法。故安天分析人员提醒用户，严防来历不明的邮件附件和网站，保持杀毒工具的实时监控，并定期做好重要数据备份工作。

目前 Mamba 新变种样本已由安天追影威胁鉴定器检出。

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、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、动态行为 (Windows7) 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、智能学习鉴定器将文件判定为木马程序。

文件名	b9b6045a45dd22fcaf2fc13d39eba46180d489cb4eb152c87568c2404aecac2f
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.06 MB
MD5	79ED93DF3BEC7CD95CE60E6EE35F46A1
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Mambretor.D
判定依据	BD 静态分析

报告地址：https://antiy.pta.center/_lk/details.html?hash=79ED93DF3BEC7CD95CE60E6EE35F46A1

◆ 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、Office2003、Flash、Wps、FoxitReader、AdobeReader

◆ 文件操作

操作	新建
文件路径	c:\xampp\http\log.txt

◆ 运行环境

操作系统	Windows 7 6.1.7600 Build 7600
内置软件	默认、IE9、Office 2007、Flash、Wps、FoxitReader、AdobeReader

◆ 文件操作

操作	新建
文件路径	c:\xampp\http\log.txt

◆ EXIF 信息

描述	值
File Size	1086 kB
File Type	Win32 EXE
MIME Type	application/octet-stream
Machine Type	Intel 386 or later, and compatibles
Time Stamp	2017:04:06 04:53:19+08:00
PE Type	PE32
Linker Version	12.0
Code Size	117248
……	……