安天周观察

安天官方微博　安天官方微信

主办：安天　2017 年 11 月 27 日（总第 113 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天携手广州大学共建网络空间高级威胁对抗联合实验室

11 月 20 日上午，安天和广州大学联合建立的“网络空间高级威胁对抗联合实验室”（以下简称“联合实验室”）签约揭牌仪式在广州大学举行。联合实验室将针对网络空间安全领域高级威胁的挑战，综合分析高级威胁对政企网络、智慧城市、关键信息基础设施等场景的影响。形成校企共建、培养复合人才、输出先进工程成果的模式。

本次签约揭牌仪式由广州大学网络空间先进技术研究院院长田志宏主持，中国工程院院士、广州大学网络空间先进技术研究院名誉院长方滨兴，广州大学党委书记屈哨兵，安天首席技术架构师肖新光等出席了本次签约仪式并致辞。

与会校企来宾共同为联合实验室举行了揭牌仪式，此后方滨兴院士向安天首席架构师肖新光、安天移动安全公司 CEO 潘宣辰、安天深圳研发中心负责人康学斌颁发了广州大学企业导师聘书。

校企联合具有非常强的优势互补关系，将是充分发挥双方各自特长、实现产学研无缝对接、可同时满足核心技术研究和产业化需要的最佳途径。双方成立联合实验室，以广州大学的科研力量来推动网络安全的创新产业发展；同时以安天的需求为导向，支持和推动实验室在相关核心技术方面的研究和积累。联合实验室将成为双方合作的窗口和新技术科研成果的中试基地和产业化基地。

作为中国网络安全的民企国家队，安天将依托自身在威胁检测引擎、端点防护、流量监测、威胁分析、态势感知等多方面的综合技术积累，希望能为高校科研创造一个基于企业工程能力基础展开、学术拓展和技术创造的优秀环境，与广州大学共建网络安全的工程体系，共同为国家培养能够有效直面网络安全挑战的复合型工程人才。

永州市副市长周荣峰一行莅临安天参观调研

11 月 22 日，永州市市委常委、市人民政府副市长周荣峰，市经信委主任高守凯，市网信办主任蒋旭军，市经开区管委会副主任廖为华，经开区财政局局长伍千舟，经开区商务局副局长陈征遥等一行领导莅临安天北京办公区进行参观调研，安天总裁胡忠华全程陪同接待。

安天相关负责人首先向来宾展示了安天态势感知与监控预警平台以及其在普通场景及应急场景下的响应过程及分析、研判过程。之后为来宾介绍了组成安天态势感知平台的安天智甲终端防御系统、探海威胁检测系统、追影威胁分析系统等安天安全产品。在安天对高级威胁发现、捕获和分析方面所做的工作中，重点介绍了安天针对“白象”、“方程式”等攻击组织的 APT 攻击情况、所使用的攻击装备等的分析进展。

永州市位于湖南省南部，是国家历史文化名城，唐宋八大家之一的柳宗元曾为其写下《永州八记》。如今的永州是一座活力迸发、开放崛起的“现代化”新城，其云计算、大数据产业的发展处于湖南省前列。当今时代，网络安全事故频发，今年 6 月份正式实施的《中华人民共和国网络安全法》中指出，要“保护关键信息基础设施免受攻击、侵入、干扰和破坏”。网络安全保障对云计算、大数据产业来说是最基础的保障。

安天作为专注于威胁检测防御技术的能力型安全厂商，具有 17 年威胁对抗经验，依托自主先进的威胁检测引擎等系列核心技术和专家团队，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。针对永州市加快发展云计算、大数据等相关产业，安天可提供配套的网络安全防护体系及安全服务，通过全线安全产品、技术能力及对网络安全人才的培养引进，为永州市网络安全保驾护航贡献自己的一份力量。

参观调研结束后，各位来宾对安天的技术、产品和解决方案能力表示肯定，并对与安天开展合作表示期待。

每周安全事件

类 型	内 容
中文标题	Crooks 设置了一个假的赛门铁克博客来传播 macOS 质子恶意软件
英文标题	Crooks set up a fake Symantec Blog to spread the macOS Proton malware
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	macOS 质子恶意软件的一个新的应变软件正在通过博客欺骗安全公司赛门铁克的合法博客传播。攻击者使用的是原始站点相同的域名注册信息创建一个伪造的博客 symantecblog[dot]com。该站点的 SSL 数字证书 Comodo 颁发的合法证书，而不是 Symantec 的证书颁发机构。 有关 CoinThief 恶意软件新版本的帖子正在推广名为“Symantec Malware Detector”的应用程序，该应用程序用于分发 OSX .Proton。 恶意的 Symantec 恶意软件检测器应用程序会显示一个带有 Symantec 徽标的简单窗口，需要授权才能执行系统检查。如果受害者同意运行该检查，则会请求管理员密码，从而允许恶意软件窃取密码，在后台安装 Proton 恶意软件。 一旦安装，Proton 恶意软件会收集用户信息，如管理员密码和其他个人身份信息（PII）。
链接地址	http://securityaffairs.co/wordpress/65902/malware/macos-proton-malware.html

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 10 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.Hhyy.a[prv,exp] 2017-11-20	该应用程序内嵌恶意插件，运行后台私自下载其他软件，并创建桌面快捷图标诱导用户安装，同时会上传收件箱短信造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.xrTcp.a[prv] 2017-11-20	该应用程序为测试应用程序，程序运行会通过 socket 连接到远程服务器，获取用户短信信息、通讯录和通话记录等隐私信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.ZywAppstore.a[exp,sys] 2017-11-21	该应用程序包含风险代码，监听收件箱拦截特定短信并自动回复，影响用户正常使用，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.bbq.a[exp,rog] 2017-11-21	该应用程序内嵌恶意代码，运行私自下载恶意子包，动态加载，私自推送广告，下载安装未知应用，造成用户资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.DollFill.a[exp] 2017-11-21	该应用程序伪装 WhatsApp 更新应用，无实际功能，运行推送全屏、banner 等广告，造成用户资费损耗。（威胁等级高）
		Trojan/Android.SmartT.a[exp,rmt,spy] 2017-11-22	该应用程序伪装正常应用程序，实际是间谍程序，接收远程指令下载安装指定文件、卸载指定文件、访问指定网页、进行 USSD 通信、修改访问主页等，会造成用户资费损耗，影响用户正常使用，建议卸载。（威胁等级高）
		G-Ware/Android.VpsDrop.a[exp,rog] 2017-11-23	该应用程序为游戏，应用非官方版本，植入广告子包和其他软件，运行后要求用户安装推广软件，频繁推送广告，造成用户流量消耗，影响用户体验，建议卸载。（威胁等级高）
		Trojan/Android.WapreachSpy.a[prv,rmt,spy] 2017-11-24	该应用程序伪装正常应用程序，运行后通过解析消息指令，后台窃取用户短信、联系人、通话记录、地理位置、手机存储数据等隐私记录，私自下载其他软件、私自录音，并将隐私信息上传至指定服务器。造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Rootnik.af[exp,sys] 2017-11-24	该应用程序安装无图标，后台联网下载 ROOT 文件私自提权，静默下载并安装未知文件，建议立即卸载，避免造成资费损耗。（威胁等级高）
		Trojan/Android.ExpensiveWall.a[exp,rog] 2017-11-24	该应用程序伪装正常应用程序，运行后通过 webview 方法加载的 JS 广告页面，并在用户不知情的情况下，诱导用户点击按钮，然后触发发短信操作，造成用户资费消耗，建议卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	微软 Office 内存损坏漏洞导致远程命令执行 CVE-2017-11882	Microsoft 微软在例行系统补丁发布中，修复了一个 Office 远程代码执行的严重漏洞，编号 CVE-2017-11882。该漏洞类型为缓冲区溢出，位于 EQNEDT32.EXE 组件。受害用户打开恶意的 office 文档时，无需交互，就可能执行恶意代码。（威胁等级高）
	较为活跃样本	Trojan[Banker]/Win32.Banaris	此威胁来自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。（威胁等级高）
		Trojan[Backdoor]/Win32.AutoIt	此威胁来自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[Ransom]/Win32.Zerber	此威胁来自一类可以加密用户数据的木马程序。该家族样本是勒索软件，运行后加密用户文件，加密后播放声音提示用户文件已被加密，需支付比特币才可以解密。（威胁等级中）

人工智能和机器学习需要包容性

Patrick Hill / 文　安天技术公益翻译组 / 译

如果企业在应用预测分析、人工智能和机器学习方面具有前瞻性思维，那么他们可以使这些技术具有包容性，以便所有人都能使用。

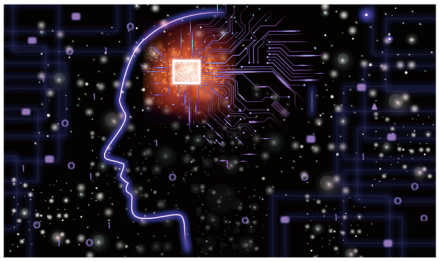
试想一下，如果一件东西在设计时没有将你或像你一样的人考虑在内，却能驱动你日常生活中的各种互动。它可以控制向你推销什么产品、你如何使用（或不使用）某些产品，影响着你与执法机构的交互，甚至决定你的医疗诊断和医疗决策。

人工智能（AI）和机器学习（ML）的核心问题正在凸显。AI 算法本质上是嵌入代码中的意见。人工智能可以通过在构思、测试和实施过程中排除不同观点来创造、规范或加剧偏见。年龄歧视、残疾歧视、性别歧视和种族歧视正在被嵌入到一些作为“智能”系统基础的服务中，这些系统决定我们如何被分类、营销、服务或歧视。

ML 输出与重复的数据、图片和文字关联输入没什么两样。如果这些输入是由一个小的，同质的工程师或产品经理组成的小组来选择的，且没有这个小组之外的人进行细化或审查，则输出结果会有偏差，几乎无法检查底层的逻辑。这意味着训练数据的选择需要涵盖复杂的（而不是单一的）观点。如果这些技术的样本很小且一致，则算法将会从不完整的数据、图片和文字中继承偏差并加强这种偏差。

同质团队、测试和数据会产生问题。以简单的照片识别系统为例，2015 年夏天，Google 照片应用程序将两张黑人的照片标记为了大猩猩。

还有一些 AI 和 ML 基于数据驱动的见解开发，如果这些数据不够包容，可能会造成破坏性的，甚至危及生命的后果。今年早些时候，澳大利亚阿德莱德大学（University of Adelaide）进行了一项研究，48 名参与者都是



60 岁以上的老人，研究人员使用人工智能技术分析参与者的器官照片，预测哪些人将在 5 年内死亡，准确率达 69%。虽然以这样的准确度进行预测的能力是惊人的，但在分析少量样本时要吸取教训。

这些信息可用于 ML 目的，帮助制定医疗决策并提供建议。但还有个关键问题：参与者是什么种族？这是至关重要的，因为某些种族罹患某些疾病的几率较高，例如黑人女性罹患肌瘤的几率较高，拉丁美洲人群更可能患糖尿病和肝病。如果数据集不包括这类信息，则可能导致不同的治疗结果，包括误诊、无法做出诊断或治疗效果不佳。

智能应用程序也可以决定你如何、何时以及为什么花钱。广告公司正在测试 IBM Watson 的 AI 功能，以便为客户推荐感兴趣的产品。例如，通过理解用户在对话中表现出的个性、语气和情绪来实现个性化的推荐——如果这些推荐不会与身份分析混为一谈，那还真是不错。但要避免一个可能的结果：应用程序根据你的声音模式确定你更可能来自洛杉矶中南部而非比佛利山庄，因此只为你提供黑人学院和大学的信息。

我们应避免这种情况，创建一个更具包容性的 AI，以下是一些能够提供帮助的措施。

组件一个多元化的团队。如果核心团队中没有能够代表不同类型的客户的成员，你是否可以在其他团队中找到？从其他职能团队中引入多元化员工可以提供更多的视角。如果在公司内部仍然无法找到具有代表性的员工，那么将客户带入开发周期如何呢？你可以在创建用户故事的过程中获得他们的反馈，或让他们参与演示。

找到多样化的训练数据集。如果你的目标是为广大受众提供服务，那么扩大您的来源以获得每个细分受众群的足够数据至关重要。随着语音命令用户界面的使用越来越多，有许多人因为命令不被理解而感到沮丧。为什么呢？因为他们有口音。语音服务的早期训练数据大部分来自使用中性口音（如广播员的口音）收集数据的研究人员和大学生（同质群体）。Google 的语音识别服务正在扩展训练数据集，为解决导致偏见和服务无法使用的狭窄数据源问题树立了榜样。

GoDaddy 也发现，我们需要明确获取足够深度的客户数据，以便涵盖每个群体。举例来说，我们的域名搜索建模团队最初使用我们的美国模式来决定在其他国家显示哪些域名，但是发现它比非智能模式更加糟糕。为什么呢？在相同的模式下，其他国家的客户的表现相当不同。直到我们把具体的国家分成不同的模式时，才看到了明显的改善。

法律的步伐落后于技术，后者推动创新，而前者在通过立法或制定政策之前要先看看结果如何。如果企业在应用预测分析、人工智能和机器学习方面具有前瞻性思维，那么他们可以在不需要新的法律法规的情况下使这些技术具有包容性。所有公司，不管规模大小，都有明确的步骤把这项技术带给所有人。这始于团队中的某个人的疑问：“我们是否在构建一个涵盖所有人的未来愿景？”

原文名称	The Need for Inclusion in AI and Machine Learning
作者简介	Steven Aldrich 是 GoDaddy 的首席产品官。Bär í A. Williams 是 Marqeta 的副总法律顾问。
原文信息	2017 年 11 月 6 日发布于 InformationWeek 原文地址 https://www.informationweek.com/big-data/ai-machine-learning/the-need-for-inclusion-in-ai-and-machine-learning/a/d-id/1330464?
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《新型勒索软件 GIBON 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，一款新的勒索软件 GIBON 开始活跃。今年 5 月份地下黑市中就已经出现了这款勒索软件的身影。多个网站出售这款勒索软件，价格为 500 美元。广告语用俄语撰写，详细描述了这款软件的特点和功能。

GIBON 主要利用垃圾邮件传播，但确切的传播机制现在还不清楚，主要攻击被感染计算机中除 Windows 文件夹以外的文件。一旦其感染计算机后，GIBON 会连接到其 C & C 服务器，并发送包含时间戳、Windows 版本和“注册”字符串（用于通知 C & C 新的受害者）的 base64 编码字符串去感染下一个受害者。随后服务器会返回一个 base64 编码的字符串，作为 GIBON 的勒索通知。利用这种设置，攻击者可以即时更新赎金，而不必编译新的可执行文件。一旦受害者注册到 C&C 服务器中，GIBON 就会在本地生成一个加密密钥，然后以 base64 编码的字符串形式将其发送到 C&C 服务器。该密钥用于加密计算机上的所有文件，并为所有加密文件附加上 .encrypt 扩展名。在加密过程中，GIBON 会继续对服务器执行 ping 操作，表示加密正在进行。加密完成后，则会向服务器发送最终消息，包含字符串“完成”、时间戳、Windows 版本以及加密的文件数量。最后 GIBON 会在每个已加密文件的文件夹中加入赎金通知，要求受害者通过电子邮件 bomboms123@mail.ru 或子公司 yourfood20@mail.ru 联系攻击者以获取付款说明。

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勒索软件样本的检出。

勒索软件

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述勒索软件进行有效检测，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。

最终依据静态分析鉴定器将文件判定为恶意程序。

文件名	30b5c4609eadafc1b4f97b906a4928a47231b525d6d5c9028c873c4421bf6f98
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	523KB
MD5	5BAED5607749DEABDDD1722F3C3BFA0F
病毒类型	恶意程序
恶意判定 / 病毒名称	VCS/Instruction.PEEPOCheck
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

◆ 静态启发式检测

检测类型	检测点	详细说明
PE 结构	含有 tls 表	恶意代码作者常用的反调试技术。PE 结构中的 TLS 结构早于程序运行。
编译指令	未知壳	未被公开的壳，经常被恶意代码使用，用来保护恶意程序被查杀。
PE 结构	无版本信息并且不是 GCC 编译器	除 GCC 编译器外，常规编译器均默认包含版本信息。如果不是 GCC 编译器，并且不包含版本信息，显然是作者故意抹掉版本信息，逃避追查。
PE 结构	PE 的子系统是 GUI	基于海量恶意代码和受信白名单文件名进行数据挖掘，恶意程序通常不包含 GUI。
PE 结构	入口点遮蔽	使用了入口点遮蔽（Entry-Point Obscuring,EPO）的病毒编码技术。EPO 技术可以躲避杀毒软件的检测。