安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 01 月 01 日 (总第 118 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天北京公司上榜中关村成长企业 TOP100

2017 年 12 月 26 日，由北京市科委、中关村管委会指导，北京中关村高新技术企业协会与中关村创业投资和股权投资基金协会联合主办的“2017 中关村高成长企业 TOP100”评选活动颁奖典礼在京落下帷幕，安天北京公司成功入选。

中关村高成长 TOP100 活动紧扣中关村示范区战略发展和中心工作，聚焦中关村示范区具有核心技术、创新能力强、发展速度快、拥有良好发展前景的优秀企业，已成为发现探索示范区优秀企业的平台，从一定程度上推动了示范区企业行业自律和标准化机制的建立。

上榜企业均为国家级高新技术企业，覆盖国家重点支持的八大技术领域，是所在行业的主力军，且均处于发展的快速上升期，普遍具有长期发展战略规划和短期部署、自主创新能力强、注重企业文化、社会影响力和品牌建设，其技术和产品在行业中具有较大的影响力。

本次评选活动共有 4000 多家企业参与，评委会秉承公平、公正、公开、公益相结合的“四公”原则，围绕参选企业三年来的经营状况、发展能力、核心竞争力、诚信、年收入等各方面进行考察。安天北京公司作为安天集团面向政企客户服务的核心企业及产品化中心，其自主研发创新能力、近年来的快速发展及作为网络安全企业的社会责任感等各方面均获得了评委会的认可，成功上榜“2017 中关村高成长企业 TOP100”。

以德加密货币交易所 DNS 遭黑客劫持，损失超 26.6 万美元

以德（EtherDelta）是用于以太坊（Ethereum）与 ERC20 兼容代币（已经部署在 Ethereum 区块链上的代币）之间进行交易的加密货币交易所。它并不需要登录，并且可以在全世界任何地区都能安全使用。因其分布式、去中心化以及加密签名交易的特性，而深受加密货币交易者的欢迎。

在上周三，这个加密货币交易所遭遇了黑客攻击，许多用户在不知情的情况下将其代币发送给了黑客，而不是用于交换。

据调查统计，至少有 308 个以太币（约价值 266,789 美元）以及其他潜在价值超过数十万美元的代币被盗。

EtherDelta 是一个去中心化交易所，提供去中心化、分布式交易，它涵盖了几乎所有类型以太坊代币的交易。

与较大的交易所相比，它的交易量并不大，但是在 ICO（初始投币产品）中生成新的代币之后，这对于交易者来说是重要的第一步。

显然，支配 EtherDelta 行为的智能合约在攻击中并没有受到损害。相反，攻击者成功地劫持了 EtherDelta 的 DNS 服务器，并为交易者提供了一个虚假版本。虚假网站模仿了真实网站的域名，这比常见的网络钓鱼攻击更为危险。

整个攻击只存在了几个小时，真实的 EtherDelta 网站很快就得到了恢复。但就是在这几个小时期间，已经有很多交易者向黑客发送了以太币或其他代币的令牌。

这些代币从下午 1:40 开始流入，直到大约晚上 8 点。攻击者在周四凌晨 1:30 左右将大部分资金转移到了其他地址。

EtherDelta 官方在 Twitter 上确认了这一攻击事件，并建议所有用户暂时不要使用该网站。

每周安全事件

类 型	内 容
中文标题	某俄罗斯银行运营的自动取款机可能会因五次按下“Shift”键而被黑掉
英文标题	ATMs operated by a Russian Bank could be hacked by pressing five times the ‘Shift’ key
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	我们多次警告ATM运行Windows XP操作系统的风险。最近，俄罗斯博客平台Habrahabr的一名员工发现，这些系统很容易被黑客攻击，据报道，运行Windows XP的Sberbank银行的ATM受到容易被利用的安全漏洞的影响。 用户发现，通过按SHIFT，CTRL，ALT和WINDOWS五种特殊键，可以绕过防止访问ATM操作系统的各种组件的全屏锁定。 通过按SHIFT键5次，就可以访问Windows设置并显示任务栏和操作系统的开始菜单，这样用户就可以通过使用触摸屏来访问Windows XP了。这个漏洞允许黑客修改ATM启动脚本并在机器上安装恶意代码。 根据德国网站WinFuture的说法，Sberbank几乎在两周前就被通知了ATM的安全漏洞。该银行确认立即解决了安全问题，但发现该缺陷的用户声称，他所访问的终端上仍然存在此问题。
链接地址	http://securityaffairs.co/wordpress/67128/hacking/atms-russian-bank-hack.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

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.Bol7.a[prv，spy] 2017-12-25	该应用程序运行后申请设备管理器，可根据拨号指令显示和隐藏图标，会保存用户设备信息、通话记录、短信信息、照片和视频信息，会根据用户设置进行email或者ftp上传，同时会接收短信远程控制手机，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.letmespy.a[prv，spy] 2017-12-26	该应用程序为间谍软件，运行后隐藏图标，后台窃取用户短信、联系人、通话记录、地理位置等信息，并上传至远程服务器。造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.SoapControl.a[rmt，sms] 2017-12-26	该应用程序运行后隐藏图标，通过Soap获取指定网站信息，根据信息控制手机拦截短信、群发短信、挂断电话，会造成资费消耗和信息泄露，建议卸载。（威胁等级中）
		Trojan/Android.egamex.a[pay] 2017-12-28	该应用程序为游戏类应用，程序运行后，后台会订阅付费服务，私自发送付费短信，监听、拦截短信并发送回执短信，造成用户资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.roilstap.a[prv，exp] 2017-12-28	该应用程序伪装系统更新，运行诱导激活设备管理器，上传用户固件信息、安装列表、收件箱短信，还会私自下载未知文件，造成用户隐私泄露和资费损耗，请卸载。（威胁等级高）
		Trojan/Android.AnubisSpy.a[prv，rmt，rtt] 2017-12-28	该应用程序伪装正常软件，私自释放文件提权。后台解析远程控制命令，监控用户手机，窃取短信、照片、视频、联系人、电子邮件帐户和浏览器历史记录。私自截图，录制电话等音频数据。窃取用户社交软件信息，并将这些隐私信息上传至服务器，会造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.PickBitPocket.a[pay] 2017-12-29	该应用程序伪装bitcoin交易应用，欺骗诱导用户购买交易，其实际支付地址定向到指定账户，造成用户资费损耗，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.BankerSpy.e[prv，rmt，spy]	该应用程序启动后隐藏图标，接收远程指令上传用户短信、联系人、通话记录、位置等隐私信息，通过远程数据构造钓鱼界面窃取用户的银行相关信息，还会执行拦截短信，发送短信等危险行为，造成用户隐私泄露，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	WebLogic XMLDecoder反序列化漏洞（CVE-2017-10271）	Oracle Fusion Middleware中的Oracle WebLogic Server组件的WLS Security子组件存在安全漏洞。使用精心构造的xml数据可能造成任意代码执行，攻击者只需要发送精心构造的HTTP请求，就可以拿到目标服务器的权限。攻击者可利用该漏洞控制组件，影响数据的可用性、保密性和完整性。（威胁等级高）
	较为活跃样本	Trojan[Backdoor]/Win32.Agent	此威胁来自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）
		Trojan[Exploit]/SWF.Angler	此威胁来自一个木马家族。该家族因Angler Exploit Kit而得名。该家族的样本使用了SWF的漏洞对用户的设备进行感染，从而执行任意恶意代码。（威胁等级中）
		Trojan/Win32.Inject	此威胁来自一种木马类程序。该家族将自身以某种方式注入到其它进程中（避免用户和杀毒软件感知、清除），隐藏自身，并在后台执行恶意行为。因此该病毒家族是一种通过行为来命名、定性的木马类程序。（威胁等级中）
		Trojan/Win32.Pirminay	此威胁来自一种木马类程序。该家族入侵电脑后，会修改注册表信息，以便隐藏自己躲避杀毒软件的查杀。该家族的不同变种具有不同的恶意行为，如：自动下载恶意程序、允许黑客远程入侵、窃取用户信息（账号密码）等。（威胁等级中）

企业是时候投资人工智能了？

John Edwards / 文　安天技术公益翻译组 / 译

几十年来，人工智能（AI）被视为一个“未来”的概念，也许公司是时候做些真正的投资了。

埃森哲公司（Accenture）最近的一项调查显示，85%的企业高管计划在未来三年大力投资于与人工智能相关的技术。根据该报告，大部分投资将集中在主要的业务流程，以支撑公司的财务和会计、营销、采购和客户关系活动。

IBM Watson 首席架构师鲁奇尔·普瑞这样认为：“在各行业的企业中，人工智能技术可以广泛应用于前端、中端和后端流程。人工智能的能力，如对话、视觉和语言技术，可以用来解决一系列实际的企业问题，提高生产力，促进各个领域的新发现。”

进入企业

埃森哲应用智能公司首席技术官让－吕克·彻斯特兰发现，在高科技行业，人们强烈地感觉到人工智能即将跨越鸿沟并成为企业转型技术。“已经有证据表明人工智能的影响力，它在医疗和生命科学等领域的影响力将会更大，如促进乳腺癌检测或个性化药物开发等。”

纽约大学斯特恩商学院的教授瓦森特·达哈表示，只要有数据存在，人工智能就可以投入使用。他解释说：“人工智能可用于客户服务、市场营销、规划、收集新客户或资产等。”

根据 IBM 的一项研究，世界上 80%的数据不在网络上，而是在企业内部闲置。普瑞说：“今天，大多数组织只能够探索这些‘隐藏’数据的一小部分。”人工智能是解锁隐藏资源的关键。

达哈指出，人工智能为企业提供了三个

基本的好处：从数据中持续学习，改进决策并使其更加一致，提高运营效率并降低成本。

审计、税务和咨询公司 Grant Thornton 的市场、客户和行业全国管理合伙人尼科尔·约且指出，在提高速度、准确性、可用性和可审计性的同时，人工智能还可以降低成本。她表示：“任何涉及结构化数字数据和业务规则的过程都将受益。人工智能还可以协助前台功能，如通过聊天机器人和移动消息与客户交互，以解决常见的客户问题。”

戴尔 EMC 公司人工智能战略的首席技术专家赛德·塔贝特认为，人工智能在安全应用方面的前景非常光明。他指出：“多年来，基于人工智能的模式识别技术已应用于各种 IT 和网络安全应用中，主动管理系统性能或阻止安全威胁。这些能力只会越来越普遍。”

优势评估

普瑞说：“人工智能已经不再是一项‘还不错’的技术了，它正在成为企业工具库中的重要组成部分。大规模部署人工智能技术的企业将大大提高生产力，使员工能够处理更复杂、更具创造性、影响更大的任务，开辟全新的探索和发现途径。”

根据约且的说法，业务流程改进可以通过几个指标来衡量，比如降低人员成本，提高速度、准确性、质量、可重复性、可用性、可审计性和生产力。“机器人不休假、不生病，也不休息。”她打趣地说。

菲斯特建议说：“实施人工智能所带来的改进应该通过对当前绩效进行基准测试，然后与人工智能部署后进行比较来测量。”

开始行动

对于计划使用人工智能的企业来说，第一步是确定该技术能够对企业的哪些领域产生最大的影响。菲斯特解释说：“一旦公司确定了这些领域，他们就可以与著名的学术机构、领先的技术供应商和行业分析师合作，更好地了解可用的人工智能技术，并将其部署在可以轻松测量的受控环境中。”

约且说，企业应该采取主动的方法，即盘点当前的服务，了解人工智能技术能够如何改善它们。她补充说：“他们还应该评估人工智能可以帮助或加强哪些内部手动重复流程，以便更好、更快地为客户服务。”

要想充分利用人工智能的潜力，企业领导人必须能够清晰地表达自己的目标和期望，然后准备正确的工具、数据和人才。普瑞解释说：“另外，在部署人工智能技术之前，检查企业中是否有人已经在使用人工智能，因为跨部门的协作可以节省时间。”

为了避免因人工智能内在的复杂性而陷入困境，许多企业选择“AI 即服务”（AI-as-a-service），在图像识别和自然语言处理等领域使用产品化的现成 API 和 AI 应用程序。彻斯特兰说：“试验这些经过验证的实际应用，以展示人工智能的潜力，做好失败的准备并继续前进。”

原文名称	Is It Time for Your Organization to Invest in AI?
作者简介	John Edwards，John Edwards 是一位资深的商业技术记者。
原文信息	2017 年 12 月 13 日发布于 InformationWeek 原文地址 https://www.informationweek.com/big-data/ai-machine-learning/is-it-time-for-your-organization-to-invest-in-ai/d/d-id/1330683?
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《File-Locker 勒索软件分析报告》

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勒索信为韩语的勒索软件 File-Locker。一旦受害者遭受该勒索软件攻击，需要向攻击者支付 50K 韩元解密文件。通过对 File-Locker 分析发现，该勒索软件属于 Hidden Tear 的变种（Hidden Tear 是在 2015 年出现在开源社区 github 的用于学习和教学用途的勒索软件，但逐渐被恶意攻击者修改滥用）。File-Locker 对 Windows .NET 用户有效而不仅是韩语用户，加密成功后将加密文件后缀名修改为“.locked”，加密方式是使用对称加密算法 AES，并且没有与其他加密算法结合使用，因此 File-Locker 可以通过查找硬编码的密码进行解密。

通过对 File-Locker 勒索软件的样本分析发现，样本编译环境是 Microsoft Visual C# v7.0 / Basic .NET (managed)，样本使用 windows 10 图标作为伪装，一旦被受害者点击执行，将会扫描受害者机器的文件目录，包括桌面、图片、文档、下载、音乐和视频目录，并针对常见文档扩展名进行加密。随后在桌面创建 Warning!!!!!!.txt 勒索信息文件。通过对样本反编译，得到 AES 加密密钥“dnwls07193147”，因此可通过该密钥对加密文件进行解密。

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。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，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。

最终依据智能学习鉴定器将文件判定为木马程序。

文件名	ransomb6b5e455c4ebe875907aa185988c2eb654ed373dc0e6b712a391069d63dc5c3f
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	391 KB
MD5	6FFD90E8B1B4C38F801D2A694CD6C01C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.HiddenTear.gen
判定依据	静态分析

进程监控

检测类型	检测点	详细说明
PE 结构	非微软的版本信息	非受信厂商的版本信息。具有较低的受信级别。
PE 结构	PE 有附加数据	PE 文件包含附件数据通常用来对抗云检测。云检测通常使用全文 HASH 进行检测，在 PE 尾部增加一段数据，不影响程序正常执行，但会使程序的全文 HASH 发生改变，从而逃避云检测的查杀。

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

UDP 信息

源 IP	源端口	目的 IP	目的端口
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.246	68
192.168.122.246	137	192.168.122.255	67
192.168.122.246	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.246	1025
192.168.122.246	123	13.65.245.138	123
13.65.245.138	123	192.168.122.246	123
192.168.122.246	138	192.168.122.255	138

文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.exe	6ffd90e8b1b4c38f801d2a694cd6c01c	N/A	N/A