安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 04 月 09 日 (总第 130 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

不忘初心缅怀先烈遗志，寸土不让守卫网络安全

清明将至，为缅怀革命先烈，继承发扬革命优良传统，努力学习和践行两会精神，哈尔滨安天科技集团股份有限公司党支部组织开展了“不忘初心缅怀先烈遗志，寸土不让守卫网络安全”的参观活动。

铭记历史，传承精神

4 月 4 日下午，安天的优秀党员、团员们来到东北抗联博物馆革命教育基地进行参观学习，重温抗联历史。在讲解员的引导和讲解下，馆内的陈列场景将东北抗日联军十四年的光辉历史生动再现，主要展现了从“九一八”事变爆发到苏联红军进入东北期间，东北抗联战士在中国共产党的领导下，在白山黑水间同侵略者展开殊死斗争、保卫民族家园的史实，全面具体地展现了东北儿女不惧来犯共赴国难，英勇抵抗日本军国主义侵略的伟大光辉历史。通过橱窗内的珍贵文物和立体布景，以及一个个东北抗联形象的真实还原，将同事们带入了那段前赴后继、不畏牺牲的峥嵘岁月。

缅怀是为了更好地继承先烈遗志，在十四年艰苦卓绝的抗日斗争中，广大抗联指战员铸就的“爱国守土、团结御海、浴血奋战、视死如归、艰苦卓越、百折不挠”的东北抗联精神，安天的工程师们通过这次参观活动，接受了一次爱国主义教育和红色教育精神的洗礼，汲取了更多努力奋斗、继续前行的力量与勇气。

守卫安全，砥砺前行

安天已经开启了第三次创业的新征程，在之前的发展历史上也曾经历过多次的弹尽粮绝，也曾经历过多次的艰难困苦，但是安天人始终坚持着初心，秉承着对网络安全的执着追求，不断探索着这份融合了爱国主义、正义力量和技术追求的远大理想。习近平总书记在十九大报告中指出“更加自觉地维护我国主权、安全、发展利益”；李克强总理在两会政府工作报告中强调“坚决有力维护国家主权、安全、发展利益”。作为网络安全行业中的民企国家队，安天始终坚持走能力型安全厂商道路，坚持为用户创造和保障价值的信仰，坚持直面安全威胁的信念和勇气，安天在保卫网络疆土的事业上义不容辞，责无旁贷。

作为中国的网络安全工作者，安天的工程师们就是要用自己的技术、产品和服务维护我国的网络主权、网络安全和国家与人民的发展利益，通过创新的网络安全技术和手段，为实现“网络强国”的目标保驾护航。安天也将在社会主义新时代的新征程中展现新作为、做出新贡献，矢志艰苦奋斗、永葆本色。

警惕电脑扬声器泄漏敏感数据

近期，来自以色列本古里安大学的安全研究人员演示了一种名为“Mosquito”的攻击技术，该技术将允许攻击者通过扬声器或耳机从物理隔离或联网计算机中提取数据。

研究人员解释称，该攻击方法的隐蔽性非常高，它可以通过扬声器的超声波信号来发送和接收数据。这项技术可以将音频输出插孔转换成输入插孔，然后再将扬声器转换为麦克风。这是现代音频芯片组的一种功能，也可以说是一种特性，并且可以通过软件来实现转换。攻击者也可以通过特殊制作的恶意软件来利用这种功能，然后将目标主机的扬声器或耳机转换成麦克风，并通过超声波信号完成两台计算机设备之间的数据提取（最远距离为 9 米左右）。

目前 Mosquito 攻击仍处于试验阶段，但就实验结果来看，当前几乎所有的平台都会受到这种安全风险的影响，尤其是物联网设备，而这种安全漏洞将有可能把个人数据甚至整个企业的数据进一步暴露在网络威胁之下。除此之外，趋势科技前沿威胁研究团队的 Stephen Hilt 还对当前最流行的两款扬声器系统进行了分析，并且成功利用 Mosquito 攻击从目标系统中提取出了数据。这也就意味着，目前很多运行在企业环境中的计算机 / 网络系统都将会暴露在这种安全风险之中。

文章来源：https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/mosquito-attack-shows-how-malware-can-exfiltrate-data-via-pc-speakers

每周安全事件

类 型	内 容
中文标题	Facebook 泄漏事件再升级，受影响用户从 5000 万增长到 8700 万
英文标题	Facebook: Cambridge Analytica Accessed Data on 87 Million Users, Not 50 Million
作者及单位	Catalin Cimpanu
内容概述	美国时间 4 月 4 日，Facebook 首席技术官 Mike Schroepfer 在官网发布声明，描述了数据泄露事件之后 Facebook 近期采取的一系列加强隐私保护的措施。但他同时也表示，Cambridge Analytica 从 Facebook 获取的用户信息高达 8700 万，比之前的 5000 万多出不少。其中，超过 80% 的用户都是美国人。 Facebook 计划在 4 月 9 日星期一通知所有受影响的用户，并在他们的 Facebook 时间表顶部显示通知消息。同时，Facebook 还计划发出另一条通知，提醒所有用户（不仅是受影响的 8700 万人）查看可访问其 Facebook 数据的应用，让用户删除他们不愿意使用的软件。 为了防止有些用户忽略这些提醒，不审查自己的账户安全。Facebook 还将采取其他应对措施：如果用户在过去三个月中未使用该应用，它会自动降低应用对用户数据的访问权限。
链接地址	https://www.bleepingcomputer.com/news/security/facebook-cambridge-analytica-accessed-data-on-87-million-users-not-50-million/

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 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	较为活跃的样本	Trojan/Android.Dmrcla.d[prv,rmt,spy]	程序运行诱导激活设备管理器，释放加载恶意子包，执行私自提权，将通话录音、手机截屏、记录键盘输入信息等上传，还会拦截短信、私自发送短信，删除通话记录，造成用户隐私泄露和资费消耗，建议立即卸载。
		Trojan/Android.BankerSpy.g[prv,spy]	该应用伪装软件，运行后隐藏图标，检测用户金融软件安装状态，后台拦截用户短信，并将用户短信内容通过短信发送至指定号码。造成用户隐私泄露和经济损失，建议卸载。
		G-Ware/Android.Fake360.b[exp,rog]	该程序伪装 360 相关应用，运行后台私自下载安装广告应用，后台推送广告，会造成用户流量损耗，建议卸载。
		Trojan/Android.lanyou.b[pay]	该程序运行会解密加载恶意支付插件，私自上传手机固件信息，解析返回的扣费数据，发送扣费短信并自动回复，给用户造成经济损失，建议卸载。
		Trojan/Android.kamanDownload.a[exp,rog]	该软件运行后隐藏图标，后台下载安装未知应用，且存在自动发送短信行为，会对用户的资费造成消耗，建议立即卸载。
		Trojan/Android.cxbox.b[exp,rog]	该应用包含恶意子包，运行后私自下载并加载广告子包，后台推送广告，造成用户流量损耗，建议卸载。
		Trojan/Android.Fonobospy.a[prv,spy]	该程序伪装成系统应用，安装无图标，后台上传用户位置信息、通讯录、通话记录以及短信记录等，可能会加载广告，造成用户隐私泄露，建议立即卸载。
		Trojan/Android.nbank.f[prv,spy]	该应用伪装金融类 APP，运行会上传用户短信记录、通话记录、联系人信息等聊天信息到远程服务器，造成用户隐私泄露，建议卸载。
		Trojan/Android.qctoMonitora[prv,rmt,sys]	该应用是一款间谍应用，程序运行会激活设备管理器，监听通话开启通话录音，私自拍照，联网上传用户短信信息、通话记录、通话录音、GPS 位置信息和照片到指定服务器，远程控制，接收指令后删除用户文件，造成用户隐私泄露，影响用户使用，建议立即卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Ubuntu 本地提权漏洞（CVE-2017-16995）	BPF（Berkeley Packet Filter）是一个用于过滤（filter）网络报文（packet）的架构，其中著名的 tcpdump、wireshark 都使用到了它。而 eBPF 就是 BPF 的一种扩展。然而在 Linux 内核实现中，存在一种绕过操作可以导致本地提权。
	较为活跃样本	Trojan[Backdoor]/Win32.Daniel	该病毒家族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。
		Trojan[PSW]/Win32.Ohalf	该病毒家族是一种密码窃取类程序。该病毒家族样本运行后会窃取用户登录凭证及其他信息。
		Trojan[IM]/Win32.EvilDoer	该病毒家族是一种通过 IM 传播的木马程序。该家族样本通过即时通讯程序传播，运行后可能窃取用户信息并造成其他伤害。
		Trojan[Proxy]/Win32.Webjoi	该病毒是一种实现代理功能的木马，攻击者的机器隐藏在代理服务器中，可以执行匿名的活动和攻击，当进行网络溯源时，很难定位到攻击者。

神经进化将推动人工智能发展到一个新的水平

James Kobielus / 文　安天技术公益翻译组 / 译

开发人工智能（AI）系统的下一步是自动化神经网络架构搜索。

进化是创造这些词背后的智慧的历史过程。它也负责产生读者用来掌握文字表达的内容的神经联系。

任何开发“通用人工智能”的努力都必须在一定程度上重演神经网络形成并与周围世界相适应的进化过程。AI 研究人员多年来一直在开发更复杂的“神经进化”方法。现在看来，已经到了大规模进入商业化 AI 主流的时候了。（译者注：强人工智能 [Strong AI] 或通用人工智能 [Artificial General Intelligence] 是具备与人类同等智慧、或超越人类的人工智能，能表现正常人类所具有的所有智能行为。）

随着 AI 成为机器人技术的推动力量，越来越多的开发人员正在探索替代方法来训练机器人掌握近乎无尽的环境任务。对于可以训练机器人像人类一样走路，像海豚一样游泳，像长臂猿一样在树上摆动，像蝙蝠一样在空中敏捷飞行的方法，他们都有着新的兴趣。正如我在一篇文章中所指出的那样，机器人革命激发了 AI 研究人员扩大智能范围，以涵盖任何能够使任何实体在某些环境中探索、开发、适应和生存的先天能力。

在这个新时代，我们看到更多的研究专注于进化算法，这些算法旨在帮助神经网络通过反复试验训练场景自动演化其内部结构和联系。从更广泛的角度来看，关于“神经机器人学”的商业和研究重点正在加强，此外还有强化学习、具身认知、群体智能和多目标决策等重叠领域。（译者注：Reinforcement learning，强

化学习，是一种重要的机器学习方法，又称再励学习、评价学习。强化学习是指从环境状态到动作映射的学习，以使动作从环境中获得的累积奖赏值最大。Embodiedcognition，具身认知，也称“具体化”[embodiment]，是心理学中一个新兴的研究领域。具身认知理论主要指生理体验与心理状态之间有着强烈的联系。生理体验“激活”心理感觉，反之亦然。Swarm intelligence，群体智能，这个概念来自对自然界中昆虫群体的观察，群居性生物通过协作表现出的宏观智能行为特征被称为群体智能。Multi-objective decision making，多目标决策，是指对多个相互矛盾的目标进行科学、合理的选优，然后作出决策。）

正如肯尼思·斯丹利（Kenneth O. Stanley）在这篇引人入胜的文章中指出的那样，开发人员越来越需要复杂的技术来加速神经网络结构优化，这促进了神经进化和深度强化学习领域之间的融合。正如他所指出的，OpenAI 的研究人员开发了一种神经进化方法，该方法可以提高传统深层强化学习技术在各种训练任务中的表现。通过这种方法（采用神经网络架构，并简单地调整人造神经元之间的权重），研究人员可以远远超出 AI 训练的传统焦点，并使用模拟的“自然选择”通过迭代来演变架构本身。

在斯丹利的文章中，他提出了神经进化可能很快成为每个实践数据科学家的 DevOps 工具包的标准功能。他讨论了一种假设情景：迭代生成、测试并选择替代神经网络架构并将其选入机器人仿真实验室。

斯丹利称，鉴于 GPU 的可用性和性价比以及云中其他 AI 优化的硬件处理能力稳步提高，这种场景对于主流开发人员来说越来越可行。他表示，像传统的深度学习一样，“神经进化”也可以从大量硬件投资中受益。与所有进化算法一样，神经进化的优势在于一组人工神经网络可以并行处理。如果有 100 个人工神经网络和 100 个处理器，则可以同时评估所有这些网络，所需的时间与评估单个网络相同。这种加速可以从根本上扩展该方法的潜在应用。

当然，没有人声称神经进化是一个成熟的领域，或者这种 AI 训练方法被广泛部署在生产环境中。然而，显然这些进化神经网络架构优化技术将在未来 3 到 5 年内开始进入“自动化机器学习”方法的主流。正如我在最近的 Wikibon 报告中所说的，为新一代开发人员提供的自动化工具日益增多，这些开发人员会将机器学习、深度学习和其他 AI 功能部署到生产应用程序中。

自动化神经网络架构搜索进入 AI 开发人员工具链只是一个时间问题。届时，它将补充已经存在的自动化特征工程、算法选择和模型训练功能。

原文名称	Neuroevolution Will Push AI Development to the Next Level
作者简介	James Kobielus。James Kobielus 是 Wikibon 数据科学、深度学习和应用程序开发领域的首席分析师。
原文信息	2018 年 3 月 30 日发布于 InformationWeek 原文地址 https://www.informationweek.com/author-bio.asp?author_id=648
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《利用 Flash 0day 漏洞传播的勒索软件“Hermes”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发现一例通过利用 Flash 0day 漏洞传播的勒索软件，名为“Hermes”。该勒索软件其实已经在很久之前就出现了，此次事件中所使用的版本是 2.1。

在 1 月底，韩国紧急响应小组（KrCERT）发布了针对有针对性攻击的零日 Flash Player 的消息。该漏洞（CVE-2018-4878）存在于 Flash Player 28.0.0.137 及更高版本中，是通过包含嵌入式 Flash 漏洞的恶意 Office 文档分发的。在公开发布几周后，垃圾邮件活动已经开始推出含有最新漏洞的恶意 Word 文档。此次事件，“Hermes”使用漏洞攻击工具包 GreenFlash Sundown 并利用该 Flash 漏洞传播自身。

勒索软件将自身复制到 %TEMP% 下，重命名为 svchosta.exe，然后删除初始样本。衍生文件“PUBLIC”包含一个带有 RSA 公钥的代码段。值得注意的是，该密钥在每次运行中都是唯一的，因此，每个受害者都会生成 RSA 密钥对。另一个文件是名为 UNIQUE_ID_DO_NOT_REMOVE 的加密数据块。它是一个包含加密 RSA 私钥的代码段，对受害者是唯一的。同一个文件夹还包含警告信息。当加密完成时，警告信息弹出。该信息文件采用 HTML 格式，名为 DECRYPT_INFORMATION.html。有趣的是，根据活动情况，在一些样本中，作者使用 BitMessage 与受害者进行交流。在每次系统启动时，它都会检查新的未加密文件并尝试对其进行加密。

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恶意代码的检出。

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、数字证书鉴定器、文件元数据分析鉴定器、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勒索软件。

◆ 概要信息

文件名	bcb96251c3e747c0deabadfecc4e0ca4f56ca30f8985cae807ca2ff29099d818
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	42 KB
MD5	237EEE069C1DF7B69CEE2CC63DEE24E6
病毒类型	勒索软件
恶意判定 / 病毒名称	VCS/Instruction.JunkCode
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	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。
编译指令	含花指令，并且非已知壳	对抗病毒分析人员分析。花指令即在程序真正执行前增加一些无用指令，误导病毒分析人员，逃避分析。
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。

◆ 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	192.168.122.51	68
192.168.122.51	137	192.168.122.255	137
192.168.122.51	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.51	1025
192.168.122.51	123	52.168.138.145	123
52.168.138.145	123	192.168.122.51	123
192.168.122.51	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	237eee069c1df7b69cee2cc63dee24e6	N/A	N/A