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 05 日 (总第 125 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

第十四届安天“奥斯卡”揭晓

2018 年春节前，代表安天年度最高荣誉的第十四届安天“奥斯卡”在安天总部所在地冰城哈尔滨揭晓。

安天“奥斯卡”始创于 2004 年，旨在表彰上一年度对网络安全事业和发展做出重大贡献的集体、个人、产品、项目、技术与活动，是安天内部唯一的官方颁奖典礼，代表安天最高的年度荣誉。本届安天“奥斯卡”设有五大类、共十五个奖项，对多个团队及个人进行了表彰。

技术创新，永不止步

习总书记在十九大报告中强调，要“加快建设创新型国家。创新是引领发展的第一动力，是建设现代化经济体系的战略支撑。”安天是视自主创新为灵魂的团队，创业十八年来，围绕威胁检测引擎、安全分析支撑平台、端点安全、流量安全、态势感知和威胁情报等领域形成了核心技术布局。

在本届安天“奥斯卡”上，“面向未知勒索软件的防御技术”项目获得**“最佳技术创新奖”**，勒索软件已经成为影响最广泛的安全威胁之一，2017 年不仅有震惊全球的“魔窟”（WannaCry）蠕虫，更有把勒索数据加密行为转化为针对基础设施攻击“战斗部”的伪必加攻击（notPetya）。**2015 年，安天内部成立了“面向未知勒索软件的主动防御技术”项目组，抓住勒索软件将进行批量文件操作或磁盘 IO 的特点，对主防点做了大量的改进。大大增强了安天智甲对勒索软件行为的拦截和识别率。在 2017 年持续跟进测试的几百个勒索软件中，在不挂接病毒库，仅仅依靠主动防御的情况下，防御成功率超过 95%。**值得一提的是，在安天内部举行的多次红蓝对抗中，勒索防护成为了唯一一次红军（防御方）取得胜利的演训科目。这是安天内部审核极为严格的奖项，多半授予有一定理论价值或算法优化类的成果，历史上多次空缺。这是安天“奥斯卡”建立实施多年来端点主防技术首次获奖，展现了安天团队在第三次创业中从单纯追求技术创新到以达成客户有效防护价值为核心的转变。

安天“奥斯卡”的另一项重量奖是**“最佳工程创新奖”，安天移动安全公司的“Section 9 网络安全情报大数据分析平台”荣获此奖项。Section 9 是安天威胁情报系统的第二版本，是安天赛博超脑系统的重要子系统，是取证、分析、溯源的利器，该平台基于敏捷大数据架构，建立分析模型、数据模型的动态组合机制，实现安全数据业务化关联，帮助分析师全面提高情报分析及决策能力，使数据达成安全价值得以最大化体现。**

安天 Section9 网络安全情报大数据分析平台

安天在态势感知系统的开发中，提出了“以资产保障为核心视角，以威胁认知为基本方法的思路”，为此安天安全可视化研发中心于 2015 年起开始研发资产可视化组件，用以服务于安天的态势感知和网络靶场系统，实现可视、交互的资产信誉评价和威胁认知，充分了解资产和威胁的关联，评价威胁对资产所造成的后果和风险。该组件连续三年获得提名，但前两年始终因和态势感知系统未达成有效的价值融合而未获奖。2017 年，该组件因在安天某重点态势感知项目和网络靶场项目中获得好评，因此在本届安天“奥斯卡”上，该组件获评“最佳形态表现奖”。

安天极为重视知识产权的积累和保护，凭借多年的积累和投入，成功成为国家知识产权优势企业和省级专利示范企业，并且首批通过了《企业知识产权管理规范》国家标准认证。2017 年底，安天获评国家知识产权示范企业，是该批唯一一家网络安全企业。**截至 2017 年 12 月 31 日，安天已向国家知识产权局提交专利申请 777 项，已获授权专利 200 项。**其中，反病毒引擎和病毒处置技术专利获得了中国第十七届中国专利优秀奖。安天专利组获评本届安天“奥斯卡”“最佳运作奖”。

应急响应，奋斗一线

安天始终站在应对安全威胁的第一线，坚持“第一时间启动，同时应对两线威胁，三系统联动，四作业面协同”的响应分析能力建设思想，在每次重大威胁事件中都能看到安天的身影。

2017 年 5 月 12 日，全球爆发大规模“魔窟”（WannaCry）勒索软件感染事件，安天在第一时间启动了“A 级信息安全灾难”应急响应，第一时间上报主管部门，第一时间到达用户现场，第一时间发布深度报告、免疫工具和专杀工具、解密工具等，向公众发布“周一开机指南”和针对用户的高频问题进行回复的 FAQ(1/2/3)。

本次应急响应工作，是安天历史上规模最大的多部门联合的重大应急响应工作，持续时间长达十余天，体现出安天在重大网络安全威胁面前“召之即来、来之能战、战则必胜”的彪悍风格。在事件响应速度、样本分析深度、应急文档和工具

（后续内容转第三版）

每周安全事件

类 型	内 容
中文标题	英特尔发布 BROADWELL 和 HASWELL 芯片的更新版 SPECTRE 修复程序
英文标题	INTEL RELEASES UPDATED SPECTRE FIXES FOR BROADWELL AND HASWELL CHIPS
作者及单位	Lindsey O'Donnell
内容概述	英特尔发布了更新的微代码，以帮助保护 Broadwell 和 Haswell 芯片免受 Spectre Variant 2 安全漏洞攻击。 根据英特尔的文件，包括 Broadwell Xeon E3，Broadwell U/Y，Haswell H，S 和 Haswell Xeon E3 平台在内的一系列旧处理器现在已经修复并可供硬件合作伙伴使用。 Spectre 和 Meltdown 缺陷在服务器和桌面处理器中占据了三个侧向通道分析安全问题的变体，可能会让黑客访问用户的受保护数据。破坏了应用程序访问任意系统内存的机制，而 Spectre 欺骗其他应用程序访问其内存中的任意位置。 Google Project Zero 在 1 月初首次披露了这些安全缺陷，影响了市场上的一系列处理器，其中包括来自英特尔、ARM 和 AMD 的处理器。最初的解决 Spectre 和 Meltdown 漏洞的修补程序是在 1 月份发布的。
链接地址	https://threatpost.com/intel-releases-updated-spectre-fixes-for-broadwell-and-haswell-chips/130144/

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.ADBMiner.a[rog]	该应用程序运行后会加载恶意挖矿脚本，影响用户手机正常使用，建议卸载。（威胁等级中）
		Trojan/Android.FakeCJWG.a[fra]	该应用程序伪装绝地求生类手游的外挂工具，诱导用户付费使用，本身无实际功能，会造成用户资费损失，建议不要使用。（威胁等级中）
		Trojan/Android.EmuSpy.a[rmt,exp,spy]	该应用程序包含恶意模拟器插件，植入后门，会通过远程指令执行发送短信、打电话、发邮件、下载安装未知应用等行为，造成用户资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.Macaw.a[exp,rog]	该应用程序包含风险代码，安装后无图标，后台拦截短信且私自发送短信，造成用户资费损耗，建议卸载。（威胁等级高）
		RiskWare/Android.InstaFollower.a[fra]	该应用程序伪装 instagram 添加关注量的工具，运行访问指定网址，本身无实际功能，请谨慎使用，避免造成资费损失和账号信息泄露。（威胁等级低）
	较为活跃的样本	Trojan/Android.FakeSystem.ae[exp,rog]	该应用程序伪装成系统应用，运行后联网获取下载配置信息，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.gnway.b[prv,rmt,spy]	该应用程序伪装成正常应用，运行隐藏图标，加载恶意网页界面，内嵌远控代码，会根据远程指令上传用户短信、彩信、联系人等隐私信息，还会执行录音、设置锁屏密码等危险行为，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.JsLocker.b[prv,rog,lck]	该应用程序伪装色情应用，运行后隐藏图标，请求激活设备管理器，上传手机设备信息、手机联系人信息，置顶界面显示用户通讯录、照片、位置等隐私信息，勒索用户付费解锁，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.JsMiner.c[exp,rog]	该应用程序被植入恶意代码，运行后执行隐式货币挖矿脚本，会消耗手机性能、减短电池寿命、消耗手机流量，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	微软 Office 公式编辑器被曝出远程代码执行漏洞（CVE-2018-0802）	Microsoft Office 软件中被曝出远程代码执行漏洞（CVE-2018-0802），攻击者可以利用此漏洞，在当前登录用户的上下文中执行任意代码。失败的攻击尝试可能会引发 DoS 攻击，全部版本受影响。（威胁等级高）
	较为活跃样本	Trojan[Rootkit]/Win32.Crypt	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后可以下载并执行其他文件，连接远程服务器发送自身信息，关闭系统防火墙，有一定威胁。（威胁等级高）
		Trojan/Win32.Inject	此威胁是一种木马类程序。该家族将自身以某种方式注入到其它进程（避免用户和杀毒软件感知、清除）中，隐藏自身，并在后台执行恶意行为。因此该病毒家族（Inject）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	此威胁是一种木马类程序。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）

覆盖广度等方面获得了业内的广泛认可。因此，本届安天“奥斯卡”向参与“魔窟”（WannaCry）应急响应工作的核心成员颁发了“最佳分析与响应行动奖”。

此次应急事件中，安天发布的蠕虫勒索软件免疫工具对“魔窟”（WannaCry）的感染传播途径进行了有效阻断，实现了主机免疫功能。该工具被 CNCERT、网信办、公安部等监管部门推荐使用。随后，应国家相关部门要求，安天工程师们连夜奋战，基于国际研究成果在第一时间开发出图形化蠕虫勒索软件解密工具，可有效获取内存秘钥，对被加密的文件进行解密。为此，本届安天“奥斯卡”“最佳公益 / 开源 / 免费工具奖”授予了安天 WannaCry 系列处置工具。

蠕虫式勒索软件 WannaCry 免疫工具（左图）和文件解密工具（右图）

值得一提的是，2017 年**安天以总分第一名的成绩，第五次蝉联获得“国家级网络安全应急服务支撑单位”资质**。

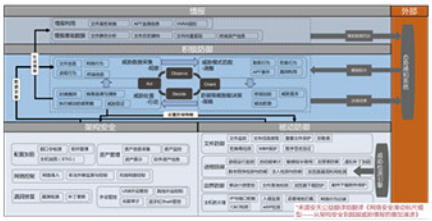
宁缺毋滥 面向实战

安天“奥斯卡”的重磅奖项“最佳产品奖”，今年以零提名空缺。这是安天评价最苛刻严格的奖项，在安天“奥斯卡”历史上，该奖项曾十二年空缺，仅有获得中国厂商首个权威国际奖项的 AVL SDK 移动反病毒引擎曾获得该奖项。

实战化是安天对产品价值的自我要求。本次安天“奥斯卡”“最佳文案奖”授予了安天技术报告《**披坚执锐决战终端**》的 PPT 演示文案。

不久前结束的“第五届安天网络安全冬训营”，以“敌情想定是前提，网络安全实战化”为主题，聚焦有效的敌情想定，面向真实的安全威胁，以期通过“实战化”的网络安全防护要求，为用户实现有效的安全价值。

端是安全之本。在此次冬训营上，**安天端点安全产品中心的专家发表了题为《披坚执锐决战终端》的演讲，该议题主要介绍终端面临的安全和应对之道，将终端安全产品的防御体系同滑动标尺模型进行了有机结合，阐述了安天网络安全实战化和终端有效防护的安全理念**，故本届安天“奥斯卡”将“最佳文案奖”授予该议题的核心参与人员。



基于滑动标尺模型的终端防御体系

服务客户 追求卓越

安天以“奋斗者公司、工程师文化、客户安全价值信仰”为企业基石，秉承“正直、彪悍、专业、协作”的团队风格，在经营发展中始终坚持“不做与反病毒厂商价值观相违背的事情”、“以网络安全为公器，君子不欺暗室”的企业底线，正是这种严谨而踏实的文化氛围，孕育出了一批具有“工匠精神”的基层员工，兢兢业业奋斗在各自的工作岗位上，打造了安天核心技术及实战化产品。在本届安天“奥斯卡”上，共有 38 位在 2017 年度表现突出的基层员工获评“优秀员工”，另**有 3 位新员工中的佼佼者获得个人奖中的特殊荣誉——“最佳新人”奖，安天历年的最佳新人奖都是安天的明日之星，其中包括安天 CTO 潘宣辰**。

在安天第三次创业的转型发展阶段，对组织能力提出了更高的要求。因此尽管有三支团队获得了最佳团队奖提名，但最终本奖项空缺。为此，安天总裁胡忠华表示：“不是这些被提名团队不够优秀，而是公司有更高的追求，对团队有更高的要求。我相信，明年这个时候，我们一定有团队获此殊荣。”

“服务客户，解决问题；应对威胁，保障价值”是安天对产品的价值认识。为表彰在技术、产品、支持、管理等工作中为网络安全事业发展、为客户做出卓越贡献的团队或个人，本届安天“奥斯卡”第一次设立了“卓越成就奖”，此奖项是目前安天最重要的奖项，获奖团队是“AVL SDK 移动引擎团队”！

安天的移动反病毒引擎为用户提供移动终端恶意代码检测能力，目前已为超过 10 亿部智能设备提供安全防护，该引擎亦为全球首个获得 AV-TEST 年度奖项的中国产品，并在 2017 年度的 AV-TEST 测试中依旧保持 4 次双百，2 次单百的好成绩。

正在国外出差的安天集团 CTO 兼安天移动安全公司 CEO 潘宣辰在发来的获奖感言中写道：“2014 年 AV-TEST 获得年度奖项，2015 年保护千万量级终端，2016 年上亿，2017 年终于实现包括华为在内国内 80% 以上手机厂商 OEM 合作，覆盖 10 亿终端，这个奖项并不是一蹴而就的，是 2010 年以来安天第二次创业不懈坚持，2015 年以来一个脚步一个台阶所造就的。这份成就源自安天创业十八年以来的点滴积累，但这个奖项，它真正意义不是过去，而是未来。我们从跟跑比自己历史长十余年的 Big AV（超级反病毒企业，编者注），到实现移动威胁检测的领跑，昭示安天人面对新的挑战突破自我、跃迁格局信念，我们有昨天的成就，有明天的突破，有后天的新的胜利。”

安天创始人、首席技术架构师肖新光对奖项做了点评，他说“这一个奖项是对安天围绕移动安全检测引擎第二次创业的阶段性总结，也告知我们荣誉属于历史，新的奋斗，才能创造新的未来。网络安全产业正在走向大工程平台支撑下的智力密集型 + 人力规模型转变，安天正在从传统安全上游企业，向具备整体解决体系的规模型能力厂商转变。面对日趋复杂的政企安全场景、面对日趋迫切的国家安全需求，我们任重道远，我们将建立新的功勋。”

新时代、新征程中，安天将继续深入学习践行党的十九大精神，以“国家队”的坚毅信念匹配总书记的要求和嘱托，不忘创业的初心，不负使命重托，以敌情想定为前提，达成产品与解决方案的“实战化”价值。安天，始终在路上！

安天发布《“蜻蜓二代”恶意代码分析报告》

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，“蜻蜓二代”恶意代码开始活跃，该样本能够感染系统并常驻于系统，并且还具有窃密文件回传、远程执行任意命令、下载扩展组件执行等功能。

该样本运行后会检测当前执行文件是否以 STService 的名称进行操作。若不是，则将样本复制到 %appdata%，利用 COM 接口在开始菜单的启动文件夹下创建快捷方式来实现自启动，修改文件时间，将文件属性修改为系统隐藏，然后以“ST Service Scheduling”为参数启动 STService.exe。若当前执行文件路径是 \STService\STService.exe，则循环创建 320 个线程，解密配置信息并与远程地址通信。样本会连接默认 C&C：37.1.202.26，向其提交计算机的基本信息并且获取控制命令，根据计算机信息构造数据包。恶意代码会从 .jpg、.png 以及 .gif 中随机选取作为上传服务器目标路径，然后加密根据计算机基本信息拼接成的字符串，通过 POST 请求回传。样本会根据响应的控制指令，执行相应的操作。样本会判断响应的数据中是否含有数据 uE4GMN，若含有，说明上线成功，然后删除 status_svr.txt 文件，否则说明上线失败。若上线失败，则判断状态标志文件“%APPDATA%\STService\status_svr.txt”是否存在，如果该文件存在，则使用备用 C&C（37.1.219.31）进行上线和控制命令的获取。

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、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、智能学习鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	1560f68403c5a41e96b28d3f882de7f1
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	76 KB
MD5	1560F68403C5A41E96B28D3F882DE7F1
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Kryptik
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	行为描述	危险等级
通过设置为系统属性隐藏文件	★★★★	延时	★★★

◆ 常见行为

填充导入表（疑似壳）	★★
获取主机用户名称	★
打开自身进程文件	★
释放 PE 文件	★
复制自身文件	★★
篡改系统文件创建时间	★★
创建特定窗体	★
获取驱动器类型	★
获取计算机名称	★
请求加载驱动的权限	★
获取系统版本	★★
设置自启动项	★★
.....	.....

◆ 监控预警

PID	创建
1224	C:\Documents and Settings\Administrator\Local Settings\Application Data\STService\STService.exe
1136	wuauclt.exe