安天发布《JAVA-VBS 联合木马样本分析报告》

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种将 java 和 vbs 结合起来，使用户感染 Adwind 远控木马和 Houdini VBS 蠕虫的新型病毒。

这种木马是一个 .jar 文件，通过钓鱼邮件的附件进行传播。当木马运行后，首先会搜索资源节，在用户目录释放一个 vbs 脚本，这个脚本中包含一大段 Base64 编码的数据。这段数据经过解码后，会在 %appdata% 目录下转换生成 ntfsmgr.jar。ntfsmgr.jar 的主要作用是在 %temp% 目录下释放一个随机命名的 .class 文件，该文件是 Adwind 远控的真正后门，它会记录用户按键、修改和删除文件、下载执行其他恶意软件、屏幕截图、访问摄像头、控制鼠标键盘等等。另外，先前释放的 vbs 脚本除了让用户感染 Adwind 木马外，还会在 %appdata% 下释放另一个随机命名的 vbs 脚本，该脚本会将自身解码为 Houdini VBS 蠕虫病毒，该病毒可以使攻击者在用户机器上下载并执行文件、运行指令、上传文件、删除文件或文件夹、终止进程等。在最近的恶意活动中我们发现，攻击者为了提高成功率，常常会将两种功能相似的恶意软件结合起来使用。

安天 CERT 提醒广大政企客户，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。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。

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 BD 静态分析鉴定器、YARA 自定义鉴定器、文件来源信息鉴定器、文件元数据鉴定器、反病毒引擎鉴定器、聚类分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	07cb6297b47c007aab43311fcfa9976158b4149961911f42d96783afc517226a
文件类型	
大小	636 KB
MD5	20081DC01818031C6E09CE9A6ABB21A7
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[VB]/Vbs.AYC
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=B855B1B7B59668AD991CF0501E4FF4CB

◆ 处置建议

安天 IEP 威胁防御系统	
时间	大约需要 30 分钟
添加私有云黑名单	进入文件云鉴定页面，找到 MD5 为“20081DC01818031C6E09CE9A6ABB21A7”的文件，将该文件加入黑名单。
评估威胁在网内的分布情况	在文件云鉴定页面，找到 MD5 为“20081DC01818031C6E09CE9A6ABB21A7”的文件，查看该文件在分布在哪些终端。 对相关文件名称进行文件追溯，通常您将在 5 ～ 10 分钟内获得您所有在线终端的同名文件信息作为参考。
进行定点清除	您可以在“安天 IEP 威胁防御系统”的首页，找到您需要处置的黑文件，进行定点清除。 您也可以在“文件追溯”的报告结果中找到您需要处置的黑文件，进行定点清除。

◆ 文件元数据分析

描述	值
File Size	636 kB
File Type	ZIP
MIME Type	application/zip
Zip Required Version	20
Zip Bit Flag	0
Zip Compression	Deflated
Zip Modify Date	2018:11:09 09:06:06
Zip CRC	0x67709c88
.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 03 月 25 日 (总第 176 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安全引擎安天造：超两成有效移动杀毒软件采用安天反病毒引擎

2019 年 3 月 12 日，世界知名测评机构 AV-Comparatives 发布了其对谷歌官方应用商店（Google Play）上架的全球 250 款杀毒软件防护能力的测评报告，旨在帮助广大用户在病毒横行的 Android 平台上遴选出具有有效防护能力的杀毒软件，为大众在选择杀毒软件时提供官方参考。而报告中指出，大约三分之二的安卓杀毒软件都不能实现广告宣传中的杀毒功能，其病毒检出率竟低于 30%，根本无法为用户提供有效防护。造成此现象的主要原因是一些开发者在移动威胁逐年增长的大环境下，追逐移动互联网模式和广告利益，通过开发虚假安全功能的软件欺骗用户，以牟取流量利益，使得虚假杀毒产品逐渐泛滥。

AVC 官网公布的本期检出率超过 85% 的杀毒产品

在此次测试中安天（Antiy）和另一家国内厂商腾讯，与卡巴斯基、赛门铁克等国际厂商均取得了检出率 100% 的满分成绩。值得一提的是，在检出率超过 85% 的有效杀毒软件中，有超过两成采用了安天反病毒引擎 *。充分证明了安天在反恶意代码和移动安全领域的重要的基础地位。

*注：安天为各客户提供的引擎能力是一致的，但因厂商更新频率设定和默认检测深度策略不同，会导致检出率有一定差异。

安天安全引擎持续演进以应对不同时代威胁

反病毒引擎作为威胁检测对抗的核心技术模块，其能力积累并非短时间内可以达成，需要多年持续大量的技术研发投入和安全运维投入。国际知名反病毒企业基本是从上世纪 80 年代后期就开始了反病毒引擎的研发。安天从 2000 年选择爬陡坡，开始自主先进反病毒引擎技术的研发，2002 年攻克了在骨干网进行全规则集线速检测的难题，基于恶意代码检测机制会结合到更多场景中的判断，2004 年安天提出细粒度可嵌入引擎理念，实现在 X86、ARM、MIPS（含 Cavium）、PowerPC 等体系架构和各种操作系统平台上的高可移植性，并可基于恶意代码类型、威胁针对性的平台、样本活跃度等情况，针对设备的工作特点、资源、需要过滤的威胁情况进行规则剪裁。

为全面捕获分析威胁，支撑反病毒引擎的持续升级，安天从 2001 年开始规划了 ArrectNET 威胁主动捕获网络，从 2002 年开始发力研发恶意代码自动化分析平台，并于 2004 年基本实现了样本全面自动化分析处理能力。对国际知名厂商在检出率上奋起直追，并在检测速度、可移植性等指标上作出了自己的特点。2006 年起，安天先后将反病毒引擎技术授权给美国等其他发达国家安全厂商使用，成为中国早期实现核心技术授权出口欧美的安全厂商。安天 AVL SDK 反病毒引擎先后获得了科技部创新基金、863 计划和发改委信息安全专项支持。

移动反病毒引擎 8 年发力保持世界领先

为从跟跑、并跑，转入领跑，安天逐渐将布局着眼于信息场景的进步与迭代变化。2010 年，安天移动安全研发中心（安天移动安全公司的前身）在武汉筹建启动，全面发力移动安全。基于安天的基础引擎和支撑体系的传统积累与理念，安天移动安全团队在负责人潘宣辰带领下，研发了 AVL SDK 移动反病毒引擎和安天第二代支撑平台体系。AVL SDK 移动反病毒引擎以深度预处理、多分支冗余检测，提升检测能力，并引入多种信誉和优化方法，提升检测速度。新一代分析支撑体系，可通过分析体系降维分析工程师工作难度、将分析工程师的经验快速转化为平台系统能力的方法，充分发挥人机协同的优势。基于安天第二代支撑平台，安天逐步建立起了赛博超脑后端支撑体系。

安天 AVL SDK 移动反病毒引擎曾以全年最高平均检出率荣获 AV-TEST“2013 年移动设备最佳防护”奖项，并获得 AV-Comparatives 2015 全年 2 次测试皆为 100% 检出率的领先成绩，以及 AV-TEST2018 全年 6 次双百成绩，领跑全球移动恶意代码检测。


国际主流安全厂商 AVT 测评成绩排行

作为全球重要的基础设施赋能方，安天一直坚持将安全能力和反病毒引擎面向合作伙伴开放。目前中国前十名防火墙厂商有一半使用安天网络侧反病毒引擎，安天移动安全与华为、高通、OPPO、vivo、

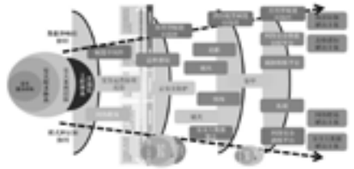
（下接第二版）

（上接第一版）

小米、银联、猎豹、APUS 等全球数百家知名企业合作，为全球超过 15 亿移动智能终端用户的安全保驾护航。

下一代安全智能引擎安天造

面对威胁的演进变化，安天提出了下一代威胁检测引擎的理念，基于面向高级威胁、体系化攻击，单点安全环节均会被绕过的特点。安天将反病毒引擎从单一的检测识别单元，提升为封装检测识别、向量拆解、关联判断的复合安全中间件。通过全格式识别、全向量解析，使反病毒引擎不仅可以输出判定结果，也为产品和态势感知平台体系输出基础静态向量数据以支撑分析研判、威胁关联追溯、客户自建



安天实战化产品图谱

深度普查和处置规则等。

随着能力全面的发展提升，安天逐渐在一些重要客户安全防御的场景中担当协助规划、整体赋能的主责，安天集团层面的研发重心也逐渐转入到实战化运行的战术型态势感知平台中。反病毒引擎也从安天的核心能力，转发为基础支撑性技术。安天赛博超脑体系，已经从安天后端自动化分析体系，进一步承担起威胁情报赋能平台的职能。在全体系架构和各种操作系统的支持上，安天还专门根据各种国产环境优化了引擎版本。

在坚持引领恶意代码检测对抗优势技术能力的基础上，安天正在走出反恶意代码方法路径依赖，向全面体系化能力成长。安天集团已经向客户承诺，到 6 月 30 日，安天全线政企安全产品的事件输出，将全面采用新的分类命名系统，双标支持 ATT&CK 与 NSA/CSS 威胁框架，恶意代码名称将仅作为标签出现。随着安天的产品和态势感知体系在更多客户落地，安天核心引擎能力也会在客户场景中创造更多的支撑价值。

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

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.FakeBank.u[prv,exp] 2019-03-18	该应用程序伪装银行相关应用，运行后加载网页脚本，诱导用户输入银行相关信息，监听用户短信，私自发送短信。造成用户隐私泄露和经济损失，建议卸载。（威胁等级高）
		Trojan/Android.OrderSpy.a[prv,exp,rmt,spy] 2019-03-19	该应用程序安装后无图标显示，监听短信，接收短信远程控制，上传用户联系人、短信、通话记录、通话录音等隐私，还会私自拍照上传，发送扣费短信，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.aljasms.a[prv,exp] 2019-03-20	该应用程序包含恶意代码，运行后加载风险网页，会窃取用户通讯录、手机基本信息，监听用户短信，私自发送短信，拨打电话。造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.SexySpy.a[prv]	该应用程序为间谍件，运行后会窃取用户短信、通讯录、通话记录等信息，并上传到远程服务器，造成用户隐私泄露，请立即卸载。（威胁等级中）
		Trojan/Android.fdbox.a[rog,rmt]	该应用程序运行后会请求激活设备管理器，通过接收指定的广播来获取指令，执行对应的操作，根据指令执行获取设备固件信息、控制屏幕锁屏或解锁、设置语言、设置 wifi、设置密码等一系列操作命令，严重影响设备正常使用，建议卸载。（威胁等级中）
		Tool/Android.wiyimi.a[prv]	该应用程序为小枫网络科技团队开发，运行后会启动 root 权限，获取手机型号、号码等相关信息，收集 QQ、微信等的相关数据记录，存在一定的风险，可能会造成用户的隐私泄露，建议谨慎使用，警惕其联网上传数据。（威胁等级低）
		Trojan/Android.InterceptaproSpy.a[prv]	该应用程序伪装系统应用，运行后会隐藏图标，私自上传用户联系人、短信、位置、Whatsapp 聊天信息等隐私，造成用户隐私泄露，请立即卸载。（威胁等级低）
		Trojan/Android.SimBad.a[exp]	该应用程序内嵌恶意广告件，联网获取推广信息，隐藏图标、推送广告、访问推广页面，存在跳转钓鱼界面等安全隐患，会造成用户资费泄露，请卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Excel 安全漏洞 (CVE-2018-8574)	当 Microsoft Excel 软件无法正确处理内存中的对象时，就会触发该漏洞。攻击者必须诱使用户使用 Microsoft Excel 打开经特殊设计的文件，才能利用此漏洞。成功利用此漏洞的攻击者可以在当前用户权限下执行恶意代码。（威胁等级高）
	较为活跃样本	Trojan[Clicker]/JS.Iframe	此威胁是一种使用 JS 脚本语言编写的、可以重定向用户访问网页请求的木马家族。该家族利用了 Internet Explorer 旧版本对特定 MIME 格式处理解析的漏洞并执行恶意行为。该家族样本多为脚本或网页文件，运行后跳转到包含恶意代码的 URL 地址，并利用漏洞下载其他恶意代码到本机运行。该家族也能被用来增加网站的点击量。（威胁等级高）
		Trojan/Win32.Waldek	此威胁是一种运行在 win32 平台下的木马程序。该家族远程监控感染者的计算机，阻止指定服务的运行，收集用户信息并回传。（威胁等级中）
		Trojan[Downloader]/JS.Redirector	此威胁是一种下载类木马程序。该家族样本通过 JS 脚本语言编写，运行后会与指定的远程服务器连接，下载其它的恶意软件到本地运行。（威胁等级中）
		RiskWare[Downloader]/Win32.Walta	此威胁是一种下载广告软件的风险软件类程序。该家族样本运行后，会在电脑中下载恶意程序并运行。该家族会修改注册表、添加启动项，以达到随系统启动的目的。（威胁等级中）
		GrayWare[AdWare]/NSIS.TornTV	此威胁是一种有广告行为的灰色软件类程序。该家族样本使用 NSIS 打包，NSIS（Nullsoft Scriptable Install System）是一个开源的 Windows 系统下安装程序和制作程序。该家族样本通过 NSIS 打包可以捆绑其他恶意代码到用户系统中。该家族伪装成网络电视软件下载器，当程序运行后会在后台连接远程服务器，下载其它恶意软件到本地运行。（威胁等级中）

2019 年 RSA 大会热点议题

Jon Oltsik/ 文　安天技术公益翻译组 / 译

很多安全专家和供应商参加了 2019 年 RSA 大会——他们有充分的理由。

上周，在多雨的旧金山，我与许多网络安全专家一道参加了 RSA 安全大会。以下是我对此次大会的一些印象。

企业领导者参与网络安全问题

曾经，我们希望企业高管能够更多地参与到网络安全中。现在看来，这一愿望已经实现。企业领导者已经明白，数字化转型与网络安全之间存在紧密联系，他们要求首席信息安全官（CISO）提供正确的数据和指标，以便他们能够衡量风险并实施正确的控制措施。但是，静态数据无法衡量诸如网络安全这样的动态环境，而大多数 CISO 只能提供静态数据。鉴于这种情况无法改变，安全专家在 RSA 大会上提出了多种创新性技术。这些技术可以持续量化风险，帮助 CISO 和企业高管制定更好的风险缓解决策。这是朝着正确方向迈出的一大步。

安全技术堆栈的每一层都在发挥作用

还记得几年前，我们被莫斯康会展中心的南北两大双层展厅震惊了。其实，RSA 主办方是用一个展示走廊将两座展厅连在了一起。为什么会有这么多供应商参加 RSA 大会呢？这是因为，受机器学习算法、云资源、自动化、托管服务等的驱动，安全技术堆栈中的每一项技术都在发挥作用。每一家供应商都有可能会带来新理念，但也有一些供应商会带来困惑。相比于流行语和大肆夸张，成功的供应商会投资于用户教育和前沿思想，旨在为现有和潜在客户提供指导和支持。

市场走向集成和平台

在 RSA 大会上，我与一些 CISO 进行了交谈。他们表示，在 2019 年，他们会删减一定比例的供应商和工具，甚至包括一些刚刚启用的供应商和工具。大型网络安全供应商正在利用集成的网络安全技术平台，逐步实现企业许可协议和基于订阅的定价，从而推动这一趋势。许多供应商正在跟踪多产品交易，并鼓励直销和分销商。为了获得成功，供应商可以通过集中管理控制台集成最佳产品，以进行配置管理、策略管理和报告。目前还处于这种转变的早期阶段，没有任何一家大型供应商具有明显的优势。但我预计到 2020 年，将会出现一些领军者。到 2021 年，至少会出现一家价值 50 亿美元的网络安全供应商。

网络安全分析符合云规模

今年初，我曾预测 2019 年将成为云安全分析之年。在 RSA 大会上，Alphabet 和微软公司分别公布了数据安全平台 Chronicle Backstory 和 Azure Sentinel，进一步证实了这一预言。这两者都是“软件即服务”（SaaS）产品，通过整合大量数据、存储、处理等技术来利用云“主场优势”。两家供应商都承认这些是第一版（Rev 1）产品，但它们的发展势头很迅猛。这两款产品也许不会成为同类产品中的领军者，但他们会影响架构和定价现状。

专业托管服务遍布各地

就小供应商来说，他们可以在 RSA 大会上寻找架构师、顾问、设计师和托管服务。很多人把这一趋势等同于企业网络安全技能的短缺——这种观点是对的，但是忽视了一个重要的问题。网络安全技术不断发展，对数据分析、规模、事件响应、风险管理决策等提出了新要求。大多数企业并不具备适应所有变化的先进技术，他们将更多地依赖于第三方的技术。在不久的将来，RSA 大会的关注点将会从产品转向服务。

云安全技术仍然不够成熟

大型企业正在关注云计算技术。但是，相比于云技术创新的速度，他们的安全控制措施与技能仍然有很大的差距，而且这个差距还在不断扩大。因此，虽然企业可能掌握了容器安全技术，但在保护微服务以及它们所依赖的 API 等方面仍然是落后的。这种差距为供应商带来了机会，但仅限于那些了解各种云技术、本地控制以及集中管理技术的供应商。与此同时，服务供应商再次受到关注。

网络安全监控

我很高兴看到网络流量分析（NTA）工具的复兴。有些 NTA 工具基于开源技术，如 Bro/Zeek、Snort 和 Suricata；有些通过机器学习技术来检测异常 / 恶意流量；有些则与端点检测和响应（EDR）工具紧密集成。企业为何要关注网络安全呢？ ESG 公司研究表明，网络安全监控通常是威胁检测的重心。换句话说，安全运营中心（SOC）分析师首先检测到网络上的可疑活动，然后转移到其他地方进行进一步调查。这使得网络成为安全迹象的重要来源。在我看来，部署更现代化的网络安全监控 / 分析工具能够获得巨大的回报，这就是此类工具风靡 RSA 大会的原因。

还有一点需要注意：RSA 与会人员对 MITRE ATT& CK 框架进行了大量的讨论。这很不错！安全行业的每个人似乎都认同该框架的优势。

原文名称	The buzz at RSA 2019 - Cloud security, network security, managed services and more
作者简介	Jon Oltsik。Jon Oltsik 是 ESG 公司首席分析师，也是该公司网络安全服务的创始人。
原文信息	2019 年 3 月 11 日发布于 CSO Online 原文地址 https://www.csoonline.com/article/3363497/the-buzz-at-rsa-2019-cloud-security-network-security-managed-services-and-more.html
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。