安天周观察

主办：安天　2016 年 3 月 14 日（总第 31 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天 RSA 西游记

为了分享在 RSA 的所见所感，安天微信公众号 (Antiylab) 发表了“RSA 西游记”系列专题，下文节选自第五回、第六回内容，完整专题请查看公众号相关文章。

第五回：斗威胁不可空有火眼，驱恶代又怎能无引擎

本回由安天传统引擎部门编写，以一个 AV 引擎开发者的角度，来总结本届 RSA。

◆ Cylance

今年安天比较关注的厂商是 Cylance，号称既不依靠特征码也不依靠云，只靠一个 40M 的未知检测引擎就能够达到很高的检出率。现场观看演示后，我们发现其检测能够定性木马、僵尸网络、敲诈程序等几个基本的分类，但并不能提供准确的家族名称。而且通过讲解，基本可以猜出其实现方式。

这对于我们是一种启发，传统反病毒引擎不仅承担检测判定恶意代码的责任，而且还需要提供精准的病毒命名。但如果这一角色可以通过威胁情报形势来弥补的话，同时其误报也可以进行更多的云端平衡的话，其实可能给反病毒引擎开发者在机器学习和判定方面留下了更多开阔地。Cylance 的思路让人想到螺旋状的创新，但 Cylance 的演示给人一种半成品的感觉，不禁让人感慨，美国用户确实非常包容创新。

◆ FireEye

今年 RSA 确实是忽如一夜春风来，威胁情报百花开。我们观看了卡巴的威胁情报系统，迈克菲的威胁情报交换系统等演示，看起来和安天的态势感知和监控预警系统大同小异。但 FireEye 的技术路线给我们的感觉是与其他传统以恶意代码检测能力为基础的厂商有差异，与新型威胁情报厂商也有不同。其重兵和能力不在载荷上，而是更加看重目标场景和事件的分析能力。同时，FireEye 号称已经拥有万台虚拟机进行样本分析，但其重心依然不是处理更多样本，而是在其中发现高级威胁。

另外，我们发现 FireEye 内置了 Sophos 的检测引擎，可以说这是对国内很有市场的反病毒技术无效论的一个绝妙讽刺。

第六回：五色旗卷风云气象，四方人聚天海灵机

本文作者：Wenster（严绍文，安天企业安全业务线副总经理）

整理本届 RSA 的资料，会让人感觉眼前一片幽蓝。即便是以黄色为主色调的赛门铁克，今年的新 LOGO 也掩映在迷离的蓝色背景里。回望美国 IT 历史，蓝色似乎注定是硅谷的主色调。但展会上也并非一蓝到底，比如卡巴斯基 Kaspersky 的青草绿、Splunk 的命令行 SHELL 黑、WEBROOT 的翡翠绿等等。即便如此，红色在展会上依然不多见。在安天搜集的资料里，以红色为主色的厂商只有三家：FireEye、Fortinet 和趋势。

◆ Fortinet

Fortinet 的展位依然是那辆敞开式的十分抢眼的红色大房车，用各种真实的产品，搭建真实的环境进行模拟。我们分析这辆车象征着救火的消防车，用来寓意 Fortinet 主打的快速 & 安全。

在产品上，Fortinet 的重心还是放在硬件产品的推广上，尤其是侧重网络安全检测的产品，讲解员为我们演示了如 HTML 和脚本上的处理，以展示其当年提出 UTM（统一威胁管理）所沉淀的底蕴。讲解员还向我们介绍了其硬件结构，以 fortiASIC 芯片为核心，通过网络处理器 ASICNP 芯片、内容处理器 ASIC CP 芯片，以及融合芯片 SOC(NP+CP) 实现对不同流量的分解加速功能，并宣称他们已经全面进入了 100G 时代。

◆ 趋势科技

趋势科技的展台被设计成一架红色飞机，机舱、发动机、机翼、航空座椅等一应俱全，很有创意。趋势科技在中国大陆市场之路走的有些一波三折，曾因产品演示选择了某个对中国带有政治敌意的病毒，导致其被踢出中国市场。通过运作重返市场后开始与国内大集成商一同推广政企用户，业务延展十分迅速。在中美关系趋冷的大背景下，趋势又把自己的中国公司卖给亚信，形成了十分受关注的亚信安全，为了配合这个交易达成，甚至迅速撤掉了一个分析“中国铁虎 (Operation Iron Tiger) 发动 APT 攻击”，攻击目标是美国国防承包商的报告。在这些操作中，尽显了东方式的精明。

Cylance 展台

FireEye 展台

上左：splunk 的命令行黑
上右：WEBroot 的绿
下左：蓝的不像赛门铁克的展台
下右：Cyphort 的亮橙也配了蓝色布景

Fortinet 展台


趋势科技展台

每周安全事件

类 型	内 容
中文标题	“透明部落”：针对印度外交、军事实施的间谍行动
英文标题	Operation Transparent Tribe targets Indian diplomats and military
作者及单位	Pierluigi Paganini，Security Affairs
内容概述	近日，研究人员注意到了两起针对在沙特阿拉伯和哈萨克斯坦使馆工作的印度外交官而发起的攻击，并由此发现了一起名为“Operation Transparent Tribe”的网络间谍活动。 据调查，参与攻击的 IP 地址在巴基斯坦，并且攻击显得很复杂。攻击者使用了网络钓鱼和水坑攻击，投放了运行远程访问木马 (RAT)MSIL/Crimson，其可以执行各种数据渗出功能，包括控制便携式摄像机，运行截屏操作以及键盘记录的能力。研究人员称该活动目标的性质和攻击者所使用的方法意味着这是一起具有国家政治性质的攻击活动。
链接地址	http://securityaffairs.co/wordpress/45093/hacking/operation-transparent-tribe.html

每周值得关注的恶意代码信息

经安天检测分析，本周 10 个移动平台和 4 个 PC 平台的恶意代码家族值得关注

平台分类	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	G-Ware/Android.Golem.a[rog，exp，rmt，opc] 2016-03-07	该程序运行后隐藏图标，后台下载恶意文件在用户不知情的情况下远程控制手机启动并运行应用，这些恶意行为会消耗大量的网络数据、电池电量和本地设备资源，造成用户资费损耗的同时还会影响用户的用机体验，建议立即卸载。(威胁等级高)
		Trojan/Android.FakeKakao.a[prv，rmt，opc]2016-03-08	该程序感染正常应用程序，后台运行收集用户短信、联系人、通话记录等信息并通过 ftp 方式上传远程服务器，此外还可以通过短信指令获取用户地理位置信息，造成用户隐私窃取。(威胁等级高)
		Trojan/Android.ygdx.a[pay，crt] 2016-03-09	该类应用运行时会向指定手机号码发送固件信息进行反馈，并会于后台联网获取配置，私自发送付费短信并拦截，给用户带来经济损失。(威胁等级中)
		Trojan/Android.dnote.a[exp，rmt，opc] 2016-03-09	该类应用会联网获取要下载的应用列表，并于后台私自下载安装，给用户造成流量消耗。(威胁等级高)
		Tool/Android.AutoXpos.a[sys，gen] 2016-03-10	该应用自动安装 Xposed 及其插件，并自动勾选重启激活插件的功能，具有极高的权限可能给用户的手机带来损害，建议谨慎使用。(威胁等级低)
	较为活跃的样本	G-Ware/Android.Fakegupdt.ax[rog，exp，gen]	该应用运行后激活设备管理器，隐藏桌面图标，后台推送广告，造成用户资费损耗，建议卸载。(威胁等级中)
		Trojan/Android.qmi.b[pay，fra，crt]	该应用伪装系统程序，运行隐藏图标，联网上传固件信息和指定系统文件，还会发送订阅短信，会给用户造成经济损失，建议及时卸载该程序 (威胁等级中)
		Trojan/Android.Hellospy.a[prv，spy，crt]	该程序安装无图标，可获取用户地理位置信息和联系人信息等并上传远程服务器，并可登录网站后台查看，可能造成用户隐私泄露，建议谨慎使用。(威胁等级中)
		RiskWare/Android.Armour.a[prv，fra，gen]	该应用为一款手机杀毒软件，存在一定的隐私泄漏风险，同时在收费上可能存在不明确的说明信息。(威胁等级低)
		G-Ware/Android.FakeBank.j[prv，exp，crt]	该程序安装运行之后会拦截短信，后台推送广告，造成用户无法正常体验以及流量资费的额外损失，建议不要安装该软件。(威胁等级低)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 内存破坏漏洞 (CVE-2015-1641)(MS15-033)	Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。 当 Office 没有正确处理内存中富文本格式文件时，存在远程代码执行漏洞，攻击者成功利用此漏洞后，可通过构造的文件，在当前用户安全上下文中执行操作。(威胁等级高)
	较为活跃的样本	RiskWare[Downloader]/Win32.AdLoad.oa	此威胁是一种风险软件的木马类程序，可以在未经用户许可的条件下侵入用户系统，并窃取重要数据，安装其他恶意软件后可以使用户的电脑性能变慢。(威胁等级中)
		Trojan[Downloader]/Win32.Banload	此威胁是一种木马类程序，病毒运行后，复制自身到 %system32%\csrss\ 下，连接网络，下载病毒文件，修改注册表，添加启动项，以达到随机启动的目的，该家族下载的文件可以盗取用户银行账号和密码，是基于特定行为来命名的家族。(威胁等级中)
		GrayWare[AdWare]/Win32.Amonetize	此威胁是一种广告行为的广告软件类程序，可以通过安装免费软件捆绑安装到浏览器。安装时可选择自定义安装，在安装过程中捆绑广告软件安装，有可能威胁用户的操作系统。(威胁等级中)

勒索软件首次攻击苹果 OS X 系统

Brian Barrett / 文　安天公益翻译小组 / 译

近期，勒索软件越来越受关注，但是到现在为止，苹果设备没有遭到过勒索软件的攻击。随着 KeRanger 的出现，这一点发生了改变，该应用程序将会在未来几年感染大量的 Mac 用户。

近日，研究人员 Claud Xiao 和 Jin Chen 首次报道了 KeRanger 的存在。他们表示，该勒索软件在 3 月 4 日第一次感染了 OS X 系统的 Transmission BitTorrent 客户端安装程序。虽然他们不知道 Transmission 是怎么被感染的，但他们指出这是一个开源项目。他们在一篇博客里写到：“可能的情况是，Transmission 官方网站被感染了，文件被重新编译的恶意版本所取代，但我们无法证实这种感染是如何发生的。”

更麻烦地是，KeRanger 用有效的证书签名了，这意味着它能够绕过苹果内置的保障措施。目前还不清楚这是如何发生的，安全专家米克 · 海波宁怀疑它只是一个窃取的代码签名证书。海波宁说：“它从官方应用程序厂商的官方网站下载，而且用一个有效的开发证书签名。它是一个勒索木马，旨在访问用户的文件，而非获得 root 权限。”

它并不需要 root 权限，因为它并不想控制你的计算机。相反地，它寻找你最关心的文件，包括照片、电子表格、账单等，从而进行勒索。一旦安装，KeRanger 会蛰伏 3 天，然后开始加密系统上的文档和文件。具体来说，它搜索 300 个不同的扩展名，包括 .doc，.mp3，.jpg 和 .txt 等等。

受害者需要支付 1 个比特币来解密文件，相当于 400 美元多一点。研究人员还指出，KeRanger“正在积极开发中”，它的下一步可能是加密 Time Machine 文件，这样一来，如果你的文件被解密，你就不能简单地调用备份了。

任何在太平洋标准时间 3 月 4 日上午 11 点到 3 月 5 日下午 7 点下载 Transmission 2.90 两个安装程序之一的用户都有可能受到影响。幸运的是，Xiao 和 Chen 指出，有一个方法可以检测是否受到了感染，以下内容取自他们的报告：

1. 使用 Terminal 或 Finder，检查是否存在 /Applications/Transmission.app/Contents/Resources/General.rtf 或 /Volumes/Transmission/Transmission.app/Contents/Resources/General.rtf。如果任何一个存在，Transmission 应用程序就被感染了，建议您删除此版本的 Transmission。

2. 使用 OS X 系统预装的“主动监控”，检查任何名为“kernel_service”的进程是否正在运行。如果是，再一次检查该进程，选择“打开文件和端口”，检查是否存在诸如“/Users//Library/kernel_service”的文件名。如果存在，该进程就是 KeRanger 的主进程。建议您通过“Quit→Force Quit”终止其运行。

3. 完成这些步骤后，我们建议用户检查 ~/Library 目录中是否存在文件“.kernel_pid”，“.kernel_time”，“.kernel_complete”或“kernel_service”，如果存在，建议将其删除。

此外，由于苹果公司已经撤销了有问题的证书，当你试图打开 Transmission 时，系统会警告它可能会有危害。如果系统发出了警告，则应将其删除。

如果你受到了影响，你的损失将达 400 美元之多。该勒索软件设置了 72 小时的时限，从今天下午开始，因此所有受影响的人都应该在周三上午之前了解他们陷入了什么样的麻烦。

海波宁说，更大的问题是，Mac 电脑正式沦为攻击者的目标。很多苹果爱好者可能认为他们的设备具有卓越的病毒防护功能。事实上，一直以来，Mac 计算机占了很小的市场份额，因此不是什么热门目标。同样地，大多数恶意软件从业者将大量的时间和精力用于攻击 Windows 计算机，因此在 Mac 计算机方面不具备核心竞争力。

海波宁说：“这不只是市场份额的问题，也是现有技术的问题。大部分赎金代码团伙对 Windows 平台的所有技术了如指掌，所以对他们来说，攻击其他平台 (无论是 Android 还是 OS X) 都是一种投资。只要他们能够轻松地攻击 Windows 平台，就不太可能去攻击其他平台。”

在 KeRanger 的案例中，可能是一个团伙厌倦了与其他若干团伙争夺同样的 Windows 设备，所以转向了未被开发的市场。如果 KeRanger 获得成功，这可能会很快改变整个攻击现状。即使不成功，不断增长的 OS X 安装数量可能会导致更多的攻击，这一点是无法避免的。

所以，OS X 遭到第一次勒索软件攻击是一个严重的问题。然而，更严重的问题是它将开创一个新局面。

原文名称	Ransomware Strikes Apple's OS X for the First Time
作者简介	Brian Barrett，《连线杂志》的作家和编辑。
原文信息	2016 年 3 月 7 日发布于《连线杂志》 原文地址 http://www.wired.com/2016/03/hack-brief-ransomware-hits-mac-os-x-first-time/
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 CERT 发布《Nimnul 感染式卷土重来》

近日，安天 CERT 发现大量网站感染恶意代码，经分析发现，这是由感染 EXE、DLL、HTML 文件的感染式病毒 Virus/Win32.Nimnul.a 引起的。这个感染式病毒感染系统中的 HTML 文件，感染后的 HTML 被安天检测为：Trojan[Dropper]/VBS.Agent.b。如果受感染系统是网站服务器，其网页都将被该病毒感染；同时，访问了该网页的用户也有可能被该病毒感染，这也是大量网站被感染的一个原因。

被分析的样本为感染式病毒，运行后会感染本地可执行程序 (EXE、DLL)，会感染全盘的网页文件 (HTML、HTM)，将自身写入到它们内部，当运行可执行程序或加载网页文件时，都会运行该病毒。该样本是在正常程序的尾部添加新的节 .rmnet，将程序入口点修改到新增加的节中，通过这种方式进行感染可执行程序。

该样本感染是通过在正常网页文件中写入一段 VBScript 脚本来实现的。这段脚本的功能是将 WriteData 这段内容转为二进制，保存为 svchost.exe 文件，存放到 Temp 目录下，并调用该程序执行。使用 IE 打开被感染的 HTML 文件，会弹出 IE 保护信息栏，点击允许之后，再次弹出安全警告是否允许活动的内容，点击是之后，会弹出警告窗口，是否允许这种交互，点击是，此时，在 Temp 文件夹下就会释放出 svchost.exe 了。所以被感染的系统都会访问这个已经失效的域名：fget-career.com。

Virus/Win32.Nimnul 家族样本在安天病毒库中共有 227 万多的 HASH，最早发现时间是 2010 年 9 月 7 日。据安天 CERT 统计，三天内有 178 个国内网站感染该病毒。因为该感染式病毒感染网页文件，并可以通过网站传播，所以安天 CERT 预测国内仍会有大量网站继续感染此病毒。

木马程序

安天【追影高级持续威胁分析系统】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：

文件被安天防线 7 发现，经由 BD 静态分析鉴定器、美国软件交叉索引 (NSRL) 鉴定器、可交换信息 (EXIF) 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、安全云鉴定器等鉴定分析。

最终依据静态分析鉴定器、动态行为鉴定器、安全云鉴定器将文件判定为木马程序。

该文件具有以下行为：增加 winlogon 自启动项；其他进程写入可疑数据；访问 DNS；填充导入表（疑似壳）；复制自身文件；访问其他进程内存；增加 run 自启动项；创建互斥体 (mutex)；释放 PE 文件；获取驱动器类型；打开自身进程文件。

文件名	d:\program files\thunder network\thunder\program\thunderpreloadsrv.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	55 KB
MD5	FF5E1F27193CE51EEC318714EF038BEF
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Packed]/Win32.Krap
判定依据	安全云

危险行为

行为描述	危险等级	行为描述	危险等级
增加 winlogon 自启动项	★★★	其他进程写入可疑数据	★★★

其他行为

行为描述	危险等级	行为描述	危险等级
访问 DNS	★	填充导入表（疑似壳）	★★
访问其他进程内存	★	复制自身文件	★★
创建互斥体 (mutex)	★	增加 run 自启动项	★
获取驱动器类型	★	释放 PE 文件	★
打开自身进程文件	★		

网络监控

域名	IP
google.com	216.58.199.14
fget-career.com	(null)

进程监控

PID：776	创建：DesktopLayer.exe
	命令行：C:\Program Files\Microsoft\DesktopLayer.exe
PID：1336	创建：iexplore.exe
	命令行：C:\Program Files\Internet Explorer\iexplore.exe

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=FF5E1F27193CE51EEC318714EF038BEF