安天周观察

主办：安天　2016 年 3 月 7 日 (总第 30 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：六进三番赴盛会 审时度势探真经

美国时间 2 月 29 日， RSA 大会在旧金山拉开帷幕，第六次参展的安天依旧是独立出展，重点展示了全域检测引擎能力、深度分析能力、纵深支持能力和高价值情报分享能力。

同时，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，下文节选自专题前四回内容，完整版本请查看公众号相关文章。

安天 RSA 西游记持续更新中……

第一回　六进三番赴盛会，日解两题化玄机

第二回　安全态度尊善果，威胁情报见虚实

第三回　动静结合风险可辨，场景还原威胁现形

第四回　逢故人同道求灵根，会新友乐见变化能

……

名词 or 动词

本届 RSA 大会的主题为“Connect to Protect”——很多国内报道将之简单的翻译为连接保护，较容易产生误解，其实稍加思考，便会发现，RSA 大会近几年的热点和理念其实都是一贯的——联合、分享，“connect”无法当作一个名词，而是继续倡导在智能、情报、各种热点纷至沓来的时候，只有协作联合才能够有效地实施保护。

矛盾 or 欣喜

安天对 RSA2016 的感觉可以说矛盾与欣喜同在，本届大会主题和关注重点不似往常那样鲜明，我们理解，一方面是网络安全继续细分化，议题和涉及企业越来越多，另外是由于 connect 东西越来越多，安全威胁继续泛化，Identity+IOT，threat Intelligence 等都成为本次展会的关键词，企业级场景下厂商明显加强了对应急事件处理和反应的重视，与威胁情报相关的能力的大量出现，也预示着在整体的安全策略中，对威胁情报的理解和应用将会更加丰富，更加专业。

参展 or 围观

作为全球网络安全行业盛会的 RSA 大会，既是一个商展也是一个聚会，既是一个比拼的竞技场也是一个注重情感交流的大 party。在几日的展会中，安天也走访了不少厂商。

◆卡巴斯基，本次参展依托其久负盛名的 KSN(Kaspersky Security Network，卡巴斯基安全网络) 进军威胁情报市场，利用其遍布全球的安装终端采集的信息，数据进入 KSN 网络，从而为整个威胁情报系统提供资源库，可以说，在威胁情报概念尚未进入业界视野之前，卡巴早已在做正确的事情。与其相比，安天也有自己的特色，安天的网络侧检测能力比卡巴起步更早。同时，安天首先选择在移动威胁情报发力，通过 AVL SDK 反病毒引擎移动版形成的终端覆盖能力，形成全球最早的移动安全威胁情报体系。我们也期待与卡巴斯基建立更多的合作，携手应对威胁。

◆ Zimperium，是一家专门做企业级移动安全产品的以色列安全公司，主打为企业级用户提供对抗下一代高级移动威胁的安全防护，同致力于移动互联网安全技术研究及反病毒引擎研发的安天 AVL Team 有着一定的相似性。zimperium 的产品思路创意十足，会首先将攻击场景还原展示给企业，然后再为对方提供解决方案。

将场景还原的方式用在移动安全上，用于可视化的展示，确实是一奇招。移动安全的发展趋势需要我们不断创新思维，安天的下一步将更有针对性的提高跨平台防范策略，并探索与相关企业、行业的合作，共同开发新的安全模式，真正做到 connect to protect。

◆ ThreatQ，作为一匹黑马，刚刚成立不到 2 年，服务就囊括了美国大型零售企业、国防科技部门、世界 500 强企业等企业，在威胁情报领域占稳脚跟。其核心产品是可视化的威胁情报平台，通过从合作伙伴提供、产品的客户端收集、商业机构购买、开源黑名单库等不同渠道，收集威胁情报综合数据，使用大数据等技术来实现对威胁情报的快速响应，快速解除威胁。

目前，安天也将推出新的移动威胁情报平台 AVL Insight，主要用于呈现移动威胁的高价值情报信息；同时通过对移动威胁的全面感知能力和快速分析响应能力，提供应对移动威胁的预警和处置策略。

安天展台

每一年参展，安天都是自己动手布展，体现了安天的工程师文化

安天 RSA2016 小分队


安天代表访问卡巴斯基展台

Zimperium 展台

ThreatQ 展台

每周安全事件

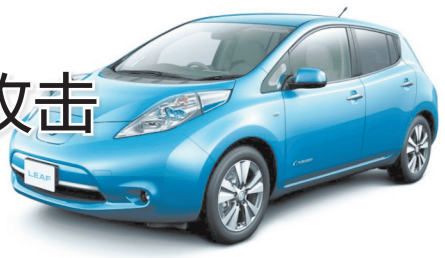
类 型	内 容
中文标题	两家德国医院受到勒索软件攻击，工作面临瘫痪
英文标题	Ransomware attacks paralyzed at least two German hospitals
作者及单位	Pierluigi Paganini，Security Affairs
内容概述	根据德国广播公司的报道，两家德国医院在近日受到了勒索软件的感染。在医院的工作人员注意到系统性能迅速降低，同时还会弹出许多错误的消息后，医院立刻中断了一切工作，让电脑、服务器、电子邮件服务器全部离线，这对医院的工作造成了一定的干扰。随后研究人员发现这种软件会锁住文件，只有给出它要求的赎金后，才能解开被恶意加密的数据，而让系统重新运行需要花费数周的时间。
链接地址	http://securityaffairs.co/wordpress/44824/cyber-crime/ransomware-paralyzed-german-hospitals.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	Trojan/Android.rootstv.a[exp] 2016-02-29	该类应用是针对智能电视的恶意应用，程序运行会利用系统漏洞提权，静默安装未知应用，远程推送应用，造成用户资费消耗。（威胁等级高）
		Trojan/Android.banklock.a[prv，exp] 2016-03-01	该应用伪装成谷歌 Play，运行后激活设备管理器，跳转到钓鱼界面并挟持界面，诱导用户输入付款方式，会造成用户资费损失，建议不要安装。（威胁等级高）
		Trojan/Android.Tesbo.a[exp] 2016-03-01	该应用植入正常应用中，运行后会私自发送短信，会造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.aqyspy.a[prv，fra，spy] 2016-03-02	该应用伪装成正常应用，运行后隐藏图标，后台窃取用户通话记录、录音、短信、彩信等并压缩联网上传；同时存在拦截屏蔽短信，私自拍摄录像，私发短息，静默安装等行为，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Tool/Android.Lacak.a[prv] 2016-03-02	LACAK-A 是一款用于监控家庭成员的程序。运行后台收集位置数据，短信，通话和浏览历史记录上传，建议谨慎使用。（威胁等级低）
	较为活跃的样本	Trojan/Android.SmsSend.it[prv，exp]	该应用程序运行获取用户通讯录信息显示到界面，点击按钮向用户联系人发送指定短信，获取用户短信信息、通讯记录信息上传到指定服务器，造成用户隐私泄露和资费消耗。（威胁等级中）
		Trojan/Android.QQspy.f[prv]	该应用伪装成 qq 应用，程序运行显示伪装的 QQ 登陆界面，诱导用户输入 QQ 账号及密码，获取用户输入的账号密码信息发送到指定邮箱，造成用户 QQ 账号等隐私信息泄露。（威胁等级高）
		Trojan/Android.simplelock.l[rog，sys]	该程序运行隐藏图标，后台调用照相机拍照同时加载指定网页配合进行勒索，建议立即卸载，避免造成资费损耗。（威胁等级中）
		Trojan/Android.Sberik.b[prv，exp，fra]	该应用伪装成 Sberbank 银行应用，程序运行会请求激活设备管理器，联网上传用户设备相关信息，监听短信，获取短信信息上传到指定服务器，获取远程指令执行发送指定短信、删除短信、设置呼叫转移、锁屏等行为，造成用户隐私泄露和资费消耗。（威胁等级中）
		Trojan/Android.InfoStealer.u[prv]	该应用程序运行隐藏图标，后台上传书签、浏览器、位置、短信、电话录音等隐私信息，建议立即卸载，避免隐私泄露。（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 Office Excel 缓冲区溢出漏洞 (CVE-2011-0104)	Microsoft Excel 是 Microsoft Office 组件之一，是流行的电子表格处理软件。Microsoft Excel 中存在缓冲区溢出漏洞，远程攻击者可利用此漏洞以当前用户权限执行任意代码，造成拒绝服务。Microsoft Office Excel 处理特制 Excel 文件的方式中存在一个远程代码执行漏洞。成功利用此漏洞的攻击者便可完全控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。（威胁等级高）
	较为活跃的样本	Trojan/Win32.AntiFW	此威胁是一种木马类程序。运行后会伪装为播放器下载工具，连接网络，下载多个广告软件，主要用来进行推广软件。具有 rootkit 的能力，尝试劫持浏览器、捆绑软件安装或下载软件安装。部分变种安装浏览器插件 (IE-BHO)、修改浏览器主页、搜索设置等。（威胁等级中）
		Worm[Net]/Win32.Allaple	此威胁是一种多线程的多态感染型的网络蠕虫类程序。它能够传播至其他连接了本地网络的计算机中并对特定的远程网站进行拒绝服务攻击。它利用网络共享进行传播，能够在网络中通过发送完整且独立的副本来完成自我复制。（威胁等级中）
		GrayWare[AdWare]/Win32.Amonetize	此威胁是一种广告行为的灰色软件类程序。它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，有可能威胁到操作系统。（威胁等级中）

特洛伊 • 亨特演示日产电动车攻击



Tom Spring / 文　安天公益翻译小组 / 译

近日，研究员特洛伊 • 亨特在一个安全研讨会指出，不安全的 API(应用程序编程接口) 存在风险。当时他并不知道，仅仅几个小时后，他会发现一个 API 漏洞，该漏洞允许攻击者对 20 万辆日产 Leaf 和 eNV200 电动汽车的车载计算机进行远程访问。

亨特在 Threatpost 接受采访时表示：“我们在研讨会上谈到，应用程序有时会错误地获取 API。一名与会者回到酒店房间，15 分钟后来电说，他发现了日产 Leaf 智能手机应用程序的一些可疑之处。”

事实证明，该漏洞允许任何知道日产 Leaf 和 eNV200 车辆识别号码 (VIN) 的人远程访问汽车的温度控制、电池状态和 GPS 日志 (包括汽车行驶的日期、时间和距离)。

这不同于查理 • 米勒和克里斯 • 瓦拉塞克在 2015 年发现的切诺基远程访问漏洞。日产漏洞的特殊之处在于，攻击非常容易实现，任何智能手机都能够远程控制 20 万辆涉事日产汽车中的任何一辆，不管它们在哪里。

随后，日产对 Threatpost 表示，它已将 NissanConnect EV 应用程序下线。一位发言人称，他们正在开发一个新的安全应用程序，但没有透露何时会上线。

亨特说，虽然日产漏洞的范围可能是有限的，但仍会让 Leaf 和 eNV200 车主头疼不已。确定风险的第一个问题是：攻击者能够控制什么？第二个问题是：攻击者能够检索到什么类型的数据？

在 GPS 追踪数据 (包括时间和行驶距离) 方面，大多数车主期望一定程度的隐私。但是，日产漏洞不仅明确侵犯了隐私，还可能会对日产车主造成真正的破坏。

在一个场景中，攻击者能够远程运行加热或冷却系统，耗光电池电量。攻击者也可能会编写一个脚本，每隔 30 秒将空调开关一次，直到无法再运行。“现在，想象一个黑客拥有上千辆汽车的 VIN 码，并运行该脚本。这可能会造成非常严重的损害。” 亨特说。

现在，VIN 码非常容易找到，并可以揭示车辆最近的维修信息。在汽车零售网站 Cars.com 上搜索日产 Leaf，就会显示数百辆汽车及其 VIN 码。知道了日产 Leaf 和 eNV200 汽车 VIN 码的最后 5 位数，就能够利用该漏洞对汽车进行远程访问。

攻击的流程如下：

首先，亨特将日产 NissanConnect EV 应用程序下载到手机上并注册。接下来，他查看应用程序与什么后端服务器通信。期间，他发现，该应用程序通过汽车 VIN 码的最后 5 个号码识别。VIN 数据位于该应用程序向日产做出的 URL 请求中。亨特发现，他能够换出 VIN 码并控制不同的汽车。

但真正让亨特吓了一跳的是，与 NissanConnect EV 应用程序通信的服务器上的 API 不对用户进行验证。任何具有凭证的人都能使用日产应用程序向特定 Leaf 汽车匿名发送请求，打开其温度控制。另一个 URL 请求允许攻击者查看电池寿命，另一个请求则返回 GPS 数据。

事实上，日产 Leaf 车主已经开始关注这一问题。车主们在留言板上抱怨 NissanConnect EV 应用程序的糟糕设计，并寻找解决方法。因为该应用程序既不可靠又麻烦，Leaf 车主试图弄明白如何操纵他们的车辆。“很多沮丧的应用程序用户发现，他们只需要在浏览器中输入一个 URL，就能打开其汽车的加热系统。”亨特说。

当亨特第一次将其发现报告给日产时，日产颇为重视。但是，亨特说，该问题被披露之后，日产给他吃了闭门羹，仍然没有解决问题。几个星期后，亨特指出，客户们逐渐意识到了这一漏洞，他告诉日产他要在自己的网站上发布该研究。

亨特说：“日产没把该问题看得很紧急。最终，我告诉日产，在该漏洞更加广为人知和被滥用之前，我要发布我的研究结果。”直到这时，日产才将涉事应用程序下线了。

实际上，这是一个网络漏洞。在该案例中，该漏洞碰巧能够控制汽车。日产只是没想到有人会逆向工程其系统。亨特认为，日产没有将安全因素考虑到系统设计中。他表示“无论是汽车制造商还是玩具制造商，都应该将安全措施内置在设计中，不应该只当事后诸葛亮。”

原文名称	Total Recall : Troy Hunt Breaks Down His Nissan Hack
作者简介	Tom Spring，一位高级技术编辑。
原文信息	2016 年 2 月 26 日发布于《Threatpost》 原文地址 https://threatpost.com/total-recall-troy-hunt-breaks-down-his-nissan-hack/116497/
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《以印度驻阿富汗大使为目标的新型恶意软件“ROVER”分析报告》

近日，安天追影小组在梳理近期恶意攻击事件时，发现了一起针对印度驻阿富汗大使的 APT 定向攻击事件。攻击者利用 CVE-2010-3333 漏洞制作富文本文件，以邮件为传播方式，实现下载木马主程序，最终窃取用户数据。

以下内容为本次攻击过程的具体描述：近日印度驻阿富汗大使收到一封发件人署名为“印度目前的国防部长”的邮件，邮件中赞扬了该大使为国家所做的贡献和取得的成功，邮件中含有一份名为“Appreciation_letter.doc”的附件。

实际上，该邮件附件是利用了漏洞 CVE-2010-3333 的一个富文本文件，一旦受害者在有漏洞的 word 版本打开该文档，就会触发漏洞。该漏洞是 office 的 RTF 解析漏洞，主要是在解析 pfragment 属性出现的栈溢出问题，漏洞函数存在于 mso.dll 模块中，漏洞函数在数据复制时其复制次数可以在 pfragment 属性中设置。因为没有对复制次数进行检测，导致栈溢出，栈溢出后可以覆盖 SEH 链，最后触发异常劫持 EIP 并跳转到 shellcode 处执行，从而完成漏洞利用。

被利用该漏洞后，受害机器将从 newsumbrella.net 下载文件“file.exe”，该程序是一个下载器，它从 newsumbrella.net 下载主 Rover 恶意软件和相关插件，随后这些文件会在受害机器上运行，盗取受害者硬盘中指定类型的文件及受害者键盘记录、屏幕截图等数据，并上传至 C2 服务器，完成攻击目的。

据了解，恶意软件 Rover 主要利用的技术为“OpenCV”和“OpenAL”，相对于当下一些先进的恶意软件，Rover 其实缺少很多常用功能，但它却能完美躲过各路安全厂商的查杀。

随着“互联网 +”时代的到来，安天追影小组预测越来越多以组织、国家为目标的“Rover”类似软件将会出现，了解其攻击行为和技术，是维护组织信息安全的关键所在。

高级威胁

安天【追影高级持续威胁分析系统】无需更新病毒库，即可实现对上述高级威胁进行有效检测，下为其自动形成的分析报告：

文件被网络威胁感知类设备发现，经由 BD 静态分析鉴定器、YARA 自定义规则鉴定器、可交换信息 (EXIF) 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。

暂时依据 BD 静态分析鉴定器、动态行为鉴定器将文件判定为高级威胁，正在等待美国软件交叉索引 (NSRL) 鉴定器进行分析。

该文件具有以下行为：格式漏洞；获取系统版本；打开自身进程文件；创建互斥体 (mutex)；连接网络；隐藏文件；获取计算机名称；创建特定窗体；获取 socket 本地名称；获取驱动器类型；获取系统内存；查找特定窗体；请求加载驱动的权限；获取主机用户名称。

同时，该文件利用了 CVE-2010-3333 漏洞。

文件名	D38E974ADED02406A4CE0681012F4232
文件类型	Document/Microsoft.RTF[:Rich Text Format]
大小	6.13 MB
MD5	D38E974ADED02406A4CE0681012F4232
病毒类型	高级威胁
恶意判定 / 病毒名称	Trojan[Exploit]/Win32.CVE-2010-3333
判定依据	BD 静态分析

◆ 危险行为

行为描述	危险等级
格式漏洞	★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
获取系统版本	★★	打开自身进程文件	★
创建互斥体 (mutex)	★	连接网络	★
获取计算机名称	★	隐藏文件	★★
获取 socket 本地名称	★	创建特定窗体	★
获取系统内存	★★	获取驱动器类型	★
请求加载驱动的权限	★	查找特定窗体	★
获取主机用户名称	★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=D38E974ADED02406A4CE0681012F4232