安天周观察

主办：安天　2016 年 4 月 4 日（总第 34 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天四地联动召开 RSA2016 交流分享会

3 月 31 日，安天哈尔滨总部、北京公司、武汉公司、深圳公司四地联动，以视频会议的方式召开了“2016 安天 RSA 之旅交流分享会”。

会上，参加本届 RSA 大会的几位代表分别从赴美筹备工作、个人收获和经验总结等角度发表了主题报告；随后大家又以座谈会的方式对会议筹备、参会行程、参展访问等内容进行了热烈讨论，大家各抒已见，表达了对本次行程的看法和总结，也对 RSA2017 做出了期待和畅想。

在本届 RSA 大会期间，安天微信公众号进行了“安天 RSA 西游记”专题的连载报道，这当然离不开 RSA 小分队成员在前线的信息采集与汇报，也离不开默契的团队合作。“蓝天之翼，赤子之心”即是小分队在 RSA 会场展现出的面貌，也是对每一个安天人的诠释。对于 RSA2016 的细心总结，是为了以更好的状态迎接 RSA2017，北馆 2010 号，安天与您明年再见！

安天微信公众号改版升级

近日，安天微信公众号 (Antiylab) 进行了改版升级，在底部添加了自定义菜单，对所有资讯进行了分门别类，方便用户与读者查找相关信息。该自定义菜单共设立“技术分享”、“安天资讯”、“产品方案”三大类一级菜单，每一个选项下设若干二级菜单。其中“技术分享”涵盖了技术报告、年度报告、病毒编年史、勒索软件专题报告等内容；“安天资讯”涵盖了 RSA 专题、冬训营资讯、资质荣誉等内容；“产品方案”涵盖了追影威胁分析系统 (PTA)、探海威胁检测系统 (PTD)、智甲终端防御系统 (IEP) 的介绍及安天技术解决方案案例。

漏洞影响一亿安卓设备 应用 Truecaller 存在远程利用

近日，安全研究人员发现呼叫管理应用程序 Truecaller 存在严重漏洞，允许任何人窃取 Truecaller 用户的敏感信息，为攻击者实施攻击提供条件。Truecaller 使用设备的 IMEI 作为其用户的唯一身份认证标签。这意味着任何人只要获得了设备的 IMEI 就能得到 Truecaller 用户的个人信息（包括电话号码、家庭地址、邮箱、性别等），并且在没有用户的同意下，可以任意篡改用户的 APP 设置，将用户暴露于恶意钓鱼者的威胁下。据统计，目前约有一亿已下载该应用的 Android 用户正处于危险之中。（文章来源：http://securityaffairs.co/wordpress/45701/hacking/truecaller-remotely-exploitable-flaw.html）

一周简讯

- 厂商确认：新浪账户体系高危漏洞 可更改他人密码
- Web 勒索软件新家族 KimcilWare Magento 商店中招
- 美国大型医护机构疑遭勒索软件 Samas 感染被迫关闭网络
- 针对勒索软件肆虐现状 安全厂商发布安天智甲终端防御系统
- 网易邮箱 52GB 数据被公开 涉及 163、126 邮箱用户
- 安天猎豹联合曝光手机扣费病毒 Client 感染超 7 万人
- 研究人员在美国自动药材供应系统发现上千远程漏洞

（安天 CERT 搜集整理，详见：创意安天论坛 http://bbs.antiy.cn/forum.php）

趋势科技客户端被曝后门 亚信安全用户或受影响

3 月 31 日，据谷歌安全团队 Project Zero 披露，谷歌的安全研究人员在安全公司趋势科技的客户端安全软件当中，发现一个低级的后门。在安装了该客户端安全软件之后，默认会启动一个网页服务器，这个服务器会针对一段精心构造的请求做出响应，启动任意在本地的程序。通过这个后门，黑客可以在网页上直接插入一段恶意代码，当安装有该客户端软件的用户打开此网页时，可以实现直接执行恶意代码，或者下载恶意代码执行。

根据 Project Zero 网页提供的信息，趋势科技表示，后门来自第三方代码，因此他们暂时无法对此进行彻底的修复，只能先提供针对这个攻击入口的缓解措施。值得注意的是，趋势科技的中国业务已经于 2015 年被亚信安全收购，因此，中国亚信安全的客户也可能中招。（文章来源：http://news.chinabyte.com/481/13736481.shtml）

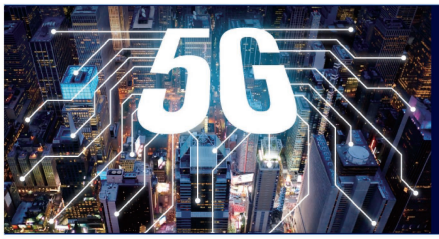
每周安全事件

类 型	内 容
中文标题	“匿名者”重启“# Opcanary”行动，目标锁定加拿大矿业公司
英文标题	Anonymous Relaunches #OpCanary，Targets Canadian Mining Firm
作者及单位	Waqas；HACK READ
内容概述	近日，黑客组织匿名者恢复了一项名为“# Opcanary”的行动，该行动以打击跨国公司为目的。其最新受害者是一家加拿大的矿业公司 BCGold，其主要业务是开采金矿和铜矿。黑客们攻击了 BCGold 公司的网站并侮辱其主页，但目前并没有发现大规模数据泄漏和数据被盗。事实上，我们可以把这次行动看作一种努力让“# OpCanary”行动重新回到大众视线的引导活动。在获得网站服务器访问权限后，匿名者成员留下了 Rick Astley 的视频《Never Gonna Give You up》（永不言弃）。可以说匿名者组织已经恢复了“# Opcanary”行动，并竭尽全力使其成功。
链接地址	https://www.hackread.com/anonymous-opcanary-targets-canadian-mining-firm/

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.sparrow.a[pay] 2016-03-29	该程序安装后无图标，当手机数据连接状态发生改变时，会向一个 URL 发送手机固件信息，将返回的数据信息处理后，会发送一条扣费短信，同时上传到一个 URL，造成用户隐私泄露，资费损失，建议立即卸载。（威胁等级高）
		Trojan/Android.habraSpy.a[prv，rmt，spy]2016-03-30	该应用伪装成 Google Play 服务，程序运行后会隐藏图标，开机自启动，拦截指定短信和电话，获取短信指令执行上传短信信息和通讯录信息、录音和拍照上传、上传浏览器书签和历史记录、上传 GPS 位置信息，造成用户隐私泄露。（威胁等级高）
		G-Ware/Android.Vnoktak.a[exp，fra] 2016-03-31	该程序伪装成系统程序，运行隐藏图标，诱导激活设备管理器，后续执行联网登录 VK 服务器获取账户信息，存在一定风险，可能会造成一定的经济损失，建议及时卸载该程序。（威胁等级低）
	较为活跃的样本	Trojan/Android.SmForw.p[prv]	该程序开机自启动，安装后隐藏图标，监听收件箱并删除接收到的短信，后台私自上传设备信息，上传拦截到的短信，有网络远程控制功能：可以执行上传收件箱信息；上传联系人信息；向指定号码发送短信；添加黑名单；删除短信的功能，会造成隐私泄露，资费消耗，建议立刻卸载。（威胁等级高）
		Trojan/Android.fakewechat.c[prv]	该应用假冒微信图标，实际无微信功能，运行后隐藏图标，获取手机联系人、通话记录、短信、位置、手机设备等信息，将手机设备信息上传到指定 URL，若上传不成功，还会发送短信给指定手机号码，危害较大，建议立即卸载。（威胁等级高）
		G-Ware/Android.Fakegupdt.bh[exp，fra]	该程序伪装成系统更新，后台触发启动推送广告，建议立即卸载避免造成资费损耗。（威胁等级低）
		Trojan/Android.GPSSpy.f[prv，exp，spy]	该程序运行后，会自动发送一条短信，并且当位置信息改变时，通过 socket 联网通信，短信上传位置信息，泄露隐私，建议立即卸载。（威胁等级中）
		Trojan/Android.PhoneCrash.b[pay]	该程序开机自启动，在用户不知情的情况下发送短信，拦截服务商指定短信，回复扣费短信，将指定短信删除，还存在获取短信验证码，模拟验证登录扣费的行为，会窃取设备上安装包信息，删除安装包的行为，危害较大，建议立即卸载。（威胁等级中）
		RiskWare/Android.FakeApp.bc[sys]	该应用为虚假应用，运行后关闭用户 wifi 连接，无其他行为，存在一定安全隐患，建议谨慎使用。（威胁等级低）
		G-Ware/Android.Fakegupdt.bg[exp，fra]	该应用伪装成系统应用，安装无图标，后台推送广告，下载安装未知应用并且卸载删除应用。建议及时卸载，避免造成资费损耗或手机无法正常使用。（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-2015-2477)	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。Microsoft Office 未正确处理内存对象时，在实现上存在远程执行代码漏洞，攻击者成功利用后，可在当前用户安全上下文中执行未授权操作。（威胁等级高）
	较为活跃的样本	Trojan[Backdoor]/Win32.DDOS	此威胁是一种后门类木马程序，运行后创建服务，通过 CMD 隐藏删除自身，连接控制端等待攻击指令。（威胁等级高）
		Trojan[Downloader]/Win32.Genome	此威胁是一种木马类下载程序，运行后连接网络，下载配置文件，查找系统中的游戏然后判断是否在配置文件中，有则下载此游戏盗号程序。（威胁等级中）
		Trojan[Backdoor]/Linux.Gafgyt	此威胁是一种木马类后门程序，运行在 linux 平台，主要功能为 DDOS 攻击、更新和下载等，可通过扫描 SSH 弱口令进行传播。（威胁等级中）



5G 网络：风险和机遇并存

Matthew Rosenquist/ 文　安天公益翻译小组 / 译

第五代网络 (5G) 会将技术大量应用于个人生活和企业运作。技术的进步带来了足够的带宽，可以支撑 500 亿智能设备连网，形成了一个所有计算设备都能连网的世界。这样的变革性技术开辟了巨大的机遇，同时也带来了难以想象的新风险。

5G 网络的最大风险

安全和隐私，特别是新兴物联网 (IoT) 的安全和隐私，是 5G 网络的最大风险。物联网将会为人们的生活带来更高的便利性、自动化、意识、娱乐和效率。然而，如果落在坏人手里，这种连网的智能设备可能会变成破坏安全和侵犯隐私的工具，并且会被滥用而成为安全风险。

有人会说工业控制系统承受着最大的风险。但是我不这样认为。工业控制系统 (ICS) 很早就用于电厂、水处理厂和化工厂。随着时间的推移，这些系统逐渐连接到互联网，但我认为，从风险角度来看，这些地方引入 5G 网络并不会导致严重的后果。ICS 运营商已经认识到风险，明白他们已经遭受了多年的攻击。为了防御风险，他们试图限制这些系统的曝光，在许多情况下故意没有进行连网。ICS 设施的智能设备在理论上是能够被利用的，但更可能的目标是复杂的控制系统，如服务器和个人电脑。

随着 5G 网络开始推出 (我们预计在 2018–2020 年)，我认为消费设备将承受最大的风险。据我预测，交通运输、医疗保健和无人机行业将会是最受影响的领域。

保护 5G 设备

用户、设备、软件、网络和后端基础设施都必须发挥作用，以改善 5G 设备的安全性。连接的可扩展性允许更多的设备进行通信，由此产生了更多的数据。设备、应用程序和数据构成了一个必须被保护的链。这一问题类似于我们目前面临的互联网问题，只是规模更大。新兴物联网设备代表了一个新的挑战，因为它们不像个人电脑、服务器和智能手机那样具有强大的自我防御能力。大多数物联网设备缺乏运行复杂的、功能丰富的安全解决方案的力量和速度。为了补偿这一点，我们应该更加重视硬件、网络、应用验证和后端基础设施等领域。

现在开始建立信任

技术领导者应该合作来定义强劲的标准，提高与生命安全相关的安全、隐私和控制，这一点势在必行。

信任是非常重要的。必须将安全纳入 5G 网络标准，尤其是考虑到物联网时，将其作为基础考量的一部分。隐私方面、给用户更多的监督、默认的匿名性和选择权则必须包含在产品和软件设计中。可能会对用户安全带来威胁的系统应具备更高的安全、管理和控制水平。随着消费者采用诸如自动运输和医疗管理系统的技术，信任水平也必须提高，以应对风险。

该行业已经到了这样一个阶段，安全成为整体设计的一部分，而不是事后的条条框框。技术领导者现在必须共同努力，为 5G 网络的基础和使用建立信任。消费者必须做好自己的本分，并大声疾呼他们的期望。安全需求是想要保持竞争力并为客户提供服务的供应商的关键驱动力。

技术领导者如何发挥作用

1. 开发基础设施和平台，在 5G 连网设备和处理来自这些设备的大量数据的后端基础设施中嵌入安全和信任。

2. 影响行业最佳实践和合作，以建立强大的框架和技术标准，实现强大的安全和隐私原则。

3. 提供一流的安全软件解决方案、防御设备和应用程序。软件具有最大的灵活性，能够协调新威胁和风险。解决方案将被定制，运行于特定计算环境中的小型或固定功能的设备，以及监管系统的可管理基础设施。

5G 网络即将到来，它能够将更多更小的设备连接到我们的电子生态系统中。这种能力会带来不可预知的机遇和风险。为了获取利益并最大限度地降低风险，技术领导者和安全专家必须协同工作，使 5G 网络的基础和后续实现更加安全和隐秘。

原文名称	5G Networks Pose Cyber Risks , Opportunities
作者简介	Matthew Rosenquist，专注安全领域 20 多年，专门开发安全策略和具有成本效益的功能。
原文信息	2016 年 3 月 17 日迈克菲实验室发布 原文地址 https://blogs.mcafee.com/mcafee-labs/5g-networks-pose-cyber-risks-opportunities/

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《paopaoche.net 游戏网站多款游戏感染分析》

近日，安天追影小组在威胁感知平台中发现了感染式病毒的踪迹，感染式病毒顾名思义，需要将自身的一部分或者全部附加到其他宿主程序上运行，一旦一个病毒文件执行，其很有可能将系统中的绝大多数程序文件都加入病毒代码，进而传播给其他电脑。

本次追影小组发现的病毒样本来自 paopaoche.net 游戏网站下载的游戏安装程序，主要获利渠道是通过统计网站计数来刷百度搜索浏览量。其主要行为是感染 exe 文件，设置自启动，设置浏览器主页，连接 paopaoche.net 下载相关配置文件，刷固定 ID 的百度搜索量，同时使用 cnzz 统计网站记录访问量，经分析，该网站多款游戏都具有以上行为，其中一些下载链接已经失活。追影小组进一步分析被感染的文件行为，发现没有刷百度搜索量的行为，只有 DNS 请求 google.com、fget-career.com 等域名的行为，由此可知，该种感染类木马刷百度流量的行为是其原始程序的行为，而非感染后的行为。

百度权重是爱站、站长工具等网站推出的针对网站关键词排名预计给网站带来流量，划分等级 0-10 的欢迎度评估数据。权重数值越大，说明网站自然流量越大，自然流量大，那么相应的关键词排名就相对靠前，而百度搜索量是与百度权重是成正比的。所以在利益的驱使下，刷百度搜索量的服务应运而生。但是刷流量等暗箱操作行为通常是通过恶意代码的方式实现的，而根据获利方式的不同其行为、手段与方法也在不断的更新，以逃避检测与追踪。安天提示各位用户，及时更新及下载正规网站程序补丁，不随意点击不明链接，都可以降低被恶意程序感染的风险。

病毒程序

安天【追影高级持续威胁分析系统】无需更新病毒库，即可实现对上述病毒程序进行有效检测，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、关联分析鉴定器、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。

暂时依据 BD 静态分析鉴定器、关联分析鉴定器、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病毒程序，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：感染文件；其他进程写入可疑数据；增加 winlogon 自启动项；设置 IE 首页；读取自身文件；自启动；连接特殊 URL；获取驱动器类型；通过设置为系统属性隐藏文件；填充导入表 (疑似壳)；释放 PE 文件；创建快捷方式；获取系统内存；访问 dns；获取系统版本；访问其他进程内存；获取计算机名称；获取 socket 本地名称；文件下载；篡改系统文件创建时间；复制自身文件；连接网络；创建特定窗体；独占打开文件；打开自身进程文件；获取主机用户名称；查找特定窗体；创建桌面快捷方式；请求加载驱动的权限；疑似查找浏览器进程；疑似桌面控制。

文件名	5C31C088AD82424537E641D10BF8A5F9
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	2.31 MB
MD5	5C31C088AD82424537E641D10BF8A5F9
病毒类型	病毒程序
恶意判定 / 病毒名称	Virus/Win32.Nimnul.a
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
感染文件	★★★★	其他进程写入可疑数据	★★★
感染文件	★★★★	增加 winlogon 自启动项	★★★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=5C31C088AD82424537E641D10BF8A5F9

其他行为

行为描述	危险等级	行为描述	危险等级
设置 IE 首页	★★	读取自身文件	★★
自启动	★	连接特殊 URL	★
获取驱动器类型	★	通过设置为系统属性隐藏文件	★
填充导入表（疑似壳）	★★	释放 PE 文件	★
创建快捷方式	★★	获取系统内存	★★
获取系统版本	★★	访问 dns	★
获取计算机名称	★	访问其他进程内存	★
文件下载	★	获取 socket 本地名称	★
复制自身文件	★★	篡改系统文件创建时间	★★
创建特定窗体	★	连接网络	★
独占打开文件	★	打开自身进程文件	★
获取主机用户名称	★	查找特定窗体	★
创建桌面快捷方式	★	请求加载驱动的权限	★
疑似查找浏览器进程	★★	疑似桌面控制	★