安天周观察

主办：安天　2016 年 6 月 13 日（总第 43 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天举办 16 周年生日纪念活动

2016 年 6 月 6 日，是安天成立 16 周年的生日，安天各地都以自己的方式举办了生日纪念活动，并通过视频直播的方式，召开全员大会，回顾过往，立足当下，展望未来。

右上：安天创始人、首席技术架构师发表演讲
右下：安天研发副总裁王小丰发表演讲

反思与展望

在全员大会上，安天创始人、首席技术架构师以“安天第三次创业”为主题发表了演讲，他回顾了安天前两次创业时的种种经历，认为这两次创业是有意义、有价值的，但同时也存在不足。而安天的第三次创业将以深化用户价值导向，打造企业级产品体系和销售平台，全面提升优胜能力和团队规模为发力点。这是对安天全员的一次挑战，必须做到共同努力，没有短板。

安天研发副总裁王小丰也以《打造优质研发供应链，支撑安天第三次创业》为题目进行演讲，对安天的研发体系进行了分类、阐述、反思与设计。

礼物与祝福

在这样一个有纪念意义的日子里，每一位安天人都收到了一份特别的“16 岁生日礼物”。这其中有陪伴了安天十几年的反病毒老兵，也有刚刚加入这个集体的新鲜血液。而这些勤勤恳恳、兢兢业业的安天人又将最美好的祝愿与期盼送给了安天。

变革与前行

随着企业规模的成长与发展，安天开始重新调整自身定位，形成了以安天实验室为总部，以企业安全、移动安全业务线为两翼的集团化布局。在这种发展模式下，安天将始终坚持以先进威胁检测能力为支撑，以海量装机量为基础，以恪守传统反病毒价值观为原则。坚持防御者的立场，坚持保障用户价值的使命，坚持对安全威胁受害者感同身受的情感，坚持对原则和底线的敬畏。为“服务客户，解决问题。应对威胁，保障价值！”做出努力。

16 年前，几名热爱网络安全技术的青年因同样的信念走到了一起，成立了一支有信仰的安全团队——安天实验室。16 年后，安天选择变革，积蓄力量，整装待发，坚定信心，斗志昂扬，期待以更加成熟、更加卓越的形象出现在大家面前。

安天各地举办 16 周年生日纪念活动

安天各地通过视频直播共同召开全员大会

小伙伴们领取“16 岁”生日礼物 并写下祝福送给安天

安天举办端午节趣味活动

为了迎接端午节的到来，安天举办了一系列有趣的活动，为小伙伴们增添节日气氛。

安天北京办公区于 6 月 5 日举办了一次 Family day，在周末的午后，小伙伴带上家人与一份闲适的心态，来到安天，一起包粽子，画蒲扇，共度端午欢乐家庭日的好时光。




左：包粽子从妈妈抓起，抓病毒从娃娃抓起
下：安天端午大礼包 你有没有心动

安天哈尔滨总部也在端午节前，为大家带来了节日的气息，香包，粽子，五彩绳，撞鸡蛋，做一个安天小伙伴，是如此的幸福。

每周安全事件

类 型	内 容
中文标题	俄罗斯最大社交网站 VK.com 被黑，1.71 亿用户账号仅售 1 比特币
英文标题	171 million VK.com accounts stolen by hackers
作者及单位	Zack Whittaker；ZDNet
内容概述	近日，俄罗斯最大社交网站 VK.com 被黑客入侵， 1.71 亿名用户账号信息泄露。VK.com，始创于 2006 年，前身为 vkontakte.ru，是俄罗斯最大的类“Facebook ”社交网站，用户超过 3.5 亿，初期用户集中于俄语国家，目前 VK 提供 70 多种语言版本以服务全球用户。 此次泄露的信息包括完整的用户名、电子邮件地址以及纯文本密码，很多账号还含有位置和电话号码信息。目前，黑客组织在网络黑市上兜售了其中的部分账号数据——涉及 1 亿名账户，容量约为 17GB。不过令人匪夷所思的是，他们在黑市上对这些数据的要价仅为 1 比特币，约合 580 美元。
链接地址	http://www.zdnet.com/article/vkontakte-vk-hacked-171-million-accounts-sold-dark-web/

每周值得关注的恶意代码信息

经安天检测分析，本周 9 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.GoogleSync.a[prv，rmt，exp，spy]2016-06-05	该应用伪装成系统程序，安装无图标，会监听短信，拦截指定短信，获取短信指令执行远控操作，包括窃取用户短信、通讯录、通讯记录、gps 位置信息、设备和 sim 卡相关信息等一系列隐私信息，并通过发送短信和发送邮件的方式上传。另外还包含设置静音、飞行模式、复制文件、打包压缩文件等行为，会造成用户隐私泄露和资费消耗。（威胁等级高）
		RiskWare/Android.zwpay.a[pay，rog] 2016-06-06	该应用运行后隐藏图标，后台获取短信，删除特定短信，包含联网支付和短信支付等风险代码，可能会造成用户资费损失，建议不要安装。（威胁等级低）
		G-Ware/Android.Fadeb.a[rog，exp] 2016-06-06	该程序伪装系统应用安装无图标，运行后联网上传固件信息，获取配置信息，下载恶意 apk，建议立即卸载，避免造成资费损耗。（威胁等级低）
		Trojan/Android.Vkezo.a[prv] 2016-06-06	该应用程序为一款音乐软件，包含恶意代码会获取用户登陆账号密码信息，上传至远程服务器，造成用户隐私泄露，建议及时卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.Downloader.bx[exp，rmt]	该程序伪装成系统应用，安装无图标，后台联网上传固件信息，获取配置信息，接收指令下载 apk 静默安装，建议立即卸载，避免造成资费损耗。（威胁等级中）
		G-Ware/Android.HiddenAds.t[rog，exp]	该应用程序包含广告插件，安装无图标，联网获取配置信息下载广告 SDK，推广广告，会造成资费损耗，建议卸载。（威胁等级低）
		Trojan/Android.FakeFB.d[prv，fra]	该应用伪装成 Facebook 升级程序，诱导用户输入 Facebook 账号密码，后台获取手机固件信息和 Facebook 账号密码，造成用户隐私泄露，建议不要安装。（威胁等级中）
		G-Ware/Android.chro.b[rog，exp]	该应用运行后隐藏图标，当用户浏览网页时将网址重定位，加载推广广告和色情网址，造成用户资费损耗，建议卸载。（威胁等级低）
		Trojan/Android.QQspy.i[prv，exp]	该应用伪装成 QQ 刷钻工具，诱导用户输入 QQ 账号密码，然后通过短信转发，造成用户隐私泄露，建议不要安装。（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 CVE-2015-2545 EPS 文件处理内存破坏漏洞 (MS15-099)	Microsoft Office 处理 EPS 文件存在内存破坏，允许攻击者构建恶意文件，诱使应用解析，可使应用程序崩溃或执行任意代码。（威胁等级高）
	较为活跃的样本	Trojan[Dropper]/Win32.FrauDrop	此威胁是一种具有捆绑行为的木马类程序，会损坏被感染电脑的注册表文件，阻止用户访问系统。同时会随系统运行自启动，并利用连续弹窗和虚假警告消息欺骗用户，还会损坏任务管理器和系统还原功能。此外，该家族会感染操作系统，收集用户隐私信息发送给黑客。（威胁等级中）
		Trojan[Downloader]/Win32.Dofoil	此威胁是一种下载类木马程序，运行后会在电脑中下载并运行未知程序或恶意软件，干扰系统正常运行，同时会修改系统设置。该家族及其变种主要通过恶意软件、被感染的网站、垃圾邮件、社交媒体网站恶意链接、文件共享网络等方式进行传播。（威胁等级中）
		GrayWare[AdWare]/Win32.BrainInsty	此威胁是一种具有广告行为的木马类程序，运行后会在电脑中下载并安装多个程序，如 IE 工具栏，推广软件等程序。（威胁等级中）

美联储不断遭受攻击

Tom Spring/ 文　安天公益翻译小组 / 译

驱动全球金融市场的美联储于近日透露，在过去的 5 年中，它已遭到了多达 50 次的网络攻击。

作为对路透社信息自由法案要求的响应，公众第一次了解了该政府机构是如何对抗连续网络攻击的。

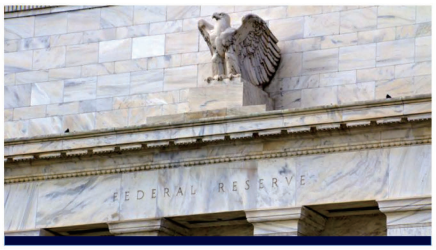
美联储在报告中指出，他们总共记录了 310 起事件，其中有 140 起是黑客攻击。报告中列举的事件涵盖 2011 年至 2015 年，来自其中一个美联储机构——设在华盛顿的美联储委员会。

根据美联储委员会发布的报告，在 310 起事件中，81 起涉及恶意代码，54 起涉及未授权的访问，32 起涉及信息泄露。

路透社记者吉森·兰格指出，有些事件可能只是有人不小心将电子邮件发送给了错误的收件人。兰格报道说，这些文件被高度编辑，范围有限，不包括影响美联储的其他 12 个私人拥有的区域分支机构的事件。

路透社获得的记录显示，美联储至少把 4 起黑客事件归类为间谍活动。据路透社报道，其中的 2 起间谍活动涉及信息泄露。路透社获得的记录并没有显示数据的性质。

路透社报告称："美联储的网络安全



专家团队共确定了 51 起涉及美联储委员会的信息泄露事件。"

安全专家并不感到惊讶，并表示，美联储的事件追踪记录多于私营金融机构。他们指出，更糟的是，正如信息自由法案要求所述，美联储更不可能透露事件的详细信息。

战略网络风险投资公司的 CEO，前世界银行安全团队成员汤姆·凯勒曼说："美国法律要求美国银行透露任何此类安全事件的信息。这些规则是为了增加公众对金融体系的信任和信心。但是美联储却不用遵守这些规定，这是对公众的损害。"

凯勒曼指出，这些攻击是联邦政府在 2 月份公布的泄露事件的一小部分。当时，联邦调查局发布了一份公告，指出一个名为 APT 6 的组织早在 2011 年就侵入了美国政府的计算机系统，多年来不断窃取敏感数据。

在发布公告的时候，联邦调查局没有提供攻击的细节以及哪些政府系统被感染。政府官员说，他们知道初始攻击发生在 2011 年，但不知道幕后黑手是谁。

至于谁偷了什么、偷了多少、什么时候偷的，路透社也没获得多少信息。

凯勒曼说，他怀疑，黑客攻击美联储是为了窃取资金。这与孟加拉银行的事件一样，黑客利用一家银行的纽约联邦储备银行账户发起欺诈交易，从孟加拉银行账户窃取了 8100 万美元。

"黑客越来越聪明，对内幕信息越来越感兴趣。这样他们能够领先美国政府的宏观战略举措。"凯勒曼说。

"从一家金融机构窃取 2000 万美元 VS 提前得知一家主要的金融机构明天要向瑞士法郎投资 100 亿美元，在哪种情况下黑客能够窃取更多的资金？如果选择后者，那么黑客的收益将不可同日而语，会远远多于 2000 万美元。"

凯勒曼预计，针对金融机构的黑客攻击会越来越多。在应对此类攻击方面，金融机构存在较大的安全空白。"网络金库并没有与威胁全景同步演变，因此黑客能够利用这些空白。美国金融系统的安全架构必须进步，以便应对现代的网络窃贼。"

原文名称	Federal Reserve Target of Constant Attacks
作者简介	Tom Spring，Threatpost 副主编。
原文信息	2016 年 6 月 2 日《Threatpost》发布 原文地址 https://threatpost.com/report-federal-reserve-target-of-constant-attacks/118443/
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《一起针对印度外交和军事资源的 APT 攻击事件分析报告》

近日，安天追影小组在梳理恶意攻击事件时发现了一起针对印度外交和军事资源的 APT(高级持续性威胁) 攻击事件，该攻击流程与通常的 APT 攻击手法相似，均为使用邮件携带附件的方式来敲开受害者的防御之门，附件可触发漏洞进而使受害者下载远控木马并安装，从而达到控制受害者主机的目的。

该事件起源于发往印度驻沙特阿拉伯与哈萨克斯坦大使馆的邮件，发往两个使馆的邮件内容与附件完全相同，内容大意为寻求帮助，附件是文件名为“Harrasment Case Shakantula.doc”的文档，经分析该文档为 rtf 文本格式，受害者运行该 rtf 文件后，会触发微软 ActiveX 漏洞 (CVE-2012-0158)，进而释放恶意样本“MSIL/Crimson”，随后该样本会感染用户的计算机，然后下载功能更强大的远程控制木马组件，至此受害者已经处在攻击者的监控之中，包括控制摄像头、截屏操作以及键盘记录等功能。

经分析，攻击者还使用一个虚假的印度博客新闻网站来为恶意样本服务，同时分析数据显示参与攻击的 IP 地址在巴基斯坦，其攻击过程不仅是上述两封邮件，还依赖于水坑攻击和多个网络钓鱼邮件活动得以实现。

水坑攻击最常见的做法是分析攻击目标的上网活动规律，找出攻击目标经常访问的网站的弱点，先将此网站攻破并植入攻击代码，一旦攻击目标访问该网站就会中招。网络钓鱼则是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息 (如用户名、口令) 的一种攻击方式，通常这个攻击过程不会让受害者警觉，属于“社会工程攻击”的一种形式。

在恶意软件盛行的网络环境中，广大用户需要提高防范意识，养成良好的上网习惯，尤其是对于陌生发件人发来的带附件的邮件，请谨慎点击，以免成为攻击者的“囊中之物”。目前，安天追影产品已经可以对上述恶意样本进行检出，并分析出其恶意行为。

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、美国软件交叉索引 (NSRL) 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。

最终依据动态行为鉴定器将文件判定为高级威胁。

文件名	68773F362D5AB4897D4CA217A9F53975
文件类型	Document/Microsoft.RTF[:Rich Text Format]
大小	259 KB
MD5	68773F362D5AB4897D4CA217A9F53975
病毒类型	高级威胁
恶意判定 / 病毒名称	Trojan[Exploit]/Rtf.Generic
判定依据	动态行为

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
仿冒 SVCHOST	★★★★	利用漏洞释放 PE 文件	★★★★
格式漏洞	★★★★		

该文件具有以下行为：仿冒 SVCHOST、利用漏洞释放 PE 文件、格式漏洞、关机、自启动、隐藏文件、填充导入表 (疑似壳)、释放 PE 文件、获取系统内存、增加 run 自启动项、获取系统版本、获取计算机名称、创建特定窗体、获取驱动器类型、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、请求加载驱动的权限。

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
关机	★	自启动	★
隐藏文件	★	填充导入表 (疑似壳)	★★
获取系统内存	★	释放 PE 文件	★
获取系统版本	★★	增加 run 自启动项	★
创建特定窗体	★	获取计算机名称	★
获取驱动器类型	★	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	★	请求加载驱动的权限	★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=68773F362D5AB4897D4CA217A9F53975