安天周观察

主办：安天　2016 年 7 月 11 日（总第 47 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加哈尔滨大数据产业发展论坛并发表演讲

7 月 3 日，哈尔滨市发改委联合哈尔滨市电视台共同举办了一场“哈尔滨大数据产业发展论坛”。论坛邀请到了中国工程院院士刘韵洁、中国家发改委高技术司信息化处处长王娜、国家信息中心信息化研究部副主任单志广、中央财经大学中国互联网经济研究院院长孙宝文、中关村大数据产业联盟秘书长赵国栋、浪潮集团副总裁王方等国内多位大数据领域专家和知名企业代表，围绕加快发展哈尔滨大数据产业，打造中国北方数据中心等主题进行了深入的探讨。

王娜处长对国务院印发的《促进大数据发展行动纲要》进行了解读，她指出，在抓紧推动大数据发展与应用的同时，要做好数据保密工作，保障数据安全，做到“有数据、用数据、管好数据”。

单志广副主任就目前国内大数据发展总体情况及国家发展大数据产业的战略布局进行了发言。他指出，目前全国大数据产业已在京津冀、长三角、珠三角等地区得到了良好的发展，与各行各业相融合，逐渐成为城市发展的新增长极。

刘韵洁院士则针对哈尔滨市建设国家北方大数据中心应具备的条件及规划方向进行了发言。他认为中国当前的数据中心空间布局不合理，尚未形成优势互补的产业布局，北部尤其匮乏，因此加快建立我国北方大数据中心具有很大的必要性。哈尔滨在发展大数据方面具有地理、气候、地质、资源、人才、区位等优势，应该积极搭建大数据政策、人才、科研、产业环境，打造大数据科技创新高地和产业高地，为城市发展增添新动力。

安天技术负责人作为企业代表参加了本次会议，并带来了本次论坛唯一来自企业界的主题演讲——《大数据对网络安全技术和产业发展的支撑价值》。他表示，网络安全威胁目前呈现出了两个走向，其一是随着“互联网 +”战略向关键基础设施和基础的工业等传统领域纵深延展，从而使传统安全风险和网络安全风险合流，导致国计民生和工业系统的关键数据也可以通过互联网被窃取；其二是随着智能化向智能穿戴、智能家庭等新型领域的泛化延展，从而使细粒度化和私密化的个人信息被获取和攻击。这两种威胁走势一方面导致网络威胁的结果从虚拟空间转移到实体空间，另一方面也导致网络威胁最终侵害的目标变为以数据为主。

安天技术负责人表示，大数据不仅仅是网络安全技术保护的对象，同样也是网络安全技术和工程体系所依赖的基础资源和基本方法。其介绍了安天当前的感知与捕获能力，事件和样本规模，向量提取等情况。并通过案例介绍了安天依托所拥有的大数据资源，进行样本同源关联、APT 分析溯源等方面的工作。安天坚持以云计算为基础架构、以大数据为资源对象、结合人工智能与专家经验，不断提升安全能力。助力哈尔滨构建大数据产业生态体系，努力将哈尔滨打造成为立足东北、辐射全国、影响东北亚的国家大数据产业创新发展先行区。

报告结束后，安天技术负责人与孙宝文、赵国栋、王方等专家一同，与听众进行了互动交流。

一周简讯

- 调查显示：针对交通部门的网络攻击呈现出增长趋势
- 公安部联合网信办启动网络诈骗举报联动机制
- Android 将采用新机制遏制快速增长的锁屏勒索
- 勒索软件 MIRCOP 已破解，研究者发布解密工具
- 微软 Office 旧漏洞仍在流行，被用于传播恶意软件
- 5000 万安装量安卓键盘应用，被曝后台收集用户信息
- 点击欺诈软件 Kovter 不断演化，新版本伪装成火狐更新

（安天 CERT 搜集整理，详见：http://bbs.antiy.cn）

安天举办夏游活动

近日，安天哈尔滨总部举办了一次清凉解暑的夏游活动，小伙伴们来到有着“天然氧吧”之称的伊春，在炎炎夏日远离城市的喧嚣，置身蓝天白云下，青山绿水间，凉爽的漂流之旅，浪漫的篝火晚宴，亲近自然的登山活动，安天小伙伴们释放压力，放飞心情，留下了一段美好的回忆。

每周安全事件

类 型	内 容
中文标题	联想 Thinkpad 存在零日漏洞 可以绕过 windows 安全防护功能
英文标题	Lenovo ThinkPad zero-day bypasses Windows security
作者及单位	Juha Saarinen；IT news
内容概述	近日，安全专家在联想 ThinkPad 系列笔记本电脑中发现了一个 0 day 漏洞，攻击者可以利用该漏洞移除系统闪存上的写入保护，重写固件的保护代码，绕过硬件和 Windows 系统的安全防护功能。该漏洞已被命名为“ThinkPwn”，由“ThinkPad”和“Pwned”衍生而成。目前，联想公司还未提供相应的漏洞补丁。同时，安全专家表示，从理论上说，这一漏洞不仅会存在于联想笔记本电脑中，其他品牌的机器也有可能会受到影响。
链接地址	http://www.itnews.com.au/news/lenovo-thinkpad-zero-day-bypasses-windows-security-430090

每周值得关注的恶意代码信息

经安天检测分析，本周有 10 个移动平台恶意代码和 4 个 PC 平台恶意代码值得关注

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.Jpy.a[exp，fra] 2016-07-04	该应用伪装成系统程序，运行后释放广告子包，上传手机固件信息，执行插屏及通知栏推送等行为，影响用户正常用机体验，会造成资费损耗，建议及时卸载。（威胁等级高）
		Trojan/Android.zslocker.a[rog，prv，exp]2016-07-04	该应用程序伪装成其他应用，运行后会私自发送短信，获取 root 权限，释放恶意子包到系统文件，恶意子包运行会隐藏图标，请求激活设备管理器，进行锁屏勒索和界面置顶勒索，窃取用户输入的 qq 账号和密码，发送到指定邮箱，建议及时卸载。（威胁等级高）
		Trojan/Android.smshost.a[pay] 2016-07-04	该应用程序安装无图标，程序运行后会联网获取订购服务信息，私自发送付费订购短信，监听短信，拦截指定号码发送的短信，造成用户资费消耗。（威胁等级高）
		Trojan/Android.androidmobgate.a[prv，rog] 2016-07-06	该应用运行后会隐藏图标，后台获取用户设备固件信息、短信信息、通讯录、通讯记录、浏览器书签、gps 位置等信息，同时监听来电，获取通话录音保存到指定文件并联网上传，造成用户隐私泄露。（威胁等级高）
		G-Ware/Android.Bihoo.a[exp，rog]2016-07-07	该应用程序伪装成系统应用，后台推广广告，私自下载 APK，造成用户资费损耗，建议及时卸载。（威胁等级低）
	较为活跃的样本	Trojan/Android.SmsThief.ai[prv，exp]	该应用安装无图标，运行时会向指定号码发送安装报告，监听来信，向指定号码转发来信内容，造成隐私泄露和资费消耗，建议及时卸载。（威胁等级高）
		Trojan/Android.Gugi.b[prv，exp，rmt]	该应用伪装成其他应用，运行后会隐藏图标，请求激活设备管理器，私自发送短信，监听短信，拦截指定短信，利用钓鱼界面诱骗用户输入银行相关账号和密码，窃取用户短信、通讯录等信息，造成用户隐私泄露和资费消耗。（威胁等级中）
		Trojan/Android.FakeFlashPlayer.n[exp，rog]	该应用伪装成 FlashPlayer，程序运行后会隐藏图标，请求激活设备管理器，监听短信，拦截指定短信，私自发送指定短信，造成用户资费消耗。（威胁等级中）
		G-Ware/Android.Adleak.a[exp，sys]	该应用程序运行后隐藏图标，尝试激活设备管理器，后台释放风险子包，申请 root 权限，加载运行子包文件，执行广告推送，造成用户资费消耗，建议及时卸载。（威胁等级低）
		G-Ware/Android.jianmo.ah[rog，exp]	该应用伪装成 QQ 免流量工具，运行后激活设备管理器，置顶界面，勒索用户添加指定 Q 群进行付费解锁，造成用户资费损失，建议不要安装。（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 2007 / 2010 OLE Arbitrary Command Execution (CVE-2014-6352)	远程攻击者可借助特制的 OLE 对象利用该漏洞执行任意代码。该漏洞类似沙虫漏洞 (cve-2014-4114) 的一种变种，是针对原来版本的漏洞补丁。（威胁等级高）
	较为活跃的样本	GrayWare[AdWare]/Win32.SrchResults	此威胁是一种辅助搜索的灰色软件家族，该家族样本运行后安装浏览器插件，在搜索时提供更多结果，弹出广告，占用系统资源，影响用户使用。（威胁等级低）
		Trojan[DDoS]/Win32.Mavros	此威胁是一种可以实行 DDoS 攻击的木马家族，该家族样本运行后会连接远程控制服务器，并向其发送上线包，接受攻击者控制，有一定威胁。（威胁等级中）
		Trojan[Downloader]/Win32.Netshelled	此威胁是一种可以开启用户 netshell 的木马家族，该家族样本运行后会连接网络与远程服务器进行通信，可能会下载其他恶意代码或接受攻击者的控制。（威胁等级中）

“加密绕过漏洞”影响到一半安卓设备

Tom Spring/ 文　安天公益翻译小组 / 译

近日，芯片制造商高通 (Qualcomm) 的移动处理器被发现存在一个漏洞，该漏洞允许攻击者破解设备上的全磁盘加密 (FDE)。不幸是的，目前已有 60％的安卓手机使用了该处理器，而其中只有 10% 的手机不会受到此类攻击。

Duo Labs 的研究人员表示，该漏洞与安卓系统的媒体服务器组件和高通的安全执行环境 (QSEE) 的一个安全漏洞有关。总之，这些漏洞允许物理访问手机的人绕过全磁盘加密 (FDE)。

盖尔・本尼亚明尼 (Gal Beniamini) 和 Duo Labs 在今年 5 月发布了一份研究报告。基于这份报告，盖尔・本尼亚明尼于近日发现了这个漏洞。当时，双方都强调了谷歌的媒体服务器组件中的一个之前未打补丁的漏洞 (CVE-2016-2431)。此后，谷歌修复了该漏洞，但是大部分安卓手机还没有收到更新包。

Duo Labs 估计，57％的安卓手机仍然容易受到相关的媒体服务器的攻击。Duo Labs 在一篇博客中写到：“根据数据统计，今年 1 月有 60％的安卓手机容易受到攻击。相比于此，目前的数据安全状况已经有所改善，下降为 57％的安卓手机容易受到最新的攻击。”

如果预先安装的未修复媒体服务器漏洞仍旧存在，本质上攻击者就可以利用其实行对 FDE 的泛函数微分方程密码攻击。

类似于 iPhone，安卓手机也限制用户输入密码来解锁设备的频率和次数。而谷歌也像苹果公司一样，推出了安卓设备解密尝试和选项之间的延迟，在几次失败的密码解密尝试后，它会擦除用户的信息。在安卓操作系统中，设备的加密密钥由硬件支持的按键组件 KeyMaster 生成，KeyMaster 是设备的一个功能，运行于操作系统的安全部分。

本尼亚明尼在一份技术报告中写到：“但是，KeyMaster 模块的安全性如何呢？KeyMaster 模块的实现由系统级芯片代工生产 (OEM) 厂商提供。正因为如此，它是完全无记录的 (实质上是一个黑盒)。我们可以从安卓的官方文件中找到一些内容，比如 KeyMaster 模块为安卓设备提供了一个机会，使其能够提供硬件支持的、强大的安全服务。但这肯定是不够的。”

KeyMaster 模块依赖于高通的可信执行环境 QSEE。这其中使用的高通芯片允许攻击者逆向工程未打补丁的安卓系统中的 QSEE 和 KeyMaster 模块使用的代码。在这个案例中，攻击者可以针对安卓系统的 TrustZone 软件部分执行密码攻击，而不需要担心因为尝试密码次数过多而遭到安卓硬件的主要 (非安全) 部分擦除数据。

本尼亚明尼指出：“安卓设备的全磁盘加密效果只能与 KeyMaster 的 TrustZone 内核媲美。只要发现一个 TrustZone 内核漏洞或 KeyMaster trustlet 漏洞，就会直接导致 KeyMaster 密钥的泄露，从而对安卓设备的全磁盘加密执行攻击。”

本尼亚明尼表示，在这些条件下，OEM 厂商可以与执法机构合作破解全磁盘加密。“由于密钥提供给了 TrustZone，OEM 厂商可以简单地创建并签名 TrustZone 图像，从而提取 KeyMaster 密钥并将其闪存到目标设备。这将允许执法机构使用泄露的密钥轻松地暴力破解设备的全磁盘加密密码。”他写道。

原文名称	Encryption Bypass Vulnerability Impacts Half of Android Devices
作者简介	Tom Spring，Threatpost 副主编。
原文信息	2016 年 7 月 5 日 Threatpost 发布 原文地址 https://threatpost.com/encryption-bypass-vulnerability-impacts-half-of-android-devices/119039/
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《一种针对沙箱检测的逃逸技术分析》

近日，安天追影小组在产品样本分析测试中，发现了某一样本会出现异常崩溃的现象，而这种现象会导致追影威胁分析系统无法对其进行监测。通过逆向分析，追影小组发现这是因为该样本在调用 OpenServiceA 这个 API 的过程中，先自写了一部分汇编代码，然后再调用剩余的代码，导致了其在追影中执行时会发生异常，而在普通环境中却可以正常运行的情况。

追影威胁分析系统对样本的监测分析主要依赖于 HOOK 一些关键的 API，而大多数 API 的前五个字节的作用是打开栈帧。经分析，该样本在调用 OpenServiceA 时，会先自写并执行 API 里的一部分汇编代码，然后直接跳转到 API 自写汇编代码的后面去执行，这样整个 API 所属代码都可以得到完整执行，也就不会发生执行错误，类似于代码分块执行。但是，当使用 mhook 库中的功能函数对 API 的前 5 个字节进行 HOOK 的时候，样本的执行流就会进入到 HOOK 的 API 的前五个字节的内部，执行结构就会被打乱，程序也会出现异常，导致提前退出。

这种方法不仅仅影响 OpenServiceA 这一个 API，如果攻击者精心构造，甚至可以使所有 HOOK 的 API 都可以受到影响。

针对以上情况，追影小组提出两种解决方法：

1. 把 HOOK 点移到更底层：即将 HOOK ntdll 里的一些 API 直接在 RING0 进行 HOOK。

2. 更改 HOOK 点的位置：即从 API 头部开始，向后移动几个字节后再选择在合适位置开始 HOOK。

这两种方法都可以有效地解决该样本导致的不能正常 HOOK 的问题。

网络安全就是一场攻防博弈，随着沙箱技术越来越成熟，攻击者也开始注重在恶意软件里运用反沙箱技术来对抗检测。对此，追影威胁分析系统会持续提高对威胁的检出能力。目前，经过安天追影小组的研究，对于上述样本，追影威胁分析系统已经可以采取其他方式对其进行识别，从而达到检出效果。

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：

文件被网络威胁感知类设备发现，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 BD 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。

文件名	F5D2A6E81CD9B23D4899371B296B8A8C
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	240 KB
MD5	F5D2A6E81CD9B23D4899371B296B8A8C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.QVod
判定依据	安全云

◆ 危险行为

行为描述	危险等级
疑似 Virus/Win32.KillAV 家族	★★★★★

该文件具有以下行为：疑似 Virus/Win32.KillAV 家族、获取系统版本、填充导入表 (疑似壳)、查找指定内核模块、读取自身文件、获取计算机名称、打开自身进程文件、获取驱动器类型、获取系统内存、查找特定窗体、独占打开文件、遍历进程、获取主机用户名称、启动指定服务、疑似查找杀软进程、疑似桌面控制。

同时，该文件通过 2 种方式对虚拟机、沙箱技术进行检测。

◆ 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	★★	填充导入表 (疑似壳)	★★
查找指定内核模块	★	读取自身文件	★★
打开自身进程文件	★	获取计算机名称	★
获取驱动器类型	★	获取系统内存	★★
查找特定窗体	★	独占打开文件	★
遍历进程	★	获取主机用户名称	★
疑似桌面控制	★	疑似查找杀软进程	★★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=F5D2A6E81CD9B23D4899371B296B8A8C