安天周观察

主办：安天　2016 年 9 月 19 日（总第 57 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加阿拉伯国家网络空间安全管理与保障研修班

9 月 12 日，由商务部和国家互联网信息办公室共同举办的——“阿拉伯国家网络空间安全管理与保障” 研修班在北京天坛饭店举办，共有来自阿尔及利亚、埃及、约旦、巴勒斯坦、苏丹等国家的互联网领域官员 20 名学员参加培训。在本次培训中，有安天选派出在安全研究和应急响应方面具有经验的工程师担任本次培训的讲师。

阿拉伯国家网络空间安全管理与保障研修班是中国国家领导人积极倡导的对外援助培训项目，已成为促进中国与各有关国家友谊和合作的桥梁。本期研修班旨在加强中国与阿拉伯国家在信息化发展与管理领域的交流与合作，研修班组织学员对网络安全保障体系建设进行了系统学习，并采用专家授课、同行间经验交流、厂商技术人员交流等多种形式，使培训学员更多地了解网络安全技术的发展趋势并围绕信息化管理进行探讨。

在培训班上，安天讲师为学员们带来了题为《APT 分析技术及案例研究》的演讲，他主要介绍了一些 APT 事件分析技术，如鱼叉式钓鱼邮件、水坑攻击、样本关联分析的方法，并结合白象事件等几起 APT 攻击事件举例了 APT 溯源、定位的一些技术手段。他表示目前 APT 攻击正在严重威胁各国关键基础设施和重要机构单位的安全。APT 攻击通常带有国家和政治经济集团背景，以高级攻击技术为突破，实现针对目标网络和信息系统的持续信息获取，并造成进一步“灾难性”破坏。

同时，安天讲师分享了《安天反 APT 综合解决方案》；安天反 APT 综合解决方案融合网络流量和端点检测防护先进技术，辅以深度鉴定环节，在网络边界、关键网段、工作站、服务器和移动终端形成部署。基于安天自主研发的 AVL 动静态检测引擎，方案可深度检测威胁载荷和相关行为，精确检测已知恶意代码和安全风险，标定可信文件与资源，结合安全可视化能力，让高级威胁无所遁形。安天技术人员精彩的演讲、专业的视角使之得到与会人员的高度重视与认可。

欧洲最大贸易公司 BDSwiss 被攻击大量敏感数据遭泄露

近日，欧洲最大的贸易公司 BDSwiss 公司遭遇数据泄露，相关黑客向持有洗钱、谋杀及诈骗、新纳粹活动照片、好莱坞明星裸照、护照以及信用卡等信息的所有者提出指控。

自称为 The Control(I) 集团的黑客们侵入 BDSwiss 公司官方网站，并窃取到高度敏感数据信息。其中一部分资讯已经通过某文件共享站点进行曝光。该集团组织的此轮攻击揭露了大量由 BDSwiss 公司组织的洗钱与诈骗活动。他们特别指责 BDSwiss 公司通过赖夫艾森银行，利用洗钱活动将资金由塞浦路斯转向科索沃。The Control (I) 集团将其余数据公开出售。这部分信息的总价达到 65 比特币 (34858.03 欧元)，这应该意味着其中包含着更为敏感的信　息。(https://www.hackread.com/bdswiss-trading-hacked-data-leaked/)

核监督机构在朝鲜核试验前遭遇 DDoS 攻击

近日，存储核试验数据的图像分析众包项目 (PCIA) 的服务器在朝鲜核试验之前两天受到 DDoS 攻击。此次攻击迫使 PCIA 不得不将其 “geoserver” 下线，该服务上保管了全球各核试验基地与核设施的卫星图像等数据。PCIA 官方尚未正式指责任何国家，但是此次攻击时机的选择令人怀疑。

不久前，朝鲜进行了核试验，在该国东北部丰溪里引爆了一颗一万吨的弹头，造成了 5.3 级地震。丰溪里也是 PCIA 项目监测的一个地点，其他的敏感地点有俄罗斯、伊朗、缅甸及其他国家。朝鲜不是唯一有可能发动攻击的国家。攻击发生 10 天前，PCIA 将俄罗斯新地岛核试验场添加到列表中。通过 PCIA 网站提供的功能可以进行查看，但是该页面至今没有加载任何卫星图像。(http://news.softpedia.com/)

一周简讯

- 研究人员发现全盘加密勒索软件新成员 Mamba
- 世界反兴奋剂机构疑因鱼叉式钓鱼邮件遭黑客入侵
- 漏洞预警 :Mysql 代码执行漏洞，可本地提权
- 报告称半数云应用恶意代码传播勒索软件
- 研究人员证明 NAND 镜像技术可破解 iPhone 密码
- 银行木马 Dridex 瞄准亚欧小国及企业银行部门
- 免费远控木马 Darktrack 或将成为主流 RAT

(安天 CERT 搜集整理，详见：http://bbs.antiy.cn)

每周安全事件

类 型	内 容
中文标题	土耳其黑客继续对奥地利政企发动单边网络攻击
英文标题	Turkish Hackers Continue to Pester Austrians in a One-Sided Cyber-War
作者及单位	Catalin Cimpanu；Softpedia
内容概述	近日，土耳其黑客组织 (Aslan Neferler Tim) 向奥地利政企发动新一轮服务拒绝式网络 (DoS) 攻击，此轮攻击的目标为奥地利国民银行 Austrian National Bank (OeNB)，黑客组织 Aslan Neferler Tim 事后发推声称对此攻击事件负责。 据悉新一轮针对奥地利国民银行的攻击并非 DDoS 攻击，黑客发动了每分高达 500 万封邮件的服务拒绝攻击，最终击垮了银行服务器。银行方面声称黑客没有获得任何访问客户数据的权限。
链接地址	http://news.softpedia.com/news/turkish-hackers-continue-to-pester-austrians-in-a-one-sided-cyber-war-508264.shtml

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 5 个 PC 平台的恶意代码值得关注

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.Socksbot.a[rmt，prv]2016-09-10	该应用程序运行会接收远程服务器发送的指令与远控服务器通过 socket 进行通讯，远控端可使用户设备变成 SOCKS 代理，这样远控端可通过用户设备访问设备所属内部网络从而窃取用户内网的隐私信息，造成用户隐私泄露。（威胁等级高）
		G-Ware/Android.RogAd.a[rog，exp]2016-09-11	该应用运行会加载释放广告子包，匿名弹窗插屏广告，广告界面难关掉而且可能在无意操作中就下载，具有流氓行为，建议卸载。（威胁等级低）
		Trojan/Android.vdsoft.a[prv，spr]2016-09-11	该应用伪装成系统应用 ConfigUpdat。点击后隐藏自身图标，收集用户短信、通话记录、联系人信息、书签等隐私信息并上传。向联系人群发包含恶意软件 picture.apk（自身）链接的短信。造成用户隐私泄露、资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.NzCopro.a[prv]2016-09-13	该应用监听手机 APP 安装消息，拦截未接短信，收集用户隐私信息，静默发送短信，造成用户隐私泄露、资费消耗，建议卸载。（威胁等级中）
		G-Ware/Android.siza.a[spr]2016-09-15	该应用程序伪装成人应用，诱骗用户点开运行，恶意推广恶意 url，建议直接卸载。（威胁等级低）
	较为活跃的样本	RiskWare/Android.FakeQQ.h[fra，exp]	该应用伪装成 QQ，实际上是一款私彩赌博的游戏，需要上传卡号和密码到服务器验证，请及时卸载以免造成隐私泄露和经济损失。（威胁等级低）
		G-Ware/Android.FakeApp.bm[rog，exp]	该应用无实际功能，程序运行会频繁推送广告诱骗用户下载，具有一定流氓行为，建议卸载。（威胁等级低）
		Trojan/Android.SmsSend.ki[spr，exp]	该应用程序运行时会遍历联系人并向之发送推广欺诈短信，同时向指定号码发送短信，这会造成资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.E4Aspy.aa[prv，fra，rmt]	该应用程序安装无图标，启动后点击会无提示发送短信，并删除信息，通过 ftp 上传至服务器，造成隐私泄漏，建议用户卸载。（威胁等级中）
		Trojan/Android.SmsThief.au[prv，exp]	该应用伪装成正常应用，运行后短信转发用户手机固件信息和短信，通过 FTP 上传用户短信，造成用户隐私泄露和资费损耗，请立即卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Cisco Adaptive Security Appliance SNMP 远程代码执行漏洞 (CVE-2016-6366)	Cisco Adaptive Security Appliance (ASA) Software 的 SNMP 代码存在安全漏洞。远程攻击者发送构造的 SNMP 数据包到受影响系统，可造成系统重载或远程执行任意代码。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.FraudLoad	此威胁是一种通过网络资源，如免费软件、共享软件及其他已感染应用等进行传播。该家族感染用户电脑后，会自动替换或删除重要文件，使系统崩溃。当用户打开某些程序时，会弹出“没有响应”或“因内存不足操作失败”等提示。该家族同时会在系统中删除或添加一些文件。（威胁等级中）
		Trojan/Win32.Sasfis	此威胁是一种可以通过恶意邮件及自动下载等方式入侵电脑。该家族运行后，会将自己注入进程中，以隐藏运，并会在电脑中下载很多文件。（威胁等级中）
		Trojan/Win32.Intervan	此威胁是一类运行后会在本地下载恶意软件并执行。该家族经常用来在电脑中安装木马和其它恶意软件，同时保护恶意应用程序不被反病毒软件检测到。（威胁等级中）
		Trojan[Backdoor]/Win32.DarkKomet	此威胁是一种通常通过垃圾邮件附件、恶意链接及网上的免费应用下载等方式传播。该木马会监控用户的行为，并为黑客打开系统后门，这会导致用户的信息被窃取。该木马会将窃取到的信息发送给黑客，同时该木马还可以下载其他恶意软件。（威胁等级高）

Libutils 漏洞追溯到 Stagefright

Michael Mimoso / 文　安天公益翻译小组 / 译

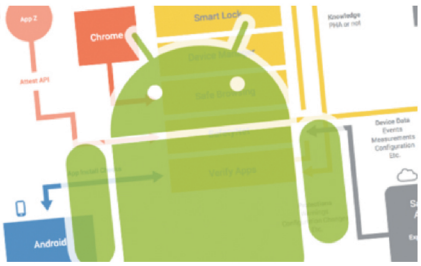
本周的安卓安全公告修复了威胁几乎所有安卓设备的漏洞，这说明安卓生态系统很脆弱。

该公告解决了 50 多个漏洞，其中 9 个因为远程代码执行的可能性被谷歌列为严重级别。首先，谷歌修复了高通芯片的两个 Quadrooter 漏洞，以及 jhead 库中一个可能被特制 JPEG 文件利用的严重漏洞。

谷歌的内部研究团队 Project Zero 如法炮制，在周三披露了 Libutils 的一个严重漏洞的详细信息，而该漏洞已在本周被修复。该漏洞让人回想起去年 10 月披露的第二个 Stagefright 漏洞，虽然它被公认难以利用，但是也能影响目前大多数安卓设备。就像 Stagefright 漏洞和安卓设备的 Mediaserver 组件一样，任何调用 Libutils 的应用程序都面临风险。

Zimperium 实验室的平台研究和开发副总裁约书亚·德雷克 (Joshua Drake) 指出："这类似于 Stagefright 2.0 漏洞，它涉及一个核心库，有很多不同的攻击向量。该漏洞涉及 libstagefright，它不是一个 Stagefright 漏洞，但是攻击向量涉及 libstagefright。"

谷歌研究员马克·布兰德 (Mark Brand) 发布了该漏洞的详细技术说明，以及围绕 Mediaserver 的概念验证漏洞利用。其他可能受影响的安卓应用程序包括 system_server，drmserver，keystore 和 SurfaceFlinger。



Duo Labs 安全研究主管史蒂夫·曼祖克 (Steve Manzuik) 表示："基本上，任何使用该库的应用程序都存在漏洞，目前尚不清楚有多少应用程序和服务使用这个库。但是在概念验证中，Mediaserver 用来演示该漏洞，当然它也是 Stagefright 的目标。目前看来，漏洞利用的难度中等。在现代安卓系统上，必须绕过地址空间格局随机化 (ASLR)。"

布兰德的报告说，Libutils 的漏洞代码在于 UTF-16 和 UTF-8 之间的转换。UTF-16 是 16 位的 Unicode 转换格式，能够编码所有可能的 Unicode 字符。

"这是一个非常严重的漏洞，因为漏洞代码路径可以从许多不同的攻击向量访问，它既可用于远程代码执行，也可用于本地权限提升 (提升到高权限 system_server SE Linux 域。"

布兰德说，他发现了 Libutils 和 UTF-16 的一个小问题，他可以借由此控制缓冲区分配和溢出的大小。

他还说，Mediaserver 是一个完美的远程漏洞利用攻击向量，其中 Unicode 转换在 ID3(译者注：一般是位于一个 mp3 文件的开头或末尾的若干字节内，附加了关于该 mp3 的歌手，标题，专辑名称，年代，风格等信息，该信息就被称为 ID3 信息。) 标签的处理过程中实现。例如，MP3 文件使用 ID3 标签描述音频文件的内容，例如歌曲标题，歌手姓名和其他元数据。

德雷克说：如果使用 Stagefright 库，就会通过 ID3 解析接触到该漏洞。Stagefright 使用存在该漏洞的 Unicode。"

布兰德指出，以前的 Stagefright 研究帮助他设计了一个会造成系统崩溃的概念验证。他说，绕过 ASLR 和其他减灾措施 (特别是在 Android-N 系统) 是更大的挑战。

布兰德说："Android-N 系统引入了很多强化措施，其结果非常不错。这并不是说，Android-N 系统上无法利用该漏洞，而是说完整的链条会更加复杂。"

最初的 Stagefright 研究促使研究者深入挖掘 Mediasever 数月的时间，而安卓安全公告包括了 Mediasever 中至关重要的远程代码执行漏洞。德雷克认为 Libutils 较小的代码库预示着另一个漏洞报告高峰。

德雷克说："我认为很多安卓代码过去没有获得足够的关注，现在获得了越来越多的关注。随着安卓奖励计划的发展，在不久的将来很多关键漏洞会被发现。"

原文名称	Patched Android Libutils Vulnerability Harkens Back to Stagefright
作者简介	Michael Mimoso，卡巴斯基《安全周报 (Threatpost)》编辑。
原文信息	2016 年 9 月 9 日发布于《安全周报 (Threatpost)》 原文地址 https://threatpost.com/patched-android-libutils-vulnerability-harkens-back-to-stagefright/120481/
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《Sakula 木马样本分析报告》

近日，安天追影小组在整理网络安全事件时，对 Sakula 木马家族系列样本进行了深入的逆向分析。Sakula 木马是典型的远程控制类型的木马，攻击者能够对被控端进行交互式命令执行控制，同时根据样本编译时的时间戳可知该木马在 2012 年至 2015 年均保持活跃状态。Sakula 木马传播方式主要通过使用 CVE-2014-0322 漏洞攻击来针对 web 服务器进行传播或者伪造正规厂商的数字签名来欺骗用户进行感染。在感染主机后使用 HTTP 协议进行通信，网络通信内容经过异或加密后传输，且通过注册表设置自启动以及设置恶意服务来维持对被控端的控制，还运用了 UAC 绕过技术来绕过 UAC 防护。

通过分析可知该样本由 Microsoft Visual Studio 平台编写，攻击对象主要针对 windows 系列平台，样本文件中的配置字符串、资源信息等敏感信息都经过简单的异或加密从而达到自我保护的目的。

感染时该 Sakula 木马样本通过修改注册表，针对 HKEY_LOCAL_MACHINE 中的 Run 键值篡改来设置恶意代码的自启动行为，然后释放木马文件 MediaCenter.exe 到系统 C:\WINDOWS\TEMP\MicroMedia\ 目录，同时调用 cmd 命令行执行加载 UAC 绕过模块 rundll.dll 来绕过系统 UAC 防护，最后利用 cmd 命令行进行隐藏自身和自删除行为。经分析该类样本的主要的功能模块包括针对感染主机的远程 cmdshell 访问控制模块、文件控制模块、上传下载模块、获取感染主机信息模块、自身卸载模块以及 C2 配置信息更新模块等。

通过对 Sakula 木马样本的分析，可以看到远控类木马样本的攻击仍然处于活跃状态，对于网络安全从业者来说不能够掉以轻心，针对家族类木马更要进行深入的剖析和研究，从中总结出合理的分析解决方案来维护用户安全。安天提醒电脑使用者：日常工作中要有网络威胁防范意识，在面对安全事件时及时寻求专业人员的帮助，同时对于企业来说对内部服务器要进行定期安全检测、加强运维人员的安全意识，使用正规软件防止恶意代码的感染。目前，该类样本已经能够被追影产品检出。

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、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、智能学习鉴定器、安全云鉴定器等鉴定分析。最终依据 BD 静态分析鉴定器、静态分析鉴定器、动态行为鉴定器、智能学习鉴定器将文件判定为木马程序。

该文件具有以下行为：删除自身、使用 cmd 删除自身、读取自身文件、自启动、连接特殊 URL、释放 PE 文件、增加 run 自启动项、获取系统内存、获取系统版本、打开自身进程文件、创建特定窗体、获取驱动器类型、独占打开文件、获取计算机名称、获取主机用户名称、查找指定内核模块、请求加载驱动的权限、疑似桌面控制。

文件名	F25CC334809BD1C36FD94184177DE8A4
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	320 KB
MD5	F25CC334809BD1C36FD94184177DE8A4
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Scar
判定依据	静态分析

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
删除自身	★★★★	使用 cmd 删除自身	★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
读取自身文件	★★	自启动	★
连接特殊 URL	★	释放 PE 文件	★
获取系统内存	★★	增加 run 自启动项	★
打开自身进程文件	★	获取系统版本	★★
获取驱动器类型	★	创建特定窗体	★
获取计算机名称	★	独占打开文件	★
查找指定内核模块	★	获取主机用户名称	★
请求加载驱动的权限	★	疑似桌面控制	★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=1D09000F9C7AF81D6EB8E5D4D7C5F139