安天周观察

主办：安天　2016 年 11 月 28 日（总第 66 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

全国人大代表一行莅临安天总部参观指导

11 月 22 日，全国人大代表一行在哈尔滨市政府相关人员的陪同下莅临安天总部参观考察，了解了安天的发展历史和近况，参观并听取了安天最近在技术创新和产品研发等方面的汇报，考察了安天安全威胁感知捕获体系和可视化平台。

参观中，安天负责人为人大代表一行详细介绍了安天的发展近况。目前，安天在安全检测引擎、移动安全、网络协议分析还原、动态分析、终端防护、虚拟化安全等方面形成了全能力链布局，监控预警能力覆盖全国、产品与服务辐射多个国家和地区。围绕安天的反病毒引擎核心技术，研发了探海流量检测系统、智甲终端防护系统、追影深度分析系统、镇关威胁阻断系统等针对于党政军和重要行业、企业的反 APT 高级威胁监测、防护产品和解决方案。近年来，安天率先深入分析了包括“APT-TOCS”、“白象”、“方程式”等多起 APT 攻击事件。

安天多次在重大网络事故和网络安全事件的响应中发挥关键作用，参与了国内重要会议和活动的网络安保工作，为十七大、十八大、2010 年起的历届两会、北京奥运会、上海世博会、广州亚运会、2014 年 APEC 会议、抗战胜利 70 周年阅兵、G20 峰会等会议保驾护航，并曾荣获重大活动信息安全保卫工作突出贡献奖。

人大代表一行对安天的工作表示认可。同时，他们也对安天提出了希望，希望安天能够继续精耕反病毒引擎技术，增强对安全威胁的全景关注能力，在技术领域创新、创造出更优异的成绩，以更优质的产品为国家网信大战略做出贡献。

安天参加 XDef2016 并发表演讲

11 月 21 日 -22 日，第五届全国网络与信息安全防护峰会 (XDef2016) 在武汉召开，来自全国各地的网络安全专家共同探讨了网络与信息安全防护的热点问题。

此次会议邀请了来自国家创新与发展战略研究会、公安部网络安全保卫局、教育部高等学校信息安全专业教学指导委员会、中国互联网协会网络与信息安全工作委员会等重点单位的多位领导莅临会议并发表特邀报告。来自国内多家网络安全企业的资深专家发表演讲。其中，安天实验室副总工、安全研究与应急处理中心（安天 CERT）负责人李柏松，发表了题为《从反恶意代码视角看关键基础设施防护》的专题报告。

报告从安天近年在“白象”、“乌克兰停电”、“方程式”等多起 APT 攻击事件中捕获和分析的恶意代码出发，分析 APT 攻击手段的变化规律，并对关键基础设施存在的安全问题作出深入解读。李柏松在报告中指出，针对关键信息系统的攻击与防御，不再是单点技术手段之间的简单博弈，需要采用体系化的防御思想，在网络流量侧检测能力、基于虚拟执行的深度分析能力、基于白名单 + 安全基线的终端防护能力以及针对云和虚拟化节点的防御能力等方面建立布防点，以日志数据聚合分析和事件重构汇集体系能力、以威胁情报共享汇集厂商能力，并以事件响应与取证分析作为支撑能力，建立全域融合防御体系，有效地对抗针对关键基础设施的高级网络安全威胁。

安天荣获哈尔滨市“示范性高技能人才（劳模）创新工作室”称号

11 月 23 日，在哈尔滨职工技术创新推进工作会议上，安天荣获“哈尔滨市示范性高技能人才（劳模）创新工作室”称号，李柏松代表安天做汇报发言。他表示，安天创新工作室经过长时间的探索研究，形成了党政工齐抓共管的网格化管理模式，围绕提升质量、提高效率、降低成本等方面做了大量扎实有效的尝试和探索，取得了较好效果。

安天创新工作室不仅为公众提供重大恶意代码和安全事件的应急响应服务，还多次参与重大活动的安保工作，其中有 9 名工程师获评奥运网络安保功臣。

最后，李柏松表示会把创新工作室真正建设成为安天人才的摇篮、创新的基地、研发的平台、示范的中心，为维护网络安全、为实现哈尔滨的全面振兴发展贡献安天人的智慧与力量。

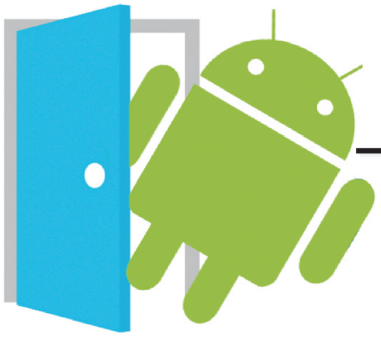
每周安全事件

类 型	内 容
中文标题	欧亚多家银行 ATM 取款机遭黑客攻击
英文标题	Cobalt Hackers Attack ATMs with Malware Forcing Them to Spit Out Cash
作者及单位	Bogdan Popa；Softpedia
内容概述	近日，网络攻击的消息接连不断，报道称有黑客攻击 ATM 机，使其不停向外吐钞票。俄罗斯的安全公司称黑客攻破了银行的内部系统，系统被恶意软件攻击之后，黑客可以控制位于欧洲和亚洲许多地区的的一大批 ATM 机。一旦成功，黑客们就可以继续攻击 ATM 机，使机器吐出其中的现金钞票。 安全调查员并未公布受攻击的具体银行名单，但他们称英国、俄罗斯、西班牙、波兰、荷兰、罗马尼亚、爱沙尼亚、亚美尼亚、保加利亚等国家的 ATM 机受到了攻击。 两家最大的取款机制造商 Diebold Nixdorf 和 NCR Corp 称他们已经发现了这一危险。
链接地址	http://news.softpedia.com/news/cobalt-hackers-attack-atms-with-malware-forcing-them-to-spit-out-cash-510412.shtml

每周值得关注的恶意代码信息

经安天检测分析，本周有 9 个移动平台恶意代码和 4 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	较为活跃样本	Trojan/Android.oxti.g[exp]	该应用程序运行后会隐藏图标，后台频繁访问色情网址，会造成用户的流量损耗。（威胁等级高）
		Trojan/Android.AutoSMS.l[pay，fra]	该应用伪装成微信程序，运行后隐藏图标，后台拦截指定短信，并删除指定短信，开通多种付费业务，具有窃取用户 ID 号、imei 号，手机固件信息等行为。会造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.E4AQQspy.k[prv]	该应用伪装成 QQ 辅助工具，运行后会诱导用户输入 QQ 账号和密码，并联网上传，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.emial.dm[rmt，prv，exp]	该应用会伪装成正常应用，运行后会激活设备管理器，隐藏图标。在后台接收短信指令，完成拨打电话、拦截转发短信等操作。通过邮箱发送用户短信内容和手机号码，会造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
		PornWare/Android.GSexplayer.ad[exp，rog]	该类应用为色情播放器程序，运行后会有诱惑性内容诱导用户付费。请注意提示信息，建议使用健康绿色软件。（威胁等级中）
		G-Ware/Android.HiddenAds.ak[rog，exp]	该应用伪装成屏保图片，安装后无图标显示，运行后会弹出广告，在后台下载安装未知应用，同时收集并上传用户固件、已安装程序等隐私信息，会造成用户隐私泄露、资费消耗，建议卸载。（威胁等级低）
		Trojan/Android.Downloader.cq[exp]	该应用安装后无图标显示，运行后会收集用户固件和通话记录等隐私信息，并联网下载未知应用。会造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.simplelock.q[rog，sys]	该应用运行后会隐藏图标，并请求激活设备管理器，利用强制置顶界面来勒索用户通过银行卡付费解锁，会造成用户手机无法正常使用。（威胁等级高）
	新出现的样本家族	Trojan/Android.SmsThief.ay[prv，exp]	该程序会伪装安全应用，运行后隐藏图标，会私自发送短信到指定号码，窃取用户短信息内容，造成用户隐私泄露资费消耗，建议立即卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 系统提权漏洞 CVE-2016-7255	Microsoft Windows 的 CVE-2016-7255 漏洞。如果 Windows 内核模式驱动程序无法正确处理内存中对象，则会存在多个特权提升漏洞。成功利用此漏洞的攻击者可以在内核模式下运行任意代码。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[Banker]/Win32.Banaris	此威胁是一种以窃取网络银行敏感信息为目的的木马类程序。该病毒会伪装成正常数据，以获取认证。该病毒利用各种途径，使黑客获得数字证书来伪造文件。该家族还会收集用户的机密信息，如网上银行详细信息和密码等，并将窃取的数据远程发送给黑客。（威胁等级高）
		Trojan[Banker]/Win32.Banaris	此威胁是一种木马类程序。该家族善于将恶意文件注入用户电脑，破坏安全系统，使电脑很容易受到远程黑客的攻击。该家族通过下载免费软件、点击恶意链接、收取垃圾邮件等方式传播。（威胁等级中）
		Trojan[Ransom]/Win32.Cryptor	此威胁是一种可以加密用户文件并勒索赎金的木马家族。该家族样本运行后遍历系统磁盘并加密文件，会向用户勒索赎金以解密，有一定威胁。（威胁等级低）



一些安卓设备的固件中发现后门

Chris Brook / 文　安天公益翻译小组 / 译

近日，近三百万台安卓设备存在漏洞，该漏洞使黑客能够感染设备的无线 (OTA) 更新，用 root 权限远程执行命令。

这个问题来源于研究人员所说的“OTA 机制的不安全实施”，用于与 Ragentek Group 制造的软件相关的更新。

Anubis Networks 的研究人员在近期公布了这个问题，他们指出，相关二进制文件的通道上的通信未加密，这为中间人攻击打开了大门。

Anubis Networks 的研究人员 Dan Dahlberg 和 Tiago Pereira 在近期公布了这个漏洞。他们说：“从二进制文件到第三方端点的所有事务都通过未加密的通道进行，这不仅在通信期间暴露了用户的信息，同时允许攻击者发出协议支持的命令，其中的一个命令会允许攻击者执行系统命令。”

该公司的研究人员称，涵盖 55 个不同型号的 280 万台安卓设备存在该二进制文件漏洞。

几天前，当 CERT(软件工程研究所的一个部门) 在其漏洞注释数据库中警告了这个问题，它指出，Ragentek 的代码的行为类似于 rootkit，因为该二进制文件以 root 权限运行并且未加密。CERT 补充说，这使得攻击者很容易在设备上安装应用程序或更新配置，以及执行任意命令。

根据 CERT 的警告，存在漏洞的二进制文件大多发现在低成本设备中，包括由 BLU Studio，Infinix，DOOGEE 和 LEAGOO 制造的设备。研究人员声称，他们从百思买购买了其中一个测试的设备 BLU Studio G，指出该问题影响了现成的设备。

Anubis Networks 表示，它与 BLU (受该二进制文件影响最严重的供应商)，Google 和 CERT 一起报告该问题并警告供应商。

该公司的研究人员意识到，除了 Ragentek 的域，这些设备还试图联系两个域，直到这时他们才了解该问题的全部内容。直到 Anubis 发现并购买了这些域，它们才被注册。Dahlberg 和 Pereira 在介绍该问题时警告说，如果攻击者了解并购买了这些域，他们就可以自由控制将近三百万设备，甚至不需要执行中间人攻击。

近期，Kryptowire 的研究人员说，有科技公司生产的手机在未经用户同意或知情的情况下传输个人身份信息。该固件使用随某些设备 (如 BLU R1 HD 手机) 附带的 OTA 更新系统来监控用户。用户的数据，在某些情况下用户的短信信息和通话记录，会被转发到该公司的服务器上。CERT 指出，位于佛罗里达州迈阿密的手机制造商 BLU Products 修复了 Anubis Networks 发现的问题。BLU Products 的首席执行官 Samuel Ohev-Zion 在给《纽约时报》的简报中称，其公司的 12 万部手机受到了该问题的影响，表示未来的更新将修复这一问题。

除了 BLU，其余的供应商尚未就此问题发布声明。

原文名称	Backdoor Found in Firmware of Some Android Devices
作者简介	Chris Brook，卡巴斯基《安全周报》副编辑。
原文信息	2016 年 11 月 21 日发布于《安全周报》(Threatpost) 原文地址 https://threatpost.com/backdoor-found-in-firmware-of-some-android-devices/122075/
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《Mayday 家族样本分析报告》

近日，经过安天追影小组对 Trojan[DDoS]/Linux.Mayday 家族的分析监控，获知该家族的最近两次攻击活跃时间，并监控到 Mayday 家族参与了 2016 年 10 月的 Dyn 攻击。该家族样本最早版本在 2013 年末就已经出现，到现在已经衍生 8 个版本。开始从样本硬编码 IP 类型的 C2，过渡到通过域名查询获取动态 C2 的 IP。

尽管 Mayday 家族的版本一直在衍生和完善，但其通信协议等基本框架并没有变，DDoS 攻击类型也基本没有变化，主要包括：dns flood，tcp flood，udp flood，cc flood，icmp flood 这几种攻击方式。通过对 Mayday 家族样本分析比较，发现虽然样本在常驻“肉鸡”——样本备份和自启动方面仍有完善的空间，但是样本的模块封装十分完善，条理清晰，这也是家族版本能快速衍生的原因之一。其中主要封装的 CTaskInfo（指令任务处理）模块（类），CManager（消息处理）模块，CNetBase（网络处理）模块，CServerIP（与 CNC 数据交互）模块，CStatBase（状态信息 – 或许系统版本配置等信息）模块。

通过长期监控获知，Mayday 家族的僵尸网络控制节点主要分布于国内，也有相当一部分分布于美国，而国内的主要分布于东部沿海的省份，集中于苏浙两省。Mayday DDoS 在近两个月中，相对比较活跃的周期为 9 月中旬 –10 月上旬、11 月 5 日 –11 月 10 日，两个周期中都有 5W+ 次攻击目标。其中 11 月 5 日 –11 月 10 日是一个井喷式爆发期，每天有 20W+ 次攻击目标，发动攻击控制节点主要分布于美国，且攻击目标也集中于美国。在 Mayday DDoS 沉默期间，还监控到 Mayday DDoS 也参与 10 月下旬对美国 Dyn 的 DDoS 攻击，根据僵尸控制节点量预计攻击流量贡献达 80G+。

Mayday 发展至今已是 Linux x86 僵尸网络的常见家族，该家族的出现并快速遍布于互联网，严重影响互联网的安全健康发展，损坏了广大网民安全利益，损耗互联网及设备资源。经过安天追影小组的长期监控与跟踪，从目前掌握的情况看，Mayday 家族目前还没有样本备份和自启动，因此，如果计算机被植入 Mayday 家族只需要删除样本并重新启动即可。

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、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 静态分析鉴定器将文件判定为木马程序。

该文件具有以下行为：疑似 DDOS 攻击、获取系统配置信息。

文件名	F626DDF162DEC2F8B097AFFF91BD5564
文件类型	BinExecute/Linux.ELF
大小	1.08 MB
MD5	F626DDF162DEC2F8B097AFFF91BD5564
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Mayday
判定依据	BD 静态分析

◆ 运行环境

操作系统	中标麒麟
内置软件	默认

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
疑似 DDOS 攻击	★★★★	获取系统配置信息	★★★

◆ EXIF 信息

描述	值	描述	值
File Size	1102 kB	File Type	ELF executable
MIME Type	application/octet-stream	CPU Architecture	32 bit
CPU Byte Order	Little endian	Object File Type	Executable file
CPU Type	i386		

报告地址：https://antiy.pta.center/_lk/details.html?hash=F626DDF162DEC2F8B097AFFF91BD5564