安天周观察

主办：安天　2016 年 1 月 4 日 (总第 23 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

中国网络安全产业联盟（筹）成立 安天当选常务理事单位

2015 年 12 月 29 日，由中央网信办指导的中国网络安全产业联盟在北京宣布成立。中央网信办副主任王秀军到场并致辞，安天作为常务理事单位出席了本次成立大会。

联盟作为由中国网络安全行业的代表性企业自愿联合、共同发起组建的非营利性组织，包括 1 家理事单位，8 家常务理事单位，23 家理事单位和 145 家会员单位，涉及网络安全各细分领域。旨在营造良好的网络安全产业发展环境，保障中国国家网络安全和用户利益，推动网络安全产业做大做强。

在会议上，王秀军副主任表示，我们要充分认识面临的网络安全形势和做好网络安全工作重要性、紧迫性，加强网络安全技术攻关，培育网络安全产业，提升网络安全防护能力，切实维护好网络安全。要树立全球视野和开放心态，抓住信息技术革命带来的历史性机遇；充分发挥联盟平台和桥梁作用，促进产业协同发展，多向主管部门建言献策，做大做强网络安全产业。据悉，联盟近期将重点围绕推进网络安全产业环境改善、共同开拓海外市场、提升网络安全产业竞争力等方面开展工作。

安天中标海关总署信息安全产品采购项目

近日，安天成功中标“海关总署 2015 年金关工程二期信息安全产品 (六) 采购项目”02 包，中标的产品为高级持续性威胁 (APT) 检测设备。海关总署作为国家重要的进出境监督管理机关，统一管理全国海关，是国内较早信息化的部门，已实现了高度的办公自动化、无纸化。既涉及国计民生又接触海量信息的特点，使海关总署容易成为高级可持续性威胁 (APT) 重点攻击的目标。

特别是近几年，手机、平板电脑等移动计算设备的引入，对其安全防护和威胁检测提出了更大的挑战。安天针对海关总署网络面临的威胁提供全面的威胁检测和分析解决方案，使网络在加快威胁响应速度、应对 APT 事件及时止损、安全事件追踪、提升检测深度等方面的能力得到大幅度提升。

安天在反 APT 的一线战斗多年，积累了丰富的经验，同时拥有长达十五年反恶意代码研究的深厚技术底蕴。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、服务器和移动终端达成部署。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，帮助用户“看见”威胁，并认清威胁，让高级威胁无所遁形。

安天中标 2016 中央政府采购项目

近日，中央国家机关政府集中采购，2016 年信息类产品协议供货采购项目中标公告发布。经过项目评审委员会严格审核，安天网络安全产品，镇关威胁阻断系统 PTF 成功入围本年度中央政府采购目录，使安天成为中央国家机关各级行政事业单位的供应商之一。

中央国家机关采购协议供货是目前我国级别最高的政府采购项目，可综合体现出各大供应商的信誉、产品品质、性价比和服务等多方面能力。安天此次成功中标入围，意味着中央政府和行业专家对其产品的肯定。

每周安全事件

类 型	内 容
中文标题	欧洲信用卡终端协议漏洞允许提取卡的磁条数据和密码
英文标题	European Credit Card Terminals Are Plagued with Serious Vulnerabilities
作者及单位	Joseph Cox，Motherboard
内容概述	当美国准备为信用卡交易更换芯片密码模型时，欧洲一直在幸福地使用着更安全的用于个人交易的方法。但欧洲的方法其实存在很严重的问题，发现它们也只是迟早的事。近日德国新闻节目 Tagesschau 表示，研究者们将会详细地展示欧洲支付终端（在输入一个四位数密码之前，用户进行卡片插入的设备）的一些漏洞和设计缺陷。这些漏洞可能会被黑客利用来窃取受害者的 PIN 码和磁条卡，甚至伪装成终端，将资金发送到德国的任何一个银行账户上。也有人担心这些漏洞可能会影响到其他欧洲国家的系统。
链接地址	http://motherboard.vice.com/read/european-card-terminals-are-plagued-with-serious-vulnerabilities

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 5 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.ITracker.a[prv，exp] 2015-12-23	该应用伪装成系统应用，安装无图标，后台接收短信指令，获取用户地理位置信息并通过短信发送，造成用户隐私泄露，建议卸载。（威胁等级高）
		G-Ware/Android.dqfsll.a[rog，exp] 2015-12-24	该应用安装无图标，开机自启动，包含拦截短信，发送订阅、点播等扣费服务短信，可能造成用户资费消耗。（威胁等级中）
		G-Ware/Android.sppromo.a[rog，exp] 2015-12-24	该应用伪装成其他应用，运行时加载浏览器访问博彩、交友等网站，还会诱骗用户下载未知应用，会造成用户资费损耗，请谨慎使用。（威胁等级低）
		Trojan/Android.smsremote.a[prv，fra，spy]2015-12-25	该应用程序为一款间谍类软件，伪装成系统程序，运行需要配置手机号码邮箱地址信息，后台联网会上传手机收件箱、通讯录内容，还含有反馈跟换 sim 卡信息和隐藏桌面图标的功能，若非本人安装，请及时卸载。（威胁等级中）
		G-Ware/Android.BBSDKSer.a[rog，exp]2015-12-25	该应用运行时会联网获取数据解密资源文件，加载其他恶意应用和大量广告，激活设备管理器，锁定屏幕使用户无法正常操作，会造成用户资费损耗，建议卸载。（威胁等级低）
		Trojan/Android.remark.a[prv，fra，exp] 2015-12-25	该应用伪装成正常应用，诱导用户输入身份证、银行卡号、联系人信息和手机号码等隐私信息并联网上传；后台监听拦截特定短信并上传短信，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
	较为活跃的样本	G-Ware/Android.HiddenAds.i[rog，exp，prv]	该应用伪装成系统应用，安装无图标，私自联网上传用户设备相关信息，私自联网下载推送广告应用，还能静默安装和静默卸载，具有一定的流氓行为以及可造成用户资费消耗。（威胁等级低）
		Trojan/Android.InfoStealer.r[prv，exp]	该应用安装无图标，运行后会获取手机固件信息和手机号码并联网上传，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.SmsThief.y[prv，fra]	该应用伪装成正常应用，运行后隐藏图标；通过短信转发用户手机固件信息和拦截的短信内容并删除短信记录，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.FakeFlashPlayer.j[prv，fra，rog]	该应用伪装成 flash 插件，运行后激活设备管理器，隐藏图标，取消激活设备管理器则会强制锁定用户界面；获取收件箱信息并用短信转发；后台获取固件信息和手机号码并上传，可能会加载网页，诱导用户输入谷歌账号和密码，造成用户隐私泄露，建议不要安装使用。（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 Outlook 爆严重漏洞，可允许远程代码执行 Microsoft Office RCE 漏洞 -CVE-2015-6172	当 Microsoft Outlook 分析经特殊设计的电子邮件时，存在远程执行代码漏洞。成功利用此漏洞的攻击者可以登录用户身份运行任意代码，并完全控制受影响的系统。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[Backdoor]/Win32.DDOS.de	此威胁是一种后门木马类程序，它可以连接远程服务器接受攻击者恶意操作，主要包括 DDOS 攻击和升级下载等功能。（威胁等级中）
		Trojan[Downloader]/Win32.XorCalc.jb	此威胁是一种具有下载行为的木马类程序。运行后会释放可执行文件；访问远程服务器，下载其他恶意可执行程序；添加注册表信息，并添加计划任务，用来执行恶意程序。（威胁等级中）
		Trojan/Win32.Winlagons.fs	此威胁是一种木马类程序。运行后会劫持浏览器，使用户访问黑客指定网站下载恶意程序。通过不断下载恶意程序到被感染计算机中，使系统无法承受巨大的资源占用，导致系统崩溃。（威胁等级中）
		GrayWare[AdWare]/WinLNK.Clicker.ur	此威胁是一种灰色软件类广告程序。可以弹出大量广告信息，并在被感染计算机上下载其他病毒。侦听黑客指令，连接指定站点，弹出大量广告条幅，用户一旦点击带毒广告，立即在用户计算机上安装其他病毒。（威胁等级中）

政府手机监控设备的机密目录

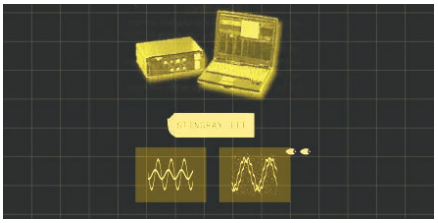
Jeremy Scahill，Margot Williams/ 文　安天公益翻译小组 / 译

近日，The Intercept(《拦截者》) 获得了一份机密的美国政府目录文件，该文件包含美国军事和情报机构使用的几十个手机监控设备，同时包含很多之前未被公开的信息，介绍了联邦执法机构和美国警察的间谍能力。

该目录包括知名监视设备品牌 Stingray、波音“污物箱”和几十个比较模糊的设备的详细信息，这些设备可以安装在车辆、无人机和战斗机上。一些设备用于静态位置，而另一些则可以随身携带。它们拥有诸如 Cyberhawk，Yellowstone，Blackfin，Maximus，Cyclone 和 Spartacus 的名字。在目录中，NSA(美国国家安全局) 被列为一个设备的供应商，另外，有的设备是为 CIA(美国中央情报局) 开发的，有的则是为特种部队开发的。近三分之一的条目涉及之前似乎从未被公开的设备。

一位担心国内执法军事化的情报界线人向 The Intercept 提供了该目录。其中几个设备可以涵盖多达 10，000 个唯一电话标识符的“目标清单”。大多数设备可用于定位用户，但是文件表明，一些设备具有更高级的功能，如窃听通话和窥探短信。据称，针对被捕手机设计的两个系统能够提取媒体文件、地址簿和笔记，其中一个可以检索删除的短信。

目录中的许多设备，包括 Stingray 和污物箱，是蜂窝基站仿真器，它们通过模仿大型电信公司的信号塔进行操作。当一个人的电话连接到伪造的网络时，它会发



送唯一识别码 (根据无线信号的特征) 和手机的位置信息。也有迹象表明，蜂窝基站仿真器或许可以监控通话和短信。

在该目录中，随每个设备列出了有关如何批准其使用的指南；答案通常是通过“地面部队指挥官”，或使用管理军事和情报行动 (包括秘密行动) 的两个美国代码之一。但是在国内，这些设备的使用违反了宪法规定的公民权利，包括《宪法第四修正案》(禁止非法搜查和扣押)。它们经常在无搜查令或者称为过于宽泛的搜查令的情况下使用。法官和公民自由团体抱怨说，这些设备的使用细节未被公开，甚至在法庭诉讼中也是如此。

蜂窝基站模拟器的原型 Stingray 由哈里斯公司在 2003 年注册商标，最初由军事、情报机构和联邦执法机构使用。另一家公司 Digital Receiver Technology(目前由波音公司拥有) 开发了污物箱，这是一种更强大的蜂窝基站模拟器，获得了 NSA、CIA 和美国军方的青睐，是追捕恐怖分子嫌疑人的好工具。据报道，与 Stingray 相比，该设备可以在更广的范围内追踪超过 200 部手机。

“蜂窝基站模拟器的保密是完全没有道理和不合法的”，电子前沿基金会的林奇说，“任何警官或侦探都不应向法院或被告人隐瞒如何进行调查刑事的信息。”法官们是终结蜂窝基站模拟器保密的最重要的倡导者之一，他们提出的方法包括获得搜查令。有时，警方试图隐瞒在刑事案件中使用了 Stingray，迫使法官提供通过设备获得的证据。

9 月份，美国司法部发布了使用 Stingray 和类似设备的指南，指出，联邦执法机构必须根据“确实缘由”获得搜查令后才能使用这些设备，而且必须删除获取的无辜者的任何数据。然而，该指南中的一个条款颇为模糊：在“特殊情况”下，联邦机构不必根据“确实缘由”获得搜查令。美国公民自由联盟、电子前言基金会和一些国会重要成员也表示，联邦政府的“特殊情况”过于宽泛，敞开了滥用的大门。

“由于蜂窝基站模拟器可以收集很多无辜者的大量信息，简单的获取搜查令也是不够的。”电子前言基金会的律师林奇说，“应该限制警官对此类设备的使用，在规定的时间段内使用。在提供搜查令的‘确实缘由’时，官员还需要说明设备的功能。”

美国公民自由联盟和电子前言基金会认为，公众有权检查设备 (激发对具有潜在深远影响的技术的辩论) 的类型。韦斯勒说，The Intercept 获得的目录“填补了一个很重要的空白。执法机构应该义不容辞地说明他们所使用的监控设备，以及如何保护《第四修正案》规定的隐私权。”

原文名称	A Secret Catalogue of Government Gear for Spying on Your Cellphone
作者简介	Jeremy Scahill 是 The Intercept 的三位创始编辑之一，是一位调查记者、战地记者和作家。
原文信息	2015 年 12 月 18 日《The Intercept》 原文地址 https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/
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《盗取过期签名的 DDoS 样本分析报告》

近日，安天追影小组在分析样本的过程中发现了一款带有过期签名的 DDoS 恶意程序。其盗用的数字签名属于韩国 NHN 公司美国分公司，主要目的是为了躲避杀软检测。为了搜索网络犯罪证据，获取恶意代码和作者的来源，追影小组进行了基于安天实验室两款产品追影威胁分析系统 (PTA) 和探海威胁检测系统 (PTD) 的恶意代码分析与追踪。发现样本存在多种恶意行为，属于远程控制木马，主要目的是控制用户计算机，窃取用户私密信息，损害计算机系统等。

通过样本分析可以发现，此 DLL 样本的功能大部分都是跟 DDoS 相关的。而且其每次获取的攻击目标都是从指定的域名上动态获取到的。再结合种马，从规模上来说，就属于分布式的 DDoS 了。在用户感染此样本后，就会充当其中的一台 DDoS 肉鸡，还会面临一些敏感数据泄漏，恶意程序安装，Hosts 被修改造成钓鱼劫持，网络性能低下等影响，具有极强的危害性。

由 PTD 查询结果表明，该样本活跃时间约为 2015 年 11 月 3 日至 2015 年 11 月 28 日。目前，该 DDoS 样本仍处于极度活跃状态，根据定时 (时间间隔为半小时) 投递 PTA 分析报告显示，仅仅在一天内，就有数十家网站疑似遭到 DDoS 攻击，主要为国内的一些在线销售减肥药网站、在线赌博网站、电子交易平台等。由报告结果同时可知，该样本攻击行为的触发时间大部分为 10 点至 22 点，正好处于各网站访问量较多的时间段，在这个时间段遭受到 DDoS 攻击，会对网站运营造成巨大影响与损失。

通过对黑客的追踪，追影小组发现攻击者使用 fabao.309420.com:7002 作为 C&C 服务器，分发 DDoS 攻击任务，并可实现简单的远程控制。域名所有者名为 WU YUAN，注册邮箱为 wu_yuan@163.com，常活动地区为广东广西。目的可能是敲诈或者同业竞争。

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、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、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。

该文件具有以下行为：使用 cmd 删除自身；访问 DNS；访问文件尾部；创建服务；获取计算机名称；更新服务配置信息；释放 PE 文件；获取驱动器类型；文档篡改；独占打开文件；结束进程；连接网络；启动服务。

同时，该文件会对虚拟机、沙箱技术进行检测。

文件名	B8F83B1E12AC61D8045A44561C5B7863
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	327 KB
MD5	B8F83B1E12AC61D8045A44561C5B7863
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Win32.DDOS
判定依据	安全云

◆ 危险行为

行为描述	危险等级
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
访问 DNS	★	访问文件尾部	★
获取计算机名称	★	创建服务	★
释放 PE 文件	★	更新服务配置信息	★
文档篡改	★★	获取驱动器类型	★
独占打开文件	★	结束进程	★★
启动服务	★	连接网络	★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=B8F83B1E12AC61D8045A44561C5B7863