安天周观察

主办：安天　2015 年 10 月 12 日（总第 11 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加 2015 中国互联网安全大会

安天参加了 9 月 29 日 -30 日在北京国家会议中心召开的 2015 中国互联网安全大会 (ISC2015)。安天在此次会议中设立了展位，现场发放技术文章汇编和最新版病毒通缉令，吸引了安全爱好者的关注。29 日下午，安天在两场分论坛中做了主题演讲。

其中，在“数据驱动安全之 APT 与新威胁论坛”上，安天副总工李柏松就《网络安全威胁中的商业军火》进行了主题演讲，报告从 hacking team 说起，从传统 PC 平台和新兴移动平台两个方面，结合具体案例，介绍商业化攻击平台的应用现状，最后综合考虑实施成本、实施效果等多方面因素，讨论如何应对商业化攻击平台带来的网络安全威胁。

在智能移动终端攻防论坛上，安天武汉移动安全公司潘宣辰就《移动反病毒工程化体系中的降维思维》进行了主题演讲。提出移动恶意代码的数量增长，技术升级和对抗博弈的背后是攻击者和防御者的全面对抗。报告结合过去 5 年，移动反病毒引擎和工程化体系从无到有的建设过程中的经验和体会，分享如何在移动恶意代码对抗中的通过降维的方法进行高效的系统性对抗。

斯诺登泄露：英政府记录全球互联网数据

近日，外媒援引美国国家安全局 (NSA) 举报人 Edward Snowden 泄露的情报文件称，英国监听机构国家通信情报局 (GCHQ) 正在进行一个称为“Karma Police”的项目，一直记录全球用户的互联网流量数据。该项目由 GCHQ 主导，为监测罪犯和恐怖分子的上网习惯他们建立了一个收集全球互联网用户在线活动的数据库。根据该文件显示，GCHQ 已经非法在其庞大的数据中心记录了全球互联网用户的网络流量，对用户连接到网络上的历史记录及社交网络活动等进行记录。（文章来源 http://en.egg-life.net/article/111164）

【安天 CERT】发布《疯狂的窃密者——TEPFER》报告（第四版）

文评

我们向屠呦呦先生学什么？

国庆长假最为振奋人心的消息当属：屠呦呦先生获得诺贝尔生理或医学奖。获奖消息传出，我们看到欣喜，看到祝贺，而更多的则看到的是带有各种固有情绪、预设立场的借题发挥与借势表达，一切事件和人物仿佛都沦为了各种观点 PK 碰撞的场景和道具。在这种喧嚣中，最质朴的声音反而被压制了——那就是思考屠先生为何能取得这样的成就。在这个信仰凋零，榜样被冷落的时代，作为网络安全厂商，我们在向屠先生致敬的同时，更要思考“我们该向屠先生学习什么”。

屠先生最优秀、为世界肯定的的研究工作完成于历史环境极为恶劣的“文革”时期，实验器材，参考资料极为匮乏，科研工作受到很多干扰。根据媒体报道“屠呦呦只好自己动手，从市场上买来 7 口大缸，在缺乏通风设备的陋室里，用挥发性很强、具有一定毒性的药剂浸泡、提取青蒿的精华。”在那篇集体署名《一种新型的倍半萜内酯——青蒿素》的论文中，曾提及应用傅立叶综合法做电子密度函数逼近，而有网友感叹，在没有电子计算机和建模软件的情况，这是多么艰难的工作。在历经 380 多次实验，190 多个样品，2000 多张卡片的尝试中，她自己也坦言，怀疑自己的路是否走对，而仍在坚持并不曾放弃；而从“青蒿一握，以水二升渍，绞取汁，尽服之”对低温萃取的灵感提示，看似顺理成章，但屠先生和研究集体对之前对其他大量无效“验方”排除与试错的结果。而面对提取物可能有毒的猜疑，她更是大胆的亲身试药。她的工作既有鉴定的当下目标又兼具长远价值，这项在经年累月中寻找突破和进展的事业拯救了很多人的生命。饶毅在对屠呦呦科研工作的评价中有一句话非常的中肯，“他们有才能，但并非才华出众，而是以自己的能力，在合适的工作上，认真做好工作，做出了重要发现。”这就是我们面对一切科学探索工作的前提，需要全心投入，需要踏实、认真与坚持。

（下转第三版）

每周安全事件

类 型	内 容
中文标题	新型的 DDoS 攻击：来自智能手机浏览器
英文标题	New DDoS attack uses smartphone browsers to flood site with 4.5bn requests
作者及单位	Liam Tung，ZDNet
内容概述	安全专家近日发现，智能手机浏览器也能产生流量巨大的泛洪攻击。发现来自手机端浏览器发起的 DDOS 攻击。安全专家分析称，一个移动广告网络已经可以控制将成千上万的手机浏览器同时指向在一个网站，使这个网站服务器宕机，从而达到分布式拒绝服务攻击的目的。据 DDOS 防护服务商 CloudFlare 所述，从监测的数据中发现他们一个客户的网站在几个小时内就收到 45 亿次的页面请求，而经过解析发起页面请求的源 IP 地址和对象，发现是来自具有中国 IP 地址的手机浏览器。
链接地址	http://www.zdnet.com/article/new-ddos-attack-uses-smartphone-browsers-to-flood-site-with-4-5bn-requests/#ftag=RSSbaffb68

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周 6 个移动平台和 9 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.PornClk 2015-9-24	该应用伪装成色情应用，运行后会自动隐藏图标。后台加载广告，联网下载 apk 推广成人购物网址，可能会私自发送订阅短信。(威胁等级低)
		Trojan/Android.dealapp 2015-9-26	该应用运行时会隐藏图标，获取手机 root 权限，拦截指定短信，获取短信信息，通话信息联系人信息，地理位置，发送到指定号码等。(威胁等级中)
		GrayWare[AdWare]/Android.Leapp 2015-10-02	这是乐盟广告件，采用 ImageView 方式弹出广告，静默下载推广应用，给用户造成资费消耗。(威胁等级中)
		Trojan/Android.Chathook 2015-10-03	该应用安装会申请 root 权限，Hook 相关聊天界面，获取用户 QQ 和微信聊天信息并上传远程服务器，造成用户隐私泄露。(威胁等级高)
		Trojan[SMS]/Android.Fakeinst 2015-10-04	俄罗斯的程序，伪装成其他程序的安装程序，运行后在后台向指定号码发送扣费短信，造成用户被恶意扣费。(威胁等级高)
	较为活跃的样本	RiskWare[RiskTool]/Android.SmsPay.k	该类应用包含支付插件，运行后会诱导用户进行付费。此外，还会联网弹通知栏推送应用、创建桌面快捷方式，诱导用户点击下载推广等行为，请注意提示信息，按需使用。
PC 平台恶意代码	新出现的 0day	WinRAR 5.21 – (Expired Notification) OLE 远程命令执行漏洞 2015-10-01	攻击者可利用该漏洞实施中间人攻击，执行任意代码。(威胁等级高)
		Truecrypt 7 / VeraCrypt 1.13-Drive Letter Symbolic Link Creation Privilege Escalation Exploit CVE-2015-7358 2015-10-05	攻击者能够控制一个受限的用户账户，可以利用这个安全漏洞在系统中进行提权。(威胁等级高)
	重要的恶意代码相关事件样本	Trojan[PSW]/Win32.Tepfer 2015-9-27	Tepfer 家族以窃取 FTP、邮箱、网站、比特币等账号和密码为目的。通过自带密码表尝试破解系统开机密码并辅助用来破解 chrome 浏览器缓存的网站登陆账号、密码信息；通过 .dat 文件窃取比特币信息。(威胁等级中)
	活跃的格式文档漏洞、0day 漏洞	CVE-2012-1856 又称“MSCOMCTL.OCX RCE 漏洞”	在 MSCOMCTL.OCX 中的 Common Controls 内的 TabStrip ActiveX 控件中存在漏洞。远程攻击者可利用该漏洞通过特制的文档或 web 页面，触发系统状态破坏，执行任意代码。(威胁等级中)
	新出现的样本家族	Trojan[Downloader]/Win32.InstallHide 2015-09-24	此威胁是一类可以释放其他恶意代码的木马家族。该家族样本运行后释放 VBS 脚本，收集用户系统信息，包括计算机名、操作系统版本、登录用户名，并有自删除行为。(威胁等级低)
		Trojan[Backdoor]/Win32.Miniduke 2015-9-25	此威胁是一类 APT 事件中所命名的木马家族。该家族样本可以在用户机器上建立后门，攻击者可以远程控制用户机器，如复制文件、删除文件、结束进程等。(威胁等级中)
		Trojan/Win32.Sakelua 2015-9-27	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后调用 IE 打开网页，在后台会开启另外一个进程连接 C&C 服务器，可以收集用户信息并回传。(威胁等级中)
	较为活跃的样本	GrayWare[AdWare]/Win32.OutBrowse.heur	该威胁是一种具有下载行为的恶意风险类程序。该类家族的通常使用 NSIS 打包，可以浏览用户的输出信息。
		GrayWare[AdWare]/Win32.MultiPlug.heur	该威胁是一种灰色软件类程序。具有反虚拟机、反调试功能，运行会添加自启动项，会弹出广告，具有一定风险。

为什么很难起诉 NSA ？必须证明它在窥探你

Andy Greenberg / 文　　安天公益翻译小组 / 译

想要通过诉讼解除美国秘密监控项目实施的监控，必须证明自己的隐私权受到了侵犯，而这种证明总是陷入两难境地。

几年前，爱德华·斯诺登披露 NSA 利用《爱国者法案》收集任何美国人的元数据之后，一个由宪法律师和保守派活动家拉里·克莱曼领导的原告团队状告奥巴马政府侵犯了《第四修正案》赋予他的隐私权。2013 年，一个低级法院批准了他的强制令请求，勒令 NSA 停止监控其数据。但是奥巴马政府驳回了这一裁决，因为原告无法提供证明 NSA 秘密窥探他们的证据，该法院不得不就这个老问题拒绝下发强制令。

“要想具备起诉资格，原告必须证明他遭到了‘具体和特别的’伤害，换句话说，原告必须展示自己的元数据被政府收集，但克莱曼团队掌握的事实并不能完全证明自己的元数据被不断收集。”法官贾尼斯·罗杰斯·布朗在意见中写道。法官布朗指出，斯诺登泄露的一份文件显示，NSA 收集 Verizon Business Network Services 所有用户的元数据，但是并没有显示出 NSA 收集 Verizon Wireless 用户的元数据，而克莱曼是后者的用户。虽然 NSA 自称，在国内监控项目中，几乎每一个无线运营商都公平地参与游戏，但是布朗认为，克莱曼无法证明自己的通信被监控，因此申请强制令的理由不成立。

电子隐私信息中心的律师艾伦·巴特勒说：“这起案件是卡夫卡式的噩梦 (卡夫卡式是人在荒诞的、强制性的外力面前孑然无助的写照)，原告试图挑战笼罩着他们的非法监控项目。”

事实上，“如何证明你是秘密间谍活动的受害者”是任何挑战 NSA 情报项目合法性的人士面临的一道坎。挑战政府机密活动的关键难点是：你无法让法院回答政府的活动是否合法，除非你能够证明政府不允许你证明的东西。

斯蒂芬·威廉斯写道：“在 8 月 28 日的法庭审理中，一名法官竟然辩驳说，NSA 有权不透露原告是否遭到了监控。原告抱怨说，政府不应该简单地通过资料保密来躲避法律责任”。“政府对大规模数据收集的范围予以保密是该项目的特点，而不是缺陷。”斯蒂芬·威廉斯最后评价道。

尽管在克莱曼案件中，奥巴马政府利用“证据”问题获得了胜利，但是法院的裁决也没给 NSA 带来多大的好处。在这一诉讼案件中，法官裁定其元数据项目从未获得美国国会的授权，而国会已经通过了《美国自由法案》，从而正式结束了该项目。NSA 被要求在 11 月终止其元数据收集活动。8 月 28 日的裁决并没有结束诉讼，法院只是驳回了克莱曼要求的能够立即停止其信息收集活动的强制令，现在，克莱曼的官司将继续在低级法院审理。

EPIC 的巴特勒说：“‘证据’问题仍然存在，原告无法要求美国法院裁决 NSA 的活动违反了宪法《第四修正案》的隐私保护条款。我们需要知道，这是搜查 vs 这不是搜查；这是合法的 VS 这是不合法的。我们需要彻底解决该问题的决策，一路踢皮球不是什么好事儿，长此以往，问题就会变得毫无意义，因为这会失去弄清楚法律实质的机会。”

上诉法院的裁决让人想起了《第二十二条军规》(注：Catch-22《第二十二条军规》是美国作家约瑟夫·海勒发表于 1961 年的著名反战小说)。小说通过漫画式的夸张荒诞手法，讲述了二战时期美国一个空军中队的故事，小说情节荒唐滑稽，人物性格反常无理，对战争和美国官僚权力制度进行了强烈的讽刺。具有无上权力和随意性的第二十二条军规并不存在而又无所不在，是一种有组织的却混乱的和疯狂的制度化象征。它既是一项具体而荒谬的法律条文，更是一种抽象的专制现实。它永远对，你永远错；它总有理，你总没理。它总是与灭绝人性的官僚体制如影随形，使你永远无法摆脱，无法逾越。

原文名称	Why It’s Hard to Sue the NSA? You Have to Prove It Spied on You
作者简介	Andy Greenberg，《连线杂志》的资深作家，研究领域涵盖安全、隐私、信息自由和黑客文化。
原文信息	2015 年 8 月 28 日《连线杂志》发布，原文地址 http://www.wired.com/2015/08/hard-sue-nsa-prove-spied/
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。

(上接第一版)

在屠先生眼中作为伟大宝库的中医药，“不是捡来就可以用。”在先生这种举重若轻的表达背后，是大量线索、原料、古方的排除、甄别、提炼、萃取、不同方法的尝试、失败，以及失败后的再尝试，这种通过失败不断积累的探索，其真如在大海中寻觅一根银针。而回到我们从事的网络安全事业，我们面对蜂拥而过的流量，面对数以亿计的样本，而驾驭着各种大数据的方法和云端能力，掌握着各种分析方法与分析资源我们，依然不能有效的从中发现更多关键威胁，也许我们缺少的不仅是更多的探针、更多的存储和计算资源，而是我们与前辈相比，缺少足够的踏实、认真与坚持。

生物制药和网络安全，一个要挽救人的生命，一个是对抗对信息系统的威胁，虽然隔行如隔山，但高尚的事业有相同之处，那就是让世界更安全、更美好。高尚的事业，是催生伟大的成就的舞台，但取得伟大的成就需要基本的前提：踏实、认真的全身心投入与坚持。

在安天建设监控预警体系，捕获分析高级威胁的工作中，我们更需学习屠先生的踏实与认真，专注威胁检测领域的研究探索，坚定的进行基础能力和支撑体系建设，在海量的威胁事件中，达成对高级威胁“百万军中，可取上将之首级”的产品技术能力和服务水准。

【安天 CERT】发布

《疯狂的窃密者——TEPFER》报告

近期，安天 CERT(安全研究与应急处理中心) 研究人员发现木马家族 Tepfer 较为活跃。并对木马家族 Tepfer 进行解读分析，形成分析报告。

该家族最早出现于 2011 年，以窃取 FTP、邮箱、网站、比特币等账号和密码为目的，至今已有数十万变种。Tepfer 主要通过注册表项或子键获取 FTP 的账号并获取安装目录下的 .dat 加密文件，通过破解算法获取密码；通过自带密码表尝试破解系统开机密码并辅助用来通过浏览器窃取用户已保存的网站登陆账号和密码。以 Chrome 浏览器举例，Chrome 将用户保存的网站密码存储在本机目录中：%Application Data%\Google\Chrome\User Data\Default\Login Data 该文件是 SQLite 数据库文件，并使用系统账户密码进行了加密。Tepfer 通过暴力破解系统开机密码，可以间接解密用户使用 Chrome 浏览器保存在本机中的网站登陆账号和密码。Tepfer 将收集到的信息保存到 SQLite 数据库中，并使用 RC4 算法加密，发送至远程服务器；通过 .dat 文件窃取比特币信息。

报告中，安天 CERT 研究人员介绍，Tepfer 家族可以盗取 60 种以上的 FTP 客户端软件所保存的密码；10 种以上的浏览器保存的密码；31 种比特币信息；还能获取多个邮件客户端所保存的密码，可以看出恶意代码作者进行了大量的信息收集、资料整理、账号密码存放位置的研究等工作，熟悉各种网页、数据库、邮箱、其他工具的密码存储方案。该家族是一个无需交互、自动窃密并上传的木马家族，主要利用垃圾邮件进行传播，并将窃取的这些信息加密后上传到指定的网站。

安天 CERT 研究人员发现，Tepfer 家族至今活跃范围仍然很广泛，且 Tepfer 家族的信息接收服务器数量在近期仍在增长。Tepfer 家族的作者对 FTP 的兴趣极大，制作了相当繁杂的账号及密码的窃取方法，想必一定花费了作者不少的时间和精力。Tepfer 的自我更新能力不强，因其作者更注重代码的质量和细节。Tepfer 家族的作者在全球范围内收集密码信息，以备它用。

安天 CERT 提醒广大用户，及时修改 FTP 软件的默认密码保存位置，不要使用简单的开机密码。

(报告原文：http://www.antiy.com/response/tepfer.htmll)

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

该木马程序由安天威胁检测系统发现，经过追影威胁分析系统分析。经由 BD 静态分析鉴定器、YARA 自定义规则鉴定器、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。

依据 BD 静态分析鉴定器、静态分析鉴定器最终将文件判定为木马程序。该文件具有以下行为：访问 DNS；获取主机用户名称；创建互斥体 (mutex)；连接网络；创建特定窗体；独占打开文件；获取计算机名称。

文件名	./blow.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	85 KB
MD5	D8C177781BA316966CE0567253C67CE1
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[PSW]/Win32.Tepfer
判定依据	BD 静态分析

◆ 网络监控

	IP 地址	端口
IP	185.24.98.196	80

	域名	IP
域名解析	obiheros.com	185.24.98.196

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
访问 DNS	★	获取主机用户名称	★
创建互斥体 (mutex)	★	连接网络	★
独占打开文件	★	创建特定窗体	★
获取计算机名称	★		

◆ 静态启发式检测

检测类型	检测点
编译指令	未知壳
PE 结构	无版本信息并且不是 GCC 编译器

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=D8C177781BA316966CE0567253C67CE1