安天周观察

主办：安天　2015 年 12 月 21 日（总第 21 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天入选 2015 年度国家知识产权优势企业

近日，安天入选由国家知识产权局评选的，2015 年度国家知识产权优势企业。2000 年，在安天创建之初，由于团队规模有限，难以承担知识产权相关的成本，致使一些初始的技术创造没有得到有效地保护。随着安天地成长和发展，自 2009 年起，开始逐步重视知识产权工作，建立起比较完备的知识产权体系。截至目前为止，安天共申请专利 359 项，获得授权 85 项。2015 年已申请专利 73 项，其中一项关键专利获得第十七届中国专利奖。

安天始终专注于威胁检测领域的发现，在恶意代码检测、APT 检测等领域建立了竞争优势，确立了以基础检测能力为核心的专利导向。其中，已完成审查的核心检测引擎相关专利授权率接近 100%。同时，通过检测场景、处置技术、态势展现等进行专利点布置，逐渐形成自己的专利特色。

国家知识产权局此次认定旨在实现知识产权强企发展目标，通过提升企业知识产权创造优势、知识产权运用优势、知识产权保护优势等方面，不断增强市场竞争力。此次入选知识产权优势企业的网络安全相关厂商还包括奇虎和猎豹移动等。这表明互联网安全厂商和积极应对新威胁的厂商，具有积极的知识产权追求。

第三届网络安全冬训营可登陆官网报名

由安天承办的第三届网络安全冬训营将于 2016 年 1 月 7 日 -9 日，在哈尔滨友谊宫举行。网络安全技术爱好者可登陆冬训营官网 http://wtc.antiy.com/ 获取报名方式，嘉宾演讲主题及会议日程等讯息。据悉，本期冬训营将以“情报的支撑，塔防的实践”为核心议题。届时，安天将为网络安全保卫者与爱好者提供一个分享、交流的机会和平台。

AVG、McAfee 和卡巴斯基软件存在相同安全漏洞

近日，安全研究人员在免费杀毒引擎 AVG 中发现了一个严重的漏洞。

该杀毒软件在一个可预测的地址中分配了用于读、写和执行权限的内存，而攻击者掌握到这个内存地址后，则可以利用它向目标系统中注入恶意代码并执行，从而将杀毒软件变成黑客的攻击工具。

通过进一步分析，研究人员发现 VirusScan 企业版 8.8 和卡巴斯基 Total Security 2015 也受此漏洞的影响。（文章来源：http://securityaffairs.co/wordpress/42688/hacking/antivirus-critical-vu）

安天荣获 2015 年度科技兴检奖二等奖

近日，安天参与的“移动终端安全检测关键技术研究与应用”项目荣获了由国家质检总局颁发的，2015 年度科技兴检奖二等奖。在项目研究过程中，安天与中国信息安全认证中心、国家无线电监测中心检测中心、东南大学、西安西电捷通无线网络通信股份公司共 5 家单位，群策群力，协作研究，重点突破了操作系统漏洞分析技术、移动恶意代码检测技术、网络安全检测技术等关键技术，建立了移动终端安全检测认证服务模式和移动恶意代码分析环境，形成为移动运营商、移动终端生产企业、移动终端用户提供专业化的移动终端安全检测服务和认证能力。

其中安天主要负责移动终端应用软件和操作系统的安全检测技术研究和相关系统研发，重点突破了移动终端恶意代码分析技术和移动终端防火墙实现方法，研制了移动终端操作系统漏洞检测系统、移动终端操作系统证书安全检测系统、用户访问控制模型安全检测系统、移动终端应用软件安全检测系统，建立了移动终端恶意代码的检测和移动应用软件的完整性检测服务能力。目前，该项目成果已应用于中兴、金山等公司的移动终端和应用产品研发中，取得了显著的经济和社会效益。

每周安全事件

类 型	内 容
中文标题	Joomla 存在远程代码执行漏洞，立即修复！
英文标题	Critical Joomla RCE bug actively exploited，patch immediately!
作者及单位	ZeljkaZorz，HELP NET SECURITY
内容概述	Joomla 被发现一个存在八年的远程代码执行漏洞 (RCE)。受影响的 Joomla 版本包括从 1.5 版本到 3.4.5 版本。Sucuri 首席技术官 Daniel Cid 周一表示，让人更为担心的是，该漏洞已经通过各种渠道传播出去，被使用超过两天。Daniel Cid 建议 Joomla 用户，立即检查服务器日志。检查是否有来自 146.0.72.83、74.3.170.33、194.28.174.106 的请求。同时，可在日志中检索“JDatabaseDriverMysqli”或者“O:”关键字，如果能找到他们，那么可以认为你的网站已经不安全了，需立即修复，启动应急响应。
链接地址	http://www.net-security.org/secworld.php?id=19233

每周值得关注的恶意代码信息

经安天检测分析，本周 9 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	G-Ware/Android.moonbro.a[rog，exp] 2015-12-14	该应用伪装成系统播放器，实际为包含大量色情网址的浏览器，运行后会创建快捷方式，获取手机固件信息和程序列表信息并上传，诱导用户点击下载色情应用，造成用户隐私泄露，建议卸载。(威胁等级低)
		Trojan/Android.BatterySafe.a[exp] 2015-12-15	该应用程序安装无图标，运行无提示。发送注册短信，拦截指定短信并自动回复，同时存在下载行为，会给用户造成一定的资费损耗，建议立即卸载。(威胁等级高)
		G-Ware/Android.Videomanage.a[exp，prv，rog] 2015-12-16	该应用程序伪装成系统应用，安装无图标，诱导激活设备管理器防卸载。运行后台下载 APK，诱导用户点击安装，通过通知栏及桌面快捷方式的行为推广应用，建议立即卸载，避免造成资费损耗。(威胁等级低)
		Trojan/Android.sandrorat.a[prv，exp，rmt]2015-12-16	该应用程序伪装成安全软件，运行时在后台上传用户的设备信息，获取远程控制指令，根据远程控制指令可以上传用户的短信，联系人信息，通话记录，浏览器书签，GPS 地理位置信息，进行后台录音，后台删除或者插入短信，联系人信息，后台增加手机账户，远程控制发送短信，拨打电话，后台推送应用，会造成用户的隐私泄露，造成资源消耗，建议用户谨慎使用。(威胁等级中)
	较为活跃的样本	RiskWare/Android.Gglm.a[exp]	该应用程序安装无图标，运行联网下载指定程序并会执行静默安装操作，还含有推广程序行为，存在安全风险，会给用户带来一定的资费消耗，请及时卸载该程序。(威胁等级低)
		Trojan/Android.appgenuine.c[prv，rog，exp]	该应用程序运行会推送其他软件，后台私自下载安装大量的 apk 文件并加载调用，上传用户设备信息、地理位置信息、应用安装列表信息、IP 地址、mac 地址等信息，私自下载安装 root 工具提权，强制停止运行安全软件，造成用户隐私泄露和资费消耗。(威胁等级高)
		Trojan/Android.HiddenApp.f[exp，sys]	该应用伪装成色情应用，运行会释放广告子包至系统目录下，后台私自联网上传手机固件信息，下载指定的应用程序，执行有界面安装操作，存在安全风险，会给用户造成资费消耗和一定的经济损失，请及时卸载该程序。(威胁等级中)
		Trojan/Android.emial.cn[prv，rmt，exp]	该应用伪装成正常应用，运行后隐藏图标，激活设备管理器；后台接收指令，拦截用户短信，获取用户短信、手机号码和手机固件信息并通过短信和邮箱转发，造成用户隐私泄露，建议立即卸载。(威胁等级中)
		Trojan/Android.E4AQQspy.c[prv]	该应用欺骗用户输入 QQ 帐号和密码，然后联网上传，建议用户立即卸载，使用官方正版应用。(威胁等级高)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 内存破坏漏洞 (CVE-2015-1641)(MS15-033)	攻击者可以通过该漏洞构造嵌入 docx 的 rtf 文档进行攻击。word 在解析 docx 文档处理 displacedByCustomXML 属性时未对 customXML 对象进行验证，可以传入其他标签对象进行处理，造成类型混淆，导致任意内存写入，最终经过精心构造的标签以及对应的属性值可以造成远程任意代码执行。(威胁等级高)
	较为活跃样本	Trojan[GameThief]/Win32.OnLine Games.ababo	此威胁是一种木马类程序，这种木马通常被攻击者用来盗取网络游戏账号、密码和其他的虚拟财产信息进行牟利。这类病毒本身一般不会对抗杀毒软件，但经常伴随着 AV 终结者、机器狗等病毒出现。(威胁等级中)
		Trojan/Win32.Scar.ejkj	此威胁是一种木马类程序。恶意行为包括删除修改数据，监控网络连接，允许攻击者对用户系统进行远程控制等。其变种可能根据不同的进攻目的而设计，一般具有多种恶意行为，一旦侵入用户系统，将会造成很大的破坏。(威胁等级中)
		Trojan[Downloader]/Win32.Adload.efgf	此威胁是一种具有下载行为的木马类程序，其主要功能为下载恶意代码到本机加载运行。部分变种具有加载广告软件的行为。(威胁等级中)
		Trojan/Win32.Inject.urga	此威胁是一种具有注入行为的木马类程序，自身以某种方式注入到其他进程以避免用户和杀毒软件的感知清除，有些变种可以进行自我的 U 盘传播，有些变种木马运行后会修改系统时间、试图关闭多种杀毒软件、木马还能从黑客指定的网址上下载多个病毒执行，将自身复制到所有磁盘进行传播。(威胁等级中)

中国政府称已逮捕了入侵 OPM 数据库的黑客

Ellen Nakashima/ 文　　安天公益翻译小组 / 译

中国政府最近逮捕了据称与今年 OPM(美国人事管理局) 数据库入侵事件有关的几个黑客，这次入侵导致了 2200 多万现任和前任联邦雇员的记录遭到泄露。逮捕行动发生在习近平主席 9 月份对美国进行国事访问之前。美国官员说，这些行动貌似是为了缓解中美两国的紧张局势。

中国对美国政府和企业数据的黑客活动一直是两国之间紧张关系的根源。近日，总检察长洛雷塔 . 林奇和国土安全部部长杰伊 . 约翰逊会见了中国高级官员，制定了执法方面的指导方针，便于协力调查恶意网络活动。OPM 黑客活动 (两波) 也被提上议事日程。

如果被拘留的人确实是黑客，那么此次逮捕将标志着已被定性为美国历史上最具毁灭性的政府数据入侵事件的第一项问责措施。但是官员们表示，很难确定被捕者是否与 OPM 入侵事件有关。“我们不知道，中国声称逮捕的黑客是否真有其罪。”一位因为这个问题的敏感性而不愿透露姓名的美国官员称。

自 6 月份发生了入侵事件后，美国政府官员就表示，他们怀疑此事有中国政府的介入，特别是 MSS(国家安全部)。一些官员说，黑客可能是 MSS 承包商，他们可能自行其事，但是了解该机构会对这些数据感兴趣。此次入侵活动损害了美国政府雇员及其家人的敏感的个人、财务和生物特征数据。中国政府一再坚持称，未涉及此次入侵活动。

《华盛顿邮报》此前报道说，此次逮捕行动涉及美国企业数据的窃取。实际上，逮捕行动与 OPM 入侵事件有关。在与习近平主席举行峰会前，中国官员从媒体报道得知，奥巴马政府正在准备对从入侵美国公司获利的中国企业发动经济制裁。习近平主席的特使孟建柱很快就到了在华盛顿，会见了美国官员，美国官员认为他是为了应对可能的制裁。这些官员说，孟建柱似乎认为美国主要关心OPM入侵事件，而不是针对美国公司的网络攻击。他声称，中国政府并没有指挥 OPM 入侵事件，并表示会逮捕幕后黑客。

美国官员将 OPM 入侵事件定位为传统的间谍活动，即通过间谍活动来帮助外国政府。在这个案例中，其目的是建立美国政府雇员和官员的数据库。专家说，这些信息可以帮助外国政府招募间谍或勒索雇员。或者，这些信息可以帮助他们编写更有效的“鱼叉式网络钓鱼”电子邮件，假装来自同事或家人。这些邮件包含恶意软件，一经激活就会感染计算机。如果中国抓住了真正的凶手，这将是我们可能看到的最重要的网络犯罪逮捕，哥伦比亚大学国际公共事务学院的高级研究学者杰森·希利这样说。

该消息出现于其他突破之后。在峰会上，习近平主席做了一个历史性的承诺：中国永远不会从事网络空间的经济间谍活动。到此，中国政府从来没有承认进行此类间谍活动，其重点是针对企业，而不是政府。两个星期前，习近平主席在土耳其安塔利亚 G-20 峰会上对 19 位国家元首重申了这一承诺。在 G-20 峰会上，所有领导人第一次承诺，他们的国家将不会从事网络工业间谍活动。

“过去两个月震惊不断。”希利说，“谁会想到，我们会从商业间谍活动零规范和 OPM 入侵事件零举措发展为新的 G20 规范和 OPM 黑客逮捕行动呢？这是令人难以置信的外交成就。”官员和分析人士说，综合因素导致了中国的行为改变。经济制裁威胁是关键，去年对 5 位 PLA(中国人民解放军) 军官的对网络经济间谍活动指控也起到了重要的作用。官员和分析人士说，继起诉之后，PLA 逐步减少了对美国公司的黑客攻击，不过 MSS 的活动一直持续或有所回升。官员说，中国对这些起诉非常痛心，在每一次会议上都会提起。

周三，白宫新闻秘书乔希·欧内斯特被问及中国政府是否真得逮捕了与 OPM 入侵事件有关的嫌疑人，欧内斯特拒绝发表评论，但表示，奥巴马总统在巴黎会见了习近平主席，并提出了网络安全问题。“在我们与中国的关系中，这仍然是重中之重。”欧内斯特说。(图片来自网络)

原文名称	Chinese government has arrested hackers it says breached OPM database
作者简介	Ellen Nakashima，《华盛顿邮报》的国家安全记者，专注于情报、技术和公民自由问题。
原文信息	2015 年 12 月 2 日《华盛顿邮报》，原文地址 https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html
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《< 芈月传 > 下载传毒事件分析报告》

近日，有用户反映疑似有恶意代码借助电视剧《芈月传》的热播进行社工传播。安天随即监控到一例以视频种子传播为途径的木马事件。该木马运行后会下载安装一些互联网软件的静默包，以及访问各类商业网站。攻击者则会从中获取付费安装收益和流量收益。

研究人员在百度知道搜索“芈月传全集资源”等类似关键字，可检索出大量含有资源的帖子。在这些帖子中，研究人员发现了 2 个帖子的回帖中含有此次恶意木马的下载链接地址，两者均通过百度网盘进行下载传播。经过比较，两个来源的文件 hezalicjlbca.exe 和 mejihiglajehh.exe 是一致的，文件 MD5 值都是 F2023EC1EB35FA23230C32C1C38D99EE。

研究人员将该样本投放到安天追影威胁鉴定系统 (PTA) 中，发现其主要威胁行为“payforAd”，即利用广告付费流量获利，判断其为付费广告类木马病毒。从 PTA 数据中提取到该广告木马进程内存数据中的字符串中显示，该工具能够下载的静默安装包涵盖 UC 浏览器、QQ 旋风、百度影音、搜狐影音等软件。

在安天以往的分析案例中，所下载的搜狐影音静默包，通常名称中就包含广告计费文件名的 ID 信息。此次样本进程监控中，搜狐静默包的名称为“SoHuVA_4.5.77.0-c204900003-nti-ng-tp-s.exe”。同时，其关联到搜狐影音静默包下载链接为“http://120.55.72.128/1444057988-647-12481/”，静默包名称为“SoHuVA_4.5.77.0-c207715-nti-ng-s-run-x.exe”。其中包含攻击者分账的 ID 信息，ID 为“c204900003”和“c207715”。

在此次事件中，黑客利用了《芈月传》的热播，抓住了广大网民对此剧的热情和追剧心理，进行了流氓工具的传播。对此，安天提示广大网民，黑产组织会抓住各种热门话题传播木马，获取非法利益。请大家随时提高警惕，避免个人损失。

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、数字证书鉴定器、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。

最终依据动态行为鉴定器将文件判定为木马程序。

该文件具有以下行为：增加防火墙设置；读取自身文件；增加 run 自启动项；填充导入表 (疑似壳)；释放 PE 文件；获取系统内存；获取系统版本；访问文件尾部；获取计算机名称；获取 socket 本地名称；查找浏览器进程；遍历进程；连接网络；创建特定窗体；获取驱动器类型；独占打开文件；打开自身进程文件；获取主机用户名称；查找指定内核模块；查找特定窗体；请求加载驱动的权限。

文件名	mejilhiglajehh.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.39 MB
MD5	F2023EC1EB35FA23230C32C1C38D99EE
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Shiz.raj
判定依据	动态行为

◆ 危险行为

行为描述	危险等级
增加防火墙设置	★★★★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=F2023EC1EB35FA23230C32C1C38D99EE

◆ 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	★★	增加 run 自启动项	★
填充导入表 (疑似壳)	★★	释放 PE 文件	★
获取系统内存	★★	获取系统版本	★★
访问文件尾部	★	获取计算机名称	★
获取 socket 本地名称	★	查找浏览器进程	★★
遍历进程	★	连接网络	★
创建特定窗体	★	获取驱动器类型	★
打开自身进程文件	★	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	★	查找特定窗体	★