安天周观察

主办：安天　2016 年 1 月 18 日 (总第 25 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天荣获中国专利优秀奖

由国家知识产权局和世界知识产权组织共同开展的第十七届中国专利奖评选结果近日揭晓，安天出品的专利“基于线程行为的木马窃取文件检测方法和系统”荣获了 2015 年度中国专利优秀奖。

本次获奖的专利技术主要被应用在安天反病毒引擎相关产品当中，在实际的产品化过程中，该专利能够以高准确，低误报的方式识别窃取文件的木马行为和恶意代码行为，进而准确地判定恶意代码。同时，专利涉及的技术在沙箱方案的实现中，可以准确识别未知窃取类型的木马，使其识别的安全事件在海量的信息中快速准确的定位威胁，发现威胁。方便管理人员发现威胁事件，进而帮助相关企业完成安全事件的追踪。

另外，针对窃取文档攻击行为，该专利的识别更具有普适性。这种普适性可以针对新出现的木马，使企业网内信息单向流动，保护企业的隐私，无需频繁升级就可以对抗大部分窃取类型的未知威胁，具有较好的对抗未知能力。在实际的产品抗衰减能力上起到非常好的作用，降低了维护成本的同时也节约了设备的规则空间，获得行业内外的青睐。

中国专利奖评选活动自 1989 年起，至今已成功举办 17 届。本届共评选出金奖 20 项、外观设计金奖 5 项、优秀奖 507 项、外观设计优秀奖 57 项。安天自 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，共申请专利 359 项，获得授权 85 项，2015 年首次荣获中国专利优秀奖。

FSI 2016 威胁情报实战沙龙即将开启

FSI 2016 威胁情报实战沙龙将于 2 月 19 日在上海举办，会议将采取圆桌辩论会的形式。届时，安天移动威胁情报中心、阿里威胁情报中心、360 威胁情报中心、烽火台威胁情报联盟、微步在线、百度威胁情报中心、腾讯威胁情报中心等机构代表将参会并分享经验。

新闻简报

◆ 趋势杀毒曝远程执行漏洞 可盗取用户所有密码

近日，安全研究人员塔维斯·奥曼迪 (Tavis Ormandy) 发现趋势科技杀毒产品中存在漏洞，可致任意网站执行远程代码盗取用户的所有密码。当用户在 Windows 上安装趋势科技杀软时，名为密码管理器的默认组件也会被安装并在开机时自动启动。该密码管理器主要是通过 node.js 由 JavaScript 编写，为处理 API 会请求打开多个 HTTP RPC 端口。奥曼迪说大约需要 30 秒就能发现一个任意命令执行，打开 UrlInDefaultBrowser，它最终映射到 ShellExecute()，这意味着任何网站可以启动任意命令。奥曼迪在与趋势官方的来往邮件中写道，“这意味着网络上的任何人都能完全静默地偷走你的所有密码，还能在无需用户互动的情况下执行任意代码，我真心希望你们能清楚问题的严重性。”(文章来源：https://code.google.com/p/google-security-research/issues/detail?id=693)

◆ 谷歌移除 13 款含恶意病毒应用

近日，谷歌从 Play 商城中移除了 13 款含“大脑测试程序”(Brain Test) 恶意病毒的应用程序。据了解，Brain Test 恶意病毒爆发后会感染应用程序进行非授权下载，恶意为应用刷榜，并尝试得到系统授权。Brain Test 很难彻底删除，甚至能够从工厂重置中存活，用户只能通过清楚系统分区以及彻底的 ROM 刷机才能处理掉 Brain Test。而这些恶意程序至少被下载了 500000 次，估计 20 万到 100 万安卓用户将受到影响。(文章来源：http://www.techweekeurope.co.uk/security/firewall/google-play-android-malware-apps-183468)

◆ Fortinet 防火墙发现硬编码后门

研究人员在 Fortinet 的防火墙系统 FortiOS 中发现一个硬编码的 SSH 后门，影响版本号 4.3 到 5.0.7。这个硬编码的密码是 FGTAbc11*xy+Qqz27。Juniper 的防火墙之前被曝光过两个后门，其中一个就是硬编码的管理权限密码。

Fortinet 否认硬编码密码是后门，称这个漏洞是一个管理身份认证问题，表示早在 2014 年 7 月就释出补丁修复了，漏洞是被他们的安全团队识别出来的。研究人员说，FortiOS 5.2.3 中还是存在有这个硬编码密码，虽然不能被利用，但非常可疑。(文章来源：http://securityaffairs.co/wordpress/43551/hacking/fortinet-fortios-ssh-backdoor.html)

每周安全事件

类 型	内 容
中文标题	CWA 黑客入侵美国国家情报总监 Clapper 的邮箱
英文标题	CWA hackers breached US DNI Clapper 's email，broadband account
作者及单位	Zeljka Zorz，Help Net Security
内容概述	近日，美国国家情报总监詹姆斯·克拉珀 (James Clapper) 的邮箱被一名黑客入侵，这名黑客属于一个名为 Crackas With Attitude(CWA) 的黑客组织，该组织在 2015 年 10 月份曾侵入美国中央情报局 (CIA) 主管约翰·布伦南 (John Brennan) 的个人邮箱。 一名名为 Cracka 的成员声称，他已经入侵克拉珀的 Verizon FiOS 宽带账号、个人邮箱以及他妻子的雅虎邮箱；并且使得每一通打到克拉珀家庭座机的电话都会转接到 Free Palestine Movement。美国国家情报总监办公室的发言人表示，目前有关当局正在对此次攻击事件进行调查。
链接地址	http://www.net-security.org/secworld.php?id=19328

每周值得关注的恶意代码信息

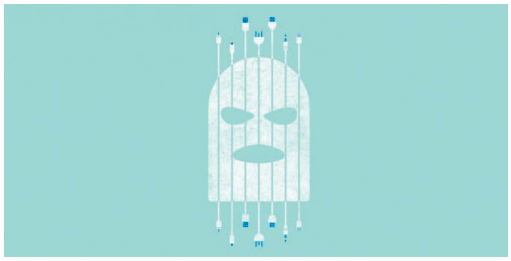
经安天检测分析，本周 10 个移动平台和 4 个 PC 平台的恶意代码家族值得关注

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	Tool/Android.krTracker.a[prv，spy] 2016-01-11	该应用程序为一款间谍软件，通过设置会执行联网上传用户短信箱、通话记录、地理位置等隐私信息，存在一定的安全风险，如非本人安装，建议立即卸载该程序。(威胁等级低)
		Tool/Android.fooltool.a[sys] 2016-01-11	该应用是恶搞软件，会让用户手机有一定几率无法拨打电话和 wifi 打开失败，同时会开启传感器使手机耗电增加，建议卸载。(威胁等级低)
		Trojan/Android.locSpy.c[prv，rmt] 2016-01-12	该应用安装无图标，运行后远程接收短信指令，获取地理位置相关信息上传到指定服务器，并通过短信向远程控制号码反馈运行结果，造成用户隐私泄露，建议卸载。(威胁等级中)
		Trojan/Android.FakeSexApp.b[fra，pay] 2016-01-12	该应用程序伪装色情应用，运行后加载正常网站，无提示调用正常支付插件发送付费短信，建议用户立即卸载，以免造成更多经济损失。(威胁等级中)
		G-Ware/Android.jianmo.r[rog，sys] 2016-01-14	该应用伪装成 QQ 刷钻工具，运行后向开发者发送反馈短信，置顶界面，勒索用户付费，造成用户手机无法正常使用，建议卸载。(威胁等级低)
		Trojan/Android.SmsThief.z[prv] 2016-01-15	应用通过接收短信指令窃取用户联系人，并将联系人信息回复至来信号码，同时删除指令短信，建议用户立即卸载。(威胁等级中)
	较为活跃的样本	Trojan/Android.SmsSend.in[exp]	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。(威胁等级中)
		RiskWare/Android.Downloader.bd[exp]	该应用是一款天气应用，包含风险代码，程序运行会联网上传设备相关信息，私自联网下载 jar 文件加载调用，存在一定风险，可能造成用户资费消耗，建议卸载。(威胁等级中)
		Trojan/Android.InfoStealer.s[prv]	该应用运行后诱导用户点击从而窃取用户手机固件信息、电子邮箱账号、通讯录等隐私信息，建议卸载。(威胁等级中)
		G-Ware/Android.Fakegupdt.ao[rog，exp]	该应用无实际功能，多伪装成色情图片，运行后打开指定网页或色情资源，但应用包含大量流氓广告，诱骗用户下载安装等行为，建议用户谨慎使用。(威胁等级中)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Reader 双重释放远程代码执行漏洞 (CVE-2016-0935)	Adobe Reader 在处理 PDF 文档内畸形的 ExtGState 字典时存在安全漏洞，可导致双重释放。攻击者利用此漏洞可在当前进程上下文中执行任意代码。(威胁等级高)
	较为活跃的样本	RiskWare[Downloader]/Win32.AdLoad.oa	此威胁是一种传播、下载广告软件的木马类程序。可以在未经用户许可的条件下侵入用户系统，并窃取重要数据。安装其他恶意软件后可以使用户的电脑性能变慢。(威胁等级中)
		Trojan[Downloader]/Win32.Homa.er	此威胁是一种具有下载行为的木马类程序。该家族类程序可以下载，如木马，病毒，广告软件或间谍软件的威胁。可以偷偷进入系统，并创建注册表项，以确保在系统每次重新启动时执行。(威胁等级中)
		Trojan/Win32.Inject.bu	此威胁是一种具有注入行为的木马类程序，将自身注入到其他的进程中，可以实现隐藏自身，以免被查杀，可以在后台连接黑客指定的服务器，下载其他的网游盗号木马、后门程序、下载器、广告插件等恶意程序。(威胁等级中)

物联网是如何被黑的

Andy Greenberg/ 文　安天公益翻译小组 / 译

曾经有一段时间，人们将网络空间 (电脑和黑客的数字世界) 和血肉空间 (现实世界) 区分开来。任何人在网络空间遭到黑客攻击后都可以撤退到可靠的物理世界。但是现在，物联网将数字世界的所有漏洞引入到了现实世界中。2015 年，这一趋势更加清晰，以下的黑客攻击更是使得 2015 年成为不安全的物联网之年。



连网汽车

2015 年 7 月，安全研究人员查理・米勒和克里斯・瓦拉塞克向《连线杂志》展示，他们能够远程攻击 2014 版吉普切诺基来禁用其传输和刹车，这永久性地改变了汽车行业的“汽车安全”概念。他们的研究导致菲亚・特克莱斯勒发出了前所未有的召回通知，宣布召回 140 万辆汽车，并向车主邮寄 U 盘，以修复有漏洞的信息娱乐系统并阻止对 Sprint 网络 (连接轿车和卡车) 的攻击。

在 8 月份的 Defcon 黑客大会上，CloudFlare 首席安全研究员马克・罗杰斯和移动安全公司 Lookout 的联合创始人兼 CTO 凯文・马哈菲披露了特斯拉 S 型汽车的一组漏洞。这些漏洞能够将车主的笔记本电脑连接到仪表板后面的汽车网线，使用软件命令启动该售价 10 万美元的汽车并进行驾驶；或者，它们能够在汽车的内部网络中植入远程访问木马，在车主驾驶期间远程切断引擎。这使得特斯拉通过无线方式直接向涉事汽车发送修复包，修复了大多数车辆。这些黑客攻击不仅为汽车产业敲响了警钟，也为消费者和监管者敲响了警钟。

医疗设备

当然，被黑汽车并不是唯一能够导致伤亡的物联网设备。关键的医疗器材和设备也存在软件和架构漏洞，使得攻击者可以劫持并控制它们，导致致命后果。2015 年，阿拉巴马大学的学生攻击了植入 iStan(一个机器病人，用于医科学生的培训) 的心脏起搏器并从理论上杀死了它。“我们能够加快心跳；也可以减慢心跳。”阿拉巴马大学模拟项目总监麦克・雅各布斯告诉 Motherboard。“如果它有一个除颤器，大多数心脏起搏器都有，那我们可以不断地震动它。”学生们根据前人的研究进行了此次测试，但是他们提供了一个很好的概念证明，展现了此类攻击带来的真实后果。但糟糕的是，医疗设备的许多问题都无法用一个简单的软件补丁进行修复，而是需要重新设计系统。所有这一切都需要时间，这意味着医院和患者在若干年后才能看到更安全的设备。

其 他

对于任何消费产品，2015 年似乎不止一家公司急切地添加 Wi-Fi 功能。在另一方面，保护 Wi-Fi 连接似乎是一个低优先级任务。

美泰公司在其 Hello Barbie 中添加了 Wi-Fi 连接，用于启用实时人工智能对话，但是这会使 Hello Barbie 智能手机应用程序连接遭到拦截，芭比娃娃记录的所有音频都会被拦截。三星“智能冰箱”旨在通过 Wi-Fi 同步用户的谷歌日历，但是由于它不验证 SSL 证书，使得用户的 Gmail 凭证遭窃。即使婴儿监视器，也存在黑客窥探孩子的风险，安全公司 Rapid7 的一项研究发现，测试的所有 9 个监视器都很容易被攻击。

甚至连枪支也难逃黑客攻击的风险。7 月，黑客夫妇鲁纳・山特维克和迈克尔・奥格向《连线杂志》展示，他们可以控制启用 Wi-Fi 的 TrackingPoint 狙击步枪。山特维克和奥格利用步枪的不安全的 Wi-Fi 来改变其自动瞄准范围系统的变量，从而禁用步枪、使其错过目标，甚至击中他们选择的而非预定目标。“在这里向 TrackingPoint 等公司传递一个消息”，山特维克说，“当你把技术应用于新事物时，你就会遇到新的安全挑战。”

当然，这个结论也适用于任何以消费者为中心、思考着将其产品连网的公司。但是，对于那些具有杀伤力的产品 (不管是枪支、医疗植入物，还是汽车)，我们希望 2016 年人们会更加重视。

原文名称	How the Internet of Things Got Hacked
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 12 月 28 日《连线杂志》，原文地址 http://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/
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《黑暗力量文档样本分析报告》

近日，乌克兰伊万诺—弗兰科夫斯克地区大约有一半的家庭 (约为一百四十万的人口) 遭受了停电的困扰，整个停电事件持续了数小时之久。据乌克兰的新闻媒体 TSN 电视台的报道，此次停电事件是由黑客攻击所导致的，并且在发电站遭受攻击的同一时间，乌克兰境内的其他多家能源公司也遭受到了黑客有针对性的网络攻击。据调查，黑客使用了高度破坏性的恶意软件 BlackEnergy(黑暗力量) 在乌克兰境内的三处变电站制造了严重的破坏性事件。

根据 ESET 公司公布的黑暗力量攻击乌克兰事件的样本信息，安天追影小组通过态势感知平台获取了相关样本。针对其中一个 xls 格式文档进行分析后发现，文档原始名称可能为 Додаток1.xls 即“应用程序 1.xls”，打开后会出现包含俄语的信息。利用追影威胁分析系统 (PTA) 可以自动对其进行检测，发现该 xls 文档包含恶意的宏代码，宏运行后释放名称为 FONTCACHE.DAT 的 PE 文 件，Black Energy NTP plugin 在自启动目录添加快捷方式自启动，注入 IE 进程进行反弹连接 C2 控制 IP 信息 5.149.254.114。

安天追影小组发现黑暗力量进行 DDoS 攻击时会使用 NTP 反射 / 放大技术。这个技术需要欺骗源 IP 地址的数据包，而 Windows 限制 TCP/IP 数据包使用伪造的源 IP 地址进行发送数据。黑暗力量通过释放安装 winpcap，利用这个库进行原始数据包构造，把源 IP 修改为攻击目标的 IP。在 UDP 协议中正常情况下，客户端发送请求包到服务端，服务端返回响应包到客户端。但是 UDP 协议是面向无连接的，所以客户端发送请求包把源 IP 修改为受害者的 IP，最终 NTP 服务端会返回响应包到受害者的 IP，这就形成了一次反射攻击。NTP 包含一个 monlist 功能，也被成为 MON_GETLIST，主要用于监控 NTP 服务器，NTP 服务器响应 monlist 后就会返回与 NTP 服务器进行过时间同步的最后 600 个客户端的 IP，响应包按照每 6 个 IP 进行分割，最多有 100 个响应包，这就达到了放大攻击的效果。

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：利用漏洞释放 PE 文件；设置自启动项；格式漏洞；连接特殊 URL；创建互斥体 (mutex)；隐藏文件；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；打开自身进程文件；获取 socket 本地名称；篡改系统文件创建时间；连接网络；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；查找特定窗体；请求加载驱动的权限。

文件名	97B7577D13CF5E3BF39CBE6D3F0A7732
文件类型	Document/Microsoft.XLS[:Excel 97-2003]
大小	718 KB
MD5	97B7577D13CF5E3BF39CBE6D3F0A7732
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.SGeneric
判定依据	动态行为

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
利用漏洞释放 PE 文件	★★★★	设置自启动项	★★★
格式漏洞	★★★★		

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
连接特殊 URL	★	创建互斥体 (mutex)	★
隐藏文件	★★	填充导入表 (疑似壳)	★★
释放 PE 文件	★	获取系统内存	★★
释放 PE 文件	★	获取系统版本	★★
打开自身进程文件	★	获取 socket 本地名称	★
连接网络	★	篡改系统文件创建时间	★★
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	★	查找特定窗体	★
请求加载驱动的权限	★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=97B7577D13CF5E3BF39CBE6D3F0A7732