安天周观察

主办：安天　2016 年 5 月 16 日（总第 39 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加 2016 中国物联网安全大会并发表主题演讲

5 月 11 日，2016 中国物联网安全大会在无锡召开，近 350 位物联网及安全相关领域的专家和企业代表参加了本次会议，共同探讨了物联网产业发展中遇到的一些安全问题。

作为物联网安全领域的热点话题，无线通信安全近些年一直受到人们的关注。安天微电子与嵌入式研发中心高级工程师赵世平，在大会上发表了题为《可扩展物联网无线通信安全性研究工具的构想与实现》的演讲，向参会嘉宾展示了安天自行研发的可扩展物联网无线通信安全性研究工具。该工具包括可扩展硬件平台和支持二次开发的软件工具两部分，可有效降低物联网无线以及硬件安全研究的难度，同时又可以提高安全研究的效率。安天研究人员将已实现的硬件平台和软件工具在部分实际物联网无线通信场景中进行了安全性测试，得到了一定的预期效果，证明了这一工具的可行性。目前，该项研究仍处于完善阶段。

安天荣获『北京市专利示范单位』称号

近日，经北京市知识产权局评选，安天被授予“北京市专利示范单位”称号，这是继荣获“2015 年度国家知识产权优势企业”和“2015 年度中国专利优秀奖”后，相关主管部门给予安天在知识产权和专利方面的又一项肯定。

据了解，本次评选的目的在于提高北京市企事业单位知识产权保护与综合运用能力，加快培育知识产权优势企事业集群，提升产业创新力与竞争力。本次评选依据规则分别从专利创造能力、专利管理能力、专利运用能力、专利保护能力和专利经费投入产出效益等方面对参选单位进行了评定，经过初步筛选、现场答辩、专家评审、社会公示等环节，最终认定 55 家企事业单位为北京市第七批专利示范单位。

安天首批通过《企业知识产权管理规范》国家标准认证

近日，企业知识产权管理规范标准化专题培训会在北京举行。安天被授予“《企业知识产权管理规范》国家标准认证单位”称号，成为首批通过该认证的十五家单位之一。

据了解，开展本次认证的目的在于建立和完善企业知识产权管理体系，提升企业知识产权综合管理能力，推动《企业知识产权管理规范》国家标准实施，引导企业建立健全企业知识产权管理规范。安天自 2009 年起，开始逐步重视知识产权，建立起比较完备的知识产权体系，稳步推进相关工作。截至目前为止，共申请专利 402 项，获得授权 105 项。

一周简讯

- 印度铁路订票网站遭到攻击 1000 万乘客信息泄露
- 关键医疗设备在心脏手术期间因杀软扫描崩溃
- AVL 移动安全团队曝光利用极光推送 SDK 的恶意程序
- 研究人员发现勒索软件新家族 Enigma，仅针对俄罗斯
- 安全厂商发现首例具有简体中文提示的比特币勒索软件
- APT 组织兵风暴自 4 月起攻击德国基督教民主联盟网络
- 孟加拉央行失窃案中恶意代码或与索尼攻击案有关手

（安天 CERT 搜集整理，详见：创意安天论坛 http://bbs.antiy.cn/forum.php）

4 月钓鱼网站排名出炉：山寨“建设银行”居首

炮制逼真的山寨网站对广大用户实施钓鱼诈骗，是当下不法分子使用的常见诈骗伎俩。用户如果访问了这些钓鱼网站，并按照提示填写真实信息，就会导致个人信息或银行卡信息被盗，从而导致经济损失。

根据 12321 网络不良与垃圾信息举报受理中心的统计，4 月钓鱼网站排名 TOP10 分别为：假冒建设银行、假冒奔跑吧兄弟、假冒工商银行、假冒 10086、假冒淘宝、假冒招商银行、假冒中国好声音、假冒 Apple、假冒我是歌手、假冒农业银行。其中排行第一的假冒“建设银行”举报量达 716 件次，比 3 月份增加了 24.0%。

（文章来源：http://www.c114.net/news/52/a953122.html）

每周安全事件

类 型	内 容
中文标题	Google Play 商店又现 190 款感染恶意程序的 Android 应用
英文标题	190 Android Apps Infected with Malware Discovered on the Google Play Store
作者及单位	Catalin Cimpanu；Softpedia
内容概述	近日，俄罗斯安全企业 Dr.Web 表示，他们在 Google Play 上发现了 190 款感染 Android.Click.95 恶意程序的 Android 应用，该恶意程序会在用户的浏览器中强行加载一个 URL，包含恐吓软件类的信息，欺骗用户其设备遇到了问题。如果用户想要解决问题，该恶意程序会引导用户去下载另一款 APP，并且每隔 2 分钟就弹出一次提醒，以此来获得广告点击收入。Dr.Web 表示已经将相关情况报告给了谷歌方面，而谷歌已经对这 190 款受感染的应用执行了下架处理。
链接地址	http://news.softpedia.com/news/190-android-apps-infected-with-malware-discovered-on-the-google-play-store-503824.shtml

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	Trojan/Android.Facksystem.a[rog，fra，sys]2016-05-10	该应用程序伪装成系统程序，安装无图标，运行后上传用户已安装程序包名信息，联网获取卸载列表，执行对指定程序的静默卸载，造成用户隐私泄露和系统破坏，建议及时卸载该程序。（威胁等级高）
		Trojan/Android.PooyeshPardaz.a[prv，rog，spy]2016-05-11	该应用程序是一款国外间谍应用，可设置隐藏图标，可监听短信，拦截指定短信，获取短信指令执行发送地理位置信息、删除短信、删除通讯录和通讯记录、拨打电话、启动飞行模式等等，私自发送指定短信和回复反馈短信，监听拨打电话并拦截指定拨号，根据拨号指令调出该应用界面。（威胁等级高）
		Trojan/Android.EmailLoc.a[prv，exp，fra] 2016-05-12	该程序伪装成系统应用，运行后隐藏图标，后台获取用户地理位置信息和收件箱内容并通过邮箱转发，造成用户隐私泄露和资费损耗，建议不要安装。（威胁等级高）
		Trojan/Android.SMSfraud.d[fra，exp]2016-05-12	该程序伪装成其他应用，运行时遍历联系人并发送推广欺诈短信，在造成资费消耗的同时，还有可能给您的亲友造成一定的经济损失，建议卸载。（威胁等级高）
		RiskWare/Android.SMSreg.ba[exp]2016-05-13	该应用程序无实际功能，运行后私自下载文件并发送注册短信，造成用户资费损耗，建议不要安装。（威胁等级低）
	较为活跃的样本	Trojan/Android.Downloader.bv[rog，exp]	该应用安装无图标，程序运行会私自下载未知文件，私自删除卸载应用，造成用户资费消耗。（威胁等级低）
		Trojan/Android.emial.db[prv，rmt，spr]	该应用运行后短信转发用户手机号码和手机固件信息，接收短信指令，私自发送短信订阅付费内容；群发短信，传播恶意网址，造成用户隐私泄露和资费损失，建议不要安装。（威胁等级中）
		Trojan/Android.b4aspy.b[prv，rmt，sys，spy]	该应用程序伪装成系统应用，安装无图标，后台接受指令进行上传用户隐私、修改系统设置、清除手机数据等高危行为，建议立即卸载，避免造成隐私泄露。（威胁等级中）
		RiskWare/Android.SmsSend.jl[exp]	该应用运行后无明显扣费提示，用户若不慎点击会发送扣费短信，造成用户资费损失，建议谨慎使用。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	微软“WebDAV”提权漏洞 (cve-2016-0051)	该漏洞存在于 Microsoft Web 分布式创作和版本管理 (WebDAV) 中，如果 Microsoft Web 分布式创作和版本管理 (WebDAV) 客户端验证输入不当，那么其中就会存在特权提升漏洞。成功利用此漏洞的攻击者可以使用提升的特权执行任意代码。（威胁等级高）
		微软 Office Excel 远程代码执行漏洞 (CVE-2016-0035)	Microsoft Office 中的漏洞。最严重的漏洞可能在用户打开特制 Microsoft Office 文件时允许远程执行代码。成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Cray	此威胁是一类具有自动下载行为的木马类程序。可以在电脑中下载并安装其他程序，这些程序可能是恶意软件或恶意软件组件，从而使用户电脑感染恶意程序。（威胁等级高）
		Trojan[Downloader]/Win32.Codecpack	此威胁是一种具有下载行为的木马类程序，该家族通过垃圾邮件窃取用户的账号信息，入侵用户电脑后，会修改默认设置让自己在系统中运行。还会在电脑中打开后门，使电脑很容易受到其他恶意软件的威胁，还可能带来广告弹窗等问题。（威胁等级高）
		Trojan[Rootkit]/Win32.Podnuha	此威胁是一种木马类程序，入侵电脑后，会在系统中加入恶意代码，修改 Windows 启动项。系统被修改后会导致文件丢失、程序运行错误、系统启动故障、蓝屏、系统冻结或崩溃等问题。此外，该家族会利用系统缺点在电脑中注入新威胁，如蠕虫、Rootkit、键盘记录器、恶意软件、间谍软件等。（威胁等级高）

沃森超级计算机“承担”安全职责

Tom Spring/ 文　安天公益翻译小组 / 译

IBM 正在利用沃森 (Watson) 超级计算机的强大功能来防御病毒、勒索软件和 DDoS 攻击。近日，IBM 公布了一项雄心勃勃的计划：每天从安全数据库向沃森输入数亿个数据点，使沃森能够发现正在发生的异常，在它们造成任何损害之前将其阻断。

IBM 将该服务称为“网络安全沃森”(Watson for Cyber Security)，称该服务在一年前就已经开始对客户进行测试了。该服务基于“云”，充分利用沃森的“认知技术”。但是，IBM 公司表示，他们首先需要对沃森进行培训，使其能够更好地理解结构化数据和非结构化的安全数据。

IBM 安全部门副总裁迦勒·巴洛 (Caleb Barlow) 说：“就像任何一个刚接触安全的人一样，沃森需要了解恶意软件、勒索软件、木马、病毒、脚本漏洞等之间的差异。”

IBM 表示，为了帮助沃森识别各种以前、目前和未来的威胁，他们与 8 所大学达成了合作，包括麻省理工学院、加州州立理工大学和渥太华大学。这些大学的学生们负责向沃森提供和注释系统安全报告和数据，由此“教学”沃森识别威胁。

IBM 不断致力于从一家以硬件为中心的公司转型为基于云、分析、移动、社交和安全的公司，此举正是这种努力的一部分。在过去的一年中，IBM 已经对安全领域进行了大量投资，包括今年早些时候以 20 亿美元的价格收购了私营网络安全公司 Resilient Systems。

在 IBM 的转型中，沃森超级计算机是一个重点项目。首席执行官吉尼·罗曼提 (Ginni Rommety) 表示，沃森超级计算机带来了“认知时代”，它能够帮助企业了解大数据并获得成功。就其本身而言，沃森已经应用到很多 IBM 人工智能业务中，包括 Watson for Oncology，Explorer，Watson's Internet of Things，Discovery Advisor 和 Engagement Advisor。根据 SEC(美国证券交易委员会) 的文件，到目前为止，这些投资已经收回了成本；而且在 2015 年沃森已为 IBM 公司赚了 20 亿美元。

巴洛说：“一旦沃森掌握了一定的知识量，它就不需要太多帮助了，它可以自己教学自己。”那么，沃森需要被计算机工程系的学生们教学多久呢？巴洛表示尚未确定。

一旦运作，“网络安全沃森”就会从 IBM 客户接收到数亿的离散安全数据点，每天还会获得稳定数量的安全博客、白皮书、视频字幕、新闻文章、安全百科、安全预警、CVE 数据、机器生成的安全报告、社交媒体的安全讨论等等。IBM 表示，这些数据还包括其 X-Force 库中 20 年的安全信息、上报到美国国家漏洞数据库中的超过 75,000 个已知软件漏洞、每年发布的 1 万份安全研究报告和每月发布的超过 6 万篇安全博客。

巴洛说：“每天都会产生大量的安全数据，安全分析师们面临着严重的速度挑战。”

巴洛说，接下来，IBM 将会利用沃森认知引擎的力量来筛选非结构化和结构化数据，以确定趋势、识别新的风险并预测攻击。他预测，互联网上 80% 的数据是非结构化的，对安全专家来说是有价值的。

原文名称	IBM's Watson Supercomputer Takes On Security
作者简介	Tom Spring，Threatpost 的副主编。
原文信息	2016 年 5 月 10 日《Threatpost》发布 原文地址 https://threatpost.com/ibms-watson-supercomputer-takes-on-security/117999/
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《利用“白加黑”绕过检测的远控分析》报告

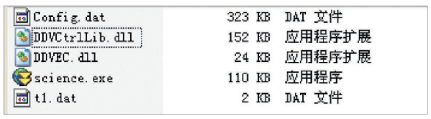
近日，安天追影小组通过威胁感知平台发现一个远控样本，经分析该样本与前段时间国内知名果粉社区威风网被挂马事件的木马同源。该样本通过“白加黑”的方法绕过检测，运行过程中会释放一个带有数字签名的白文件和一些加密文件，并通过栈溢出的方式来实现注入，最终达到远控的目的。

分析过程

1. 释放阶段

此阶段主要是释放一些白文件以及一些加密的数据文件，其中 Config.dat 是加密的黑文件，t1.dat 跟域名相关，science.exe 是个关键文件，其是 9158 旗下产品中的升级程序，而 DDVCtrlLib.dll、DDVEC.dll 是其需要引用的库文件。

随后样本带参运行 science.exe 文件，参数很长，主要是加密后的 shellcode，可以触发栈溢出来执行代码。最后样本通过批处理来自删除。



释放文件截图

2. 注入阶段

触发溢出的地方是 vsprintf 函数，由于没有校验传入的参数的长度导致栈溢出。溢出成功后，通过覆盖返回地址，跳入存放 shellcode 的地方开始执行，shellcode 的主要功能是解密 Config.dat 黑文件，然后加载运行，该样本主要是创建服务来自启动，然后启动服务，自己结束退出。

服务启动后，又通过触发栈溢出来执行 shellcode，该样本主要是创建傀儡进程 svchost，然后注入恶意代码，至此，远控模式悄然开启。

3. 远控阶段

样本根据计算机名组成字符串来创建互斥体，收集用户电脑上的敏感信息，如盘符、处理器、内存、杀软等。

根据 t1.dat 解密出需要连接的 IP：192.168.1.122，然后连接获取指令，经分析该远控的主要功能包括：获取磁盘信息、屏幕截取、录音、反弹 cmd、运行 PE 文件、关机、重启、注销、自删除、联网下载文件、弹出消息、键盘记录、获取剪贴板内容等。

综上所述，此远控为了躲避杀软的查杀使用了第三方白文件的漏洞来达到恶意代码执行的目的，溢出后又把恶意代码注入 svchost 系统及进程中执行，然后连接远端获取控制指令。由于磁盘中可执行程序都是白文件，导致大部分杀软都无法识别，但安天追影产品依然可以通过其恶意行为将其检出为恶意样本。

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、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、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：其他进程写入可疑数据、删除自身、可疑进程名称、填充导入表 (疑似壳)、自启动、关机、释放 PE 文件、访问 dns、获取系统版本、创建挂起的进程、访问其他进程内存、获取计算机名称、篡改系统文件创建时间、创建服务、设置调试器权限、连接网络、创建特定窗体、获取驱动器类型、独占打开文件、遍历进程、获取主机用户名称、启动服务、删除指定服务、疑似桌面控制。

文件名	0DE20150ACDE9A4AD710BEEF3FCFC010
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	844 KB
MD5	0DE20150ACDE9A4AD710BEEF3FCFC010
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
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
其他进程写入可疑数据	★★★	删除自身	★★★★
可疑进程名称	★★★★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=0DE20150ACDE9A4AD710BEEF3FCFC010

其他行为

行为描述	危险等级	行为描述	危险等级
填充导入表 (疑似壳)	★★	自启动	★
关机	★	释放 PE 文件	★
访问 dns	★	获取系统版本	★★
获取计算机名称	★	创建挂起的进程	★
篡改系统文件创建时间	★★	访问其他进程内存	★
创建服务	★	设置调试器权限	★
创建特定窗体	★	连接网络	★
获取驱动器类型	★	独占打开文件	★
遍历进程	★	获取主机用户名称	★
启动服务	★	删除指定服务	★★
疑似桌面控制	★		