安天周观察

主办：安天　2017 年 5 月 8 日（总第 86 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天 APT 项目获北京市科学技术奖三等奖

4 月 26 日，北京市委、市政府在北京会议中心隆重举行 2016 年度北京市科学技术奖励大会。安天的《追影安全平台反 APT 技术研究与应用》项目荣获“北京市科学技术奖三等奖”。

会上，北京市委常委、市委教育工委书记林克庆宣读了《北京市人民政府关于 2016 年度北京市科学技术奖励的决定》。市委书记郭金龙，市委副书记、市长蔡奇为科技工作者颁奖，对他们为首都科技事业发展作出的贡献致以崇高敬意和热烈祝贺。

2016 年共有 180 项成果荣获北京市科学技术奖，其中，以企业为主体的产学研联合攻关成果显著。安天此次获奖的项目《追影安全平台反 APT 技术研究与应用》针对近年来广受关注的高级持续性威胁 (APT) 网络安全热点问题，建设了针对高级威胁的实景模拟研究环境，进行深层次基础理论研究，设计了新一代恶意代码自动分析流水线体系。

该项目成果已与现有网络安全设备有效融合，在恶意代码威胁识别、高级威胁识别中获得良好的示范应用，促进了产业界和学术研究的良性互动，推动了恶意代码自动分析技术理论和工程技术的发展，形成安全堡垒，为信息安全工程建设提供了全面的解决方案。

安天获通信网络安全服务安全设计与集成（一级）能力评定证书

日前，安天获得由中国通信企业协会颁发的“通信网络安全服务安全设计与集成（一级）能力评定证书”。通信网络安全服务能力评定是指对通信网络安全服务单位从事通信网络安全服务综合能力的评定，包括技术能力、服务能力、质量保证能力、人员构成与素质、经营业绩、资产状况、获得奖励情况等要素。

通信网络安全服务能力分为两种类型：风险评估、安全设计与集成。安全设计与集成是指对所服务的通信网络的安全框架进行设计，形成安全建设规划，并对计划实施的安全策略细化，在安全解决方案的基础上，实施安全产品集成、安全软件定制开发、安全加固或其它的安全技术和咨询服务。

该资质的获得，进一步完善了安天的资质体系，安天技术产品能力和服务能力再一次得到行业管理机构的肯定，也意味着安天可以为客户提供更高标准的安全服务。

■ 安卓系统现恶意软件 开启电筒致银行卡密码泄露

近日，据 ESET 官方报道，一个具有自动锁屏功能的银行恶意软件近期伪装成 Google Play 上的手电筒应用，广大安卓用户成为了它的狩猎目标乃至囊中之物。与其它静态式的银行业务木马不同，该木马能够动态地调整自身功能。该木马可以通过 C&C 服务器命令模拟真实应用的界面，锁住受感染设备，避免受害者发现恶意活动，拦截短信并显示伪造的通知，最终达到绕过双因素身份验证的目的。

这种恶意软件能够感染安卓系统的所有版本。而且由于功能动态变化的特点，它不会受限于应用程序的类型——只需获得安装在受害设备上应用程序的 HTML 代码，在启动该应用后用 HTML 代码伪造的虚假屏幕覆盖掉就可以了。（来源：http://www.cnnvd.org.cn/news/show/id/8408）

青年节安天分获集体、个人两项表彰

五四青年节当日，黑龙江团省委、共青团哈尔滨市委员会分别举行纪念五四运动 98 周年暨先优表彰大会。

安天在两个活动中分别荣获一个集体奖章和一个个人奖章，分别是由黑龙江团省委颁发的“黑龙江省青年五四奖章集体”荣誉，和由团市委向安天副总工程师李柏松颁发的“哈尔滨市青年五四奖章”。

每周安全事件

类 型	内 容
中文标题	联想 IBM Storwize 附带的 USB 初始化工具内含恶意文件
英文标题	USB drives containing IBM tool found infected with malicious code
作者及单位	Bradley Barth；SCmagazine
内容概述	近日，据外媒报道，联想 IBM Storwize 磁盘阵列附带的 USB 闪存驱动器的初始化工具内含恶意文件。调查显示，以下系统型号的 01AC585 USB 闪存驱动器初始化工具可能含有恶意文件：V3500-6096 型号的 02A、10A，V3700-6099 型号的 12C、24C、2DC，V5000-6194 型号的 12C、24C。此外，联想 IBMStorwize 序列号以 78D2 开头的设备不受该恶意软件影响。 联想专家表示，恶意软件并不影响存储系统的完整性或性能。当初始化工具从 USB 闪存驱动器启动至计算机初始配置时，它将自身复制到桌面或笔记本电脑的硬盘驱动器上的临时文件夹或恶意文件中。初始化 USB 闪存驱动器包含一个名为 InitTool 的文件夹，该工具与恶意软件同时被复制到该文件夹中。 IBM 与联想目前已采取必要措施，防止供应链出现其他任何问题、避免问题 USB 闪存驱动器继续流出。
链接地址	https://www.scmagazine.com/usb-drives-containing-ibm-tool-found-infected-with-malicious-code/article/653835/

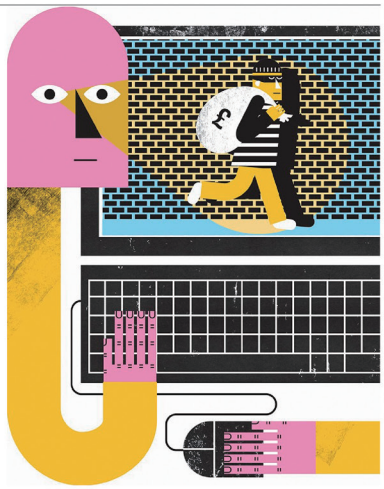
每周值得关注的恶意代码信息

经安天检测分析，本周有 9 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

平台分类	关注方面	名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.Onespy.a[prv] 2017-05-01	该应用为一款间谍程序，运行后会激活设备管理器，窃取用户各项基本隐私，通过远控端发送命令控制手机，造成用户隐私泄露。建议立即卸载。（威胁等级中）
		Trojan/Android.xnspy.a[prv，exp] 2017-05-01	该应用为一款间谍程序，运行后会窃取用户短信、手机固件信息、通讯录、Email、通话记录、定位、拍照摄像、网页浏览历史信息等各项基本隐私，造成用户隐私泄露。建议立即卸载。（威胁等级高）
		Trojan/Android.qingsuo.a[rog，spr] 2017-05-03	该应用程序运行后诱导用户点击下载免流、轰炸、病毒等恶意程序，使用户手机感染病毒，造成资费损耗，建议卸载。（威胁等级中）
		G-Ware/Android.StealMoneyGame.a[rog，pay]2017-05-04	该游戏应用运行后存在不明显的提示信息，以领取道具名义频繁加载弹窗，诱导用户点击进行付费操作，给用户造成资费损失，同时还有短信拦截、删除短信的行为，建议卸载。（威胁等级低）
	较为活跃的样本	Trojan/Android.Faketaobao.l[prv]	该应用会伪装成淘宝，会窃取用户的淘宝账号及密码相关信息，造成用户隐私泄露。（威胁等级中）
		Trojan/Android.jianmo.ck[rog]	该应用程序运行后会置顶锁屏界面，要求用户联系指定 QQ 解锁，建议立即卸载。（威胁等级中）
		Trojan/Android.FakeInst.el[exp，rog]	该应用程序伪装成正常应用，运行后激活设备管理器并隐藏图标，后台下载其他应用，加载大量广告，造成用户资费损失，建议卸载。（威胁等级高）
		Trojan/Android.emial.fj[prv，exp]	该应用程序伪装成文档应用，隐藏图标，通过邮件上传用户信箱和通讯录隐私信息，造成隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.QQspy.bh[prv，exp]	该应用程序运行诱导用户输入 QQ 账号密码，通过短信转发，造成隐私泄露和资费损耗，建议立即卸载。（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 畸形 EPS 文件漏洞 (CVE-2015-2545)(MS15-099)	Microsoft Office 是一款微软发布的办公处理应用套件。Microsoft Office 处理 EPS 文件存在内存破坏，允许攻击者构建恶意文件，诱使应用解析，可使应用程序崩溃或执行任意代码。（威胁等级高）
	较为活跃的样本	Trojan/Win32.Trickster	此威胁是一个木马家族。该家族的样本在执行后会连接远程服务器，上传所窃取的信息，并受进一步控制。例如更新自身程序、接受控制命令并执行等。（威胁等级中）
		GrayWare[AdWare]/Win32.DealCabby	此威胁是具有广告行为的恶意软件家族。其样本执行后会安装浏览器辅助插件，并在系统的通知区域、浏览器中弹出推广信息，影响用户的使用体验。（威胁等级低）
		Trojan[Downloader]/Win32.Crossder	此威胁是一类具有下载行为的木马家族。该家族的样本在执行后会连接远程服务器，下载其他程序并执行，并接受进一步的控制。（威胁等级中）
		Trojan/Win32.Downeks	此威胁是一个木马家族。该家族的样本通常随其它恶意软件捆绑而来。该家族的样本在执行后会下载其它恶意程序、添加自身启动项、并窃取计算机名、用户名、C 盘序列号、操作系统版本、处理器类型、安装的反病毒软件以及屏幕截图等信息。（威胁等级中）

xDedic 市场数据对企业造成威胁

Kelly Sheridan / 文　安天公益翻译小组 / 译



近日，新的 IBM 报告显示，2016 年最常被攻击的行业是金融服务行业，其遭受的攻击同比增长了 29%。

网络犯罪分子通常追着钱走，越来越多的攻击者开始瞄准金融服务机构。在 2016 年，数据泄露事件、漏洞数量、通过物联网执行的 DDoS 攻击都出现了增加。

IBM X-Force 威胁情报指数发现，金融服务行业已经成为犯罪分子的头号目标，遭受的攻击比其他行业高出 65%。该行业遭受的攻击同比增长了 29%，从 2015 年的 1310 起增加到 2016 年的 1684 起。

威瑞森 (Verizon) 高级网络工程师戴夫·高兰德 (Dave Hylender) 说：“攻击者的主要目标是赚钱，这是大多数攻击的驱动力。”黑客也会通过攻击医疗或其他机构获得大量数据信息来勒索，但需要配合繁琐的额外步骤才能将这些数据变现并开立诈骗账户。而攻击金融服务机构则削减了网络犯罪分子与资金之间的中间步骤，所以越来越多的黑客选择金融服务机构进行攻击。他解释道，如果黑客能够在银行系统中植入恶意软件，他们会更容易地获取资金。威胁源可以执行一系列非法活动，如获取用户名和密码、提取资金、创建假借记卡等等。

IBM X-Force 威胁研究员米歇尔·阿尔瓦雷斯 (Michelle Alvarez) 指出：“如果能够成功感染金融服务机构，攻击者就能获得可观的利润。攻击医疗和零售机构也能够获利，但是攻击金融服务机构能够省去许多中间环节。”

在 2016 年，金融服务机构被攻击次数猛增 937%，达到 2 亿次。高兰德指出，网络犯罪背后有很多动机，除了经济利益之外，威胁源的目标也可能是知识产权和商业机密。

IBM 的数据显示，对金融服务机构来说，内部人员造成的攻击占 58%，而外部攻击只占 42%，但是大多数内部人员并不知道他们造成了伤害。

超过一半 (53%) 的内部攻击源自“疏忽人员”，他们在无意间遭到了钓鱼攻击，或者来自其他连网系统的内部攻击。报告指出，在“疏忽人员”造成的威胁方面，金融服务机构面临的威胁最为严重。

高兰德说，拒绝服务攻击和网络攻击也是很严重的问题。威瑞森近期发布的《2017 年数据泄露调查报告》显示，与信息服务公司相比，金融和保险公司遭受的网络应用程序攻击数量高出 5 倍。他表示，一些企业能够承受将其网站下线一天。但是金融服务机构不能，尤其是开通了重要网络业务的大银行。三至四年前，针对银行的网络应用程序攻击开始增加，目前仍然是该行业的最大威胁。

“如果你是金融服务机构，那么你需要保护你的网络业务。”高兰德表示，“你的大部分资产和业务就在网络上，你需要对其进行控制。”

IBM X-Force 恶意软件研究人员还发现，用于攻击商业银行账户的恶意软件数量有所增加。商业恶意软件重出江湖了，IBM 对经常遭到 SQL 注入和 Shell 命令注入攻击的客户进行了监控。

阿尔瓦雷斯表示：“从 2014 年中期开始，这一趋势就开始了。一些恶意软件，包括 Dyre，Dridex，GozNym 和 TrickBot，开始瞄准商业银行服务。”她建议各公司评估其网络安全“免疫系统”，找出自己的漏洞，并考虑以下问题：你的终端安全吗？你对当前的威胁有足够的了解吗？你具有适当的身份管理解决方案吗？

高兰德建议密切关注员工的活动，确保每个人只能获得他们真正需要的信息。他说，企业还应该为所有网络应用程序实施多因素身份验证。

阿尔瓦雷斯表示，员工培训也很重要。企业应该教员工识别可疑的电子邮件，这样企业就可以避免成为网络钓鱼诈骗的受害者，并降低“疏忽人员”造成的攻击风险。

原文名称	Financial Services Sector the #1 Target of Cybercriminals
作者简介	Kelly Sheridan，Dark Reading 副编辑。
原文信息	2017 年 5 月 1 日发布于 Darkreading 原文地址原文出处　http://www.darkreading.com/endpoint/financial-services-sector-the--1-target-of-cybercriminals/d/d-id/1328775?
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《浏览器劫持恶意代码分析报告》

近日，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时，注意到一个通过劫持浏览器注入 JS 脚本，进行投放广告来获利的恶意代码，该恶意软件为“WebJs”。该恶意代码通过捆绑在其他第三方应用软件、注册机传播，运行后静默方式运行，劫持用户浏览器，注入恶意的 JS 脚本代码，来投放相关广告。

经分析，该恶意代码使用 Visual C++6.0 编写。样本运行后会验证版本信息并下载最新版本，判断系统版本，如果系统版本是 XP 则在注册表中添加自启动，HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，如果是 XP 以上系统则使用 Schedule.Service 组件，来设置计划任务。样本运行后从资源中释放 DLL 文件，利用 Windows 消息挂钩注入 DLL 到浏览器进程中，并挂钩关键 HTTP 请求 API(Hook 浏览器的 connect 函数)，当用户浏览器有 HTTP 数据请求时，进行劫持 HTTP 链接，并篡改 HTTP 响应包，向 HTML 网页中插入恶意代码来实现投放广告的目的。

通常我们在浏览网页的时候，会在浏览器上看到各种广告悬浮，我们认为这些都是由正常网站推送，而殊不知有些悬浮广告是由恶意代码通过劫持浏览器来推送的。安天 CERT 提醒广大网络使用者，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。目前，安天追影产品已经实现了对该类浏览器劫持样本的检出。

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，依据行为即可实现对上述木马程序进行有效检测，以下为其自动形成的分析报告：

文件被内部组件发现，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、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

根据动态行为（默认环境）得出该文件具有以下行为：

文件名	周观测 20170502 样本
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	308 KB
MD5	637F7B0883DDA35A8F7B8C0B99904420
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	BD 静态分析

运行环境

操作系统	Windows XP 5.1.2600 Service Pack 3 Build 2600
内置软件	默认、IE6、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

危险行为

行为描述	危险等级
延时	★★★

其他行为

行为描述	危险等级	行为描述	危险等级
获取主机用户名称	★	查找浏览器进程	★★
查找指定内核模块	★	获取计算机名称	★
获取系统版本	★★	连接特殊 URL	★
增加 run 自启动项	★	获取 socket 本地名称	★
从资源中释放 PE 文件	★★	释放 PE 文件	★
连接网络	★	利用 Windows 消息挂钩注入 DLL	★★
获取系统内存	★★	独占打开文件	★
创建特定窗体	★	获取驱动器类型	★
自启动	★		

延时、获取主机用户名称、查找浏览器进程、查找指定内核模块、获取计算机名称、获取系统版本、连接特殊 URL、增加 run 自启动项、获取 socket 本地名称、释放 PE 文件、从资源中释放 PE 文件、利用 Windows 消息挂钩注入 DLL、连接网络、独占打开文件、获取系统内存、获取驱动器类型、创建特定窗体、自启动。

报告地址：https://antiy.pta.center/_lk/details.html?hash=637F7B0883DDA35A8F7B8C0B99904420