安天周观察

主办：安天　2016 年 7 月 25 日（总第 49 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加首届中国网络安全产业大会并发表演讲

7 月 16 日，由中央网信办网络安全协调局指导，中国网络安全产业联盟主办的“2016 年中国网络安全产业大会”在北京召开。各领域专家领导、国内外企业齐聚一堂，对我国网络安全产业发展进行了深入探讨，共图我国网络安全产业健康快速发展。

中央网信办网络安全协调局副局长卿昱莅临大会主会场并致辞，她代表主管单位充分肯定了中国网络安全产业联盟成立半年以来所取得的成绩，并希望联盟作为中国网络安全产业的重要力量在推动产业发展上发挥越来越大的作用。

中国网络安全产业联盟常务理事、安天技术负责人在主会场带来了一场题为《中国网络安全产业的危局、症结与希望》的演讲。他首先提出：“网络安全能力的完善是中国作为网络大国走向网络强国必备的一个支点”，他以一张竖版中国地图解读了我国目前面临的网络安全风险态势，并指出大国网络空间面临的挑战是传统大国博弈和地缘利益竞合关系在网络空间的延展，大国的网络空间能力要由攻击者和窥视者来检验。他进一步介绍了安天捕获、分析、追溯的一些 APT 攻击事件，并专门介绍了安天刚刚发布的报告《白象的舞步——来自南亚次大陆的网络攻击》中的最新内容。

安天技术负责人认为网络安全技术是一个围绕机密性、完整性、可用性、真实性等安全属性展开的专业窄带领域，其技术方法是围绕规划、检测、防御、处置、加固、分析、加密、认证、取证、溯源等动作展开的。如果不断拓展网络安全技术的外延，把网络安全当做一个筐，把很多基础 IT 领域的产品和技术都塞进去，不但不利于解决网络安全问题，还只会使网络

（下转第三版）

安天助力 HITCTF 竞赛圆满落幕

近日，由安天、360 联合赞助的 HITCTF 竞赛圆满落幕，本次竞赛作为一场网络攻防的精彩演绎，在很大程度上增加了哈尔滨市各高校对 CTF 竞赛（夺旗大赛）和网络安全的关注度。竞赛采取线上形式，考题范围涵盖 Web、逆向、渗透、移动安全、密码分析、取证与隐写等方向，其中部分试题由安天提供。

竞赛共吸引了来自哈尔滨工业大学、黑龙江大学、吉林大学、成都大学、西安科技大学等高校的 47 支战队。最终来自哈工大的参赛选手，获得了本届 HITCTF 竞赛的第一名。在本次比赛中取得优异成绩的各位选手，不但可以获得丰厚的奖金，还可以得到一次到安天实习的机会。参赛队员们对本届 HITCTF 竞赛表示认可，并期待明年第二届 HITCTF 竞赛可以有更多的挑战和机遇。

安天总部举办“网安新兵训练营”

近日，安天哈尔滨总部举办了为期一周的“网安新兵训练营”，即安天 2016 新员工培训。24 位讲师为新员工准备了丰富的课程，分别从企业历史、企业文化、企业制度、企业产品、企业技术、企业目标规划等方面对安天进行了详尽的介绍，使新员工可以快速地了解安天，融入安天团队。同时，部分讲师也分享了从业以来的经验和感想，使新员工对网络安全这个领域有了新的认识和理解。

除了常规培训课程，新员工们还参加了“平衡天平、抢占高地、枕头大战”等一系列既有趣又富有挑战性的户外拓展活动，体验了团队协作的乐趣与重要性。

在培训课程的尾声，新员工们与安天技术负责人进行了一次深入地对话，对于新员工提出的各种问题，安天技术负责人进行了细致地解答，并表示很期待与各位新员工一同在网络安全这样一个有未来的领域中，开拓属于安天的新篇章。

每周安全事件

类 型	内 容
中文标题	黑客窃取波兰国防部数据 要求支付赎金 5 万美元
英文标题	Hackers Steal Data from Polish Defence Ministry and Ask for $50,000 Ransom
作者及单位	Catalin Cimpanu；Softpedia
内容概述	近日，Pravyy Sector 黑客组织公然在 Twitter 上敲诈波兰政府，他们表示，如果波兰不向其提供的乌克兰银行账号或比特币地址支付 5 万美元的赎金，他们就会泄漏从波兰国防部窃取的数据。 为了证明自己手上确实掌握有真实数据，Pravyy Sector 在 Twitter 上泄露了部分可能从波兰国防部窃取的文件，包括官方文件扫描以及截图，波兰国防部电脑桌面截图，以及含有 1368 个条目的 Excel 文件。该 Excel 文件类似本地内联网日志，包含轻量级目录访问协议 (LDAP) 路径、登录次数、错误的登录以及其他类似细节。
链接地址	http://news.softpedia.com/news/hackers-steal-data-from-polish-defense-ministry-and-ask-for-a-50-000-ransom-506342.shtml

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.Acecard.a[rog] 2016-07-19	该应用程序运行后私自联网下载恶意子包，执行有界面的安装操作，子包会弹出虚假钓鱼界面，获取用户隐私信息，造成用户隐私泄露，建议及时卸载。（威胁等级高）
		RiskWare/Android.Surya.a[prv] 2016-07-20	该应用程序运行后上传用户固件信息、位置信息以及保存在本地的数据到远程服务器，存在隐私泄露的风险，建议立即卸载。（威胁等级低）
		Trojan/Android.Godless.b[rog，exp，sys]2016-07-20	该应用程序伪装成 Google 插件，安装无图标，后台模拟 googleplay 下载协议实现 googleplay 商店应用搜索、浏览、下载，造成用户流量资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.simplelock.o[rog，sys]2016-07-22	该应用运行后会请求激活设备管理器，强制置顶界面，显示设备 ip 地址和设备信息，提示文件已被锁勒索，需要用户通过 iTunes vouchers 付费解锁，造成用户手机无法正常使用。（威胁等级中）
	较为活跃的样本	Trojan/Android.QQspy.m[prv，exp]	该应用程序伪装成 QQ，运行后展示虚假界面，短信窃取用户登陆账号和密码信息，造成用户隐私泄露，建议及时卸载。（威胁等级高）
		Trojan/Android.emial.dg[prv，rmt，exp]	该应用伪装成中国移动积分应用，诱导用户输入手机号码，会隐藏图标，获取手机固件信息并通过邮箱转发，监听拦截短信，获取恶意手机号码，同时向该号码发送短信，获取用户联系人并短信转发，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.Downloader.ca[rog，exp]	该应用程序安装无图标，在后台私自下载未知应用静默安装，并且私自启动安装程序在后台运行，造成资费损耗和电量损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.InfoStealer.w[prv，exp]	该应用程序伪装成正常应用，运行后隐藏图标，诱导用户输入邮箱账号密码，后台窃取通话录音、短信、浏览器历史记录、通讯记录、位置等用户隐私信息，并通过短信发送，建议立即卸载，避免造成隐私泄露。（威胁等级高）
		G-Ware/Android.HiddenAds.ab[rog，exp]	该应用程序伪装成系统应用，安装无图标，后台联网获取关键数据，频繁创建桌面图标，私自调用浏览器跳转到指定网页，建议立即卸载，避免造成资费损耗。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 无效索引远程执行代码漏洞 (CVE-2014-6334)	如果 Microsoft Word 在分析经特殊设计的 Office 文件时未正确处理内存中的对象，则会导致当前用户的上下文中存在远程执行代码漏洞。这可能允许攻击者执行任意代码，从而损坏系统内存。以下产品受到影响：Microsoft Word 2007 SP3，Word Viewer，Office Compatibility Pack SP3。（威胁等级高）
	较为活跃的样本	Trojan/Win32.Cryptodef	此威胁是一类可以加密用户文件，并勒索金钱的木马家族。该家族样本运行后会加密用户重要文档，弹出信息，用户必须付费才可以解密。（威胁等级中）
		Trojan/Win32.Wurser	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后连接远程服务器，收集系统信息并回传，还可以打开 cmd shell，进行一系列的恶意操作。（威胁等级中）
		Trojan/Win32.SandboxLover	此威胁是一类可以窃取用户信息，并有反虚拟机功能的木马家族。该家族样本运行后连接远程服务器，接受恶意操作，包括上传和下载文件、删除文件、运行文件等，同时可以判断当前环境是否为虚拟机环境，有一定威胁。（威胁等级中）
		Trojan[Spy]/MSIL.POS	此威胁是一类可以窃取用户信用卡信息的木马家族。该家族样本可以被用于 POS 机上，运行后可以在当前内存中查找与信用卡信息相关的字符串和算法，一旦发现，就会窃取并发送给远程服务器。还可以与远程服务器通信，接受恶意操作。（威胁等级高）

ATM 被窃取 200 万美元，两名嫌犯被追捕

路透社 / 文　安天公益翻译小组 / 译

台湾地区调查人员怀疑，近日 2 名俄罗斯人利用恶意软件攻入了一家大型银行的自动柜员机，从几十台自动柜员机中取走了超过 200 万美元，这是台湾地区出现的第一个此类案例。

调查人员指出，犯罪嫌疑人可能使用手机触发了第一银行的 41 台自动柜员机，使其吐出大量钞票。闭路电视摄像机显示，在每次取款时，嫌疑人迅速拿走吐出的钞票并离开，目前，他们仍然逍遥法外。

调查人员正在不断拼凑犯罪活动的实施过程，此次犯罪显示出，目前针对亚洲地区的 ATM 攻击越来越大胆。今年 5 月，一个犯罪组织在 3 个小时中，通过 14,000 次取款从日本 ATM 机中取走了 1,300 万美元。

自发现盗窃之后，台湾地区已经冻结了将近 1000 台此类自动柜员机 (由德国德利多富提供) 的取款业务。整个台湾地区 27,200 台自动柜员机的近 4% 受到了影响，客户不得不使用其他机器。

调查人员表示，两名俄罗斯犯罪嫌疑人已经确定，但是拒绝透露他们的名字。他们认为两名嫌疑人已经离开了台湾地区，但他们仍在调查是否有第三个人介入了犯罪活动。

相关发言人林政贤说：“到目前为止，我们认为该犯罪可能是远程完成的，如通过手机、笔记本电脑或被黑的第一银行员工电脑进行的。”

第一银行报告称，嫌疑人从自动柜员机窃取了 7,000 万新台币，约合 220 万美元。取款分多次进行，白天和晚上都有。

调查人员已经确定了用于触发取款的 3 个不同的恶意程序。他们在一份声明中指出：“在对恶意软件进行测试后，我们确定，被攻击的自动柜员机将立即根据恶意软件的命令吐出钞票。”

美国迪堡以 17 亿欧元 (18.8 亿美元) 的价格收购了德利多富自动柜员机，目前已经成为 ATM 的全球领导者，占 35% 左右的市场份额。

德利多富目前表示，他们已被告知台湾地区的 ATM 机遭受了攻击。德利多富的一位官员通过电子邮件告诉路透社记者：“攻击遵循类似的模式，我们还有银行都意识到它们的存在。警方、银行和德利多富的专家正在调查攻击的详细信息。为了支持当地团队，我们派出了安全专家。”

目前，调查人员拒绝对事件的细节发表评论，只是说第一银行将承担损失。他们还表示，第一银行的用户将不会受到影响，当地银行已经被要求在下个月建立自己的 ATM 机监控系统。

目前，台湾地区至少有四大金融机构暂停了其 ATM 的取款服务，以此作为预防措施。他们没有透露取款服务何时会恢复，也没有说暂停服务是否会影响其金融业务。

原文名称	Taiwan seeks two Russian suspects in $2 million ATM malware heist
作者简介	路透社，一家国际新闻机构，总部位于英国伦敦金丝雀码头。
原文信息	2016 年 7 月 13 日路透社发布，原文地址 https://en.wikipedia.org/wiki/Reuters
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)

安全不堪重负。他通过 2015 年全球主要国家和地区网络安全投入对比分析、中美网络安全上市企业经营数据分析等内容，解读了中国网络安全产业面临的问题。他认为网络安全技术发展需要以产业为动力，而产业是一种经济循环，是企业把市场回报投入到整个研发生产，改进产品服务，新产品进入市场，然后产生利润回报，再滚动到生产和研发的一个过程，只有形成持续不竭的循环增长，才会有技术的变革，才会有能力的持续成长。而国内网络安全产业发展的根本问题是内需不足，没有足够的市场，形不成足够的采购需求，产业就不会有相应的动力。

他以安天高级威胁检测产品“追影”为例，解读了自主创新安全产品的成本构成，说明了为什么低于成本价中标是对创新的一种伤害，以及会导致劣币驱逐良币，并最终伤害国家网络安全的基础能力。同时他指出，网路安全技术是当前中国信息技术门类中，积累最为系统，没有明显短板，而且已经有部分国际领先亮点的领域，我们不应妄自菲薄。

他表示，网络安全业界坚信随着总书记在“419 网信工作会议讲话”中提出的“安全和发展要同步推进”的要求得到逐步落实，随着网安业界同仁的共同努力，中国网络安全产业一定会迎来一个跨越式的大发展，成为中国网络强国的屏障。他也希望可以有更多年轻人加入到网络安全这个充满未来的行业中，一起努力，并肩战斗。

安天发布
《白象的舞步——来自南亚次大陆的网络攻击（一）》

近日，安天发布了名为《白象的舞步——来自南亚次大陆的网络攻击》的分析报告，披露了两组针对我国多领域的高频度 APT 攻击事件。安天对这一系列针对中国教育、科研、军事等领域的攻击行动，进行了近四年时间的持续监测、捕获、跟踪、分析，并将报告中的两组攻击统称为——“白象行动”。安天追影小组将在“安天周观察”发布三期报告，详尽地分析“白象行动”所涉及的三个样本。

1.“白象一代”概况

2012 至 2013 年，安天陆续捕获了来自白象组织的多次载荷投放，并依托关联信息同源分析，找到了数百个样本，这些样本多数投放的目标是巴基斯坦，少数则针对中国的高等院校和其他机构。

为了区分“白象行动”中两组不同的攻击波，我们将 2012 至 2013 年高度活跃的这组攻击称之为“白象一代”。“白象一代”投放了至少近千个不同 HASH 的 PE 样本，使用了超过 500 个 C&C 域名地址；其开发人员较多，开发团队技能混杂，样本使用了 VC、VB、.net、Autoit 等多种环境开发编译；同时其未使用复杂的加密算法，也未发现使用 0day 漏洞或 1day 的漏洞。PE 免杀处理是该攻击组织所使用的主要技巧，这也正是攻击中的 PE 载荷数量很大的原因之一。由于以上原因，“白象一代”被划分为轻量级 APT 攻击。

2. 样本行为

经分析，第一波攻击窃密样本 hash 0e9e46d068fea834e12b2226cc8969fd 功能如下：

1) 遍历磁盘文件，上传敏感文件及主机信息到服务器；

2) 添加启动项；

3) 遍历敏感文件 (*.doc; *.docx; *.xls; *.ppt; *.pps; *.pptx; *.xlsx; *.pdf)；

4) 上传文件到服务器；

5) 生成上传文件列表；

6) 文件上传前，规则化重命名文件；

7) 获取电脑主机信息；

8) 在当前用户以及所有用户启动文件夹中添加启动项。

3. 总结

从“白象行动”中我们可以看到，我国大量的基础信息安全环节和产品能力还不到位，“白象一代”被安天定性为轻量级 APT 攻击，以免杀 PE 辅以有限的社会工程技巧进行投放，但却成功入侵了中国的高等学府。目前，安天追影威胁分析系统已经可以对“白象行动”的相关样本进行检出，并持续提升对未知威胁的检测能力。

（未完待续，完整报告：http://www.antiy.com/response/WhiteElephant/WhiteElephant.html）

木马程序

安天【追影威胁分析系统】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、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、静态分析鉴定器、动态行为鉴定器、安全云鉴定器将文件判定为木马程序。

该文件具有以下行为：疑似 Hangover_ron_babylon 恶意代码、获取系统版本、打开自身进程文件、查找指定内核模块、设置自启动项、读取自身文件、连接特殊 URL、文件下载、请求加载驱动的权限、创建特定窗体、获取驱动器类型、获取系统内存、独占打开文件、访问文件尾部、获取计算机名称、获取主机用户名称、疑似桌面控制。

文件名	0E9E46D068FEA834E12B2226CC8969FD
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	282 KB
MD5	0E9E46D068FEA834E12B2226CC8969FD
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Spy]/Win32.KeyLogger.acqh
判定依据	安全云

◆ 危险行为

行为描述	危险等级
疑似 Hangover_ron_babylon 恶意代码	★★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
获取系统版本	★★	打开自身进程文件	★
查找指定内核模块	★	设置自启动项	★★
读取自身文件	★★	连接特殊 URL	★
文件下载	★	请求加载驱动的权限	★
创建特定窗体	★	获取驱动器类型	★
获取系统内存	★★	独占打开文件	★
访问文件尾部	★	获取计算机名称	★
获取主机用户名称	★	疑似桌面控制	★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=0E9E46D068FEA834E12B2226CC8969FD