安天周观察

主办：安天　　2015 年 8 月 10 日 (总第 4 期) 试行　本期 4 版　　微信搜索：antiylab

“一级学科研讨会”与会部分专家考察安天总部

安天小编 / 文

8 月 4 日，由中央网信办指导，中国网络空间安全协会 (筹) 主办，哈尔滨工业大学承办的“首届网络空间安全一级学科建设研讨会”在哈尔滨举行。来自全国 60 多所知名高校和科研单位的一百多位院长、专家、系主任和网络安全专业人士参与研讨会。

随着网络安全获批成为国家一级学科，和国家对网络空间安全的高度重视，网络安全人才的培养成为了产学研各界热议的问题。国内安全企业启明星辰、安天等也参加了会议。

来安天总部考察的部分专家合影

在会议室热烈讨论

会后，来自中国科学技术大学、华中科技大学、武汉大学、北京航空航天大学、国防科技大学、西安电子科技大学、北京交通大学、解放军信息工程大学等 14 所高校和来自国家信息中心、机械工业出版社等相

(下转第三版)

美国国安局 (NSA)：中国黑客 5 年内成功入侵 600 多家美国企业机构

近日，NBC 发布了 NSA(美国国安局) 威胁行动中心的一份简报，简报指出有超过 600 家的企业和机构遭到了中国黑客的入侵，并在地图上标示出了被攻击的企业、机构的具体地理位置。该简报是由一个匿名者提供给 NBC 的，其内容显示：中国黑客对 Google、国防承包商 (如洛克希德马丁公司)、航空交通控制系统等显示出了“浓厚的兴趣”。

简报中还暗示了 NSA 已经跟踪中国的网络攻击很多年，通过对中国的网络监控，他们能将这些攻击与特定的来源关联起来，并且简报中还详细列出了每一次攻击的具体来源。

据称，五年间，共有 600 多家美国的企业和机构被中国黑客成功侵入。美国正在筹划“反制”中国黑客。碰巧的是，该简报中还泄露了当下 NSA 和国防部领导正游说建立“cyber-deterrent”应对网络威胁计划。cyber- deterrent 是一种网络攻击能力，可以对那些攻击美国网络的敌人给予大规模且很严重的还击。

(文章来源：http://arstechnica.com/tech-policy/2015/07/nsa-report-shows-china-hacked-600-us-targets-over-5-years/)

安天 CERT 发布《解开勒索软件的真面目》报告

8 月 5 日，安天 CERT 发布一篇名为《揭开勒索软件的真面目》报告，对近两年在网上盛行的恶意软件“勒索软件”进行了分析解读。报告中介绍了何为勒索软件、其主要的传输手段、表现形式、分类以及演进史。文章中还列举了勒索软件对网民进行勒索的真实案例并给出了不同平台的下的防御建议。勒索软件的技术含量不高，却对用户的数据安全造成严重危害。

安天工程师建议，只有安装侧重于保护数据安全的工具或部属针对企业安全特点的安全产品，才能尽可能避免给勒索软件以可乘之机。(报告地址：http://www.antiy.com/response/ransomware.html)

APT(高级持续性威胁)

类 型	内 容
中文标题	黑客利用日本宾馆 WiFi 窃取机密 间谍活动或持续 4 年
报道时间	2015 年 8 月 4 日
关联对象	卡巴斯基研究所；WiFi
内容概述	据日本共同社报道，俄罗斯信息安全公司“卡巴斯基研究所”近日发布消息称，黑客利用高档宾馆的 WiFi 从入住的企业高管及研究负责人的电脑等终端窃取机密信息的事件频频发生。卡巴斯基研究称，黑客似乎能提前掌握企业高层等入住宾馆的计划，这样的间谍活动至少已持续了 4 年。 据悉，黑客首先侵入宾馆的系统，使连上 WiFi 的住客电脑上显示软件更新的画面，引诱安装病毒程序，从而窃取企业的机密信息。宾馆及受害企业的名称未透露。目前已在日本发现超过 2000 台电脑感染病毒，占全球总确认数量的 2/3。 卡巴斯基研究所表示，“正与相关警方共同致力于减少攻击造成的损失”，呼吁人们在旅行地谨慎更新软件，并安装杀毒软件加以应对。
链接地址	http://www.myhack58.com/Article/html/1/4/2015/65337.htm

恶意代码信息

经安天【CERT】检测分析，本周有 1 个移动平台和 14 个 pc 平台的恶意代码新家族值得关注

病毒分类	病毒名称	病毒特点
移动平台	Trojan[Banker]/AndroidOS.SmsBlock 发现时间：2015-07-28	一类安卓平台的银行家木马。该家族会获取网络连接状态，在未授权情况下访问特定网站，会向用户显示一些诈骗短信，会获取用户的联系人信息。
PC 恶意代码	Trojan[Spy]/VBS.Agent 发现时间：2015-07-27	一类使用 VBS 脚本写成的具有监视功能的木马家族。该家族样本可以访问系统安全中心，记录下系统所拥有的防火墙和反病毒软件，并生成记录文档。
	Trojan[Spy]/MSIL.Recam 发现时间：2015-07-30	一类间谍件，属于木马家族。该家族样本运行后可能会连接网络下载其他恶意代码并安装，收集用户敏感信息并回传等。
	Trojan[Rootkit]/Multi.Goodkit 发现时间：2015-07-31	一类可以窃取用户系统信息的木马家族。该家族样本通过邮件或系统漏洞感染计算机，运行后可以连接网络下载其他恶意代码并执行、收集系统敏感信息并回传给攻击者、发送邮件、修改本地文件等。
	Trojan[Ransom]/Script.Agent 发现时间：2015-07-31	一类用于勒索用户的木马家族。该家族样本是一类脚本，运行后会加密脚本中指定后缀文件。加密后，当用户点击被加密的程序，会弹出网页，引导用户购买解密密钥等。
	Trojan[PSW]/Win32.Puty 发现时间：2015-07-31	一类窃取用户密码的木马家族。该家族样本伪装成 PUTTY 程序，运行后，会修改注册表文件，搜集某些应用程序 / 服务的登陆、FTP 等账户和密码，并会发送到远程服务器上。
	Trojan[PSW]/Perl.Agent 发现时间：2015-07-31	一类窃取用户密码的木马家族。该家族样本是一类 perl 脚本，伪装成代理期，会搜集用户应用或者服务、FTP 等账户和密码信息，并回传到指定的 URL 上。而且，该样本会影响用户性能。
	Trojan[Banker]/JS.PhishPay 发现时间：2015-07-28	一类网络钓鱼的木马家族。该家族是一类 js 脚本，在浏览器中运行，会向用户显示一个伪装的银行在线支付办理的页面，诱导用户输入银行卡信息和个人信息。
	Trojan[Backdoor]/Win32.Zaluper 发现时间：2015-07-28	一类后门的木马家族。该家族样本运行后，会联网下载并运行恶意软件，设置后门程序，收集用户信息并回传。降低系统吸能，占用资源。
	Trojan/Win32.Wauchos 发现时间：2015-07-30	一类恶意下载的木马家族。该家族样本运行后，会在未授权的情况下下载安装其他恶意程序，而且会修改注册表，并禁用 LUA。会持续扫描 c：/windows/systeme32 目录，降低系统性能，占用系统资源。
	Trojan/Win32.Viknok 发现时间：2015-07-30	一类具有威胁性的木马家族。该家族样本通过不安全网页浏览和垃圾邮件安装到系统。该样本会与特定 C&C 服务器建立联系，用于接收指令。该家族样本能绕过 UAC，隐秘性强。
	Trojan/Win32.Gophe 发现时间：2015-07-29	一类带有威胁性的木马家族。该家族样本可以在 PC 上执行一系列有黑客发出的指令，并且会下载安装其他恶意程序。
	Trojan/Win32.CloudLook 发现时间：2015-07-28	一类带有恶意下载功能的木马家族。该家族样本运行后，在未经授权情况下，收集用户信息，回传至指定服务器，而且会下载恶意程序。占用系统资源，降低系统性能。
	Trojan/NSIS.InstallALL 发现时间：2015-07-27	一个恶意广告推广的木马家族。该家族是会感染浏览器插件，不断向用户弹出广告窗口，而且开机自启动。该样本会在控制面板下的添加 / 删除伪造一个假的条目，欺骗用户已经删除该样本，但系统重启后依旧会弹出广告窗口。
	Trojan/MSIL.IRPlan 发现时间：2015-07-27	一类具有威胁性的木马家族。该家族有写权限映射文件，会修改注册表，占用系统资源，设置后门程序，创建互斥量，降低系统性能。

斯诺登呼吁 IETF：请为用户而非间谍创建一个互联网

Kieren McCarthy / 文　　安天公益翻译小组 / 译

7 月 20 日，NSA(美国国家安全局) 举报人爱德华·斯诺登参与了 IETF(互联网工程任务组) 布拉格会议的网络直播，谈到了全球通信网络基础工程的一系列可能改变，这些改变将使政府更难开展大规模的监控活动。此外他一直敦促全球领先的互联网工程师小组设计一个“以用户为中心并保护人们隐私”的未来网络。

由于不是正式的 IETF 会议，只是布拉格事件参与者使用 IETF 场地组织的会议，所以该会谈并没有记录，只是一些与会者发了实时推特。它沿袭了电影《第四公民》的风格，该电影记录了斯诺登在香港一家酒店向记者泄露 NSA 文件的经过。

斯诺登在会议上反问道：“互联网为谁服务？ IETF 的最终客户是谁？”。答案是用户，而不是政府，也不是企业。

但是，他说：“目前的互联网协议泄露了太多的用户数据，我们需要以一种持久的方式将个人身份和角色分离开来”。

并强调信用卡的普遍在线使用会将个人身份与在线活动联系起来。

“如果这创造了更多的元数据，那就是坏事一件，因为元数据能够毁掉一个人”他说。相反，网络协议应该“遵循用户的意图”。他认为，DNS(域名系统) 查询和实际内容都应该被加密，这样的话，常态就是加密而非监控了。

斯诺登似乎对互联网协议的运作模式具有很好的了解，他指出了一个叫做 SPUD 的新协议，其结合了传输协议，能够减少用户在线互动时数据需要经过的“中间设备”的数量。

斯诺登指出，网络路径是间谍获取信息的最佳地点，每一个中间设备都是潜在的攻击点。但也警告说，SPUD 可能会使核心 UDP 互联网协议成为“泄露用户意图元数据的新渠道”。

他还指出，可识别的“持久”硬件地址是“极其危险的”，因为当用户使用无线互联网连接时，它能够将用户与 MAC 地址联系起来，这会导致用户身份和位置的迅速泄露。

斯诺登的讲话赢得了全场起立鼓掌。这不足为奇，IETF 和互联网工程师往往具有较强的独立性，并且他们很多人对 NSA 成功破解 IETF 开发的关键互联网协议 (甚至促使一些工作组开发便于间谍访问的新标准) 耿耿于怀。

斯诺登爆料后，IETF 的第一反应是建立一个新的 RFC 文件，目前该文件成为“目前最佳方法”。在 RFC 7258 中，该组织指出，“大规模监控是一种普遍的隐私攻击，IETF 将努力减轻大规模监控”。

原文名称	Snowden to the IETF - Please make an internet for users , not the spies
作者简介	Kieren McCarthy，The Register 的记者。
原文信息	2015 年 7 月 20 日发布于 The Register，http://www.theregister.co.uk/2015/07/20/edward_snowden_to_the_ietf_please_design_an_internet_for_the_user_not_the_spy/
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)

关单位共 30 位专家来到安天总部考察。参观了安天的反病毒博物馆和其他技术主题展室，观看了安天追影高级持续威胁分析系统等反 APT 系列产品的演示，安天技术负责人向来访专家介绍和展示了安天安全威胁感知捕获体系和后台分析流水线。

各方热烈探讨了网络安全人才培养机制、安全企业现有的人才需求、安全企业对教学科研提供工程资源的支持等问题。安天技术负责人向来访专家介绍了安天与有关高校紧密合作，在企业工程能力与高校科研能力结合方面所做一些尝试。如安天正在与国防科技大学共同建立“同源性样本分析标准范例集”。安天负责人介绍了在 2014 年提出的“安全工程师的能力结构和成长路径设计规划”、“网络安全工作者必读书目”等助动人才成长的计划，并期待高校、业内兄弟公司、出版机构能共同参与到这一计划中来，与会专家就这两项计划进行了热烈讨论，并对安天的发展提出了诸多宝贵的建议。各位老师的鼓励与建言，让安天获益良多，北航李舟军老师更是临行前为安天赋诗一首。

安天创业以来，积极参与教育和公益性活动，如支持高校 ACM 大赛、信安大赛等技术活动；为 GPG 等开源软件提供捐赠等。安天曾与哈尔滨工业大学建立联合应急响应组和病毒研究组，尝试与清华、武大等推动“捕风计划”、与清华合作推动“探云计划”等。安天多次与有关高校合作承担了国家自然科学基金、863 等相关科研课题。

安天在 2014 年、2015 年在哈尔滨先后两次举办“网络安全冬训营”，主题分别为“凛冬将至”与“北风乍起”，2016 年 1 月，安天将举办第三届网络安全冬训营，暂定主题“朔雪飞扬”。安天期待冬训营活动中看到更多高校师生来到北国冰城。

警惕 Office 远程代码执行漏洞 (CVE-2015-0097)

3 月，微软发布了一个 Office 的远程执行漏洞 (CVE-2015-0097) 安全补丁。7 月，安全研究人员 Eduardo Prado 公开了该漏洞的 POC 利用代码，攻击者能迅速适应流行的应用程序 (如微软 Office) 的最新漏洞，并且利用它结合知名的恶意软件 (如 PlugX) 定制攻击版本。由于 PoC 是公开的，很有可能有更多的攻击者会在他们的恶意活动中使用它。(原文链接：https：//www.fireeye.com/blog/threat-research/2015/07/cve-2015-0097_exploi.html)

安天安全研究人员对于这个 office 漏洞进行了分析，做出以下判断：CVE-2015-0097 是一个远程代码执行 (RCE) 漏洞，是由于微软 Office 应用程序存在一逻辑错误导致，Office 文档可以通过 MSScriptControl.ScriptControl.1 控件像 HTML 文件那样打开。如果文档包含有效 HTML 语句，HTML 会进入到本地安全区域。嵌到 HTML 正文里的脚本利用 ADODB.Recordset ActiveX 控件写入磁盘中 . 通过写入脚本到用户的 startup(开始) 文件夹中，攻击者可以完成远程代码执行并实现持久启动。

安天安全研究人员指出：此漏洞能够利用 Office 所有的文档格式，危害极高。受影响的版本范围包括：Microsoft Excel 2007 SP3，PowerPoint 2007 SP3，Word 2007 SP3，Excel 2010 SP2，PowerPoint 2010 SP2，and Word 2010 SP 。被攻击成功的电脑会被获取文件、发起 DDos 攻击，查看所有信息，窃取你的键盘输入密码以及知晓浏览器中的密码。

通过安天的追影高级持续威胁分析系统可以监控到 offdiag 和 DW20 进程创建，Office 诊断和系统崩溃，文档格式有高可疑。

目前，CVE-2015-0097 的安全补丁已发布，所以针对此漏洞的最有效防御措施是保持微软 Office 套件打上最新的补丁。

高级威胁

安天【追影高级持续威胁分析系统】无需更新病毒库，可实现对 Office 的远程执行漏洞 (CVE-2015-0097) 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，经由安全云鉴定器、智能学习鉴定器、动态行为 (默认环境) 鉴定器等鉴定分析。

依据动态行为鉴定器最终将文件判定为高级威胁。

该文件具有以下行为：格式溢出；获取系统版本；打开自身进程文件；关机；请求调试权限；获取主机用户名称；获取计算机名称；创建特定窗体；获取驱动器类型；获取系统内存；查找特定窗体；独占打开文件；请求加载驱动的权限。

文件名	192E6C88B3110D4890921FFDB318F586
文件类型	Document/Microsoft.RTF[:Rich Text Format]
大小	52 KB
MD5	192E6C88B3110D4890921FFDB318F586
病毒类型	高级威胁
恶意判定 / 病毒名称	Trojan[Exploit]/Win32.RTF
判定依据	动态行为
下次鉴定时间	约 2 周

◆ 危险行为

行为描述	危险等级
格式溢出	★★★★

◆ 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	★
关机	★	请求调试权限	★
获取主机用户名称	★	获取计算机名称	★
创建特定窗体	★	获取驱动器类型	★
获取系统内存	★★	查找特定窗体	★
独占打开文件	★	请求加载驱动的权限	★

◆ 文件操作

操作	文件路径
新建	c:\docume~1\alluse~1\applic~1\micros~1\office\data\opa12.dat
新建	c:\documents and settings\localservice\application data\microsoft\office\mso1033.acl
新建	c:\windows\temp\39359.cvr
新建	c:\windows\temp\39359.od
新建	c:\windows\temp\dw.log
新建	c:\windows\temp\a940.dmp
新建	c:\windows\temp\temporary internet files\content.ie5\index.dat
新建	\??\c:\windows\temp\temporary internet files\content.ie5\desktop.ini
新建	\??\c:\windows\temp\temporary internet files\content.ie5\8psf60lf\desktop.ini
新建	\??\c:\windows\temp\temporary internet files\content.ie5\l0h31j9g\desktop.ini

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=192E6C88B3110D4890921FFDB318F586