安天周观察

主办：安天　2015 年 10 月 26 日（总第 13 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

空军专家委考察团参观安天总部

10 月 20 日，由空军装备研究院某研究所所长、中国工程院院士费爱国带队的空军专家委考察团一行6人来到安天总部考察。

在新建成的安天展厅里，考察团观看了安天探海威胁检测系统、追影威胁分析系统、智甲终端防御系统等解决方案的演示，了解了安天的历史、发展现状及在技术创新上做的努力。安天技术负责人还带领各位专家参观了安天的反病毒博物馆、技术主题展室及安天安全威胁感知捕获体系和可视化演示。

在随后的讨论中，专家委成员和安天技术负责人就安天安全产品能力及如何与军队需求相结合、针对部队等特定对象的防护措施等问题进行探讨。

安天技术负责人向专家们介绍了安天产品在空军部队构建防护系统中可发挥的能力，针对费院士提出的“病毒在网络中横向移动时，怎么能够发现它是可疑东西移动？”和“在已知情况下可以发现安全威胁，是根据行为异常还是流量异常监控”等问题，安天技术负责人表示，这需要不断提升对手作业成本、方式和空间。通过桌面与服务器之间端口检测、增强内网检测能力和采用可视化能力手段获知端与端的移动等思路解决。

费院士及同行的专家们肯定了安天在安全方面做出的努力和成绩，表达了将安天安全产品与军队相结合的希望。费院士说：“网络安全是一场高人之间的博弈，而部队管理机制可以更有效检验和配合安全产品。从党政军角度出发，希望民企能够跟踪军队用户方面的需求，关注军队和国防安全系统安全威胁，为国防事业贡献力量。

新闻简报

ISIS 试图网络攻击美国电力公司

根据美国 CBS 电视台报道，ISIS 恐怖分子正在尝试网络攻击美国电力公司，进而关闭美国城镇和企业电力供应，但是没有成功。黑客还没有成功的原因是其技术技能较低，但联邦调查局官员警告说，这可以通过购买所需要的工具进行弥补，在黑市上容易买到相关攻击设备。（文章来源 http://www.cnbeta.com/articles/439753.htm）

日本两大机场遭黑客攻击　疑为知名黑客组织所为

据外媒报道，日本成田机场与中部机场日前曾经遭到黑客攻击。日本千叶县与爱知县警方在调查后发现，攻击这两座机场计算机系统的，可能是知名的国际黑客组织“匿名者”。（文章来源 http://news.sohu.com/20151019/n423591738.shtml）

普通电邮藏病毒，英国数千银行账户被黑损失巨大

据报道，英国国家重案署 (National Crime Agency，NCA) 公布，最近有黑客研发一款精密的恶意病毒，借将病毒隐藏在普通电邮中，入侵多国使用电子网络银行户口的用户计算机，盗取帐户数据后，交给不法分子进行诈骗。据指，该款软件在全球造成的损失达 7.8 亿港元（约合人民币 6.39 亿元），单在英国，就估计有数千账户被黑，损失达 2.4 亿港元（约合人民币 1.97 亿元）。据报道，该病毒名为“Dridex”，黑客把这种病毒加入隐藏在电邮和附件之中，用户一经开启即“中招”，最受影响的被指为 Windows 用户。（文章来源 http://www.mirror.co.uk/news/uk-news/hackers-user-computer-virus-harvest-6629699）

美国调查黑客入侵道琼斯：或是俄黑客所为

埃菲社报道称，美国联邦调查局 (FBI) 介入对道琼斯公司遭黑客入侵事件的调查。旗下拥有《华尔街日报》等媒体的道琼斯公司近日承认，黑客入侵可能导致 3500 人的信息泄露。报道称，美国总统奥巴马 4 月份下令对实施网络攻击或网络间谍行为的外国机构或个人实施制裁，并采取其他措施保护国家免受“黑客”袭击。（文章来源 http://mil.news.sina.com.cn/2015-10-19/1511841559.html）

每周安全事件

类 型	内 容
中文标题	TalkTalk 网站遭受攻击，或致 400 万客户数据被盗
英文标题	Data of 4 million TalkTalk customers likely stolen in wake of website attack
作者及单位	ZeljkaZorz， Help Net Security
内容概述	TalkTalk，英国最大的电信运营商之一，其网站于 10 月 21 日 (周三) 遭受一次“严重的持续性网络攻击”，可能导致近 400 万客户的个人数据被盗。泄露的数据可能包括客户的姓名、地址、出生日期、电子邮件地址、电话号码、TalkTalk 账户信息、信用卡详细情况以及银行账号详情。TalkTalk 已经通知了可能会受到影响的客户，并请伦敦警察厅网络犯罪部门进行调查；同时公司将为所有客户进行一年的信用监控。
链接地址	http://www.net-security.org/secworld.php?id=19019

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周 7 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.FakeFlashPlayer.i 2015-10-16	该应用伪装成 FlashPlayer，运行会请求激活设备管理器，隐藏图标，上传用户收件箱信息，接受远程指令，发送指定的短信，并拦截特定的短信，可能导致扣费。给用户造成隐私泄露和资费消耗。(威胁等级中)
		Trojan/Android.SysChecker.e 2015-10-17	该程序安装无图标，触发启动释放恶意子包，联网下载未知应用静默安装，拦截回复指定短信，可能会造成资费损耗，建议卸载。(威胁等级中)
		Trojan/Android.wsms.b 2015-10-17	应用运行后隐藏图标，拦截用户所有短信并通过服务器上传，对用户隐私造成严重的损害，建议用户立即卸载。
		Trojan/Android.lazyor.a 2015-10-19	程序运行后释放子包程序，隐藏自身，伪装成系统应用，自身会联网获取指令向指定号码发送指定短信，释放子应用会打开色情页面，无实际意义，对用户的安全造成极大损害，建议用户立即卸载。(威胁等级高)
		Trojan/Android.Downloader.al 2015-10-20	该应用伪装色情视频播放器，运行会后台私自下载 apk 应用频繁弹框安装界面，调用支付接口进行短信支付，频繁联网，造成用户资费消耗。(威胁等级高)
		G-Ware/Android.FakeSex.a 2015-10-20	该应用伪装成色情播放器，诱骗用户下载安装未知应用，诱骗用户激活设备管理器，会调用支付模块发送短信进行支付，造成用户资费消耗 (威胁等级高)
		Trojan/Android.Fakegupdt.s 2015-10-20	该程序安装运行之后，要求激活设备管理器，使用户不能正常卸载，并捆绑了恶意结构，就算主程序卸载之后还是能存在于设备上，并伪装成系统升级服务，诱导用户点击下载广告，会造成用户大量的流量资费的损失。建议不要安装该软件。(威胁等级中)
PC 平台恶意代码	新出现的样本家族	Trojan/MSIL.Trup 2015-10-20	此威胁是一类使用 MSIL(微软中间语言) 编写的木马类程序的统称，可以窃取用户信息、下载并安装其它恶意代码，通常会注入到其它进程中来隐藏自身并修改注册表使其自启动，也可能利用漏洞创建后门进行恶意操作。(威胁等级中)
		Trojan/Win32.BlackMirror 2015-10-16	此威胁是一类木马程序。运行后会在系统目录下释放一个 DLL 文件，并加载运行。收集系统信息并回传到 C&C 服务器上。(威胁等级中)
		Trojan/Win32.JripBot 2015-10-16	此威胁是一僵尸网络类木马程序。运行后在用户数据目录下副本文件，并将其注入到 Explorer.exe 进程中。链接网络等待指令。(威胁等级中)
		Trojan[Ransom]/Win32.Rotor 2015-10-19	此威胁是一类可以对用户文件加密并可能勒索赎金的木马家族。该家族样本运行后加密用户系统中文档、可执行程序、配置文件等，加密后在文件名尾加上攻击者的邮箱地址，只有联系该攻击者，支付赎金，才可能获取解密程序，(威胁等级中)
	活跃的格式文档漏洞 0day 漏洞	“Word RTF ‘listoverridecount’ 远程代码执行漏洞” CVE-2012-2539	该漏洞通过特制的 RTF 数据，远程攻击者利用该漏洞执行任意代码或导致拒绝服务 (内存破坏)。又名“Word RTF ‘listoverridecount’ 远程代码执行漏洞”。

汽车黑客攻击的 5 大教训

Andy Greenberg / 文　　安天公益翻译小组 / 译

这个夏天是黑客攻击的奥斯卡盛会。在 Black Hat、Defcon、Summercon、HOPE 和 Usenix 等各大会议上，追求名利和声望 (偶尔也追求使世界更安全的梦想) 的善意黑客们向全球观众展示了他们能够做什么。今年，他们向我们展示了：他们可以“黑进”汽车。

在过去 3 个月的一系列“概念证明”攻击中，安全研究人员展示了各种攻击手段，包括解锁车门、打开风挡刮水器、改变方向盘的反向，甚至在高速公路使吉普车瘫痪等。对于关注此类头条新闻的人来说，这看起来像是联网汽车启示录。

现在，让我们来回顾一下被称为“汽车攻击史诗”的 2015 年夏天，希望能够抛掉恐惧并找到一些经验教训。下面是我们所学到的教训。

1. 汽车公司需要黑客

当黑客查理·米勒和克里斯·瓦拉塞克展示，他们能够完全地远程控制 2014 款吉普切诺基，并关闭其刹车和变速器时，克莱斯勒在声明中回应，他们组织了“嵌入式系统质量工程团队”，致力于确定和实施软件的最佳实践。

但是，该团队显然没有找到或修复任何安全漏洞，包括连接到互联网的汽车仪表板计算机和关键驱动系统。要想使汽车免遭像米勒和瓦拉塞克般黑客的攻击，汽车公司的安全团队将不得不雇用他们审查代码的安全漏洞，然后才能进行部署。

2. 汽车需要免疫系统

漏洞是不可避免的。即使汽车公司开始趋之若鹜地雇用黑客，或以其他方式极大地提高安全审核技能，他们也无法找到所有的漏洞。

I Am the Cavalry(一个非营利性的草根安全公司，致力于弥合黑客和汽车行业之间差距) 的创始人之一乔希·科尔曼表示，他们需要能够实时地检测、记录并响应攻击的汽车功能。这意味着，汽车制造商需要以某种方式构建汽车，使得任何漏洞的损害都得以限制。

尽管越来越多的汽车连接到互联网，但是大多数联网车辆还不具备接收“网络”更新的能力。就米勒和瓦拉塞克的吉普车攻击事件，克莱斯勒的响应是：向 140 万客户邮寄 U 盘进行更新 (这可不是一种安全的修复技术)。

3. 汽车网络安全超越汽车本身

并不是每一个汽车攻击漏洞都归咎于汽车公司。今年 8 月，UCSD 安全研究团队证明了这一点，他们攻击了由汽车保险公司提供的一款可插入汽车仪表盘的 OBD2 端口常见的小工具，来跟踪汽车的速度和加速。最后，研究人员通过短信攻破了这一小型的、不安全的联网加密狗，从而访问克尔维特的内部网络并禁用其刹车。

换言之，联网设备也能为黑客提供打入汽车 (即使本身未联网的汽车) 的通道。智能手机也可以提供一种更简单的进入汽车的途径，然后攻击使得通用汽车、克莱斯勒、宝马和奔驰争夺一个软件补丁。它说明了，插入汽车的小工具也会成为漏洞。

4. 客户需要注意

当汽车公司开始为不安全买单时，他们就会开始对安全进行投资。如果消费者将消费转移到汽车的安全性上，那么汽车公司也会这样做。

2014 年，查理·米勒和克里斯·瓦拉塞克通过分析汽车的架构和机械规格，列出了最容易被攻击的汽车、卡车和 SUV(运动型多用途汽车)。但是，米勒也承认，该名单无法明确地帮助用户做出购买选择。

如果一些国会议员有办法，那么将汽车安全性纳入购买决策就会变得更加容易。当然，米勒赞同后来颁布的“要求经销商在汽车窗户上张贴信息卡，展示汽车的安全和隐私信息以及其他数据”的法案，并说道：“这是一个公共安全问题，汽车公司并没有挺身而出，告诉我们他们在做什么。作为消费者，我们除了自我保护之外别他法。我认为政府强制性地做出改变是一个绝佳的机会。”

5. 监管者也要注意

NHTSA(美国国家公路交通安全管理局) 是最直接负责汽车安全的政府机构，它采取了前所未有的措施，迫使克莱斯勒召回了 140 万辆汽车，以修复米勒和瓦拉塞克指出的安全漏洞。

汽车攻击的新世界说明，NHTSA 将不得不寻求能不间断召回每一个漏洞修复和发现汽车公司漏洞之间的平衡。它在 7 月份要求克莱斯勒迅速修复漏洞，最起码说明它已经不再沉睡了。

原文名称	5 Lessons From the Summer of Epic Car Hacks
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 10 月 8 日《连线杂志》发布，原文地址 http://www.wired.com/2015/10/five-car-hacking-lessons-we-learned-this-summer/
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。

打击网络犯罪，PTD 和 PTA 实现追踪广告流量木马

随着互联网技术的发展，新型的网络犯罪将计算机信息系统、互联网作为侵害对象或者犯罪工具，既包括侵入、危害计算机信息系统的新型犯罪，也包括传统犯罪在互联网上的新型表现形式，越来越多的组织、个人成为其受害者。

近期，安天追影团队发现一个利用 Rootkit 隐藏的广告流量木马。

该木马造成的获利的犯罪过程为：嫌疑人以各种手段传播木马，致使大量受害主机下载该木马，受害主机感染木马后，会自动访问“领跑网吧广告传媒 (域名为 lingpao8.com)”的计费广告链接，该公司的业务是广告传媒、浏览首页、开机广告等，领跑按照推广流量分给下家收益，通过大量受害机访问对应的广告链接，犯罪嫌疑人即可从领跑公司获得相应收益。

针对网络犯罪涉案人数众多且无法逐一收集相关言词证据的问题，《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》建议要综合全案证据，依据电子数据、书证等证据记录的情况，认定被害人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实。

在对此付费广告木马线索的分析、监控、回溯过程中，使用安天探海威胁检测系统 (PTD) 和安天追影威胁分析系统，实现了追踪网络犯罪的案例，通过发现线索、分析、监控等手段，追踪犯罪证据、犯罪嫌疑人，有效的协助网路犯罪案件的顺利侦破。展示了 PTD、PTA 产品在打击网络犯罪中的强大功能。

PTD 即安天探海威胁检测系统，是安天自主研发的网络流量检测设备，它支持以下业务和解决方案：

——部署于网络核心交换机处，通过镜像接口获取流量，对流量进行检测与分析，并通过图、表、日志等形式直观显示网络态势；

——支持分布式多级部署，可集中管理、呈现整网综合网络态势 (风险分布、风险实时监控与告警、高危 TOP 统计等)；

——与安天 PTA 联动，发现未知威胁，构筑完备的反 APT 防线。

PTA 即安天追影威胁分析系统，是安天出品的一款应对 APT(高级持续性威胁) 攻击的设备级鉴定产品。追影威胁鉴定系统的目的是用于检测和分析一切可能用于 APT(高级可持续威胁) 攻击的文件，它利用虚拟加载执行、动态监测进行深度安全分析，从而有效检测 0day 格式溢出应对高级安全威胁，深度提取可执行样本行为针对未知木马进行判别，提供详细的文件结构及行为报告。

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

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。

依据动态行为鉴定器、智能学习鉴定器最终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；注入其他进程；劫持 API(Inline Hook)；填充导入表 (疑似壳)；连接特殊 URL；隐藏文件；请求调试权限；释放 PE 文件；获取系统内存；获取系统版本；访问文件尾部；访问其他进程内存；获取计算机名称；获取 socket 本地名称；遍历进程；访问 DNS；创建服务；连接网络；创建特定窗体；获取驱动器类型；独占打开文件；打开自身进程文件；获取主机用户名称；启动服务；查找指定内核模块；从资源中释放 PE 文件到系统目录；查找特定窗体；请求加载驱动的权限。

文件名	FDA5CF3A25896F5EB08C622E5FEC3150
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	444 KB
MD5	FDA5CF3A25896F5EB08C622E5FEC3150
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Rofin.A
判定依据	智能学习

◆ 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	★★★	注入其他进程	★★★★
劫持 API(Inline Hook)	★★★★		

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=FDA5CF3A25896F5EB08C622E5FEC3150

◆ 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)	★★	连接特殊 URL	★
隐藏文件	★	请求调试权限	★
获取系统内存	★★	释放 PE 文件	★
访问文件尾部	★	获取系统版本	★★
获取 socket 本地名称	★	访问其他进程内存	★
访问 DNS	★	获取计算机名称	★
创建特定窗体	★	遍历进程	★
独占打开文件	★	创建服务	★
启动服务	★	连接网络	★
查找指定内核模块	★	获取驱动器类型	★
从资源中释放 PE 文件到系统目录	★★	打开自身进程文件	★
请求加载驱动的权限	★	获取主机用户名称	★
		查找特定窗体	★