安天周观察

主办：安天　2016 年 1 月 11 日 (总第 24 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

第三届网络安全冬训营“翔雪飞扬”回顾

2016 年 1 月 7 日，由黑龙江省委网信办、黑龙江省公安厅主办，安天承办的第三届网络安全冬训营在哈尔滨友谊宫开幕，为期 3 天。来自中国信息安全测评中心、国家互联网应急中心等行业管理机构；复旦大学、哈尔滨工业大学、哈尔滨工程大学等高校；中国电子科技集团公司三零所、五十四所等院所等单位的学者、专家、网络安全从业者和爱好者近 300 人参加了此次冬训营。

黑龙江省委网信办李耀东主任为冬训营致辞，他表示，冬训营是既富有行业特色又兼具地域特色的网络安全活动，既有北国冰城的特色，也代表了网络安全面临的形势。来自全国网络安全行业的友人欢聚在此，坦诚交流，共商网络安全之计，共话互联网治理之道，希望冬训营将为这座四季分明，具有风情韵味的城市增加更多的活力。

真知灼见

本届网络安全冬训营以“情报的支撑，塔防的实践”为核心议题，邀请到了国内一流网络安全技术专家、院校研究者、安天第一线的网络安全工程师带来了内容丰富，且具有极强实践性的演讲议题，涉及到 APT(高级持续性威胁) 事件分析、热点安全事件分析、移动安全等热点内容。

安天讲师议题	
安天研究院	《反 Rootkit 工具的发展演进》
安天反病毒引擎研发中心	《恶意代码网络犯罪追踪》
安天 CERT (安全研究与应急处理中心)	《2015 年安天应对的威胁事件回顾分析》
安天移动安全研发中心 (AVL TEAM)	《浅谈移动养殖系统和 IOS 安全》
安天移动安全研发中心 (AVL TEAM)	《基于移动威胁情报的安全价值观》
安天反病毒引擎研发中心	《 Adobe Flash 恶意代码分析》
安天 CERT (安全研究与应急处理中心)	《浅析 PowerShell 威胁攻击》
安天微电子与嵌入式研发中心	《工欲善其事，必先利其器——通用硬件安全开发平台的研制和应用案例》
安天数据研发中心	《你的眼睛喜欢看什么》
安天 CERT (安全研究与应急处理中心)	《解析 VBA 宏病毒》

专业碰撞

目前，APT 已成为网络安全的主要威胁，威胁情报共享亦成为热点话题，在本届冬训营中许多学员的提问都是针对高级威胁和威胁情报共享等新兴方向的。

在安天看来，威胁情报要以可靠的基础威胁检测能力为基础，应对 APT 威胁需要依托传统和新的布防点，参考塔防等纵深防御的思路来建设，通过多个环节持续的阻截和消耗攻击者的能力，同时使多个环节间有效的响应等有效的实践和手段来支撑起信息化的大厦。

意外惊喜

为帮助学员对议题加深理解与研究，同时本着沉淀与分享，交流与提升的理念，安天为每一位学员准备了丰富的学术资料，包含技术文章汇编《移动安全专题第二分册》和《APT 专题第二分册》以及《安天反高级威胁解决方案》等。其中《APT 专题第二分册》属于首次发布，包括了此前从未公开的分析报告 (索尼事件)、很少抛头露面的 (HangOver) 以及近期公开的 APT 事件 (方程式、APT-TOCS) 和技术演讲 PPT 等诸多内容。

此外，为感谢所有讲师的付出，冬训营特地打造了一套纯银纪念币，为本届网络安全训练营增添了一份惊喜。

安天技术负责人肖新光：弹道有痕—中国面临的 APT 攻击的风险与案例分析

原中油瑞飞技术总监黄晟：塔防在私有云安全中的实践

ThreatBook 创始人 CEO 薛峰：威胁情报落地姿势

网络安全专家 Pott1：社会工程学攻击建模 (3)

国家 973 项目首席科学家杨珉：移动应用隐私保护研究

炼石网络 CipherGatewayCEO 创始人 白小勇：塔防在 CipherGateway 安全加固方面的思路及实践

神州网云 CEO 宋超：威胁情报在 APT 攻击检测事件中的价值体现

每周安全事件

类 型	内 容
中文标题	时代华纳疑似被入侵，30 多万客户资料数据泄漏
英文标题	Time Warner Cable：Customer data “may have been compromised”
作者及单位	NARINDER PURBA，WeLiveSecurity
内容概述	美国最大的有线电视公司时代华纳，近日表示旗下约有 32 万用户的邮件和密码信息已被黑客窃取。据悉，这些邮件和密码信息很有可能是通过网络钓鱼的方式获得，同时也可能是保存了时代华纳用户数据的第三方合作商信息泄露所致。 然而，时代华纳出现相关的数据安全问题已经不是第一次了。在 2009 年，一个叫做 David Chen 的博主就在他的博文中说，他发现在时代华纳的调制解调器和无线路由器之间存在着漏洞，此事曾引起了舆论的广泛关注。
链接地址	http://www.welivesecurity.com/2016/01/07/time-warner-cable-customer-data-may-compromised/

每周值得关注的恶意代码信息

经安天检测分析，本周 10 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.100goujs.a[prv] 2016-01-04	该应用伪装成系统应用，安装无图标，后台接收短信指令，获取用户地理位置信息并通过短信发送，造成用户隐私泄露，建议卸载。（威胁等级高）
		RiskWare/Android.FakeMycheering.a[fra]2016-01-04	该应用属于非官方应用，重打包的“柠檬助手”，恶意篡改，植入了广告代码和风险代码，建议卸载该应用，下载安装官方正版应用。（威胁等级低）
		Trojan/Android.eneity.e[pay，rmt] 2015-12-24	该应用植入其他正常应用，运行后会私自发送付费短信；接收短信指令，根据指令发送付费订阅短信，造成用户资费损失，建议卸载。（威胁等级低）
		Trojan/Android.fakebaidusdk.b[exp] 2016-01-05	该应用程序运行后台联网上传固件信息，下载未知文件，会造成一定资费损耗，建议立即卸载。（威胁等级中）
		G-Ware/Android.HiddenAds.j[rog，exp]2016-01-06	该应用伪装成正常应用，无实际功能，运行后加载广告，会造成用户资费损耗，请谨慎使用。（威胁等级低）
		Trojan/Android.BqSpy.s[prv，spy] 2016-01-07	该应用运行后会隐藏图标，请求激活设备管理器，开机自启，后台联网上传用户设备相关信息，私自发送指定短信，监听短信，拦截指定短信并删除短信，造成用户隐私泄露。（威胁等级中）
	较为活跃的样本	Trojan/Android.Downloader.bc[exp]	该应用伪装成系统应用，安装无图标，私自联网上传用户设备相关信息，私自联网下载推送广告应用，还能静默安装和静默卸载，具有一定的流氓行为以及可造成用户资费消耗。（威胁等级中）
		Trojan/Android.SmsSpy.l[prv，exp，spy]	该应用运行会隐藏图标，私自发送短信，联网上传用户短信信息、通讯录信息、通话记录、浏览器历史记录和书签等信息，监听来电进行通话录音并联网上传，造成用户隐私泄露和资费消耗。（威胁等级中）
		Trojan/Android.FakeInst.dv[exp，sys]	该应用程序本身无实际功能，运行后隐藏图标，拦截短信，同时后台频繁联网可能会造成一定流量资费损耗。程序存在大量敏感高危权限可能会私发短信上传通讯录信息，建议立即卸载。（威胁等级中）
		Trojan/Android.FakeApp.av[prv，exp]	该应用程序伪装成刷钻应用，诱骗用户输入 QQ 账号密码，后台通过发送短信窃取用户隐私，建议立即卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 紧急修补漏洞——CVE-2015-8651	Adobe Flash Player 紧急修补漏洞 CVE-2015-8651，涉及一处整数溢出缺陷，可在受影响用户的电脑上远程执行代码，夺取系统控制权。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/NSIS.Adload.akj	此威胁是一种具有下载行为的木马类程序。通常使用 NSIS（开源的 windows 系统下的程序制作工具）将木马与正常程序捆绑在一起，主要功能是通过网络下载广告类程序。（威胁等级中）
		Trojan/Win32.Zbot.deb	此威胁是一种后门木马类程序。它可以接受远程控制、组建僵尸网络、窃取用户信息的间谍木马类程序。它能够持续的通过邮件的方式进行投放。（威胁等级中）
		Trojan[Dropper]/Win32.Mudrop.bdu	此威胁是一种具有捆绑行为的木马类程序，运行后取得用户完全控制权限，关闭安全软件，发送本机信息给控制端，并自行下载大量病毒文件到本地，危害极大。（威胁等级中）
		Trojan[Downloader]/Win32.Hmir.aeh	此威胁是一类具有下载行为的木马类程序。它们会自动下载并运行其他程序，收集储存在计算机中有价值的信息，如密码及其他数据，从而获取邮件与 FTP 账户。（威胁等级中）

2016 年我们将面临的最大安全威胁

Kim Zetter/ 文　安天公益翻译小组 / 译

任何研究网络安全的人都知道，黑客技术越来越大胆和复杂。在过去的一年里，出现了几个新的趋势，新的一年无疑将带来更多新趋势。我们预测，2016 年将出现以下情况。

◆ 勒索攻击

继 2014 年年底的索尼攻击事件后，我们预测，2015 年将会出现更多的勒索攻击。这里，我们所说的“勒索攻击”是指：攻击者威胁要公布敏感的公司或客户数据，逼迫受害者付钱或者满足其他要求。在这些攻击下，即使你已经备份了数据，不在乎黑客锁定了你的系统，但是数据被公布会毁掉你和你的客户。追踪此类攻击只有一个问题。如果受害者妥协并支付赎金，公众可能不会知道勒索的发生。但是，2015 年至少发生了两起记录在案的勒索攻击：婚外情网站 Ashley Madison 攻击事件；阿拉伯联合酋长国 InvestBank 攻击事件。勒索攻击者深知企业和高管们的命门，如果处理不好，公司的秘密将会被泄露，客户将会提起诉讼，高管们将会失去工作。我们预测，2016 年此类攻击将会更为普遍。

◆ 更改或操控数据的攻击

在今年的证词中，国家情报总监詹姆斯·克拉珀向国会陈述，更改或操控数据以破坏其完整性 (而非删除或公布被盗数据) 的网络攻击将会是我们的下一个噩梦。NSA(美国国家安全局) 和美国网络司令部的负责人迈克·罗杰斯说了同样的话。与 Stuxnet 造成的物理破坏相比，数据破坏更加难以察觉。这是因为，数据变化可以非常细微，但会造成巨大的后果和影响。有没有人记得上世纪 90 年代 Lotus 1-2-3 漏洞，这是一个无意的错误。但是，攻击者可以进入金融和股票交易系统，更改数据，根据其目的迫使股票价格上升或下降。某些类型的数据操控甚至可能导致死亡。第一次海湾战争期间，由于控制计算机的软件故障，一枚爱国者导弹在沙特阿拉伯未能拦截进入的飞毛腿导弹，导致 28 名士兵丧生，这也是一个无意的错误。

◆ 芯片密码创新

每当安全社区关闭一个攻击途径后，黑客们总会迅速适应并找到另一个途径。当零售商不再存储客户的信用卡号码和交易信息时，黑客们进入其网络，获取被发送到银行进行验证的实时未加密数据。当零售商加密传输中的实时数据时，攻击者则在 POS(销售终端) 读卡器上安装恶意软件，在刷卡之后和数据加密之前获取数据。现在，银行和零售商已经开始推出新的芯片密码卡，再次防御黑客的攻击。但是，这不会完全防止欺诈行为；只是简单地将攻击从实体商店转移到在线商店。我们预测，此类在线诈骗将会增加。

◆ 物联网僵尸网络的兴起

有许多人说，2015 年是物联网之年；但是，2015 年也是物联网被黑之年。这一年，很多连网产品被证明易受黑客攻击，包括连网的汽车、医疗设备、滑板和芭比娃娃。如果说 2015 年是概念证明物联网设备攻击的一年，那么 2016 年将是许多概念攻击成真的一年。我们已经发现的趋势是利用物联网设备形成僵尸网络。黑客不再劫持笔记本电脑，而是利用物联网设备的大型网络，如 CCTV(闭路电视) 监控摄像机、智能电视和家居自动化系统来形成僵尸军团。

◆ 更多的后门

2015 年年末，Juniper Networks 公司披露，它的某些防火墙的固件中存在高级黑客安装的两个后门。其中一个后门允许攻击者解密通过 Juniper 防火墙 VPN 的受保护流量，说明罪魁祸首是国家攻击者，因为只有政府情报机构才具备足够的资源来拦截大量 VPN 流量，利用后门受益。更令人吃惊的是，该后门程序基于一个追溯到 NSA 的后门。没有证据显示，Juniper 后门是由 NSA 安装的；更可能的是，NSA 的间谍合作伙伴 (可能是英国或以色列) 或美国的敌人安装了该后门。但是现在，公司和研究人员确切地知道，该后门在系统中的样子以及它如何运作。我们预测，2016 年，随着企业更严格地审查其系统和产品，更多后门将会被发现。

原文名称	The Biggest Security Threats We'll Face in 2016
作者简介	Kim Zetter，《连线杂志》一位屡获殊荣的资深记者，研究范围包括网络犯罪、隐私和安全。
原文信息	2016 年 1 月 1 日《连线杂志》，原文地址 http://www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/
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《SQLServer 样本追踪分析报告》

近日，安天追影小组注意到在某反病毒论坛有用户反映：Windows 服务器运行速度很慢，服务器的 CPU 被大量占用。经分析原因是被恶意运行了旺宝平台刷流量的挂机软件，在后台大量访问淘宝链接。黑客利用大量挂马，通过挂机软件进行刷流量赚钱，导致服务器运行速度缓慢，且运行在服务器的某杀毒软件不能识别，人为手动删掉后仍会出现。

经过 PTA 追影系统分析，此样本属于捆绑式恶意刷广告的恶意程序，主要释放旺宝刷流量的相关程序。主要特点是通过访问数据库是否成功来实现是否继续运行，通过占用任务管理器句柄来实现无法使用 taskmgr.exe 以达到无法结束此恶意刷流量软件 (由于网吧的关闭按钮实现的最小化的功能)。通过查找窗口类名及按钮对象来实现旺宝软件的一键隐藏功能。

该恶意程序首先通过远程连接数据库以判断网络是否通畅，然后查询远程数据库中的数据与被挂载机器的 IP、mac 和系统版本，再判断是否是黑客自己操作。除此以外，样本释放的衍生文件都是旺宝站点上的程序，其中的刷流量的旺宝 ID 为 622202。远程数据库的地址为阿里云免费提供的临时域名：qds199747491.my3w.com。该域名的主要行为是和 SQLSEVER 数据库通信，然后下载相关的旺宝软件，并提交刷流量任务。通过黑客追踪，可以发现，万网通过为购买 IP 服务的客户，提供一个临时的万网 my3w.com 下的免费二级域名，从而避免了备案信息和注册信息的登记。黑客正是采取了这种较为隐蔽的方式来隐藏自己的身份。

安天追影分析小组提醒大家，恶意挂机刷流量软件已经发展的很久很成熟了，用户不能因为安装了杀毒软件就放松警惕，有异常情况时，一定要及时检查电脑的安全性能。

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。

最终依据静态分析鉴定器、动态行为鉴定器将文件判定为木马程序。

文件名	BD960EB60878542CA40625034476B19D
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	5.24 MB
MD5	BD960EB60878542CA40625034476B19D
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Scar
判定依据	静态分析

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
Microsoft SQL Server 端口扫描	★★★	隐藏文件	★★★★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=BD960EB60878542CA40625034476B19D

该文件具有以下行为：Microsoft SQL Server 端口扫描；隐藏文件；读取自身文件；连接特殊 URL；获取驱动器类型；请求调试权限；释放 PE 文件；获取系统内存；增加 run 自启动项；访问 DNS；获取系统版本；打开自身进程文件；获取 socket 本地名称；结束进程；连接网络；创建特定窗体；独占打开文件；遍历进程；从资源中释放 PE 文件；获取主机用户名称；获取计算机名称；查找特定窗体。

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
读取自身文件	★★	连接特殊 URL	★
获取驱动器类型	★	隐藏文件	★★
请求调试权限	★	获取系统内存	★
释放 PE 文件	★	增加 run 自启动项	★
访问 DNS	★	获取系统版本	★★
获取 socket 本地名称	★	打开自身进程文件	★
结束进程	★★	连接网络	★
创建特定窗体	★	释放 PE 文件	★★
独占打开文件	★	遍历进程	★
从资源中释放 PE 文件	★★	获取主机用户名称	★
获取计算机名称	★	查找特定窗体	★