安天周观察

主办：安天　2017 年 1 月 9 日（总第 72 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

第四届网络安全冬训营召开

2017 年 1 月 6 日 -7 日，由黑龙江省委网信办、黑龙江省公安厅主办，安天承办的第四届网络安全冬训营在哈尔滨召开。

黑龙江省委网信办副主任王春涛，黑龙江省公安厅网安总队研究员孙安娜代表主办方为冬训营致开幕词。来自中国信息安全测评中心、国家保密科技测评中心、泰尔实验室等信息安全管理和测评机构；来自国防大学、清华大学、国防科技大学、哈尔滨工业大学、北京邮电大学、解放军信息工程大学、中国民航大学、天津理工大学等高校；来自部队、军工、能源、交通、金融、运营商等领域的专家、用户近 500 人参加了本届冬训营。

本届冬训营围绕“有效防护，价值输出”的主题展开。探讨安全检测、分析、防御技术以及大数据和威胁情报资源如何转化为真正有效的用户侧能力，如何更好的驱动全网威胁追溯、有效止损和绕前防御。研讨针对面向资产价值防护的威胁解决方案、端点防御的新技术工程实现、探索沙箱向威胁情报的可靠输出、介绍流量分析视角的安全服务模式等。

（从左到右）原国防科技大学研究院徐纬地、数字观星创始人郭亮、炼石网络 CEO 白小勇、安天创始人 / 首席技术架构师肖新光、前中油瑞飞信息安全高级技术总监 / 塔防模型的最早提出者黄晟、360 企业安全集团总裁吴云坤。

本届冬训营由一天的开放式技术报告和一天的专题培训组成，共进行了 15 场技术报告演讲。

在冬训营首日现场，安天发布了《安天 2016 年网络威胁年报（征集意见稿）》（下称《威胁年报》）。《威胁年报》总结和回顾了 2016 年网络安全威胁，展示了安天态势感知和深度分析视角下的高级威胁、信息泄露和黑产大数据、供应链安全、IoT 安全等年度热点分析构成。与会专家对安天年报内容进行研讨，提出修订意见，最终版的《威胁年报》将在春节前发布。

2017 年 1 月 6 日：开放式技术报告

- 安天 2016 年网络威胁年报征求意见稿发布
- 寻找安全的起点
- 重要 APT 事件安天年度分析工作总结
- 移动威胁情报架构解析和实践分享
- 数据时代的企业安全观念
- 《六维空间》流量安全分析方法：助力 APT 全过程检测
- CipherGateway 产品安全实践与塔防模式探索

2017 年 1 月 7 日：专题培训

- 下一代威胁检测引擎
- 移动威胁对抗升级——人与机器辩思
- 面向新兴威胁的终端防护技术
- 关键威胁的持续追踪与网络监测
- 基于本地沙箱的威胁情报输出
- 方程式组织 SPARC 架构样本的分析调试
- APT 样本关联与溯源方法
- SRAM 型 FPGA 的信息安全风险浅析
- 安天可视化的成长历程和自我批判
- Panel Discussion

报评

共筑“冰峰屹立”

网络安全冬训营到今年已是第 4 届。

网络安全冬训营是由安天发起并承办的一项网络安全交流培训活动，在每年一月北国最寒冷的日子里举行。每届冬训营分别设立一个富有冬季色彩的营语，已举行的四届分别为：“凛冬将至”、“北风乍起”、“朔雪飞扬”和“冰峰屹立”。同时，每届冬训营又会设置不同的主题，以此来进行议题的选取与设置。

在 2014 年第一届冬训营时，参加者还仅仅定位在：网络安全从业者、网络及信息安全监督管理部门等，注重的是知识性和技能性，很欣喜的是安天在基础检测、分析能力上的积累也得到了参与者的认可。2015 年，冬训营已经成为一个更大平台，冬训营的规格更高，来宾也更多，由时任中科院信息工程研究所副所长的孟丹主持，众多业内知名专家带来了网络安全战略、安全发展趋势、操作系统安全、加密认证安全等方面的研究成果与总结反思。2016 年，第三届冬训营的参加者已近 300 人，从主题“情报的支撑、塔防的实践”来看，围绕高级威胁、威胁情报等新兴方向，演讲内容更加注重实践性，关乎攻防焦点、关注新锐威胁。

伴随着安天的业务转型和发展，2016 年，安天开始了“第三次创业”，我们在思考如何能将积累了 15 年的威胁检测防御能力有效地转化为客户保障价值。今年冬训营的主题直接而明确——“有效防护，价值输出”，我们认为所有安全技术的发展和进步，包括安全检测、分析、防御技术以及大数据和威胁情报资源最终都要转化为真正有效的用户侧能力；所有技术点的起源、发展和价值体现最终都靠用户实践来检验和达成。

冬训营是一场分享，也是一场汇报，是一个永不结束的循环，近 500 从全国国各地莅临而来的嘉宾，便是安天人所说的“智者 . 安天下”中的智者，在“直面威胁，创造价值”的用户面前，安天永远扮演能力输出和服务的角色。在后续发展中，以可靠的检测、分析能力为基础，“深度赋能客户”，安天希望协助客户建立难以被攻击者预测的差异化能力和专有化的安全经验，与我们的用户一同越过江湖，成于沧海，不畏艰险，共同铸就“冰峰屹立”。

每周安全事件

类 型	内 容
中文标题	国际航空订票系统存在安全漏洞
英文标题	Changing travelers flight bookings is really too easy for hackers
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，国外媒体报道称，数千万人每天在用的“旅行预订系统”非常不安全，它缺乏应有的身份认证方案。相关研究人员指出，处理航班预订服务的“全球分布式系统”(GDS) 存在严重的安全问题。攻击者可利用系统的弱点，从而轻易更改、取消旅客预订的航班甚至可以利用退款系统为自己购买机票。GDS 可以看作是一个包含旅行预订等所有信息的庞大数据库，其中就有所谓的 PNR——也就是乘客姓名记录。它的数据内容包括旅行者的姓名、行程、旅行日期、票据细节、电话号码、电子邮件、护照信息、信用卡卡号、座位号和行李信息等。旅行数据对于骗子和钓鱼者来说相当有价值，利用这些数据，攻击者可以发起有针对性的攻击或是欺诈。
链接地址	http://securityaffairs.co/wordpress/54969/hacking/flight-bookings.html

每周值得关注的恶意代码信息

经安天检测分析，本周有 10 个移动平台恶意代码和 4 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.cashstealer.a[prv，exp]2017-01-02	该应用程序安装后无图标显示，启动后会诱导用户输入账号和密码并上传至服务器。会弹出虚假支付界面并锁定界面，诱导用户输入微信支付密码并上传至服务器。私自获取 root 权限，替换微信桌面快捷方式，窃取用户短信，窃取配置文件，删除系统文件夹，卸载微信。同时该应用包含风险代码，会将其他风险 apk 写入系统应用中，造成用户隐私泄露、财产损失，建议立即卸载。（威胁等级高）
		Trojan/Android.XAgent.a[rmt，prv]2017-01-02	该应用程序会篡改正常的应用，加入间谍类恶意代码。程序运行后会连网获取指令并上传用户隐私信息至服务器，其中包括用户手机固件信息、安装程序列表信息、短信信息、浏览器历史记录和书签、通讯录、通话记录、位置信息、SD 卡文件列表和文件信息、WiFi 相关信息，会造成用户隐私泄露。（威胁等级低）
		Trojan/Android.SexPay.a[exp，rog]2017-01-03	该程序是色情应用，运行后会在用户不知情的情况下私自连网并支付，造成用户资费消耗。（威胁等级高）
		Trojan/Android.Switcher.a[sys，rog]2017-01-05	该程序伪装成知名应用，程序运行会在后台获取设备所连 WIFI 的网关，并通过暴力破解方式登录到路由器设置界面，修改路由器 DNS 设置等信息，会导致用户访问网站异常及访问恶意网站。（威胁等级高）
	较为活跃的样本	Trojan/Android.Rootnik.p[rog，exp]	该应用程序无实际功能，运行后会检查 root 环境，下载文件进行 root，同时包含发送短信风险代码，会造成资费损耗，影响系统稳定，建议卸载。（威胁等级高）
		Trojan/Android.SmsSend.lk[exp，rog]	该应用程序会诱骗用户点击付费，私自发送短信订购付费业务，造成用户资费消耗，建议立即卸载。（威胁等级高）
		Trojan/Android.HiddenAds.au[exp]	该应用程序会伪装成系统应用，安装后无图标显示，运行后会弹出广告，其中包含 Google、Admob、Facebook 等各种广告插件，会造成用户资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.HiddenApp.q[exp，rog]	该应用程序会伪装成系统应用，安装后无图标显示，会私自后台连网并上传手机固件信息，会获取配置信息再次访问，建议用户警惕该程序私自下载，造成资费损耗。（威胁等级高）
		Trojan/Android.Fake Flash Player.w[prv，rmt，rog]	该应用程序会伪装成 FlashPlayer 插件，运行后会隐藏图标，诱导用户激活设备管理器，后续弹出虚假 Google Play 登录界面，诱导用户输入银行卡账号和密码等信息并上传至服务器。接收远程指令，执行上传短信，上传手机固件信息和收件箱内容，清除用户数据等操作。会向联系人群发送指定短信，短信转发用户手机固件信息，造成用户隐私泄露和资费消耗，造成财产损失，建议立即卸载。（威胁等级高）
		G-Ware/Android.jianmo.bn[rog，sys]	该应用运行后会激活设备管理器，并置顶界面，勒索用户添加指定 QQ 进行付费解锁，造成用户资费损失，建议不要安装。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	PHPMailer 命令执行漏洞 (CVE-2016-10033)	PHPMailer 是一个基于 PHP 语言的邮件发送组件，被广泛运用于诸如 WordPress、Drupal、1CRM、SugarCRM、Yii、Joomla! 等用户量巨大的应用与框架中。CVE-2016-10033 是 PHPMailer 中存在的高危安全漏洞，攻击者只需巧妙地构造出一个恶意邮箱地址，即可写入任意文件，造成远程命令执行的危害。（威胁等级高）
	较为活跃的样本	Trojan/Win32.Neurevt	此威胁是一种木马类程序。该家族样本运行后会添加自动启动项，劫持 Windows 系统还原程序，将自身文件拷贝到系统文件夹下，伪装成系统文件进行启动。设置进程保护，防止进程被系统结束，并向服务器发送信息。（威胁等级高）
		Trojan[Downloader]/Win32.Voila	此威胁是一种下载类木马程序。该家族样本运行后会与指定的远程服务器连接，下载其它恶意软件到本地运行。（威胁等级中）
		Trojan[Backdoor]/Win32.AutoIt	此威胁是一种后门类木马程序。该家族是通过 AutoIt 编写的后门程序。样本运行后会连接远程服务器，等待接收上传和下载文件、监视用户屏幕、记录键盘击键、查看进程和窗口等控制指令。（威胁等级高）

2017 年四大网络安全威胁新常态

Michael Mimoso / 文　安天公益翻译小组 / 译

勒索软件、物联网僵尸网络、漏洞赏金计划和政府漏洞买卖等事情经常出现在我们的风险评估、防御战略和预算决策中。时至今日，它们已经不能再被称为“新闻”了，就像老式病毒、数据泄露和垃圾邮件那样无所不在。

勒索软件

加密勒索软件的出现颠覆了网络犯罪的模式，这也成为了恶意软件的一个新常态。恶意软件会加密用户的文件、文件夹或硬盘，要求用户支付赎金来解密。2016 年，DDoS 攻击已经不再是排名第一的勒索途径，Cryptolocker、Locky、Petya 和数十个其他勒索软件样本横空出世。

虽说勒索软件并不新鲜，但它导致了 2016 年的多起重大攻击事件。它们的影响包括：医院被迫将病人转移到其他医疗机构，执法机构无法访问记录数据库，公共事业机构惴惴不安等。

从一定程度上说，这些事情是可以被遏制的。通常我们通过老式恶意软件，就能够较快地掌握新威胁的特征，但是勒索软件的发展速度很快，我们不能通过这种方式掌握它的特征。为了应对勒索软件的攻击，FBI 甚至签发了全国警报，要求受害者提交攻击相关的数据，这在网络犯罪史上是史无前例的。

物联网僵尸网络

物联网僵尸网络通常是指 DDoS 攻击，攻击者利用其控制下的数千个终端对银行或企业发送垃圾流量，造成它们的服务中断。犯罪分子利用物联网设备搭建了僵尸网络，他们发现，启用 IP 路由功能的闭路电视摄像头和录像机的某些功能无法轻易被修复。这些设备分布广泛并已经联网，并且它们通常采用非常简单的密码。一旦这些密码被破解，攻击者就能控制这些设备，为 Mirai 恶意软件增加猎物。黑客 Anna-Senpai 在黑客论坛上公布了 Mirai 的源代码，技术高超的黑客可以利用这些代码开发新变种，用以攻击新的目标。

针对域名系统供应商 Dyn，针对安全记者布莱恩·克雷布斯 (Brian Krebs) 和主机托管公司 OVH 等的攻击只是冰山一角。Dyn 攻击事件尤其令人担忧，因为它中断了 Dyn 的各类长达几个小时的客户服务，受影响的客户主要位于美国东海岸，包括 Spotify，Twitter 等。安全专家认为，政府必须加强监管，要求制造商遵守一定的安全标准，以便保护消费者和核心服务。

漏洞赏金计划

漏洞赏金计划已经不是新闻了，它已被较为广泛的使用在公司中。

虽然不是每个公司都设立了公共漏洞赏金计划，但是很多公司在其他公司 (如 HackerOne、Bugcrowd、Synack 等) 的帮助下都设立了私人漏洞赏金计划。

漏洞赏金计划是对上报漏洞的人进行奖励。黑客可以合法地探究公司的网络资产，找到漏洞，通过既定的渠道上报这些漏洞，赚取一些赏金。十年前，研究人员发起了“拒绝免费漏洞”活动，他们受够了免费向微软等公司上报漏洞，还要时刻担心自己会不会被起诉。

美国军队、美国国防部和通用汽车公司都设立了漏洞赏金计划。虽说不是所有公司都会支付赏金，但是很显然，更多的研究人员乐意上报漏洞。根据最近的 NTIA(国家远程通信和信息管理局) 调查结果，比起赚取赏金，黑客们更希望与厂商保持连续和开放的通信。

政府漏洞买卖

政府购买漏洞和漏洞利用代码，并保留这些漏洞。政府的任务与企业不同，它其中的一个任务是保护国家安全，这涉及到情报收集。另一个则是利用漏洞来监视敌人。政府会购买漏洞，编写漏洞利用代码，并利用漏洞监视敌人。詹姆斯·邦德 (《007》系列小说、电影的主角) 曾经在床头灯和画作后面发现了监听设备。如果这些事发生在今天，他需要找的是 MacOS Rootkit。这就是今天的游戏方式，政府强大的购买力导致了高级别的网络间谍活动。

在美国，我们会有一种错觉，政府的这些权力是受检查和控制的。但是，公民实验室等机构发现政府在猖獗地滥用这些权力，它们利用这些工具来窥探和危害公民利益。人们希望避免这种权力滥用，要求全面禁止政府的漏洞购买活动或实现漏洞购买的完全透明化，但这是很难实现的。

原文名称	The 7 Most Sensational Breaches Of 2016
作者简介	Michael Mimoso，卡巴斯基《安全周报》编辑。
原文信息	2016 年 12 月 28 日发布于《安全周报 (Threatpost)》，原文地址 https://threatpost.com/four-new-normals-for-2017/122584/
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《僵尸网络 Dofloo 家族分析》

近日，安天追影团队经过长时间对 Trojan[DDoS]/Linux.Dofloo 家族的详细分析与监控获知：Dofloo 家族控制节点主要分布于美国，其攻击主要目标为中国和美国。安天还监控到 Dofloo 家族参与了 2016 年 10 月美国的 Dyn 攻击事件。

Dofloo 家族从 2014 年诞生，发展至今已经相当的完善和成熟了。其僵尸网络的被控制端已渗透进 linux x86、64、Arm 路由、Windows 系列以及物联网中，而且它的同一个控制端可以同时兼容控制上述环境的被控端。除此之外，Dofloo 家族在静态配置解密及通信协议上都使用了加密算法，其攻击指令使用了 AES 加密算法，因此增加了监控它的难度。

Dofloo 家族为了让控制端能够兼容更多版本的被控端，所以采用了相同的通信协议。它使用的 DDoS 攻击类型不变，主要包括：DNS Flood、TCP Flood、UDP Flood、CC Flood、ICMP Flood 这几种攻击方式。

经过安天分析发现，为了达到长期有效威胁受害系统的目的，被控端会编辑受害系统自启动服务文件 (/etc/rc.local、/etc/rc.local、/etc/rc.d/rc.local、/etc/init.d/boot.local)，将样本自身注入，实现样本自启动。随后它会获悉系统相关配置信息，作为被控端的首包数据向控制端发送，然后循环等待接收控制端发送的指令。被控端接收到的攻击指令数据是控制端经过 AES 加密算法加密的密文，需要对数据使用密钥进行解密才能得到明文。

Dofloo DDoS 家族在设计当初就已经具备前瞻性需求，攻击者可以远程控制被控端执行多种类型的攻击。通过分析监控到的攻击数据可知，控制端在每一次下达攻击目标时，命令被控端使用的攻击线程量经常在 50+，这也就极大的增加了每台被控端的攻击流量。攻击目标经常是在遭受攻击后 30 秒内就已经宕机，这也是 Dofloo 家族的攻击数量相对其他家族较少的原因之一。

目前，Dofloo 已经是僵尸网络的常见家族。Dofloo DDoS 的出现后快速遍布于互联网中，损耗互联网及设备资源，影响了互联网的安全健康发展，损坏了广大网民的利益。

因此，如果计算机等网络设备被植入 Dofloo 家族，就需要删除样本并删除 Dofloo 样本的自启动数据。如果是路由器设备被植入，还需修复默认登录密码。

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、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、智能学习鉴定器将文件判定为木马程序。

该文件具有以下行为：疑似 ddos flood 流量攻击、获取计算机系统版本、样本自启动。

文件名	52A695E909CA648F63629A0B2B426BBE
文件类型	BinExecute/Linux.ELF
大小	4.86 MB
MD5	52A695E909CA648F63629A0B2B426BBE
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Dofloo.VERSONEX
判定依据	BD 静态分析

报告地址：https://antiy.pta.center/_lk/details.html?hash=52A695E909CA648F63629A0B2B426BBE

◆ 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 2007，Flash，WPS，FoxitReader，Adobe Reader

◆ 危险行为

行为描述	危险等级
疑似 ddos flood 流量攻击	★★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
获取计算机系统版本	★★	样本自启动	★★