安天周观察

主办：安天　2016 年 12 月 5 日（总第 67 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天第四届网络安全冬训营即将开启

由安天主办的第四届网络安全冬训营——“冰峰屹立”将于 2017 年 1 月 6 日至 7 日在冰城哈尔滨举行。本届冬训营将围绕“有效防护，价值输出”这一主题展开，旨在自我批判安天作为安全厂商和研究者的主观局限和技术优越感，回归安全技术为用户提供有效的防护能力和价值保障的本质。

本届冬训营将通过一天的开放式技术报告和一天的专题培训的组合形式，集中探讨安全检测、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。同期，冬训营也将透过各种热点的迷雾，以专业务实的态度，深入挖掘用户的真实安全需求，为安全技术、产品与服务实现有效的客户价值寻找落地方式，探寻可实施的解决方案。

即将过去的 2016 年，对于中国的网络安全事业是非凡的一年。习近平总书记在“4·19 讲话”中提出“树立正确的网络安全观”、“安全和发展要同步推进”，为“网络强国”指明了方向；网络安全法的正式颁布，明确了各相关主体的责任与义务，为网络安全事业的发展建立了法律保障。

目前，中国网络安全行业已经到吹响新征程号角的时刻。安天在此时选择“冰峰屹立”作为本届冬训营的营语，意在继承往届冬训营“凛冬将至”、“北风乍起”和“朔雪飞扬”主题的同时，以更加务实的视角和更加积极、朴素的姿态，不畏冰寒，携手前行，共同铸就“冰峰屹立”。

活动报名、会议嘉宾及日程请关注安天微信公众号 antiylab 或冬训营官方网站 wtc.antiy.com。

安天获得《商用密码产品销售许可证》

近日，安天哈尔滨总部和北京公司分别通过各地区密码管理局的严格审核、现场考察，以及国家密码管理局的批准，获得国家密码管理局颁发的《商用密码产品销售许可证》。


商用密码产品销售许可证
（国密局销字 SXS2891 号）
单位名称：哈尔滨安天科技股份有限公司
销售范围：销售经国家密码管理局审批并通过指定检测机构产品质量检测的商用密码产品
有 效 期：2016 年 11 月 20 日至 2019 年 11 月 19 日
国家密码管理局
2016 年 11 月 20 日


商用密码产品销售许可证
（国密局销字 SXS2889 号）
单位名称：北京安天电子设备有限公司
销售范围：销售经国家密码管理局审批并通过指定检测机构产品质量检测的商用密码产品
有 效 期：2016 年 11 月 20 日至 2019 年 11 月 19 日
国家密码管理局
2016 年 11 月 20 日

商用密码产品是由国家密码管理机构指定的单位生产，并严格控制在国家密码管理机构批准的范围内。未经指定，任何单位或个人不得从事商用密码的生产。从事商用密码产品的销售必须向国家密码管理机构申报，经批准后方能进行。

本次获得《商用密码产品销售许可证》，意味着安天哈尔滨、北京两地可销售经国家密码管理局审批并通过指定检测机构产品质量检测的商用密码产品。这表明安天在融入国家商用密码体系中有了长足的进步，也进一步提高了公司在信息安全领域的服务能力，为国家网络安全建设保驾护航。

◆ NTP 漏洞可导致操作系统 Windows 触发 DoS

近日，研究人员发布针对 cve-2016-9311 漏洞的 PoC，这个漏洞能够导致 NTP 守护进程崩溃，并且触发 Windows 系统拒绝服务。NTP 是一种广泛用于时钟同步的协议，这种协议能够在多个系统同步时间，因此能被黑客利用。

之前，有专家曾报告过 NTP 协议的漏洞，他表示，这个漏洞能够被黑客利用来进行大规模的 DDoS 攻击。2014 年 4 月，有人使用最大规模 (400Gbps) 的 DDoS NTP 放大攻击使得 Cloudfare 的欧洲服务器陷入瘫痪。（文章来源：http://www.freebuf.com/vuls/121129.html）

一周简讯

- 远控木马 NetWire 回归，窃取支付卡数据
- 斯诺登最新泄露：AT&T 大厦或为 NSA 基地
- xHamster 色情网站数据泄露，数十万账号被售卖
- cURL 工具及库中被发现远程代码执行严重漏洞
- 勒索软件 Kangaroo 由开发者经远程桌面手动安装
- UberCENTRAL 工具漏洞可致用户数据泄露
- 黑色星期五邮件被用于向亚马逊客户钓鱼

（安天 CERT 搜集整理，详见 http://bbs.antiy.cn）

每周安全事件

类 型	内 容
中文标题	德国电信遭黑客攻击：90 万路由器下线 大量用户无法访问互联网
英文标题	Deutsche Telekom confirmed that more than 900,000 routers began to have serious problems connectivity problems due to a cyber attack.
作者及单位	Pierluigi Paganini；Securityaffairs
内容概述	近日，德国电信遭遇网络攻击，超 90 万路由器无法联网，德国电信方面已经确认了此事。据悉，断网事故始于当地时间 11 月 27 日 (周日)17：00 左右，持续数个小时。这些被攻击的路由器除了被用于联网服务外，德国电信用户还用这些路由器来连接电话和电视服务。根据德国媒体 abendblatt.de 报道，“德国联邦信息技术安全局 (BSI) 发现，在某个全球范围内的攻击发生之后，德国电信路由器出现了无法联网的问题。根据 BSI 的说法，受保护的政府网络也遭到了上述攻击，但得益于有效的保护措施，政府网络受到的攻击被击退。” 目前，德国电信并未提供攻击的技术细节，也没有透露受影响的路由器型号。
链接地址	http://securityaffairs.co/wordpress/53871/iot/deutsche-telekom-hack.html

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 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	较为活跃样本	Trojan/Android.AutoSMS.m[pay]	该应用会私自发送扣费短信，拦截并回复回执短信，同时会删除用户短信，造成用户资费损失。建议卸载。(威胁等级中)
		Trojan/Android.jianmo.ay[rog，sys]	该应用运行后会自动置顶界面，勒索用户进行解锁，造成用户经济损失。建议卸载。(威胁等级高)
		Trojan/Android.Triada.q[exp，rog]	该应用安装后无图标显示，运行后会私自获取 root 权限，下载并提权安装应用程序，后台推送流氓广告，造成用户资费损耗。建议卸载。(威胁等级高)
		Trojan/Android.emial.dp[spr]	该应用运行后会隐藏图标，于后台遍历用户联系人信息并私自发送恶意链接，造成用户资费损耗。建议卸载。(威胁等级中)
		Trojan/Android.emial.dq[prv]	该应用运行后会激活设备管理器，隐藏图标并私自卸载安全软件，获取用户短信和联系人信息并发送到指定号码，造成用户隐私泄露和资费损耗。建议卸载。(威胁等级中)
		Trojan/Android.oxti.m[exp]	该应用运行后会隐藏图标，使后台频繁访问网址，造成用户的手机流量损耗。
		Trojan/Android.Rootnik.k[rog，sys]	该应用安装后无图标显示，运行后会私自下载恶意应用和提权工具，获取 root 权限，静默安装恶意应用，静默卸载其他应用，造成用户资费损失和破坏系统稳定性。建议卸载。(威胁等级中)
		Trojan/Android.emial.dv[prv，exp]	该应用会伪装成移动积分应用，运行后会监听用户短信内容，拦截并窃取用户短信，造成用户隐私泄露和资费消耗。建议卸载该应用。(威胁等级高)
		Trojan/Android.QQspy.p[prv，exp]	该应用伪装成 QQ 刷钻工具，诱导用户输入账号密码和密保问题并通过短信转发用户信息，造成用户隐私泄露和资费损耗。建议卸载。(威胁等级高)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	多款 Adobe 产品远程代码执行漏洞 CVE-2014-8439	因多款 Adobe 产品中存在安全漏洞，攻击者可利用该漏洞执行任意代码或造成拒绝服务 (无效的指针逆向引用)。以下产品及版本或将受到影响：基于 Windows 和 OS X 平台的 Adobe Flash Player 15.0.0.167 以及之前版本和 13.0.0.244 以及之前版本；基于 Linux 平台的 Adobe Flash Player 11.2.202.406 以及之前版本；Adobe AIR 15.0.0.249 以及之前版本；基于 Android 平台的 Adobe AIR 15.0.0.252 以及之前版本；Adobe AIR SDK 15.0.0.249 以及之前版本；Adobe AIR SDK & Compiler 15.0.0.249 以及之前版本。(威胁等级高)
	较为活跃的样本	RiskWare[Downloader]/Win32.AdLoad.oa	此威胁是一种具有传播和下载广告软件行为的木马类程序，在未经用户许可的条件下侵入用户系统窃取重要数据，安装其它恶意软件后会使用户的电脑性能变慢。(威胁等级中)
		Trojan[Backdoor]/Linux.Gafgyt	此威胁是一种木马类后门程序，在 Linux 平台运行，主要功能为 DDoS 攻击，更新和下载应用程序，主要通过扫描弱口令进行传播。(威胁等级中)
		GrayWare[AdWare]/Win32.Amonetize	此威胁是一种具有广告行为的灰色软件类程序，通过安装免费软件捆绑安装到用户浏览器，会威胁操作系统。建议用户安装时可选择自定义安装。(威胁等级中)

旧金山市交通局遭勒索软件攻击

Tom Spring / 文　安天公益翻译小组 / 译

近日，旧金山市交通局 (SFMTA) 遭遇勒索软件攻击。交通局内部计算机和支付系统先后遭到攻击，攻击组织窃取了该局 30G 的数据。

旧金山市交通局发表的一项声明表示：“11 月 25 日，SFMTA 遭到了勒索软件攻击。目前，事态已经得到遏制，我们优先恢复了系统。”

SFMTA 指出，黑客设法使支付系统崩溃。同期，《旧金山检察官报》报告表示，攻击者要求交通局支付 100 比特币的赎金来恢复计算机系统。

声称对 SFMTA 攻击事件负责的黑客表示，“我们不住在美国，但我们希望旧金山市交通局识时务。如果他们不支付赎金，我们将发布 30G 的数据和文档，包括合同、员工数据、LLD 计划、客户信息等。”

旧金山市交通局发言人保罗·罗斯 (Paul Rose) 表示，攻击者是在虚张声势，客户的隐私和交易信息并没有泄露。

罗斯说：“我们从来没有考虑过支付赎金，也不打算支付。该攻击没有渗透我们的防火墙，我们的内部员工能够将系统恢复。”

他补充到，交通服务从未受到影响，驾驶员的安全从未面临风险。罗斯说，SFMTA 决定为客户开通检票闸机，以“尽可能减少客户交易的任何影响”。他拒绝进一步评论，表示正在进行调查。

安全专家怀疑攻击者是否真窃取了 SFMTA 数据，认为黑客的声明只是为了逼迫 SFMTA 支付赎金。

Mimecast 网络安全战略家 Matthew Gardiner 认为：“这只是钱的问题。如果交通局的系统恢复，攻击者将试图以另一种方式获取赎金。例如，威胁交通局他们将公开数据。”

AlienVault 的安全倡导者 Javvad Malik 说：“没有任何迹象表明他们已经获取了数据。在无法提供任何数据样本的情况下，我们只能相信攻击者的话。”

据了解，攻击者使用的是勒索软件 HDDCryptor(也称为 Mamba) 来执行攻击，该勒索软件主要加密目标的硬盘而非单个文件。Morphus Labs 的研究人员表示，一旦 Mamba 感染了机器，它会用自定义主引导记录 (MBR) 覆盖现有的 MBR，并加密硬盘。

《旧金山检察官报》报告称，攻击感染了旧金山市交通局 8,565 台计算机中的 2,112 台。并指出，攻击不仅影响了交通局的支付系统，而且影响了调度和电子邮件系统。

Tripwire 的高级 IT 风险和安全战略总监 Tim Erlin 指出：“当网络攻击对物理世界产生影响时，总是让人担忧。近年来这种事情越来越多，我们需要更加关注。”

他说：“SFMTA 有适当的系统，来应对不是恶意的计算机攻击，并允许他们在各种不同的情况下迅速恢复正常。”

这次攻击没有威胁到乘客安全，但是 Erlin 说他预计影响物理世界的网络攻击数量会增加。

在过去的一年里，各地均不同程度的出现了几个网络攻击影响人身安全的警告。例如，在今年 7 月，网络风险管理发布了一份报告，称圣犹达医疗的心脏植入设备易受网络攻击，并警告说医院是黑客的主要目标。联网的医疗设备很容易成为目标，攻击者通过窃取病历或通过对救命的医疗设备进行勒索攻击而迅速获利。

原文名称	Hackers Make New Claim in San Francisco Transit Ransomware Attack
作者简介	Tom Spring，卡巴斯基《安全周报》副主编。
原文信息	2016 年 11 月 28 日发布于《安全周报》(Threatpost) 原文地址 https://threatpost.com/hackers-make-new-claim-in-san-francisco-transit-ransomware-attack/122138/
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《Mirai 变种利用 7547 端口漏洞传播分析报告》

近日，安天联合电信云堤发布针对 Mirai 新变种威胁分析报告。报告指出，利用捕风蜜罐捕获到 Mirai 新变种，该变种利用最近公布的 7547 端口漏洞进行传播，并对公布漏洞的 payload 进行了修改使之可以下载执行 Mirai 样本。通过对互联网流量监控，发现了大量 IoT 设备进行 7547 端口扫描，这些设备已经被新 Mirai 变种攻陷。

经分析发现，近期披露的 D1000 TR 064 服务器 TCP 端口 7547 漏洞，攻击者通过发送某些 TR 064 命令，指示运行该服务器的设备打开防火墙上的 80 端口，继而允许攻击者从互联网访问设备的 web 管理界面。通常 D1000 的默认登录密码是默认 Wi-fi 密码，这可以通过另一个 TR064 指令来获取。攻击者利用该漏洞的关键代码向端口 7547 发送 TR064 命令，设置新 NTP 服务器的方式，在 NewNTPServer1 中采用指令来解除防火墙对 80 端口访问限制。

Mirai 变种的 C&C 配置加密方式与源码泄露的家族没有变化。连接 C&C 服务器的 23 端口，上线包数据为 0x00000001。

被感染的路由器会执行两个命令。第一个命令是关闭 7547 端口，第二个命令是停止 telnet 服务，使用户无法远程更新固件。然后，被感染的路由器会生成随机 IP，攻击者对这些 IP 的 7547 端口进行扫描与漏洞入侵。样本利用 7547 漏洞进行了相应的改造，可直接下载远程样本，修改可执行模式并且运行。

通过电信云堤抽样流量分析获得：

确认被感染具有 7547 扫描能力的节点，主要通过包括扫描节点自身是 IoT 设备，扫描节点多次使用相同端口扫描，扫描节点发出攻击漏洞方法进行发现。

确认感染设备总数为 306778，感染设备主要开放服务或设备信息包括 RomPager/4.07、DVRDVS、TR069 Connect Request Server、DHT Nodes、HuaweiHomeGateway。

目前发现感染的节点主要地区 top10 如下表所示。

国家	节点	国家	节点
巴西	107166	伊朗	11573
英国	61854	澳大利亚	8002
爱尔兰	18268	泰国	7159
拉美其它地区	17210	意大利	6243
土耳其	13863	芬兰	5294

随着物联网的高速发展，物联网设备数量大幅增加，黑客正是利用了这一点使其作为攻击对象和跳板进行攻击。这也提醒了物联网用户，需要提高对物联网设备的安全防护意识，提高攻击入侵物联网设备的成本，以及加强物联网设备的安全威胁监测预警。以上内容均是安天已经在进行的工作。

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、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：执行命令、端口扫描、已知 payload 发送。

文件名	0ACC2CB0DCC2CE9A67A857FED5DE9278
文件类型	BinExecute/Linux.ELF
大小	81 KB
MD5	0ACC2CB0DCC2CE9A67A857FED5DE9278
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[DDOS]/Linux.Mirai.7547
判定依据	智能学习

◆ 运行环境

操作系统	中标麒麟
内置软件	默认

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
执行命令	★★★★★	端口扫描	★★★★★
已知 payload 发送	★★★★★		

报告地址：https://antiy.pta.center/_lk/details.html?hash=0ACC2CB0DCC2CE9A67A857FED5DE9278