安天周观察

主办：安天　2016 年 8 月 29 日（总第 54 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加“首届网络空间战略论坛暨中国信息安全网上线发布会”并发表演讲

8 月 27 日，由国家军民融合委员会、中国互联网发展基金会和中国信息安全测评中心联合指导，《中国信息安全》杂志社和北京华夏文化交流促进会联合主办的“首届网络空间战略论坛暨中国信息安全网上线仪式”在京召开。来自人民军队、政府部门、科研院所、网络安全企业、新闻媒体的 300 余位嘉宾到场参会。

在“网络空间战略论坛年度人物颁奖仪式”上，中国人民解放军北部战区副参谋长安卫平、中国人民解放军战略规划咨询委员会委员叶征、中国人民公安大学原书记 / 校长、中国警察法学研究会会长程琳等十位对“网络空间战略论坛”做出突出贡献的人物颁发荣誉证书和奖杯。安天技术负责人肖新光也有幸获得这一奖项。

“网络空间战略论坛”主编秦安主持了“网络中国繁荣世界高端对话”活动，龙永图、刘慧、安卫平、富彦斌、张文木、肖新光，分别解读了网络强国的路径、文化、力量、架构、战略、产业等方面的问题。

“网络空间军民融合主题演讲”环节，安天带来了《网络安全能力的层次与路径思考》的主题演讲。报告从分析国家层面、政府机构层面和个体用户层面不同的安全需求入手，揭示不同层次的网络安全风险，以及风险的相互转化情况。介绍了国内网络安全产业特别是民营企业所拥有的技术基础与能力，并通过分析 IT 技术领域的军民能力相互转化的规律，思考网络空间安全领域的企业能力如何有效转化为国家能力。

报告指出传统的军事技术发展由于具有极为领衔的前瞻性和承担成本的能力，因此往往远远领先于民品和普通工业技术。但在一些新兴领域，民品企业和服务带来的模式变革可以颠覆传统安全能力；民品由于大量的用户基数和持续改进迭代，其易用性远远高于军品，其产品质量也可以达到军品的程度。而在网络安全领域，当前网络安全核心技术的核心创新能力、动力、资源与人才，都分布在企业，特别是民企，这已经是一个既定事实。

报告通过对比当年美以联手炸毁伊拉克核反应堆的“巴比伦行动”与美以联手攻击伊拉克离心机设施的“奥林匹克行动”（即震网事件），说明了网络装备的效费比优势。又对比了震网事件与乌克兰国家电网遭遇攻击停电事件，说明通过网络攻击关键技术设施的难度和成本正在降低。要用国防实力和装备成本来衡量关键基础设施防护能力建设。

报告最后指出，产业能力是中国网络安全能力的技术基础，人才水土和动力之源。从国防装备的成本角度，重新思考网络安全的价值，才能更好的理解网络安全技术的价值。无论对人民军队的网络空间整体能力建设还是对于民族网络产业来说，都有可能是当前的一个关键。

同时，安天作为本次会议的支持单位之一，在大会现场设有资料台，安天的《白象的舞步——来自南亚次大陆的网络攻击》、《乌克兰电力系统遭遇攻击停电事件综合分析报告》等资料收到与会者的广泛好评。

黑客利用受感染 PC 上的虚拟机隐藏自身行迹

近日，安全公司报告称，恶意人士已经开始使用新型战术，即在目标设备上安装并运行虚拟机，旨在隐藏自己的踪迹。这些虚拟机负责模拟文件系统，且大多数情况下运行在现有操作系统之内。通俗地讲，虚拟机属于系统之内的操作系统，允许用户通过点击图标轻松打开桌面内的“Linux”或者“Windows 98”。虚拟机一般由软件开发人员用于测试产品，且经常被嵌入至安全软件等其它应用当中。（来源：http://www.easyaq.com/newsdetail/id/971437448.shtml)

一周简讯

- 安天 AVLTeam 发布移动银行应用仿冒攻击威胁分析报告
- 勒索软件 DetoxCrypto 出现新变种
- 研究人员发现新的微软 UAC 绕过方法
- Linux 蠕虫 PNScan 暴力破解路由器并安装后门
- 安卓木马 DroidJack 借助短信钓鱼链接传播
- 安全厂商发现创建 P2P 僵尸网络的 Linux 木马
- 工业网络厂商 Moxa 部分网络设备存身份验证漏洞

（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	BTS 软件存在严重漏洞，黑客能劫持并摧毁移动信号塔
英文标题	Attackers Hijack Cellular Phone Towers Thanks To Critical Flaws
作者及单位	Kavita Iyer；TechWorm
内容概述	近日，安全研究人员发现基站收发台 (BTS) 存在三大严重安全漏洞，一旦被攻击者利用，便能攻击、劫持并摧毁移动信号塔。核心 BTS 软件服务中存在的第一个漏洞会将设备曝于外部连接之下，攻击者利用该漏洞通过互联网便能入侵 BTS 收发器。攻击者能发送 UDP 数据包到特定管理端口，并利用设备的内置功能。这样一来，攻击者便能远程控制 BTS，修改 GSM 流量，从传输数据提取信息、摧毁基站，甚至更糟。第二个漏洞是因过大的 UDP 数据包导致的内存缓冲区溢出。第三个漏洞与第一个漏洞有关。如果攻击者发送自定义 UDB 流量至 BTS，因为控制通道不需要验证，攻击者便可以在 BTS 的收发器模块执行命令。
链接地址	http://www.techworm.net/2016/08/hackers-can-hijack-cell-phone-towers.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 5 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.Saiva.a[pay] 2016-08-22	该应用程序会诱导用户开启网络服务，会私自发送短信订阅并支付付费服务（包括包月视频和咪咕音乐）并拦截服务提供商反馈的消息通知。会造成用户经济损失，建议立即卸载。（威胁等级高）
		Trojan/Android.SmsSpy.q[prv，exp] 2016-08-23	该应用运行后会隐藏图标，会私自联网上传用户设备的相关信息，获取短信内容信息并执行联网上传操作，会造成用户隐私泄露。（威胁等级高）
		G-Ware/Android.Svpeng.i[prv，exp，rog]2016-08-24	该应用程序会伪装成色情应用，诱导激活设备管理器，劫持界面弹出的 FBI 勒索界面，诱导用户输入银行卡号、日期、CVV 等信息并联网上传，建议立即卸载，避免造成隐私泄露和资费损耗。（威胁等级低）
		Trojan/Android.AutoSMS.k[exp] 2016-08-22	该应用程序无实际功能，运行后，后台会拦截并转发短信，会造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
	较为活跃的样本	G-Ware/Android.Svpeng.j[exp，rog]	该应用程序会伪装成色情应用，运行后会隐藏图标，诱导激活设备管理器防卸载。劫持界面弹出勒索界面，建议立即卸载，避免造成资费损耗。（威胁等级低）
		G-Ware/Android.jianmo.ap[rog，sys]	该应用程序伪装成抢红包插件诱导用户点击，并诱导激活设备管理器，置顶界面。勒索用户添加指定 QQ 群进行付费解锁，会造成用户资费损失，建议不要安装。（威胁等级低）
		Trojan/Android.SmsThief.as[prv，exp]	该应用程序无实际功能，运行后，后台会执行拦截并转发短信操作，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级中）
		Trojan/Android.simplelock.p[rog，sys]	该应用程序运行后会隐藏图标，请求激活设备管理器，强制置顶界面勒索并用户付费解锁，造成用户手机无法正常使用。（威胁等级中）
		Trojan/Android.Downloader.cf[exp，fra]	该应用程序伪装成系统应用，安装后无图标，触发启动后获取 apk 下载链接并私自下载未知应用。会获取广告相关文件并反射调用，造成用户资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.SmsSend.kb[exp]	该应用程序为色情视频应用，运行后会根据视频内容诱导用户发送短信到指定号码，请注意收费提示信息，以免造成的财产损失，建议使用健康绿色软件。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Internet Explorer 脚本引擎内存损坏漏洞 (CVE-2016-0189)	Internet Explorer 在处理内存中的对象时，JScript 和 VBScript 引擎的呈现方式存在远程执行代码漏洞。这些漏洞会损坏内存，通过攻击者在当前用户的上下文中执行任意代码。成功利用这些漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，攻击者则可以控制受影响的系统。攻击者可随后安装程序，查看、更改或删除数据，或者创建拥有完全用户权限的新帐户。（威胁等级高）
	较为活跃的样本	Trojan[Spy]/Win32.Ranbyus	此威胁是一类具有监视功能的间谍件类木马家族，复制自身到 %windows% 目录下连接远程服务器，会下载恶意代码并接受攻击者控制，添加计划任务使其自启动。（威胁等级中）
		Trojan[Downloader]/Win32.ChePro	此威胁是一类下载者木马家族。它运行后会下载并安装其他恶意代码，窃取用户敏感信息，如银行密码等。占用系统资源，影响用户使用。（威胁等级中）
		Trojan[Backdoor]/Win32.Matsnu	此威胁是一类窃取用户信息的木马家族，属于后门。该家族样本运行后会连接网络、禁用注册表编辑器、允许恶意代码绕过防火墙。（威胁等级中）
		GrayWare[AdWare]/NSIS.InstallMonetizer	此威胁是一类安装广告网络的灰色软件家族。该家族样本运行后，会连接网络下载安装名为 InstallMonetizer 的一款面向桌面软件开发者的广告网络，安装后有推广广告，会诱导用户安装。（威胁等级低）

必虎路由器惊现多个漏洞

Chris Brook / 文　安天公益翻译小组 / 译

近日，研究人员已经确定，必虎路由器存在多个漏洞，攻击者能够用它来做几乎所有事情。攻击者能够绕过其身份验证，分析存储在路由器系统日志中的敏感信息，甚至通过硬编码的 root 密码以 root 权限来执行操作系统命令。

IOActive 实验室的安全顾问陶·苏瓦吉购买了一款这种路由器，他将其称为“uRouter”。打开路由器之后，能够提取其固件，访问 shell 并分析其代码。之后，苏瓦吉逆向工程了一些二进制文件，发现了三种不同的方式可以获得访问路由器网络界面的管理员权限。

根据 IOActive 发布的博客，该路由器莫名其妙地接受了用户提供的任何会话 ID cookie 值，这意味着任何人都能冒充通过身份验证的用户。攻击者甚至可以使用硬编码会话 ID 7000000000000000，或者读取系统日志和使用任何管理员 SID cookie 值，来访问路由器的身份验证功能。

苏瓦吉说，在此之后，攻击者可以轻松地从管理员权限提升到 root 用户权限。有些功能，如负责解析请求主体中

的 XML 并找到相应回调函数的功能，甚至不需要用户进行身份验证就能够使用。攻击者使用命令行数据包分析工具（如 tcpdump），来窃听路由器的流量。攻击者可以修改其配置来重定向流量，插入一个持续性后门，或者删除设备上的重要文件使其无法运作。

苏瓦吉写到：“该路由器缺乏默认的防火墙规则，如果它连接到互联网，则无法阻止攻击者从广域网访问它。”

苏瓦吉指出，他本以为已经找出了该路由器的所有漏洞，但是在启动时，他又发现它默认启用安全外壳协议（译者注：SSH，Secure Shell 的缩写；SSH 为建立在应用层基础上的安全协议，是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。），并在每次启动时重写硬编码的 root 用户密码。

这意味着，任何知道路由器 root 密码的人都能够通过 SSH 连接到路由器，并获得 root 权限。管理员无法修改或删除硬编码的密码。因此，用户最好不要将必虎无线路由器连网！“

该路由器甚至将一个可疑的第三方 JavaScript 文件，注入到用户的 HTTP 流量中。苏瓦吉指出，该文件本该具有“先进的过滤功能来加强隐私”，但是它的内核模块看起来很奇怪且在启动时加载，可以很容易地用来执行攻击。”

路由器的安全性往往被消费者和公司忽视，前者经常忽视更新固件，而后者有时无法充分地保护设备。

今年初夏，美国网件公司不得不发布固件更新来解决硬编码加密密钥的问题，该问题可能会允许攻击者以管理员权限访问设备，执行中间人攻击，或被动解密捕获的数据包。

原文名称	Multiple Vulnerabilities Identified in “Utterly Broken” BHU Routers
作者简介	Chris Brook，卡巴斯基《安全周报 (Threatpost)》的副编辑。
原文信息	2016 年 8 月 19 日发布于《安全周报 (Threatpost)》 原文地址 https://threatpost.com/multiple-vulnerabilities-identified-in-utterly-broken-bhu-routers/120015/
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《Operation Ghoul 样本分析报告》

近日，安天追影小组梳理网络安全事件时，发现了一起针对工业组织名称为“Operation Ghoul”的 APT 攻击事件，并对相关样本做了简要分析。攻击者通过鱼叉式网络钓鱼邮件来传播包含木马的压缩文件，利用社会工程学手段诱导受害者下载运行木马，并在感染者主机上收集敏感数据，如密码、按键和屏幕截图等信息。攻击者通过将受害组织的敏感数据对外出售来获取利益，从而会造成了受害者大量信息泄露。该事件的攻击目标主要包括超过 30 个国家的工业管理组织、工业企业以及制造业企业。

经安天追影小组分析，Operation Ghoul 木马使用 Microsoft Visual C# Basic. NET 编写，攻击者主要通过发送银行付款单据、信用卡收据账户确认函、保险赔付单等具有诱导性邮件的方式，来进行传播木马病毒。一但受害者点击网络钓鱼邮件，即会下载运行间谍木马，进而感染受害者的 Windows 平台。

该事件的相关木马样本是基于商业鹰眼间谍软件的源代码开发的，包含多种窃听模块。恶意代码会通过自启动服务和篡改系统配置来达到自启动的目的，同时使用反调试、调试器提权和超时的技术来达到自我保护、系统提权和隐藏目的。经分析窃听模块主要窃取如下信息：键盘按键记录、剪贴板数据、文件 FTP 服务器凭证、本地客户端通信信息、本地电子邮件客户端账户数据、本地安装的应用程序许可证信息、定时截屏信息、明文密码等。Operation Ghoul 间谍木马在窃取相关数据后，会通过伪造 HTTP GET/POST 请求，和利用邮箱信息传输模块调用公用邮箱服务器：mail.ozlercelikkapi.com、mail.eminenture.com 邮件向攻击者传输窃取的信息，从而使感染者的信息数据泄露，对受害用户有很大的危害性。

此次攻击事件造成的安全信息泄露数据量庞大，常见的社会工程学手段仍然能够造成大量的的网络安全信息泄露。安天提醒网络使用者：提高安全意识，不要随意点击不明来源的邮件或社交网站中的链接，不要轻易下载邮件中不明来源的附件，养成及时更新操作系统和软件应用的好习惯。目前该类恶意代码已经可以被安天追影产品检出。目前，安天追影产品已经实现了对 Operation Ghoul 样本的检出。

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。

最终依据动态行为鉴定器、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：删除自身、疑似键盘记录、获取系统版本、创建挂起的进程、设置调试器权限、查找指定内核模块、读取自身文件、填充导入表（疑似壳）、访问其他进程内存、获取计算机名称、创建特定窗体、获取主机用户名称、获取驱动器类型、获取系统内存、独占打开文件、启动服务、打开自身进程文件、疑似桌面控制、疑似查找杀软进程。

文件名	55358155F96B67879938FE1A14A00DD6
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	743 KB
MD5	55358155F96B67879938FE1A14A00DD6
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Spy]/MSIL.Siplog.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
删除自身	★★★★	疑似键盘记录	★★★

◆ 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	★★	创建挂起的进程	★★
设置调试器权限	★	查找指定内核模块	★
读取自身文件	★★	填充导入表 (疑似壳)	★★
访问其他进程内存	★	获取计算机名称	★
获取主机用户名称	★	创建特定窗体	★
获取系统内存	★★	获取驱动器类型	★
启动服务	★	独占打开文件	★
疑似桌面控制	★	打开自身进程文件	★
疑似查找杀软进程	★★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=55358155F96B67879938FE1A14A00DD6