安天周观察

主办：安天　　2015 年 8 月 17 日（总第 5 期）试行　本期 4 版　　微信搜索：antiylab

“国家网络与信息安全信息通报机制技术支持单位工作会议”召开

安天小编 / 文

8 月 13 日，由公安部第十一局、国家网络与信息安全信息通报中心、北京市公安局网络安全保卫总队主办，中国科学院软件研究所承办的“2015 年国家通报机制技术支持单位工作会议”在北京召开。

会议由国家网络与信息安全信息通报中心黄小苏处长主持，公安部网络安全保卫局总工程师郭启全、中国科学院软件研究所所长赵琛、北京市公安局网络安全保卫总队石锐大队长等参加了会议并致辞。

目前已经有 50 家单位和机构成为通报机制技术支持单位，其中包括安天、绿盟、知道创宇等安全厂商，公安部第一研究所信息安全等级保护测评中心、中国软件测评中心等测评机构，和阿里巴巴、360 等互联网安全厂商等。

技术支持单位利用各自的技术专长，对重要信息系统和重点网站开展安全监测，并将发现的问题及时上报，为网络安全的态势感知和通报预警工作提供支持。

【安天 CERT】发布

《采用多种沙箱识别技术的 Kasidet 家族分析》报告

（第四版）

英国一电信运营商遭黑客入侵　240 万网络用户信息或泄露

8 月 10 日消息，据《华尔街日报》杂志报道，英国电信运营商 Carphone Warehouse 表示，约有 240 万在线用户的个人信息遭到黑客入侵，其中包含加密的信用卡数据。

Carphone Warehouse 在一份新闻通稿中透露，其网站和互联网服务遭到黑客侵袭，调查显示有多达 240 万用户的个人数据——包括姓名、地址、出生日期和银行卡细节在内——可能遭到黑客访问，其中多达 9 万名客户的加密信用卡数据可能也遭到黑客入侵。Carphone Warehouse 表示，其已立即采取行动确保公司系统安全，同时与电脑安全公司展开联合调查，进而确定具体哪些数据受到影响。

旧金山电脑安全公司 OPSWAT 的副总裁麦克·斯皮克曼 (Mike Spykerman) 表示，“现实情况来看，数据外泄已经不再是什么大不了的问题，但对于 Carphone Warehouse 数据外泄应该另当别论，因为只有部分外泄信息是加密的，而大量数据都没有进行加密。”(http://www.fromgeek.com/telecom/23984.html)

关于互联网网络安全威胁治理行动开展情况的通报

7 月 27 日，互联网网络安全威胁治理行动正式通过 CNCERT 邮箱和 12321 热线接收互联网网络安全威胁的举报。

截至 8 月 9 日，行动共接到投诉威胁举报事件 487 起，包括普通网民举报 38 起和单位举报 449 起。

在行动参与单位中，安天、杭州安恒、深信服举报网页篡改、网页跳转等网站安全事件 217 起，安天举报恶意 APP 事件 28 起，阿里巴巴举报拒绝服务攻击事件 1 起。(http://www.cert.org.cn/publish/main/12/2015/20150811133356200153498/20150811133356200153498_.html)

APT(高级持续性威胁)

类 型	内 容
中文标题	英国招聘网络遭黑客攻击，用户信息网上转储
英文标题	UK job recruiters network hit by hacker，user info dumped online
作者及单位	ZeljkaZorz，Help Net Security
内容概述	TEAM(The Employment Agents Movement)，英国一家最大的独立招聘网，遭到一名沙特阿拉伯黑客的攻击。 表面上，黑客使用了 SQL 注入漏洞，访问了 jobsatteam.com. 会员数据库。 该名黑客网上转储用户信息到 Pastebin 网站。所泄露的信息包括：邮箱、用户名、密码、姓名，以及网站管理员和近 2600 名网站用户的电话号码。 该网站主页目前仍显示“维护中”。 根据该黑客发布的推文内容，他也攻击了其他网站，如：ihimlen.dk，http://knapp.com，http://www.assa.ua 等，同样转储了网站的用户数据库。
链接地址	http://www.net-security.org/secworld.php?id=18739

恶意代码信息

经安天【CERT】检测分析，本周有 5 个移动平台和 7 个 pc 平台的恶意代码家族值得关注

病毒分类	病毒名称	病毒特点
移动恶意代码	GrayWare[AdWare]/AndroidOS.Onar 发现日期：2015 年 8 月 3 日	一类广告的灰色软件家族，会未经用户授权，建立网络连接，向用户弹出广告窗口(威胁较低)。
	RiskWare[Monitor]/AndroidOS.Reaper 发现日期：2015 年 8 月 4 日	一类监控类的风险软件家族。会监控手机进程、流量等，搜集用户信息(风险较低)。
	GrayWare[AdWare]/AndroidOS.Ganlet 发现日期：2015 年 8 月 5 日	一类广告的灰色软件家族，是恶意广告推广(威胁较低)。
	GrayWare[AdWare]/AndroidOS.MobiDash 发现日期：2015 年 8 月 9 日	一类广告的灰色软件家族，是恶意广告推广(威胁较低)。
	Trojan/AndroidOS.Triada 发现日期：2015 年 8 月 10 日	该威胁会窃取用户信息，未经授权访问通讯录和联网下载恶意程序。
PC 恶意代码	Trojan[PSW]/HTML.BankFraud 发现日期：2015 年 8 月 5 日	一类窃取用户密码的木马家族。该家族是钓鱼网页，诱导用户注册，骗取用户的邮箱和邮箱密码(威胁较低)。
	Trojan[Ransom]/Win32.Raas 发现日期：2015 年 8 月 6 日	一类索勒用户的木马家族。该家族运行后开机自启动，遍历文件夹，加密可执行文件，在样本目录出生成一个 txt 文件，告诉用户交赎金方式。
	Trojan/Win32.EquationLaser 发现日期：2015 年 8 月 6 日	该威胁会释放恶意程序，修改注册表和线程注入，会导致计算机重启，并收集用户信息(威胁较低)。
	Trojan[Backdoor]/Win32.Mivast 发现日期：2015 年 8 月 7 日	该威胁会判定用户系统是否为 Admin 账户，打开所入侵电脑后门，让恶意黑客未经授权访问和控制电脑。
	Trojan[Backdoor]/Linux.IrcShell 发现日期：2015 年 8 月 8 日	一类 Linux 系统下的后门木马家族，该威胁会打开所入侵电脑后门，进行恶意操作。
	Trojan[Dropper]/MSIL.Small 发现日期：2015 年 8 月 11 日	一类下载器木马，运行后会连接指定 URL 进行恶意下载行文(威胁较低)。
	Trojan/Win32.LuckyMouse 发现日期：2015 年 8 月 12 日	这种威胁可以让恶意黑客未经授权的访问和控制您的电脑。

黑客可以使狙击步枪失效或更改其目标

Andy Greenberg / 文　　安天公益翻译小组 / 译

只要在狙击步枪上安装一台计算机，就可以把最业余的射手变成世界级的射手。但是，在这个计算机辅助武器上添加无线连接后，您可能会发现，您的智能步枪似乎突然间有了自己的想法，这与您的目标可不甚相同。

在 2 个星期前的黑帽黑客大会上，安全研究人员鲁纳·山特维克和迈克尔·奥格计划展示对两支售价 13,000 美元的 TrackingPoint 自瞄准步枪的为期一年的黑客工作的成果。这对已婚的黑客夫妇开发了一套技术，允许攻击者通过其 Wi-Fi 连接攻陷步枪，并利用其软件中的漏洞。他们的手法能够改变步枪的计算变量，使步枪莫名其妙地错过目标，使步枪的计算机失效，甚至能够阻止步枪发射。在向《连线杂志》提供的展示中，研究人员能够精确地更改步枪的瞄准系统，这会导致子弹击中黑客的目标，而非射手的目标。

TrackingPoint 步枪于 2011 年推出，该公司已售出了千余支高端的、基于 Linux 的自瞄准步枪。可以指定目标，设置变量，如风、温度、弹药的重量。扣动扳机后，这个计算机化的步枪就会自己选择确切的发射时间，只有在枪管完全面向命中目标时才会激活撞针。其结果是，即使是新手也能够从一英里外击中目标。

但是，山特维克和奥格发现，他们可以利用步枪软件中的漏洞链来控制这些自瞄准功能。其中第一项是 Wi-Fi，这是默认关闭的，但可以启用，这样可以将拍摄的发射视频传输到笔记本电脑或 iPad。当 Wi-Fi 打开时，枪的网络有一个默认的密码，在 Wi-Fi 范围内的任何人都能够连接到它。黑客可以把步枪作为服务器，通过访问 API 来改变瞄准应用的关键变量。(当分解了其中一支步枪后，这对黑客夫妇找到了可更改的变量。他们使用 eMMC 读卡器复制了计算机的闪存数据。) 通过 Wi-Fi 连接，攻击者还可以将自己添加到设备上，作为“root”用户，从而完全控制其软件、对瞄准变量做出永久改变，或删除文件使得镜筒无法操作。如果用户设置了 PIN(个人识别码) 来限制其他用户对步枪的访问，root 攻击者还是能够充分访问步枪，并用一个新的 PIN 锁定步枪，使步枪所有者无法访问。攻击者甚至可以使撞针 (一个计算机控制的螺线管) 失效，从而阻止步枪发射。

山特维克和奥格研究了两挺售价为 13,000 美元的 TP750 步枪的电路板并逆向工程了其软件

尽管步枪似乎瞄准了右侧的目标，但是研究人员能够让它击中左侧靶心

奥格用一台笔记本电脑黑了步枪的 WiFi，改变它的发射角度。同时，鲁纳·山特维克使用 TP750 步枪射击 50 码开外的目标。

TrackingPointTP750 镜筒中的视图

在与《连线杂志》的电话访谈中，TrackingPoint 创始人约翰·麦克海尔表示，他赞赏山特维克和奥格的研究，该公司将与他们合作开发软件更新，以便尽快修复步枪的缺陷。他说：“当准备好后，该更新将以 U 盘的形式邮寄给客户。”但他认为，软件漏洞不会从根本上改变步枪的安全性。“射手得扣动步枪的扳机才能发射，而且射手有责任确保步枪指向安全的方向”麦克海尔说，“即使步枪被黑，发射的基本‘目标’也不会改变。”

鉴于 TrackingPoint 面临的财务困境和考虑到消费者手中持有的漏洞步枪只有千余支，山特维克和奥格说，他们不会公布完整的漏洞利用代码。但是步枪的缺陷显示出：未来各种对象 (包括致命武器) 越来越多地连接到互联网，并且会很容易遭到黑客攻击。“很多东西都连接到了互联网，包括汽车、冰箱、咖啡机等，现在连步枪也连接上了”山特维克说，“在这里向 TrackingPoint 等公司说一句，当你把技术应用于那些以前没有应用过的项目上时，就会面临之前未曾想过的安全挑战。”

原文名称	Hackers Can Disable a Sniper Rifle—Or Change Its Target
作者简介	Andy Greenberg，《连线杂志》的资深作家，研究范围涵盖安全、隐私、信息自由和黑客文化。
原文信息	2015 年 7 月 29 日发布于《连线杂志》，原文地址 http://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/
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 CERT】发布

《采用多种沙箱识别技术的 Kasidet 家族分析》报告

近日，安天 CERT(安全研究与应急处理中心)的研究人员捕获了一个针对调试器、模拟器、虚拟机、沙箱、在线自动化样本分析系统的僵尸样本 (Bot)，安天 CERT 研究人员发现该 Bot 样本为 Kasidet 家族，样本版本号为 3.9.4。样本的主要功能是：DDoS 攻击、键盘记录器、窃取文件(如，比特币钱包)、USB 传播、反调试，反虚拟机和反沙箱以及 FTP 嗅探功能。

在分析中，报告对样本的创建进行详细分析后发现，Kasidet 家族具有多种反调试、反沙箱和反虚拟机的功能，样本首先创建线程 1 检测样本是否运行在调试状态下、是否运行在沙箱或虚拟机中。线程 1 创建后会通过调用 IsDebuggerPresent 和 CheckRemoteDebuggerPresent 两个函数检测程序是否运行在调试环境中；如果是，则创建线程 2 弹出错误对话框，然后创建 DOS 格式批处理文件，之后利用 cmd.exe 执行该批处理文件删除自身，退出进程。如果样本没有发现其在调试环境下运行，会通过查看系统用户名、文件路径名两种方式检测样本是否运行在沙箱或自动化病毒分析平台中；利用进程句柄检测样本是否运行在 VM 和 Sandbox 中；利用注册表键检测样本是否运行在 VM 虚拟机、VBox 虚拟机、QEMU 模拟器 (KVM 虚拟机使用此模拟器) 或 BOCHS 模拟器中。接下来，通过系统用户名检测沙箱或虚拟机、获取系统信息、发送上线的 POST 数据并判断系统安装的浏览器信息等一系列进程的创建进而将受害者主机变为一个“僵尸”。

在这篇报告中，安天 CERT 的研究人员针对 Kasidet 家族对调试器、模拟器、虚拟机、沙箱和在线自动化恶意代码分析平台的检测进行了详细分析。

从 Kasidet 家族反制在线自动化恶意代码分析平台的方法上看，该家族的作者有可能通过对常见的在线自动化恶意代码分析平台进行过针对性的研究，利用收集各种系统信息的恶意代码提炼出反制在线自动化恶意代码分析平台的方法，并应用到 Kasidet 家族中。

安天 CERT 的研究人员对 Kasidet 家族的其他版本进行对比分析发现，不同的 Kasidet 家族变种对模拟器、虚拟机、沙箱的检测也略有不同。例如，有的变种通过检测虚拟机运行时所需要的 DLL 文件来判断是否运行在虚拟机中。(可搜索安天微信公众号 antiylab 及时关注最新报告)

恶意程序

安天【追影高级持续威胁分析系统】无需更新病毒库，可实现对 Kasidet 家族进行有效检测，下为其自动形成的分析报告

该恶意程序由安天威胁检测系统发现，经过追影威胁分析系统分析。经由 BD 静态分析鉴定器、美国软件交叉索引 (NSRL) 鉴定器、数字证书鉴定器、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将文件判定为恶意程序。

该文件具有以下行为：

根据进程名称复制文件；隐藏文件；获取主机用户名称；篡改系统文件创建时间；复制自身文件；打开自身进程文件；请求调试权限；释放 PE 文件；获取驱动器类型；增加 run 自启动项；获取计算机名称。

文件名	4298A3CFC3E890A4AF82C1721EB4372D
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	103 KB
MD5	4298A3CFC3E890A4AF82C1721EB4372D
病毒类型	恶意程序
恶意判定 / 病毒名称	Trojan[Bot]/Win32.Kasidet
判定依据	BD 静态分析
下次鉴定时间	约 2 周

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=4298A3CFC3E890A4AF82C1721EB4372D

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
根据进程名称复制文件	★★★	隐藏文件	★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
获取主机用户名称	★	篡改系统文件创建时间	★★
复制自身文件	★★	打开自身进程文件	★
请求调试权限	★	释放 PE 文件	★
获取驱动器类型	★	增加 run 自启动项	★
获取计算机名称	★	隐藏文件	★★