安天周观察

主办：安天　2016 年 7 月 4 日（总第 46 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天移动安全公司与泰尔终端实验室正式签署战略合作协议

6 月 28 日，安天移动安全公司与泰尔终端实验室在北京正式签署战略合作协议，共建战略合作伙伴关系。双方将在移动网络安全领域开展全面合作，进一步实现优势互补、信息共享、互利共赢，提升框架协同层次和水平，携手为手机厂商创造移动安全价值。

目前，安天移动安全公司与泰尔终端实验室在安全检查工具上已经开展了良好的合作。随着本次战略合作协议的签署，双方将达成更紧密的合作，在预置应用安全检测、移动生态链安全监测、移动漏洞检测分析等方面提供更好的服务，并在移动信息安全技术、标准建设、业务拓展、客户服务等各个方面，进一步扩大合作范围，强化合作内容，提升合作价值。

本次战略合作对双方均意义重大，安天实验室首席架构师表示：“此次安天与泰尔战略合作框架协议的签署，是按照习总书记在视察安天时所做出的‘网络安全是国家安全的重要组成部分。维护国家网络安全需要整体设计、加强合作，在相互学习、相互切磋、联合攻关、互利共赢中走出一条好的路子来。’的指示，在移动终端安全检测领域加强合作的一个典型范本”。

泰尔终端实验室主任王南也表示：“将安全公司最前沿的安全技术和嗅探到的安全事件快速映射到实验室检测中，让终端厂商、应用软件开发者快速提升产品安全性，有效应对最新安全攻击，提升整个产业的安全防护能力。”

未来，安天移动安全公司与泰尔终端实验室将进一步探讨和尝试更多的战略合作模式，充分利用彼此的技术实力和检测优势，为手机厂商提供更加便利、更加高效的服务，共同致力于推动智能移动终端生态环境的净化。

安天各地党支部开展纪念中国共产党成立 95 周年活动

为纪念中国共产党成立 95 周年，安天各地党支部按照“两学一做”指示，集中开展了系列活动，将党的精神融入到企业内部。

哈尔滨安天党支部

7 月 1 日，以迎接中国共产党成立 95 周年为契机，哈尔滨安天党支部开展了“两学一做”学习教育活动。安天哈尔滨总部的 42 名党员全体参加了本次活动，党支部按照惯例为各位党员分发了党章和党徽，全体党员在党支部书记苗文起的带领下，面对党旗进行了庄严的宣誓，重温了入党誓词，增强了身为党员的荣誉意识和表率意识。

随后哈尔滨全体党员集体观看学习了“习近平总书记在庆祝中国共产党成立 95 周年大会上的重要讲话”，一同回顾了党成立 95 周年以来的伟大历史贡献。总书记在讲话中指出“无论顺境逆境，我们党从未动摇对马克思主义的信仰。”这对于在座的每一位党员来说，都是一种激励，提醒着他们不忘初心、继续前进。

哈尔滨安天党支部全体党员重温入党誓词

北京安天党支部庆祝建党 95 周年党员学习交流活动

北京安天党支部

北京安天党支部紧跟党的步伐，积极开展“两学一做”学习教育活动，在党支部书记陈淑兰的带领下，进行了思想汇报与交流工作，用文字抒发了对党的热爱。每一位党员都阐述了对总书记重要讲话精神的心得体会，以及对“两学一做”积极落实的感受，抒发了对党的祝福之情。同时，北京安天全体党员表示坚决拥护党的领导，弘扬爱国主义精神，从自身做起，努力学习，刻苦钻研，对党忠诚、为党分忧，为建设世界科技强国努力，为保障网络安全做出更扎实、更有效地工作。

哈尔滨安天党支部荣获“先进基层党组织”称号

6 月 28 日，在中共哈尔滨市委庆祝中国共产党成立 95 周年暨表彰大会上，哈尔滨安天党支部被授予“先进基层党组织”荣誉称号。

哈尔滨安天党支部自成立以来紧紧围绕网络安全领域的工作实际，积极探索基层党组织建设的新思路、新方法，深入开展“两学一做”学习教育活动，认真学习总书记系列讲话与网信工作座谈会讲话精神，提升党支部建设的能力和活力，针对企业特点创新党建工作，为打造绿色健康的网络安全环境做出了贡献。

每周安全事件

类 型	内 容
中文标题	勒索软件 Locky 卷土重来 已感染 49 个域名
英文标题	Locky Ransomware is back! 49 domains compromised!
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，安全专家们发现了大量的恶意邮件，经过一段时间的调查分析，专家们发现前不久消失的勒索软件 Locky 再次卷土重来，并且比从前多了许多新特征，比如：它添加了反分析技术，配备了可以解码有效负载参数的 javascript。对于如何预防勒索软件 Locky，专家建议用户禁用 vssadmin.exe 服务，因为这样可以防止勒索软件删除卷影副本，受害者们还会有很大机会可以自行恢复加密文件。
链接地址	http://securityaffairs.co/wordpress/48725/malware/locky-ransomware-back.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	RiskWare/Android.adevman.a[exp]] 2016-06-27	该应用程序运行后强制要求激活设备管理器，后续通过推送插件私自下载指定程序，执行有界面的安装操作，存在一定安全隐患，会造成用户流量损耗，建议及时卸载。（威胁等级高）
		RiskWare/Android.Iguanasms.a[exp，rmt]2016-06-29	该应用程序是一个应用市场，会监听指定短信，接收指令内容，下载安装 APK 或音频文件，并且具有支付功能，存在一定资费损耗风险，建议谨慎使用。（威胁等级中）
		Trojan/Android.Zkkkkz.a[sys，fra]2016-06-29	该应用伪装成系统程序，运行后隐藏图标诱导激活设备管理器，后台联网上传手机固件信息，获取推广数据，申请 root 权限并私自篡改浏览器主页，执行推送广告操作，存在一定安全隐患，会造成用户资费消耗，建议及时卸载。（威胁等级高）
		G-Ware/Android.OloadMain.a[rog，exp]2016-06-30	该应用程序运行后隐藏图标，诱导激活设备管理器，后台联网下载指定推广程序，执行广告推广操作，存在一定安全风险，会造成用户流量损耗，建议及时卸载。（威胁等级低）
		RiskWare/Android.Gibdy.a[prv] 2016-06-30	该应用程序运行后会上传手机系统版本、手机分辨率、国家、cpu 类型等设备信息至远程服务器，并在后台执行 banner 广告推送，会造成用户隐私泄露，建议及时卸载。（威胁等级低）
	较为活跃的样本	G-Ware/Android.Fakegupdt.bo[exp，rog]	该应用程序伪装成色情程序，运行后释放恶意子包，执行私自下载风险子包、加载广告插件、创建桌面图标等操作，影响用户正常用机体验，造成资费消耗，建议及时卸载。（威胁等级低）
		Tool/Android.viettrack.c[sys]	该应用是一款短信电话屏蔽软件，用户可以设置黑名单，软件会根据黑名单的数据进行拦截屏蔽，如非自主安装，建议及时卸载，以免影响手机正常使用。（威胁等级低）
		G-Ware/Android.HiddenAds.z[rog，exp]	该程序伪装成系统服务，安装无图标，后台推送通知栏广告，建议立即卸载，避免造成资费损耗。（威胁等级低）
		Trojan/Android.Dendroid.c[prv，exp，rmt，sys]	该程序伪装成系统应用，在后台接收远程指令，进行上传收件箱短信、发送短信、删除收件箱短信、加解密 SD 卡文件、锁定用户界面等操作，建议立即卸载，避免造成资费损耗和隐私泄露。（威胁等级中）
		G-Ware/Android.jianmo.af[rog，sys]	该应用程序伪装成游戏辅助应用，运行后诱导激活设备管理器，激活后会设置锁屏密码锁定手机，造成手机无法正常使用，建议立即卸载。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Advantech WebAccess 缓冲区溢出漏洞 (CVE-2016-0860)	WebAccess HMI/SCADA 软件提供远程控制与管理，可使用户在设施管理系统、发电站、楼宇自动化系统中，轻松查看与配置自动化设备。在 Advantech WebAccess 8.1 之前的版本中，BwpAlarm 子系统存在缓冲区溢出漏洞，远程攻击者通过构造的 RPC 请求，利用此漏洞造成拒绝服务。（威胁等级高）
	较为活跃的样本	RiskWare[RiskTool]/Win32.OfferInstall	此威胁是一种风险软件类程序，该家族样本运行后会联网下载浏览器插件并安装，可能会弹出广告，而且具有反虚拟机功能，占用系统资源，影响用户使用。（威胁等级中）
		Trojan[Spy]/Win32.FinSpy	此威胁是一种间谍木马程序，该家族样本可以监视用户系统操作，连接远程服务器下载并安装其他恶意代码，回传用户敏感信息，造成一定威胁。（威胁等级中）
		Trojan[Exploit]/Linux.Enoket	此威胁是一种溢出型木马程序，该家族样本运行后可以对 Linux 系统进行溢出攻击，攻击形式多样化，会造成一定威胁。（威胁等级中）

25,000 台 CCTV 设备构成的僵尸网络

Chris Brook/ 文　安天公益翻译小组 / 译

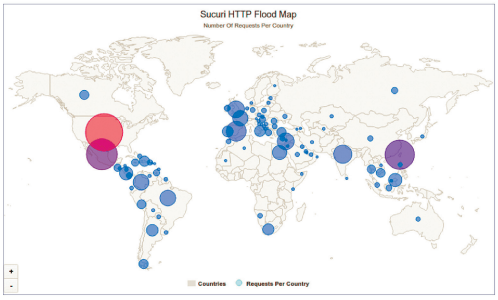
近日，一个完全由连网闭路电视设备构成的僵尸网络使用一系列 HTTP 请求，致使一家珠宝店的网络整体瘫痪了好几天。

发现该僵尸网络的研究人员表示，目前，物联网设备已经开始被用来开展分布式拒绝服务攻击了，他们对这一点并不感到意外，但是他们没有想到，这种攻击能够持续这么久，并且使用了超过 25,000 台闭路电视 (CCTV) 设备。

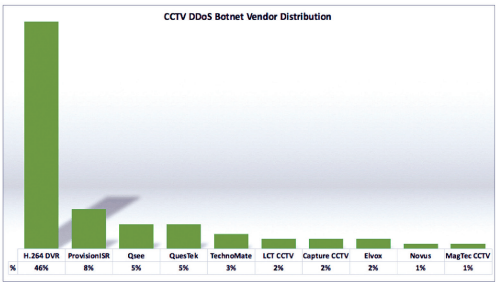
最先发现该珠宝店遭到攻击的是 Sucuri 的研究人员，他们发现珠宝店遭到了第 7 层 HTTP 洪泛攻击，导致每秒生成 35,000 HTTP 请求。并且他们还发现，在随后的一次进攻中，请求的数量有所增加，一秒之后达到了 50,000 个请求，这促使 Sucuri 进一步研究了该攻击的来源。

Sucuri 公司的创始人和首席技术官丹尼尔·西德表示，在这之后，他们发现了 25,513 个不同的 IP 地址生成了一个持续几个小时的 DDoS 攻击，其中大多数 IP 地址位于台湾，其他的 IP 地址主要分布在印度尼西亚、墨西哥、马来西亚和以色列。

研究人员分析了地理分布，发现该僵尸网络实际上依赖于全球 100 多个国家和地区的 IP 地址。研究人员经过继续分析发现，该僵尸网络的流量主要源于运行 Cross Web Server，它是一种软件，可用于多种不同的 CCTV 硬盘录像机。



HTTP 洪区



CCTV DDoS 僵尸网络厂商分布

Sucuri 还指出，其中约 46% 的 CCTV 设备是 H.2644 网络数字视频录像机。其他设备包括由以色列公司 Provision-ISR，在家得宝和好市多商店销售设备的制造商 Q-See，总部设在越南的制造商 Questek 生产的闭路电视盒。

西德表示，BusyBox 是所有的设备的运行软件，它以单一的可执行文件提供 Unix 工具，可以运行于 Linux、Android 和 FreeBSD 系统。但是，在今年 3 月，Sucuri 发现了一个远程代码执行漏洞，该漏洞影响了 70 个 CCTV 厂商生产的硬盘录像机 (DVR) 盒，但是目前还不确定该僵尸网络是否与此漏洞有关。当时，Provision-ISR，Q-See 和 Questek 的设备都受到了该漏洞的影响，但西德表示，目前这一点未经证实。

西德指出，考虑到这一点，他们无法快速地修复 CCTV 设备。即使他们能够做到，攻击者也会直接移动到下一个目标。

西德说：“不幸的是，作为网站所有者，你无法修复和保护这 25,000+ 闭路电视设备。也无法修复数百万存在漏洞、被用作僵尸网络和 DDoS 放大方法的设备。而且这只是其中的一小部分问题，一旦设备被修复，攻击者就会寻找其他容易被破解的设备。”

去年秋天，Incapsula 的研究人员也发现了类似的 CCTV 僵尸网络，该公司的一个客户也遭受了一系列的 HTTP 洪泛攻击，全球 900 台闭路电视设备每秒生成约 20,000 个请求。与 Sucuri 审查的 DVR 一样，所有被感染的设备都运行 BusyBox。然而，在这种情况下，内部的恶意软件会积极寻找易受暴力字典攻击的开放的 Telnet/SSH 服务。

目前，Sucuri 公司正在联系那些设备已被感染的网站。同时，Sucuri 公司认为，如果有用户已经使用了这样的设备，他们至少应该保证做到去修复并隔离它们。

原文名称	Botnet Powered by 25，000 CCTV Devices Uncovered
作者简介	Chris Brook，《Threatpost》副编辑。
原文信息	2016 年 6 月 28 日发布于《Threatpost》，原文地址 https://threatpost.com/botnet-powered-by-25000-cctv-devices-uncovered/118948/

安天发布
《ELF 格式恶意代码伪装 GET 请求发动 CC 攻击》分析报告

近日，安天追影小组在持续追踪网络犯罪的过程中，发现了一款将 CC 攻击数据包中的 User-Agent 伪装成 Windows 系统的 ELF 格式恶意代码的样本。

ELF 格式是 Linux 下的可执行文件格式，User-Agent 则是 HTTP 协议的一部分，包括浏览器类型、操作系统及版本等信息，Web 服务器可以通过该字段获取客户端的信息。

CC 攻击是 DDoS 攻击的一种，基于 HTTP 层面，主要用来攻击页面。在 CC 攻击中，攻击者通常会模拟具有大量用户访问目标的 Web 服务器的某个页面，消耗大量的服务器资源，使得服务器没有办法响应正常用户的访问。

CC 攻击分为两类，代理 CC 攻击与肉鸡 CC 攻击。代理 CC 攻击是指黑客借助代理服务器生成指向目标服务器的合法网页请求，而肉鸡 CC 攻击是指黑客控制大量肉鸡发起大量对目标服务器的合法网页请求。相比之下，肉鸡 CC 攻击更难防御，因为肉鸡可以模拟成正常用户访问网站的请求。

追影小组所捕获的样本就选则了肉鸡 CC 攻击，研究人员通过分析发现，该样本发动 CC 攻击时，会将其攻击数据包中的 User-Agent 伪造成来自 Windows 系统的 IE 浏览器，假装成正常的请求，使得 CC 攻击数据包难以被检测，同时，这样还会影响一些安全设备对肉鸡操作系统的误判，使得基于 UA 规则的特征查杀失效，达到隐藏发动攻击的肉鸡系统信息的效果。

近年来，DDoS 攻击的平台逐渐由 Windows 转向 Linux。这是因为网络上的 Linux 服务器性能比家用电脑更优，安全关注程度又较低，比较容易入侵，攻击者更乐于将其作为发动 DDoS 攻击的肉鸡。

安天追影小组提醒广大 Linux 服务器管理员，要时刻关注服务器的安全防护，及时修复漏洞，定期检测是否存在异常的网络数据。

木马程序

安天【追影威胁分析系统】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、动态行为 (Linux) 鉴定器等鉴定分析。

文件名	9DDEA24FEF90B4F049B4A90438AAAA7F
文件类型	BinExecute/Linux.ELF
大小	4.86 MB
MD5	9DDEA24FEF90B4F049B4A90438AAAA7F
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Dofloo
判定依据	动态行为 (Linux)

◆ 危险行为

行为描述	危险等级
ELF_Pretend_WinUA	★★★★★
LinuxAESDDoS	★★★★★
LinuxHacktool_eyes_scanner	★★★★★
连接已知 C&C 主控	★★★★★

最终依据 BD 静态分析鉴定器、动态行为 (Linux) 鉴定器将文件判定为木马程序。该文件具有以下行为：

ELF_Pretend_WinUA、LinuxAESDDoS、LinuxHacktool_eyes_scanner、连接已知 C&C 主控、获取 CPU 信息、连接网络、获取网卡信息。

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
获取 CPU 信息	★	连接网络	★
获取网卡信息	★		

◆ 网络监控：UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.11	35456	192.168.122.1	53
192.168.122.1	53	192.168.122.11	35456

◆ 进程监控

PID：-	创建：/tmp/1467357353.25-9DDEA24FEF90B4F049B4A90438AAAA7F.elf.zy.elf
	命令行：[/tmp/1467357353.25-9DDEA24FEF90B...]

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=9DDEA24FEF90B4F049B4A90438AAAA7F