安天周观察

主办：安天　2016 年 9 月 5 日（总第 55 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

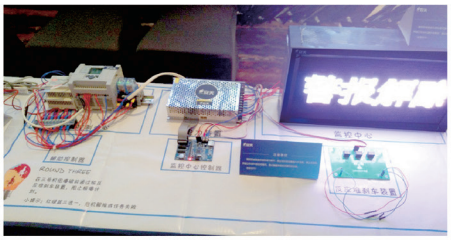
安天研究人员在安全焦点峰会进行两场主题演讲

8 月 29 日 -30 日，XCon2016 安全焦点信息安全技术峰会在京召开。该峰会已连续举办 15 届，是国内历史最为悠久、最有代表性的民间信息安全会议。安天多位研究人员曾在安全焦点信息安全技术峰会上发布超过十场重要演讲。

在本次大会上，安天移动安全研究员陈传文做了题为《无线应用通信安全》的主题演讲，对无线客户端的安全问题进行了深切的交流与分享。

报告着眼于无线客户端，从客户端载体、证书和证书验证等方面入手，展现了国内外浏览器对安全设计理念的不同，论证了：客户端 HTTPS 安全编程既简单又相对安全，错误的自定义实践反而会严重损害 HTTPS 的安全性。这些错误的实践包括：不限于使用自签使之对攻击而言退化成为普通的 HTTP 名证书且验证不当，覆　盖 X509TrustManager 实现不当，设置不安全的证书域名验证方式，忽略 Webview 抛出的 SSL 错误。报告还提供了各种不同定制程度的 HTTPS 访问实现的正确示例。

安天微电子与嵌入式安全研发中心主任、资深研究员桑胜田做了题为《SRAM 型 FPGA 的信息安全风险浅析》技术演讲。他在演讲中就 FPGA 的安全问题作了深刻的阐述，并呼吁 FPGA 应用企业和安全厂商紧密协作，共同应对 FPGA 特有的安全挑战。



桑胜田指出，在基因测序，大数据分析，机器学习等应用的需求牵引和微电子技术发展的推动下，FPGA 正逐渐从专用的电子器件转变为通用信息处理的计算工具，FPGA 特有的技术特性使其在高性能计算方面展现出了巨大优势和潜力。

在演讲中，桑胜田报告从 FPGA 的产业结构、FPGA 工作原理和开发应用模式特点等方面入手，讲述了其所面临的特有的信息安全挑战。重点介绍了 FPGA 系统可能的攻击面，恶意逻辑篡改带来的安全风险。报告还指出了针对 FPGA 逻辑攻击的检测、防御和分析取证的难点。

他最后还在现场操作演示了电磁辐射、LED 指示灯和 VGA 夹带信息泄露等 FPGA 攻击，分析目前 FPGA 封闭硬件架构和闭源工具链等潜在安全隐患，并以实例演示信息泄露威胁，希望引起对逐渐走进通用计算领域的 FPGA 安全问题的重视。

安天在本次大会上设有展位，主题为“安天硬件与外设安全探索之旅”，并增设互动游戏环节，通过运用真实的工业控制环境，来把虚拟的故事背景贯穿始终，使挑战者能够亲身接触并进行操作可用于真实工控环境当中的设备，进而了解真实工业控制场景中的控制机制。

同时，现场安天也为对工控安全感兴趣的小伙伴提供了安天原创的技术汇编五《工控系统安全分册》，以及技术汇编八《移动安全专题第二分册》、汇编十《高级持续性威胁（APT）专题第二分册》、《乌克兰电力系统遭遇攻击停电事件综合分析报告》等资料，受到与会安全研究者、爱好者的好评。

用 WiFi 信号就能捕获击键记录盗取密码

近日，据外媒报道，来自美国密歇根州立大学和中国南京大学的研究人员找到这样的方法，他们通过一个普通路由器使用 WiFi 信号准确检测出击键记录。

研究人员指出，在受到最小信号干扰的环境下，攻击者能通过中断路由器 WiFi 信号来检测出用户在键盘上的击打记录，然后利用这些数据盗取他的密码，准确率达到 77% 到 97.5% 之间。而除了获取击键记录之外，WiFi 信号还能用于读取用户手势、嘴唇动作。（来源：http://news.secwk.com/article/newinfo/detail/7508294271018309 81#?sideActiveTab=fast）

一周简讯

- 安攻击者利用恶意代理窥探 HTTPS 加密流量
- MinecraftWorldMap 网站泄露 7 万用户账号
- BitLocker 增强工具包含可用于后门的漏洞
- 新型勒索软件 FairWare 目标为 Linux 服务器
- 研究人员曝光黑客劫持 Chrome 浏览器新伎俩
- 研究人员发布分析报告揭示勒索软件 ZEPTO 机理
- 谷歌登录页面 BUG 可导致自动下载恶意软件

（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	至少 6800 万 Dropbox 用户存在数据泄露风险
英文标题	Dropbox 2012 Mega Breach Affected over 68 Million Users
作者及单位	Catalin Cimpanu；Softpedia
内容概述	近日，云储存服务提供商 Dropbox 向广大用户发布邮件，要求尽快完成密码重置。其原因是安全团队最近在网络上发现了一批账户凭证，并相信应该就是 2012 年数据泄露事件中流出的。尽管在最初的声明中并未明确有多少用户受到影响，不过在近期的报道中表示至少有 6800 万用户存在数据泄露风险。据报道，从数据交易社区和 Leakbase 掌握的消息中发现了 68680741 条 Dropbox 的账户凭证，其中包括用户的邮件地址、Hash 值、密码等等，一位匿名 Dropbox 员工证实了这些数据的真实性。根据 Motherboard 的用户数据缓存，因使用 bcrypt hashing 功能，将近 3200 万密码是安全的，此外加盐的 SHA-1 Hash 也能够了一层保护。
链接地址	http://news.softpedia.com/news/dropbox-2012-mega-breach-affected-over-68-million-users-507783.shtml

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.mjgamecc.a[prv, sys]2016-08-29	该应用程序运行后会释放恶意子包程序，执行私自提权，会上传手机地理位置信息以及已安装程序包信息，执行创建桌面快捷图标、推送通知栏等操作，并对下载的程序执行静默安装，存在一定安全风险，会造成用户的隐私泄露和资费消耗，建议及时卸载。（威胁等级高）
		G-Ware/Android.FakeUcaddon.a[rog, exp]2016-08-30	该应用会伪装成正常应用，会弹窗显示升级并诱导用户点击下载安装，安装后会隐藏图标，后台会获取当前运行的程序信息并上传到服务器，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级低）
		Trojan/Android.eaegmt.a[prv, rmt, exp]2016-09-01	该程序会伪装成正常应用，运行后会隐藏图标，激活设备管理器。后台会窃取手机固件信息、用户短信、用户通讯录并上传到服务器。会私自访问 url 并下载图片，接收远程控制指令设置呼叫转移、群发短信、启动 ussd 服务，会给用户造成隐私泄露和财产损失。建议立即卸载。（威胁等级高）
		Trojan/Android.dice.a[exp, rog] 2016-09-01	该应用运行后会隐藏图标，包含恶意支付插件，会私自发送短信、拦截指定短信，造成用户资费消耗，建议谨慎使用。（威胁等级高）
	较为活跃的样本	Trojan/Android.XMApp.a[rog, sys, exp]2016-09-01	该程序运行后会私释放恶意子包，会执行私自提权，执行安装、卸载指定程序、更改杀软本地白名单，会对手机安全造成严重影响，后续还会加载广告插件，会执行广告推广操作，影响用户正常体验，建议及时卸载。（威胁等级高）
		Trojan/Android.apptask.a[pay, prv] 2016-09-02	该应用安装后无图标，运行后会调用子包，监听拦截短信、删除短信。会上传手机固件信息，获取支付号码并通过短信进行支付，造成用户资费损失，建议立即卸载。（威胁等级高）
		Trojan/Android.Triada.k[exp, rog]	该应用程序会伪装系统应用，运行隐藏图标并释放恶意子包，私自下载释放广告子包，执行通知栏、插屏、创建快捷方式的推广操作，会弹出虚假提示诱导用户安装虚假应用，会造成用户资费消耗，建议及时卸载。（威胁等级低）
		Trojan/Android.InfoStealer.z[prv]	该应用运行后会私自联网窃取用户设备固件信息、短信信息、通讯录信息和通讯记录信息，会造成用户隐私泄露。（威胁等级低）
		RiskWare/Android.SmsThief.at[prv, exp]	该应用运行后无实际功能，包含获取用户接收的短信并通过短信和联网方式上传的风险代码，会造成隐私泄露和资费损耗，建议不要安装。（威胁等级中）
		G-Ware/Android.jianmo.aq[rog, sys]	该应用会伪装成 QQ 点赞精灵，会在界面置顶，勒索用户添加指定 QQ 群进行付费解锁，获取手机固件信息并转发，会造成用户隐私泄露和资费损失，建议立即卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Reader 双重释放远程代码执行漏洞 (CVE-2016-0935)	Adobe Reader 在处理 PDF 文档内畸形的 ExtGState 字典时存在安全漏洞，会导致双重释放。攻击者利用此漏洞可在当前进程上下文中执行任意代码。（威胁等级高）
	较为活跃的样本	Trojan/Win32.Wurser	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后会连接远程服务器，收集系统信息并回传，它还可以打开 cmd shell，进行一系列的恶意操作。（威胁等级中）
		Trojan/Win32.Paneidix	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后，会连接远程服务器并接受恶意操作，收集用户信息并回传。（威胁等级中）
		Trojan[Downloader]/Win32.Carbanak	此威胁是一类会窃取用户银行信息的木马家族。该家族样本运行后会连接远程服务器下载恶意代码，窃取用户银行帐号密码。（威胁等级中）
		Trojan[Downloader]/Win32.Nurjax	此威胁是一类可以下载恶意代码的木马家族。该家族样本运行后会劫持浏览器，在用户浏览特定网页时会重定向到恶意页面，下载恶意代码并运行。（威胁等级中）

100 万物联网设备遭到 BASHLITE 恶意软件感染

Tom Spring / 文　安天公益翻译小组 / 译

近日，研究人员指出，超过 100 万台消费者连网摄像机和数字视频录像机 (DVR) 遭到僵尸网络操控者的入侵，他们利用这些设备执行 DDoS 攻击。

Level 3 威胁研究实验室 (Level 3 Threat Research Labs) 表示，攻击者使用了一个名为 BASHLITE 的小型恶意软件家族执行这些攻击。

Level 3 通信公司首席安全官戴尔·德鲁 (Dale Drew) 说："这项研究使我们很震惊。在分析 BASHLITE 恶意软件时，我们发现它被用于一个组织化和结构化大大超出我们预期的僵尸网络。"

研究人员指出，BASHLITE 负责分配规模不等的 C&C 服务器和僵尸网络。7 月份，他们追踪了与该恶意软件家族有关的 C&C 服务器，发现它们只与 74 台僵尸机器通信。后来，研究人员又发现，该恶意软件家族与多达 120,000 台僵尸机器通信。德鲁说，进一步分析 BASHLITE 恶意软件之后，他们发现了一个包括近 100 台 C&C 服务器的僵尸网络。一些 C&C 服务器每天会执行超过 100 次的 DDoS 攻击，其中，75% 的攻击持续时间不超过 5 分钟。

德鲁说："我们有一种错觉，以为一些貌似小规模的僵尸网络不会造成很大的伤害。其实，这些僵尸网络是分块的，当人们研究这些僵尸网络时，往往只看到了一部分，而不是整个网络。"

该公司在其技术报告中写道，该恶意软件背后是诸如 Lizard Squad 和 Poodle Corp 的黑客组织，这些组织越来越多地利用物联网设备来构建僵尸网络，执行 DDoS 攻击并提供 DDoS 攻击服务。

报告指出："攻击者获得设备的访问权限后，他们懒得去找出设备的架构。相反，他们会立即执行 busybox wget 和 wget 命令来检索他们的 DDoS 僵尸程序载荷。然后，他们会尝试运行该恶意软件的多个版本，直到有一个版本能够运行为止。"

在 100 万台受感染的终端设备中，96% 是物联网设备（其中 95% 是摄像机和录像机），约 4% 是家庭路由器，不到 1% 是 Linux 服务器。研究人员说："这代表了僵尸网络组成的巨大转变，不同于过去基于服务器和家庭路由器的 DDoS 僵尸网络。"

研究人员说，连网录像机是攻击者的主要目标，因为它们唾手可得。很多录像机配置了 Telnet，启用网络界面，并使用默认凭证。该公司指出："这些设备大多运行嵌入式 Linux 系统，当有提供视频流所需的带宽时，它们能够提供大量的 DDoS 僵尸机器。"

协助 Level 3 进行分析的 Flashpoint 公司指出，在过去的几个月中，他们一直在追踪与 BASHLITE 恶意软件家族有关的 200 台 C&C 服务器。与复杂的恶意软件不同，和该攻击活动有关的 C&C 服务器 IP 地址硬编码到恶意软件中，往往只指定一个 IP 地址，因此很容易被安全研究人员发现。

研究人员写道："僵尸网络操控者似乎并不关心这个问题，因为他们能够很容易地创建新的 C2 服务器并重新感染僵尸机器。"

Level 3 公司指出，大多数受感染的终端与少数几个公司有关，这些公司实施松散的物联网设备安全标准，有的公司甚至没有实施这种安全标准。Level 3 在报告点名大华科技 (Dahua Technology)，它是设备遭到该恶意软件攻击的三家厂商之一。德鲁称，该公司正准备修复漏洞，不久将会进行部署。

这已经不是连网摄像机第一次被用于僵尸网络攻击了。今年初，Sucuri 研究人员发现了一个规模小得多的、包括 25,000 台连网 CCTV 设备的僵尸网络。此外，Arbor 的安全工程和响应团队 (ASERT) 也在今年初发现了一个利用 1,300 台网络摄像机的僵尸网络。

原文名称	BASHLITE Family Of Malware Infects 1 Million IoT Devices
作者简介	Tom Spring，卡巴斯基《安全周报 (Threatpost)》的副主编。
原文信息	2016 年 8 月 30 日发布于《安全周报 (Threatpost)》 原文地址 https://threatpost.com/bashlite-family-of-malware-infects-1-million-iot-devices/120230/
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《ProjectSauron 间谍平台样本简要分析报告》

近日，安天追影小组在整理网络安全事件时，发现了网络间谍平台 ProjectSauron 的 APT 攻击事件并进行了简要分析。ProjectSauron 是一个模块化平台，旨在实现持续性的网络间谍活动，并长期管理被控制的网络间谍活动目标。该平台使用了改进的 LUA 脚本引擎来实现平台的核心功能和插件，对所有的攻击模块和网络协议都使用了强加密算法，例如 RC6，RC5，RC4 等。ProjectSauron 平台的攻击目标主要是通信加密软件，平台中的攻击模块能够窃取加密密钥，配置文件，以及获取与加密软件相关的关键基础设施服务器的登陆凭证等，有着较高的危害性。

经分析，ProjectSauron 平台通过散播含有恶意代码的软件升级脚本，会在攻击目标进行软件升级时，诱导用户触发恶意脚本，进而在攻击目标系统内存中注入一个较小的下载模块，一旦在联网环境下启动，该下载模块就会连接到一个硬编码的内部或外部 IP 地址上，并从中下载更大的攻击模块。安天追影小组针对 ProjectSauron 平台攻击模块中 MD5 值为 6cd8311d11dc973e970237e10ed04ad7 的样本进行分析，发现该样本是一个 Microsoft Visual C++ 的功能 DLL 库。ProjectSauron 平台被动后门模块被激活时，通过该功能 DLL 库进行相关间谍窃密行为模块的启动和下载。该 DLL 含有 Initialize 模块和 Password 模块，Initialize 模块用来下载攻击模块和执行攻击者命令，Password 模块用来运行 LUA 攻击脚本窃取信息。在内存中加载后，Initialize 模块会启动对 http://www.msftnc*.com/ncsi.txt 域名的 GET 请求下载攻击模块以及对 104.99.238.* 的 IP 地址的进行反向连接，同时我们也收集到对 104.131.61.*、wildhorses.awardspac*.info 等多个 IP 以及域名的通信行为，Password 模块会在 Windows 域控制器 (DC) 的内存中加载一个 Windows 密码过滤器，用于窃取明文形式的敏感数据。

通过对 ProjectSauron 平台的分析了解，可以看出恶意代码商业化的快速发展以及技术的多样性正在逐渐威胁到个人信息的安全。安天提醒网络使用者注意网络环境的异常情况，避免攻击者通过鱼叉式钓鱼邮件或其他手段入侵企业网络。目前，安天追影产品已经实现了对该类样本的检出。

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。最终依据静态分析鉴定器将文件判定为木马程序。

该文件具有以下行为：独占打开文件、填充导入表（疑似壳）。

文件名	6CD8311D11DC973E970237E10ED04AD7
文件类型	BinExecute/Microsoft.DLL[:X86]
大小	380 KB
MD5	6CD8311D11DC973E970237E10ED04AD7
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[:HEUR]/Multi.Remsec
判定依据	静态分析

◆ 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

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
独占打开文件	★	填充导入表（疑似壳）	★★

◆ 网络监控

UDP 信息			
源 IP	源端口	目的 IP	目的端口
0.0.0.0	68	255.255.255.255	68
192.168.122.1	67	192.168.122.97	67
192.168.122.97	137	192.168.122.255	137

进程衍生关系
LoadDll.exe

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=6CD8311D11DC973E970237E10ED04AD7