安天周观察

主办：安天　2016 年 9 月 12 日（总第 56 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天为 G20 杭州峰会保驾护航

2016 年 9 月 5 日，举世瞩目的二十国集团领导人第十一次峰会 (G20) 在浙江杭州圆满落幕。安天作为本次 G20 峰会网络安保的重要支撑单位之一，通过安天网络安保团队多日的安全值守及不懈努力，为大会召开保驾护航，圆满完成了本次峰会网络安保任务。

为保障本次 G20 网络安全防护工作的顺利推进，安天成立了专门的 G20 峰会项目组。2016 年 6 月中下旬，项目组便参与本次保障工作，对杭州 1300 余家网站进行安全检测时发现近百处安全漏洞。为提供相关重要基础设施的监测与防护工作，安天派驻多位技术专家前往杭州现场值守；安天技术专家前期通过对重点单位网站的风险排查，及时于会前对重点单位网站进行系统


聘　书

兹聘请哈尔滨安天科技股份有限公司为二十国集团峰会网络安全保卫工作技术支持单位。

二十国集团峰会网络安全保卫组
（公安部网络安全保卫局代章）
2016 年 7 月 6 日

加固，进一步增强抵御骇客攻击能力。与此同时，安天哈尔滨本部大后方也成立了 G20 峰会保障组，组织 120 名工程师在线进行 7×24h 不间断值守，对其防护的重点网站进行全面监控，并结合各方收集到的威胁情报，来保证网络安全防护工作的严密周到。本次 G20 峰会项目组中很多成员都经历了北京奥运网络安全保障的洗礼和实战检验，多位工程师曾获得奥运网络安保一等功臣。

“能作为安天对 G20 峰会安保支撑活动的成员之一很荣幸，不管峰会期间有多累，我觉得很值得”、“此次峰会保障任务的圆满完成，受到峰会安保组领导的高度肯定及表彰，这份荣誉不仅仅是获得奖章的同事，更多的是颁发给我们整个安天应急响应团队”安天技术专家崔宇楠、郝兴俊表示。

像 G20 这样国家级重大活动的网络安保工作，安天经常参与其中，多次在重大网络事故和网络安全事件的响应中发挥关键作用，参加了十七大、十八大、2010 年起的历届两会、北京奥运会、上海世博会、广州亚运会、2014 年 APEC 会议、抗战胜利 70 周年阅兵等重大活动的安保工作，并荣获重大活动信息安全保卫工作突出贡献奖。

在此次高规格要求的会议安全保障结束后在，安天受到多方上级单位的肯定和表扬。回望过去，安天与众多网络安全同行厂商共同打赢了 G20 峰会网络安保的大决战，留下了一个安全而美好的杭州西子湖畔 G20 形象；面向未来，安天将继续不断完善自身防御应急机制和技术能力，积极吸取安保期间的宝贵经验，为今后重要网络安保工作打下更坚实的基础。

安天实况转播国足世界杯预选赛

9 月 6 日，安天总部实况转播了中国男足国家队在 2018 年世界杯亚洲区预选赛十二强赛第二轮主场迎战伊朗队的比赛。哈尔滨后勤小伙伴们为大家准备了零食和饮料，让大家更好的观看精彩的比赛，为国足加油。突破梦想、创造奇迹！中国球迷准备好了，中国队，你永远不会独行！

Yandex 浏览器漏洞允许黑客窃取用户浏览器数据

近日，Albeniz 的研究报告指出，CSRF（跨站请求伪造）漏洞存在于 Yandex 浏览器中，CSRF 漏洞的使用手段极其简单，只需要让用户点击进入某个预先设置好的恶意网页，就可以触发漏洞。而这个网页需要包含一个用于创建 Yandex 浏览器数据同步功能的登录入口，以及提交数据时经由黑客的证书。

CSRF 漏洞会开启一个数据自动同步功能，将数据备份并发送给黑客一份。如果被攻击用户不能发现漏洞并加以处理，浏览器的数据同步功能，会持续将信息传输到黑客的账户之上。（来源：http://www.easyaq.com/newsdetail/id/1442219444.shtml）

每周安全事件

类 型	内 容
中文标题	Dropbox 2012 重大数据泄露影响了超过 6800 万用户
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，数据泄露索引网站 LeakedSource 报告称，俄罗斯的 Yahoo—Rambler.ru 2012 年遭受了大规模的数据泄露事件，未知黑客设法盗取近 1 亿用户记录。LeakedSource 声称从 Jabber ID 为 daykalif@xmpp.jp 的黑客处收到数据，这名黑客先前还向 LeakedSource 提供了音乐流服务网站 Last.fm 2012 被窃数据。 数据分析显示，每个用户条目包含 Rambler.ru 用户名、ICQ 号（IM 聊天工具）、密码字符串以及一些内部数据。LeakedSource 表示，密码字符串未经哈希加密，以明文储存在数据库内。这起数据泄露事件与 VK.com 类似，密码也已明文的方式储存，未经哈希或加盐处理。最常用的密码非常容易破解，这些密码包括 asdasd、123456、000000、654321、123321 或 123123。
链接地址	http://thehackernews.com/2016/09/russias-largest-portal-hacked-nearly.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 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.suoji.a[rog, sys]2016-09-05	该应程序伪装成腾讯游戏辅助工具，运行后会激活设备管理器，强制锁屏，后台会私自下载恶意应用，建议卸载。（威胁等级高）
		Trojan/Android.Twitoor.a[rmt, bkd]2016-09-07	该应用伪装，成其他应用，运行后会隐藏图标，后台定时访问指定 Twitter 账户，会从该账户中获取指令和下载信息，私自下载恶意应用，会伪装成系统更新推送，诱导用户点击安装。避免造成资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.Guve.a[rmt, prv, exp, sys]2016-09-07	该程序伪装成正常应用，运行后会发送注册短信，并联网获取指令，发送短信、下载安装指定应用、卸载指定应用。监听收件箱，拦截指定短信并上传，并发送订阅短信。避免造成资费损耗和隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.AF3Shell.a[exp, sms]2016-09-08	该应用程序安装后无图标，启动运行后会动态加载，由 /assets 目录下的数据文件解密得到的子包，连接恶意 url 下载数据，并依据从中解析得到的短信目标地址及短信内容发送短信，这类短信是扣费短信。会给用户造成资费损失及经济损害，建议立即卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.emial.dh[prv, exp]	该应用运行后会隐藏图标，获取用户短信和手机联系人信息并通过邮箱和短信转发。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）
		Trojan/Android.Downloader.ci[exp]	该应用程序植入在刷赞应用中，私自下载恶意 apk，后台会推广广告，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.SmsSend.kf[exp, sms]	该应用程序伪装成帮助本地用户连接登录指定网址的上网工具，会在用户不知情的情况下向指定号码发送苹果相关产品的预约订购短信，会解析用户短信，查看收信信息，会造成用户经济损失。建议立即卸载。（威胁等级高）
		Trojan/Android.Dendroid.e[prv, exp]	该应用程序安装后，会私自执行联网获取指令操作，根据指令内容进行本地恶意活动，如读取用户短信信息并上传至服务器，同时还将下载数据中的特定部分私自以短信发送。造成用户隐私泄露及资费损失，建议立即卸载。（威胁等级高）
		Trojan/Android.Downloader.ch[rog, exp]	该应用运行后会私自下载推广应用并静默安装，会造成用户资费损耗，建议卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Word 远程代码执行漏洞 (CVE-2015-0097) (MS15-022)	Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。Office 解析构造的 Office 文件时存在 Local Zone 相关错误，攻击者利用此漏洞可执行任意代码，破坏内存。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Shell.Gafgyt	此威胁是一类使用 shell 脚本编写的木马家族。该家族样本运行后会关闭 iptables 防火墙，使用 kill -9 及 killall 命令结束多个进程，并使用 busybox 下载恶意代码替换正常文件。（威胁等级中）
		Trojan[Dropper]/Win32.AceDeceiver	此威胁是一类可以释放恶意代码的木马家族。该家族样本由 AutoIt 脚本编写，运行后会释放 AutoIt 脚本执行工具及恶意脚本，会使用工具调用恶意脚本。（威胁等级中）
		Trojan[Ransom]/Win32.Zerber	此威胁是一类可以加密用户数据的木马家族。该家族样本是勒索软件，运行后会加密用户文件，并播放声音提示用户文件已被加密，勒索用户支付比特币解密。（威胁等级中）
		Trojan[Backdoor]/Win32.Qakbot	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，会连接远程服务器接受攻击者的恶意操作，包括文件管理，进程查看等。（威胁等级高）

共享私钥的设备数量大幅增加

Tom Spring / 文　安天公益翻译小组 / 译

近日，奥地利咨询公司 SEC Consult 的研究人员指出，自去年 11 月以来，共享密钥和证书的互联网网关、路由器、调制解调器和其他嵌入式设备的数量增加了 40%。

这份名为《密钥屋》的报告于近期发布。报告指出，使用已知 HTTPS 服务器证书和私钥的设备急剧增加，这很容易引发中间人攻击的增加，会导致更广泛的入侵。SEC Consult 指出，在过去的 9 个月中，这一数字已经从 320 万 (2015 年 11 月) 增加到今天的 450 万。

SEC Consult 高级安全顾问史蒂芬·维埃沃克在博客中写到：“这一趋势有很多原因。其中一个重要原因是，厂商无法为其产品的安全漏洞提供补丁，即使能够提供补丁，嵌入式系统也很少打补丁。”

SEC Consult 在去年末进行了初始研究，分析了 70 家厂商超过 4,000 台嵌入式设备，固件使用的公共 / 私人 SSH 密钥和和 X.509 证书。当时，研究人员说，近 600 个独特的私钥被多个设备共享。

SEC Consult 指出，近期发布的报告涵盖了 331 个证书，包括共享私钥和 553 个非共享私钥。再次检查证书和密钥之后，老问题得到了证实。Broadcom SDK “Daniel” 证书被 50 万台设备使用，Multitech/Texas Instruments 证书被 28 万台设备使用。

SEC Consult 发现了多个阿尔卡特 – 朗讯 OmniAccess 固件使用的，新的共享证书 / 私钥对。

维埃沃克表示：“与我们发现的其他大多数证书不同，该证书由浏览器信任的证书签发机构 (GeoTrust) 签名，签发给 securelogin.arubanetworks.com，有效期到 2017 年 8 月。事实证明，阿鲁巴网络公司 (Aruba Networks) 是阿尔卡特 – 朗讯 OmniAccess 产品线的代工厂。该证书是 ArubaOS 的一部分，也用于各种阿鲁巴产品。网络上的 49,000 台设备正在使用此证书。”

SEC Consult 表示，ArubaOS 证书是默认的 HTTPS 服务器证书和 WPA2–Enterprise 801.X 认证。维埃沃克写到：“这允许攻击者执行各种讨厌的中间人攻击 (主动 / 被动 HTTPS 解密，非法接入点等)。”

以设备制造商尤比奎蒂网络公司 (Ubiquity Networks) 为例，据报告，其使用不安全的 SSH 密钥和 HTTPS 证书的网络设备减少了 62%。维埃沃克指出：“减少的主要原因很可能是各种僵尸网络，它们利用弱效凭证和严重的漏洞，包括利用任意文件上传漏洞 (简单的远程执行代码，可用的 Metasploit 模块)。”

SEC Consult 指出，尤比奎蒂网络公司支持用户设备恶意软件删除论坛。维埃沃克写道：“这些僵尸网络可能迫使尤比奎蒂公司的客户为设备设置防火墙。”

在报告中，SEC Consult 指出，一些厂商意识到了该问题。维埃沃克引用了阿尔卡特 – 朗讯 OmniAccess 产品线的“安全人员”的博客：“过去，我们相信‘证书太复杂，就使用出厂默认证书，那些担心安全性的用户可以进行更新’的说法。但是现在，我认为我们给客户提供了上吊用的绳子。”

SEC Consult 提出的补救建议与 9 个月前一样。它建议设备制造商确保每台设备使用随机的，独特的加密密钥。它还建议互联网服务供应商，确保无法通过广域网端口远程访问通用平台 (Common Platform Enumerations)。最后，SEC Consult 建议最终用户为自己的设备更改 SSH 主机密钥和 X.509 证书。

维埃沃克写到：“我们不应该掉以轻心地发布私钥，因为这会使得全球攻击者大规模地利用此类漏洞。然而，我们认为任何意志坚定的攻击者可以做同样的研究，轻松获取公开固件的私钥。”

原文名称	Number of Devices Sharing Private Crypto Keys Up Sharply
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 9 月 6 日发布于《安全周报 (Threatpost)》 原文地址 https://threatpost.com/number-of-devices-sharing-private-crypto-keys-up-sharply/120379/
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《Rex Linux Trojan 样本分析报告》

近日，安天追影小组在整理网络安全事件时，针对 linux 平台下的命名为“Rex”的木马攻击事件进行了简要的分析。该样本为 linux 平台下的 elf 可执行文件，主要针对 linux 平台进行攻击，攻击者对木马样本进行了类型为 UPX3.9 的加壳保护，来躲避 linux 下的查杀手段。

“Rex”木马是典型的 linux 平台木马，攻击者利用常规的网络钓鱼技术进行木马病毒的传播。“Rex”木马在感染终端、自我复制、自我传播时会通过 CVE-2014-3704 Drupalgeddon 等漏洞，感染网络上 Drupal，Wordpress，和 Magento 等类型的网站，从而形成自己的 P2P 僵尸网络。

“Rex”木马样本主要模块为 CMS(Content Management System) 感染模块和僵尸网络攻击模块。CMS 感染模块主要针对防护较弱的网站进行 CVE 漏洞攻击，通过感染受害者的电脑，在其网站服务器上会创建一个管理员账户，用来控制 CMS。对于不同的 CMS，“Rex”木马的处理方式也较为不同。针对 Drupal CMS 时，该木马通过锁定网站的页面来进行勒索行为；针对 Wordpress CMS 时，该木马会利用 CMS 插件进行传播，并不会锁定网站和勒索赎金，只是运行恶意代码的其他功能部分；而针对 Magento CMS 时，采用 RCE 窃取漏洞攻击来进行数据库的管理员创建和感染 web 服务器。

僵尸网络攻击模块主要的攻击方式分为：针对攻击者指定目标进行常规的 DDoS 攻击、垃圾邮件轰炸式攻击、对感染主机比特币的挖矿行为、对感染 CMS 篡改网页的勒索行为，并且该木马还可以通过 BitTorrent 的 DHT 协议来进行攻击模块的二次开发和更新，攻击方式扩展性较灵活。

通过对“Rex”木马样本分析，可以看出 P2P 僵尸网络的自建过程的隐秘性，攻击手段的多样性。安天建议网站管理员，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，防止恶意代码通过钓鱼邮件或其他手段的攻击来进行感染和自我繁殖。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、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：自复制、Drupalgeddon SQL 注入攻击模块、DDoS。

文件名	1D09000F9C7AF81D6EB8E5D4D7C5F139
文件类型	BinExecute/Linux.ELF
大小	7.69 MB
MD5	1D09000F9C7AF81D6EB8E5D4D7C5F139
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.SGeneric
判定依据	智能学习

运行环境

操作系统	内置软件
中标麒麟	默认

危险行为

行为描述	危险等级	行为描述	危险等级
自复制	★★★★★	Drupalgeddon SQL 注入攻击模块	★★★★★
DDoS	★★★★★		

EXIF 信息

描述	值
File Size	7.7 MB
File Type	ELF executable
MIME Type	application/octet-stream
CPU Architecture	32 bit
CPU Byte Order	Little endian
Object File Type	Executable file
CPU Type	i386

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=1D09000F9C7AF81D6EB8E5D4D7C5F139