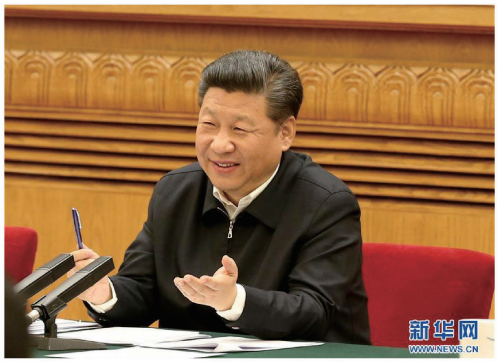
安天周观察

主办：安天　2016 年 4 月 25 日（总第 37 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

习近平总书记主持召开网络安全和信息化工作座谈会　安天技术负责人受邀参加并发言

4 月 19 日，中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平在北京主持召开了网络安全和信息化工作座谈会并发表重要讲话。中央网络安全和信息化领导小组成员，中央和国家机关有关部门负责同志，部分省市党委宣传部部长，各省区市网信办主任，部分中央新闻单位和中央新闻网站负责同志，有关专家学者，部分网信企业负责人等参加了本次座谈会。

座谈会上，来自不同领域的 10 位代表进行了发言。安天



技术负责人作为网络安全领域的代表第二个发言。一同发言的各界代表还有，中国工程院院士、中国电子科技集团公司总工程师吴曼青，阿里巴巴集团董事局主席马云，友友天宇系统技术有限公司首席执行官姚宏宇，解放军驻京某研究所研究员杨林，北京大学新媒体研究院院长谢新洲，北京市委网信办主任佟力强，华为技术有限公司总裁任正非，国家计算机网络与信息安全管理中心主任黄澄清，复旦大学网络空间治理研究中心副主任沈逸。

在听取发言后，习近平现场向发言代表提问，并在会后与他们亲切握手。习近平表示，几位同志讲的很好，分析了当前互联网发展新情况新动向，介绍了信息化发展新技术新趋势，提出了很好的意见和建议，体现了在互联网领域较高的理论和实践水平，对改进工作很有帮助。

习近平总书记与安天技术负责人亲切握手

安天参加全球领先安全技术分享会并发表演讲

近日，“数据力量——全球领先安全技术分享会”在北京召开，参会嘉宾就安全产业发展趋势，安全防护技术的发展与变革进行了深入的交流。安天移动安全团队负责人潘宣辰发表了题为《威胁情报背后的较量的思考》的演讲，主要分享了移动威胁情报在实践中的经验，引出中国和北美威胁情报厂商整体的定位和差异，并重点分享了，如何利用好安全厂商的基础设施，将其转化为威胁情报能力的方法。

近年来，在威胁情报逐步成为网络安全业界热点的背景下，安天率先选择在移动威胁情报领域发力，通过 AVL SDK 反病毒引擎移动版形成的终端覆盖能力，形成了全球最早的移动安全威胁情报体系。目前，安天将推出新的移动威胁情报平台 AVL Insight，主要用于呈现移动威胁的高价值情报信息，同时通过对移动威胁的全面感知能力和快速分析响应能力，提供应对移动威胁的预警和处置策略。

安天各地学习贯彻习近平总书记在网络安全和信息化工作座谈会上重要讲话

4 月 19 日，习近平总书记在北京主持召开网络安全和信息化工作座谈会并发表重要讲话。作为一家网络安全厂商，安天随即组织哈尔滨、北京、武汉、深圳四地公司对会议精神进行了学习和讨论。

通过逐条梳理习近平总书记在网络安全和信息化工作座谈会上的重要讲话，安天充分认识到网络空间治理的重要性和全局性。可以说习总书记挖掘了网络安全攻防博弈矛盾中的普遍联系和辩证统一，提出了网络安全的辩证法。习总书记特别强调了发展防御技术和威慑技术，在防御重点方面，特别强调“关键信息基础设施”是安全防护重点，同时强调了要全天候全方位感知网络安全态势。这些都为我们未来的工作指出了方向。

安天在今后的工作中必将全面遵守会议精神，将其运用到实际工作中，充分发挥安全厂商的责任，营造健康和谐有序的网络空间。

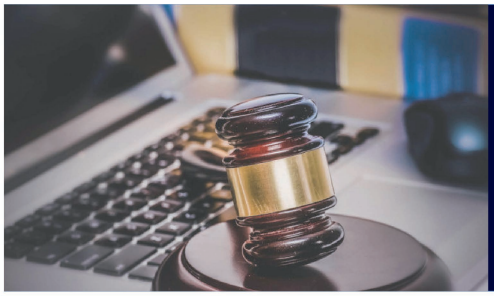
每周安全事件

类 型	内 容
中文标题	C99 php webshell 攻击加剧，大量 WordPress 站点遭受威胁
英文标题	WordPress Sites Targeted with New Attacks Using C99 PHP Webshell
作者及单位	Catalin Cimpanu；SOFTPEDIA
内容概述	近日，安全研究人员监测到 C99 php webshell 的攻击加剧，大量 WordPress 站点遭受威胁。攻击者利用站点插件的安全漏洞，通过 C99 webshell 进行感染，在最初感染的阶段，webshell 脚本被上传到服务器，并以一个文本文件存放于服务器上，通常情况下该文本文件名为 pagat.txt。基于目前的情况，安全研究人员建议使用开源扫描工具，对上传文件进行全量扫描。如果发现站点已经被感染了，需要及时变更站点的所有管理账户密码，并告知站点用户进行密码变更。
链接地址	http://news.softpedia.com/news/wordpress-sites-targeted-with-new-attacks-using-c99-php-webshell-502998.shtml

每周值得关注的恶意代码信息

经安天检测分析，本周 10 个移动平台和 4 个 PC 平台的恶意代码家族值得关注

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.lacoonbypass.a[prv] 2016-04-18	该应用无实际功能，程序运行后会获取用户联系人信息和短信信息上传到远程服务器，造成用户隐私泄露。（威胁等级低）
		Trojan/Android.impei.a[exp，prv] 2016-04-18	该应用伪装成系统应用无实际功能，运行后私自上传用户固件、位置、sim 卡等相关隐私信息，下载静默安装未知文件，建议立即卸载，避免造成隐私泄露及资费损耗。（威胁等级中）
		Trojan/Android.SmsPrv.a[prv，spy] 2016-04-18	该应用是一款间谍软件，运行后私自发送短信，设置上传号码后隐藏图标，根据短信指令窃取用户短信信息、通讯记录、位置信息、google 账号信息等，造成用户隐私泄露，建议谨慎使用。（威胁等级中）
		Trojan/Android.srvspy.a[prv，exp，spy] 2016-04-19	该应用安装无图标，运行后接收短信指令，获取 wifi、gps、存储空间大小、手机固件等相关信息并短信转发，控制 wifi 开关、开启录音、拍照、录像等功能；监听通话、获取用户通话记录并设置通话录音，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.FakeKRB.a[prv，sys，rog]2016-04-20	该程序伪装成正常应用，无实际功能，运行后隐藏图标，诱导激活设备管理器，后台检测杀软信息，关闭其他程序窗口界面，上传已安装程序包名信息至指定服务器，拦截短信执行屏蔽、转发、删除操作，造成用户隐私泄露和资费消耗，建议及时卸载该程序。（威胁等级高）
		Trojan/Android.wizard.a[prv，exp] 2016-04-20	该程序伪装成注册应用，运行后诱导用户输入电子邮箱、姓名等隐私信息，随后隐藏图标，并通过邮箱转发，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.kefremote.a[prv，fra，exp]2016-04-22	该程序伪装成正常应用，运行后无实际功能，后台获取用户手机固件信息、系统账号信息、地理位置信息并通过多个邮箱转发，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.xmpp.a[prv，exp] 2016-04-22	该应用开机自启动，要求激活设备管理器后隐藏图标。上传用户短信息、联系人信息、已安装的安全软件信息，根据返回的数据发送特定的短信。造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.FakeBank.l[prv，fra]	该应用伪装成招商银行贷款申请应用，运行后诱导用户输入身份证、银行卡号和密码等隐私信息并上传到云端，同时会拦截短信并上传，造成用户隐私泄露，可能会造成用户财产损失，建议卸载。（威胁等级高）
		G-Ware/Android.jianmo.y[rog，sys]	该程序伪装成正常应用，强制置顶界面，勒索用户添加指定 QQ 号，付费解锁手机，会造成用户资费损失，建议不要安装。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 未初始化内存使用漏洞 CVE-2015-1770	该漏洞可能在用户打开经特殊设计的 Microsoft Office 文件时允许远程执行代码。成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响会更小。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Small	此威胁是一种木马类程序，一般会伪装成正常文件欺骗用户下载或者通过一些恶意网页的辅助，通过浏览器和插件的漏洞被安装到用户的系统中。也有些变种由其他恶意软件释放或下载得到。（威胁等级中）
		Trojan[Backdoor]/Win32.DDOS	此威胁是一种后门类木马程序，运行后创建服务，通过 CMD 隐藏删除自身，连接控制端等待攻击指令。（威胁等级高）
		GrayWare[AdWare]/WinLNK.Clicker	此威胁是一种灰色软件类广告程序，可以弹出大量广告信息，并在被感染的计算机上下载其他病毒，侦听黑客指令，连接指定站点，弹出大量广告条幅，用户一旦点击带毒广告，会立即在用户计算机上安装其他病毒。（威胁等级中）



苹果和 FBI 听证会对决

Tom Spring/ 文　安天公益翻译小组 / 译

近日，在众议院能源和商务委员会听证会上，苹果和 FBI(美国联邦调查局) 的代表对正在进行的加密之争进行作证。双方承诺协同工作，以解决当前的加密僵局，找到共同立场。他们希望在听证会上澄清加密立场，弄清楚 FBI 使用“灰帽子”黑客的情况和苹果公司与中国的联系。

在听证会上，苹果总法律顾问布鲁斯·休厄尔 (Bruce Sewell) 清楚地表示，中国曾要求苹果交出 iPhone 源代码，但是苹果拒绝了这一要求。休厄尔在听证会上表示，相对于与美国执法机构合作进行犯罪调查，苹果对与中国的良好业务关系更感兴趣。

休厄尔说：“我希望很清楚地说明这一点。我们没有给中国政府提供源代码，这些指控没有任何依据。”

就雇用第三方黑客破解圣贝纳迪诺恐怖分子之一赛义德·法鲁克的 iPhone 手机一事，FBI 科技局执行副局长艾米·赫斯 (Amy Hess) 进行了辩护。她说，与以营利为目的的黑客合作并不是一个理想的情况，但是 FBI 确实无法自行破解该 iPhone 手机。

之前，一名联邦法官下令苹果公司向 FBI 提供“合理的技术援助”，帮助 FBI 破解法鲁克的 iPhone 手机，绕过手机的保护机制 (如果输入太多次不正确的密码，手机上的数据就会被擦除)。在这种情况下，苹果和 FBI 举行了该听证会。但是由于 FBI 雇用了秘密的第三方解锁手机，该会议被延迟了。

在庭审过程中，赫斯指出，联邦调查局“所需的服务和专业技能只能通过第三方获得”。就 FBI 无法自行破解手机一事，陪审团对赫斯进行了盘问。

“我不认为依靠第三方是一个好模式”，科罗拉多州民主党众议员戴安娜·德凯特 (Diana DeGette) 说。赫斯承认，FBI 需要更多的资源来开发更先进的计算机取证工具，并雇用更多的专家型人才。

苹果公司的休厄尔还谈到了执法机构的指控：苹果将会对新一代 iCloud 使用与 iPhone 相同的强加密技术。“我们还没有宣布这一点，实际上，我们会对新一代 iCloud 使用密码加密。”他说。

休厄尔和科技部门的其他代表强调了加密立场，他们指出，开设后门或有意的弱加密会对美国企业带来灾难性的影响，而且无法防止到美国境外寻求加密解决方案的犯罪分子。

议员们承认，加密并不是简单的黑或白的问题。但是，在听证会快要结束时，就政府是否应该具有依法访问加密技术和通信的能力这一问题，众议院能源和商务委员会也没有找到答案。

该委员会的主席蒂姆·墨菲 (Tim Murphy) 说：“在过去五年半的时间里，我总是听到大家谈论加密，但是没有做成任何实事。我不知道我们在等什么，我们必须找到一个解决方案。”

休厄尔指出，在过去的五年中，私营部门和执法部门的合作已经取得了很大的进步，以帮助执法部门调查涉及到加密的刑事案件。“如果我们能够摆脱官司，我们可以更多地合作。”休厄尔说。

休厄尔说，强加密和执法并不矛盾。他表示，苹果每日都与执法机关合作，帮助找到被绑架的儿童和儿童绑架者。一些工具 (如 IP 日志) 能够帮助定位失踪者，一个名为 PhotoDNA 的计划能够在线追踪儿童色情。这些例子说明，追捕犯罪分子与加密数据的关系不大，与利用技术破案的关系更大。

原文名称	Apple and FBI Faceoff at House Encryption Hearing
作者简介	Tom Spring，Threatpost 的副主编。
原文信息	2016 年 4 月 19 日《Threatpost》发布 原文地址 https://threatpost.com/apple-and-fbi-faceoff-at-house-encryption-hearing/117518/
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《大灰狼远控利用 QQ 号上线》报告

“大灰狼”远控是一款不断更新、升级的远控，安天追影小组曾经对“大灰狼”样本进行分析，《安天周观察》曾在第 22 期和第 29 期，分别发布《大灰狼远控分析》报告和《大灰狼远控变形 DNS 分析》报告，提及其具有连接到某个 QQ 号空间，通过该 QQ 号上线的行为。近期，研究人员再次披露“大灰狼”远控的另一个匿名上线漏洞，安天追影小组随即进行了分析。

该样本具有释放 PE 文件到系统目录、自复制为常见系统进程名、自删除、修改注册表、设置自启动、通过 CMD 隐藏删除自身、创建可疑进程、设置调试器权限、检查摄像头、连接网络和查找杀毒软件相关进程等行为。经追影小组分析发现，连接控制端下载的文件与之前分析的相符，同样名为“NetSyst**.dll”（** 为两位随机数字）。

样本行为：

1. 样本首先下载“NetSyst96.dll”到 APPPatch 中。

2. 自我复制到系统目录下，并以子进程的方式打开，监测和监视新硬件设备并自动更新设备驱动。

3. 通过访问“982471559”这一 QQ 号来上线，在本样本分析过程中，研究人员猜测该 QQ 号的昵称已改变，不再有效。

除了本次分析的样本，追影小组在对其他威胁事件进行情报收集的过程中，曾捕获到大量以 QQ 昵称作为上线昵称的样本，一旦访问成功，恶意软件会获取到上线 IP，受害主机将受到黑客的远程控制。

“大灰狼”远控有着较长的历史，且有专人负责开发维护，更新迭代较快。其特色为通过 QQ 昵称找到上线地址，这样的方式有利于快速更新 C2，且对避免杀毒软件的查杀有一定的作用，而“免杀”也正是其吸引用户的一个方式。为了避免被此类远控攻击，安天追影小组提醒广大用户加强安全意识，不要随意打开陌生链接，通过官方网站下载正版软件。

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 BD 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：

自复制为常见系统进程名、设置调试器权限、连接特殊 URL、文件下载、填充导入表（疑似壳）、释放 PE 文件、获取系统版本、获取计算机名称、获取 socket 本地名称、连接网络、创建特定窗体、获取驱动器类型、打开自身进程文件、获取主机用户名称、查找指定内核模块、请求加载驱动的权限。

文件名	C1B87D23115E3868E0CA604949B684EA
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	120 KB
MD5	C1B87D23115E3868E0CA604949B684EA
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Win32.Zegost.Q
判定依据	BD 静态分析

◆ 危险行为

行为描述	危险等级
自复制为常见系统进程名	★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
设置调试器权限	★	连接特殊 URL	★
文件下载	★	填充导入表（疑似壳）	★★
释放 PE 文件	★	获取系统版本	★★
获取计算机名称	★	获取 socket 本地名称	★
连接网络	★	创建特定窗体	★
打开自身进程文件	★	获取驱动器类型	★
请求加载驱动的权限	★	获取主机用户名称	★
查找指定内核模块	★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=C1B87D23115E3868E0CA604949B684EA