安天周观察

主办：安天　2015 年 12 月 28 日 (总第 22 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天荣获 CNVD“漏洞报送突出贡献单位”荣誉称号

2015 年 12 月 23 日，由国家计算机网络应急技术处理协调中心 (CNCERT)、中国互联网协会网络与信息安全工作委员会联合主办的国家信息安全漏洞共享平台 (CNVD)2015 年工作会议在京召开。

工业和信息化部网络安全管理局刘伯超处长为会议致辞，他指出随着互联网的迅速发展和普及，网络安全事件日益增多，其中，信息系统存在的高危漏洞已经成为已发网络安全事件的重要因素。他希望广大企业，特别是参与签订《中国互联网协会漏洞信息披露和处置自律公约》的企业，能按照公约要求加强行业自律，更好地发挥重要作用。

随后，中国互联网协会网络与信息安全工作委员会秘书长何世平对 2015 年度 CNVD 工作进行了总结。截止目前为止，CNVD 共收录漏洞信息 9.7 万条，事件型漏洞 4.8 万条。其中，安天公开漏洞报送数量共 6647 条。

在会上，安天、绿盟、启明星辰、天融信、奇虎 360、等 8 家公司因在漏洞信息的发现和报送等方面表现突出，被授予“漏洞报送突出贡献单位”称号；北京信息安全测评中心、中国电信、中国移动、知道创宇等 8 家单位荣获“漏洞处置突出贡献单位”称号。

做好网络信息管理和应对网络风险是一项需要脚踏实地、长期坚持的工作。安天始终专注威胁检测领域，提供先进的威胁检测能力，在漏洞检测响应领域中，安天重点监测可以被用于恶意代码传播、木马植入等相关漏洞的分布和被利用情况；对可以用于 APT 攻击的格式文档等漏洞类型，进行深度分析，完善针对未知漏洞的静态格式分析和动态沙箱检测能力。曾对破壳 (ShellShock)、沙虫 (CVE-2014-4114) 等多个严重漏洞以及依托其展开的攻击，进行持续深度分析，分析结果获得业内好评。

安天举办圣诞雪雕大赛

12 月 21 日 -25 日，安天哈尔滨总部举办了一场圣诞雪雕大赛，比赛采取部门联合方式，分为六个小组。参赛选手们不畏寒冬，发挥奇思妙想，几天时间，打造出“哆啦 A 梦、小黄人、安天创意优盘”等 6 座造型新颖的雪雕，引得路人纷纷驻足赞叹、拍照分享。

Linux 开机漏洞：连按 28 下 Backspace 可入侵系统

近日，研究人员在 Linux 开机管理程序 Grub2 中，发现一项整数下溢漏洞，编号 CVE-2015-8370。通过该漏洞成功入侵的黑客可进入 GRUB 的 RescueShell，进而提升权限、复制磁盘信息、安装 RootKit 或是摧毁包括 GRUB 在内的任何资料，即使磁盘加密也可能遭到覆写，导致系统无法工作。研究人员发现该漏洞的攻击方法相当简单：只需在 GRUB 要求输入用户名时，连续按 28 次倒退键，就可进入 RescueShell。按照此方法操作，若看到系统重启，或是进入救援模式，即可判端系统有此漏洞。(文章来源：http://www.cnbeta.com/articles/459263.htm)

安天举办 2015 年 12 月『工程师月会』

12 月 25 日，安天哈尔滨总部举办了 12 月份工程师月会。本次工程师月会，特别邀请了国防科技大学副教授温百华发表了题为《美国国家安全局 / 网络司令部信号情报 / 网络攻防作战》的演讲，对军事作战视角下的斯诺登文件体系化解读。高级研究员，赵超发表了《安全威胁情报综述》，介绍了安全威胁情报的由来、定义、作用，对国内外相关安全企业、规范标准、平台、联盟的发展现状进行介绍和分析，对威胁情报的发展趋势和存在问题进行了总结。除特邀嘉宾外，安天信息开发管理组、海外业务中心组等负责人分别就《如何建立工作流程》、《多出入口工作管理初探》等主题分享了个人的工作经验。

每周安全事件

类 型	内 容
中文标题	Microsoft Outlook 曝严重漏洞，可进行“邮件炸弹”攻击
英文标题	Microsoft Outlook flaw opens the door to “mailbomb” attacks
作者及单位	Pierluigi Paganini，Security Affairs
内容概述	近期，微软发布了一系列补丁，修复了自身产品中一些影响广泛以及关键的 Bug，包括更新微软 Office 套件版本，解决其中的部分安全问题。其中威胁级别最高的漏洞，可允许远程代码执行。如果用户打开一个专门制作的微软办公文件，攻击者可以利用该漏洞在当前用户目录下运行任意代码。而具有较小权限的用户帐户受到的影响可能会比拥有管理员权限的用户所受影响要小得多。目前，该漏洞主要影响范围涉及到 Outlook 2007/2010/2013/2016 等版本。
链接地址	http://securityaffairs.co/wordpress/42875/security/microsoft-outlook-mailbomb-attacks.html

每周值得关注的恶意代码信息

经安天检测分析，本周 9 个移动平台和 5 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.Yzmg.a[prv，exp] 2015-12-21	该应用程序安装无图标，伪装成系统应用，运行后会获取手机固件信息、安装程序信息和 QQ 号码及微信聊天记录文件大小等信息上传，造成用户隐私泄露，建议卸载。(威胁等级高)
		Trojan/Android.E4ACallLogspy.a [prv]2015-12-22	该应用程序在应用中设置按钮，用户点击后将通话记录发送至指定手机号码，建议用户谨慎使用。(威胁等级中)
		Trojan/Android.kjw.a[pay] 2015-12-23	该应用程序运行后隐藏图标，后台下载 jar 文件，动态加载并上传手机号、IMEI 等设备信息、发送 sp 扣费短信、拦截短信，建议立即卸载该软件，以免造成流量耗损和资费扣取。(威胁等级中)
		Trojan/Android.puremdm.a [prv，sys] 2015-12-24	该应用运行后请求激活设备管理器，强制锁屏；后台获取用户短信记录、通话记录、手机固件信息和程序列表信息并上传；私自发送短信反馈程序运行结果；私自下载安装未知 apk 应用，造成用户隐私泄露、资费损耗和影响手机正常使用；还包含清除用户手机 sd 卡等风险代码，建议卸载。(威胁等级高)
	较为活跃的样本	Trojan/Android.Maincheck.a [exp，sys]	该应用伪装成谷歌相关应用，运行后隐藏图标，获取手机固件信息和 root 结果上传，并下载未知 apk 文件静默安装，建议用户谨慎使用。(威胁等级中)
		Trojan/Android.Downloader.az [exp]	该应用程序安装无图标，后台联网下载或安装未知文件，为了避免造成用户资费损耗，建议卸载。(威胁等级高)
		Trojan/Android.PermAd.c [exp，sys]	该应用程序运行后，在后台联网下载未知文件，通过提权静默安装，可能会造成资费损耗，建议卸载。(威胁等级中)
		Trojan/Android.E4Aspy.v [prv，rmt]	该应用伪装成正常应用，运行后无任何实际功能，可被远端控制手机发送短信，窃取用户短信、联系人等信息，建议用户立即卸载。(威胁等级中)
		G-Ware/Android.Fakegupdt.ai [exp，rog]	该应用程序伪装成系统应用，安装无图标，运行后诱导激活设备管理器防卸载，并且存在下载未知文件的行为，建议用户卸载，避免造成资费损耗。(威胁等级低)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 远程代码执行漏洞 (CVE-2012-1535)	Adobe Flash Player 是一个集成的多媒体播放器。Windows 和 Mac OS X 平台上 Adobe Flash Player 11.3.300.271 之前版本，Linux 平台上 11.2.202.238 之前版本，在实现上存在不明细节漏洞，可允许远程攻击者通过 SWF 内容执行任意代码或造成拒绝服务。(威胁等级高)
	较为活跃样本	Trojan[Backdoor]/Win32.Small.dhl	此威胁是一种后门木马类程序，它可以连接远程服务器接受攻击者恶意操作，包括下载与更新其它恶意代码、添加删除系统文件、窃取用户敏感信息等。(威胁等级中)
		Trojan[Dropper]/Win32.Injector.hxbu	此威胁是一种木马类程序。用于对指定文件或程序注入代码或线程的黑客工具软件。对于系统一般没有主动破坏能力，主要配合其他恶意程序进行入侵活动。(威胁等级中)
		Trojan/Win32.Qhost.lfs	此威胁是一种木马类程序，改变 Host 文件内容以屏蔽某些网站的木马类程序。该家族能够通过专门用于改变 Host 文件的黑客服务器来重定向细节，从而实现对密码信息的窃取。(威胁等级中)
		Trojan[Downloader]/Win32.VB.hbou	此威胁是一种具有下载行为的木马类程序，是以 VB 语言开发的，会在系统启动时自动运行。通常是从网页中下载或是捆绑正常程序。这种类型的恶意代码通常会在用户访问具有漏洞的网站时感染计算机。(威胁等级中)

Juniper 防火墙秘密代码显示出政府后门风险

Kim Zetter/ 文　　安天公益翻译小组 / 译

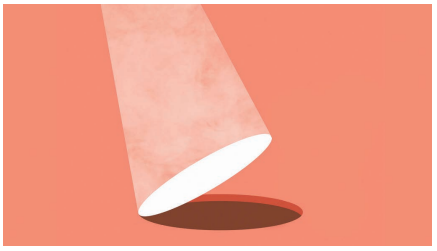
在过去几年中，加密后门一直是热议的话题。在巴黎和圣贝纳迪诺的恐怖袭击事件之后，该话题更是占据了媒体头条，变得更加炙手可热。但是没人发现，3 年前就已经有人悄悄在用来保护世界各地的企业和政府系统的网络设备的核心部分安装了后门。

近日，科技巨头 Juniper Networks(瞻博网络公司) 在一份令人震惊的声明中透露，他们已经找到了嵌入在其一些防火墙的操作系统中的“未授权”代码。该代码貌似存在于该公司多个版本的 ScreenOS 软件中，至少可以追溯到 2012 年 8 月，它允许攻击者完全控制运行受感染软件的 Juniper NetScreen 防火墙。它也允许攻击者分别解密通过 VPN(虚拟专用网络) 的加密流量。目前 Juniper 发布了软件补丁，建议客户立即安装，并指出了受影响的版本：ScreenOS 6.2.0r15，6.2.0r18，6.3.0r12 和 6.3.0r20。

安全社区特别震惊，因为至少一个后门似乎是成熟的国家攻击者的杰作。“VPN 本身的缺点 (允许被动解密) 只会对国家监控机构带来好处，如英国、美国、中国或以色列。”国际计算机科学研究所和加州大学伯克利分校的研究人员尼古拉斯·韦弗说。“对软件做出有价值的更改的前提是，你需要窃听互联网。”

但是后门也值得关注。如果攻击者通过检查 Juniper 的代码破解了密码，那么其中一个后门 (攻击者留在 Juniper 软件中的硬编码的主密码) 将允许任何人控制管理员尚未修复的 Juniper 防火墙。荷兰安全公司 Fox-IT 创始人兼首席技术官罗纳德·普林斯说，Juniper 发布的补丁提示了主密码后门在软件中的位置。通过逆向工程 Juniper 防火墙的固件，该公司的分析人员在短短 6 小时内就找到了密码。他告诉《连线杂志》，“现在，我们能够采用攻击者 (安装后门) 的方式，登录到所有漏洞防火墙。”

但是，普林斯说，Juniper 的公告和补丁引发了而另一个担忧：除了安装后门、拦截并存储通过 Juniper 防火墙的加密 VPN 流量的元凶，现在，其他任何国家攻击者都可能分析补丁并找出解密密码，从而进行解密。“如果其他国家行为者拦截经过这些 VPN 设备的 VPN 流量，他们就可以回顾历史流量，并解密此类流量。”他说。



韦弗说，这取决于 VPN 后门的确切性质。“如果类似于 Dual EC，那么你根本无法进入，你还需要知道密码。但是，如果类似于创建一个弱密钥，那么任何截获了所有流量的人都能够进行解密。”Dual EC 是一种加密算法，人们认为，NSA(美国国家安全局) 在其中植入了后门，使之变得更弱。这一因素加之获得密钥，NSA 就能够破解算法。

宾夕法尼亚大学的加密研究员和教授马特·布雷泽赞同这种说法，解密已收集的 Juniper VPN 流量的能力取决于某些因素，但是他给出了一个不同的原因。“如果 VPN 后门不要求你先用其他的远程访问 [密码] 后门”，那么将有可能解密已收集的历史流量，他说，“但我能想象设计一个后门，我必须使用远程访问后门登录，以启用允许我解密截获的流量的后门。”Juniper 网站的一个页面也似乎表明，它在一些产品中使用弱 Dual EC 算法，虽然约翰霍普金斯大学的密码学教授马修·格林说，目前还不清楚这是否是 Juniper 防火墙 VPN 问题的根源。

Juniper 发布了关于该问题的两条声明。在第二个更具技术性的声明中，该公司指出了软件中的两套未经授权的代码，它们创建了彼此独立工作的两个后门，这说明密码后门和 VPN 后门没有关系。Juniper 发言人拒绝回答声明之外的问题。

不管 VPN 后门的确切性质如何，这一最新事件恰恰说明了为何各公司 (如苹果和谷歌) 的安全专家反对在设备和软件中安装加密后门，允许美国政府访问受保护的通信。

“这是一个很好的例证。为何说政府不应该在这些类型的设备中安装后门。因为在某些时候这会适得其反。”普林斯说。

原文名称	Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors
作者简介	Kim Zetter，《连线杂志》一位屡获殊荣的资深记者，研究范围包括网络犯罪、隐私和安全。
原文信息	2015 年 12 月 18 日《连线杂志》 原文地址 http://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/
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《大灰狼远控分析》报告

近日，安天追影小组利用探海威胁检测系统 (PTD) 发现国内某电商平台被放置远控木马的核心组件。经分析确认该电商平台为广西一家本土购物平台，三宇微易购 (www.sywyg.com)。该网站属于广西贺州市三宇通信设备有限公司，同时其还开设多家线下服务站。追影小组对木马进行深入分析，发现该木马是大灰狼远程控制木马，其控制域名为 40424064.f3322.net，支持 QQ 上线功能，包含很多典型的黑客后门特征。

研究人员在分析过程中发现，样本运行后首先会判断自身命令行中是否含有 Win7 字符串，查看自身判断是否需要先进行网络文件捆绑下载运行。随后下载 dll 控件到 Windows 系统目录下的 AppPatch 目录下，文件名为 mysqld.dll。样本会对下载的控件进行校验，在文件结尾部分搜索 SSSSSSVID 字符串。通过校验后，样本就对控件进行解密，把解密后的 dll 控件动态加载进内存，调用其导出的函数，使程序流程就进入 dll。在 dll 里，首先会把原样本复制到 \Program Files\Microsoft Woknzj 目录下，文件名为 Ikkeqag，然后注册为服务启动项。注册成功后就会启动服务，使程序运行，在 C 盘目录下生成 VBS 脚本来自删除。在原始样本退出并自删除后，以服务方式启动的进程会开始执行主要功能。同样的，在其动态解密并加载控件后，进入控件导出函数，为了防止被删除，样本会打开 System 进程并复制句柄，解密出需要连接的上线域名。为了获取域名对应的 IP，除了使用微软标准 API 外，还会去一些网站查询 IP。然后会连接此域名的 1227 端口，连接成功后就开始准备接收远程指令并执行了。

通过进一步分析可以确定，该远程控制工具可以读取受害机器的磁盘、文件、音频录音，键盘记录，窃取用户的输入，包括账号密码等信息。还可以添加用户开启更多的后门，进行屏幕截取窥视用户隐私。除了远程控制功能外还具有 9 种 DDoS 功能。放置在三宇微易购网站的 DLL 文件是远控核心组件，通过加密方式保存，主要目的是把木马的核心功能与加载程序分离，这样可以躲避反病毒检查。

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、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、静态分析鉴定器、动态行为鉴定器将文件判定为木马程序。

该文件具有以下行为：删除自身；请求调试权限；检查摄像头；连接特殊 URL；扫描驱动器类型；获取 CPU 信息；填充导入表 (疑似壳)；释放 PE 文件；获取系统内存；获取系统版本；访问文件尾部；打开自身进程文件；获取 socket 本地名称；在根目录创建可执行脚本；访问 DNS；复制自身文件；创建服务；连接网络；创建特定窗体；获取驱动器类型；独占打开文件；遍历进程；启动服务；获取主机用户名称；查找指定内核模块；获取计算机名称；请求加载驱动的权限；下载文件。

文件名	B0EB375F545594DC2D8038D1BE4DD258
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	52 KB
MD5	B0EB375F545594DC2D8038D1BE4DD258
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor:HEUR]/Win32.AGeneric
判定依据	静态行为

◆ 危险行为

行为描述	危险等级
删除自身	★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
请求调试权限	★	检查摄像头	★★
连接特殊 URL	★	扫描驱动器类型	★★
填充导入表 (疑似壳)	★★	获取 CPU 信息	★★
获取系统内存	★★	释放 PE 文件	★
访问文件尾部	★	获取系统版本	★★
获取 socket 本地名称	★	打开自身进程文件	★
访问 DNS	★	在根目录创建可执行脚本	★★
连接网络	★	复制自身文件	★★
创建服务	★	创建特定窗体	★
独占打开文件	★	获取驱动器类型	★
遍历进程	★	启动服务	★
获取主机用户名称	★	查找指定内核模块	★
获取计算机名称	★	请求加载驱动的权限	★
下载文件	★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=B0EB375F545594DC2D8038D1BE4DD258