安天周观察

主办：安天　2016 年 11 月 21 日（总第 65 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天受邀做客黑龙江电视台《建龙经济论坛》

11 月 20 日，由黑龙江省委宣传部、省政府办公厅、省科顾委主办，黑龙江日报报业集团、东北网协办，黑龙江广播电视台等承办的主题为“推动民营经济大发展”的 2016 年第 3 期（总第 28 期）黑龙江建龙经济论坛在黑龙江省电视台举行。本期论坛贯彻落实全省加快民营经济发展工作会议精神，探讨黑龙江省民营经济振兴发展之路。

安天哈尔滨总部负责人李岱作为受邀嘉宾做客本期论坛，论坛还邀请了国家发改委学术委员会秘书长张燕生、省科顾委副主任刘世佳、省社科院应用经济研究所所长刘小宁、香坊区区委副书记、代区长栾志成、大庆市政府服务中心副主任张海军、福瑞邦药业集团副总经理刘云城等省内著名专家学者以及从事本土特色企业实干家做客现场，共话推动民营经济大发展战略。

李岱介绍说，现在很多企业和安天一样在发展过程中面临人才流失的问题：“我们主要采取校园招聘，自主培养的模式让企业的人才趋于稳定。但是由于这几年行业发展快速，我们无法提供像百度、阿里巴巴、腾讯、360 等互联网高企一样的待遇，所以人才流失的现象还是有的。由于只凭借黑龙江的人才吸纳是比较困难的，所以我们在北京、武汉、深圳、上海都设有分公司，这是为人才做了一个保障。他们在一线城市工作和发展其实和我们是紧密相关的，这是人才方面的解决办法。”

其次是资金的问题，由于网络安全行业的敏感度，公司在发展的前十年没有任何的风险投资。因为我们基本上是靠自主研发，所以我们不接受有外资背景的，不接受近几年的互联网厂商影响到公司未来的独立发展方向。公司所有的资本积累都用在扩大团队规模、购置设备、改善研发条件等，甚至公司的核心高管可以在十几年不分红、十几个月未发工资的情况下，先保证一线员工工资的正常发放。好在公司在 2014 年有了第一笔战略投资，现在可以说不担心生存的问题，目前比较担心发展的问题。

最后，李岱认为，像安天这样的高科技轻资产民营企业在发展中，想要融资和贷款，但没有可以抵押的资产，又不会接受有外资背景的金融公司来设计我们中国的网络安全体系，国家的支持是非常重要的。希望国家给予特殊的优惠政策或财政补贴给高科技民营企业。

外媒关注安天方程式组织系列报告

近日，国外媒体报道著名的反恶意软件组织 MalwareMustDie 发布官方声明，决定关闭其博客网站。声明文章援引安天实验室对“方程式组织”的系列分析报告，在报告中，安天研究人员逆向了“方程式组织”使用恶意软件感染 Linux 和 Solaris 平台进行入侵活动的结果，并公开了除了哈希以外的全部细节信息。

安天从 2015 年 2 月起，陆续公布了两篇针对方程式攻击组织的分析报告，分析了其针对 Windows 平台的恶意代码组件构成、对硬盘的持久化能力和对加密算法的使用。

目前，该译文被多家国内媒体转载。安天方程式系列报道请关注安天微博和官方网站。（原文链接：http://securityaffairs.co/wordpress/53285/malware/malwaremustdie-closed.html）

一周简讯

- PoisonTap 技术可向锁定 PC 安装后门
- Lynxspring 公司 SCADA 产品存严重缺陷
- 勒索软件 CrySis 被破解公开主密钥
- 勒索软件 Locky 借 OPM 泄露事件邮件传播
- 发布 Mirai 源代码的黑客论坛关闭相应版块
- D-Link 被发现可获 root 权限的 HNAP 漏洞
- 苹果应用 SHAZAM 后台监听麦克风
- 成人约会公司 FriendFinder Network 的 4.12 亿用户帐号信息被窃
- WindTalker 系统能让黑客通过 WiFi 信号盗取个人数据

（安天 CERT 搜集整理，详见 http://bbs.antiy.cn）

石破天惊处于世，榴连安全为一方

——安天“专属工程师的石榴节”主题活动

11 月 18 日下午，安天哈尔滨总部举办了“专属工程师的石榴节”主题活动。本次石榴节所用的石榴是客户为表示对安天近期分析工作及安全保护工作的满意而赠送的。安天所取得的成绩离不开辛勤工作的工程师们，为了丰富各位工程师的工作及学习生活，总工办决定开展本次内部石榴分享活动。

活动受到了工程师同事们的一致好评，大家纷纷积极参与。并表示会继续努力，以保障客户价值为中心，让产品和服务创造价值，继续与安天一起共创辉煌。

每周安全事件

类 型	内 容
中文标题	Linux 高危漏洞预警：按 Enter 键 70 秒获得 root 权限
英文标题	This Hack Gives Linux Root Shell Just By Pressing 'ENTER' for 70 Seconds
作者及单位	Swati Khandelwal; Thehackernews
内容概述	近日，Linux 被发现高危漏洞 (CVE-2016-4484)，攻击者可以通过持续按下 Enter 键 70 秒钟来获取 root initramfs shell，进而破坏 Linux boxes。漏洞存在于 Linux 流行变体中的统一密钥设置 (LUKS)。通过访问 shell，攻击者可以解密 Linux 机器，该攻击也适用于云端的虚拟 Linux boxes。受到影响的有 Ubuntu，Fedora，Debian 和许多其他的 Linux 发行版。该问题由苏格兰西部大学的讲师 Hector Marco，以及瓦伦西亚理工大学的教授助理 Ismael Ripoll 发现。他们表示该问题不需要任何特别的系统设置，并对漏洞做了分析。目前漏洞已修复，并且 Marco 和 Ripoll 已开发了一套解决方案用于抵抗攻击。不过不排除在修复期间，漏洞被伪造的可能性。
链接地址	http://thehackernews.com/2016/11/hacking-linux-system.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 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	Trojan/Android.aixunyun.a[prv，spy]2016-11-14	该应用程序为企业使用的监控类软件，运行后会开启设备管理器，会隐藏自身图标，获取设备 root 权限，会删除用户资料、开启或禁用用户摄像头、获取用户地理位置、发送短信、安装未知应用等，如非自主安装建议及时卸载。(威胁等级高)
		Tool/Android.mobilsife.a[prv，rmt，spy]2016-11-15	该应用是一款工具程序，包含手机防盗功能，会通过短信指令执行获取 GPS 位置信息、清除数据、锁屏等操作，建议用户谨慎使用。(威胁等级低)
		Trojan/Android.BankDrov.a[prv，exp]2016-11-15	该应用安装后无图标显示，运行后会监听正在运行的程序，当运行某些银行的应用时，会弹虚假界面劫持账户登录信息，并将输入的账号密码信息通过短信发送到指定号码，会造成用户隐私泄露造成经济财产损失，建议卸载。(威胁等级中)
		Trojan/Android.LockScreen.b[rog，exp]2016-11-17	该应用无实际功能，开机自启动，运行后隐藏图标，会联网上传短信、电话号码和设备信息，私自发送短信，删除短信，造成用户隐私泄露资费消耗，建议立即卸载该应用。(威胁等级高)
	较为活跃的样本	Trojan/Android.SmsThief.ax[prv，exp]	该程序运行后会收集用户短信、联系记录、浏览器搜索记录和书签、邮件信息等并且会发送给控制端，可能会造成隐私泄露，建议谨慎使用。(威胁等级高)
		Trojan/Android.FakeApp.bv[exp，prv]	该应用会伪装成 YouTube 相关应用，安装后会隐藏图标。运行后会拦截用户未接短信，无提示发送短信，会造成用户隐私泄露和资费消耗，建议卸载。(威胁等级高)
		Trojan/Android.oxti.d[exp]	该应用无实际功能，会私自发送、删除短信短信，，造成用户资费消耗，建议立即卸载。(威胁等级中)
		Trojan/Android.Metasploit.b[prv]	该应用为远程控制程序，安装后会隐藏图标，会窃取用户手机各项隐私信息，造成用户隐私泄露，建议卸载。(威胁等级中)
		Trojan/Android.FakeApp.bz[exp]	该应用会伪装成游戏程序，启动后会私自发送扣费短信，下载恶意软件并安装，造成用户资费消耗，建议卸载该应用。(威胁等级高)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 释放后重利用远程代码执行漏洞 (CVE-2016-7855)	Adobe Flash Player 是多媒体程序播放器。使用后会释放 (use-after-free) 漏洞，并会被攻击者利用来执行任意代码。CVE-2016-7855 漏洞影响 Windows、Macintosh、Linux 和 Chrome OS 平台上的 Flash Player 23.0.0.185 和 11.2.202.637 及其之前版本。(威胁等级高)
	较为活跃的样本	Trojan[Downloader]/Win32.Zurgop	此威胁是一种会连接网络下载其他恶意代码的木马家族。该家族样本运行后，在连接网络环境下，会下载其他恶意代码并执行，窃取用户敏感信息并回传，有一定威胁。(威胁等级中)
		Trojan[Dropper]/MSIL.Aotoit	此威胁是一种释放恶意代码的木马家族。该家族样本由 AutoIt 脚本编写，家族样本运行后，会释放 AutoIt 脚本执行工具及恶意脚本，并使用工具调用恶意脚本。(威胁等级中)
		GrayWare[AdWare]/MSIL.Tpyn	此威胁是一种可以连接网络下载推广应用的灰色软件家族。该家族样本运行后会下载并安装推广应用，在用户浏览网页时会弹出广告，占用系统资源。(威胁等级低)

针对防火墙的 BlackNurse 低流量 DoS 攻击

Michael Mimoso / 文　安天公益翻译小组 / 译

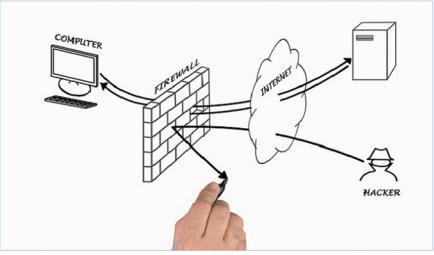
近日，研究人员指出，20 世纪 90 年代的一种拒绝服务攻击已经重现，对现代防火墙具有惊人的效力。该攻击被称为 BlackNurse，它利用 Cisco，Palo Alto，SonicWall 等漏洞防火墙的低流量互联网控制消息协议 (ICMP)，来进行攻击。

安全公司 TDC Security Operations Center，在近期发布了 BlackNurse 技术报告。报告指出，该攻击在传统上被称为“ping 洪泛攻击”，并称，在这种类型的攻击中，流量并不像发送的数据包类型那样重要。

根据 TDC 的报告，BlackNurse 基于互联网控制报文协议类型 3 代码 3 请求。研究人员说，这些是通常返回到 ping 源的数据包应答，显示目的地端口“不可达”。

在 BlackNurse 的描述中，攻击者通过使防火墙的主机 CPU 过载而导致拒绝服务 (DoS) 状态。TDC 指出，当攻击发生时，局域网端的用户将无法从互联网收发数据。目前尚不清楚 ICMP 类型 3 代码 3 请求为何会导致防火墙的 CPU 过载。然而，SANS Internet Storm Center 的研究人员认为它与防火墙日志记录有关。TDC 的报告支持这种理论。

TDC 写道：“在攻击期间，防火墙日志记录可能会增加攻击的影响，这意味着防火墙会更加耗尽。”



TDC 指出，BlackNurse 攻击类似于 ICMP 类型 8 代码 0 攻击 (也称为 ping 洪泛攻击)，但不会混淆。TDC 写道：“基于 ICMP 的攻击通常是一些 DDoS 攻击者使用的众所周知的攻击类型。”

研究人员解释称：“BlackNurse 攻击吸引了我们的注意，因为在我们的反 DDoS 解决方案中，即使流量速度和每秒数据包非常低，这种攻击也会导致客户的运作停滞。这甚至也适用于具有大型互联网上行链路和大型企业防火墙的客户。我们预测，专业防火墙设备能够处理这种攻击。

研究人员指出，值得注意的是，BlackNurse DoS 攻击流量介于 15 到 18 Mbps(或每秒 40 到 50K 数据包)。这与上个月针对 DNS 提供商 Dyn 的 1 Tbps DDoS 攻击形成鲜明对比。

低流量 DDoS 攻击是有效的，因为其目标不是通过无用流量洪泛防火墙，而是驱动高 CPU 负载。TDC 说，为此，许多防火墙厂商防御基于 ICMP 的攻击。但是阻止所有 ICMP 类型和代码不是什么好办法，因为这样可能会导致网络崩溃。

事实上，安全公司 NetreseC 在分析 BlackNurse 时指出：“我们建议您允许 ICMP 不可达消息类型 (类型 3)。拒绝 ICMP 不可达消息将禁用 ICMP Path MTU 发现，这可以终止 IPSec 和 PPTP 流量。”

对于漏洞防火墙，TDC 选择了一些思科 ASA 防火墙。SANS Internet Storm Center 在报告中指出，思科防火墙更新，更大，多内核，貌似很好。然而，SANS 技术研究所所长 Johannes Ullrich 指出，SonicWall 和一些 Palo Alto 防火墙似乎存在漏洞。报告发布之后，Cisco，SonicWall 和 Palo Alto 已跟我们取得联系，但没未回复。

TDC 指出，BlackNurse 测试包括在防火墙的 WAN 端允许 ICMP，并使用工具 Hping3(一个用于 TCP/IP 协议的免费数据包生成器和分析器) 进行测试。TDC 概述其自己的规则称，检测包括采用 SNORT IDS/IPS 规则来发现攻击。缓解包括创建“允许 ICMP 并可以配置的可信源列表”和“禁用 WAN 接口上的 ICMP 类型 3 代码 3”。

原文名称	BlackNurse Low-Volume DoS Attack Targets Firewalls
作者简介	Tom Spring，卡巴斯基《安全周报》副主编。
原文信息	2016 年 11 月 11 日发布于《安全周报》(Threatpost) 原文地址 https://threatpost.com/blacknurse-low-volume-dos-attack-targets-firewalls/121916/
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《FakeFile 样本分析报告》

近日，安天追影小组在进行网络安全事件梳理时，关注到一个不需要 root 访问权限就可以实现自身恶意操作的后门木马。经分析，该木马家族为 FakeFile 家族木马，是一种针对桌面系统而非服务器的木马家族，主要利用 PDF、微软 Office 或者 OpenOffice 文件进行传播。FakeFile 木马主要功能是窃取被感染机器上的文件并上传，并执行 shell 命令，会控制服务器 (C&C) 发送的回复包，同时，会伪装成 Windows 平台的 http 通信。

经分析，FakeFile 木马样本是一个 elf 格式文件，需要有 32 位环境兼容库才能执行。首先，当 FakeFile 木马样本运行后，该样本会将自身复制到“<HOME>/.gconf/apps/gnome-common/gnome-common” 目录下，进行搜索并替换系统中特定文件名称的隐藏文件，完成感染机器、设置自启动并隐藏自身的目的。当成功完成第一步后，FakeFile 木马样本会遍历系统，查看特定后缀名文件，包括以下后缀名称：.doc、.DOC、.xls、.XLS、.ppt、.PPT、.docx、.DOCX、.xlsx、.XLSX、.pptx、.PPTX、.odt、.ODT、.ods、.ODS、.odp、.ODP、.pdf、.PDF 等。随后，会与 C&C 服务器进行通信，接收指令。

从 FakeFile 木马家族的样本分析中，可以发现该木马具备对文件执行重命名、删除、发送文件或文件夹的全部内容至命令与控制服务器、发送文件夹内的文件清单至命令与控制服务器、创建新的文件与文件夹等操作功能。同时，还会运行文件、运行 shell 命令、设置权限、终止其进程或者将自身从受感染主机内移除。

在感染终端与 C&C 服务器通信中，感染终端会发送一个 http GET 请求的回复包。从回复包数据来看，其是伪装成一个 Windows 平台的浏览器访问请求包，回复包的 User-Agent 数据：User-Agent:Mozilla/4.0 (compatible; MSIE 5.00; Windows 98)。

随着 Linux 操作系统的日益普遍，恶意软件开发者们开始将矛头指向 Linux 计算机。不仅包括 Linux 服务器也针对桌面系统的计算机，并且 Linux 环境的恶意代码也越来越注重隐秘性，从替换劫持系统启动项中的隐藏文件，到其伪装为 Windows 环境访问浏览器的网络通信行为，都是为隐藏自身。安天追影小组提醒各电脑使用者要提高安全意识，不要随意打开未知的 PDF、微软 Office 或者 OpenOffice 等文件，注意对隐私文件的保护。

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：伪装 Windows 环境 http 协议通信、遍历系统中文档文件、释放 elf 文件、自复制、创建启动项、设置执行权限、发送数据。

文件名	EC301904171B1EBDE3A57C952AE58A3A
文件类型	BinExecute/Linux.ELF
大小	59 KB
MD5	EC301904171B1EBDE3A57C952AE58A3A
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[BackDoor]/Linux.FakeFile.a
判定依据	智能学习

运行环境

操作系统	Windows XP 5.1.2600 Service Pack 3 Build 2600
内置软件	默认

危险行为

行为描述	危险等级	行为描述	危险等级
伪装 Windows 环境 http 协议通信	★★	遍历系统中文档文件	★★★

其他行为

行为描述	危险等级	行为描述	危险等级
释放 elf 文件	★	自复制	★
创建启动项	★	设置执行权限	★
发送数据	★		

运行环境

描述	值	描述	值
File Size	59 kB	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		

报告地址：https://antiy.pta.center/_lk/details.html?hash=EC301904171B1EBDE3A57C952AE58A3A