趋势科技新闻稿

[即时发布]

英国王室宝宝成为最新社交工程攻击诱饵　美、日、澳感染严重

假 CNN 新闻报导奥巴马赠送新生礼 针对 JAVA 漏洞进行攻击

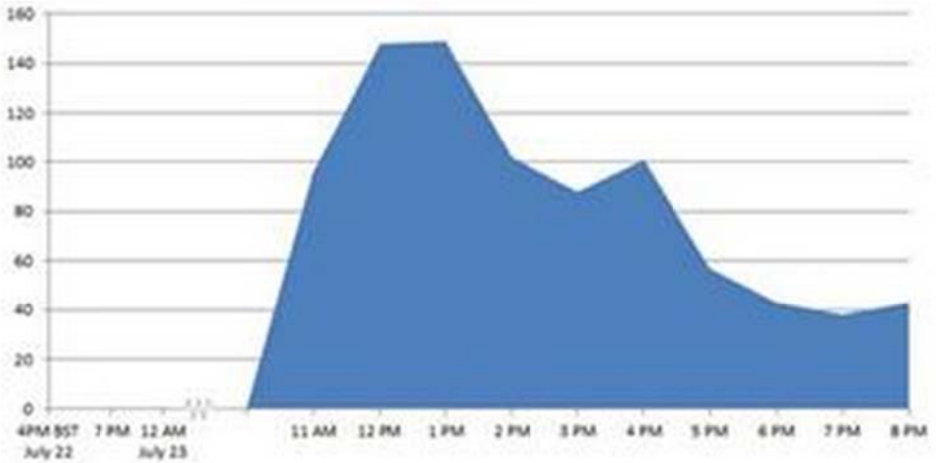
[趋势科技中国]– [2013 年 8 月 2 日]自去年年底英国王室宣布凯特王妃怀孕以来，全球翘首以盼的英国王室宝宝终于在 7 月 22 日（英国时间）诞生，在全球媒体均不断播送最新消息的同时，恶意威胁也伴随而来。趋势科技发现王室宝宝相关的垃圾邮件攻击，其中还包含假借美国新闻网 CNN 名义，报导美国总统奥巴马赠送英国王室新生儿礼物的假新闻，此漏洞攻击码为 JS_OBFUSC.BEB，JAVA 漏洞为 JAVA_EXPLOYT.RO。

此漏洞特别针对 JAVA 的两处弱点：CVE-2013-1493、CVE-2013-2423，黑客可能利用这两处漏洞植入木马程序 TROJ_MEDFOS.JET，一旦成功入侵后，将与可疑网站连接，可能下载更多恶意程序或是游走在灰色地带的广告程序。趋势科技呼吁莫因好奇心驱使而点击来路不明的链接。此类攻击防不胜防，建议通过有网页信誉评等的信息安全防护软件，方能协助封锁恶意链接。

【图 1 :假 CNN 新闻报道】

【图 2 :王室宝宝相关的垃圾邮件样本】

这些邮件伪装成来自 ScribbleLive（一种提供即时参与的服务平台），它所提供的东西是虚假的，而且点击邮件内的链接只会出现多次的重新导向，就像黑洞漏洞攻击包（BHEK）垃圾邮件的常见手法。黑洞漏洞攻击包让网络犯罪份子用来判断用户所使用软件版本，以便在网页里提供“正确”的漏洞攻击码。



【图三：王室宝宝相关威胁在正式宣布后半天开始出现】

在这起王室宝宝攻击里，会引发重新导向的脚本被侦测为 JS_OBFUSC.BEB。根据初步报告，美国、日本和澳洲是感染最多的国家。随着王室新生儿的消息不断的发酵，可以预计会有更多感染来自这三大地区。

Country	% of Hits to the Landing Page in the Last 24 hours
United States	55%
Japan	14%
Australia	10%
Others	20%

【图四：超过一半的攻击来自美国】

趋势科技（中国区）产品经理申鹤表示：“社交工程邮件往往与引人注目的全球性新闻话题一同发酵，这是黑客诱骗受害人的最佳良机，例如近期的波士顿马拉松事件和教皇选举。建议用户选取具有网页信誉评等功能的信息安全软件，并定期进行更新，以协助过滤此类恶意链接，以免成为下一位受害者。”

趋势科技 PC-cillin2013 云安全版已经在第一时间将上述网址封锁，趋势科技 PC-cillin 2013 是业界首个同时支持 Windows，Mac，Android 手机及平板电脑的安全防护软件。通过 PC-cillin 2013 云安全版后台中全球钓鱼网站监控体系，爬网系统、网页安全分级功能等最新的防控技术，能全面监测和甄别网页中的恶意代码，并通过“主动式云端拦截技术”提前一步甄别出恶意网站及链接，不给不法分子任何机会。

PC-cillin 2013 云安全版免费试用下载网址：
http://cn.trendmicro.com/cn/home/

###

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商 ,致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。

更多媒体垂询，敬请联络：

趋势科技（中国）有限公司
刘婷婷
电话：010-85252277
电子邮件：angela_liu@trendmicro.com.cn

北京谋信传习广告有限公司
那罡
电话：010-67047822
电子邮件：nagang@ctocio.com