【卡巴斯基】

[卡巴斯基 2013 年 9 月垃圾邮件报告]

【反垃圾信息中心编译】

2013/12/13

目录

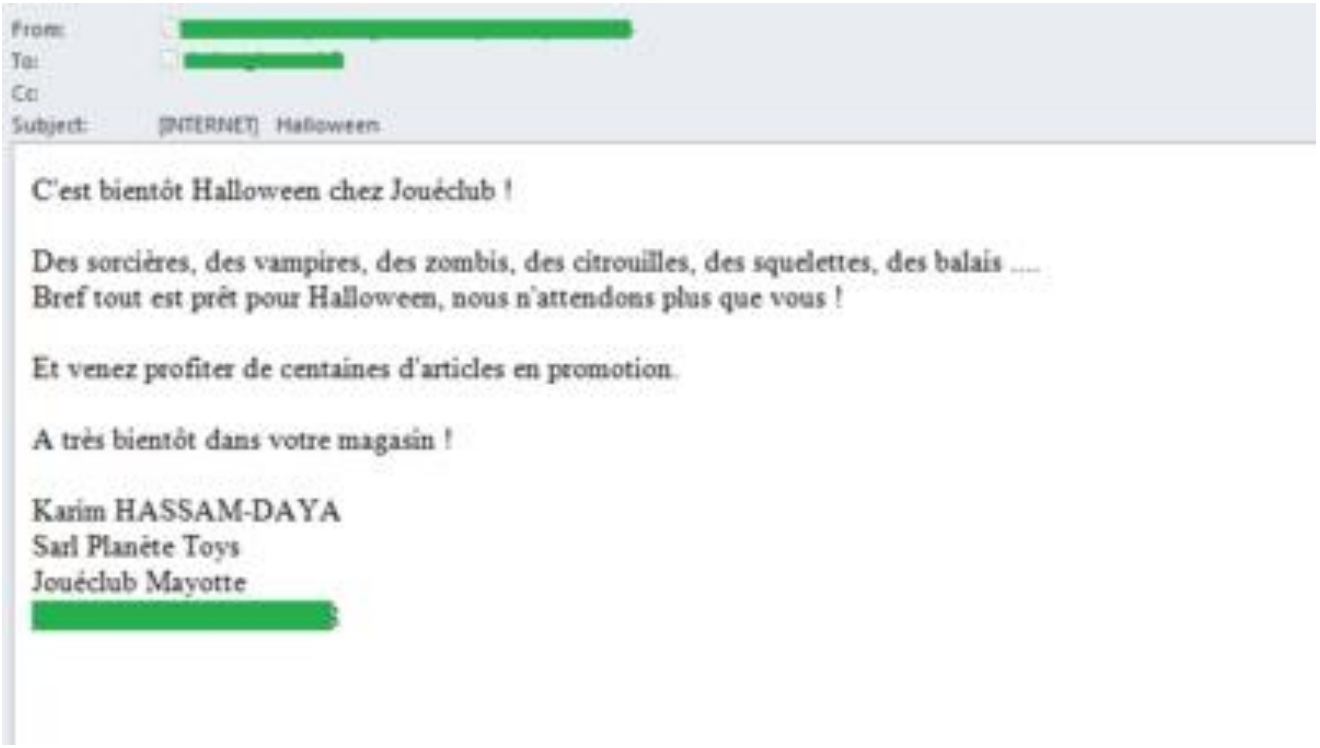
聚焦垃圾邮件

9 月份寒潮过后，卡巴斯基发现很多群发邮件是关于减少取暖费用并给房子保暖的，这些邮件常常出现在俄语和英语类垃圾邮件中。9 月份群发邮件中有很大比例是关于汽车保险和印刷服务的，尤其提供 2014 年日历。节日类垃圾邮件主要是英语类的，与万圣节相关。

万圣节垃圾邮件

每年万圣节前夕我们都会发现很多群发活动与这个节日相关。像往常一样，英语类垃圾邮件都是为万圣节服装做广告，常见的群发活动是关于冒牌包，并用万圣节南 瓜和大幅折扣来诱导消费者。中小企业也会加入群发大军，用幽灵主题推广自己的产品。当然了，节日名称常出现在邮件的主题行中吸引用户注意。

9 月份 ,我们也发现法语类万圣节群发邮件 ,垃圾邮件发送者为万圣节服装和各种装饰品做广告。


From: [redacted]
To: [redacted]
Cc:
Subject: [INTERNET] Halloween

C'est bientôt Halloween chez Jouéclub !

Des sorcières, des vampires, des zombis, des citrouilles, des squelettes, des balais ....
Bref tout est prêt pour Halloween, nous n'attendons plus que vous !

Et venez profiter de centaines d'articles en promotion.

A très bientôt dans votre magasin !

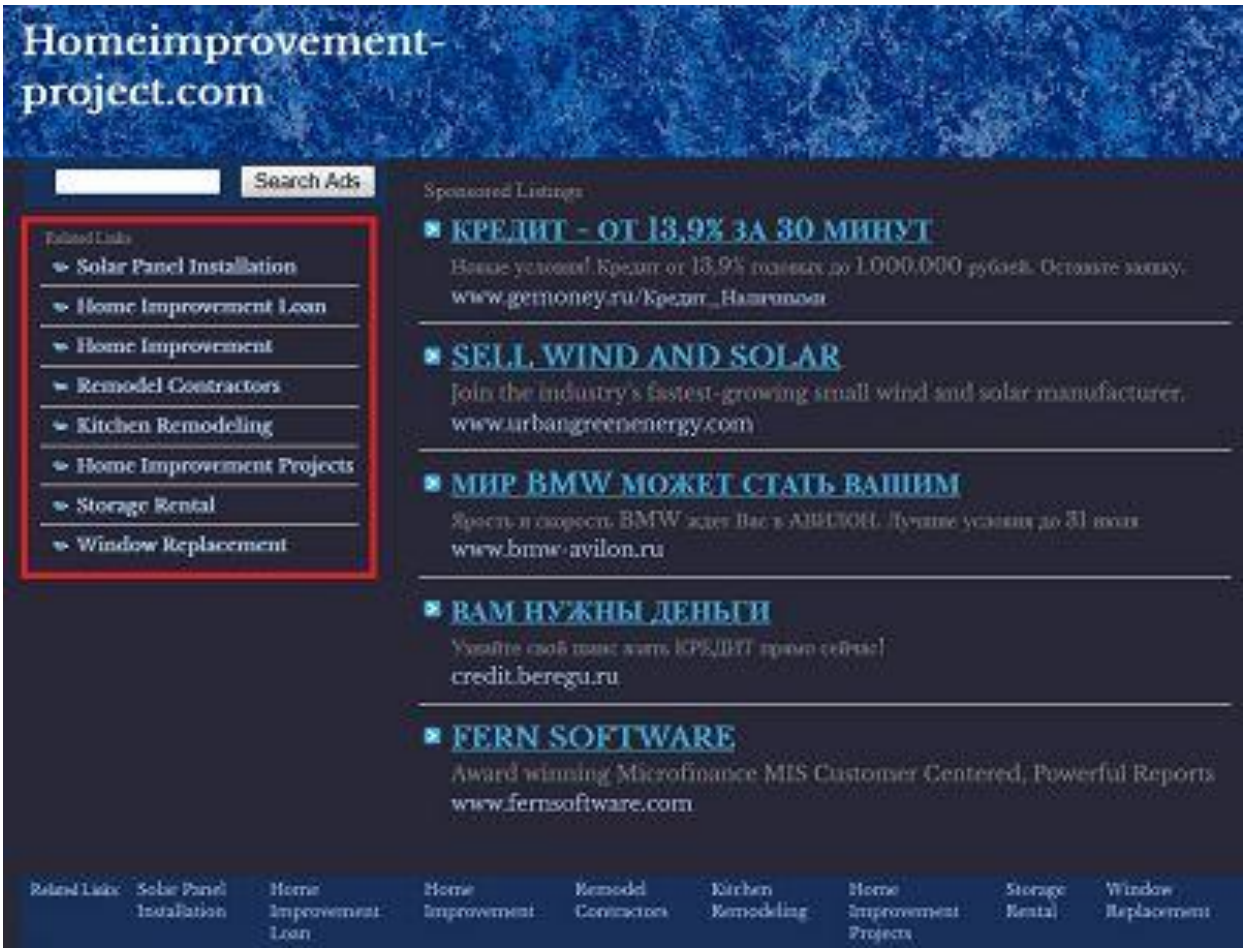
Karim HASSAM-DAYA
Sarl Planète Toys
Jouéclub Mayotte
[redacted]

与节能相关的垃圾邮件

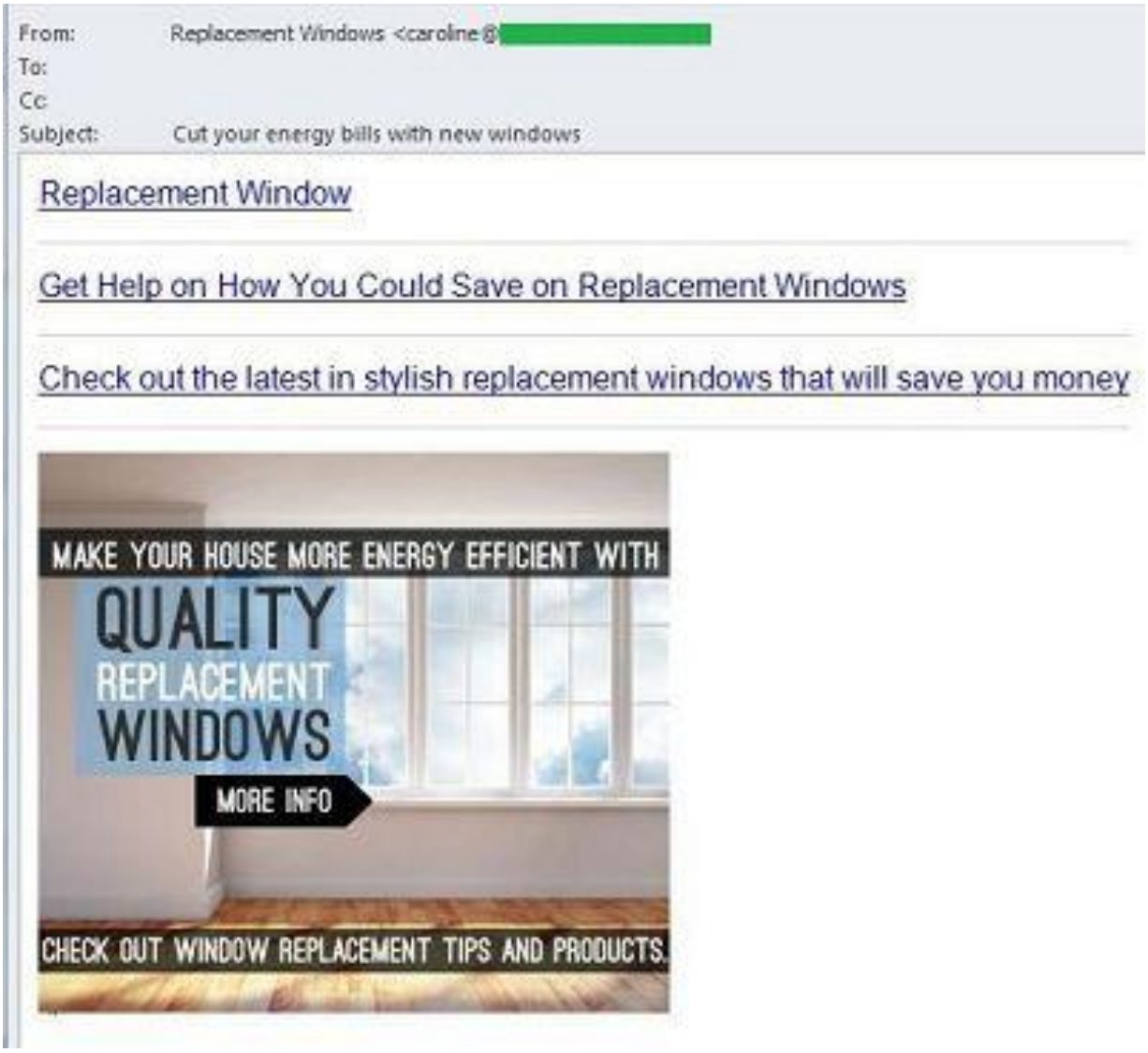
秋天到了，天气转寒，供暖和用电支出增加。这个季节性的现象被垃圾邮件发送者充分发掘。9月份的很多群发活动提供各种方式来为家庭保暖并减少物业账单。

此类型的英语群发邮件主要关于安装专业太阳能电池板。这些信息有不同的表现形式：有的包含简短文本，有的包含彩色的标语。

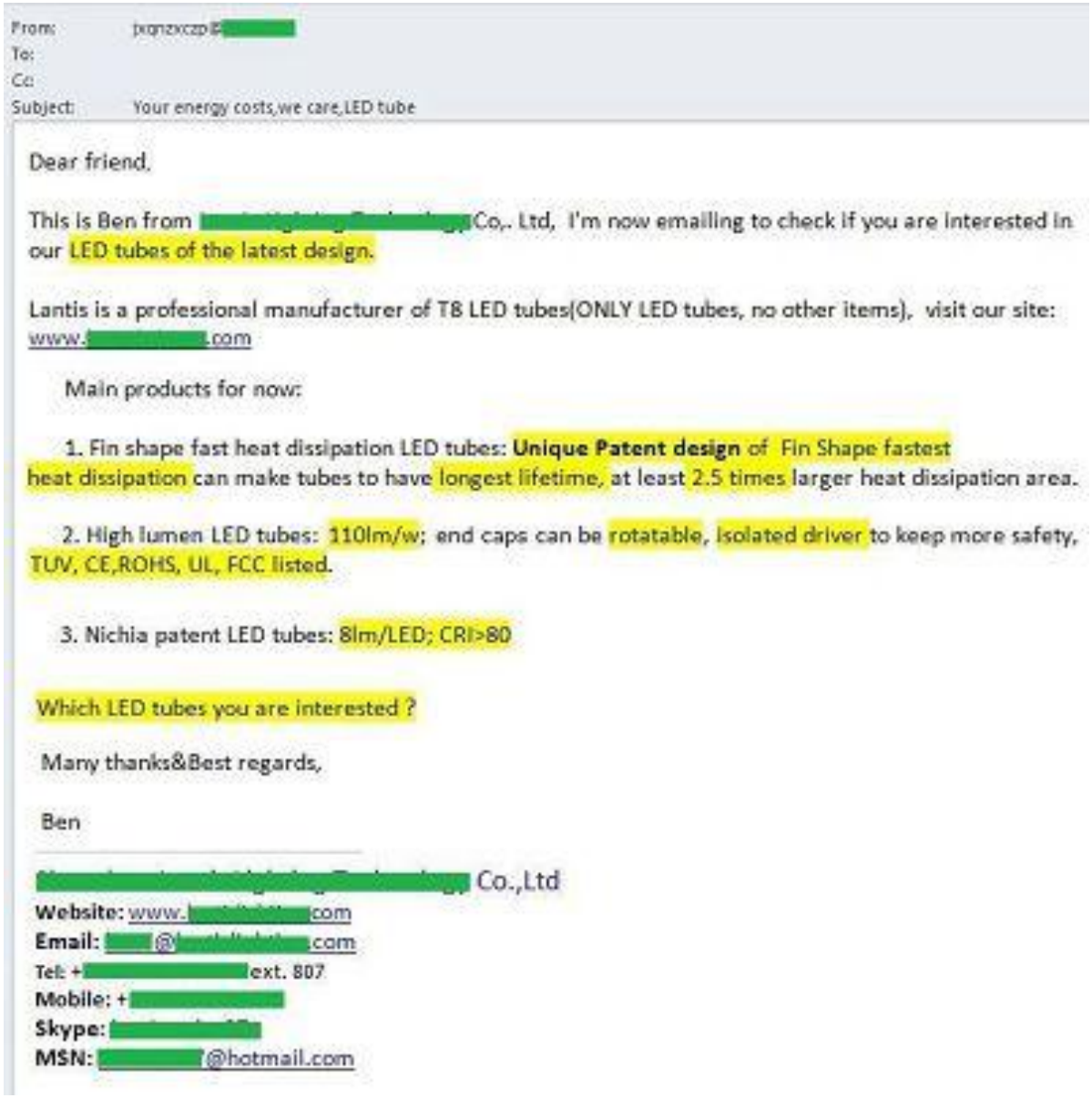
所有信息都包含一个很长的链接，将用户指引到一个新注册的域名，不同的邮件带有不同的域名。一系列引导之后，这些链接将用户指引到一个网站，此网站描述政 府为安装太阳能电池板提供补贴的方案，或是指引到一个空白网站，此网站包含能够安装太阳能电池板或出售相关设备的公司链接。



也有一部分群发邮件是关于安装隔热窗的，许诺节约热能，减少能耗开支。这些信息包含很长的链接，在一系列指引之后，将用户带到购物网站——了解更多细节并下单。



也有群发邮件是来自 LED 灯泡生产商的，也是主打节能主题。这样的邮件通常是公司经理发来的并提供了联系方式。在邮件正文中 提供了产品的细节信息，并提供了公司网站链接。这些邮件类似商业通信邮件，但是是发给通用收件人的而不是具体的个人。发件人地址是字母的随意组合，当然也就不同于邮件中的联系邮箱。



From: [redacted]
To:
Cc:
Subject: Your energy costs,we care,LED tube

Dear friend,

This is Ben from [redacted] Co,. Ltd, I'm now emailing to check if you are interested in our LED tubes of the latest design.

Lantis is a professional manufacturer of T8 LED tubes(ONLY LED tubes, no other items), visit our site: www.[redacted].com

Main products for now:

1. Fin shape fast heat dissipation LED tubes: **Unique Patent design** of Fin Shape fastest heat dissipation can make tubes to have longest lifetime, at least 2.5 times larger heat dissipation area.

2. High lumen LED tubes: 110lm/w; end caps can be rotatable, isolated driver to keep more safety, TUV, CE,ROHS, UL, FCC listed.

3. Nichia patent LED tubes: 8lm/LED; CRI>80

Which LED tubes you are interested ?

Many thanks&Best regards,

Ben

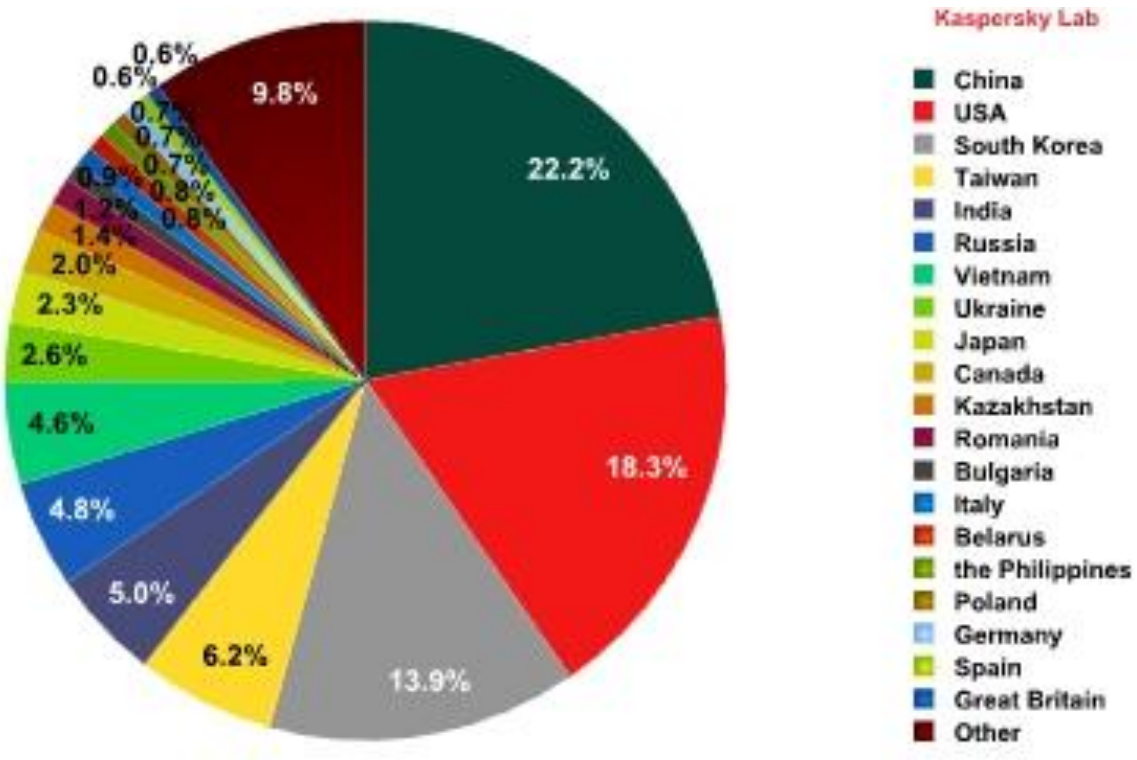
[redacted] Co.,Ltd
Website: www.[redacted].com
Email: [redacted]@[redacted].com
Tel: +[redacted] ext. 807
Mobile: +[redacted]
Skype: [redacted]
MSN: [redacted]@hotmail.com

汽车保险服务

英语垃圾邮件发送者使用汽车保险服务诱使用户提交个人信息。邮件标题许诺使用简单的方式即可大幅减少汽车保险花费。邮件中的链接指向一个新建网站，然后又将用户指引到另一个与保险服务无任何联系的网站。这个网站邀请用户回答三个问题就可以赢得苹果笔记本电脑、iphone 或 ipad。回答问题并选择了奖品之后，用户需要填写个人信息——姓名、地址、邮政编码、手机号码和邮件地址。换句话说，以奖品为借口，垃圾邮件发送者欲获取用户联系信息。

垃圾邮件来源的地理分布

2013 年 9 月，垃圾邮件占所有邮件的比例下降了 1.4 个百分点，平均为 66.2%。垃圾邮件来源国前三名仍然未变：中国第一，垃圾邮件占比 22%，比上月增加了 1 个百分点；美国第二，垃圾邮件占比 18%，比上月下降了 1 个百分点；韩国第 3，垃圾邮件占比 14%，比上月增加了 1.4 个百分点。这三个国家的垃圾邮件总量占全球垃圾邮件的 54%。



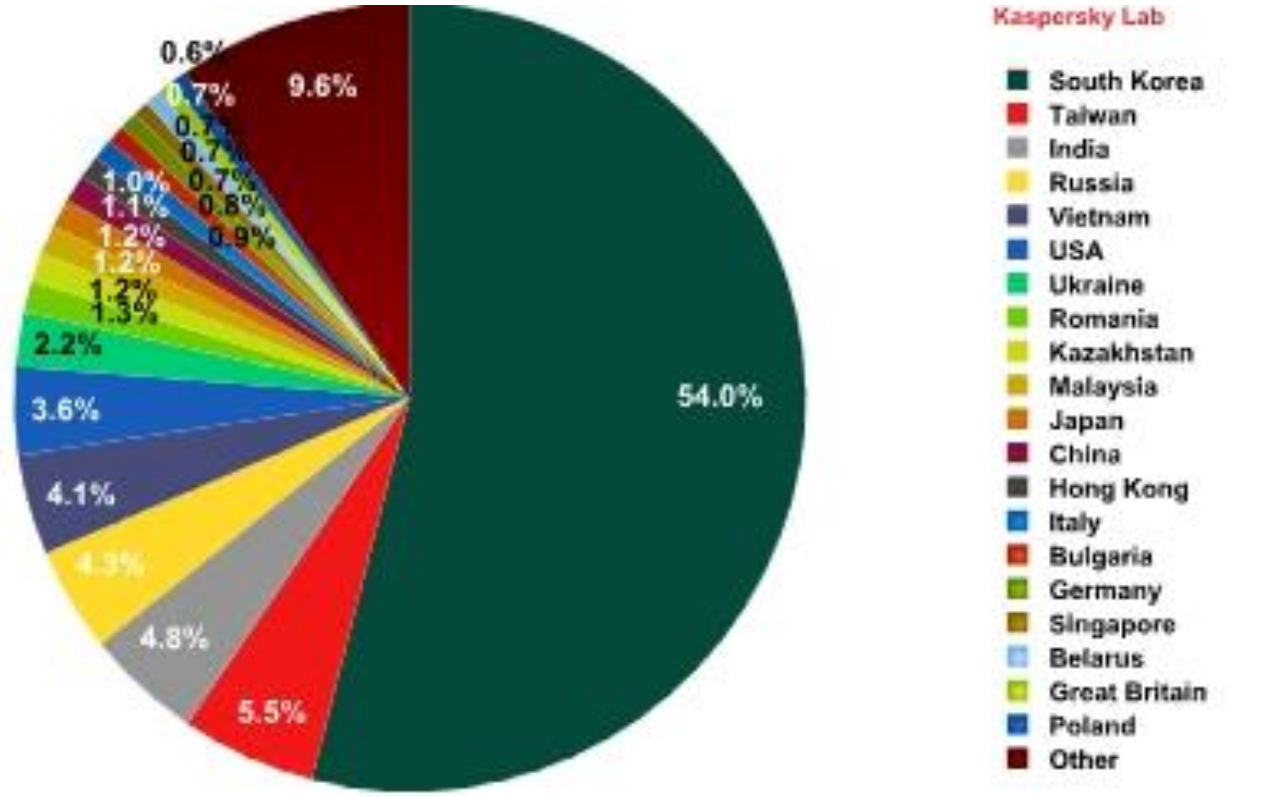
台湾仍像 8 月一样，位列第四，垃圾邮件占比 6%，上升了 0.8 个百分点。

印度上升了 2 个百分点，占 5%，排名从第 8 名前进到第 5 名。

像之前预计的一样，日本闯入前十，以 2.4%的比例排名第 9。加拿大第 10，占比 2%，排名前进了两名。

白俄罗斯和德国的比例减少：白俄罗斯（0.8%）下降了 6 个名次，德国（0.7%）也跳出了前 10。

前十名中其他几个国家的排名和垃圾邮件占比几乎没什么变化。



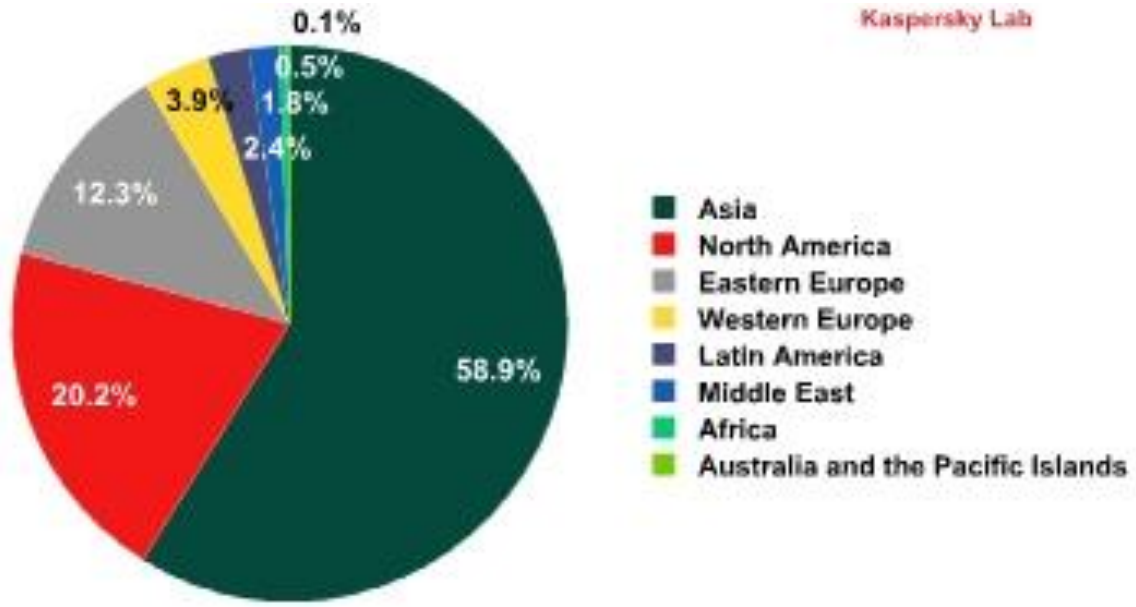
9 月份，即使比例下降了 6 个百分点，韩国仍然是向欧洲发送垃圾邮件最多的国家（54%）紧随其后的是台湾（5.6%）和印度（4.8%），印度占比上升了 2.7 个百分点，排名从第 6 上升到第 3。

上个月美国(3.6%)排名第三。9 月份，美国下降到第 6 名，尽管占比仅有轻微变化，上升了 0.3 个百分点。

俄罗斯（4.3%）和越南（4.1%）分别第 4、第 5。然而来源这两个国家的垃圾邮件总百分比上升了 1.5 个百分点。

9 月份，针对欧洲用户的垃圾邮件来源国排名前 10 中包括马来西亚（1.2%）。另外亚洲的日本（1.2%）和香港（1%）与上月相比，垃圾邮件量也增加了，分别增加了 0.6 和 0.9 个百分点。

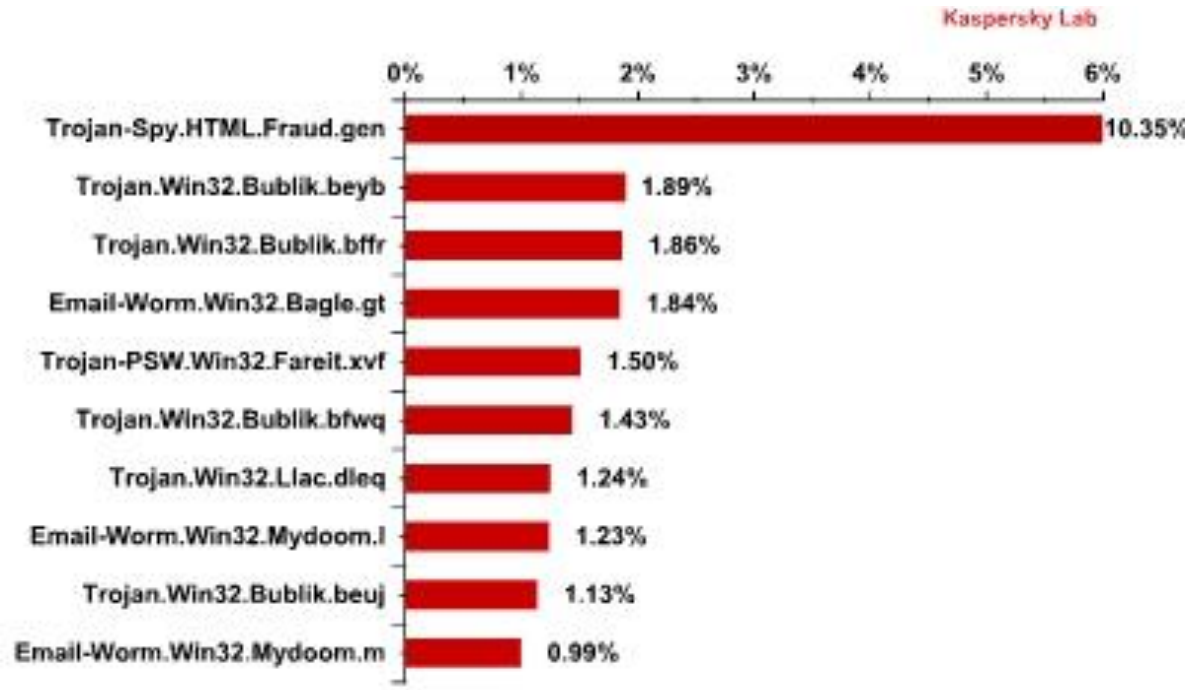
同时，9 月份来源德国的垃圾邮件（0.7%），下降了 0.8 个百分点，导致在排名中下降到第 17 名。



9 月，在垃圾邮件来源地区排名中亚洲（59%）仍然居首，与上月相比上升了 4 个百分点。尽管北美的数字上升了 2 个百分点，东欧下降了 2 个百分点，但北美（20%）和东欧（12%）仍然位列第 2 和第 3。西欧(4%)和拉美（2.4%）分列第 4 和第 5。

邮件中的恶意附件

9 月份，通过邮件传播的 10 大恶意程序发生了很大变化，出现了 5 个新成员。



Trojan-Spy.html.Fraud.gen 仍然是传播最广泛的恶意程序，它已经连续 7 个月保持第 1。概况来说，Fraud.gen 归属使用欺骗技术的木马程序家族：这些木马模仿 html 页面，并以商业银行、电子商店、软件公司的通知形式通过邮件进行传播。

9 月份排名中的 4 位新成员分别排第 2、第 3、第 6 和第 9——属于 Bublik 家族的恶意程序。主要功能是在受害人电脑上未经授权下载并安装新版本恶意软件。一旦任务完成，此程序就休眠了：将自己复制到%temp%文件，此文件模仿 Adobe 应用或文件。

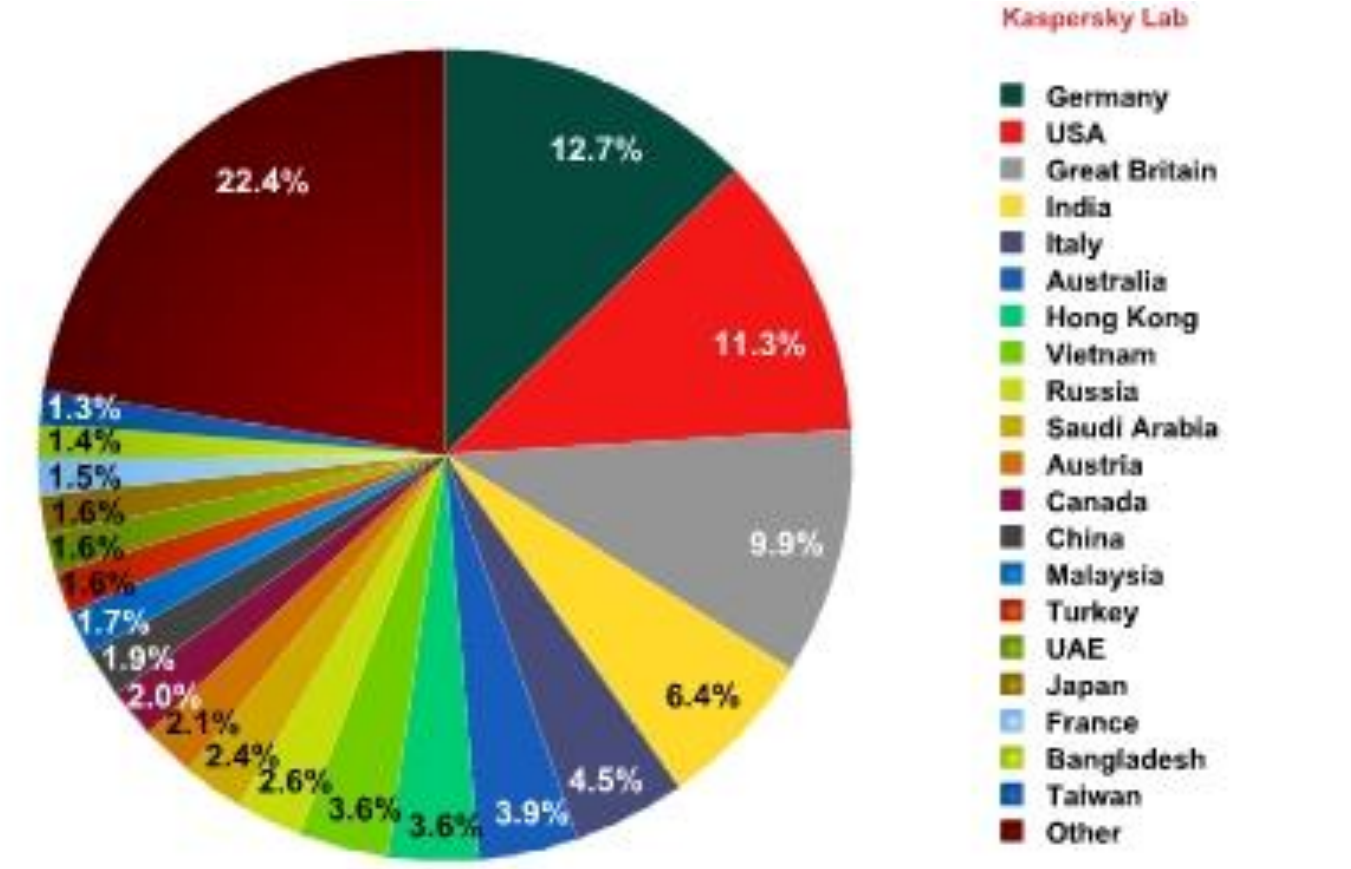
Email-Worm.Win32.Bagle.gt 排名第 4。此邮件蠕虫是个可执行的文件，以邮件附件的形式分布进行传播。像大多数的蠕虫一样，此蠕虫自我扩散到受害人的地址簿中。在用户不知情的情况下，它也能下载其他恶意程序到电脑上。为了传播恶意信息，Email-Worm.Win32.Bagle.gt 使用自己的 SMTP 图书馆。

9 月份的另一位新成员 Trojan-PSW.Win32.Fareit.xvf 排名第 5。此恶意程序专门从被盗用的计算机上窃取用户名和密码。它自己就可以进行下载更新，而不用根植于系统中，并模仿 Adobe 应用或文件。

Trojan.Win32.Llac.dleq 排名第 7。这个程序的主要任务是暗中监视用户：搜集安装在电脑上的软件信息（主要是反病毒程序和防火墙）和电脑本身的信息（处理器、操作系统、磁盘），拦截网络摄像头图片和键盘记录，并从多个应用程序截获机密数据。

Email-Worm.Win32.Mydoom.l 排名第 8。此网络蠕虫带有后门功能，以邮件附件形式，通过文件分享服务和可读网络资源进行传播。从受感染的计算机处截获邮件地址，这些地址可以被用于进一步的邮件群发。此蠕虫也直接连到收件人的 SMTP 服务器。

另一个蠕虫 Email-Worm.Win32.Mydoom.m 排名第 10，它会扫描 MS Windows 地址薄和 IE 浏览器缓存来寻找邮件地址。除了进行自我扩散，它也向搜索引擎发送隐藏的搜索请求，增加从犯罪分子服务器下载的网站流量和排名。



恶意邮件的目标国家前三名仍然未变：德国（12.67%）第 1，美国（11.33%）第 2，英国第 3，比例上升到 9.98%。

俄罗斯仍然第 9，尽管杀毒检测的比例下降到 2.6%。

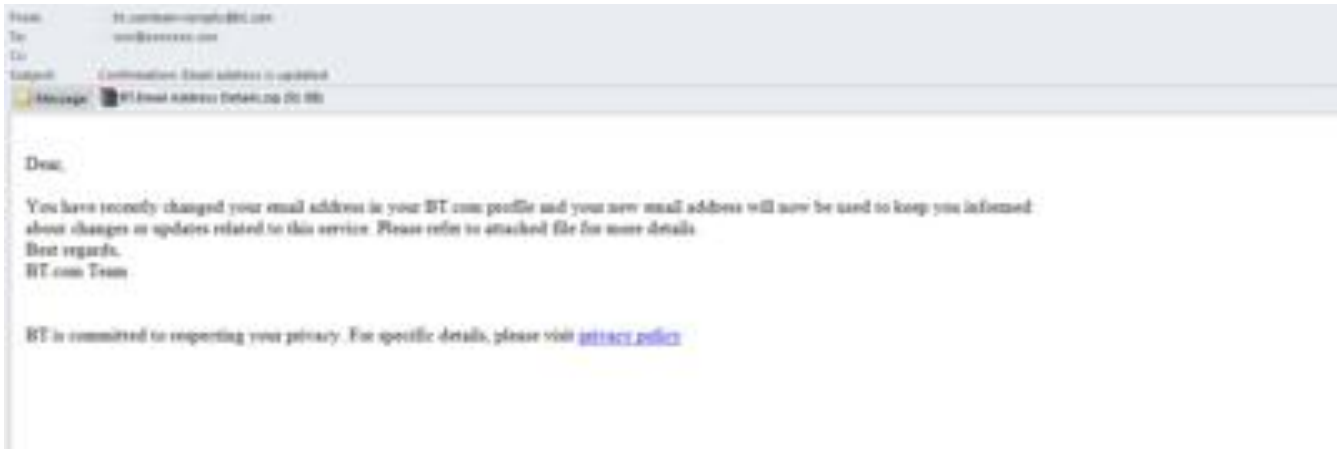
另外值得注意的是沙特阿拉伯（2.41%）在 9 月份进入前 10。

恶意垃圾邮件的特征

骗子通常不会把互联网和通信服务提供商作为自己的目标。然而，在 2013 年 9 月我们发现有些群发活动开始利用此领域的国际知名公司的名称。

英国通信公司 BT 集团被利用来散布木马——Downloader.Win32.Dofoil ,此木马在受害人电脑上下载并执行恶意软件。此虚假信息声称收件人最近指定了一个新的邮件地址，用于将来接收通知。若需了解更多信息，收件人需要打开附件，附件实际上是一个隐藏木马。为了说服收件人相信邮件的

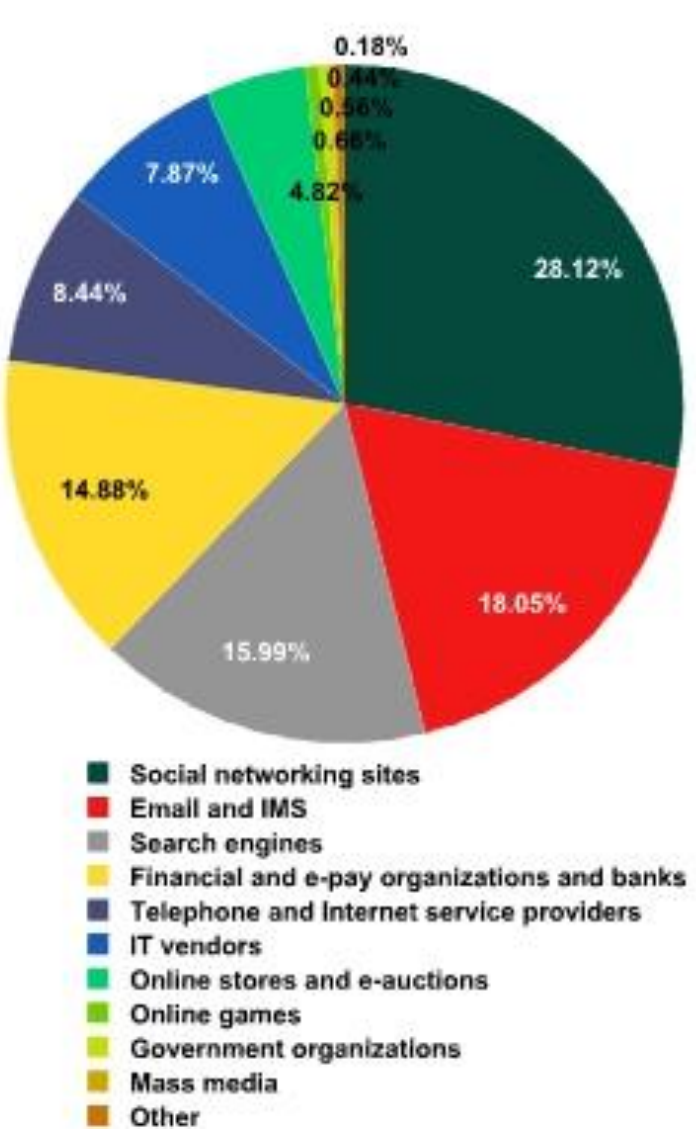
合法性，攻击者使用的邮件地址和链接乍看像是 BT 公司的。然而，个人地址的缺失和所附的可执行文件 BT.Email Address Details.pdf.exe 本可以警示用户有诈骗风险。



来自银行的虚假通知算是很常见的了。9 月，我们发现一次群发活动声称来自韦伯斯特银行。这次邮件中提到公司正在监测所有的客户交易以识别支付系统中的可疑活动。邮件包含木马下载程式 Trojan-Downloader.Win32.Angent，冒充银行的报告。为了使邮件看上去更加合法，诈骗者从一个类似官方地址的虚假地址发送邮件，邮件正文包含公司官网链接和自动签名。

钓鱼邮件

钓鱼攻击的主要目标 9 月份没有发生太大变化。社交网络仍然居于榜首（28.1%）。



钓鱼者的前 100 个目标组织，按类别分布

排名是基于卡巴斯基实验室的反钓鱼监测，每次用户尝试点击一个钓鱼链接就会激活反钓鱼监测，无论此链接是在垃圾邮件中或网页上。

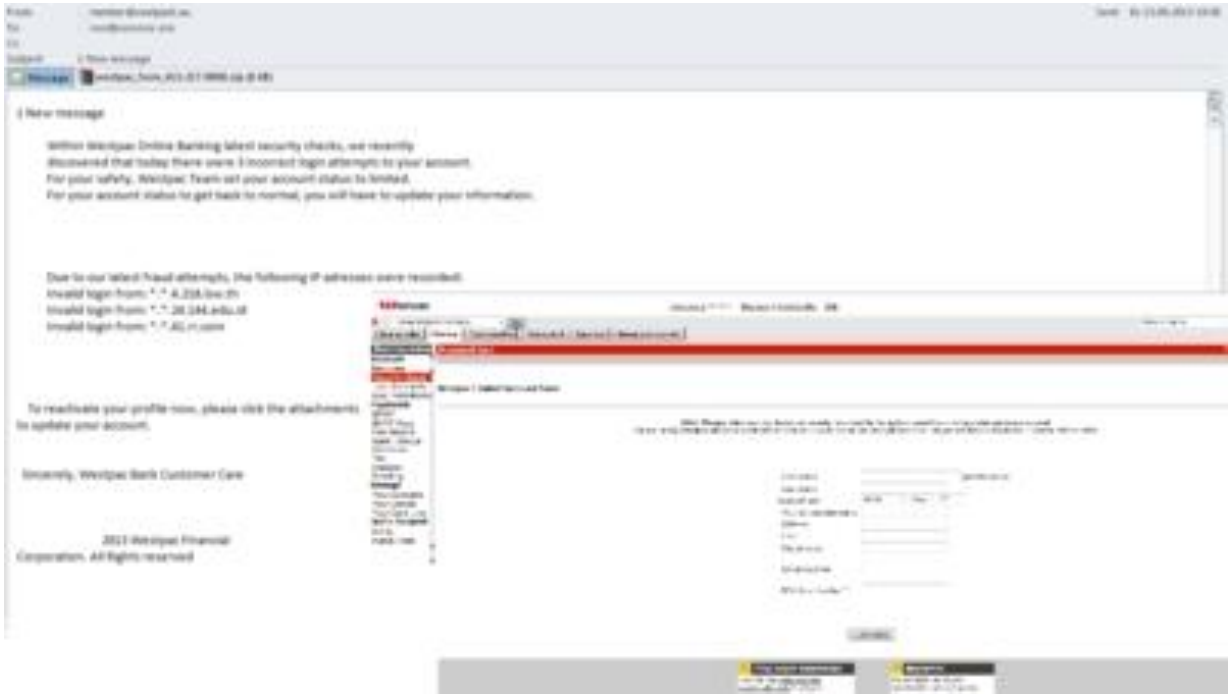
邮件和即时信息（18.1%）增加了 0.8 个百分点，仍然排在第 2 位。搜索引擎（16%）下降了 0.1 个百分比，排名第 3。

金融和电子支付(14.9%)增加了 1 个百分点仍然排在第 4 名。IT 厂商下降了 0.5 个百分点，与电话和互联网服务提供商（上升了 0.6 个百分点）互换了位置，这两类分列第 5 名和第 6 名。

9 月份，钓鱼者再次关注澳大利亚和新西兰的主要银行。2013 年 7 月我们发现有一次群发活动包含冒充来自澳大利亚和新西兰银行集团的虚假通知。这次钓鱼者试图诱导 Westpack（澳大利亚知名银行之一）客户。

攻击者甚至没有花费精力去发明新把戏——他们仅仅使用久经考验的把戏。虚假邮件通知收件人：在线银行安全系统发现收件人账户有三次未经授权的登录尝试，依据安全规则，在线银行系统已经关闭了登录入口。为了给账户解锁，用户需要打开所附文件。此文档 Westpac_form- 413- 217 -9908.zip 包含一个 HTML 页面，要求填写用户的个人信息。一旦填写了所有字段，数据即被传送给诈骗者。

钓鱼页面使用银行官网的颜色和标识，但是并不是原封不动的复制。然而，如果用户点击钓鱼页面的链接以进入网站，银行官网即在一个独立的窗口打开。为了迷惑用户，钓鱼者也提供了账户详细信息，例如 IP 地址——未经授权的尝试在键入密码时使用的。



结语

9 月份，世界垃圾邮件的比例持续下降到 66%。像往常一样垃圾邮件发送者为季节性商品和服务做广告。例如，与节能和隔热建筑相关的垃圾邮件数量大幅增加。9 月的群发活动利用节日主题——这次是关于万圣节和新年。下个月圣诞节类的垃圾邮件将会显著增加。

像之前预计的一样，对社交网络的攻击比率下降而对金融和电子支付的攻击比例增加。然而这些变化是微小的，并且钓鱼者最常攻击的单位排名没什么变化。这两种趋势在 10 月份很可能继续。9 月份，诈骗者倾向于将攻击目标从银行和快递服务转向各种通信公司。

（反垃圾信息中心编译，源文网址：

http://www.securelist.com/en/analysis/204792309/Spam_in_September_2013）