【卡巴斯基】

[卡巴斯基 2013 年 8 月垃圾邮件报告]

【反垃圾信息中心编译】

2013/12/13

目录

八月的数字

八月垃圾邮件占邮件总量的百分比与七月份相比下降了 3.6 个百分点，平均为 67.6%。

网络钓鱼电子邮件与七月相比增加了 10 倍,平均为 0.013% 。

含有恶意附件的电子邮件占邮件总量的 5.6%，与七月份相比上升了 3.4 个百分点。。

聚焦垃圾邮件

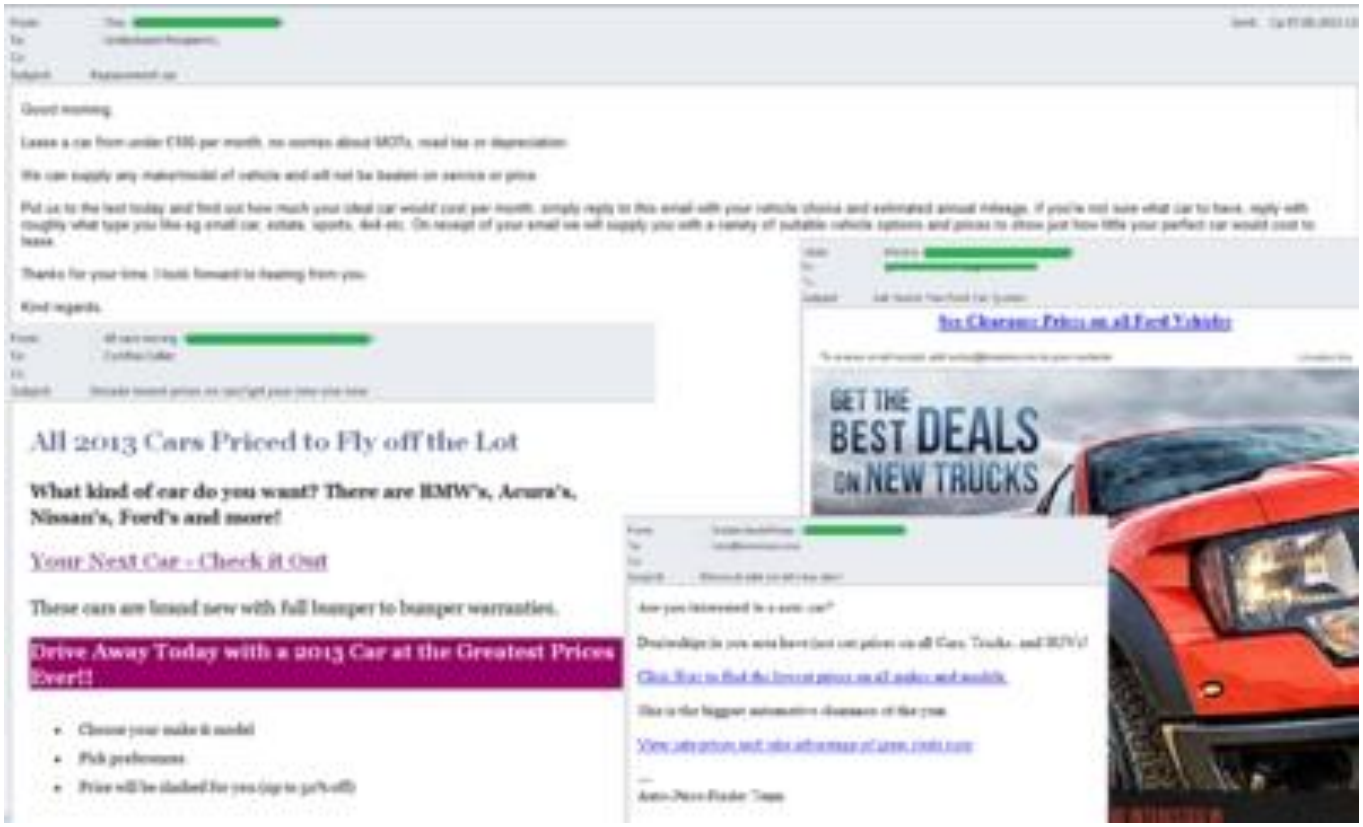
2013 年 8 月，垃圾邮件形势变得更加严峻：欺诈和恶意邮件的数量大幅增加，与总体垃圾邮件量的下降形成对比。

在新学年即将到来之时，“返校”成为垃圾邮件发送者比较喜欢的主题之一——八月，我们监测到各种学生用品的广告。也有很多垃圾邮件是关于运动和健康的生活方式的。汽车贸易商也借助群发邮件来为汽车销售和相关的服务和配件做广告。

发给驾车人的垃圾邮件

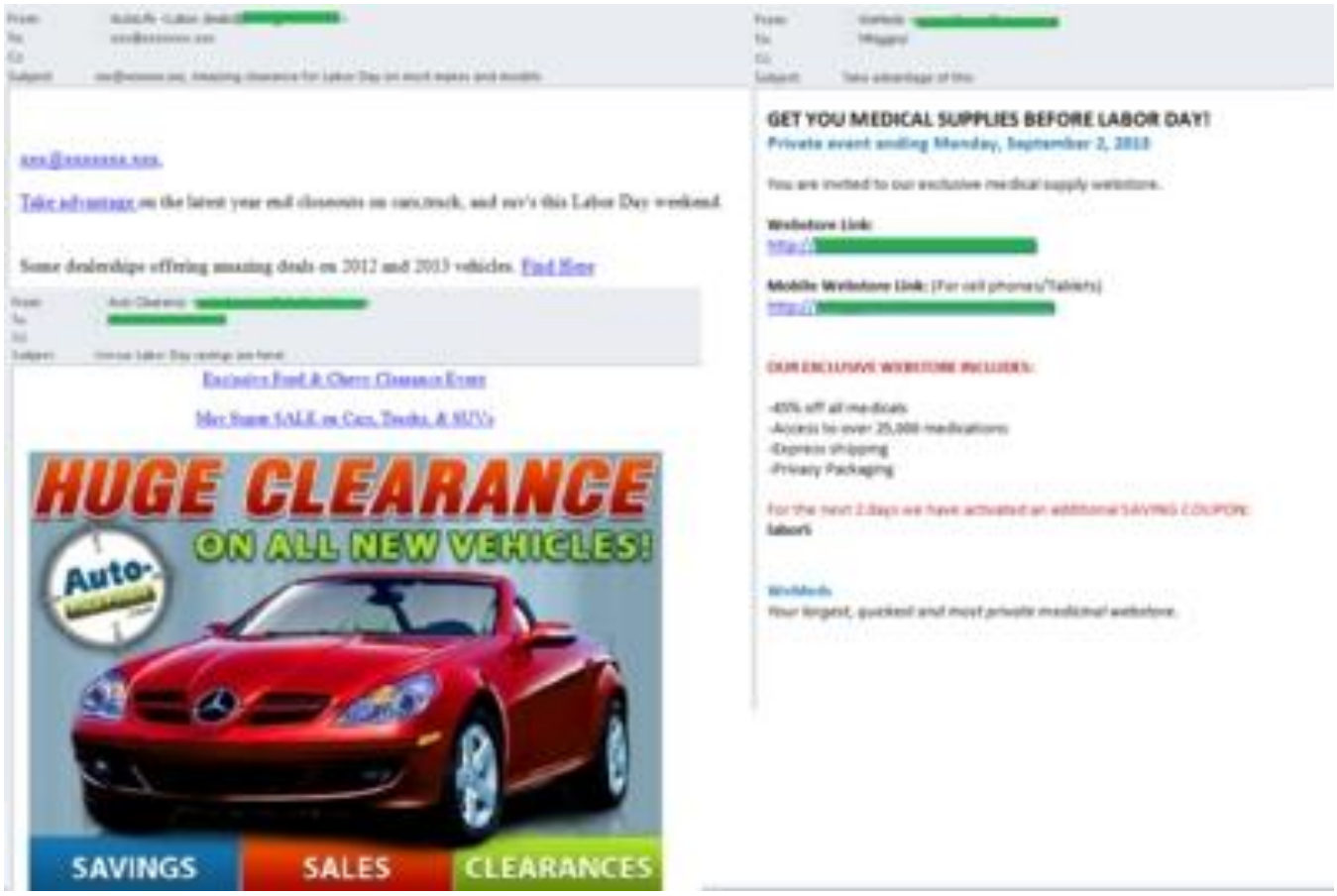
对于很多人来说，汽车不仅是一种交通工具，也是一种生活方式，需要大量时间和金钱去养护。垃圾邮件发送者很乐于开发人们对汽车的兴趣： 8 月份我们注意到大量促销类群发邮件除了提供标准的销售和维修服务外也包括一些非常新颖的与汽车相关的服务。例如，一次群发邮件的作者要求收件人参加大师课堂，学习如何制作汽车形状的蛋糕。

然而，英语类垃圾邮件通常包含廉价汽车租赁服务和知名汽车品牌的销售广告。



劳动节

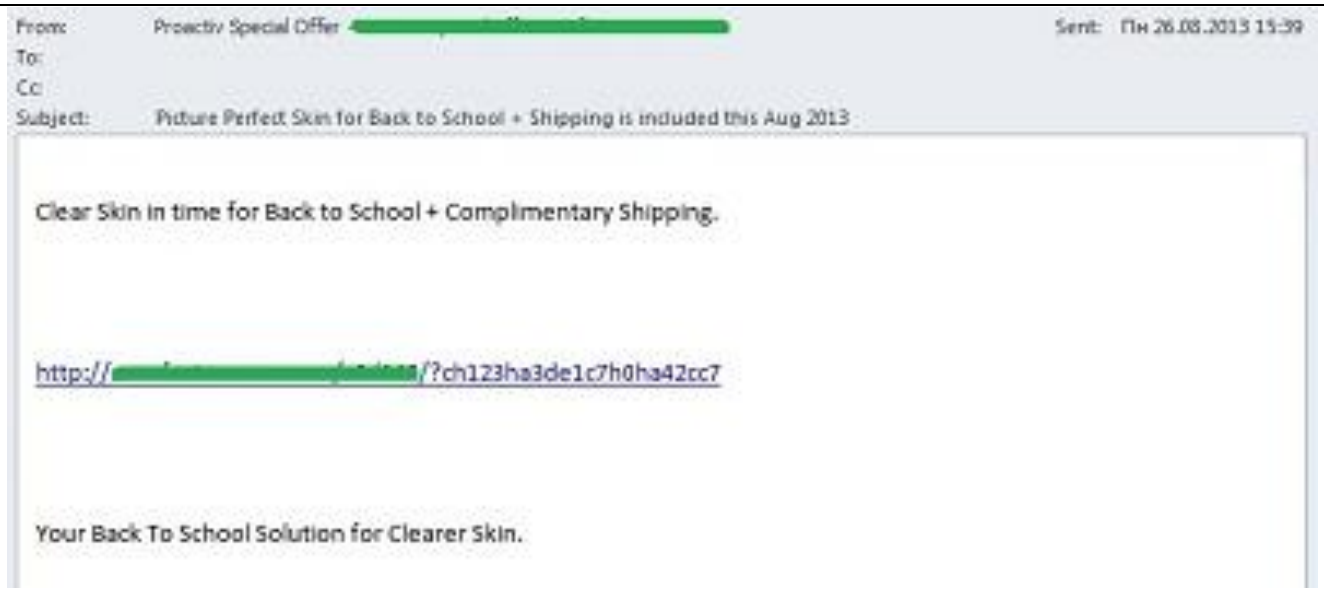
9 月的第一个周一是美国的劳动节。大多数美国人将劳动节看作是夏季结束的象征，并且是传统的夏季用品打折时间。当然了，垃圾邮件发送者会利用这一点， 这个八月，他们积极地传播汽车和药品打折的广告。为了吸引眼球并说服用户不要延误了购买时间，垃圾邮件发送者发送大量包括专属密码的邮件，许诺有此密码即 可享受额外的折扣。



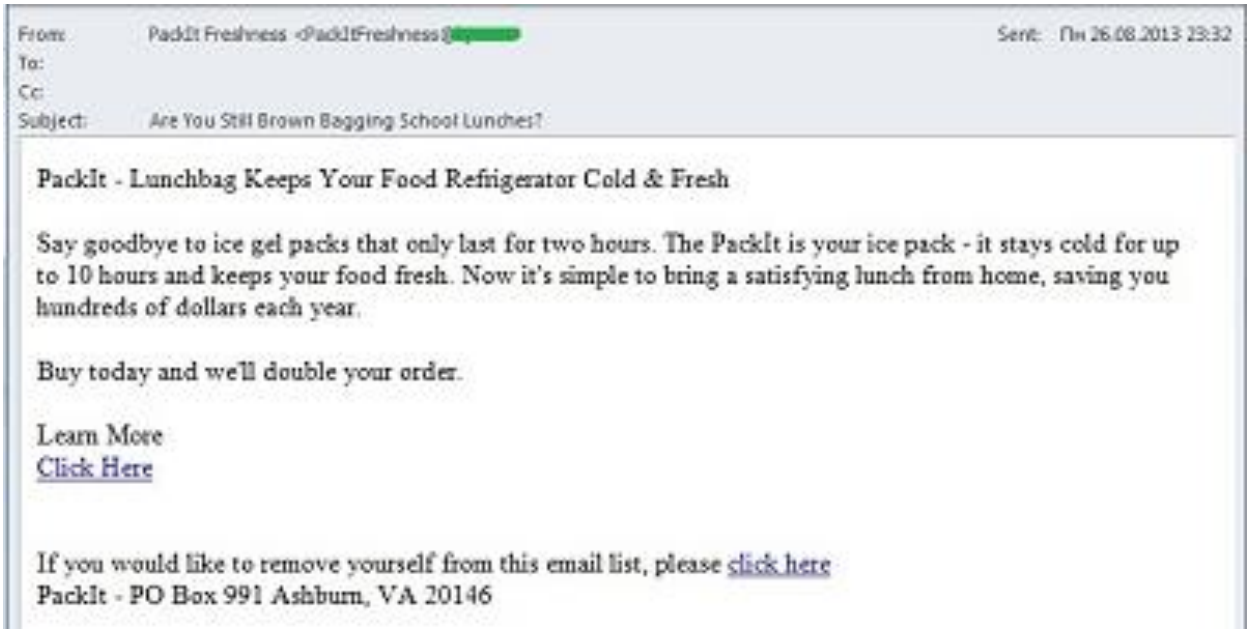
返校啦!

也许人们已经猜到了，8 月份全世界垃圾邮件发送者亲睐的主题是“返校”。新学年开始成为这个月的主题，各种学生用品在网上进行促销。

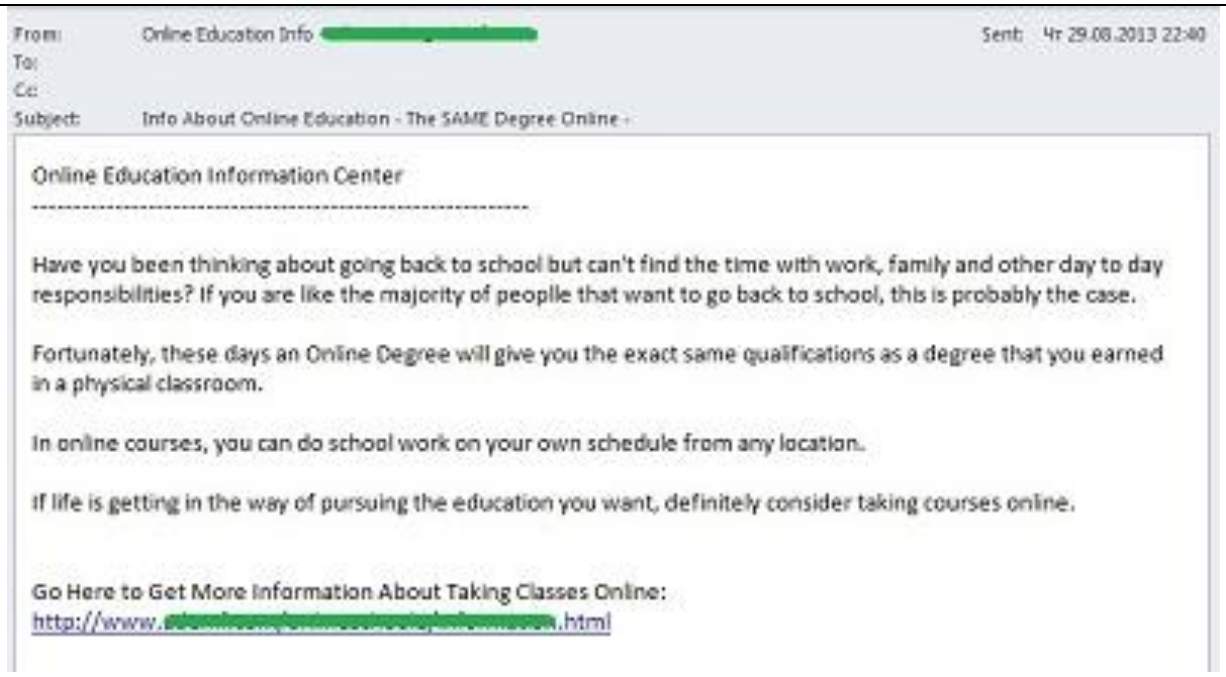
然而，有的情况是，广告商品与教育过程一点关系都没有——垃圾邮件发送者只是利用这个主题将人们的注意力吸引到他们正在做广告的产品。例如，我们发现 有一个提供护肤品的群发邮件。这些邮件表面看上去是为了让接送孩子上学的妈妈们看上去更漂亮，提供快速生效的化妆品，可以起到神奇的效果。但在这些邮件里 包含一个很长的链接，将用户重新指引到一个网站，用户需要在这个网站上选择产品寄送地区。然后地区的选择激活了一个包括出售者联系方式的页面。同时，重新 指向的这些域名在此次群发邮件活动后一周就会失效。



“你仍然是自备午餐吗”另一个群发活动的主题这样写道。这次群发活动利用学校主题来为一种特别的保鲜盒做广告。邮件作者承诺这种保鲜盒可以为食物保鲜 10 个小时。邮件中包含的单个域名是上个月才创建的。



8 月份我们仍然能看到为在线教育做广告的群发邮件。但是不同于之前的群发邮件是关于大师和博士课程的，新学年开始前的垃圾邮件是关于给考试未及格的学生提供在线教育机会。


From: Online Education Info [redacted] Sent: Чт 29.08.2013 22:40
To:
Cc:
Subject: Info About Online Education - The SAME Degree Online -

Online Education Information Center

Have you been thinking about going back to school but can't find the time with work, family and other day to day responsibilities? If you are like the majority of people that want to go back to school, this is probably the case.

Fortunately, these days an Online Degree will give you the exact same qualifications as a degree that you earned in a physical classroom.

In online courses, you can do school work on your own schedule from any location.

If life is getting in the way of pursuing the education you want, definitely consider taking courses online.

Go Here to Get More Information About Taking Classes Online:
http://www.[redacted].html

这些垃圾邮件的作者突出强调在线教育的优势：学习时间灵活，可以在家工作。如果需要更多信息，收件人会被指引到一个国外的网站，除了学位课程，这个网站也提供其他的非教育性质的服务。

医药类垃圾邮件

8 月份的垃圾邮件中还有很大一部分是与健康相关的。减肥药仍然是最受欢迎的主题之一。上个月我们看到减肥药的链接地址有俄罗斯的，也有英语互联网的。

英语减肥药类群发邮件包含的链接地址是不久前创建的。每封邮件中的链接地址都是不同的。用户点击链接后就会来到一个网站，这个网站有关于这个药品的详细说明及购买期限等。除了文本信息还附带一个宣传片——展示了药品的神奇功能并提供了已经尝试此药品的人们的推荐。


From: Natural Discovery <CadenceRichardson@[redacted]> Sent: Пн 26.08.2013 18:08
To:
Cc:
Subject: Report: Nutritional weightloss - Celeb's Doc Digs-in

Important Fitness Advice: How to get that shape you always dreamed of? - August 26, 2013

Named as the newest fastest fat burner by health experts across the nation.

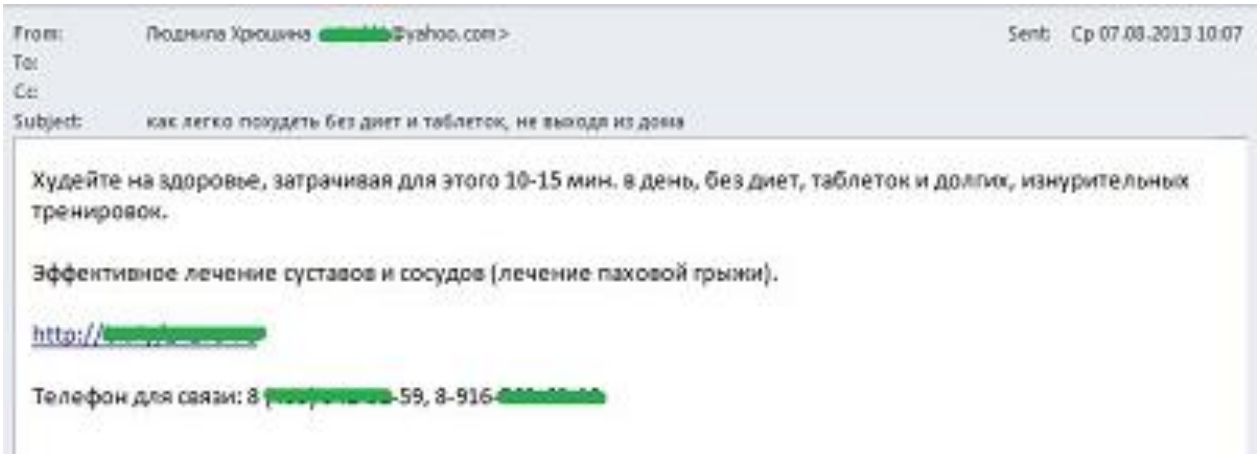
It's the newest craze in the market of dietary supplements.

It hinders fat production while suppressing your appetite,

and can help you lose weight without diet or exercise.

To find out how, take a look at Doc Oz's episode where he digs deep into it:
http://www.[redacted].php

俄罗斯语的垃圾邮件主要包含一个短小的链接，将用户指引到一个广告网站。他们常常为订购商品提供联系信息。


From: Людмила Хрюшина [redacted]@yahoo.com> Sent: Ср 07.08.2013 10:07
To:
Cc:
Subject: как легко похудеть без диет и таблеток, не выходя из дома

Худейте на здоровье, затрачивая для этого 10-15 мин. в день, без диет, таблеток и долгих, изнурительных тренировок.

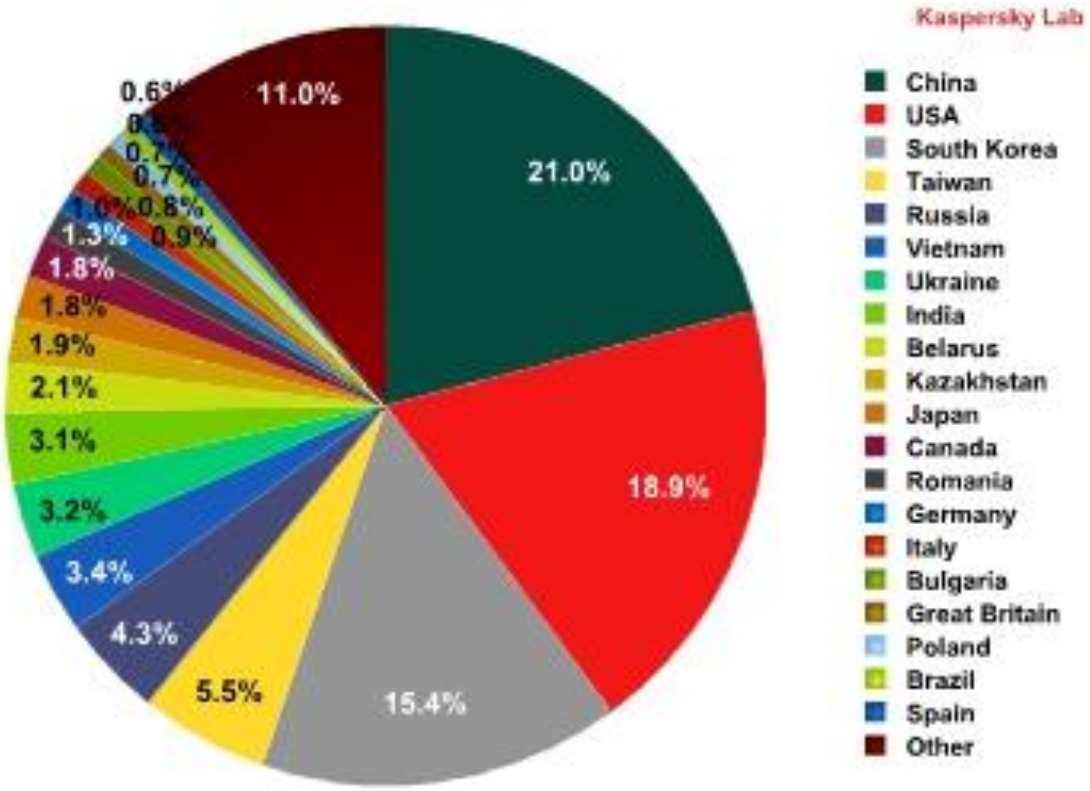
Эффективное лечение суставов и сосудов (лечение паховой грыжи).

http://[redacted]

Телефон для связи: 8 [redacted]-59, 8-916-[redacted]

垃圾邮件来源的地理分布

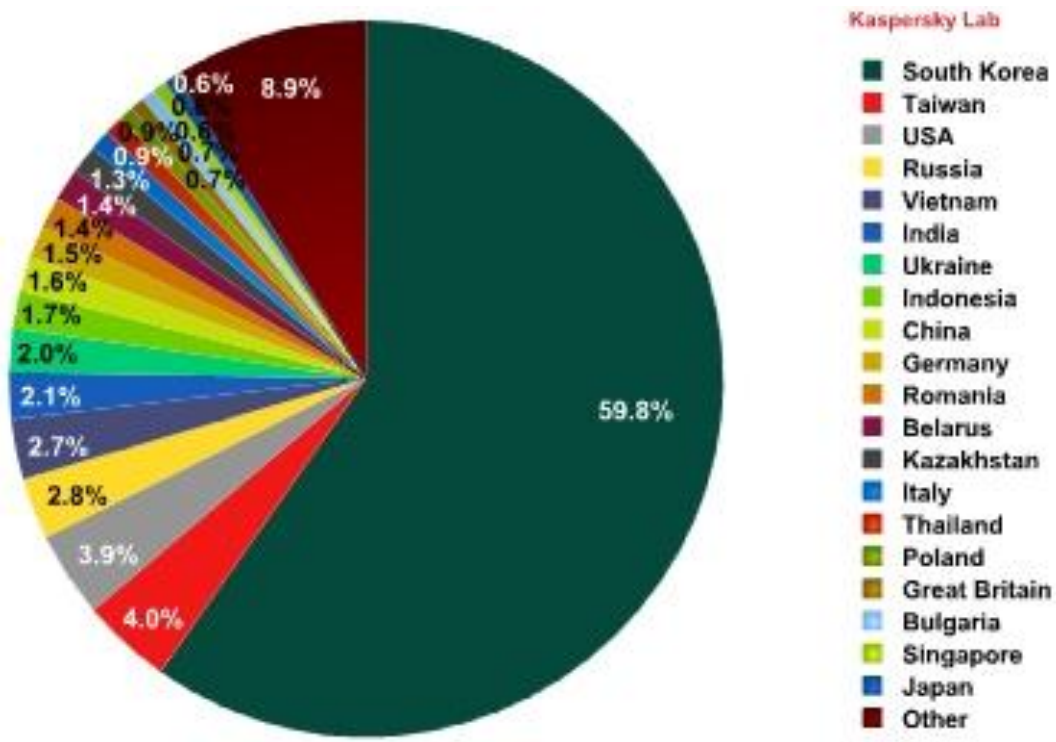
2013 年 8 月，垃圾邮件来源国前三名是：中国仍然是第一名，垃圾邮件占比 21%，比上月下降了 2.4 个百分点;美国第二，垃圾邮件占比 19%，比上 月提高了 1 个百分点;韩国第 3，垃圾邮件占比 15.4%，比上月增加了 0.4 个百分点。这三个国家的垃圾邮件总量占全球垃圾邮件的 55%。



台湾仍像 7 月一样，位列第四，垃圾邮件占比 5.5%，上升了 0.1 个百分点。俄罗斯垃圾邮件占比提高了 2 个百分点，为 4.3%，从第 10 名前进到第 5 名。

日本(1.8%)在增加了 0.9 个百分点后也前进了五个名次，现在是第 11 名。如果此增长态势继续到下个月，日本有可能进入前十。

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。

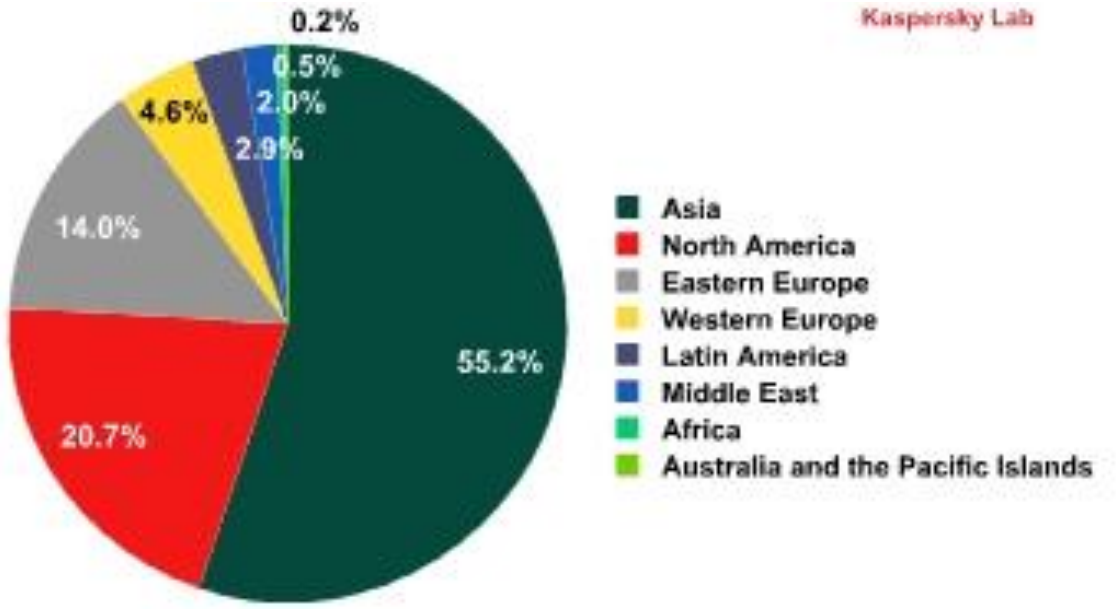


8 月份，韩国仍然是向欧洲发送垃圾邮件最多的国家(60%):垃圾邮件占比上升了 2.6 个百分点。紧随其后的是台湾(4%)和美国(3.9%)。

针对欧洲用户的垃圾邮件来源国排名中 ,俄罗斯(2.8%)第四 :上升了 1.8 个百分点——跃入前十。越南(2.7%)与上月相比下降了 0.7 个百分点，在排名中下降到第五名。

前十名中还包括第八名的印度尼西亚，而罗马尼亚(1.4)从第六名下降到第十一名已不再列表中。德国(1.5%)位列第十，与上月相比几乎没有变化。

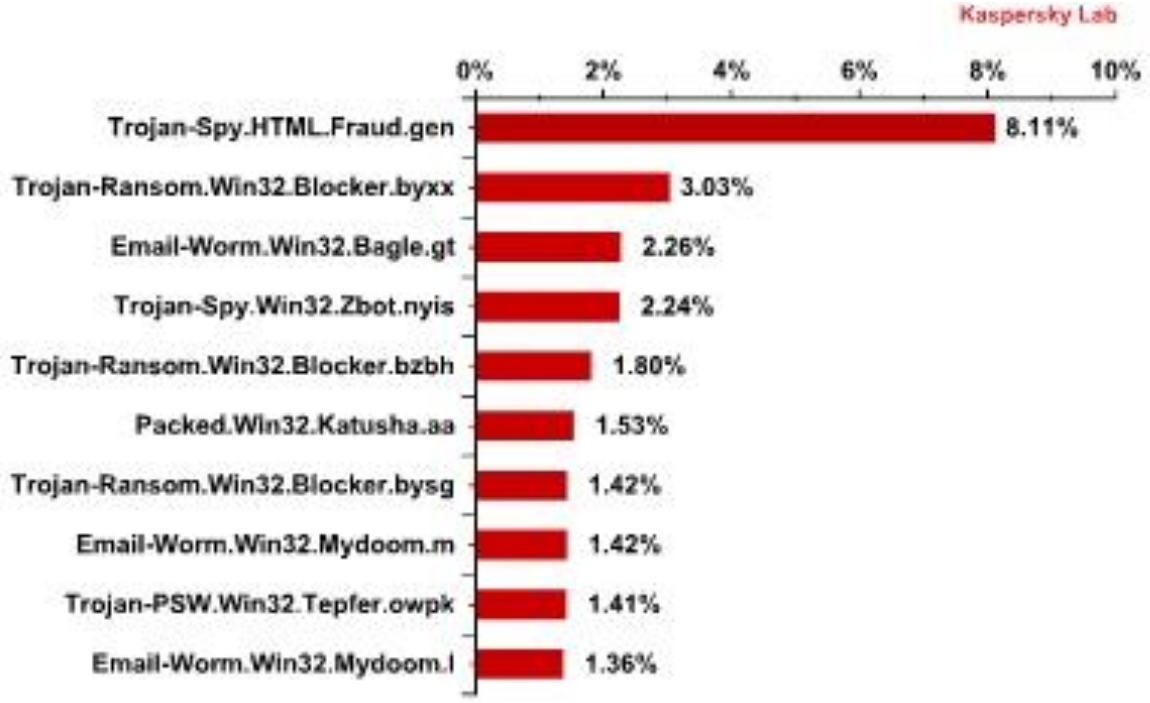
8 月，来源亚洲地区的垃圾邮件略有增加，泰国(0.9%)、新加坡 (0.6%) 和日本(0.6%)进入向欧洲用户发送垃圾邮件来源国的前二十。



8 月，亚洲(55.2%)仍然是最大的垃圾邮件来源地区。像上月一样，垃圾邮件来源地区前三名也包括北美(21%)和东欧(14%)：除了北美上升了 几近 1 个百分点之外，来源这些国家的垃圾邮件占比没有特别大的变化。西欧(4.6%)和拉美(3%)分列第四名和第五名。

邮件中的恶意附件

8 月，检测到的恶意附件占总邮件量的 5.6%，比 7 月增加了 3.4 个百分点。



Trojan-Spy.html.Fraud.gen仍然是传播最广泛的恶意程序(8.1%)。它以HTML页面的形式出现，模仿知名银行或 e-pay 的注册表格，并被钓鱼者用来为在线银行系统窃取用户凭证。

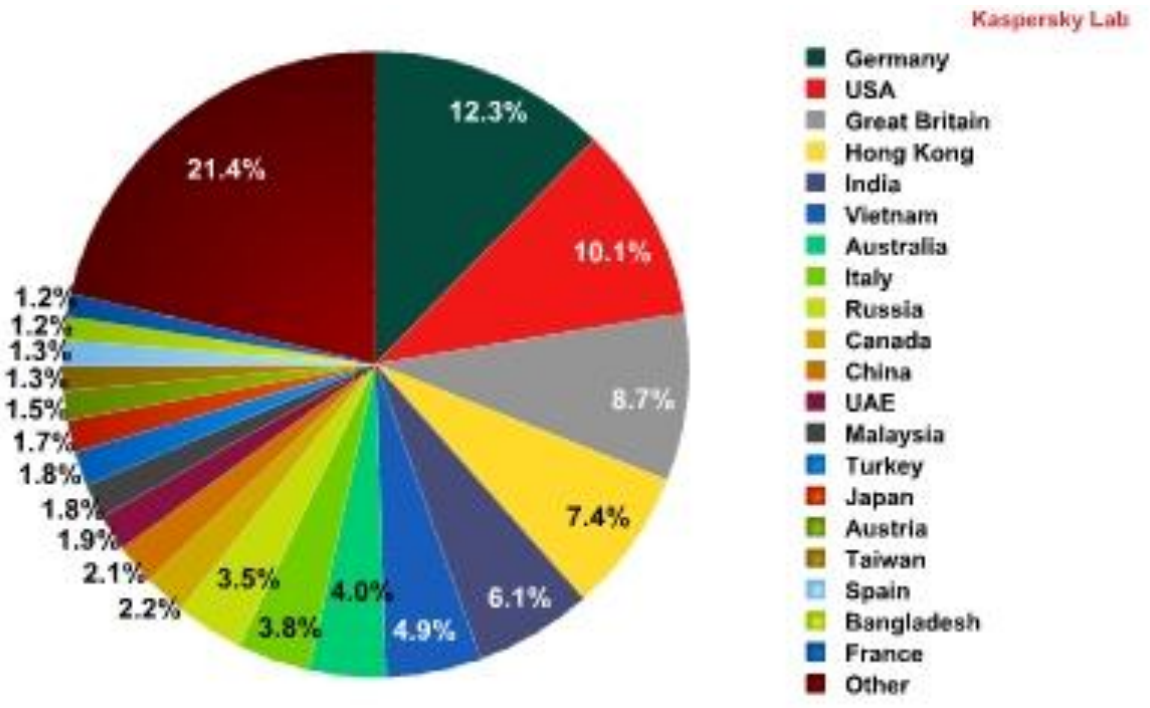
8 月份的排名包括 4 个 Trojan-Ransom.Win32.Blocker 变体。其中的三个——Trojan-Ransom.Win32.Blocker.byxx (3%), Trojan-Ransom.Win32.Blocker.bzbh (1.8%) 及 Trojan-Ransom.Win32.Blocker.bysg (1.4%)——分别排名第 2、第 5 和第 7。设计这些恶意程序是用来从用户那里敲诈勒索金钱的。他们阻止了运营系统的工作并提供了一个标语，指导如何开启计算机。例如：告诉用户向一个收费号码发送文本信息。

Email-Worm.Win32.Bagle.gt (2.3%)排在第三位。此邮件蠕虫自发到受害人的联系人列表，并以附件的形式分布。它也可以将其他恶意程序下载到用户电脑

排名第四位的是 Trojan-Spy.Win32.Zbot.nyis (2.2%)，它是臭名昭著的 Trojan-spies Zbot (ZeuS)的变体，用来窃取机密信息，包括信用卡信息。

在 8 月份的排名中，Worm.Win32.Mydoom.m (1.4%)仍然第 8。除了自我扩散之外，此恶意附件向搜索引擎发送隐藏的搜索请求，以增加网站流量和排名。

Mydoom 家族的另一个变体——Email-Worm.Win32.Mydoom.l (1.4%)——在 10 大恶意程序排名中排在最后。此蠕虫以邮件附件的形式在互联网上分布。它的主要功能是通过被感染的计算机来收获邮件地址，这些邮件地址随后可以被用于群发邮件。它也有“后门”能力。



在恶意邮件的目标国家排名中，8 月份德国(12.3%)排在了第一位，将上月的第一名美国(10.1%)挤到了第 2 位。英国(8.7%)第三。

印度(6.08%)从第 3 下降到第 5。俄罗斯(3.48%)上升了 1 个百分点，位列第 9 名。澳大利亚的占比下降到 4%。加拿大以 2.2%排名第 10。

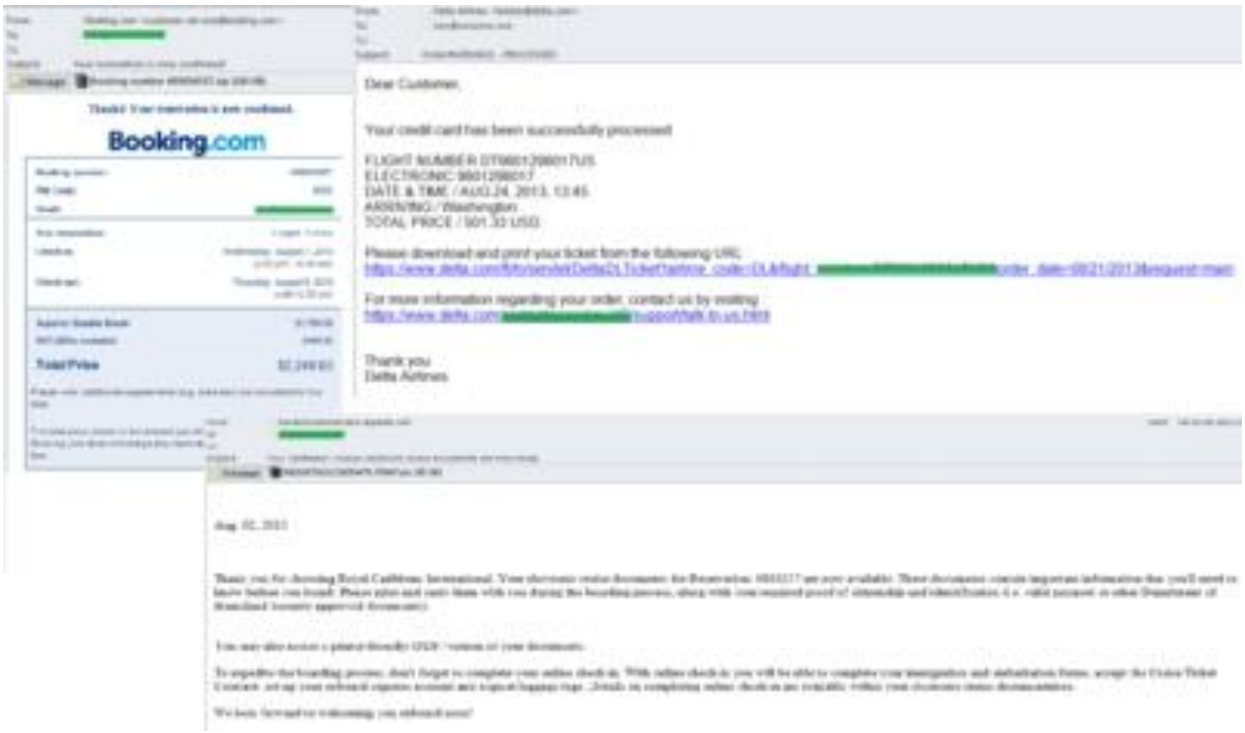
其他国家的排名变化很小。

恶意垃圾邮件的特征

虽然假期就要结束了，但是诈骗者仍在冒用行业内大公司的名字狂轰乱炸发布虚假的飞机票和酒店预订信息。像 booking.com 和 Delta Air Lines 这样的知名公司就经常被垃圾邮件发送者利用发布虚假的通知。发件人的地址通常看上去非常可信，所以就会诱导收件人打开这类邮件。

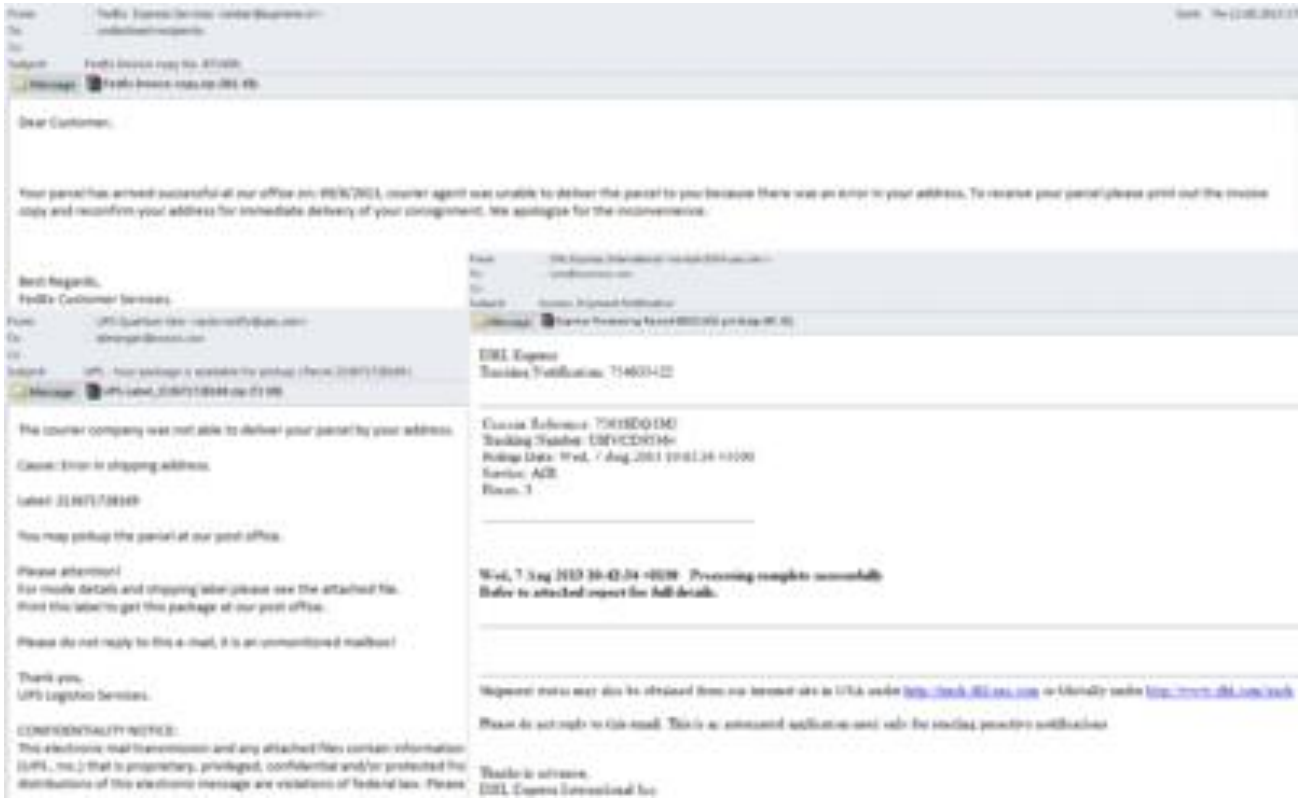
发送的邮件声称代表 booking.com 通知用户他的酒店预订信息已经确认 ,并且提供了订单信息，包括入住和退房的日期和酒店房间总的花费。此诈骗 邮件是按照官方网站的风格设计的，这种邮件和另外一种类似但不同。另有邮件模仿 Delta Air Lines 发送通知，告诉收件人他的信用卡支付已经生效并提供了编号、日期和航班费用，并要求收件人点击链接打印票据。但是如果收件人这样做了，就会有一 个恶意文件下载到电脑上。声称发自 booking.com 的邮件在附件中包含一个恶意文件。在上述两种情况下，都是使用包含 Trojan- PSW.Win32.Tepfer 的恶意文件窃取用户名和密码。

一段长时间的沉寂之后，诈骗者在 8 月份又开始冒充皇家加勒比国际邮轮发送恶意通知。恶意邮件通知用户所预订邮轮的电子文档已准备好。这些文档包含乘客 在登船前所需了解的“重要信息”并且需要和乘客的护照和文件保存在一起。实际上，此电子邮件包含 Backdoor.Win32.Androm.qt 恶意文 档，Backdoor.Win32.Androm.qt 是 Backdoor.Win32.Androm 的一个变体，用来偷偷的控制用户的计算机并将此计算 机添加到僵尸网络上。



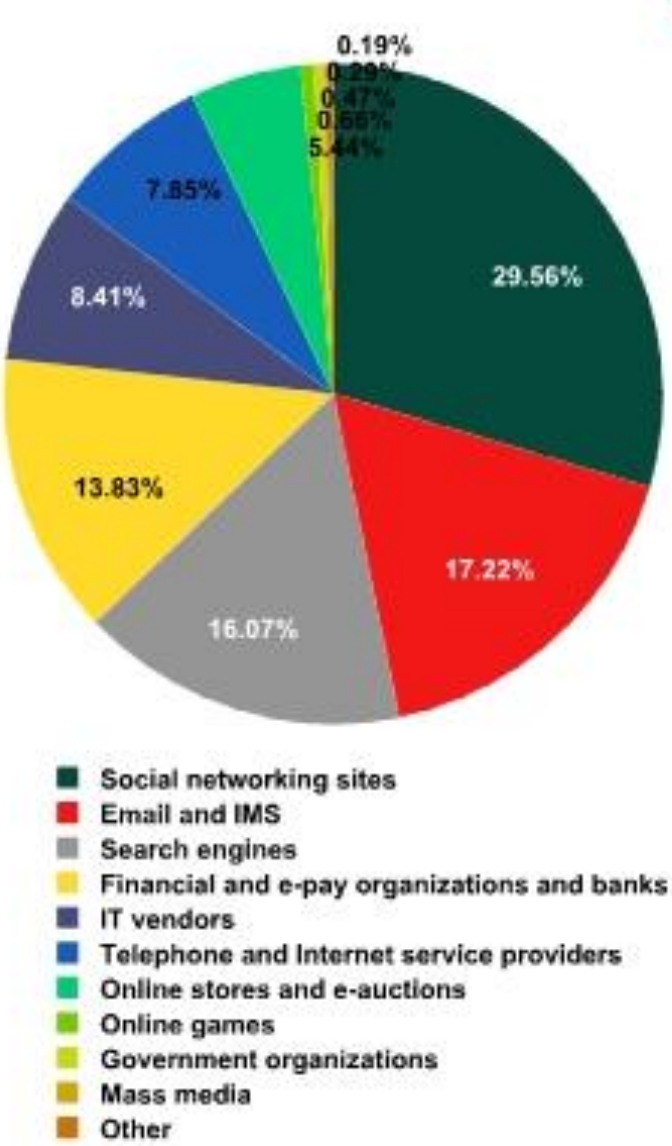
虚假通知常常利用知名国际快递服务机构的名字，例如 FedEx, UPS 及 DHL。这些虚假的通知单告诉收件人有一个邮寄的包裹因为邮件地址错误不能递送。若想收到这个包裹，收件人需要打印附件文档并给快递公司打电话确认信息， 包括邮寄地址等。恶意文件也会隐藏在声称含有包裹细节信息的文档里，而包裹信息根本不存在。垃圾邮件发送者努力使虚假通知看上去合法并且不仅使用一个表面 看上去非常真实的收件人地址，也提供不存在的单号信息、快递公司官网的真实联系方式和隐私通知单的复件。

所附文档通常是恶意文件。例如，虚假 FedEx 通知单所附的文档包含一个可执行的文档，带有来自 ZeuS/Zbot 家族的木马程序。此恶意程序被用来 窃取用户的个人信息和支付及银行账户密码。代表 UPS 发送的虚假通知包含 Trojan-PSW.Win32.Tepfer.pnfu 恶意程序，用来窃取用 户的登录名和密码。在一次声称来自 DHL 的群发邮件活动中发现了属于 Backdoor.Win32.Androm 家族的另一个恶意程序 。诈骗者利用此恶意程序进入受害者的电脑。



网络钓鱼

8 月份商业活动有所减少，因此垃圾邮件发送者的广告定单就会减少，这样他们的热情就转移到诈骗信息。结果，与 7 月份相比，全球垃圾邮件中钓鱼邮件的比例增加了 10 倍，达到 0.013%。



钓鱼者的前 100 个目标组织，按类别分布

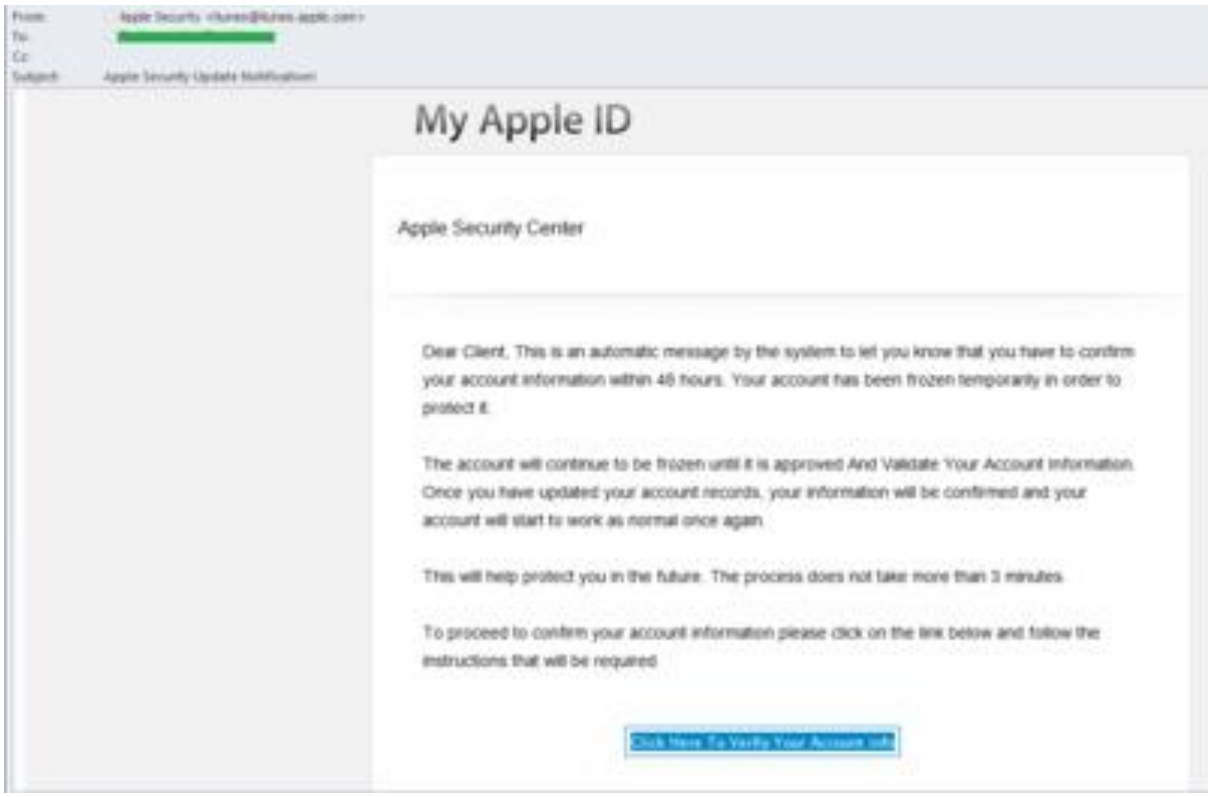
排名是基于卡巴斯基实验室的反钓鱼监测，每次用户尝试点击一个钓鱼链接就会激活反钓鱼监测，无论此链接是在垃圾邮件中或网页上。

网络钓鱼最喜欢攻击的目标在 8 月份没有什么变化。社交网站仍然位于榜首，仍然像 7 月份一样占比 29.6%。

邮件和即时信息仍排第二(17.2%) :下降了 0.4 个百分点。同时搜索引擎的百分比略有增加(16.1%)，仍在排名第 3。

金融和电子支付(13.8%)，IT 厂商(8.4%)，电话和互联网服务提供商(7.8%)，在线商店和电子拍卖(5.4%)和在线游戏(0.7%)排在 4-8 名。

8 月份，苹果是钓鱼者主要攻击的目标之一。我们频繁的遇到冒充来自苹果公司的邮件，而实际上这些是钓鱼邮件，用来欺骗用户并窃取登录名和密码。例如， 有些邮件中写道用户有 48 小时的时间可以确认 iTunes 账户细节。为了开通这个账户，收件人不得不点击邮件中的链接并按照网站上的说明去做。垃圾邮件发 送者努力给用户提供一种虚假的安全感，指出此信息是自动创建的。然而，在第三方网站上确认账户信息的请求和个人地址的缺失都应该引起用户警觉其为诈骗信 息。



结语

8 月份，世界垃圾邮件的比例下降到 67%，下降的原因可能由于每年夏季商业活动减少导致广告量减少。然而，我们仍然看到很多关于租赁或出售汽车、医药和健康的生活方式的群发邮件。另外，垃圾邮件发送者利用新学年的和美国劳动节的主题来为不同的产品销售做广告。

这个夏季垃圾邮件呈现犯罪化趋势，包含恶意文件的欺诈邮件数量上升。8 月份，窃取金融信息的落雪木马在恶意垃圾邮件中广泛传播。然而，Trojan-Ransom.Win32.Blocker 蠕虫家族也非常盛行，可以在最常检测到的恶意程序中发现一些变体。

假期中垃圾邮件发送者继续冒充大公司传播虚假酒店预订和飞机票预订信息。快递公司也吸引了诈骗者的注意，其名字常被用于网络钓鱼和传播恶意软件。

钓鱼者用苹果产品和服务窃取用户登录名和密码。俄罗斯互联网上，诈骗者模仿公共组织的官方服务，利用垃圾邮件来创建并推广在线服务，向用户窃取个人信息和金钱。

钓鱼者最易攻击的目标排名在 8 月份没有什么变化。像之前预计的一样，社交网站、电子邮件和即时通讯服务仍保持在前几名。在夏季的最后一个月，孩子和学 生使用社交网站和电子邮件服务仍然频繁，保证了钓鱼者对这个版块兴趣不减。然而到了 9 月份，商业活动开始复苏，垃圾邮件发送者的兴趣将从社交网站转移到金 融机构，对银行机构的攻击将会增加。同时，诈骗和恶意邮件的比例将有可能减少。

（反垃圾信息中心编译，源文网址：

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