【卡巴斯基】

[卡巴斯基 2013 年 7 月垃圾邮件报告]

【反垃圾信息中心编译】

2013/12/13

目录

七月份的数字

七月垃圾邮件流量比六月的流量提高了 0.1%，为 71.2%。

网络钓鱼电子邮件比六月相比减少了一半多,平均为 0.0012% 。

含有恶意附件的电子邮件占邮件总量的 2.2%，比六月提高 0.4%。

聚焦垃圾邮件

垃圾邮件热门话题

在七月，我们发现垃圾邮件发送者继续在利用大新闻进行垃圾邮件的传播，比如，英国皇室宝宝诞生，斯诺登事件。采取的手段与之前很类似：模仿新闻邮件，并附有恶意链接。

垃圾邮件发送者利用这些吸引用户的眼球的垃圾邮件上，比如利用英国皇室宝宝诞生给印刷设备和服务做广告。另外对这些服务还提供了一定的折扣。

斯诺登则被人用来做减肥产品的广告，他们在邮件内发送斯诺登的相关新闻，没有任何提及减肥的方法，然而，链接则指向广告页面。

斯诺登还被广泛利用在一个德语的 IT 安全系统的群发邮件上。因为斯诺登可以证明，互联网上的间谍行动是无处不在的。

Guten Tag, {user-name},

spätestens seit Edward Snowdens Enthüllungen weiss jeder, dass wir im Internet massiv bespitzelt werden.

500 Mio eMails werden allein jeden Monat mitgelesen!

Ist es nicht erschreckend, wenn jede private eMail, jedes Geschäftsgeheimnis mitgelesen wird?

Wenn jeder weiss, welche Webseiten Sie besuchen?

Sie können sich davor sofort schützen - mit ein paar wenigen Handgriffen.

Wie einfach das geht, lesen Sie hier:

http:

Sie können noch heute Ihre Privatsphäre wirksam schützen!

Lassen Sie dreiste Internet-Spitzel ab heute einfach aussen vor!

Viel Erfolg und sichere Grüsse,
Peter und das gesamte loos.de-Team

PS: Hier nochmal der Link für Ihren persönlichen Internet-Schutz: http:

Edward Snowden clearly said that what he fears for Russia abroad.

Journalists who got the interview in the hall were shocked by allegations Edward Snowden.

Come to us and you have familiarized many new details of this bustling business. - Read more >>

To date have all known Edward Snowden clearly said that what he fears for Russia abroad.

The journalists were in the hall were neither of which have failed to respond to spoken words.

Come to us and you have familiarized many fresh details of this popular business. - Read more >>

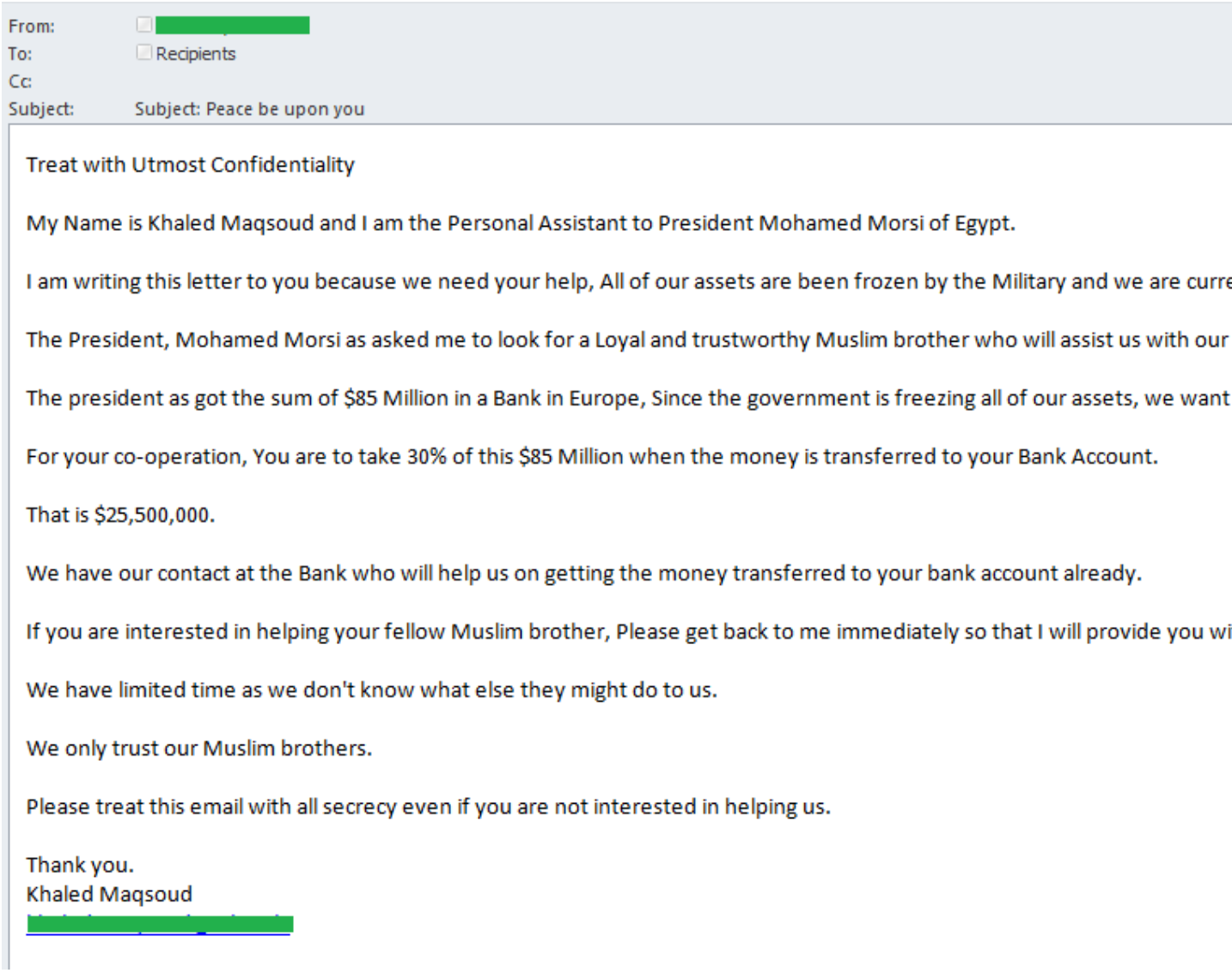
斋月

2013 年七月初开始进入穆斯林的斋月。每年我们都会受到利用这个主题的群发邮件。今年也不例外，我们收到了几个英文的群发邮件，内容不仅包括传统斋月的晚上餐馆和食品广告，还提供汽车和暑假的儿童活动的广告。

长期的热点——尼日利亚垃圾邮件

流行的“尼日利亚”邮件坐着一般都冒充是个著名的有钱人，可他们要么是死，要么是有亲戚正处于艰难的时刻。七月，埃及总统穆罕默德·穆尔西被推翻。在几天之内，我们收到了一批关于他的群发欺诈邮件。

电子邮件，据称是前总统秘书写的，宣称，穆尔西的所有帐户已经被冻结，被软禁的前总统和他的秘书在寻找一个可以转让总统的资金从一家欧洲银行到自己的帐户的穆斯林。当然，作为奖励，会提供一笔诱人的酬金。然而，传统的“尼日利亚”信件表明，受害者最终不仅仅是失望，还可能会被骗子骗走自己的钱。



From: [redacted]
To: Recipients
Cc:
Subject: Subject: Peace be upon you

Treat with Utmost Confidentiality

My Name is Khaled Maqsoud and I am the Personal Assistant to President Mohamed Morsi of Egypt.

I am writing this letter to you because we need your help, All of our assets are been frozen by the Military and we are curre

The President, Mohamed Morsi as asked me to look for a Loyal and trustworthy Muslim brother who will assist us with our

The president as got the sum of $85 Million in a Bank in Europe, Since the government is freezing all of our assets, we want

For your co-operation, You are to take 30% of this $85 Million when the money is transferred to your Bank Account.

That is $25,500,000.

We have our contact at the Bank who will help us on getting the money transferred to your bank account already.

If you are interested in helping your fellow Muslim brother, Please get back to me immediately so that I will provide you wi

We have limited time as we don't know what else they might do to us.

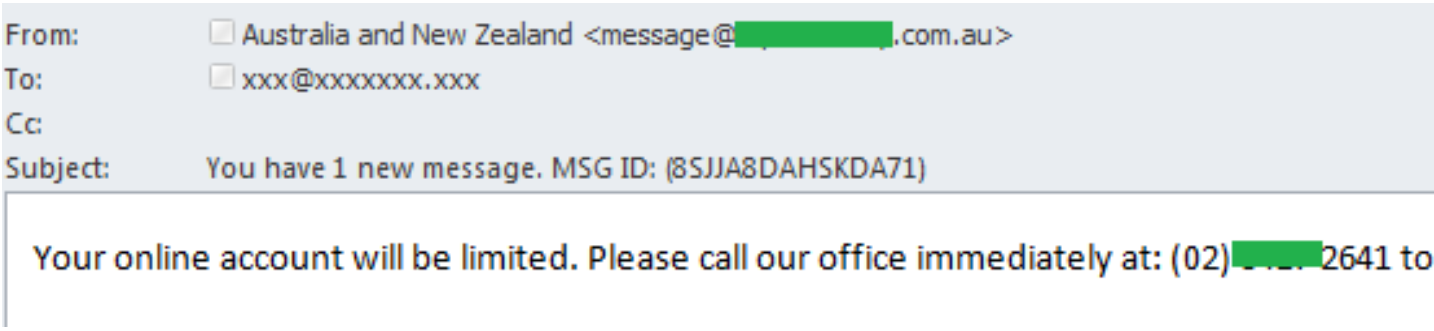
We only trust our Muslim brothers.

Please treat this email with all secrecy even if you are not interested in helping us.

Thank you.
Khaled Maqsoud
[redacted]

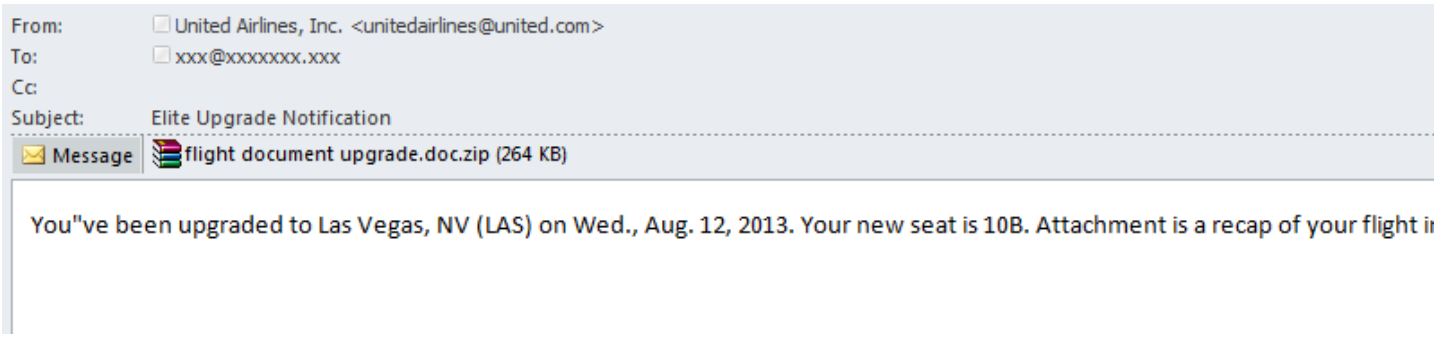
罕见的欺诈邮件

在 七月，我们捕获到的一封电子邮件，其中利用了很少见到的一种欺诈方法。用户收到据称是从澳大利亚和新西兰银行集团发送的通知邮件，告知他已被限制访问。要 恢复访问，收件人需要拨打在电子邮件中的电话号码。这样风险是显而易见的：它可能是一个高付费的号码，或者它可能通过电话实时诈骗。



恶意垃圾邮件

在旅游季的垃圾邮件是非常多的，我们收到了冒充各航空公司的恶意邮件。比如从“美国联合航空公司”的通知就被认为是假的。收信人会看到，即将乘坐的航班上，座位号已经改变，并附加了名为“flight document upgrade.doc.zip”更新的航班信息档案。这个文件包含 Backdoor.Win32.Vawtrak.a 恶意程序。



这个后门是窃取存储在浏览器， FTP 和电子邮件客户端的密码。该恶意软件还将用户的桌面截图发送给网络罪犯，并获得被感染计算机的完全访问权限，允许攻击者下载并运行各种文件。

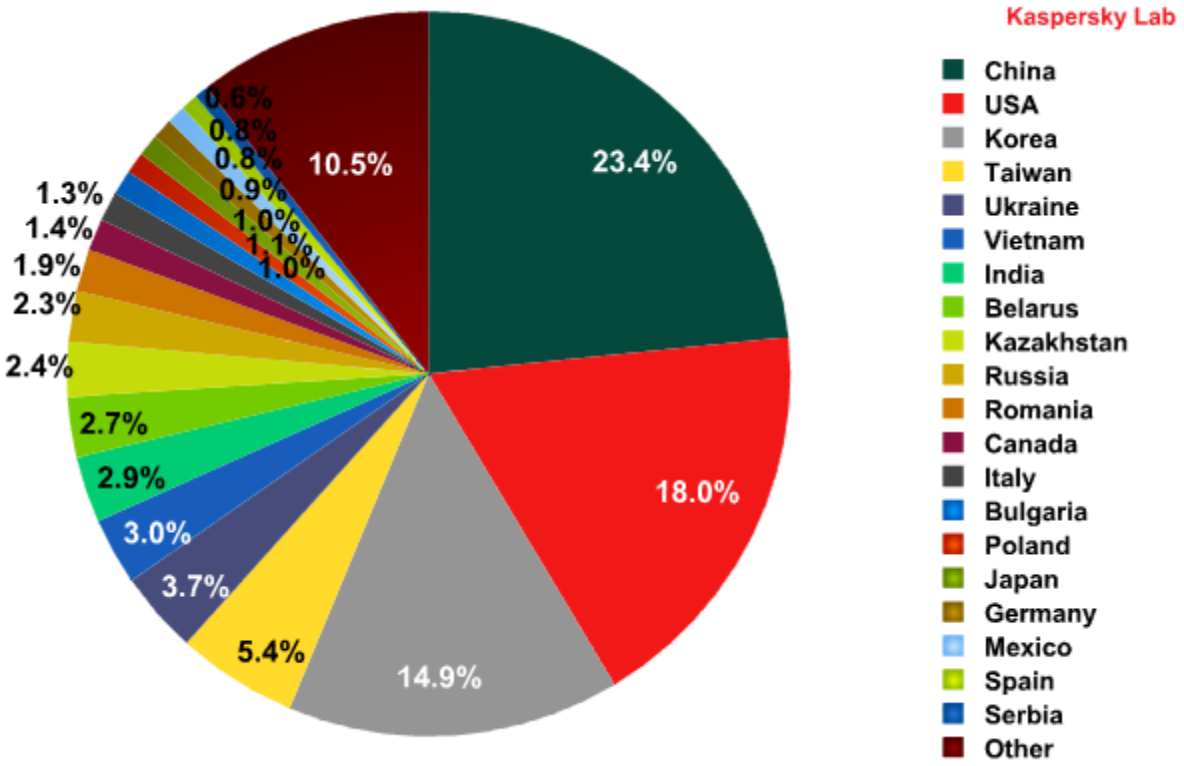
宠物商品及服务

七月，我们收到了关于宠物服务及商品的群发邮件广告。世界各地的人们都将自己的宠视为家庭成员，这位他们推广商品和服务提供了便利。这种邮件，往往是通过俄语和英语的垃圾邮件发送。

英语语言的垃圾邮件大多是宠物产品和便宜的食物。

垃圾邮件发送源地理分布

全球垃圾邮件发送国前三名在七月没有改变。

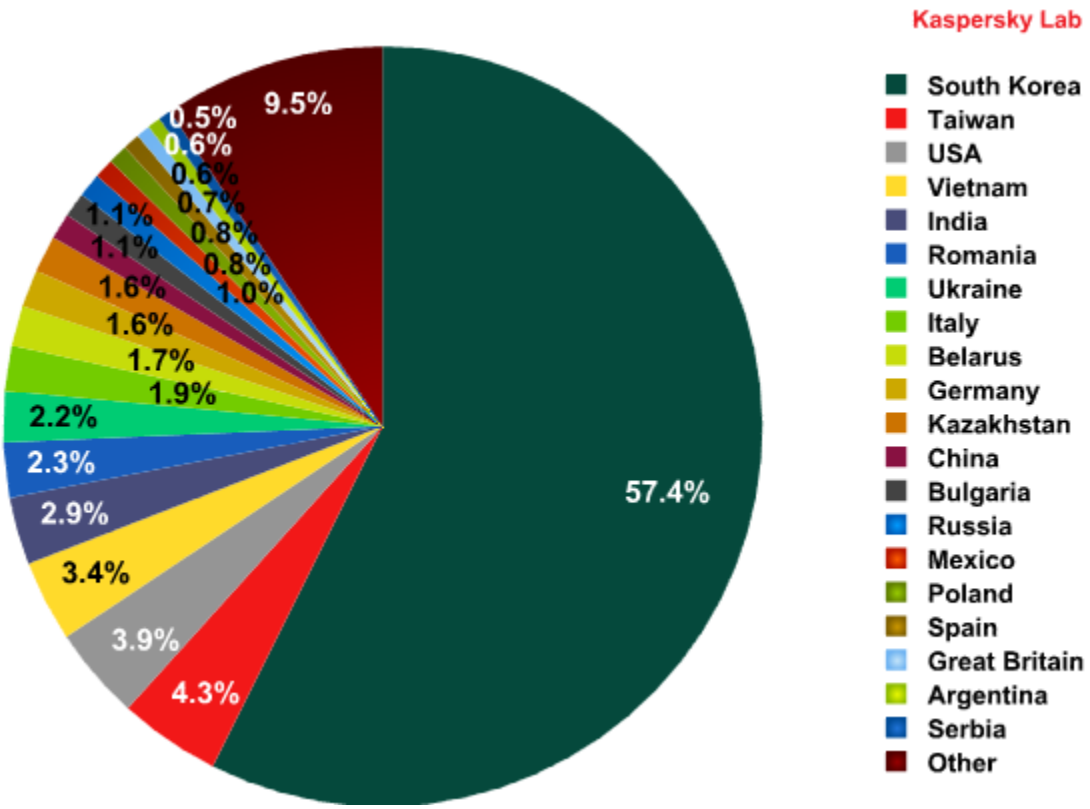


2013 年七月垃圾邮件来源国

中国排名第一，比上月（23.9%）略有下降，为 23.4% 。美国位居第二，占 18% ，同比增长 0.8%。韩国小幅增长 0.4%后，平均为 14.9%。前三名共生产了超过三分之一的世界垃圾邮件。

今年七月，印度增加了 0.4%，从第 10 上升至第七位，占 3%。日本从 2.7%降低至 0.96% ，下降了 1.74%，下跌至第十六位。俄罗斯重新进入前十名，发送了 2.3 %的垃圾邮件。

值得注意的是，罗马尼亚增长了 0.6%，平均为 1.9% ，从第十四位攀升至第十一位。

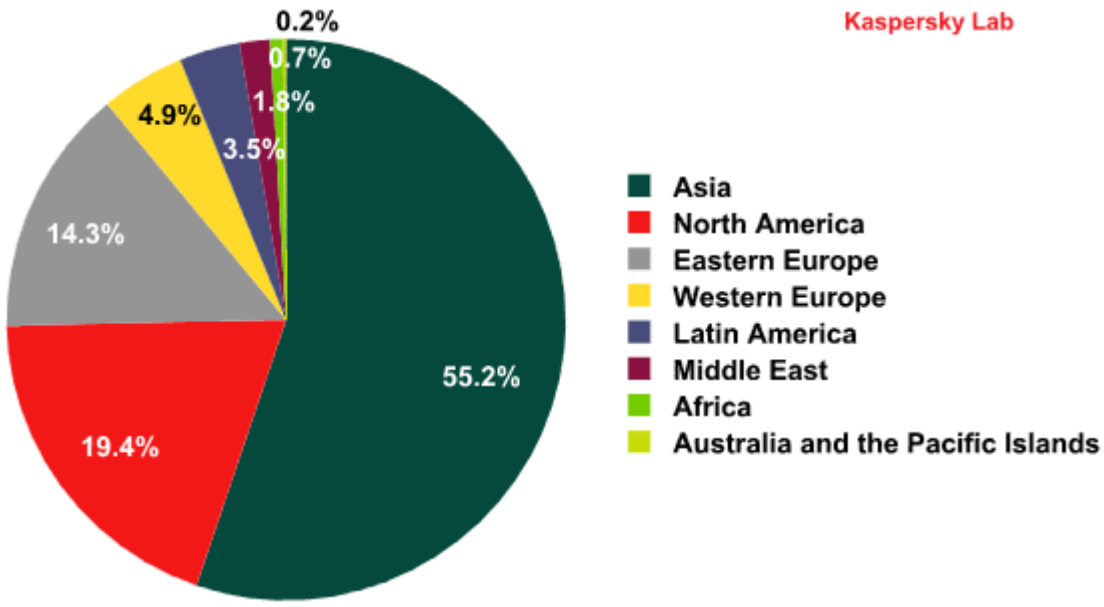


2013 年七月发往欧洲的垃圾邮件来源国

七月，排名几乎没有什么变化。韩国仍然发送欧洲用户垃圾邮件的主要来源，为 57.4%，增长了 2.1%。在未来一个月，可能继续保持增长趋势。台湾（4.3%）和美国（4%）分别为第二和第三。

意大利（1.9%）从第二位下降至第八位： 下降了 4.8%。

德国以 1.6%，名列第 10 位。

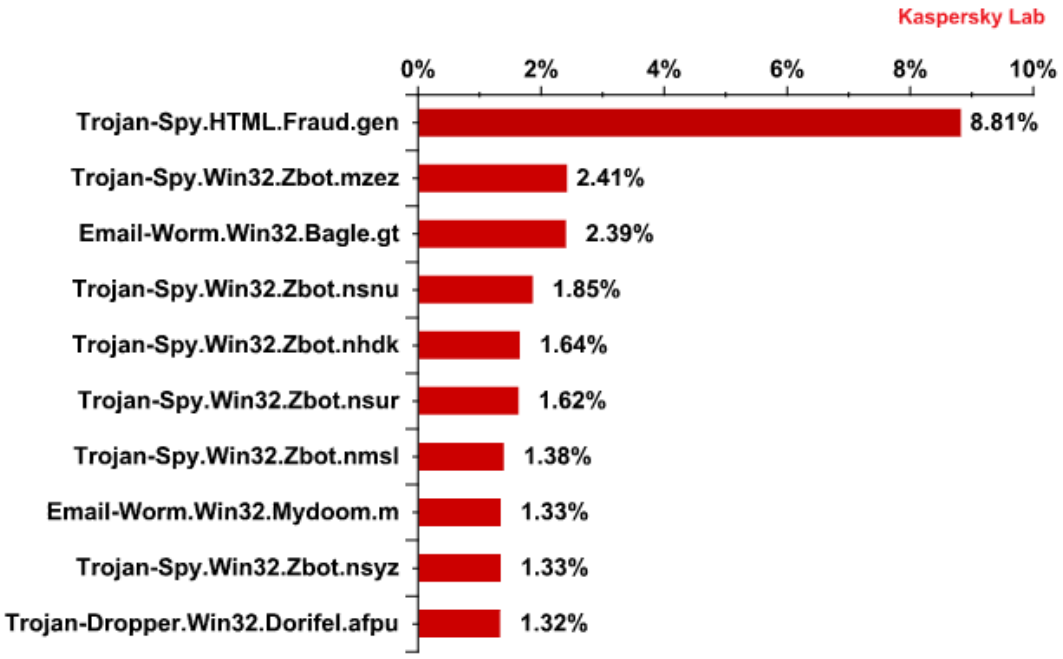


按地区分布垃圾邮件来源

亚洲（55.2%）仍然是垃圾邮件的主要来源地区，尽管下降了 2.1%。前三还包括北美（19.4%）和东欧（14%），分别增长了 0.7%和 1.1%。

含有恶意附件的垃圾邮件

七月，在 2.2%的电子邮件中检测到了恶意附件，比六月增加了 0.4%。

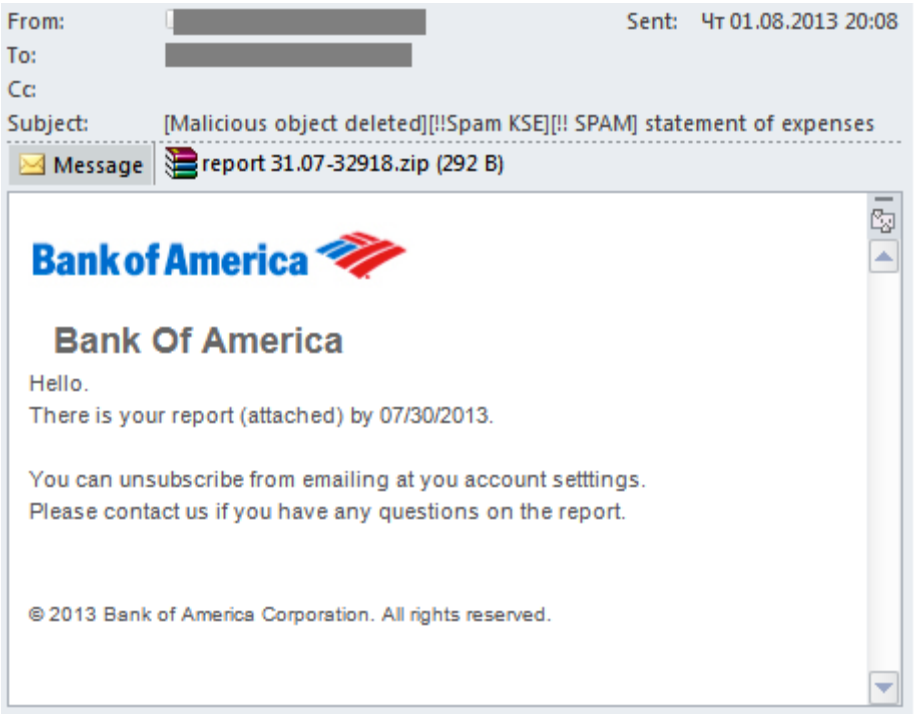


2013 年七月排名前十的通过电子邮件传播的恶意程序

七月 ,Trojan-Spy.html.Fraud.gen 依然是在电子邮件中出现的最普遍的恶意程序 ,增长了 2.9%。这个恶意程序模仿知名银行或电子支付系统的登记表格的 HTML 页的形式。用于网络钓鱼者盗取网上银行系统的用户信息。

前十名里有留个是 ZeuS / ZBOT 系列的程序。这是最流行的木马间谍之一，其变种在过去几年通过电子邮件大量传播。此木马旨在窃取用户的机密信息，包括他们的信用卡信息。

诈骗者最常使用的 ZeuS / ZBOT 系列的程序的首发是，冒充由银行，网上商店，社交网站或流行的送货服务发送的通知。这些通知的目的是诱使收件人打开恶意附件。



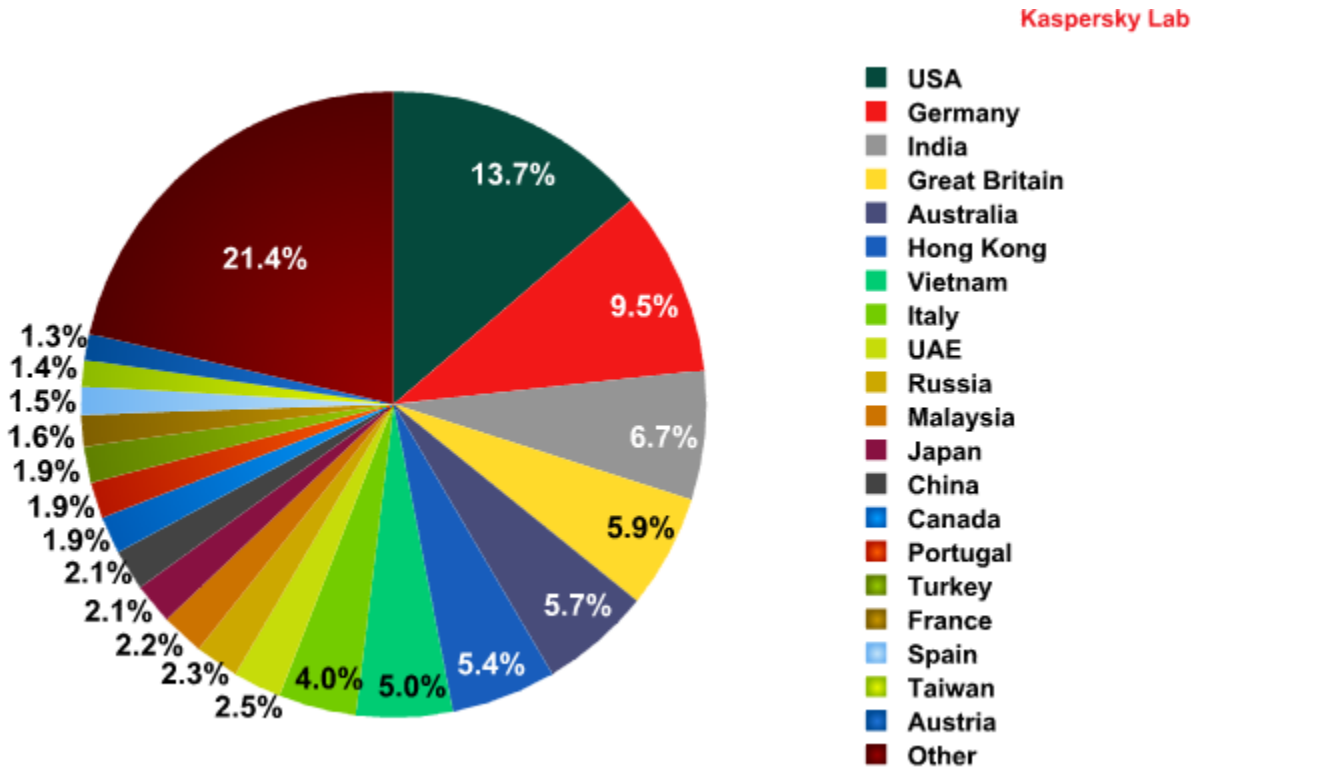
ZBOT 系列占七月通过电子邮件分发的所有恶意程序邮件的 23.4%。

Email-Worm.Win32.Bagle.gt 名列第 3，下凉了 0.1%，比六月下降一位。这个邮件蠕虫的功能是自我增殖地址受害人的地址簿，这是典型的恶意软件。它也可以与指挥中心联系，并下载其他恶意程序到用户的计算机上。

Email-Worm.Win32.Mydoom.I 增加 0.14%，排在第八。会自我增殖隐藏搜索请求发送到搜索引擎，如谷歌，雅虎， AltaVista 和 Lycos。该蠕虫会将网站上显示的搜索结果中的第一页，会与欺诈者的服务器下载的地址进行比较。如果匹配，它会打开搜索引擎页面，从而增加网站的流量和增加网站在搜索结果中的链接评级。

Trojan-Dropper.Win32.Dorifel.afpu 排名第十。它的主要功能是实现从远程服务器上下载并运行其他恶意程序。

有趣的是，SMS-Flooder.AndroidOS.Didat.a 占据第 15 位。到目前为止，这是第一次，出现了 Android 恶意程序。SMS-Flooder.AndroidOS.Didat.a 会群发短信和邮件。数量不断增长的 android 平台的恶意软件，我们预测未来的这种类型的恶意程序会呈现持续增长的趋势。



邮件防病毒检测的国家分布

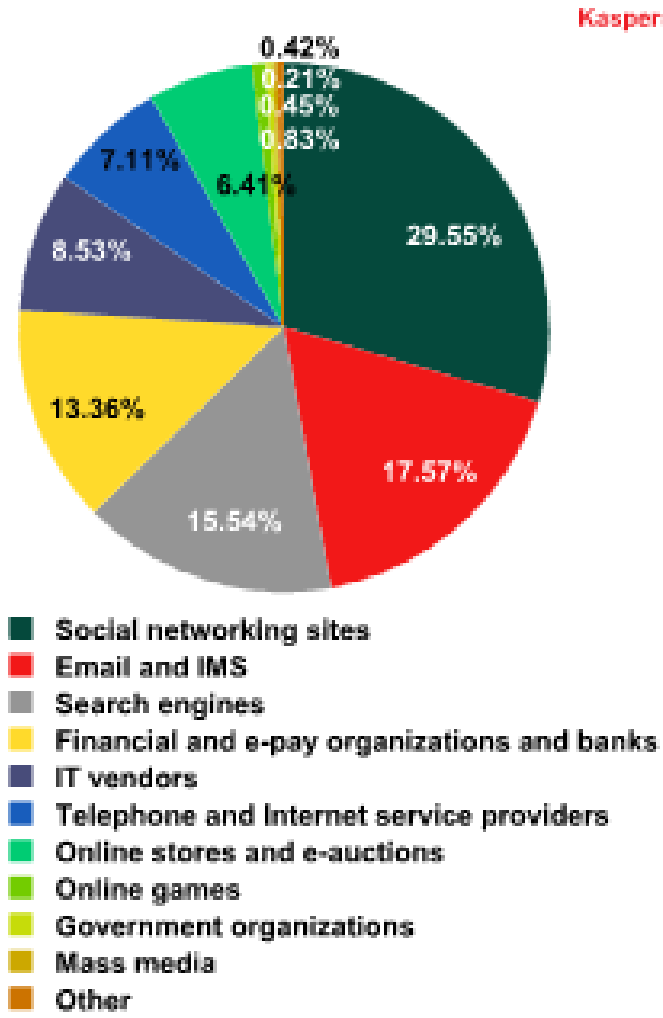
在六月的异常后，排名恢复了常态：美国第一名，增长 4.1%，其次是德国，增长 1.7%和印度，增长 0.8%。

英国从第八名上升至第四名，澳大利亚名列第五。

其他国家所占份额确实没有大的差别。

钓鱼

钓鱼邮件的百分比与六月相比减少了 50%以上，为 0.0012%



排名前 100 的是非法钓鱼网站*

这个评价是根据卡巴斯基实验室的反钓鱼组件被激活的检测，每次用户试图点击钓鱼链接，无论是否是在一个垃圾邮件或网页上的链接。

社交网站仍然是网络钓鱼攻击最有吸引力的目标：他们的比例下降了 1.7%，为 29.6% 。

在电子邮件和即时通讯服务攻击的份额增加了 4.4%，从第四上升到第二。搜索引擎（15.5%）和金融电子支付服务（13.3%）均下跌一个位置，分别第三和第四。

第 5 至第 8 名次不变：IT 供应商（8.5%） 和互联网提供商（7.1%）的分别下降 1%，在线商店（6.4%）和在线游戏（0.83%）略有增加。

七月，英国信用体系 Wonga 成为一个典型的网络钓鱼攻击的目标。发送者模仿该公司发送假通知通知，称收件人帐户数据库出现问题。如果用户未能更新他们的帐户，他们会被阻止访问。这些更新程序可在任何公司的办公室，或通过下载和填写附加的文件，通过电子邮件发送它。该邮件包含 html 文档，用户必须输入其电子邮件地址和密码。骗子便可以得到帐户的完全访问权限和权限徐可范围内的钱。

（反垃圾信息中心编译，源文网址：http://www.securelist.com/en/analysis/204792309/Spam_in_September_2013）