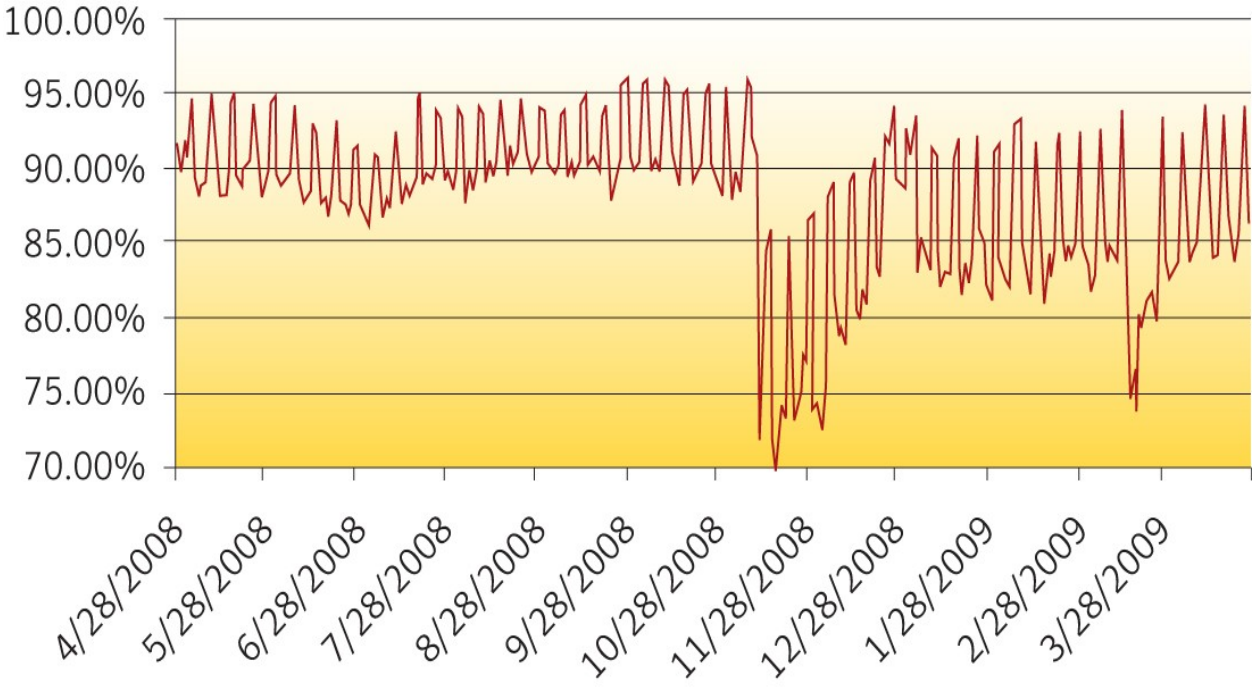
Spam volumes continue to creep back up to normal, and are currently sitting at 94 percent of their pre-McColo levels. Spam categories continue to fluctuate month to month with leisure and Internet spam decreasing eight and seven percent respectively, and financial spam increasing by six percent. The Swine Flu outbreak has also become yet another example of a current event being used by spammers to distribute their messages.

The following trends are highlighted in the May 2009 report:

- **Swine Flu Outbreak Results in Swine Flu Spam Outbreak**
- **Image Spam Makes an Unwelcome Return**
- **Spammer's Opinion Poll: President Obama's First 100 Days in Office**
- **Mother's day spam – May 2009**
- **Zombie Host IP Activity April 2009**
- **As One Free Web Service is Closed – Spammers Find More Free Services to Abuse**

Spam Percentage: The model used to calculate spam percentage now factors in network layer blocking in addition to SMTP layer filtering, and as a results represents a more accurate view into the actual spam percentage on the Internet.



Doug Bowers
Executive Editor
Antispam Engineering

Dermot Harnett
Editor
Antispam Engineering

Cory Edwards
PR Contact
cory_edwards@symantec.com

Swine Flu Outbreak Results in Swine Flu Spam Outbreak

The Swine Flu outbreak in Mexico and across the world has been making news headlines with updates coming out in real time from the Centers for Disease Control and the World Health Organization. Symantec has been monitoring these messages closely and has found that the top 20 subject lines related to this spam campaign using certain keywords are:

1. Jolie caught swine flu
2. Swine flu in NY
3. Madonna caught swine flu
4. America against swine flu
5. Madonna caught swine flu!
6. America against swine flu!
7. Swine flu in USA
8. Salma Hayek caught swine flu!
9. US swine flu statistics
10. NY victims of swine flu
11. Swine flu in Hollywood!
12. Swine flu worldwide!
13. First US swine flu victims!
14. Will swine flu attack USA?
15. Be quick! anti-swine flu drugs are almost sold out
16. US swine flu fears
17. Get swine flu medicine here
18. Order now vaccine against swine flu
19. Prevent infections with swine flu viruses
20. Stop risk of being killed by swine flu!

Health related spam samples have been observed with messages talking about medicines that could be used to fight the flu, and provided URLs to various pharmacy sites. In another example, potential victims were sent an email with a malicious PDF attachment that promised to answer questions about the Swine Flu. Symantec detects the malicious PDF file as Bloodhound.Exploit.6 and the dropped malicious file contained in the PDF as InfoStealer. Other examples of Swine Flu spam have included messages written in Spanish with links to a video. The spam message encourages the user to click on the video link by stating that *"Below is a video of the symptoms the patient may present, from when it starts up till when he dies. The following pictures are not suitable for everybody and it is recommended to be seen only by persons under their own criteria."*

While it remains to be seen whether Swine Flu spam will result in a Swine Flu spam pandemic, history tells us that current event spam campaigns will continue in an effort to lure victims and distribute spam messages. It should also be noted that spammers recently used the Italian earthquake in their messages. As always, users should be careful before opening any attachments or clicking on URL links.

Swine Flu Outbreak Results in Swine Flu Spam Outbreak

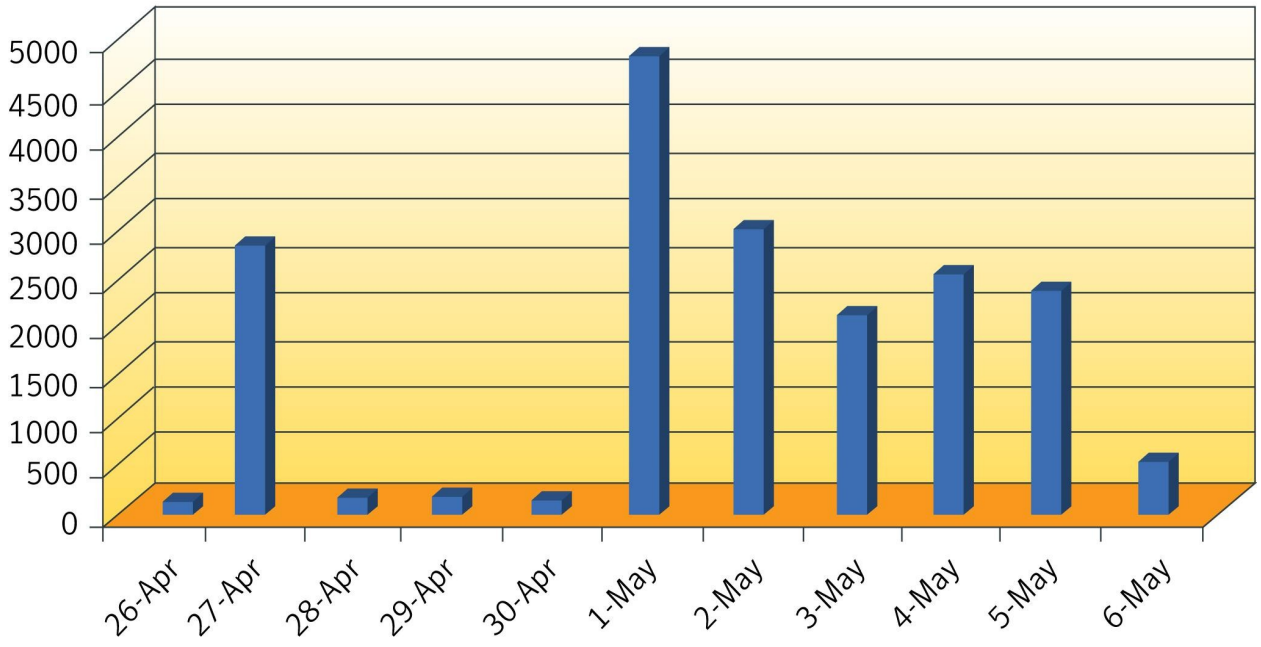


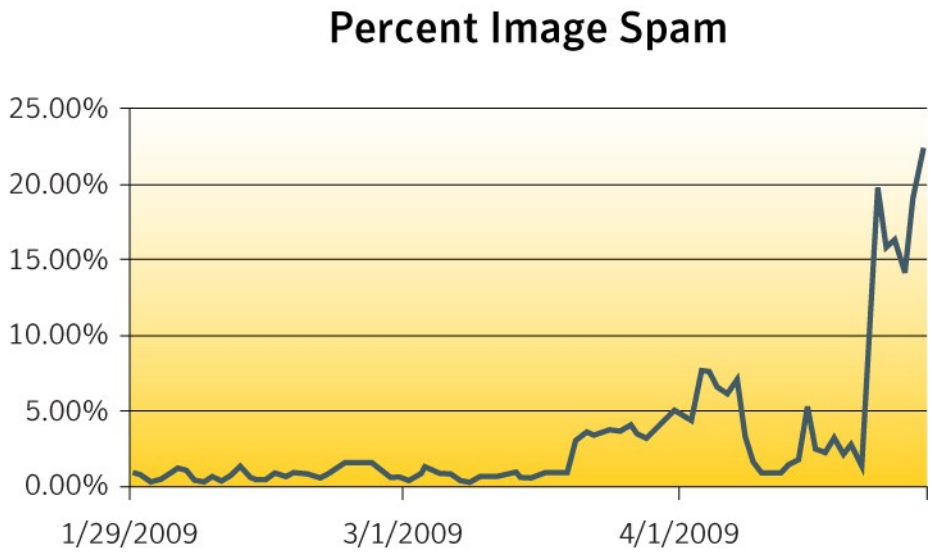
Image Spam Makes an Unwelcome Return

Image spam does from time to time reappear on the spam landscape, and in recent weeks a resurgence of image spam has been observed. Image spam is by definition a spam message which contains an attached image with little or no text, or HTML in the message body. The attached image will often contain various obfuscation techniques such as subtle changes to the color or font and added background noise contained in the image in an effort to evade antispam detection.

The call to action for the recipient is often described in the attached image itself. In the example below, a recipient would be asked to type a certain URL into the address bar of their browser. If the recipient took this action and followed this URL they would be taken to a website promoting certain pharmaceutical products.

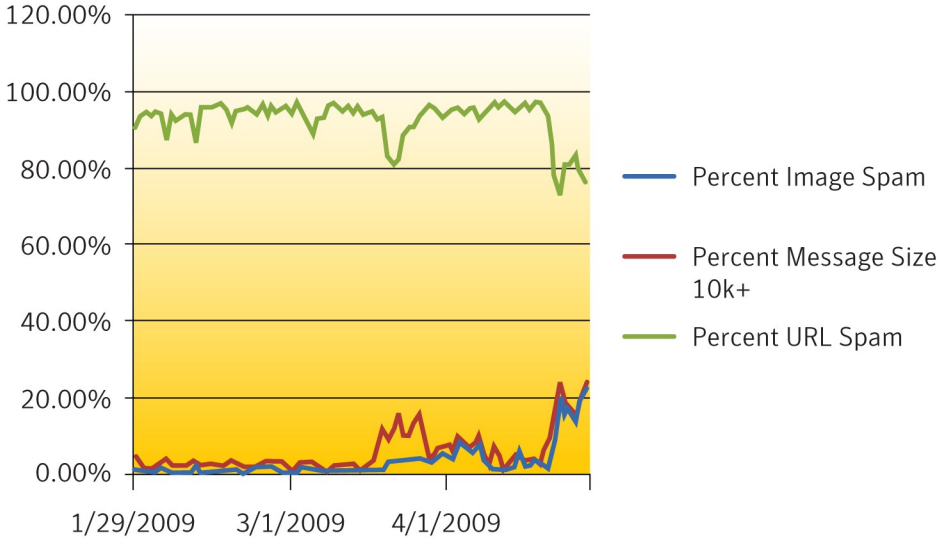
Image Spam Makes an Unwelcome Return

While image spam does not currently dominate the spam landscape as it did in 2007 —when 52 percent of all spam was image spam—image spam hit an average of sixteen percent of all spam messages towards the end of April 2009



With the return of image spam, a number of other associated spam vectors have also been observed:

1. The average size of spam messages has increased. This increase in size could put a strain on mail infrastructures and could possibly prevent end users from receiving legitimate email.
2. The number of spam messages which contain a URL has decreased and this can be attributed to the fact that the spam messages with an attached image do not have a URL in the message body.



Spammer's Opinion Poll: President Obama's First 100 Days in Office

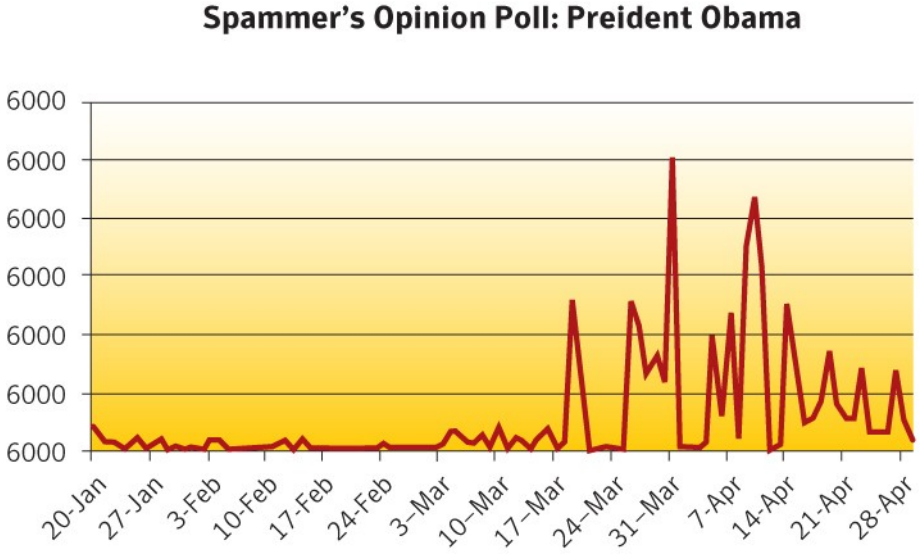
According to recent political opinion polls President Obama's approval rating currently stands at 65 percent. It is clear that spammers also continue to view him favorably after 100 days. In the last few weeks there has been a noticeable boost in the number of spam messages which use his name and popularity to promote certain spam products and services.

President Obama first became a target for Spammers in 2008 when he and his then challenger, Senator John McCain, had their names linked with portable dewrinkle machine spam, medical product spam and get-rich-quick spam messages. When President Obama took his campaign to Europe in July 2008, Spammers duly followed up with a spam campaign that contained links to malware. Since President Obama was inaugurated on January 20th 2009, spam attacks with links to his name continue to circulate.

It is not surprising that with the President's continued popularity that spammers keep latching on to his name in an attempt to evade antispam filters. This is yet another example of spammers trying to leverage current events as lures to distribute their spam messages.

The top 20 related subject lines that included the keywords "Barack" or "Obama" since January 20th:

1. On air! America is loosing Obama with no health care - Get meds now
2. Heard what Obama said ford health care!
3. Obama's health is in danger er it.
4. Obama shocked public drugs!
5. Obama caught in lurid scandal
6. New!!! Obama wants legalize!
7. Obama's hypocrite new law
8. Obama: Death was near me.
9. Obama is coward! Proof:
10. Shocking Obama revelation Program
11. Obama's wife naked!! od, get them NOW.
12. New!!! Obama wants legalize!
13. Obama Proposes Trade of AIG Executives in Primitive Swaps
14. Obama releases Loan Mod Program
15. Obama shocked
16. obama
17. Obama has OK'd Online Sale of Me
18. Obama Allows Meds Sold Online
19. Obama OKs Sale Of Controlled Meds Online
20. Obama wants to help YOU get the meds you NEED to be healthy and feel good



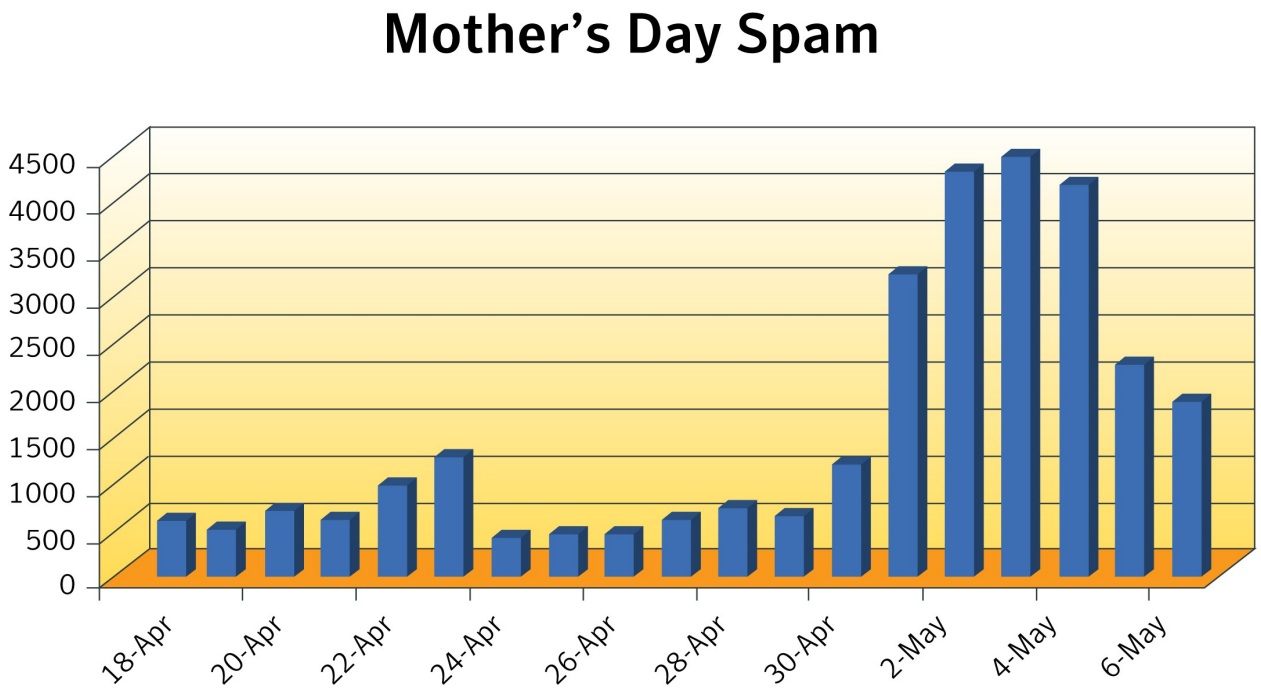
Mother's day spam – May 2009

Sunday May 10th 2009 is Mother's day in many countries around the world. This day is used by people to honor their mother. Spammers however continue to dishonor this holiday by using this day as a ruse to distribute their spam wares. Products spam-advertised this Mother's day include flowers, photo frames, jewelry, gift cards, kitchen related products, and the ever-present weight-loss products.

Top 10 related subject lines:

1. Mothers Day Flowers starting at $19.99 - FTD Flowers
2. Mother's Day Exclusive! Flowers from $19.99
3. Send Mother's Day Flowers from $19.99
4. Surprise Mom with a Personalized Gift
5. Special Mother's Day Offer! Flowers from $19.99
6. Fresh Mothers Day Flowers from $19.99
7. Send Mother's Day Flowers from $19.99.
8. 6 Days 'Til Mom's Day! A Touch Of Pink
9. Mother's Day Exclusive. Flowers from $19.99
10. Send Mom an eCard Today

While other current events such as the H1N1 flu outbreak have resulted in some high profile spam attacks, it is clear that spammers continue to believe that just like the greeting card companies, they will obtain a return on their investment when they target this particular holiday.



Zombie Host IP Activity April 2009

Zombie is a term given to a computer that has been compromised and is being used for various criminal related interests such as sending spam, hosting Web sites that advertise spam and acting as DNS servers for zombie hosts. The top 10 countries hosting active zombie machines in April 2009 are compared with the results shared in the March 2009 State of Spam report below:

The table shows that Brazil continues to dominate as the number one host of active zombie machines. Russia and Turkey at eight and seven percent respectively have increased their market share in this realm. The United States interestingly has dropped one percent and now accounts as the host for five percent of active zombie machines. It is clear that in the post- McColo era that as spam volumes continue to rise (currently at 94 percent of their pre-McColo levels) old botnets are being brought back online, and new botnets are being created in locations where investment in IT infrastructure is increasing rapidly.

Country	March 2009 %	April 2009 %	Difference
Brazil	14%	16%	2%
Russia	7%	8%	1%
Turkey	6%	7%	1%
India	6%	6%	0%
United States	6%	5%	-1%
Poland	4%	5%	1%
Germany	4%	3%	-1%
Argentina	3%	3%	0%
Spain	3%	3%	0%
Italy	3%	3%	0%

As One Free Web Service is Closed – Spammers Find More Free Services to Abuse

A top-level domain (TLD) is the part of a domain name that follows the final "dot" of any domain name. A ccTLD is a top-level domain generally reserved or used by a country or dependent territory such as co.uk. A gTLD is a global top-level domain such com. In April 2009, approximately 91 percent of all spam messages contained a URL.

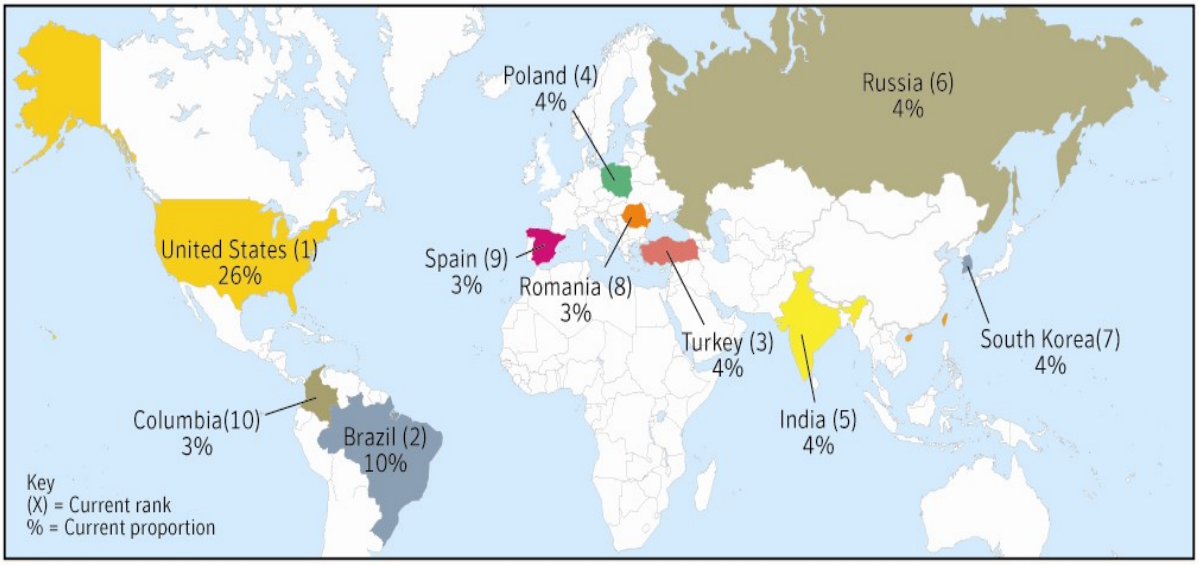
Twenty percent of the URLs observed had a cn ccTLD and sixty-four percent of URLs had a com TLD. Interestingly, three percent of URLs had a pl TLD. The increase in spam messages which contained a pl TLD can be attributed in part to an increase in spam messages that contained a free web URL that had a pl TLD.

TLD	Mar-09	Apr-09	Change
com	57.16%	64%	7%
cn	33.61%	20%	-14%
net	5.91%	9%	3%
pl	Not ranked	3.20%	N/A
org	Not ranked	1%	N/A

Sites which allow users to set up free accounts have been used in the past by spammers to promote their products and services. The rationale for spammers to set up accounts with these free resources centers around one key point - spam is about economics and spammers want to make money with minimal overhead. For spammers, the attraction is that these services are free and if one of their URLs are detected, spammers can often create another free account. With certain web hosting services closing, it is clear the spammers are now finding other free services to use and abuse.

Metrics Digest: Regions of Origin

Defined: Region of origin represents the percentage of spam messages reported coming from certain regions and countries in the last 30 days.



Country	Mar-09	Apr-09	Change
United States	28%	26%	-2%
Brazil	9%	10%	1%
India	4%	4%	0%
South Korea	4%	4%	0%
Turkey	3%	4%	1%
Russia	3%	4%	1%
Poland		4%	4%
Columbia	3%	3%	0%
Spain	Not Ranked	3%	3%
Romania	Not Ranked	3%	3%

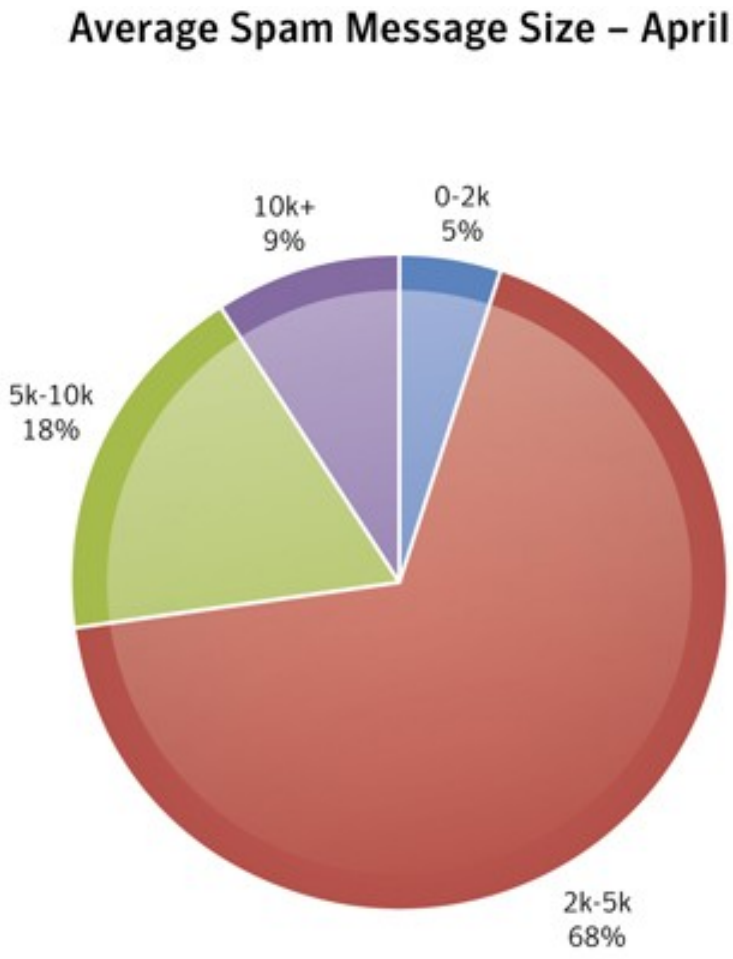
Metrics Digest: Global Spam Categories:

Category Name	March 2009	April 2009	Change
Internet	35%	28%	-7%
Health	19%	25%	6%
Leisure	17%	9%	-8%
Products	14%	14%	0%
Financial	6%	12%	6%
Fraud	2%	3%	1%
419 spam	5%	5%	0%
Adult	1%	2%	1%
Scams	1%	2%	1%
Political	<1%	<1%	No Change

- **Internet Email attacks** specifically offering or advertising Internet or computer-related goods and services. *Examples: web hosting, web design, spamware*
- **Health Email attacks** offering or advertising health-related products and services. *Examples: pharmaceuticals, medical treatments, herbal remedies*
- **Leisure Email attacks** offering or advertising prizes, awards, or discounted leisure activities. Examples: vacation offers, online casinos
- **Products Email attacks** offering or advertising general goods and services. *Examples: devices, investigation services, clothing, makeup*
- **Financial Email attacks** that contain references or offers related to money, the stock market or other financial "opportunities." *Examples: investments, credit reports, real estate, loans*
- **Scams Email attacks** recognized as fraudulent, intentionally misguiding, or known to result in fraudulent activity on the part of the sender. *Examples: Pyramid schemes, chain letters*
- **Adult Email attacks** containing or referring to products or services intended for persons above the age of 18, often offensive or inap-
- **Fraud Email attacks** that appear to be from a well-known company, but are not. Also known as "brand spoofing" or "phishing," these messages are often used to trick users into revealing personal information such as E-mail address, financial information and passwords. *Examples: account notification, credit card verification, billing updates*
- **419 spam Email attacks** is named after the section of the Nigerian penal code dealing with fraud, and refers to spam email that typically alerts an end user that they are entitled to a sum of money, by way of lottery, a retired government official, lottery, new job or a wealthy person that has that has passed away. This is also sometimes referred to as advance fee fraud.
- **Political Email attacks** Messages advertising a political candidate's campaign, offers to donate money to a political party or political cause, offers for products related to a political figure/campaign, etc. *Examples: political party, elections, donations*

Metrics Digest: Size of Messages and spam

Message Size	March 2009	April 2009	Change
0-2k	5.46%	5.30%	0%
2k- 5k	72.90%	68.00%	-5%
5k-10k	15.91%	18.00%	2%
10k+	5.73%	8.70%	3%



Metrics Digest: URLs and spam

TLD	Mar-09	Apr-09	Change
com	57.16%	64%	7%
cn	33.61%	20%	-14%
net	5.91%	9%	3%
pl	Not ranked	3.20%	N/A
org	Not ranked	1%	N/A