State of Spam
A Monthly Report

Confidence in a connected world. symantec.

April 2009

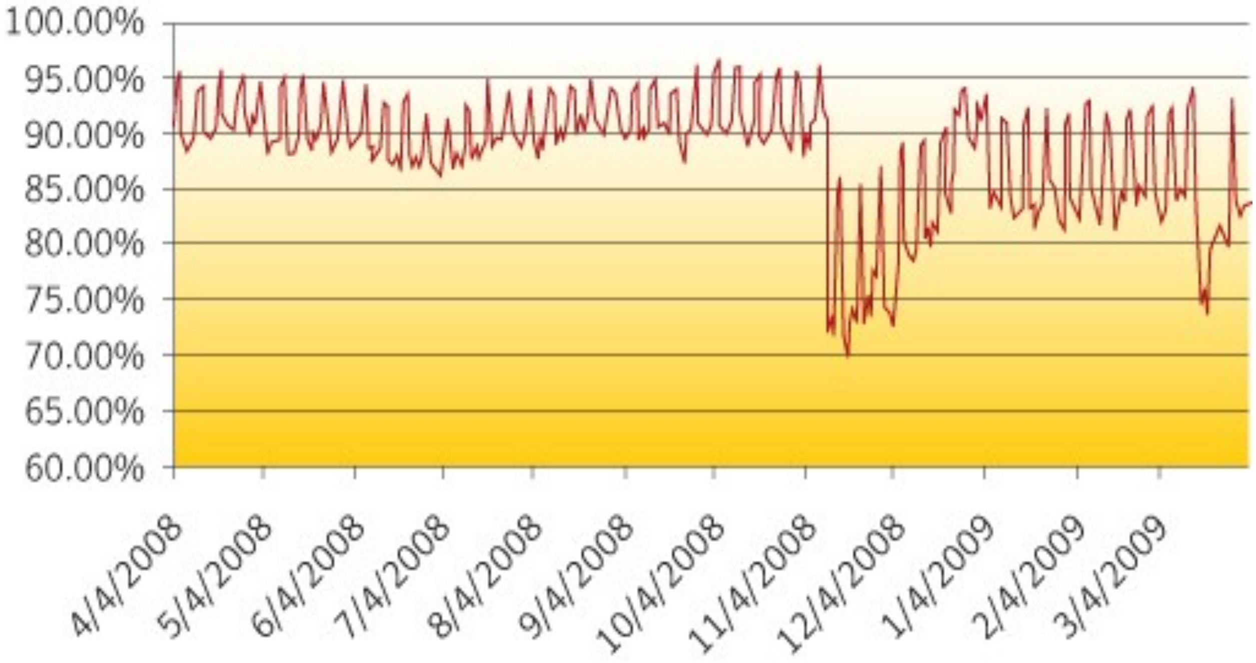
Report 28

The sudden shutdown of McColo caused a ripple that has impacted the spam landscape for five months. Spam levels have yet to match the highs we monitored previous to this event. However, as we move toward the six month mark following the November shutdown, we've watched as spam volumes have gradually crept back to approximately 91 percent of their pre-McColo shutdown levels.

Highlighted in the April 2009 report:

- **McColo Shutdown Continues to Affect the Spamscape throughout the month of March**
- **Spammers Rethink Their Mortgage Strategy**
- **Conficker Used for Fake Antivirus Software Sale**
- **Countdown to Tax Day Continues—Do Not File the "Spam Expense"**
- **"Take care about yourself!" Avoid Terror -Related Malware Spam**
- **Metrics Digest**

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

McColo Shutdown Continues to Affect the Spamscape throughout the month of March

Since the shutdown of hosting company McColo in mid-November 2008, spam volumes have slowly made their way back to "normal." Old botnets are being brought back online, and new botnets are being created. Spam volumes are now at 91 percent of their pre-McColo shutdown levels.

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 websites that advertise spam and acting as DNS servers for zombie hosts.

The top 10 countries hosting active zombie machines in March 2009 are compared below with the September 2008 results shared in the October 2008 State of Spam report :

Like September 2008, the EMEA region continues to be the leading source of all zombie IP addresses, hosting 45 percent of active zombie computers in March 2009. Of the countries making up the EMEA region, Russia now owns the title of "leading EMEA country" leading Turkey by one percent. Turkey's active zombie count fell by more than half. While EMEA continues to be the leading regional host of zombie computers, Brazil at 14 percent has jumped five percentage points and owns the dubious honor of the number one host of active zombie machines. As countries such as Brazil, India and China (which have a burgeoning middle class) continue to invest heavily in Internet and IT infrastructure, the location of active zombie machines will continue to change.

Country	September 2008 %	March 2009 %	Difference
Brazil	9%	14%	5%
Russia	8%	7%	-1%
India	6%	6%	0%
United States	6%	6%	0%
Turkey	12%	6%	-6%
Poland	4%	4%	0%
Germany	5%	4%	-1%
Argentina	4%	3%	-1%
Spain	Not Listed	3%	N/A
Italy	Not Listed	3%	N/A

Spammers Rethink Their Mortgage Strategy

Do you have the housing market blues? Does the term credit default swap send shivers down your spine? Spammers are here to help! Since the beginning of the year, spammers have been steadily utilizing sadly familiar terms from the mortgage industry in their *spamvertisements*. Monitored terms include: foreclose, foreclosure, interest rates, mortgage, and for fun, the misspelled *forclosure*.

A review of these terms makes two things apparent. First, and as usual, spammers have been complementing marketing pitches with terminology relating to current events, such as the economic downturn. There has been an increase in the use of these terms in enhancement spam and fraud spam where the intent is to steal money and/or personal information.

Second, there has been a shift in certain types of spam, such as make money fast spam, which are actually get rich quick schemes built around purchasing foreclosed homes. Many spam messages now carry the promise of avoiding foreclosure all together.

Top 20 Mortgage Related Subject Lines:

1. re: mortgage payment
2. mortgage loan information
3. a big instrument is a mortgage to success.
4. search foreclosure listings by zipcode for free... nationwide!
5. record foreclosure filings: homes given away!
6. in fear of foreclosure
7. hey mom, this can pay your mortgage
8. don't go into foreclosure
9. facing foreclosure?
10. had a hardship and facing foreclosure?
11. don't let your lender foreclose
12. home-mortgage-mess: your 30 second bailout
13. don't let them foreclose
14. fight foreclosure
15. save your house from foreclosure today
16. ; search foreclosure listings by zipcode for free... nationwide!
17. lower your mortgage. popular ontv.
18. get a free book from robert allen... the foreclosure guru.
19. find out if a reverse mortgage is right for you
20. mortgage modification may be available to you - avoid foreclosure!

Countdown to Tax Day Continues—Do Not File the "Spam Expense"

If you are a resident of the United States and haven't already filed your tax returns, maybe you should consider reading the following. The countdown to "Tax Day" (April 15 in the United States) is currently in full swing, with the IRS offering daily tips for filing.

The run-up to Tax Day in the United States has traditionally become a time when phishing directed towards the IRS becomes more prevalent. As reported in previous Symantec State of Spam reports, spammers continue to attempt to disguise themselves as the IRS, dangling tax refund offers in front of unsuspecting users.

These offers are aimed toward recipients who may be unaware that the IRS "**does not** initiate communication with taxpayers through email." The purpose of these attacks is often to collect personal details, including date of birth and debit/credit card information. However, these types of tax-related spam attacks are not limited to the United States, with spammers attempting to disguise themselves as tax collection authorities from across the world. The Irish tax authority recently became one of the latest targets.

In addition to spammers disguising themselves as the IRS and other tax authorities, Symantec has recently observed that spammers have been offering ways to save money on tax preparation as a means to enter a user's inbox. Spammers are using this method to attempt to obtain personal information from a recipient.

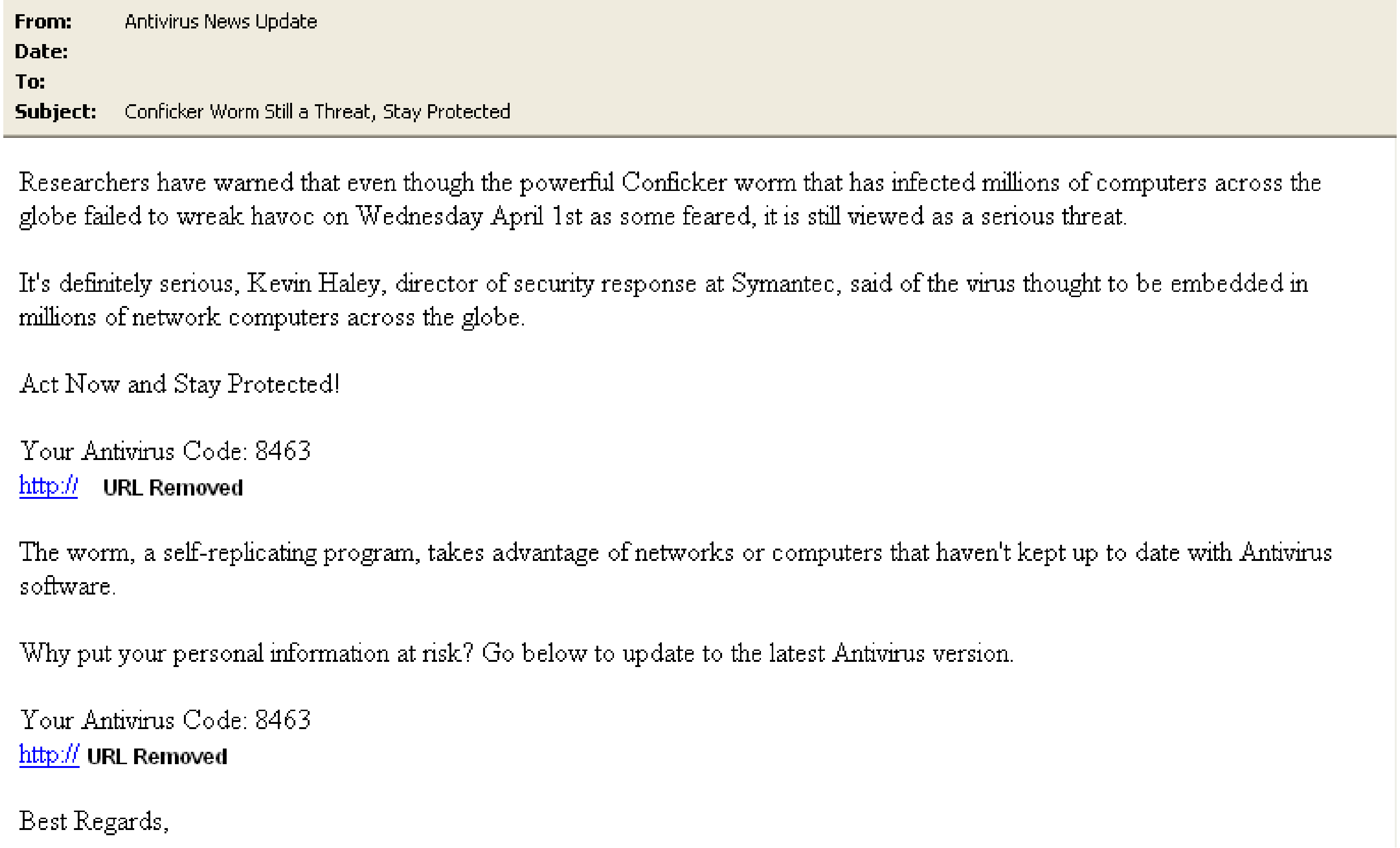
Below are the top 20 tax-related subject lines in order that they have occurred in spam messages for February 1 to March 23, 2009:

1. rebate processor position - we need your help now
2. we could help you settle irs debt now
3. don't you want something for your taxes
4. re: do you owe tax debt? read on
5. a rebate processor position offers you the chance to work at home
6. rebate processor position - easy work - great pay
7. don't you want something for your taxes
8. rebate processing jobs at home. immediate placement
9. re: need help with irs back taxes?
10. fast & accurate tax refund
11. 97% of all applicants can be helped with irs back tax
12. warranty and refund policies and wonderful discounts are available.
13. re: do you owe back taxes? we could help
14. $389 desktop, $499 laptop. amazing tax season 2-day sale.
15. need irs tax relief?..
16. no more tax increases
17. get expert tax advice with your irs issues no cost consultation
18. at home rebate-processor positions paying $390+ daily
19. back taxes got you worried?
20. back taxes got you worried?...

Conficker Used for Fake Antivirus Software Sale

April Fools' Day was anticipated as the expansion date of the Conficker worm with the possibility of a major threat launch. We have found spam samples attempting to capitalize on the frenzy over Conficker (a.k.a. Downadup), offering the latest in antivirus security software that purportedly protects users from the Conficker threat. Some of these spam messages even use names and images of software much like our own Norton AntiVirus 2009. In the example below, it even mentions the name of one of our Symantec employees frequently cited in the press.

In an attempt to increase financial gain, the product website is made to look like the product is one of our Norton consumer security solutions, by using the AntiVirus 2009 name and comparing itself with other antivirus solutions such as Spybot, Kaspersky, and AVG. After clicking on the link inside the message, we find that it redirects to a website where the user is promptly given directions on how to make a payment. Whether or not any product will be made available after the payment is made is still unknown at this point. Even if the product promised is available, its effectiveness would be questionable because it is most likely a rogue application or pirated software.



From: Antivirus News Update
Date:
To:
Subject: Conficker Worm Still a Threat, Stay Protected

Researchers have warned that even though the powerful Conficker worm that has infected millions of computers across the globe failed to wreak havoc on Wednesday April 1st as some feared, it is still viewed as a serious threat.

It's definitely serious, Kevin Haley, director of security response at Symantec, said of the virus thought to be embedded in millions of network computers across the globe.

Act Now and Stay Protected!

Your Antivirus Code: 8463
http:// **URL Removed**

The worm, a self-replicating program, takes advantage of networks or computers that haven't kept up to date with Antivirus software.

Why put your personal information at risk? Go below to update to the latest Antivirus version.

Your Antivirus Code: 8463
http:// **URL Removed**

Best Regards,

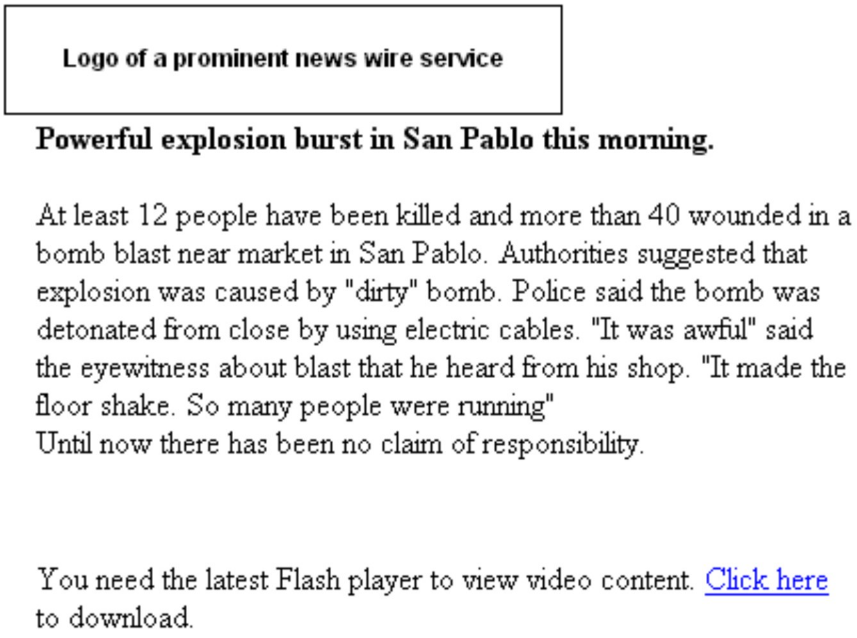
"Take care about yourself!" Avoid Terror -Related Malware Spam

With the ominous subject line *"Take care about yourself!"* fear mixed with excitement might propel some recipients to disregard security consequences and click on URLs that link to malware. In this recent example, geolocation services were used to target the recipient of the message. Depending on the relative location of the message recipient, the location of the terrorist attack differs.

In one location, the spammer indicated that there was a “Powerful explosion burst in San Pablo this morning,” and in another, they indicated that there was a “Powerful explosion burst in Pune this morning.” Following the message is a brief description of the attack including: “At least 12 people have been killed and more than 40 wounded in a bomb blast.” and “explosion was caused by ‘dirty’ bomb.”

The logo of a prominent news wire service was added to try and bring a sense of authenticity. Human curiosity might prevail for some users as they were instructed by the spammer, “You need the latest Flash player to view video content. Click here to download.” Users should not click on this link as it contains a link to downloadable malware. The link between malware and spam should not be underestimated. Spammers have long used this connection to target unsuspecting recipients.

Spammers often use human curiosity to tempt recipients into opening a spam message and click on a link, or take some other action. In this instance, spammers believe that keeping spam content relevant to a geographical location will enable them to achieve their goals.



Logo of a prominent news wire service

Powerful explosion burst in San Pablo this morning.

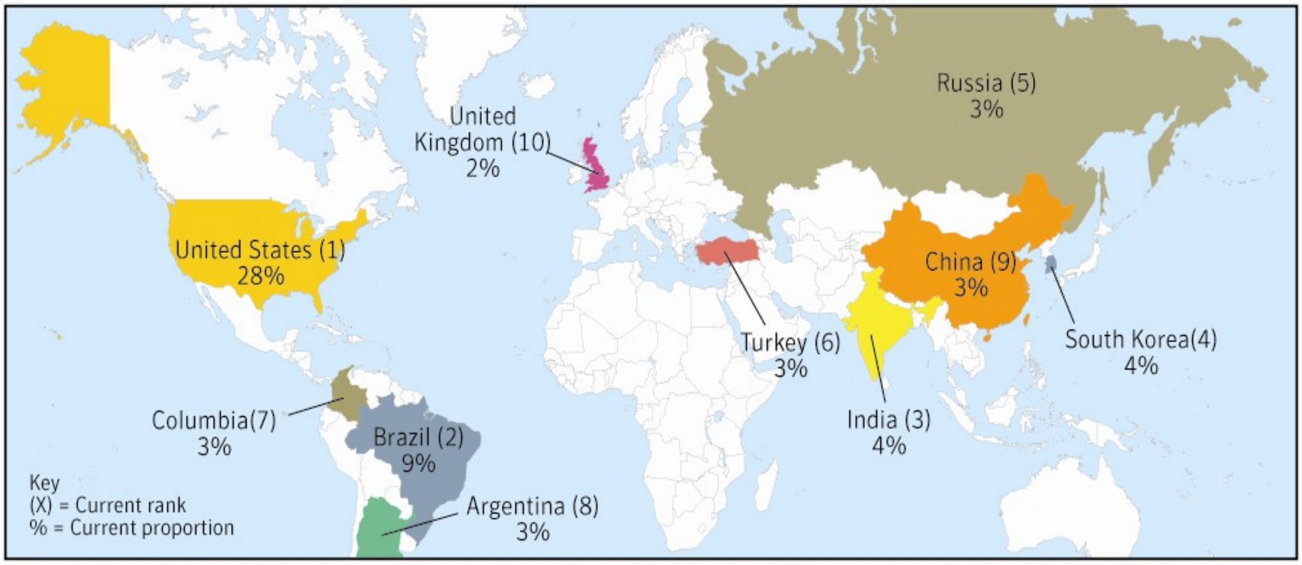
At least 12 people have been killed and more than 40 wounded in a bomb blast near market in San Pablo. Authorities suggested that explosion was caused by "dirty" bomb. Police said the bomb was detonated from close by using electric cables. "It was awful" said the eyewitness about blast that he heard from his shop. "It made the floor shake. So many people were running"
Until now there has been no claim of responsibility.

You need the latest Flash player to view video content. Click here to download.

Metrics Digest: Regions of Origin:

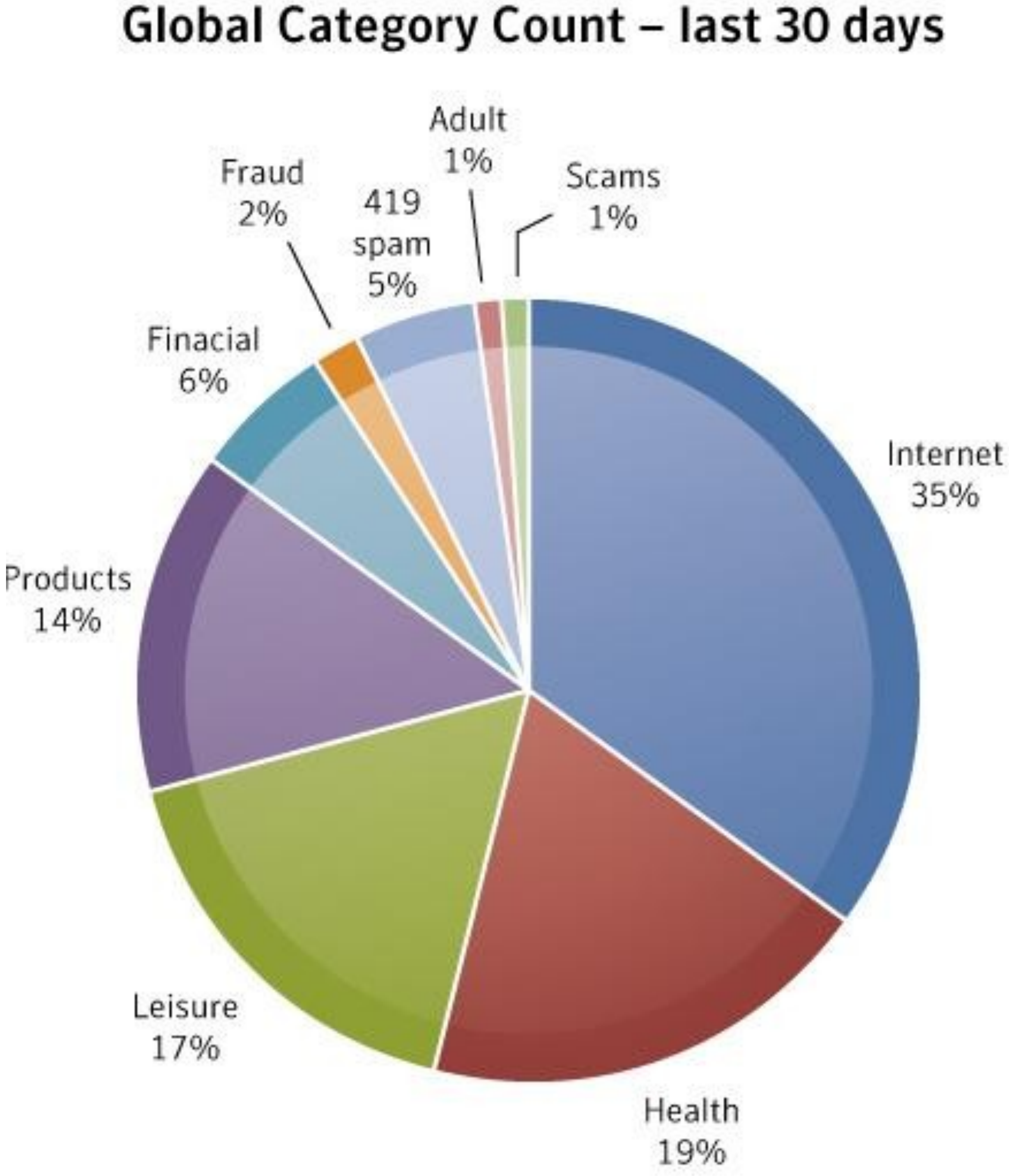
Defined:

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



Country	Feb-09	Mar-09	Change
United States	25%	28%	3%
Brazil	9%	9%	0%
India	5%	4%	-1%
South Korea	4%	4%	0%
Turkey	4%	3%	-1%
Russia	4%	3%	-1%
China	4%	3%	-1%
Columbia	Not Listed	3%	N/A
Argentina	Not Listed	3%	N/A
United Kingdom	Not Listed	2%	N/A

Metrics Digest: Global Spam Categories:



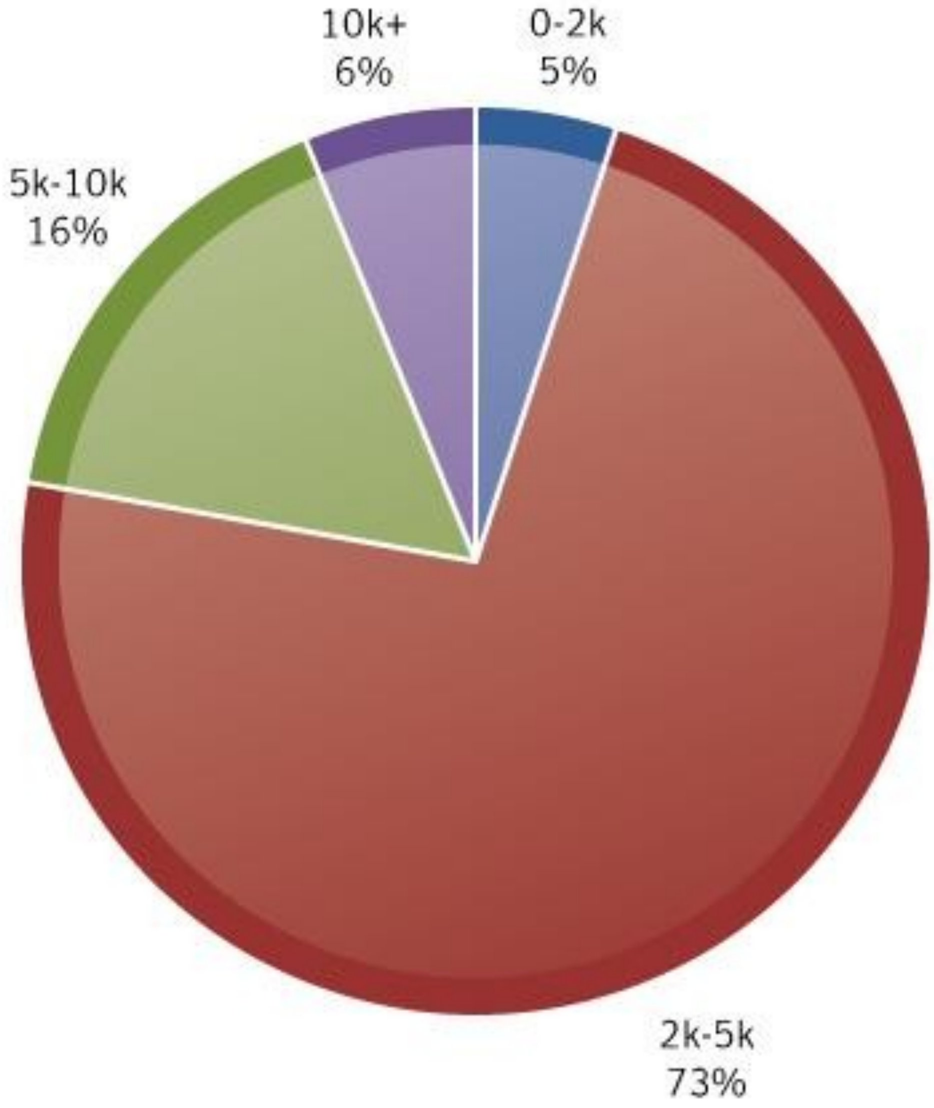
Metrics Digest: Global Spam Categories:

Category Name	Feb 09	Mar 09	Change
Internet	27%	35%	8%
Health	16%	19%	3%
Leisure	16%	17%	1%
Products	15%	14%	-1%
Financial	11%	6%	-5%
Fraud	5%	2%	-3%
419 spam	4%	5%	1%
Adult	3%	1%	-2%
Scams	3%	1%	-2%
Political	<1%	<1%	No Change

- **Products E-mail attacks** offering or advertising general goods and services. *Examples: devices, investigation services, clothing, makeup*
- **Adult E-mail attacks** containing or referring to products or services intended for persons above the age of 18, often offensive or inappropriate. *Examples: porn, personal ads, relationship advice*
- **Financial E-mail attacks** that contain references or offers related to money, the stock market or other financial "opportunities." *Examples: investments, credit reports, real estate, loans*
- **Scams E-mail attacks** recognized as fraudulent, intentionally misguiding, or known to result in fraudulent activity on the part of the sender. *Examples: Nigerian investment, pyramid schemes, chain letters*
- **Health E-mail attacks** offering or advertising health-related products and services. *Examples: pharmaceuticals, medical treatments, herbal remedies*
- **Fraud E-mail 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*
- **Leisure E-mail attacks** offering or advertising prizes, awards, or discounted leisure activities. *Examples: vacation offers, online casinos, games*
- **Nigerian spam** 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.*

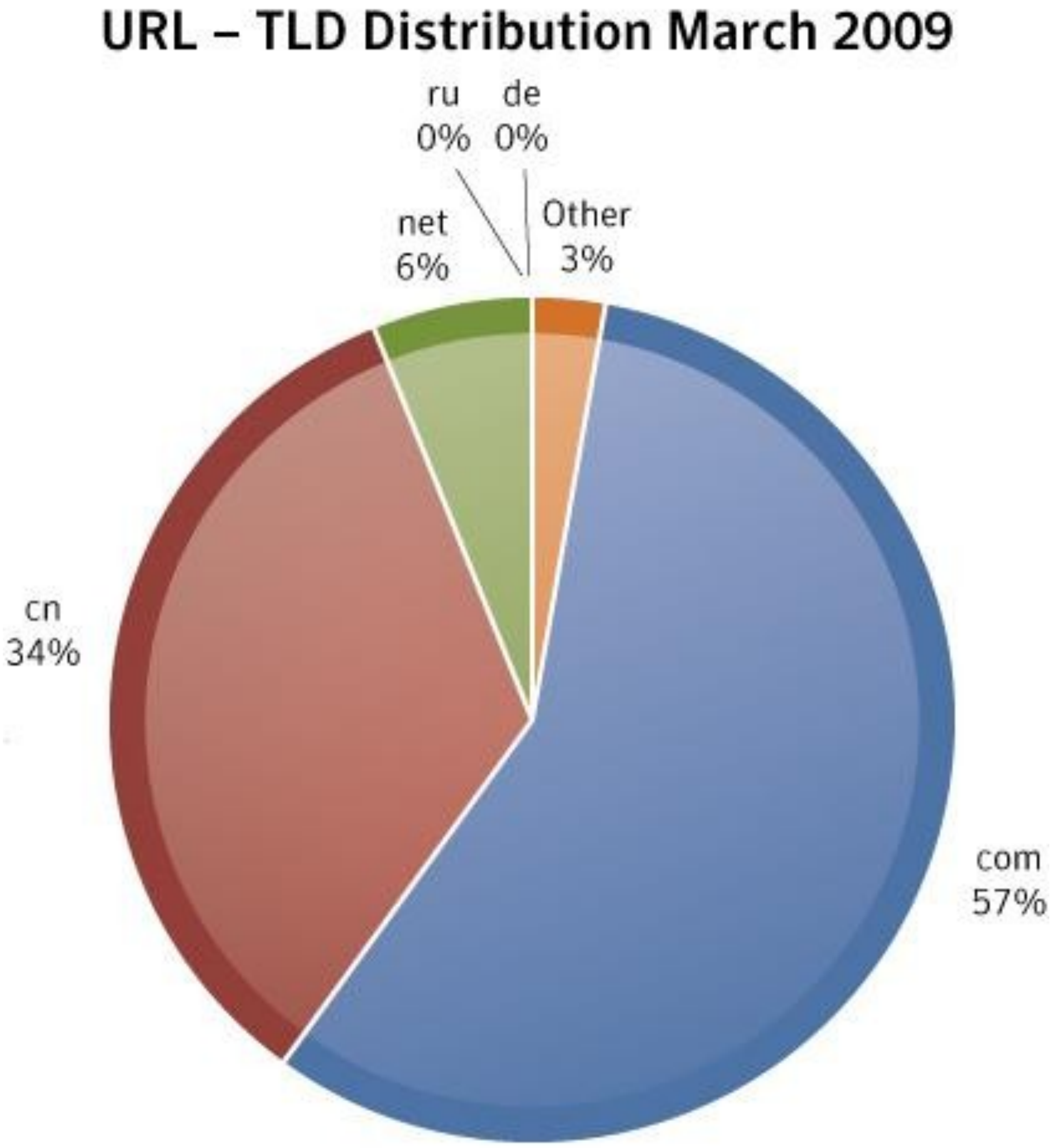
Metrics Digest: Size of Messages and spam

Message Size	Feb-09	Mar-09	Change
0-2k	8.20%	5.46%	-3%
2k- 5k	70.85%	72.90%	2%
5k-10k	18.12%	15.91%	-2%
10k+	2.80%	5.73%	3%

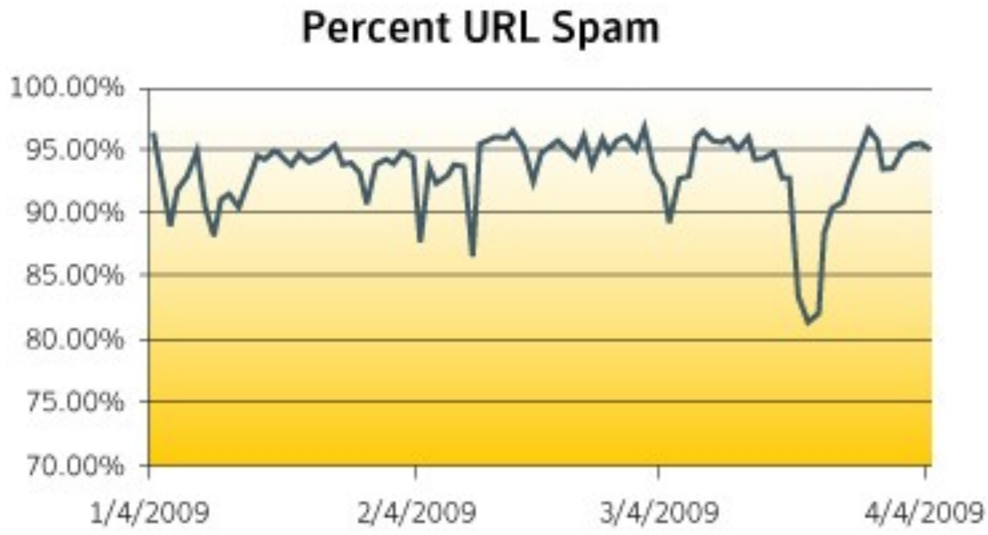


Metrics Digest: URLs and spam

TLD	Feb 09	Mar 09	Change
com	73.30%	57.16%	-16%
cn	19.64%	33.61%	14%
net	2.40%	5.91%	4%
ru	0.80%	0.29%	-1%
de	0.60%	0.39%	0%
Other	3.60%	2.60%	-1%



Metrics Digest: URLs and spam


Percent URL Spam
1/4/2009
2/4/2009
3/4/2009
4/4/2009