The State of Spam

Generated by Symantec Messaging and Web Security
Monthly Spam Landscape

‘Tis the season to be jolly, but this month’s spam levels brought little cheer to anti-spam analysts. Overall spam levels continued to increase, accounting for nearly three out of four emails in November. To put that growth trend into perspective, in May 2007 spam accounted for approximately 64 percent of all email traffic.

Highlights from this month included:

• **Let the Olympic Spams Begin:** Despite the summer games being more than 9 months away, Symantec has started seeing the first examples of spam connected to the 2008 Olympics in Beijing, China (See Page 9)
• **Britney, Lindsay, and Donny Osmond Headline Meds Spam:** Gossip headlines concerning celebrities being used in meds spam (see page 10)
• **Spammers Winter Harvest:** Symantec blocked an estimated 35 million “blank” emails sent by spammers as part of a suspected harvesting campaign to find valid email addresses for spam mailing lists (see page 10)
• **Spammers Exploit Missing Child:** As the search continues for the British child Madeleine McCann, one unscrupulous spammer tries to disguise a virus hosting site in spam emails with a link to the authentic FindMadeleine.com site. (See page 11)
• **Fraud and Scams Continue to Rise:** These categories accounted for 19% of all spam in November (up from 18% in October and 13% in September)
• **Seasonal Campaigns:**
  - Penny Stocks Use Thanksgiving Holiday Captions in Subject Line
  - Snowball Spam Fight
  - Christmas Freebie Offer
  - The Best Christmas Present Ever – A Winning Lottery Ticket

Special Spotlight: The Resurgence of Spam – 2007 in Review

While Bill Gates’ 2004 prediction that spam would be eradicated within two years clearly missed the mark, few expected spam’s extraordinary resurgence in 2007. Since 2006, spam levels have steadily climbed from 56% of all email to an all-time high of 72% of email in the most recent month’s report. Several spam “firsts” were also marked in 2007, including usage of MP3s and videos and Google alerts and searches. (See more 2007 trends and highlights on page 16)
Percentages of Email Identified as Spam

Defined:
Worldwide Internet Mail Gateway Spam Percentage represents the number of messages that were processed and classified as spam versus the total number of messages processed when scanned at the mail gateway. This metric represents SMTP layer filtering and does not include the volumes of email detected at the network layer.

A trend line has been added to demonstrate a 7-day moving average.
Global Spam Categories

**Defined:**
Spam category data is collected from classifications on messages passing through the Symantec Probe Network.

**Global Category Count**

- Financial: 15%
- Adult: 6%
- Fraud: 7%
- Health: 9%
- Internet: 18%
- Scams: 12%
- Leisure: 6%
- Products: 27%
Category Definitions

- **Product Email attacks** offering or advertising general goods and services. Examples: devices, investigation services, clothing, makeup

- **Adult Email 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 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 misleading, or known to result in fraudulent activity on the part of the sender. Examples: Nigerian investment, pyramid schemes, chain letters

- **Health Email attacks** offering or advertising health-related products and services. Examples: pharmaceuticals, medical treatments, herbal remedies

- **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 email address, financial information and passwords. Examples: account notification, credit card verification, billing updates

- **Leisure Email attacks** offering or advertising prizes, awards, or discounted leisure activities. Examples: vacation offers, online casinos, games

- **Internet Email attacks** specifically offering or advertising Internet or computer-related goods and services. Examples: web hosting, web design, spamware

- **Political 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
Regions of Origin

**Defined:**
Region of origin represents the percentage of messages reported coming from each of the following regions: North America, South America, Europe, Australia/Oceania, Asia and Africa.
Percent Image Spam

Defined:
The total number of image spam messages observed as a percentage of all spam observed.

A trend line has been added to demonstrate a 7-day moving average.
Let the Olympics-related Spam Begin

Symantec has recently seen a scam purporting to be from the China National Offshore Oil Corporation that makes claims of winning money and a trip to the Beijing Olympics in 2008. The email looks like the usual “Winning Notification” lottery emails that are all too common. However, the twist is that not only do you “win” money, but you also win a trip to the 2008 Olympics. This is the first scam that Symantec has seen that targets the coming popularity of the 2008 Olympics in Beijing. In 2004, Olympics-related spam increased steadily in volume from the beginning of the year through mid-summer, and this new scam is likely a signal of more Olympics-related spam to come.

The China National Oil Corporation is currently a hot stock market pick and owns a certain portion of valuable crude oil worldwide. By utilizing this known company to promote a “free” trip to the Olympics, the scammer is looking to generate a lot of interest on this offer. And what does the spammer hope to receive in return? Valuable personal information. Here is a sample of one of the spam emails:

---

From: XXXXXX@hotmail.com
Subject: CONGRATULATION!!! Beijing 2008 Olympics games promotion

WINNING NOTIFICATION/ FINAL NOTIFICATION
We happily announce to you the results of the China National Offshore Oil Corporation Olympic LOTTO AWARDS,International online Sweepstakes …… which subsequently won you the lottery in the 2nd category i.e. match 5 plus bonus.
Our organization here in China decided to sponsor 100 eligible adults to visit the Peoples Republic of China in August for the Olympics and you have therefore been approved to start the process of opening line of communication with our agents in other to obtain visit permits.

Your agent will immediately commence the process to facilitate the release of your funds as soon as you contact him and provide him with the below details.
*Name of Winner:
*Address:
*Nationality:
*Sex:
*Tel:
*Occupation:
*Age:
*Amount Won:
*Lucky Nos:
*Ticket No:

---

The fact that the company this scam is purportedly coming from is a hot stock market pick right now, combined with winning money and a free trip to the Olympics, is bound to incite interest amongst recipients. This is a classic example of enticement. Scammers that pretend to come from a well known source immediately ease the recipient’s doubts using the “known” factor. Then, they offer up free goods. In this case, the free goods consist not only of money but also coveted Olympics tickets.
Britney, Lindsay and Donny Osmond Headline Meds Spam

It seems that Spammers will do almost anything to try and entice users to open spam emails. A recent rush of pharmaceutical spam subject lines has included gossip headlines concerning some of the most high profile celebrities. The body of the spam message consists of plain text format with randomized Viagra product offering domains.

The following are a few subject header examples.

- Subject: Kevin’s Flight with the Angels
- Subject: Lindsay Lohan Digs Fergie’s Handbags
- Subject: Britney Spears Shops at Bel Bambin
- Subject: Britney Spears Under LAPD Investigation
- Subject: Donny Osmond Backstage with ‘Dancing’
- Subject: Kevin Escorts Victoria’s Secret Angels To L.A
- Subject: Brooke Burke and David Charvet Baby News
- Subject: Beyonce billboard ‘upsets’ Vegas residents

| From: ”Contact” <sales@xxx |
| To: xxx |
| Subject: Britney Spears Under LAPD Investigation |

Our Great offers

Buy viagra at lowest price ever!

Here - http://www.xxxx

Directory Harvest Attacks Continue to Blight Spam Landscape.

November saw millions of blank messages being sent out as part of a concerted directory harvest attack. These messages with an empty subject and body seem to be of no obvious purpose for a typical end user so why do they exist? During a directory harvest campaign, spammers bombard email servers with “guessed” email addresses. The email addresses that are not rejected are assumed to be valid and added to spam lists for a subsequent spam attack. Symantec Antispam filters blocked well over 35 million of these messages in November.
Spammers Exploit Missing Child

An attack this month preyed on the public interest in the story of the missing British child, Madeleine McCann. The email contained a link to http://madeleine2007.notlong.com/, which redirected to http://internetwonderful.com/madeleine. The second site is designed to look similar to the official McCann family site, www.findmadeleine.com, however, it actually is set up to distribute a virus. The site also contains an unauthorized use of the Symantec logo and a number of Google ads for anti-virus products.

It should be noted that although the spam email also contains a link to the legitimate findmadeleine.com site, there is no connection between the spammers and the genuine site.
Spammers Sell Email Databases.
Symantec has for some time now observed spam emails offering large databases with email addresses and other personal information for sale, with the promise that it is the best way to attract new business. Recently, Symantec has noted some of these examples are written in Spanish and Italian, possibly in an attempt to attract new business.
Seasonal Spam Attacks

**Penny Stocks Use Thanksgiving Holiday Captions in Subject Line**

Penny stock spammers have recently taken advantage of the Thanksgiving holidays in the U.S. by using common personal Thanksgiving-related words in the subject emails.

The following are a handful of sample subject lines that have been seen in millions of spam messages, which are now being blocked by Symantec Brightmail Antispam Solution.

- Subject: Be thankful on Monday
- Subject: Got your fill of turkey this weekend?
- Subject: The holiday report
- Subject: Is there anymore stuffing
- Subject: Make sure you got the gravy cause here is the main course

Many of the subject lines are intended to trick end users into clicking into the email.

| From: xxx |
| To: xxx |
| Subject: Is there anymore stuffing |
| E Tgu Takes Off As World Looks To Energy Solutions |

5 Things to think about this weekend:

1. The worlds Energy resources are of major concern
2. Without much relief in site from authorities, businesses are looking for their own solutions to energy problems.
3. SensorStat, is already providing huge relief to businesses in Florida with reductions as high as 30 percent.
4. Hotels and other large facilities are already boast in the news about the relief e T G u has brought to there energy problems.
5. Increased exposure on eTg u from an upcoming media campaign next week will certainly draw attention from investors.

If there was ever a time to pay attention Monday is your day. Last weeks heavy trading grab a lot of attention and Wednesday and Friday saw a big move to push the prices down and grab large blocks of shares doubling previous days volume. Monday this thing is going to be on the move again, get in on the gap and reap the benefits as this thing starts to rise again.

**Replica Products a Favorite for Spammers this Holiday Season.**

Products such as replica watches and handbags have long been a favorite for spammers. As December unfolds, Symantec has observed that some spammers are using holiday keywords in the subject lines of some of their attacks.

Some examples of the seasonal spam subject lines include:

- Subject: The best Christmas gifts for your nearest and dearest
- Subject: Posh accessories at reduced prices for Christmas!
- Subject: Find the most luxurious Christmas presents
- Subject: The most attractive offers for Christmas shopping!
- Subject: Have you already bought all Christmas gifts
- Subject: Christmas sale of awesome watches, pens, and lighters
- Subject: Surprise your beloved one with the most elegant Christmas present
Spam Begins to Snowball

Chain e-mails have always been a source of annoyance for many. This winter season, Symantec has observed some emails with subjects like “Wonderful News!” and “Guess What?!” Upon analysing this message, a gif image appears of a sneaky character that proceeds to throw a snowball. While this might seem like harmless fun, it’s far from it as email addresses can be harvested through the use of the snowball image. Each time the email is read, a request is sent to the server hosting the image and the user’s email address is stored in a log file on the spammer’s server. This would appear in the log as: http://example.com/bug.gif?person@domain.com.

So be careful when forwarding such emails to friends and family because even if your intention is harmless you may actually be handing their email address to a spammer.
Christmas Freebie Anyone?

Feeling the financial pinch this holiday season? Fancy a free gift worth £250 at Marks & Spencer’s department store? The following example shows a spammer using a well known UK brand to trick end users. The Subject titled Christmas Freebie reads:

“Hey, For a limited time only you can claim a FREE £250 Gift Card from Marks & Spencers!” Upon clicking the link to receive the gift card the user will be told “Sorry this offer is not available in your area. You’ll be redirected shortly.” The user then finds they have been duped – there is no £250 gift, just a bogus chat site at the end of the link. Ba Humbug!
Seasonal Lotto Scams

In a scam targeted at UK end users, spammers have updated a lottery spam email to a Christmas Bonanza special. The premise behind this scam attack remains the same as other lottery scam emails (i.e. in order to claim your prize, send personal information to a typically bogus entity or sender).

```
From: UK PRIME
Date: 17 November 2007 08:34
To: none
Subject: GOODDAY

Attention Winner
You have won the sum of 850,000.00, from the UK PRIME PROMO on our 2007 XMAS bonanza. The winning ticket was selected from a Data Base of Internet Email Users, from which your Address came out as the winning coupon. We hereby urge you to claim the winning amount quickly as this is a yearly lottery. You are therefore requested to contact immediately our Claims Department below quoting your winning numbers: WINNING NUMBER: (13)-(43)-(06)-(15) bonus # (09).
Max Ralph tel. (+44-7031949372 or +44-7045732204)
E-mail: maxralph14@gmail.com
Endeavor to email him your full names, winning numbers, email address, telephone and fax numbers immediately.
Yours Sincerely,
Marrow Juliet.
```
Special Spotlight: 2007 Year in Review

Bill Gates’ 2004 prediction of spam being eradicated within two years definitely missed the mark. But no one could have predicted the dramatic resurgence of spam in 2007, peaking at 72% of all email traffic.

Image spam was on the forefront of this resurgence, causing anti-spam vendors to come up with new techniques to detect and block these new attacks. And the creative tactics didn’t stop there. Spammers launched several spam “firsts” throughout the year, including tactics using bot herders, audio and video files, and Google alerts and searches. They also explored different protocols and platforms such as Instant Messaging, SMS and even multi-player online games.

And while spammers proved to be more evasive and sophisticated than ever, those on the anti-spam front increased their efforts to crack down on spam. There was the FBI’s Bot Roast program, the SEC’s Operation Spamalot, ISPs sharing more information, and anti-spam vendors deploying the latest blocking technologies.

Despite all the industry discussion about data loss prevention, virtualization and IT risk management, 2007 was still a headline year for spam.

Here are some notable facts and events that stand out:

**Spam Growth Trend (Average percentage of all email traffic):**
- July-Dec 2005: 50%
- Jan – June 2006: 54%
- July-Dec 2006: 59%
- Jan-Nov 2007: 70+% 

**Spam Firsts in 2007:**
- Teaming with botherders (Storm worm/Peacomm Trojan)
- Audio (MP3) and video use (i.e. YouTube)
- Leveraging Google Alerts and Search
- Use of different protocols/platforms (e.g. IM, SMS, and multi-player online games)

**Events:**
- FBI Bot Roast
- SEC Operation Spamalot
- ISP Information Sharing

**Broad Trends:**
- Image Spam (Mr. Ransom, Newsletter Spam, etc): Rapid increase, continual evolution, and steady decline to a small overall fraction
- Attachment Spam (PDFs, Zip files, etc.): Burst onto the scene with rapid increase, some expected evolution, rapid decline to nearly nothing
- Pump-and-Dump Stock Scam Spam: Remained one of the top categories of spam (21% 1H07, 30% decline from 2H06 attributed to SEC operation); continual evolution
- New Social Engineering (Beijing Olympics, California Wildfires, Saddam Hussein Execution, etc.)
- Fraud and Scam Spam: Steady increase and evolution (i.e. twists to 419 scam, Ecards, etc.)