Contributors

Kelly Conley
Manager
Symantec Security Response

Robert Vivas
Supervisor
Symantec Security Response

Sohan Mirajkar
Technician
Symantec Security Response

Sammy Chu
Technician
Symantec Security Response

Hitomi Lin
Technician
Symantec Security Response

Takako Yoshida
Customer Response Analyst
Antispam Engineering

Amanda Grady
Customer Response Analyst
Antispam Engineering

Eli Mantel
Sr. Software Engineer
Antispam Engineering

Shravan Shashikant
Pr. Business Intelligence Analyst
Antispam Engineering
Monthly Spam Landscape

This month’s report shows that spammers were more naughty than nice this past holiday season. As 2007 ended, spam surged and accounted for 75 percent of all email (up from 72% in November), increasing to 83 percent in the last few days leading up to the Christmas holiday.

Highlights from this month included:

- **Holiday Spam Spikes:** Spam levels reached new levels as spammers inserted holiday-oriented keywords into everything from subject lines to images.
- **Spammers Get Honest? Not So Fast:** Spammers tried a new twist on an old scam, falsely promising past spam victims restitution of $100,000.
- **As Oil Prices Hike, Spammers Strike:** This new spam claims to identify gas stations that fraudulently tamper with pump prices.
- **Not-So-Happy New Year:** Recipients were invited to download a fun New Year’s song and dance, but instead found themselves downloading something far more malicious.
- **Presidential Polling Scam:** Promising gift cards in exchange for opinions, spammers leverage the US presidential primaries to collect personal information.
- **Beware of Blogs:** The use of blogs within spams appears to be on the rise, particularly in China where simplified character sets are common.
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: 14%
- Scams: 10%
- Products: 30%
- Leisure: 6%
- Internet: 20%
- Health: 8%
- Fraud: 6%
- Adult: 6%
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.

Global Claimed Region of Origin

[Bar chart showing the percentage of messages from different regions: North America, South America, Europe, Australia/Oceania, Asia, and Africa. The chart indicates that Europe and North America have the highest percentages.]
Spammers Shift Focus to Holidays

As expected, spammers got extra busy during the holidays. Spam levels inched up and hovered at 75 percent of all email for most of the month, then increased as high as 83 percent in the last few days leading up to the Christmas holiday.

While the majority of the spam messages encountered in December consisted of the common spam we are all accustomed to seeing, spammers did modify their URLs with holiday-related keywords and phrases to give them a more seasonal appeal. Below are a few examples:

- replica4christmas.com
- buyholidaygiftshere.com
- discountedholidaygifts.com
- xmasgiftsfast.com
- cheapholidayoem.com

Spammers also modified the Subject lines of their emails to invoke the holiday spirit. Examples include:

- Subject: Christmas special offer
- Subject: your expected xmas gift will be your increased PE!
- Subject: Enjoy your holiday season with a new designer purse on our tab!
- Subject: Looking at buying your partner or loved one a beautiful gift this Christmas?

Even image spam was not immune to modification during the holiday season. Spammers inserted the same key seasonal words into their image spam offerings in an effort to plant ideas for holiday gift giving into consumers’ minds. Some examples of this are below.
Spammers Get Honest? Not So Fast

419 spammers who have traditionally used stories about African dictators to defraud individuals have recently changed their approach to these types of emails. Certain 419 scams observed by Symantec this month claim to offer compensation to victims of 419 scams. The scam states that payments will be supervised by UN officials and about 150 scam victims will be paid compensation of $100,000 each. It provides some URL links as a reference to money that was successfully recovered by 419 scam victims. At the bottom of the email, it explains how the money may be recovered and the fraudulent background of such emails may be observed.

You can receive your compensations payments via any of this options you Choose, DRAFT/CHEQUE PAYMENTS or WIRE TRANSFERS. I shall feed you with further modalities as soon as I hear from you.

Send a copy of your response to the official email:

barr.davolateju@hotmail.com

Yours faithfully,

Barrister David Olateju (esq).
E-mail : barr.davolateju@hotmail.com
As Oil Prices Hike, Spammers Strike

With the increasing speculation surrounding oil prices, an interesting spam email with the Subject line, “Lista de Gasolineras Fraudulentas,” was recently observed by Symantec. The email informs consumers that they can download a tool to obtain a list of gasoline stations that have been tampering with gas pumps to fraudulently overcharge for gasoline. This spam purports to have been sent by the Mexican Federal Consumer Protection Agency, but the download is actually a Trojan horse.
Not-so-happy New Year

Symantec has recently observed a spam run which attempts to help recipients celebrate the arrival of 2008 with a song and dance.

As you embrace another New 2008 Year
A New 2008 Year song
Dance to the New 2008 Year tune

When the user clicks on the link they are informed:
“Your download should begin shortly. If your download does not start in approximately 15 seconds, you can click here to launch the download and then press Run. Enjoy!”

The download is not a fun song or interesting tune, but is one of two malicious files, Happynewyear2008.exe or Happy_2008.exe. Both are variants of the Storm Worm.

Presidential Polling Scam

Spammers continue to show that they are up to date on current events. As the US presidential primaries heated up, a new gift-card spam emerged. Recipients were offered a chance to receive a $500 gift card in exchange for their opinion about Hillary Clinton’s chances of winning the 2008 elections. Instead, users were directed to a site asking for and collecting personal information about the recipient.

Subject: Tom Get a Free Gift Card for voting (Participation required. See details)

Do you think Hillary will win the 2008 presidential election? Answer now for your chance to get a $500 Visa™ Gift Card—and make sure your voice is heard!
**Attack of the Chinese Blogs**

Over the past few weeks, the frequency of Chinese spams directing recipients to blogs appears to be increasing for both the traditional and simplified characters set though most of the attacks appear to be targeting the simplified character region which is China. The categories of products being advertised in this spam type are virtually unlimited from educational products to business opportunities.

Promoting products from a public, personal blog is one of the most cost-effective spamming techniques at the spammer’s disposal. Why is this so? Blog sites are free. Traditionally spammers have hosted their wares on their own domains that they pay for. But with the abundance of free blog sites out there they can host their wares for free. Another added bonus for the blogger is that if one particular blog gets blocked by mail filters they can just move their content to another free blog.

Some examples of the Chinese blog spam are below. Each sample contains a brief description of the product and a URL link to the blog where you can see more details and purchase the product. The purchasing method is up to the promoter. Two of the purchasing methods observed include:

Emailing the spammer your product list with a COD payment
Clicking on a link to enter your credit card information.

From what Symantec has observed it seems that this new technique is being heavily tried out in the Chinese spammer circles to evaluate its effectiveness.