The State of Spam
A Monthly Report – June 2007
Generated by Symantec Messaging and Web Security

Confidence in a connected world.   symantec™

Monthly Spam Landscape

Spam activity in May 2007 was overall consistent with trends observed in previous months. However, the decline in image spam first reported in the Symantec State of Spam report May 2007, does continue.

Highlights included:

• The trend of image spam's decline continued averaging at 16% for the month of May, down from 27% and 37% in the months of April and March respectively. At its peak in January 2007, Symantec estimated that image spam accounted for nearly 52% of all spam. With the recent decline in image spam, Symantec has observed an increase in spam which use links and embedded URLs to reference images contained in spam.

• Although the percentage of image spam has declined recently, overall spam levels remained consistent for the month of May at the SMTP layer and remained on average around 65%.

• Scams and fraud spam combined continues to rise from 9% in March to 13% in May.

• Additional insight is provided below on the following tactics:
  – Focus on spam which uses links and embedded URLs to reference images.
  – 'Tis the season for Mother's Day spam.
  – 419 spam continues to evolve
  – Spam spotlight: Regional spam trends for APJ.

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.
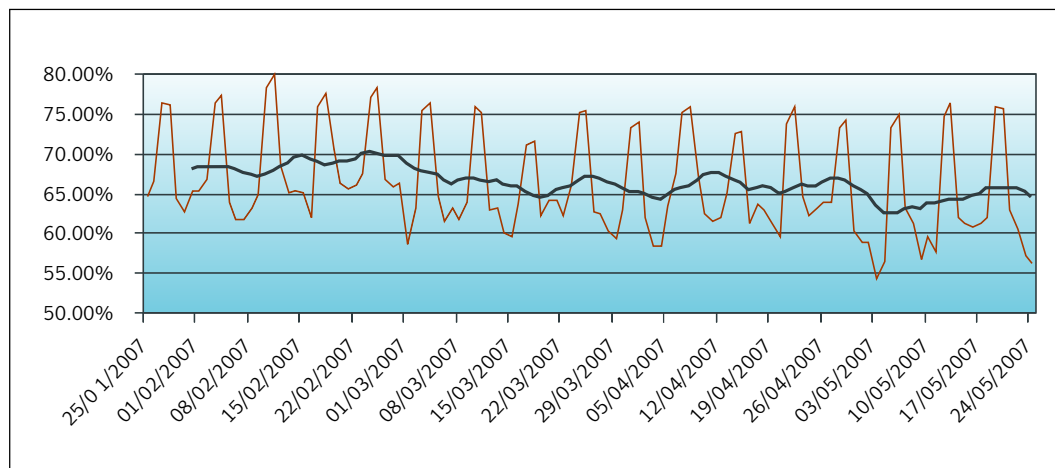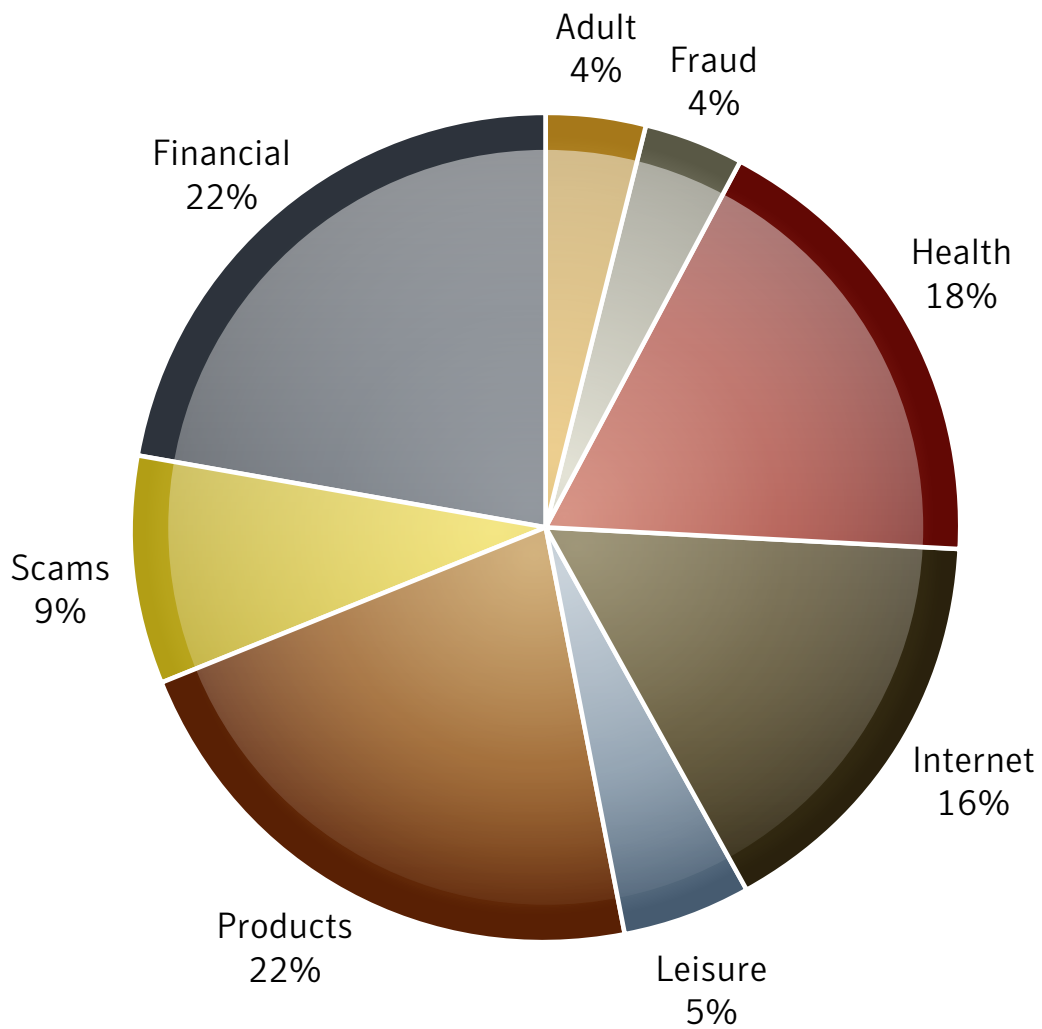

A trend line has been added to demonstrate a 7-day moving average.

Global Spam Categories

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

Global Spam Categories (90 Days)

Adult
4%

Fraud
4%

Financial
22%

Health
18%

Scams
9%

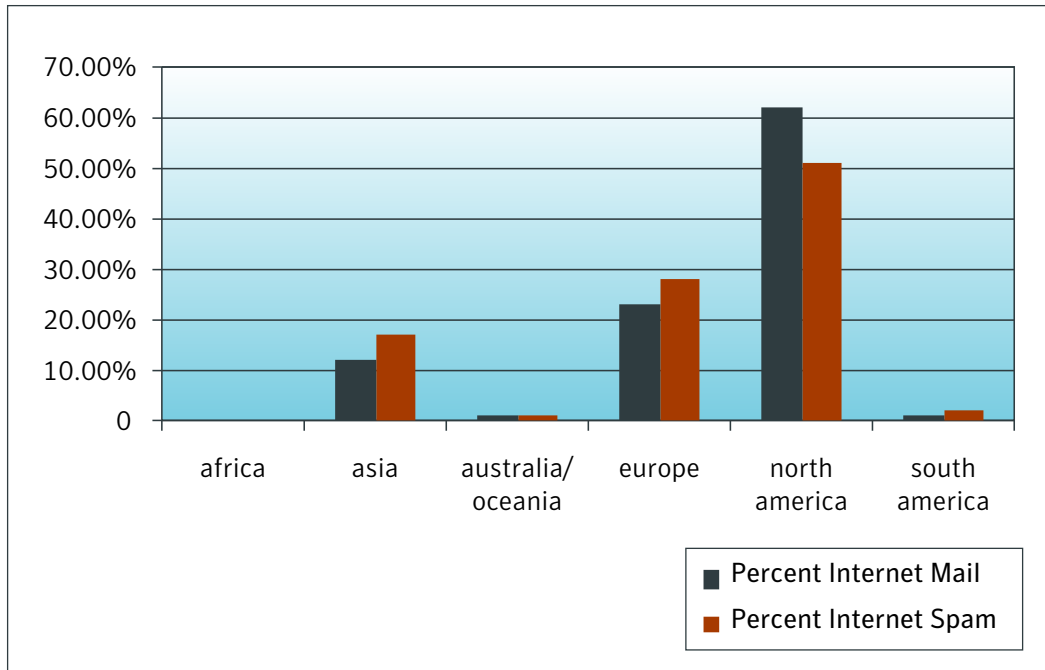Internet
16%

Products
22%

Leisure
5%

Category Definitions

- **Products 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 misguiding, 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**

- **Spiritual Email attacks** with information pertaining to religious or spiritual evangelization and/or services. **Examples: psychics, astrology, organized religion, outreach**

- **Other Emails attacks** not pertaining to any other category.

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.
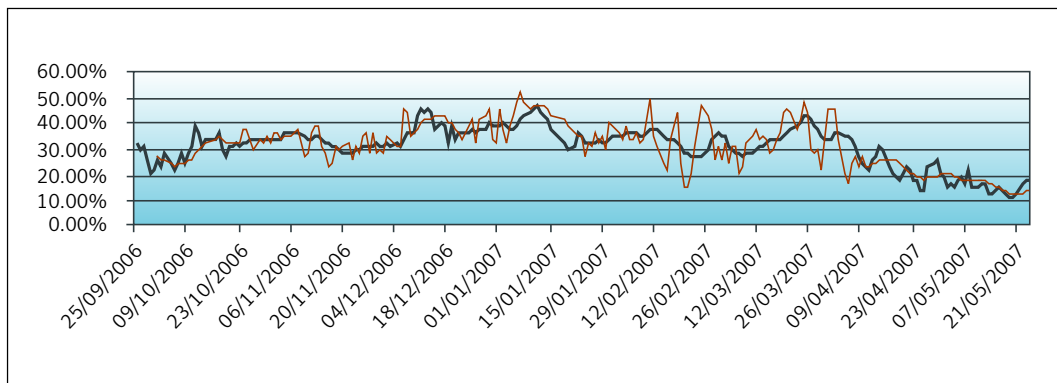
Percent Image Spam

Defined:

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

Internet Email – Percent Image Spam

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

Additional Insights

Focus on spam which uses links and embedded URLs to reference images

As discussed in last month's Symantec State of Spam report, image spammers are using alternate methods to direct recipients to specific images. Symantec highlighted how spammers were using legitimate image upload solutions as part of their spam attacks. This month, Symantec has observed a renewed focus on spam which contains links and embedded URLs which reference images. The following example shows the spam message with the embedded links displayed and later shows the message as it would be displayed for the recipient.

Guess spammers have mothers too?

Mother's Day is celebrated on different days around the globe. In the USA, mother's day is celebrated on the second Sunday of May each year. It is traditional that Mothers receive gifts and cards on this day. This year, spammers too offered the typical fare of gift cards, jewelry, and flowers for those celebrated mothers. The following are examples of the two most common types of Mother's Day spam observed this year.

419 Spam continues to evolve

As discussed in last month's Symantec State of Spam report, we continue to see 419 spam take on new and interesting twists. 419 spam which was typically used to offer oil and gas reserves in some African country has developed into this type of attack where a prospective career is offered to the recipient.

From: xxxx
To: xxxxx
Sent: May 2007
Subject: Job offer #277
Hello

My name is Roman Frolov. I am a manager of Bidding Expert Company.

We would like to offer the perspective career to you. We propose a vacancy of the regional agent. The average salary will be about $2000-4500 monthly. You can familiarize with our current vacancy.

REASON : Most customers prefer to pay within their own country and its much faster than sending an international Money Order. Small companies can't transfer international transactions. And have restricion to do international transfers. But our personal clients have business in Russia, Ukraine and other CIS countries, and they can't receive international payments. Your task is receiving and transferring payments to our clients.

You will receive and cash out several types of payments: Direct Bank Deposit, PayPal payments and rarely Money Orders. Having a PayPal account gives you an advantage of accepting even more payments.

1) Your salary is 15% from each payment.
2) You don't need to wait end of month to get paid. You salary share included to each payment.
3) You not spend your own money. All charges to withdrawal or transfer money will be shared at

payment
4) Your financial information will never reach to third parts. Its safe, private and secured type of PayPal payments.
5) You can work 1-3 hours per day or fulltime.
6) No matter whats your education or status.

You can contact with me and ask any questions by email: xxx@

Spam spotlight: Regional spam trends APJ.

- Scams spam accounts for 17% of all spam attacks in the Asia Pacific and Japan (APJ) region. This compares with a global figure of 9% for this type of spam. This could partly be accounted for by the prominence of invoice spam which is unique to this region.

- Notable regionalized spam attacks.

APJ Category Count
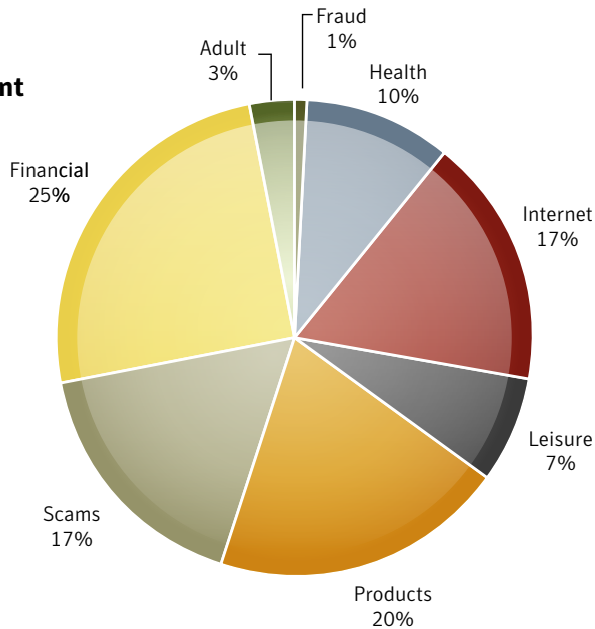
Notable regionalized spam attacks.

Invoice spam

Invoice spam remains one of the most common types of spam in this region. The premise behind this type of spam is that a 'legitimate' company will create a fake invoice and try and sell it to generate profit. In the example below, the spammer purports to be associated with a large trading company. It offers 'legitimate' invoices for sale and includes contact information so that the sale may be completed.

Invoice spam may also contain images and in this next example a 'legitimate' invoice is also offered to the recipient

Training spam

Another interesting type of spam that is unique to the APJ region is training spam. This spam attack invites the recipient to register for a class that a famous professor has been asked to attend.

From: xxx
Subject: 高管人员薪酬设计方案 665206

Date: May 2007

课程针对性的解决现实问题并培养实操技能。本课程注重实际问题的解决和学员实操技能的培养。课程中大量使用中国企业实际操作案例，集借鉴与点评为一体，注重培养学员的实操能力。课程中涉及到岗位分析、职位评估、薪酬设计、任职资格（能力）管理等方面。学员在培训结束后即可依照课程所学重新优化改造本公司人力资源管理相关模块的工作。

● 会 务 报 名
1. 会 务 组 织：创威咨询
2. 费 用：2 8 0 0元/人（含讲义、午餐、茶点、合影、通讯录）
3. 电 话：07 55-2 8 5 8 0 9 1 6 传 真：0 7 5 5-2 8 5 8 1 1 2 9
4. 报 名 方 式：电话登记-->传真确认-->发出会务确认函-->转帐报名