The State of Spam

A Monthly Report – April 2007

Generated by Symantec Messaging and Web Security

Confidence in a connected world.

Monthly Spam Landscape

Spam activity in March 2007 was fairly consistent with trends observed in previous months. Highlights included:

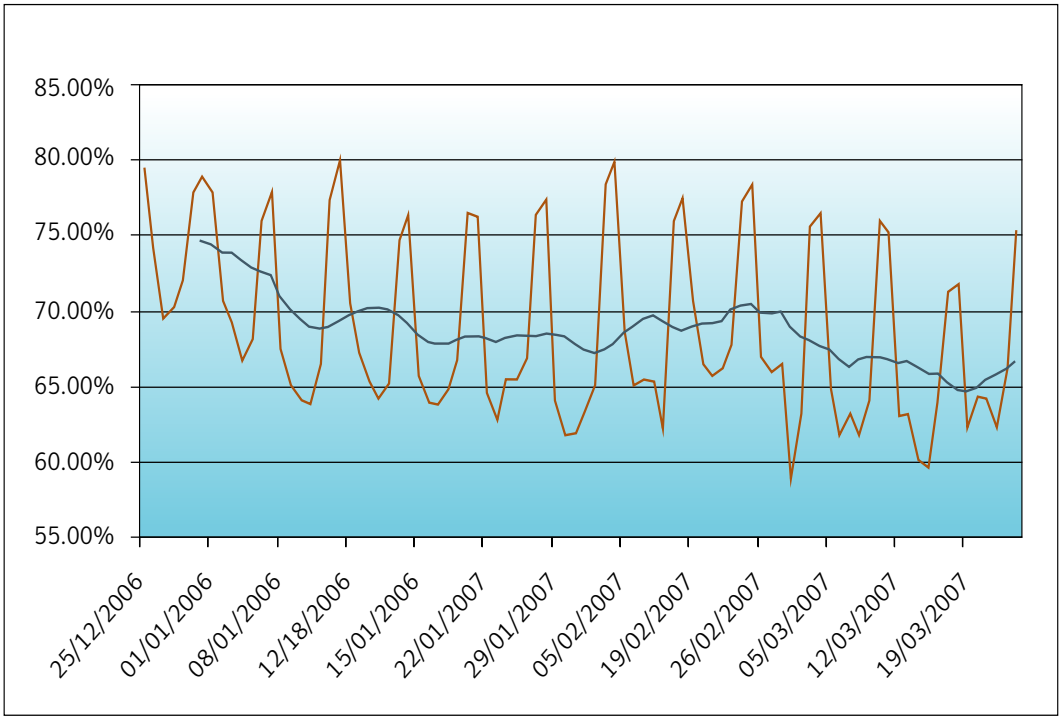
- Image spam percentages remain volatile and ended the month of March at a rate of 37%.
- Spam levels remained consistent for the month of March at the SMTP layer and remained on average around 65%.
- Technique reemerges in an effort to hide Phishing URLs.
- Spam spotlight: Regional spam trends EMEA.

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.

Internet Email Spam Percentage

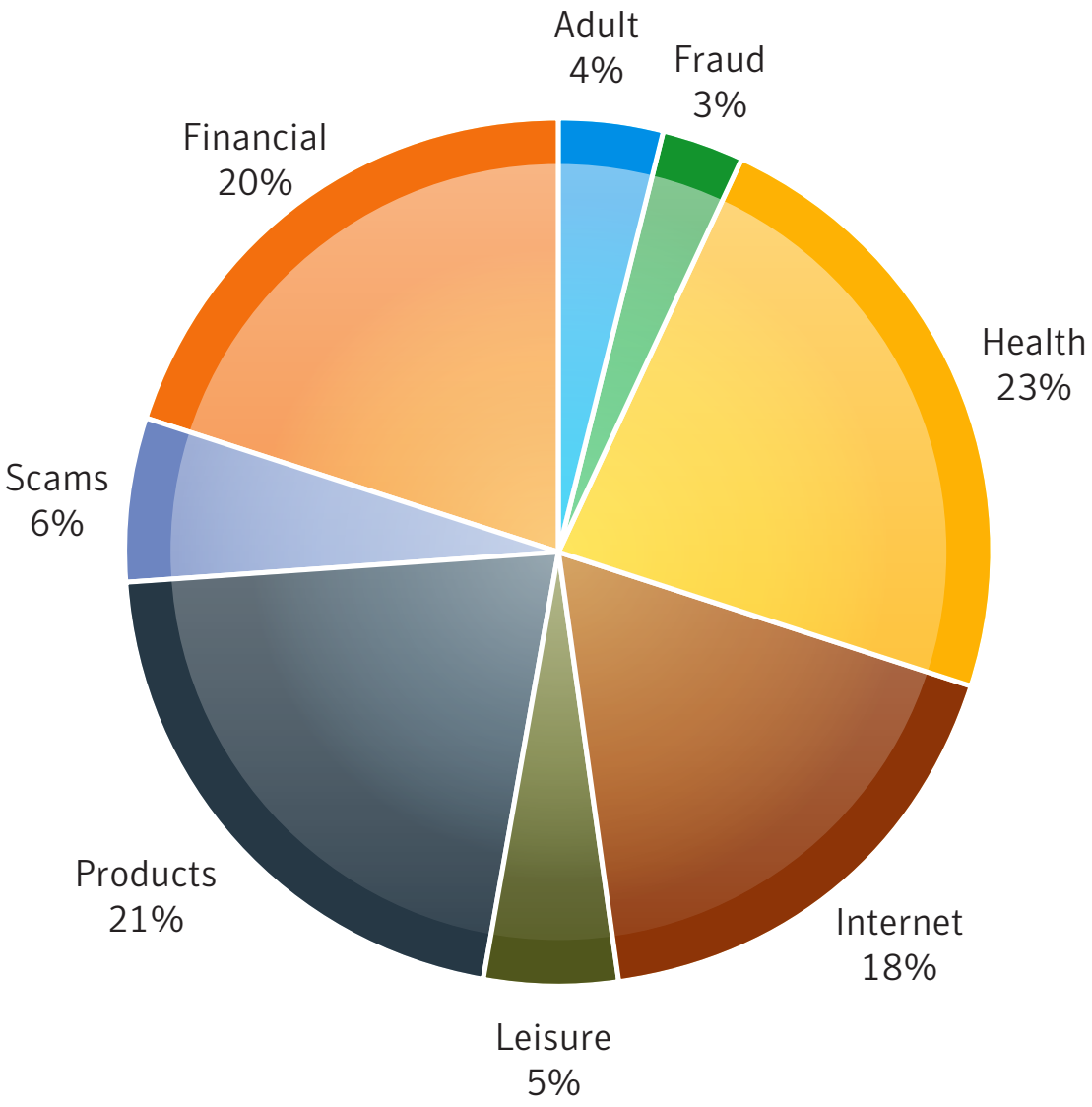


A trend line has been added to demonstrate a 7-day moving average.

Global Spam Categories

Defined:

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



Global Spam Categories

Defined:

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

Category Definitions:

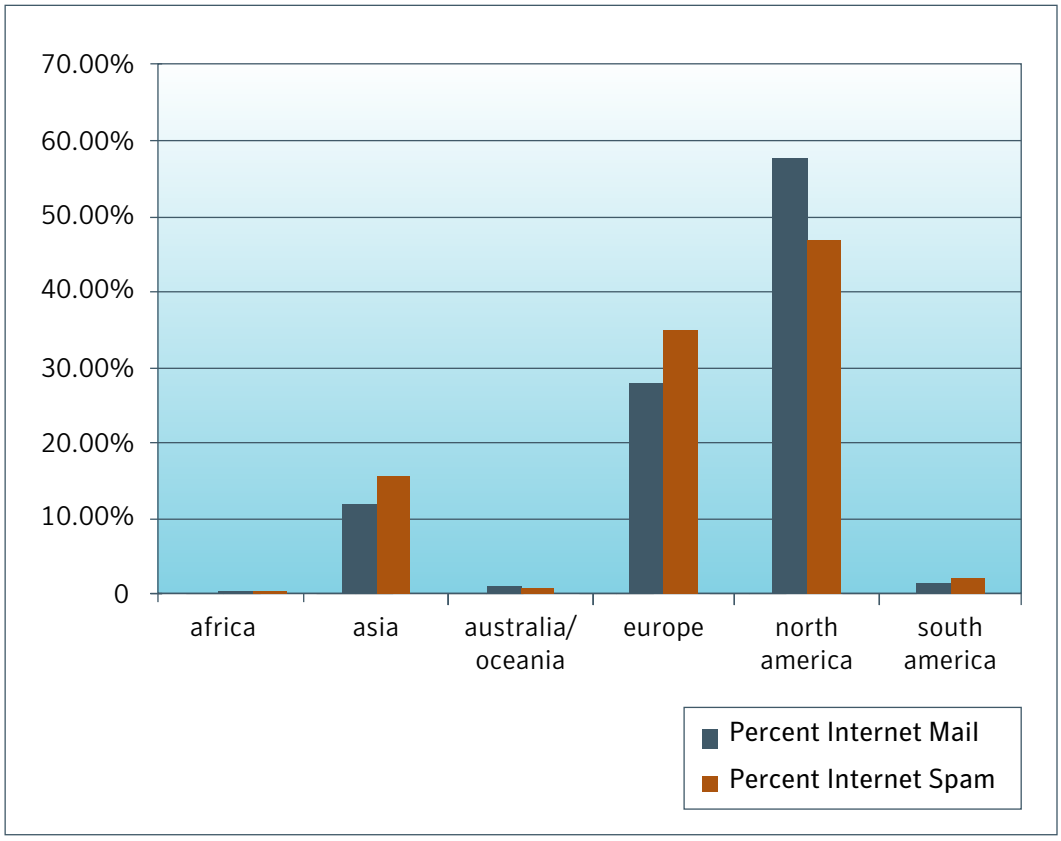
- **Products Email attacks** offering or advertising general goods and services. Examples: devices, investigation services, clothing, makeup
- **Adult Email attacks** containing or referring to products or services intended for persons above the age of 18, often offensive or inappropriate. Examples: 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.

Global Claimed Region of Origin (90 Days)

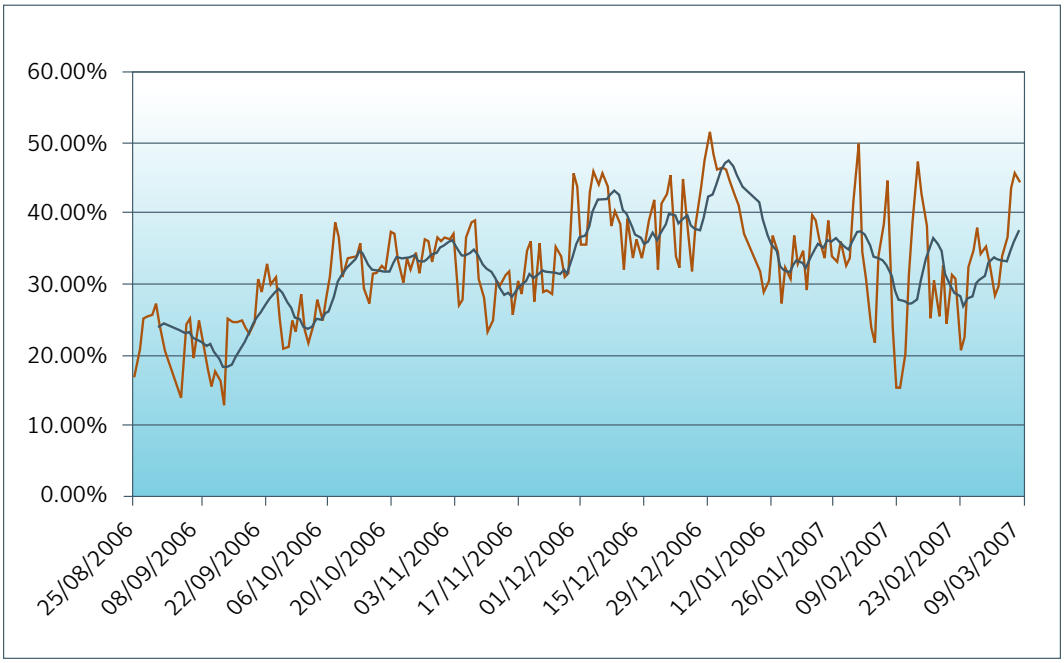


Percentages of Image Spam

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.

New Spam Techniques

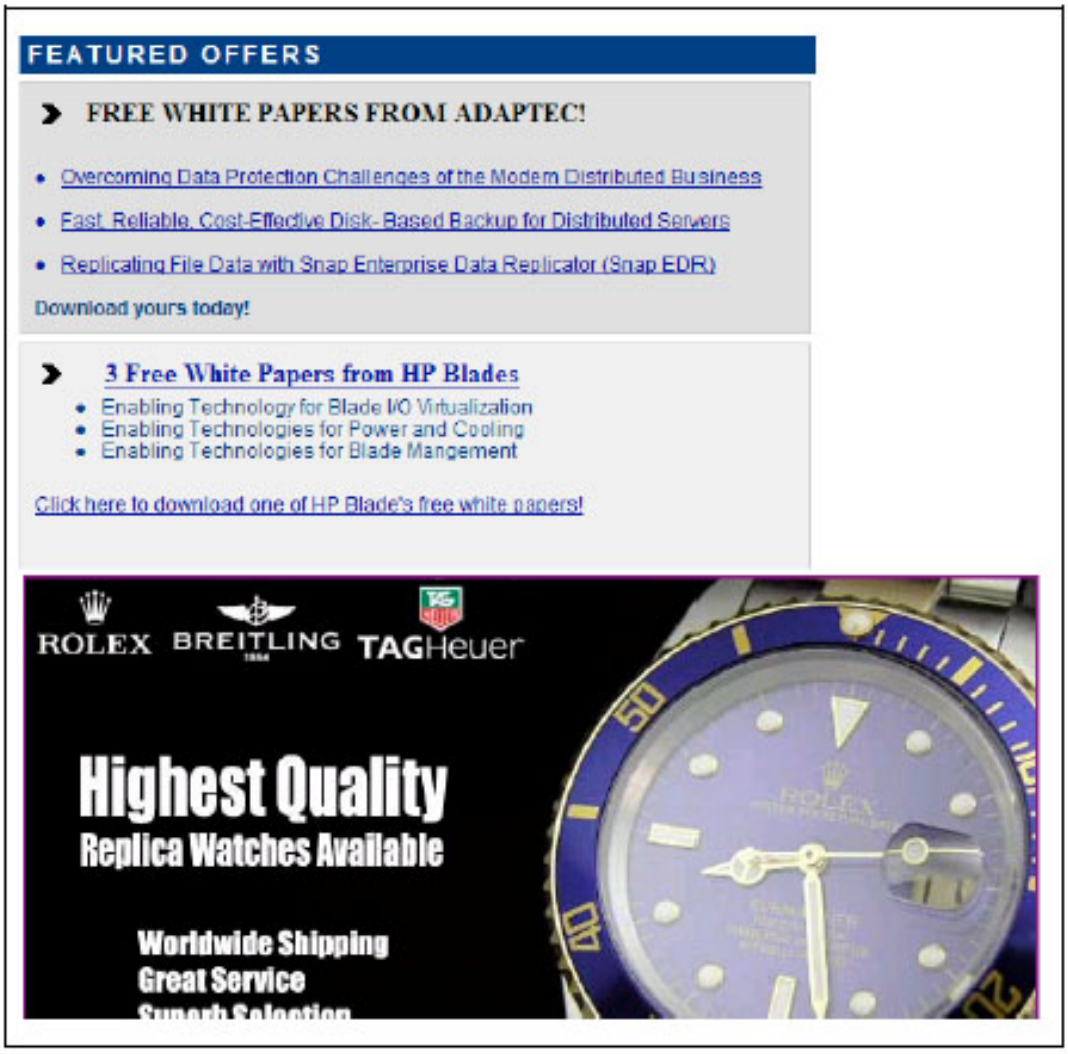
Spammers breaking up HTML links by using quotation marks (“”)

Symantec has recently analysed a spam message where the spammer used quotation marks to mangle the anchored link http. Spammers have always experimented with methods to try and evade URL filtering techniques and this seems to be another example of this

```
<html>
<Body onload='JsCriPt.enCODE:
s="h"+"t"+"t"+"p"+":"+"//"+"spammywebsite.com/spammyfolder'>
```

Time Has Yet to be Called on Replica Watch Spam

Seasonal spam attacks are common, but there has been a notable increase in replica watch spam. Replica watch spam is not a new technique, but one interesting feature of this particular replica watch spam attack is that it uses the hijack-spam technique. The body is often a legitimate-looking message such as a newsletter, which (at the end or beginning) contains a URL to a Web site selling replica watches. The headers however look like spam with the "from" and/or "subject" lines consisting of spam content. An example of such a message appears below.

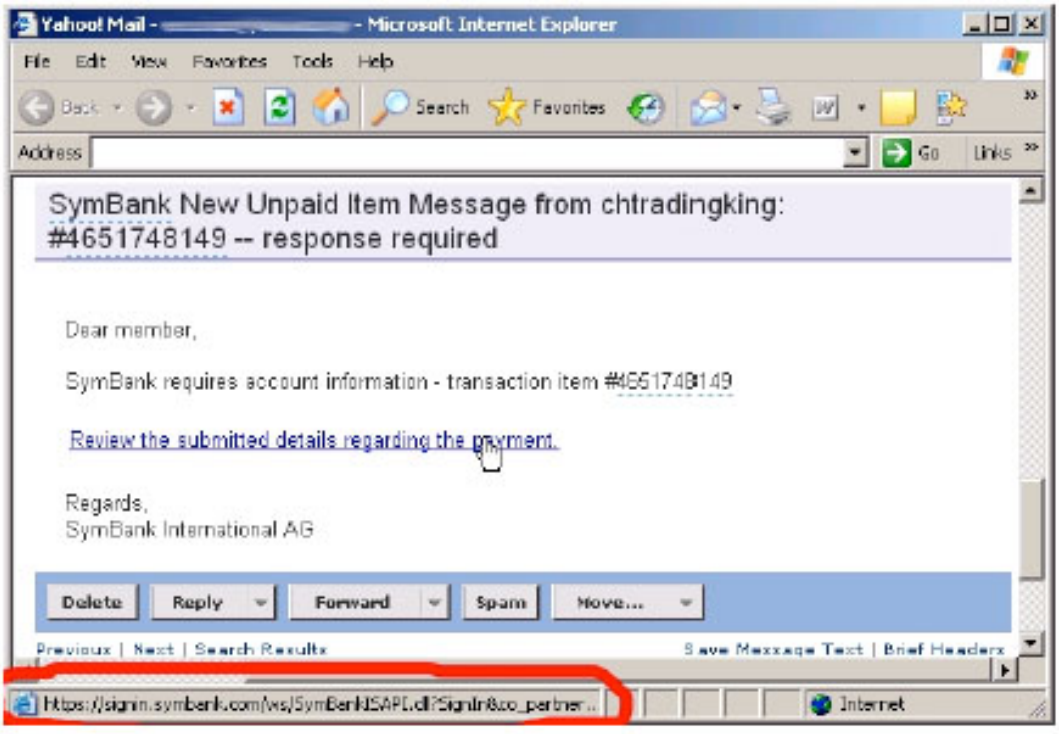


Spammers Revisiting Old Tricks

Technique reemerges in an effort to hide Phishing URLs
Symantec recently received a phishing email that made use of an interesting technique to hide a phishing site URL. When receiving a suspected phishing message, one of the methods of determining if the embedded URLs are legitimate is to pass the cursor over the underlined hyperlink and then check the URL in the status bar of your browser. In the status bar, you can see if the link belongs to the appropriate domain.

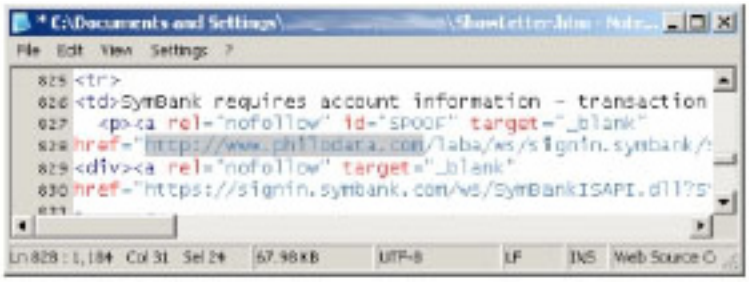
Using JavaScript, the text in the status bar can be altered. So when browsing on the Web, this is not always a reliable technique to verify the underlying URL. However when receiving an HTML email in an email client (including Webmail), JavaScript is generally neutered so it does not execute, preventing the obfuscation of the status bar via JavaScript, making this technique more reliable. However, the phishing message recently received is able to modify what is displayed in the status bar without the use of JavaScript. The message replaces the text in the status bar with the expected legitimate URL.

Take the following example, where a member of a legitimate bank known as “SymBank” is contacted (“SymBank” has been made up for the purpose of this example). The “SymBank” member receives a message asking them to login in order to verify some account transaction details. Hovering over the link, the URL appears valid, as shown in the below image:



However, looking at the HTML source of this email, it can be seen that if the linked is clicked by the “member” they will be redirected to a completely different site that will attempt to steal their credentials.

Fortunately, the URL in the status bar is only one indicator of a fraudulent message. If the "member" clicked on the URL, the resultant site would have the fake URL in the URL input area. However, this technique could possibly be used to trick someone into visiting a malicious web site and by the time that person realizes they are at a malicious web site, their machine may already have been infected.



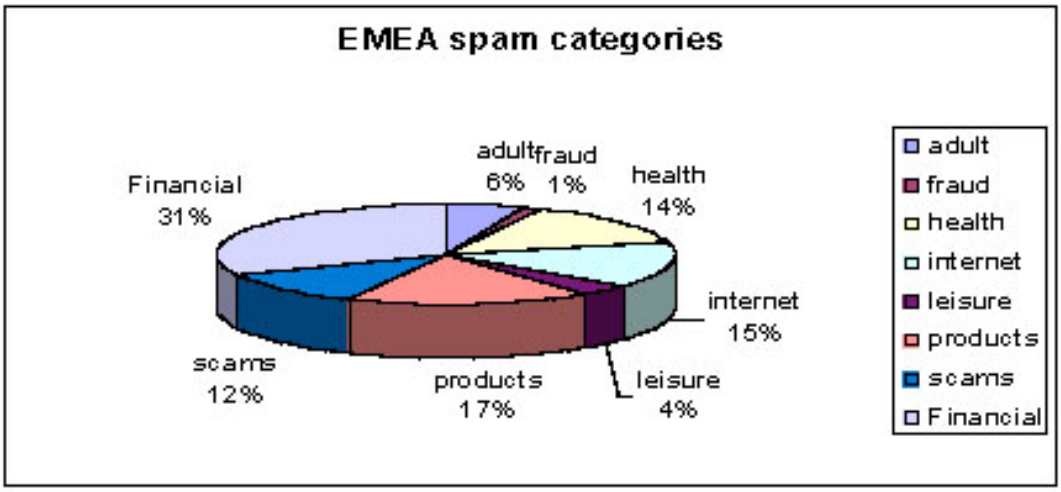
Spam Spotlight: Regional Spam Trends EMEA

- EMEA comes second only to North America as the principal source of spam messages.
- Financial spam accounts for more than 30% of all spam attacks in EMEA.
- Notable regionalized spam attacks.

EMEA Spam Categories

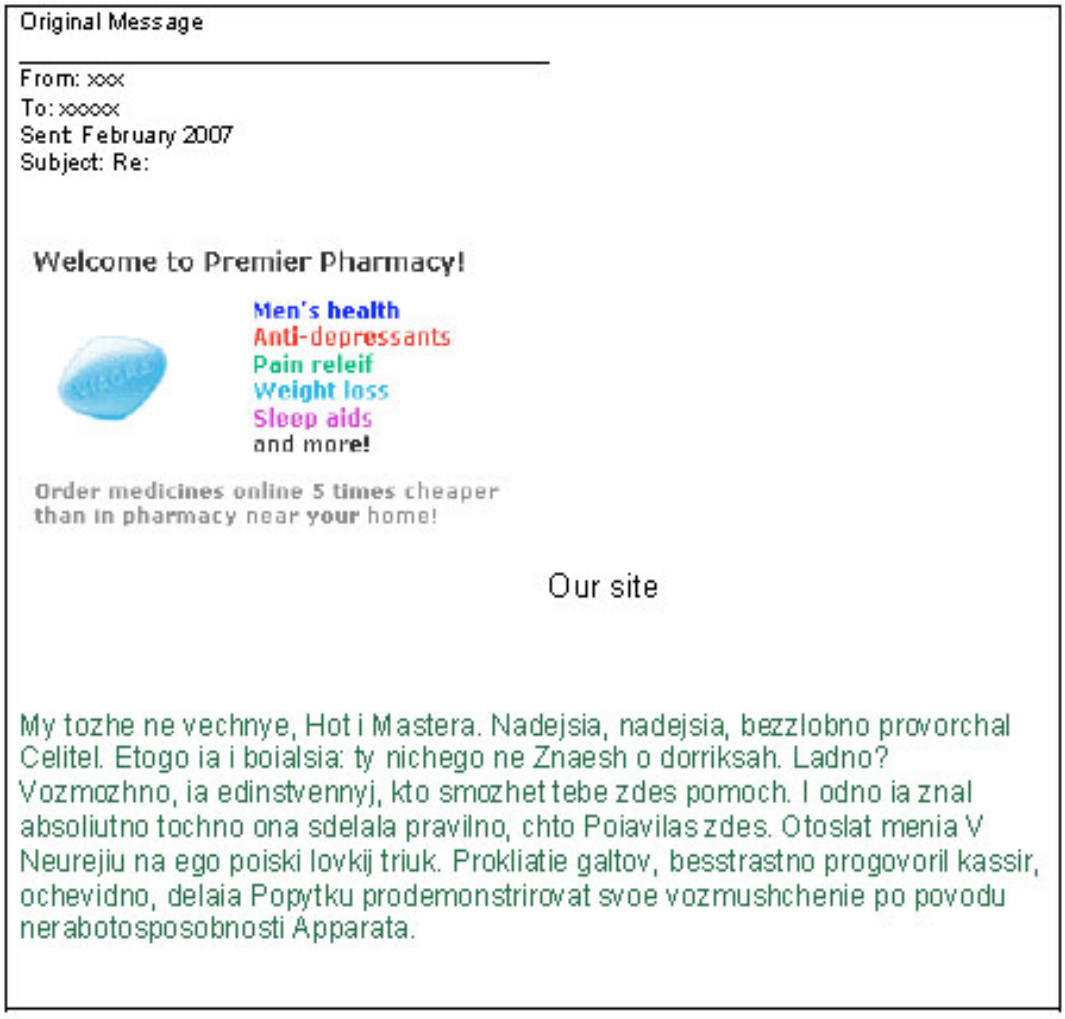
Defined:

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



Notable Regionalized Spam Attacks

Image Spam Takes a European Twist
Where once we saw random excerpts from Harry Potter books included at the bottom of image spam, a new spam technique is emerging where the spammer is now using Russian and German text in an effort to obfuscate certain anti-image spam filters. In the Russian samples, the "random text" is written in Russian using a non-cyrillic keyboard.

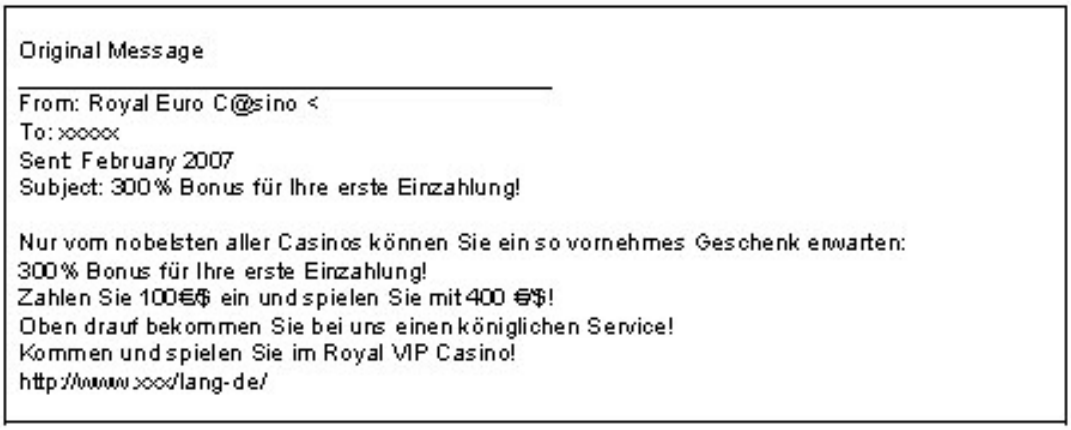


Spam Attacks Migrate into European Languages

Once only typically written in English, spam has now completed its migration into several European languages. The spam messages boast excellent bonuses if the individuals play in their VIP casinos. The URL contained in the message body directs to a URL of the form http://www.xxxxx.info/lang-it/.

The casino spam message has appeared in German, French and Italian messages.

At its peak this particular casino spam outbreak accounted for 70% of all non-English spam attacks.



Original Message

From: Royal Euro C@sino <
To: xxxxx
Sent: February 2007
Subject: 300% Bonus für Ihre erste Einzahlung!

Nur vom nobelsten aller Casinos können Sie ein so vornehmes Geschenk erwarten:
300% Bonus für Ihre erste Einzahlung!
Zahlen Sie 100€$ ein und spielen Sie mit 400 €$!
Oben drauf bekommen Sie bei uns einen königlichen Service!
Kommen und spielen Sie im Royal VIP Casino!
http://www.xxx/lang-de/