The State of Spam

A Monthly Report – August 2007

Generated by Symantec Messaging and Web Security

Confidence in a connected world.

Monthly Spam Landscape

While overall spam activity remained steady in July 2007, the tactics being used are clearly changing. Image spam is on the decline, while the use of document attachments like PDF is on the rise.

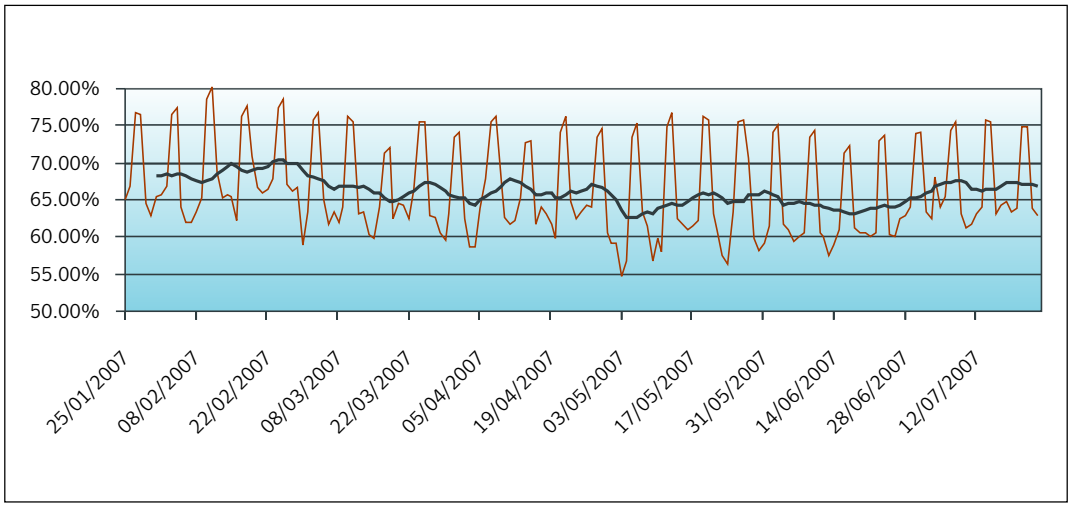
Highlights included:

- Image spam continued to decline and recorded its lowest percentage of total spam at 8% in mid July. At its peak last January, Symantec estimated that image spam accounted for nearly 52% of all spam.
- Overall spam levels at the SMTP layer in July remained consistent averaging 66% of total email.
- Additional insight is provided below on the following tactics:
  - PDF spam continued to increase and in July accounted for between 2% and 8% of all spam.
  - Excel and Zip files are increasingly being used as spam receptacles
  - Greeting card spam remains a spammer favorite.
  - Spam containing Chinese top level domains significantly increased.
- 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.



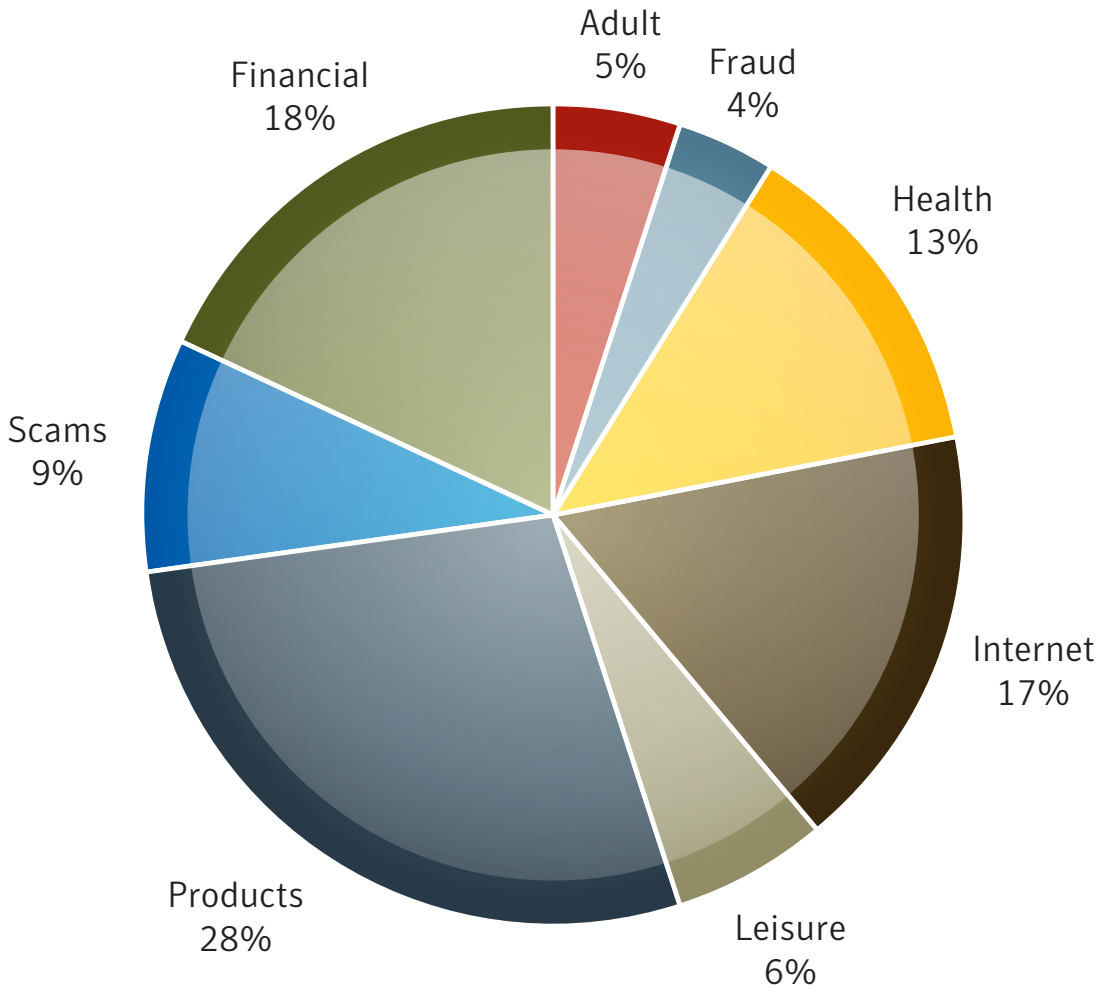
A trend line has been added to demonstrate a 7-day moving average.

Global Spam Categories

Defined:

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

Global Spam Categories (90 Days)



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 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

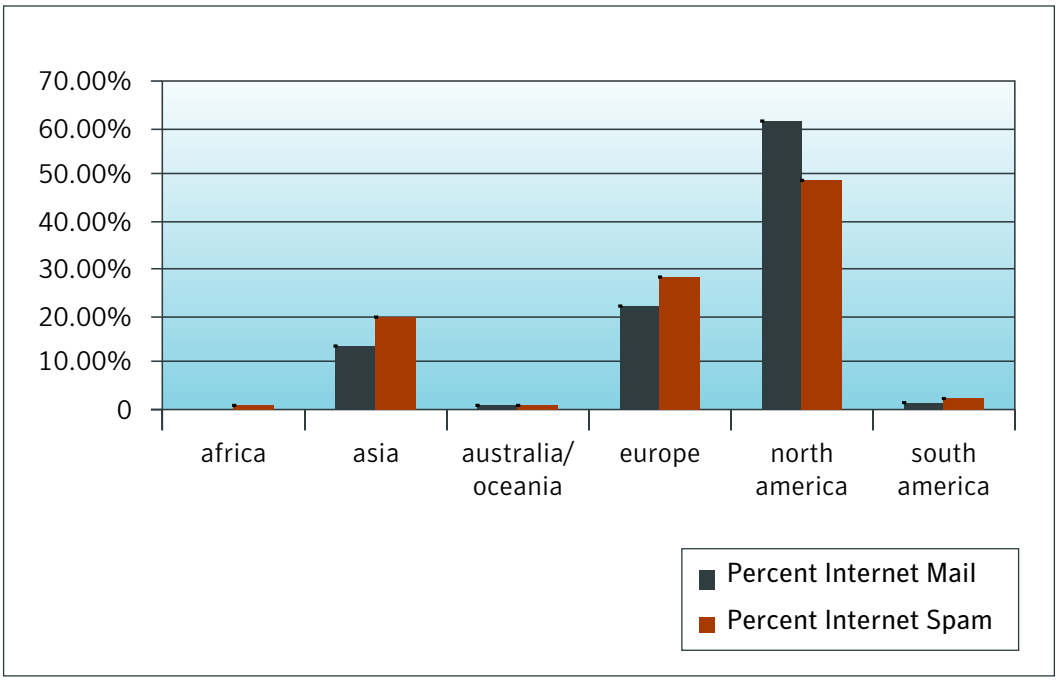
- **Spiritual Email attacks** with information pertaining to religious or spiritual evangelization and/or services. Examples: psychics, astrology, organized religion, outreach

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

Regions of Origin

Defined:

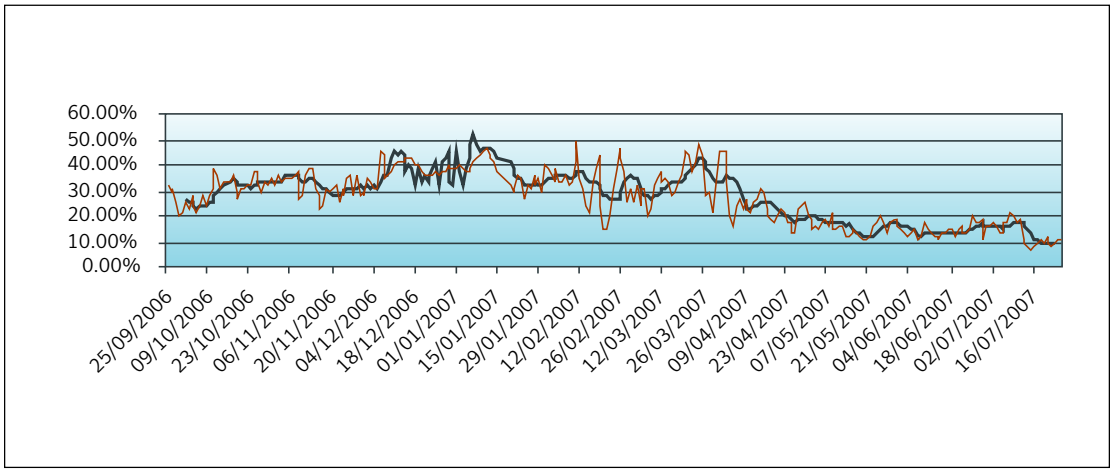
Region of origin represents the percentage of messages reported coming from each of the following regions: North America, South America, Europe, Australia/Oceania, Asia and Africa.



Percent Image Spam

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

Internet Email – Percent Image Spam



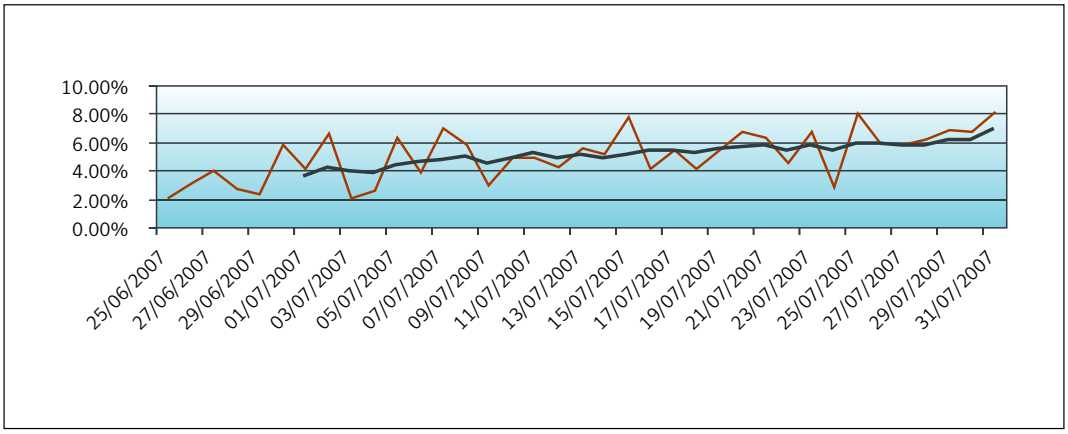
A trend line has been added to demonstrate a 7-day moving average.

Additional Insights

PDF Spam Continues With Excel And Zip Files Now Also Being Used As Spam Receptacles

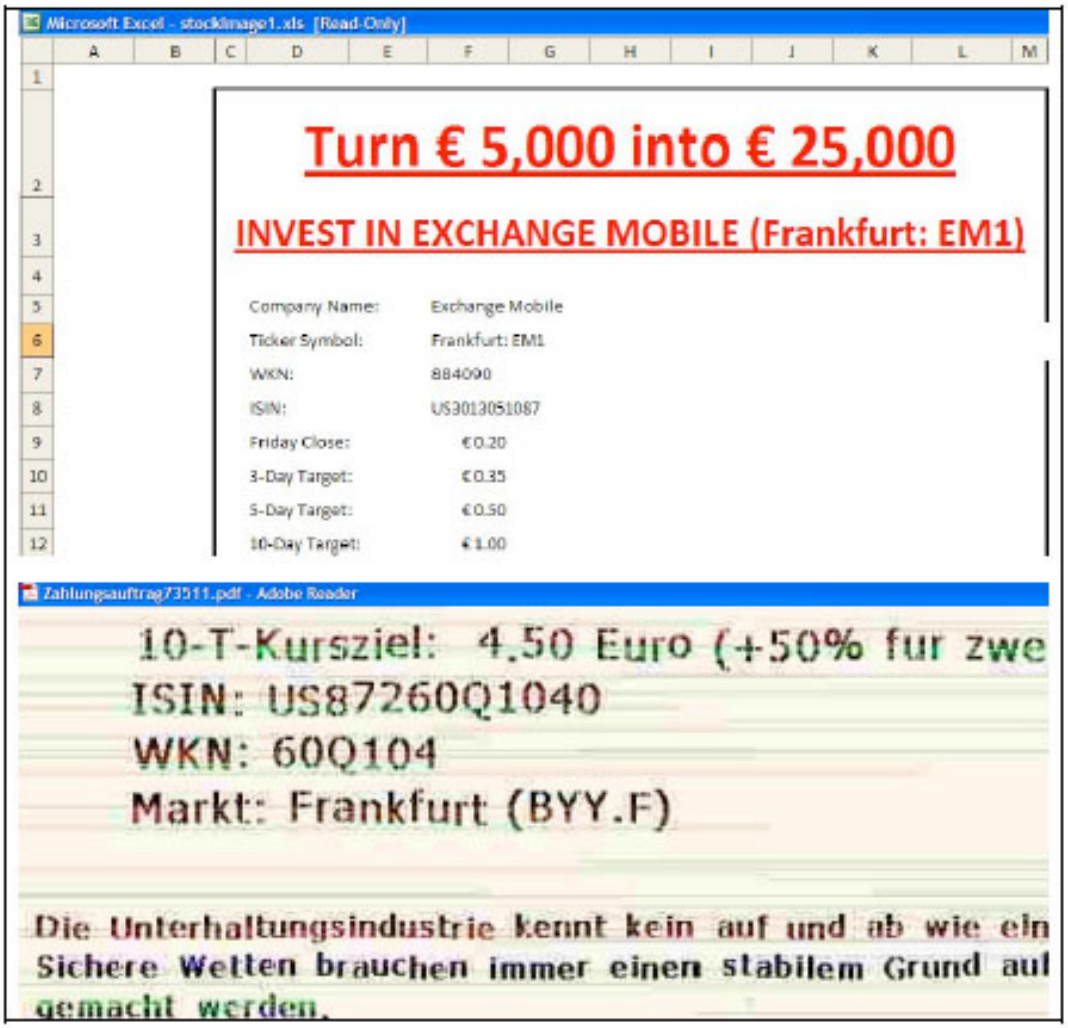
Symantec reported in May that image spam as previously defined had declined considerably in the preceding weeks. The decline in image spam has continued for the past few months, plummeting from 52% earlier in the year to about 15% of total spam. However, image spammers have not gone away.

In May and June, Symantec explained that spammers were using different techniques to reference spam images, such as directing readers to hosted image solutions. In June, Symantec observed the emergence of PDF image spam and has been actively monitoring the size of this emerging trend. In July, PDF spam accounted for between 2% and 8% of all spam.



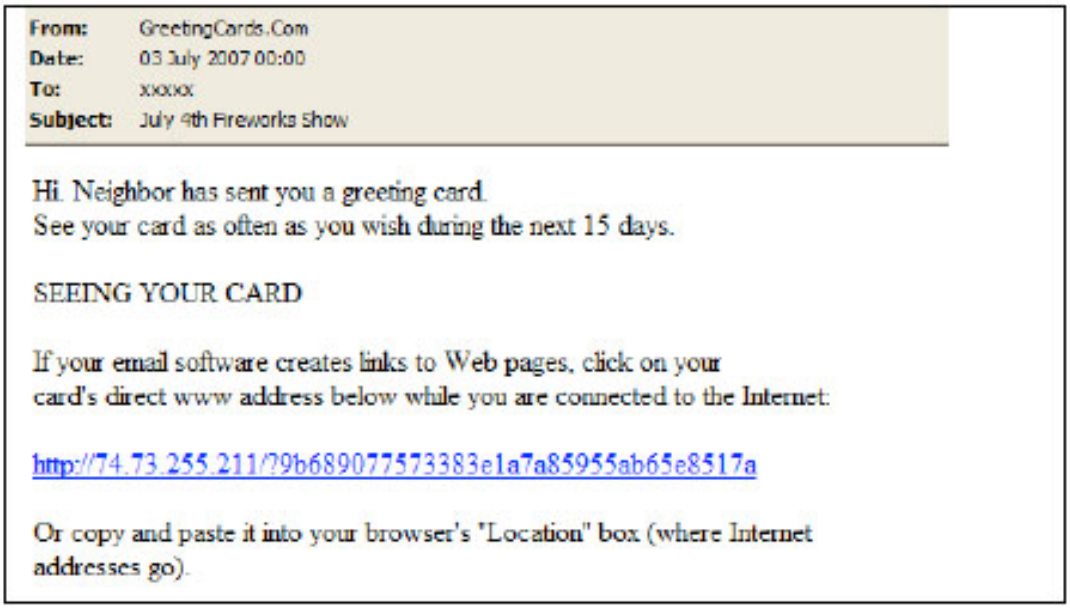
Excel And Zip File Spam Emerges

Spammers love playing the cat-and-mouse game and so, as expected, in July Symantec observed spammers using other attachments to promote stock and pharmaceutical spam. Stock and pharmaceutical spam were traditionally the most common spam types sent by image spammers. As image spam has decreased these spammers need some outlet to peddle their spam wares. The extent of spam messages using Excel and Zip files remains low at this time, but it indicates just how committed spammers are to evading antispam filters.



Greeting Card Spam Remains Spammers' Favorite

Greeting card spam containing links to viruses is not particularly new. However, it has been particularly virulent in the month of July with over 250 million of these spam messages being targeted towards a sample set of customers. The content of these messages included links ranging from everyday greetings to holiday-specific cards, such as the 4th of July. Each message contained a link to the "greeting card." The link in these cases was an exposed IP address, which is a clear indicator that it isn't a greeting card from an established and reputable Ecard service. When clicked, the link delivers a downloader—a program that accesses the Internet and downloads a Trojan onto the computer.



From: GreetingCards.Com
Date: 03 July 2007 00:00
To: xxxxx
Subject: July 4th Fireworks Show

Hi. Neighbor has sent you a greeting card.
See your card as often as you wish during the next 15 days.

SEEING YOUR CARD

If your email software creates links to Web pages, click on your card's direct www address below while you are connected to the Internet:

http://74.73.255.211/?9b689077573383e1a7a85955ab65e8517a

Or copy and paste it into your browser's "Location" box (where Internet addresses go).

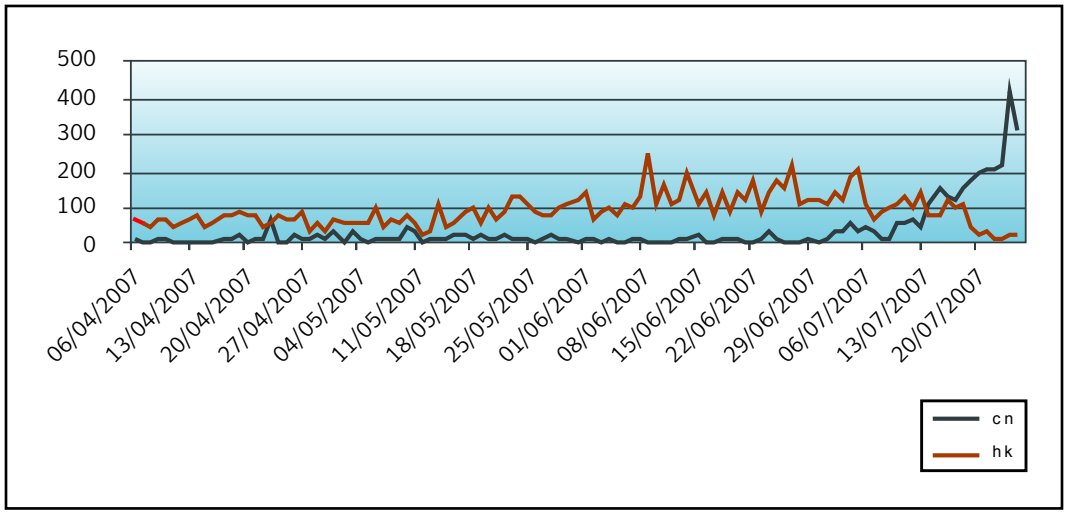
Significant Rise In Spam With URLs From Chinese Domains

In July, Symantec observed a significant increase in the number of spam messages containing URLs that use the top level domain (or "TLD) for China: 'cn.'

Possible reasons for this include:

1. Spammers have in the past used different TLDs in order to register specific names which represent their particular product or service. As the domain name gets blacklisted they may switch to another TLD.
2. Attempt to evade spam filters
3. As discussed in previous reports, spam is becoming increasingly localized with spammers using country TLDs to target a specific market or region.
4. In July, there has been a drop in URLs which have been using 'hk' TLDs. This could possibly be attributed to the recent enactment of the first phase of spam laws in Hong Kong on June 1st, 2007.

Spam Domains By TLD

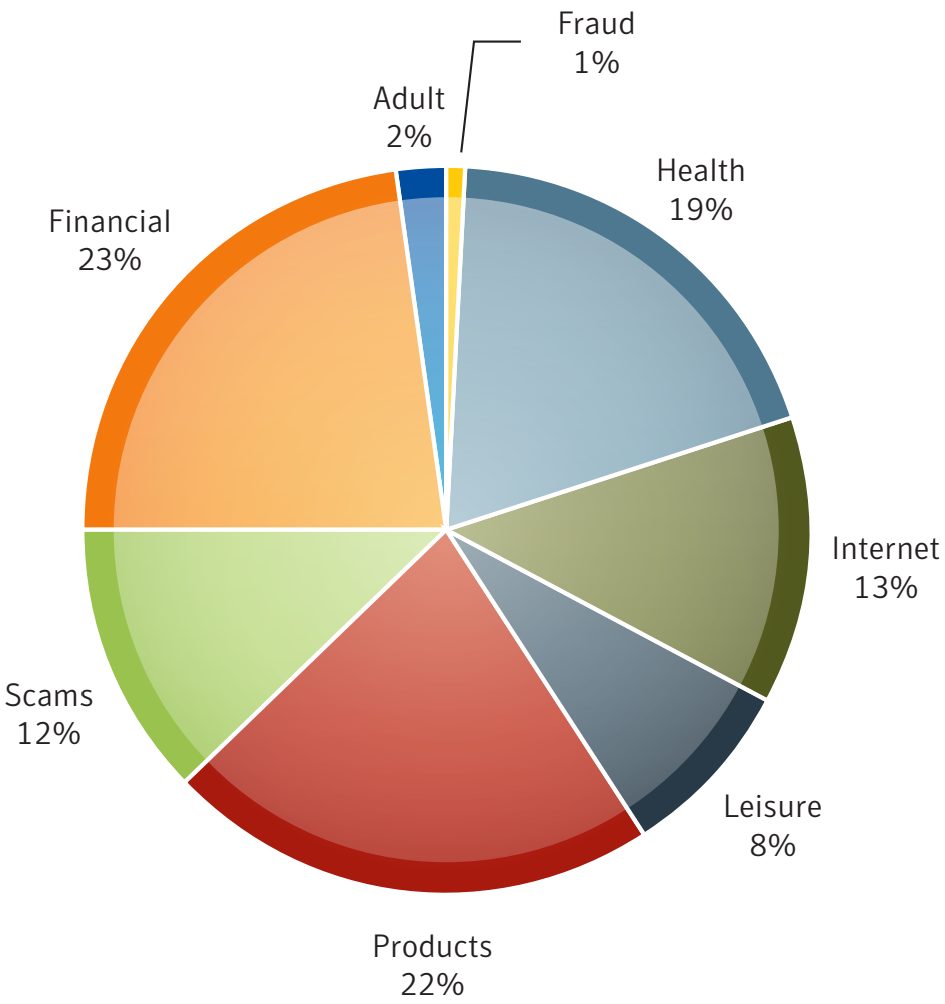


Spam Spotlight: Regional Spam Trends EMEA

There were some notable changes in EMEA spam activity in July compared to April, when EMEA trends were last discussed:

- Decreases in financial [8%] and adult [4%] spam
- Increases of 5% in both health and product spam

EMEA Category Count - Last 90 Days



The trend of localizing spam attacks to increase the target market continued in July with some particular interesting scenarios discussed below.

Casino Spam

European casino spam mentioned in the April Symantec State of Spam report continues with casino spam observed in Italian, French, and German

From: Euro::VIP::Casino
Date: 12 July 2007 11:49
To: XXX
Subject: Willkommensbonus - 400Euro!

EURO VIP Casino bietet Ihnen 4 mal 100% Ersteinzahlungsbonus auf bis zu 400€!

EURO VIP schafft jeden Monat neue Millionäre!

Kommen Sie um zu spielen!

http://mysterycasinos.com/lang-de/

From: Mario
Date: 16 July 2007 13:33
To: XXX
Subject: Ho appena scoperto uno dei più bei siti di casino online!

Ciao,

Ho appena scoperto uno dei più bei siti di casino online!

Appena ho fatto il mio deposito mi hanno accreditato 250$ di bonus, e mi hanno scritto che potrei riceverne altri 1000!

La grafica è bella e incredibilmente realistica... ho giocato a blackjack e alla roulette dal vivo (cioè con i croupier in carne ed ossa) e poi ho giocato alle stot e indovina... Ho vinto 10.000$ di jackpot!

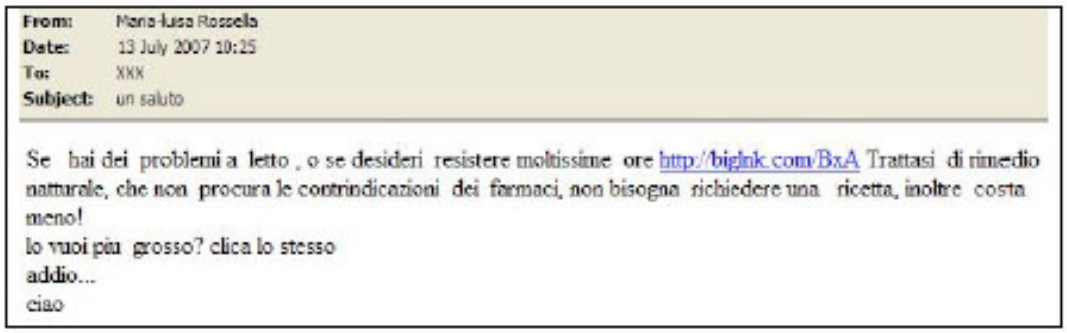
Non ci ho creduto fino a quando mi hanno fatto l'accredito sul conto un'ora fa.

Devi assolutamente provarlo!
http://supermagicjackpot.com/lang-it/

Mario.

Italian Medication Spam

Spammers believe there is a market for aphrodisiacs / enhancement medication products in Italy. The email below promises a "natural remedy." The attack was observed over several weeks with varying URLs/text in the body and subject lines designed to make the email look like it was from a friend.



From: Maria-luisa Rossella
Date: 13 July 2007 10:25
To: XXX
Subject: un saluto

Se hai dei problemi a letto , o se desideri resistere moltissime ore http://biglnk.com/BxA Trattasi di rimedio naturale, che non procura le controindicazioni dei farmaci, non bisogna richiedere una ricetta, inoltre costa meno!
lo vuoi più grosso? clica lo stesso
addio...
ciao

First UK Seller of the Apple iPhone?

This spammer claims to have top branded electronics goods including the Apple iPhone available from their UK warehouse at well below the recommended retail price. This of course is highly suspicious as the iPhone was not yet available in Europe at the time this report was published. Note that even though a UK postal address is apparently provided, contact is by email only – a further sign that this email is obviously a scam.

From: ELECTRONICS WAREHOUSE
Date: 24 July 2007 05:04
To: xxx
Subject: JUMBO SALES AND GET 2 APPLE IPHONE 8GB FREE

We are offering The Revolutionary Apple iPhone 8GB.....$290 per unit

NOTE: ALL ENQUIRES SHOULD BE DIRECTED VIA EMAIL

Emails:xxx@gmail.com
CC Emails:xxx@yahoo.co.uk

YACHTS CYAN
ELECTRONICS WAREHOUSE (UK) LTD
11 MURRAY STREET , CAMDEN ,
LONDON , GREATER LONDON , NW1 9RE

French Adult Messenger Program

Adult / dating spam purporting to be from lonely ladies trying to get in touch is nothing new. This French version is interesting though, asking the user to download a specific instant message program to get in touch with other like-minded people.