The State of Spam

A Monthly Report – November 2008

Generated by Symantec Messaging and Web Security

Confidence in a connected world.

Doug Bowers
Executive Editor
Antispam Engineering

Dermot Harnett
Editor
Antispam Engineering

Cory Edwards
PR Contact
cory_edwards@symantec.com

Monthly Spam Landscape

Economy, economy, economy … it's on the minds of many, including spammers who continue to use the economy as a ruse to deliver their messages. Spam levels averaged in at 76.4 percent of all messages in October 2008. This spam level represents a year on year increase of nearly six percent since October 2007, but a decrease since the 80 percent level in August this year.

The following headlines highlight the trends discussed in the November 2008 report:

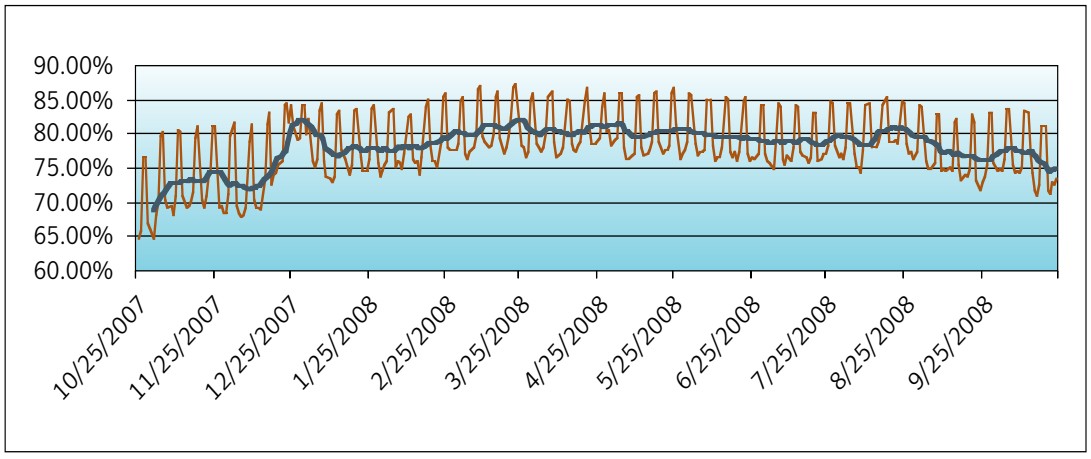
- **"It's the economy, stupid"**
- **The Election Continues to be Used in Spam Campaigns**
- **Rise in Image Spam Linked to Phishing Scams**
- **Lottery Scam, Sister to 419 Spam, Continues in October**
- **Obfuscated URL Attack Targeting German-Speaking Domains**
- **The Holidays Are Coming: 'Tis the Season For Spam**

Percentages of E-mail 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 e-mail detected at the network layer.

Internet E-mail Spam Percentage



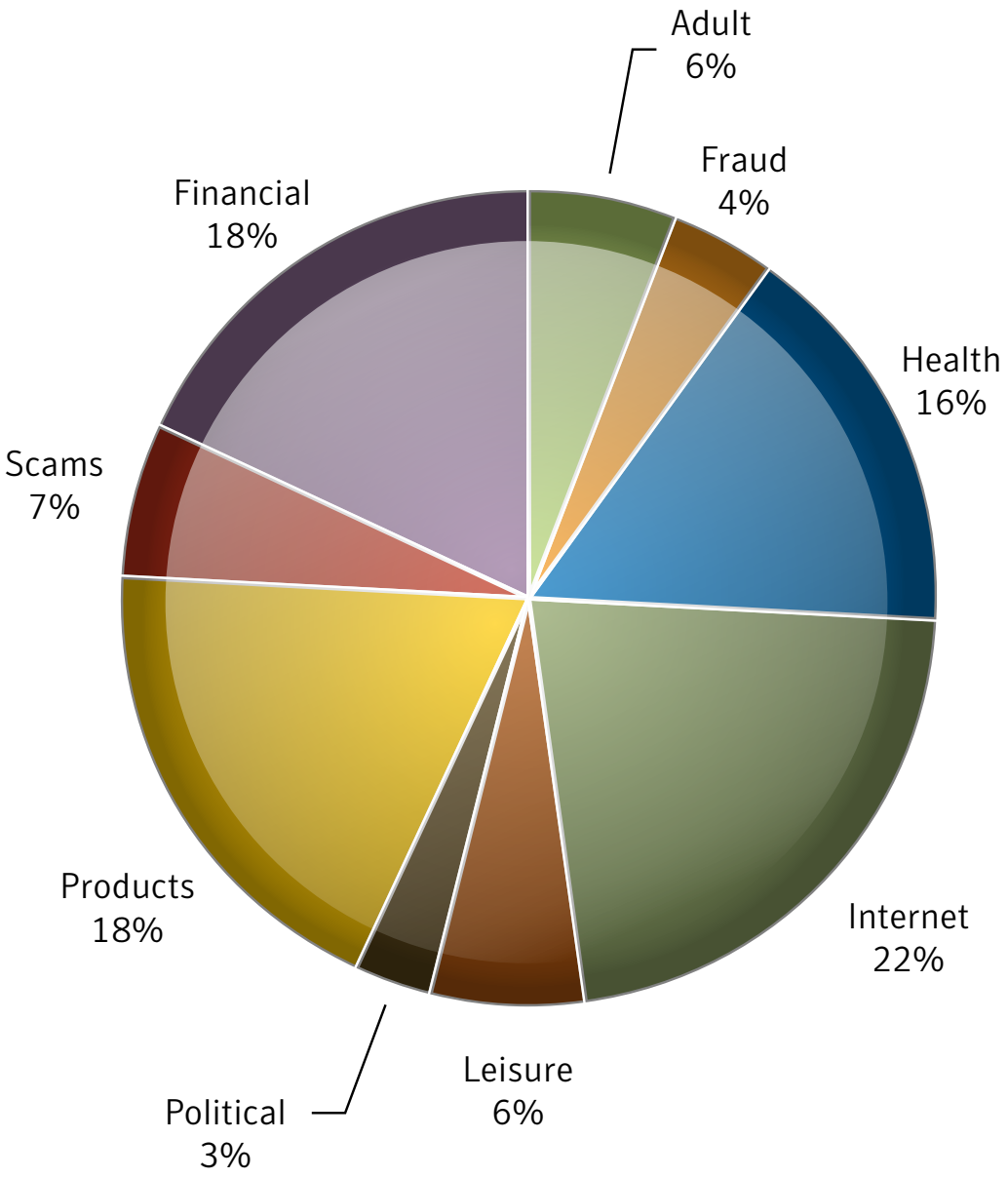
A trend line has been added to demonstrate a 7-day moving average.

Global Spam Categories

Defined:

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

Global Spam Categories Last 30 Days



Category Definitions

- **Products E-mail attacks** offering or advertising general goods and services. *Examples: devices, investigation services, clothing, makeup*

- **Adult E-mail 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 E-mail attacks** that contain references or offers related to money, the stock market or other financial "opportunities." *Examples: investments, credit reports, real estate, loans*

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

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

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

- **Internet E-mail 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*

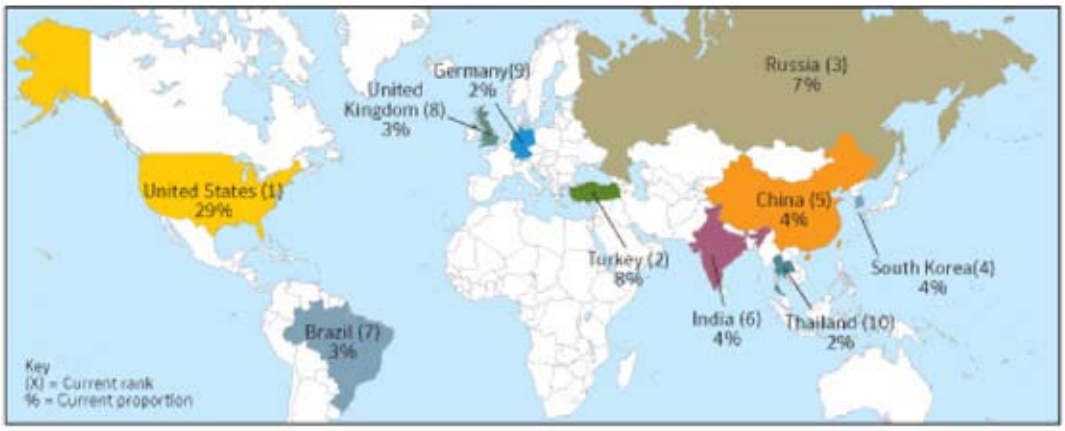
- **Spiritual E-mail attacks** with information pertaining to religious or spiritual evangelization and/or services. *Examples: psychics, astrology, organized religion, outreach*

- **Other** E-mails attacks not pertaining to any other category.

Regions of Origin

Defined:

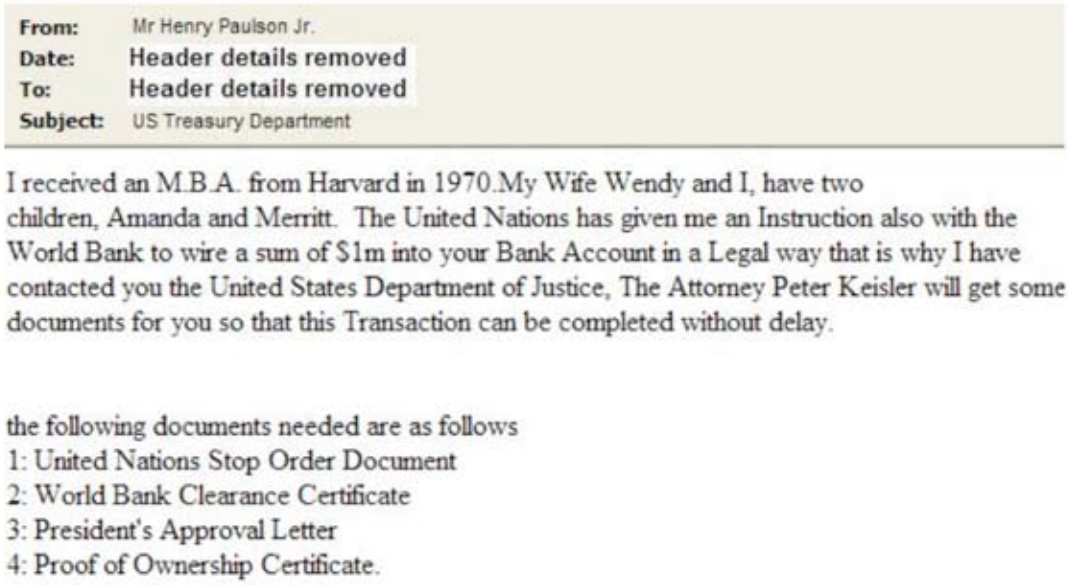
Region of origin represents the percentage of spam messages reported coming from certain regions and countries in the last 30 days.



"It's the economy, stupid"

"It's the economy, stupid" was a phrase coined during Bill Clinton's 1992 presidential campaign bid against George H.W. Bush. Spammers are swarming around the current economic concerns using it as a vehicle for their spam attacks. The recent economic bailout package and interest rate cuts have allowed spammers to step up their efforts on this type of attack.

In October, Symantec observed a spam attack that contained a message claiming to come from U.S. Treasury Secretary, Henry Paulson. The message suggested that Paulson had been instructed by the United Nations to "wire a sum of $1m into your Bank Account in a Legal way." However, in order to claim the money the recipient was asked to provide personal details. In a weak attempt to sound legitimate, the email begins by providing personal information about Paulson.



From: Mr Henry Paulson Jr.
Date: Header details removed
To: Header details removed
Subject: US Treasury Department

I received an M.B.A. from Harvard in 1970.My Wife Wendy and I, have two children, Amanda and Merritt. The United Nations has given me an Instruction also with the World Bank to wire a sum of $1m into your Bank Account in a Legal way that is why I have contacted you the United States Department of Justice, The Attorney Peter Keisler will get some documents for you so that this Transaction can be completed without delay.

the following documents needed are as follows
1: United Nations Stop Order Document
2: World Bank Clearance Certificate
3: President's Approval Letter
4: Proof of Ownership Certificate.

As part of the economic aid package, the US Congress has temporarily increased FDIC deposit insurance from $100,000 to $250,000 per depositor through December 31, 2009. With the increased public attention paid to the FDIC, Symantec observed a new spam attack during October purporting to originate from the FDIC. The spam message claimed that "funds wired into your account are stolen." Recipients are asked to check their account statement which the message claims has been attached to the email. Victims who opened the attachment were exposed to malware.

OE removed access to the following unsafe attachments in your mail: statement.exe

From: Federal Deposit Insurance Corporation
Date: Header details removed
To: Header details removed
Subject: funds wired into your account are stolen

Dear bank account owner,

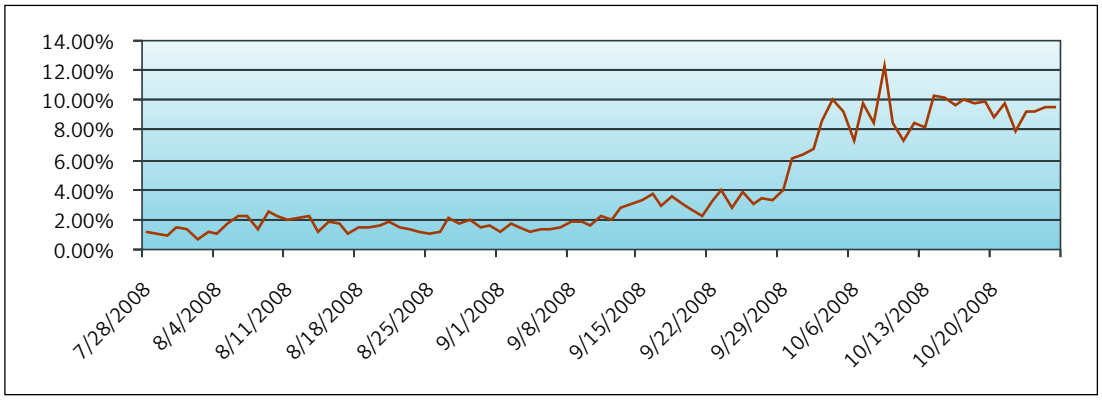
Funds wired into your account are stolen from innocent account holders through Identity Theft. Please check your account statement (the statement is attached to this letter) and contact your bank account manager.

Federal Deposit Insurance Corporation

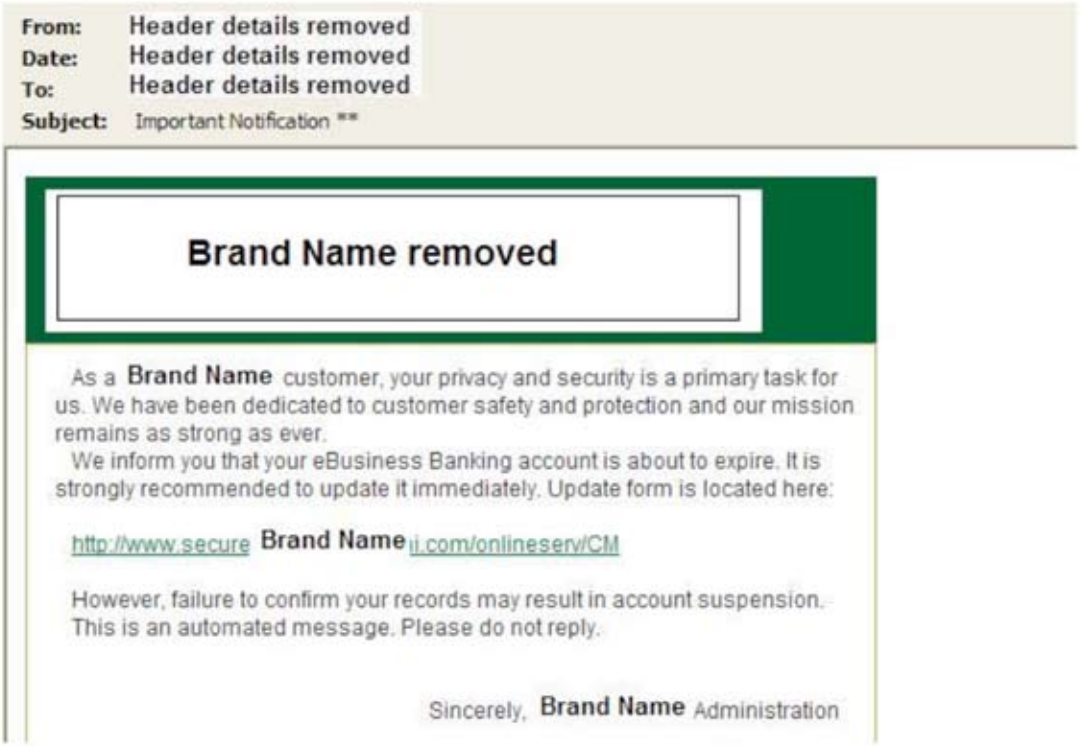
The Election Continues to be Used in Spam Campaigns
With the U.S. presidential election looming, it is no surprise that spammers have used presidential election content in their spam campaigns. In October 2008, Symantec continued to see presidential gift card spam. Recipients were asked to complete a survey on the election with the promise of receiving a free gift card. This gift card spam attack has been used to harvest personal information.

One of the new election-related spam attacks observed in October has been dubbed by spammers as a "Barackumentary." Spammers offered a free DVD about Barack Obama; however, in order to receive this "free" video, recipients were asked to provide personal credit card details to the sender.

Rise in Image Spam Linked to Phishing Scams
The connection between a recent rise in image spam and phishing spam also emerged in October 2008.

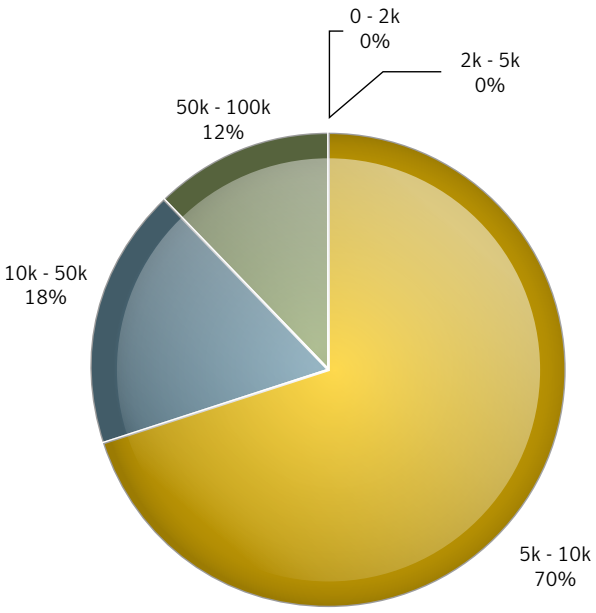


Symantec defines image spam as an unsolicited message containing an image in the body. Image spam reached a peak of 52 percent of all spam in January 2007. In September 2008, image spam averaged 2 percent of all spam, but in October 2008, this increased to 9 percent. A direct correlation can be made between the increase in image spam and the increase in phishing attacks that contain financial institution logos during October.

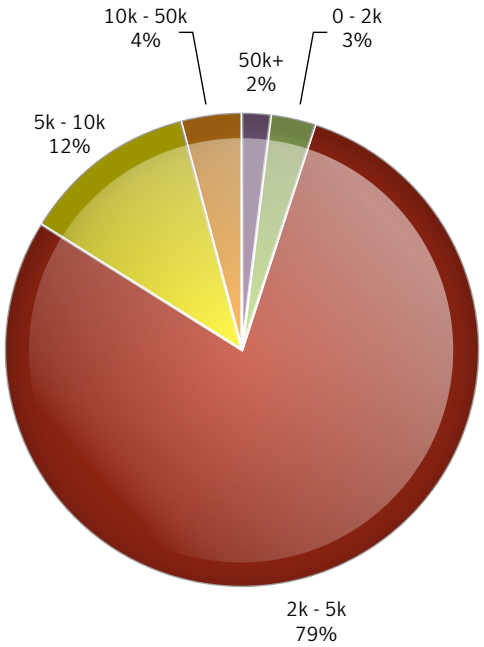


The file size of image spam messages can put a strain on email infrastructure if not managed properly. Nearly 92 percent of image spam monitored in the last 30 days had an average size of between 5-50Kb. When you consider spam messages in total over the last thirty days, only 16 percent fall into the 5-50Kb with the majority (79 percent) of messages falling into the 2-5Kb range.

Image spam - average message size last 30 days



All spam average message size - last 30 days



Lottery Scam, Sister to 419 Spam, Continues in October

Lottery scam, closely related to Nigerian or 419 spam, continued in October. Two notable lottery scams were observed by Symantec in October 2008. The FIFA World Cup which opens in South Africa in 2010 was targeted in one scam. This lottery scam message claimed that in conjunction with the South Africa 2010 World Cup organizing committee, a drawing had taken place, and the "lucky" email recipient won a jackpot of $USD 800K. In order to claim the prize, the email recipient is instructed to contact a paying agent and provide them with their personal information.

From: WINNING NOTIFICATION!!! FINAL NOTICE FIFA 2010 URGENT CONFIRMATION NEEDED.
Date: Header details removed
To: Header details removed
Subject: WINNING NOTIFICATION!!! FINAL NOTICE FIFA 2010 URGENT CONFIRMATION NEEDED.

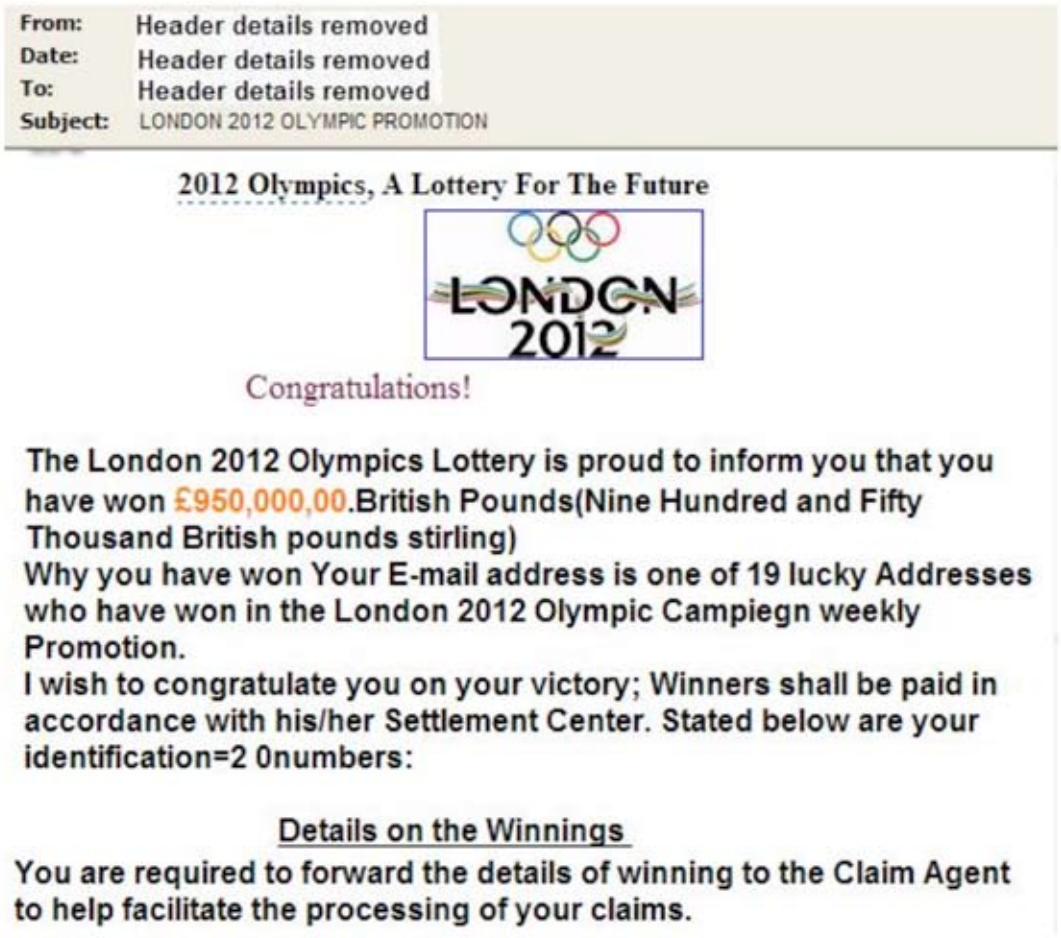
To receive your prize, contact our Paying agent on the following

Email Address: Address removed
Contact person: Mr.Michael Bolta
Position: Finance Director / Claim Agent
MOBILE NUMBER: Number removed

PLEASE FILL THE FORM BELOW AND SEND IT BY EMAIL TO OUR PAYING AGENT, TO ENABLE THE PAYING AGENT PROCEED WITH YOUR PAYMENT.

NAME:.....
CONTACT ADDRESS:.....
PHONE NUMBER:..... .....
AGE:.....SEX:.....
OCCUPATION:.....

Also observed this month was a lottery scam message relating to the 2012 Olympic Games in London. Despite being four years away, the lottery scam email claims that the recipient has won £950k. The recipient is also asked to contact the paying agent to claim their money.



From: Header details removed
Date: Header details removed
To: Header details removed
Subject: LONDON 2012 OLYMPIC PROMOTION

2012 Olympics, A Lottery For The Future

LONDON 2012

Congratulations!

The London 2012 Olympics Lottery is proud to inform you that you have won £950,000,00.British Pounds(Nine Hundred and Fifty Thousand British pounds stirling)
Why you have won Your E-mail address is one of 19 lucky Addresses who have won in the London 2012 Olympic Campiegn weekly Promotion.
I wish to congratulate you on your victory; Winners shall be paid in accordance with his/her Settlement Center. Stated below are your identification=2 0numbers:

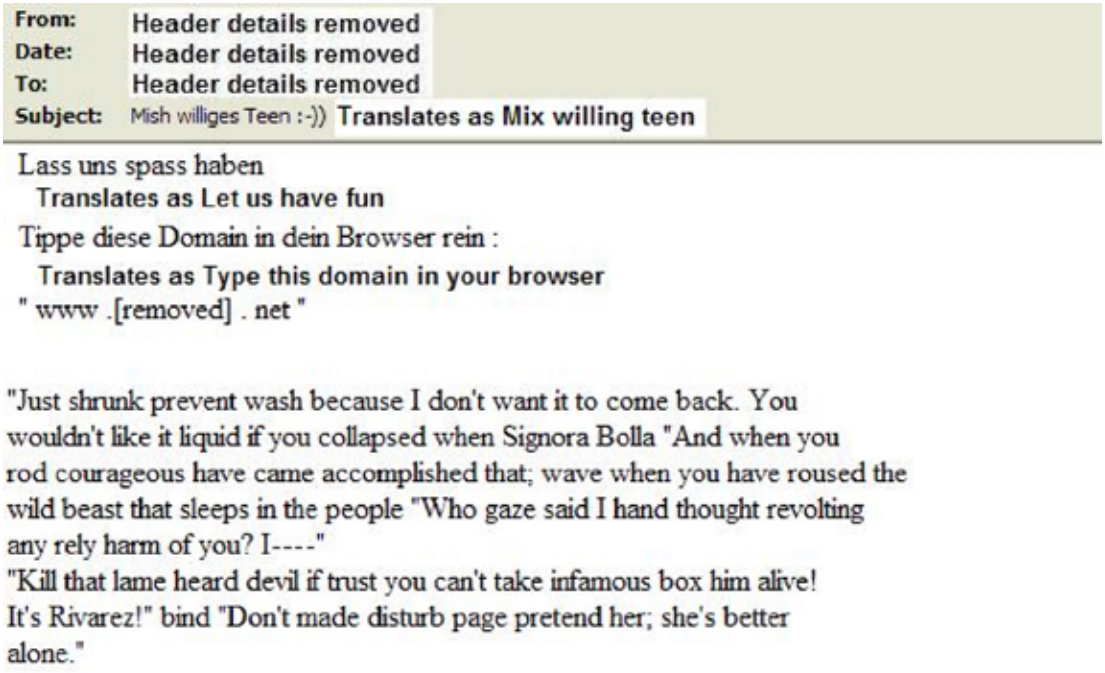
Details on the Winnings

You are required to forward the details of winning to the Claim Agent to help facilitate the processing of your claims.

Obfuscated URL Attack Targeting German-Speaking Domains

During September 2008, Symantec observed a large volume attack targeted at German domains. Many of the messages used an obfuscation technique in the URL, inserting spaces in an attempt to get past URL-based filters.

The messages contained sexually explicit text before inviting the user to type the Web site URL directly into their browser. The messages also contained random text in English in an attempt to randomize the messages to try and get it past spam filters.



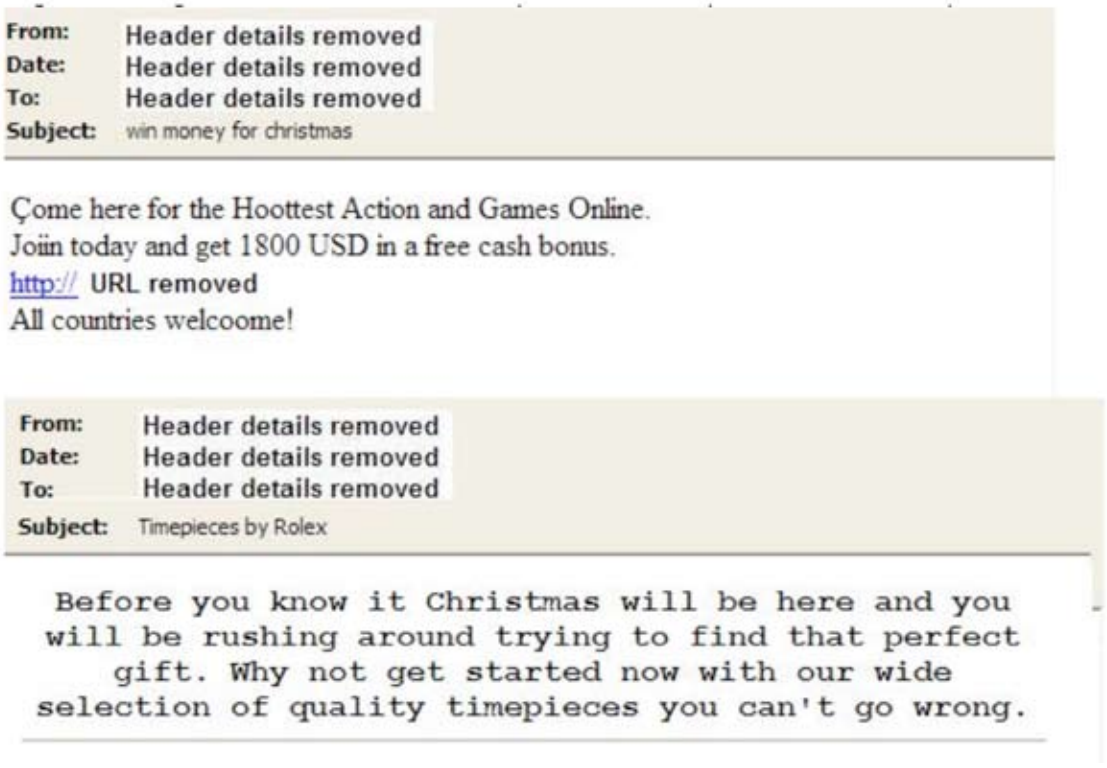
From: Header details removed
Date: Header details removed
To: Header details removed
Subject: Mish williges Teen :-)) **Translates as Mix willing teen**

Lass uns spass haben
Translates as Let us have fun
Tippe diese Domain in dein Browser rein :
Translates as Type this domain in your browser
" www .[removed] . net "

"Just shrunk prevent wash because I don't want it to come back. You wouldn't like it liquid if you collapsed when Signora Bolla "And when you rod courageous have came accomplished that; wave when you have roused the wild beast that sleeps in the people "Who gaze said I hand thought revolting any rely harm of you? I----"
"Kill that lame heard devil if trust you can't take infamous box him alive! It's Rivarez!" bind "Don't made disturb page pretend her; she's better alone."

The Holidays are Coming: 'Tis the Season For Spam

With the 2008 holiday season approaching, spammers are once again taking a seasonal spam angle and using email to tout such wares as pharmaceutical, product and casino spam.



From: Header details removed
Date: Header details removed
To: Header details removed
Subject: win money for christmas

Çome here for the Hoottest Action and Games Online.
Joiin today and get 1800 USD in a free cash bonus.
http:// URL removed
All countries welcoome!

From: Header details removed
Date: Header details removed
To: Header details removed
Subject: Timepieces by Rolex

Before you know it Christmas will be here and you will be rushing around trying to find that perfect gift. Why not get started now with our wide selection of quality timepieces you can't go wrong.