The State of Spam

A Monthly Report – June 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

The harsh economic times can be witnessed from every angle, with the rise not only in email spam, but also the sales of the actual lunchmeat product, Spam. According to NBC's Brian Williams, the spike in Spam sales is a huge economic indicator of the times, and families trying to do more with less. The exact same could be said for email spam. With spam messages accounting for over 80% of email in May 2008, the economic slowdown and its effects are definitely being targeted by spammers – preying on the hardships of people not only in the United States, but Worldwide.

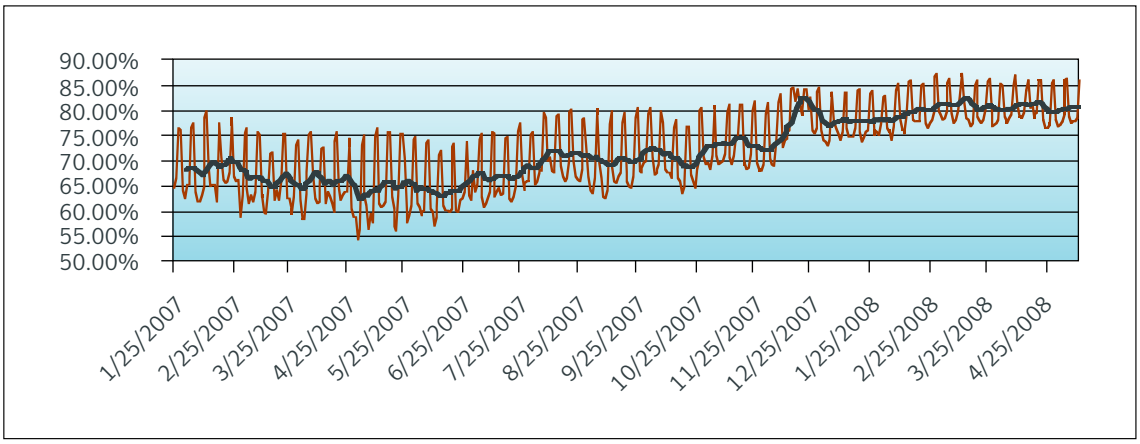
The Symantec June 2008 State of Spam Report notes the following trends:

- **Economic Climate Helps Fuel Spam Climate**
- **Phishing for Your Refund**
- **Natural Disasters Fail to Bring Out the Best in Everyone**
- **Spam Watch: Abuse of Google Brand Continues**
- **Champions League Final Tickets Scam**
- **Invoice Spam Tactics Evolve in the Face of Further Crackdown**
- **The Secret of Those Work-From-Home Job Offers**

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.



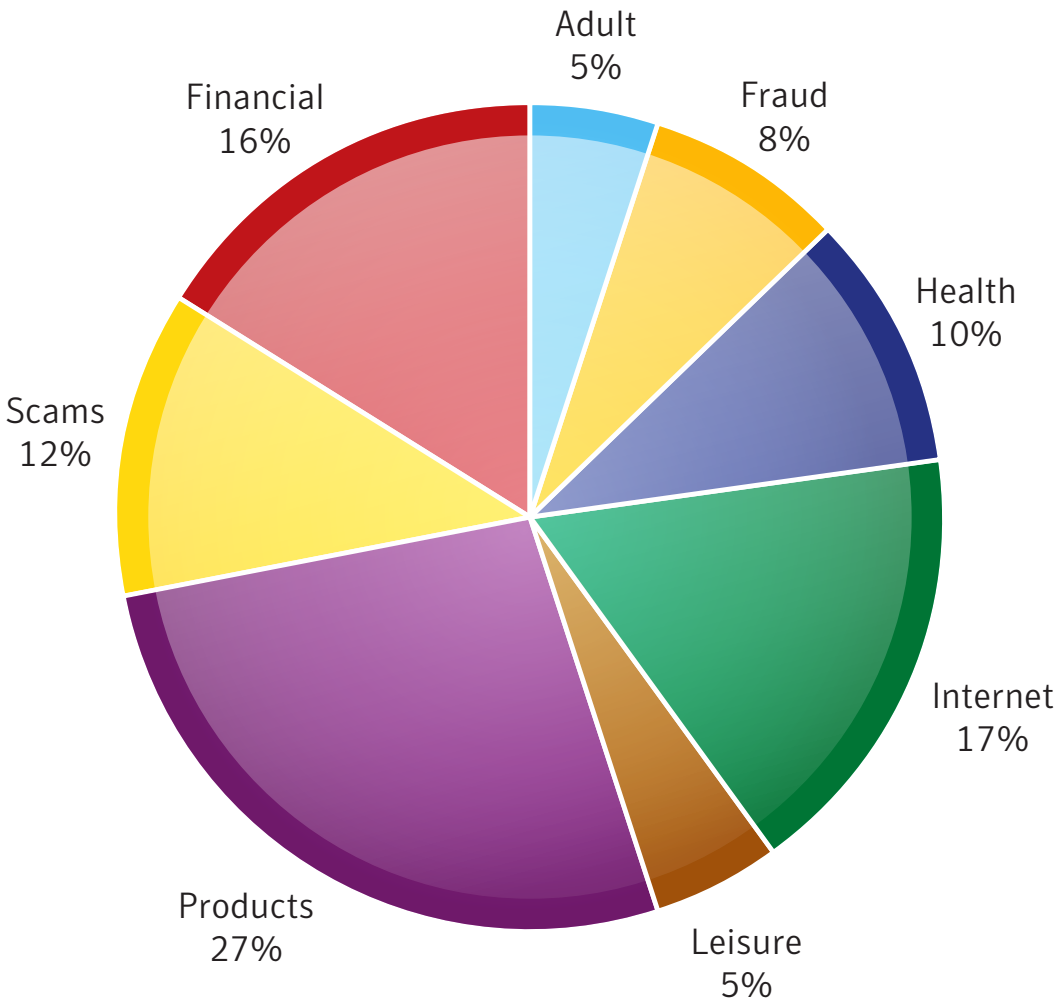
A trend line has been added to demonstrate a 7-day moving average.

Global Spam Categories

Defined:

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

Global Category Count last 30 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**

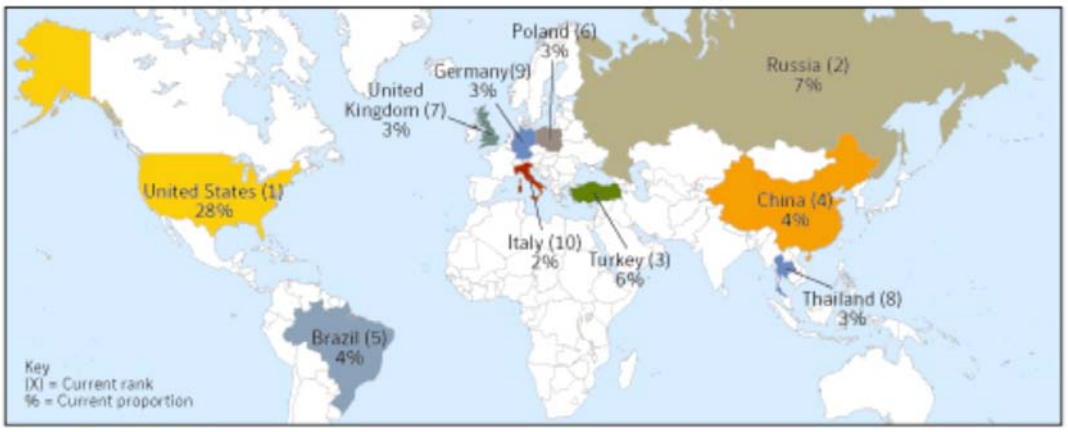
- **Political Messages** advertising a political candidate's campaign, offers to donate money to a political party or political cause, offers for products related to a political figure/campaign, etc. **Examples: political party, elections, donations**

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.

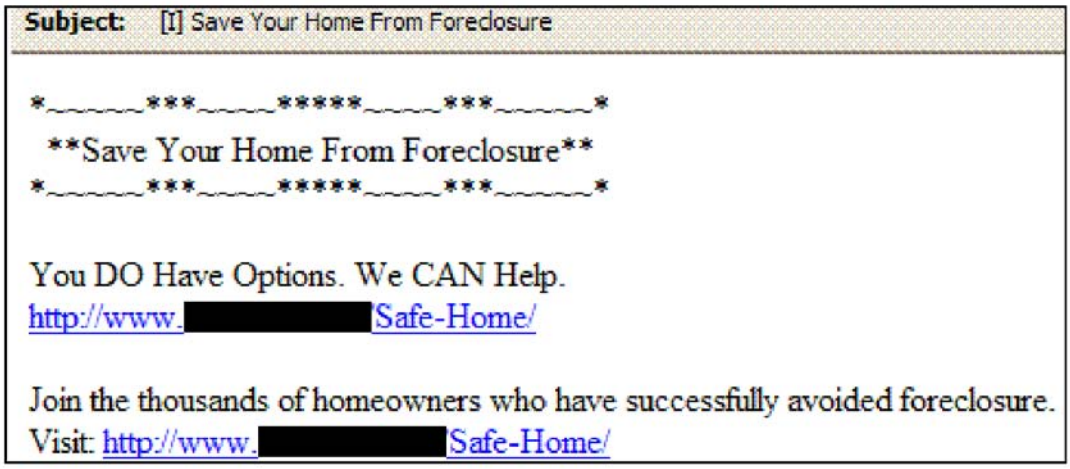
Global Claimed Region of Origin



Economic Climate Helps Fuel Spam Climate

Symantec first reported that some spammers showed an interest in the slowdown of the U.S. economy in October and November of 2007. In June 2008, Symantec continues to see spammers capitalizing on the economic slowdown in order to harvest personal information.

Some spammers have been trying to promote foreclosure loan remedies to "help" homeowners relieve their mortgage obligations and avoid negative effects to their credit ratings. In the following example, spammers ask end users to visit a website and fill out a form with their mailing address, phone number and the remaining balance of their mortgage loan. After clicking the submit button, a confirmation message appears and notes that a representative will contact them about their loan.



Subject: [I] Save Your Home From Foreclosure

*_____***_____*****_____***_____*

Save Your Home From Foreclosure

*_____***_____*****_____***_____*

You DO Have Options. We CAN Help.

http://www.[redacted]Safe-Home/

Join the thousands of homeowners who have successfully avoided foreclosure.

Visit: http://www.[redacted]Safe-Home/

The housing market slowdown is not the only element of today's economy that spammers are targeting. With the rise in fuel costs, Symantec has observed an increase in gas/fuel related spam. Among these attacks are offers of free gas, or gas cards and products that will help users obtain more miles per gallon, thereby reducing overall gas bills. In one recent example, spammers insist that with a particular device, the recipient can beat high gas prices by using water instead of gas to fuel their vehicle.

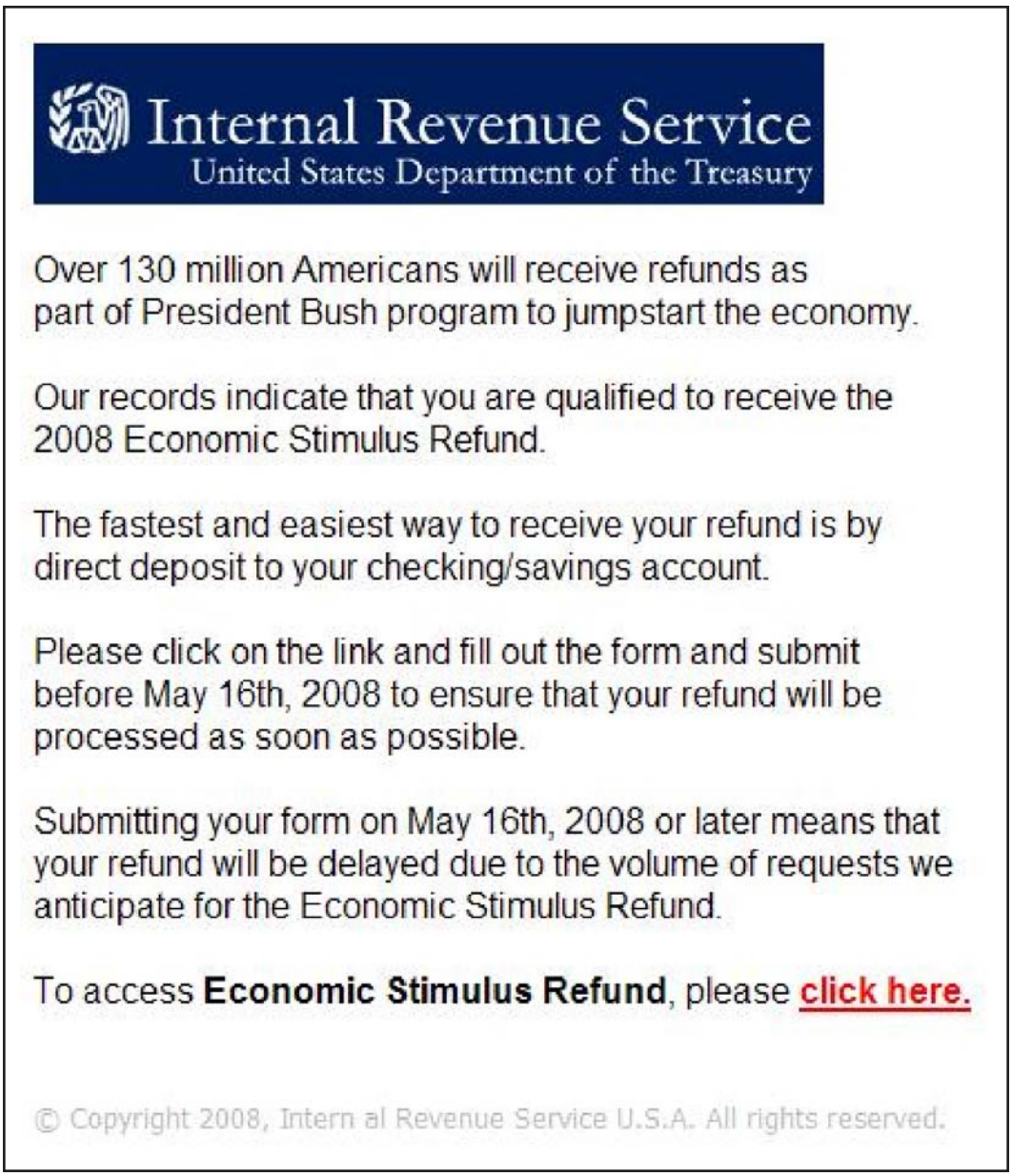
> Water instead of gas? Are you kidding? No, I'm not! Works with any model: gasoline, diesel, trucks, school buses. If you want to beat high fuel prices with a simple device anyone can install, please go to: http://xxxx.water4gas.xxxxx
>
> And, you can make money by signing up as an affiliate, too!"

The emails are unfortunately aiming to capitalize on the economic situation and prey on those in our society who are facing overwhelming financial pressures in today's economic market.

Phishing for Your Refund

In the past few months, there has been increased coverage of the U.S. government's economic stimulus package. Symantec has recently observed that some spammers are sending out phishing messages regarding the stimulus issued to taxpayers. The message contains a brief introduction of the stimulus package (similar to what a genuine I.R.S. letter might say), followed by a request from the spammer for the recipient to submit personal information. The message emphasizes that the refund will be delayed if the user does not submit the information before the given deadline.

Following the money! Once again this demonstrates that spammers consistently utilize current events to leverage their message legitimacy.



Internal Revenue Service
United States Department of the Treasury

Over 130 million Americans will receive refunds as part of President Bush program to jumpstart the economy.

Our records indicate that you are qualified to receive the 2008 Economic Stimulus Refund.

The fastest and easiest way to receive your refund is by direct deposit to your checking/savings account.

Please click on the link and fill out the form and submit before May 16th, 2008 to ensure that your refund will be processed as soon as possible.

Submitting your form on May 16th, 2008 or later means that your refund will be delayed due to the volume of requests we anticipate for the Economic Stimulus Refund.

To access **Economic Stimulus Refund**, please click here.

Natural Disasters Fail to Bring Out the Best in Everyone

The recent cyclone in Myanmar and the earthquake in China have prompted governments and individuals from all over the world to send aid to the affected regions. Predictably, this generosity has not gone unnoticed by spammers. In recent weeks, several spam messages have emerged related to these disasters.

A recent earthquake donation email scam requested donations for the China earthquake victims. The scammer used a legitimate website and inserted a fraudulent page under the root domain. When the user clicked on the URL in the spam message, they were directed to the fraudulent site and asked to make a donation.

Subject: [redacted] Because even a dollar can make the world a better place

On Monday, May 12, at 2.28 p.m. Beijing time (6:28 GMT), a major earthquake, measuring 7.8 on the Richter scale, jolted southwestern China's Sichuan Province. Several lower-scale earthquakes and aftershocks followed in the same area. The quake destroyed many buildings in the area, as well as infrastructure like communication towers.

According to the latest reports, more than 30,000 people have died and many more have been injured or are reported missing. Many schools were destroyed, including one that had at least 900 students in it. As authorities reach more remote areas, these numbers are expected to rise.

You can help those affected by countless crises around the world each year by making a financial gift to the [redacted] Response Fund, which will provide immediate relief and long-term support through supplies, technical assistance and other support to help those in need. Every dollar helps a soul.

Clicking on a URL link in the spam message brings the user to the following page

The cyclone in Myanmar also caught the attention of spammers. Approximately 4 to 5 days after the cyclone struck, charity spam emails similar to 419 spam emails emerged. The spammer in typical 419 fashion requested help from the recipient to distribute money to the victims of this tragedy in order to help ease his conscience.

Subject: Help Myanmar people

Dear friend,
I apologize if the content hereunder are contrary to your moral ethics,but i had to reach you through this medium because of the situation in my country which is very pathetic. my name is Mr.Zeyar Sandi a merchant from Myanmar (former Burma)I have been diagnosed with Pancreatic Cancer. It has defied all forms of medical treatment,

extended family members as well as a few close friends. I want God to be merciful to me and accept my soul so,i have decided to give alms to charity organizations especially after seeing what is happening in my beloved country Myanmar,I want you to help me distribute my funds to these suffering people.

Spam Watch: Abuse of Google Brand Continues

In the last year, Google has become a favorite target for spammers. In November 2007, Symantec reported the emergence of a technique where spammers manipulated Google's advanced search query and the "I'm feeling lucky" option to direct users to a spam site. In February 2008, Symantec reported that spammers manipulated parameters in Google URLs used for AdSense so that it re-directed users to a spam website. In May 2008, phishing emails purporting to come from the Google AdWords service emerged. June 2008 sees the abuse of the Google brand continue with the Google documents service becoming the latest target. Google documents is designed to allow users to create and share work online. In this particular example, a Google documents link is inserted into a spam email to direct users to a porn site.

Subject: asian honeys and more... ? tablefuls ;

Good Evening!

What's up?
I'm Chester.

ghetto girls play with themsellves.
Never seen beforee creampie pictures.

http://docs.google.com/View?revision=_latest&docid=[redacted]

http://docs.google.com/View?revision=_latest&docid=[redacted]

! SEXUAL CONTENT WARNING !

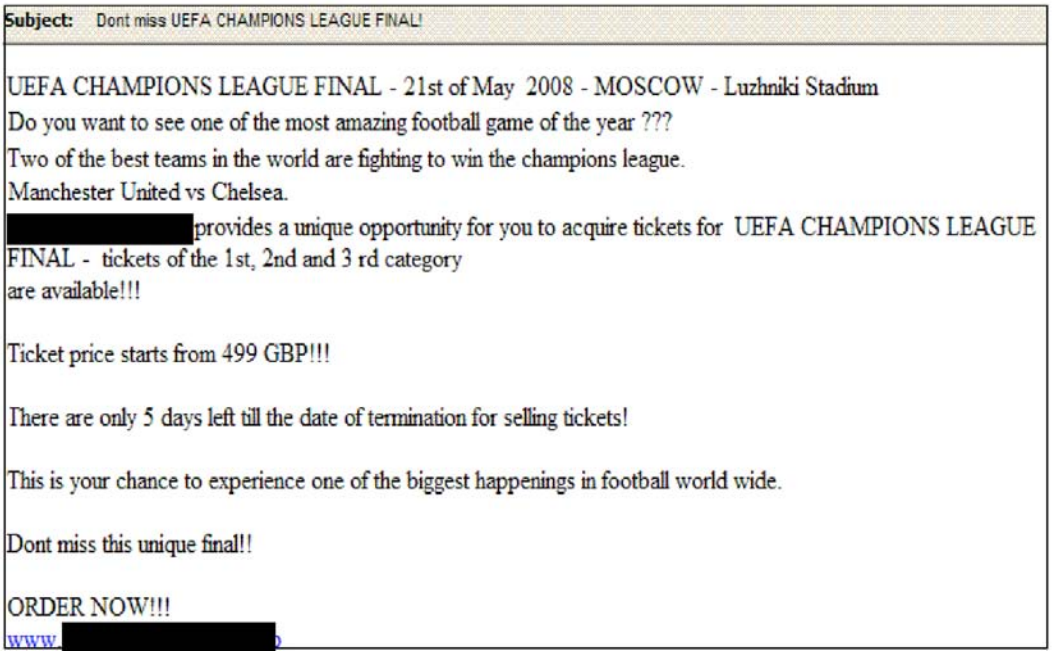
This website contains information, links, images and videos of sexually explicit material. If you are under the age of 21, if such material offends you or if it's illegal to view such material in your community we advise you not to continue.

Champions League Final Tickets Scam

The biggest football game in the European football calendar took place on May 21, 2008 in Moscow. Tickets were in big demand all over Europe for this event, and spammers certainly took notice.

Under the guise of a travel agency, the spammer offered the recipient "a unique opportunity" to acquire tickets for the game. The prospective customer was asked to click on a link to purchase the tickets and provide personal details. The recipient was then instructed to go to a legitimate online payment site to complete the transaction.

When the recipient paid for the tickets using the legitimate online payment site, the spammer requested that they email their name, surname and the unique online payment voucher number to the spammer in order to receive the tickets. The legitimate online payment website for the Champions League Final clearly states that the unique voucher number should never be emailed and only used on secure websites that accept their payments.



Subject: Dont miss UEFA CHAMPIONS LEAGUE FINAL!

UEFA CHAMPIONS LEAGUE FINAL - 21st of May 2008 - MOSCOW - Luzhniki Stadium
Do you want to see one of the most amazing football game of the year ???
Two of the best teams in the world are fighting to win the champions league.
Manchester United vs Chelsea.
[redacted] provides a unique opportunity for you to acquire tickets for UEFA CHAMPIONS LEAGUE FINAL - tickets of the 1st, 2nd and 3 rd category
are available!!!

Ticket price starts from 499 GBP!!!

There are only 5 days left till the date of termination for selling tickets!

This is your chance to experience one of the biggest happenings in football world wide.

Dont miss this unique final!!

ORDER NOW!!!
www.[redacted]

Invoice Spam Tactics Evolve in the Face of Further Crackdown

Illegal invoice offers for tax evasion purposes are one of the most frequently observed spam messages in the Chinese language. According to a press release from the Ministry of Public Security of the People's Republic of China, the Chinese police have cracked 2,963 cases involving the issuing or selling of fake invoices, detained 1,917 suspects, confiscated 10,510,000 fake invoices and smashed 101 illegal invoice printing operations in 2007.

Typically, illegal invoice spam contains either a plain text body or a graphic attachment. However, as criminals try to widen the audience for their services, Symantec has discovered spammers are taking advantage of free personalized e-card services to try and spread this type of spam message.


亲爱的 **商家** 您好：

您的朋友 **资料** 通过新浪邮箱给您寄来了一张他/她亲手绘制的涂鸦卡，

领取地址是: http://client.[redacted]m.cn/200801mailcard/show.php?id=[redacted]

新浪邮箱祝您合家欢乐，幸福安康！

Translation:

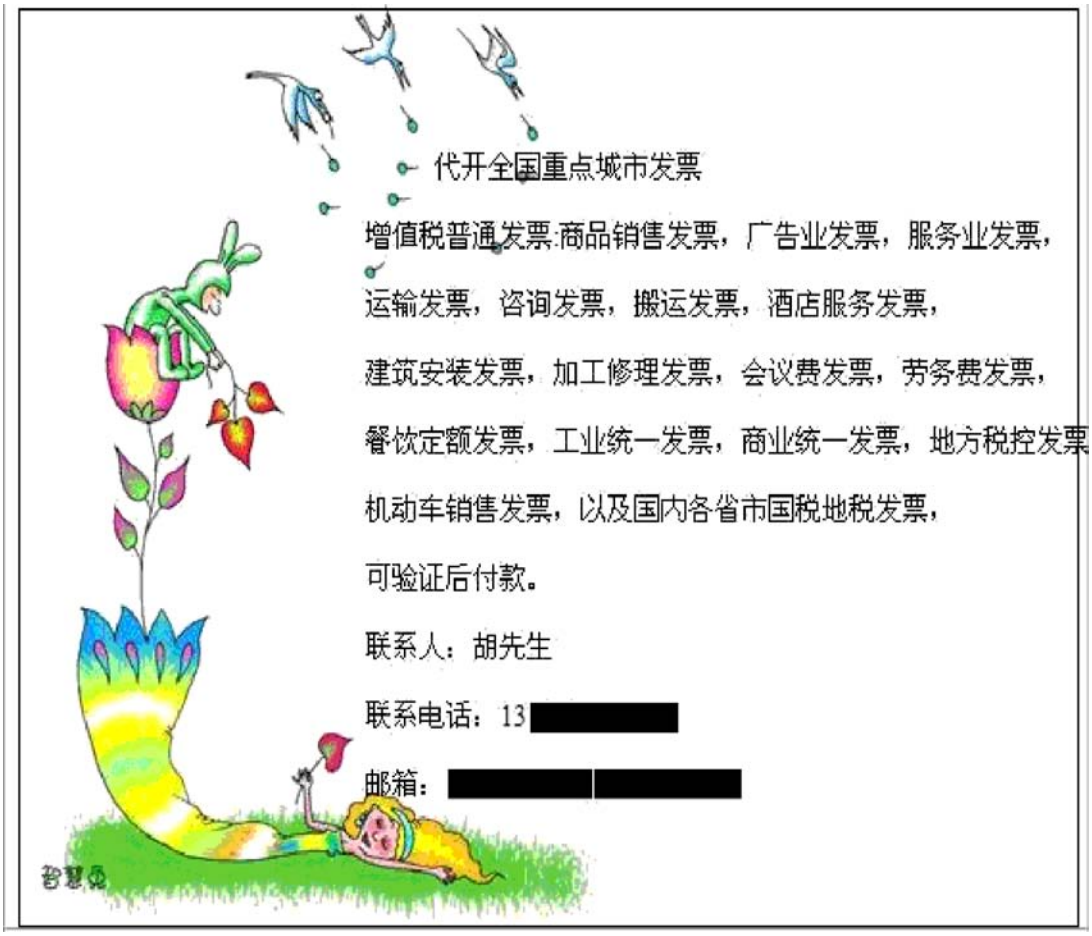
"Dear Store Owner:

Your friend "Data" has sent you a hand-drawn e-card via X mail box.

Here is your pick up address:

http://client.xxx.com.cn/200801mailcard/show.php?id=42760

If the recipient clicks on the URL the following appears.



Translation:

Nationwide invoice service

Value added invoice: Sales receipt……..

Hotel service receipt…….

.

…. Property tax receipt

Legitimacy guarantee

Since August 2006, the Public Security Department of the People's Republic of China has launched a series of special campaigns against spreading illegal information by texts or faxes concerning issuing or selling fake invoices. As the Chinese government continues to tighten its policies, spammers try to find new ways to avoid antispam filters and attract new victims.

The Secret of Those Work-From-Home Job Offers

Have you ever received an email offering you the ability to make extra income on the side for just a few hours per week, and wondered what it was all about? Well, spammers may just be looking for people to respond to their emails, or have non-suspect countries with bank accounts handle transactions for them.

This type of attack has shown no sign of decline in Italy since we reported it in our February State of Spam report. In this particular variation, the email claims to be from a Swiss watch shop selling watches of "prestigious" brands. One has to wonder who would trust this email, considering the text uses incorrect Italian, and a non-professional email address. However, considering the on-going popularity of the attack, some recipients are obviously tempted.

From: ghellere
Date: 29 May 2008 00:06
To: [removed]
Subject: 170 EUR alla settimana per 2 ore di lavoro al giorno.

Ciao,
Siamo il negozio svizzero di orologi. Dal 2002 ci occupiamo della vendita di orologi di marche prestigiosi. Ora ricerchiamo collaboratori. Vi proponiamo di collaborare con noi.
Vi presteremo istruzioni dettagliate.
Sareste interessato a ricevere informazioni in merito alla nostra proposta? Scrivete al guesto e mail JuliusdBeattyefzc696@gmail.com
Saluti,
- Monica